ID: 877850
Sample Name:
IntelCpHeciSvc.exe
Cookbook: default.jbs
Time: 05:01:56
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

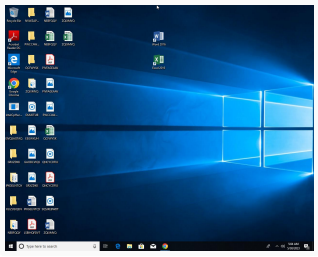
Windows Analysis Report

IntelCpHeciSvc.exe

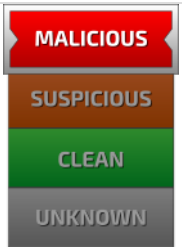
Overview

General Information

Sample Name:	IntelCpHeciSvc.exe
Analysis ID:	877850
MD5:	6b4a5a412e90…
SHA1:	7796314ed7b9…
SHA256:	62271e4b8eeb…
Tags:	exe
Infos:	



Detection



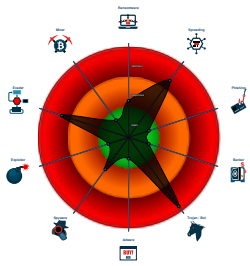
Nanocore, Neshta

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Neshta
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Infects executable files (exe, dll, sy…
- Drops PE files with a suspicious file…

Classification



Process Tree

- **System is w10x64**
- IntelCpHeciSvc.exe (PID: 5760 cmdline: C:\Users\user\Desktop\IntelCpHeciSvc.exe MD5: 6B4A5A412E90721FBA5170A25CAEFBD4)
  - IntelCpHeciSvc.exe (PID: 6824 cmdline: "C:\Users\user~1\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe" MD5: 7F00E9819E4B205654B46E0090E6763E)
- svchost.com (PID: 7040 cmdline: "C:\Windows\svchost.com" "C:\PROGRA~1\DHCPMO~1\dhcpmon.exe" MD5: 36FD5E09C417C767A952B4609D73A54B)
  - dhcpmon.exe (PID: 4728 cmdline: C:\PROGRA~1\DHCPMO~1\dhcpmon.exe MD5: 7F00E9819E4B205654B46E0090E6763E)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
neshta	Neshta is a 2005 Belarusian file infector virus written in Delphi. The name of the virus comes from the Belarusian word "nesta" meaning "something."	No Attribution	**http://** https://threatvector.cylance.com/en_us/home/threat-spotlight-neshta-file-infector-endures.htmlhttps://www.mandiant.com/resources/pe-file-infecting-malware-othttps://www.virusbulletin.com/virusbulletin/2014/08/bird-s-nesthttps://www.virusradar.com/en/Win32_Neshta.A/description	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.neshta

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "7d265ee0-5eff-4ffb-9f35-947e4a7e",
  "Group": "Default",
  "Domain1": "",
  "Domain2": "googleusercontent.ddns.net",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
IntelCpHeciSvc.exe	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
IntelCpHeciSvc.exe	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth (Nextron Systems)	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
IntelCpHeciSvc.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
IntelCpHeciSvc.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
IntelCpHeciSvc.exe	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
Click to see the 5 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth (Nextron Systems)	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	MALWARE_Win_Neshta	Detects Neshta	ditekSHen	• 0xa0e0:$s1: Delphi-the best. Fuck off all the rest. Neshta 1.0 Made in Belarus. • 0xa1a8:$s2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
Click to see the 455 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42d85:$a: NanoCore • 0x42dde:$a: NanoCore • 0x42e1b:$a: NanoCore • 0x42e94:$a: NanoCore • 0x5653f:$a: NanoCore • 0x56554:$a: NanoCore • 0x56589:$a: NanoCore • 0x6f013:$a: NanoCore • 0x6f028:$a: NanoCore • 0x6f05d:$a: NanoCore • 0x42de7:$b: ClientPlugin • 0x42e24:$b: ClientPlugin • 0x43722:$b: ClientPlugin • 0x4372f:$b: ClientPlugin • 0x562fb:$b: ClientPlugin • 0x56316:$b: ClientPlugin • 0x56346:$b: ClientPlugin • 0x5655d:$b: ClientPlugin • 0x56592:$b: ClientPlugin • 0x6edcf:$b: ClientPlugin • 0x6edea:$b: ClientPlugin

Source	Rule	Description	Author	Strings
00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x42e1b:$a1: NanoCore.ClientPluginHost • 0x56589:$a1: NanoCore.ClientPluginHost • 0x6f05d:$a1: NanoCore.ClientPluginHost • 0x42dde:$a2: NanoCore.ClientPlugin • 0x56554:$a2: NanoCore.ClientPlugin • 0x6f028:$a2: NanoCore.ClientPlugin • 0x431b2:$b1: get_BuilderSettings • 0x5b4cf:$b1: get_BuilderSettings • 0x73fa3:$b1: get_BuilderSettings • 0x42e69:$b4: IClientAppHost • 0x43223:$b6: AddHostEntry • 0x43292:$b7: LogClientException • 0x5b43e:$b7: LogClientException • 0x73f12:$b7: LogClientException • 0x43207:$b8: PipeExists • 0x42e56:$b9: IClientLoggingHost • 0x565a3:$b9: IClientLoggingHost • 0x6f077:$b9: IClientLoggingHost
00000002.00000002.580407779.0000000000409000.00000004.00000001.01000000.00000007.sdmp	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
00000000.00000003.341781141.0000000002184000.00000004.00001000.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x22b1:$x1: NanoCore.ClientPluginHost • 0x22ee:$x2: IClientNetworkHost • 0x5e21:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.IntelCpHeciSvc.exe.400000.0.unpack	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
0.0.IntelCpHeciSvc.exe.400000.0.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth (Nextron Systems)	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
0.0.IntelCpHeciSvc.exe.400000.0.unpack	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
0.0.IntelCpHeciSvc.exe.400000.0.unpack	MALWARE_Win_Neshta	Detects Neshta	ditekSHen	• 0xa0e0:$s1: Delphi-the best. Fuck off all the rest. Neshta 1.0 Made in Belarus. • 0xa1a8:$s2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]
3.2.dhcpmon.exe.134f6ddc.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 53 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Spreading

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

Drops PE files with a suspicious file extension

Drops executable to a common third party application directory

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival

Yara detected Neshta

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Stealing of Sensitive Information

Yara detected Neshta

Yara detected Nanocore RAT

Remote Access Functionality

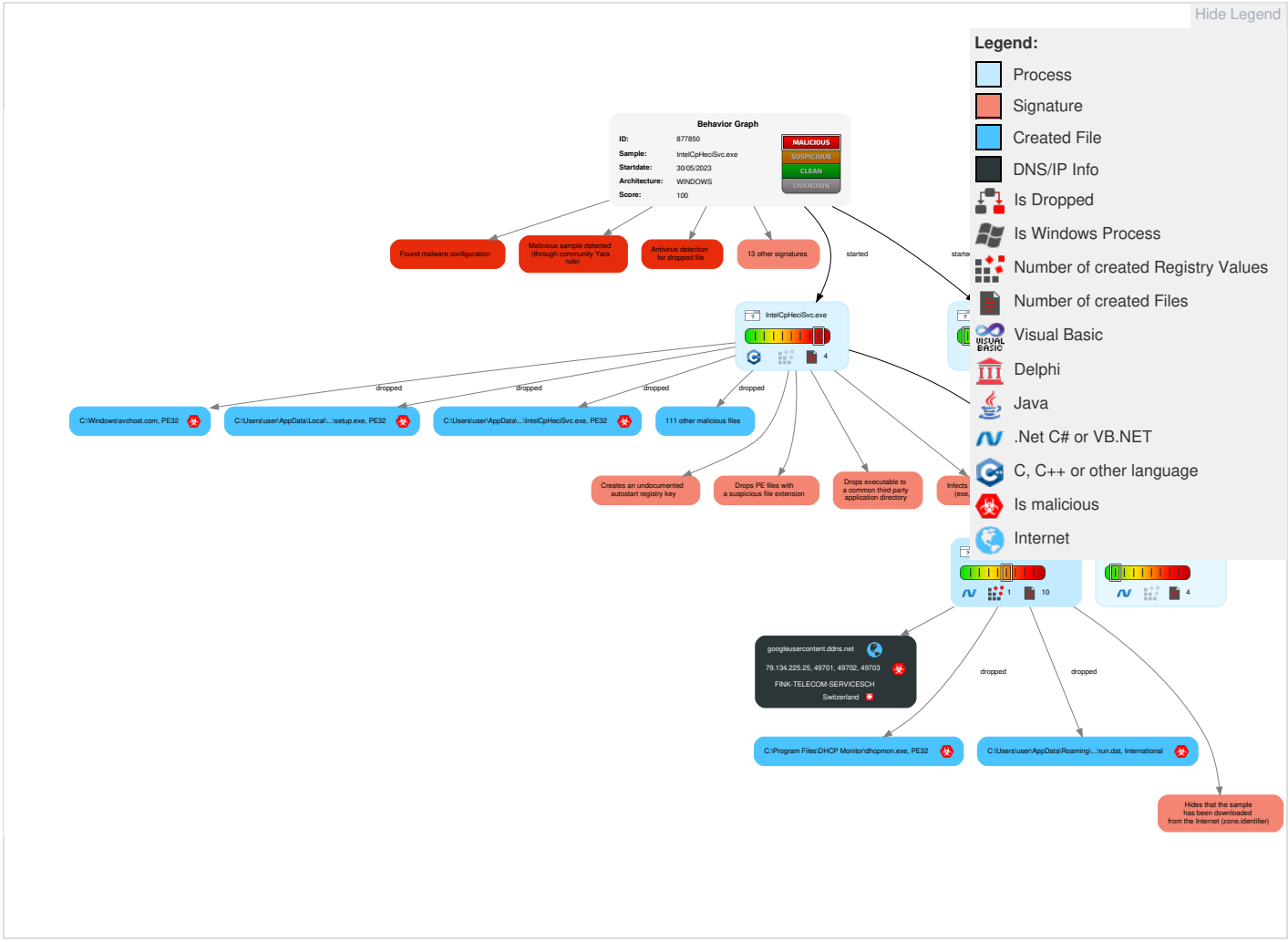
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 2 Process Injection	3 2 3 Masquerading	2 1 Input Capture	1 1 1 Security Software Discovery	1 Taint Shared Content	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

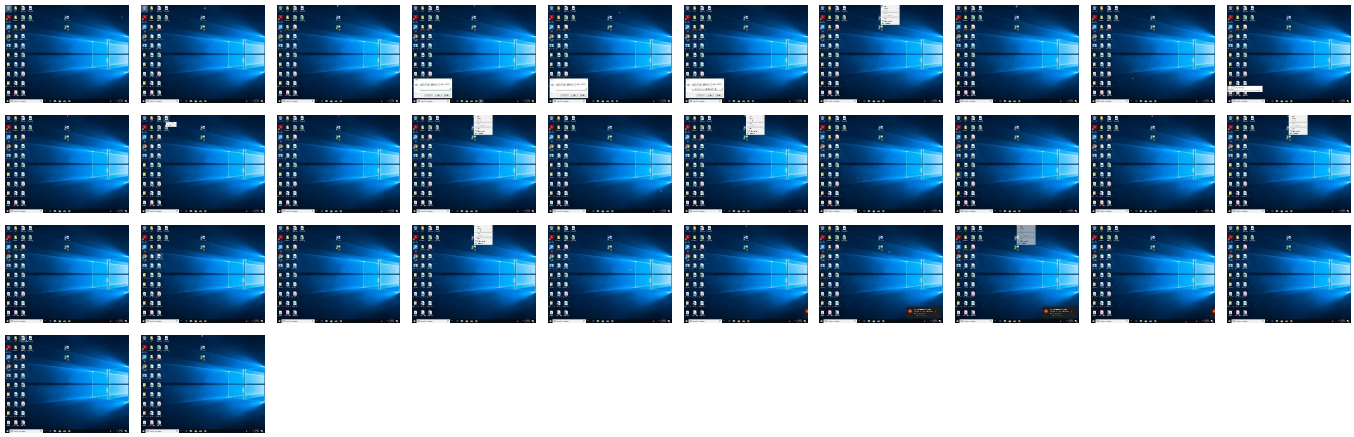
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IntelCpHeciSvc.exe	97%	ReversingLabs	Win32.Virus.Neshta	
IntelCpHeciSvc.exe	90%	Virustotal		Browse
IntelCpHeciSvc.exe	100%	Avira	W32/Neshta.A	
IntelCpHeciSvc.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Au3Info.exe	100%	Avira	W32/Neshta.A	
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Uninstall.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	100%	Avira	W32/Neshta.A	

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Au3Check.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	100%	Avira	W32/Neshta.A	
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	100%	Avira	W32/Neshta.A	
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Uninstall.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Check.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	96%	ReversingLabs	Win32.Virus.Neshta	
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	93%	Virustotal		Browse
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	98%	ReversingLabs	Win32.Virus.Neshta	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	100%	ReversingLabs	Win32.Virus.Neshta	

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChr omeNativeMessagingHost.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	98%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	96%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	98%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Au3Check.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Au3Info.exe	98%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	96%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	98%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\AutoIt3\Uninstall.exe	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	100%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	97%	ReversingLabs	Win32.Virus.Nesht a	
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	97%	ReversingLabs	Win32.Virus.Nesht a	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
googleusercontent.ddns.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
googleusercontent.ddns.net	2%	Virustotal		Browse
	0%	Avira URL Cloud	safe	
googleusercontent.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

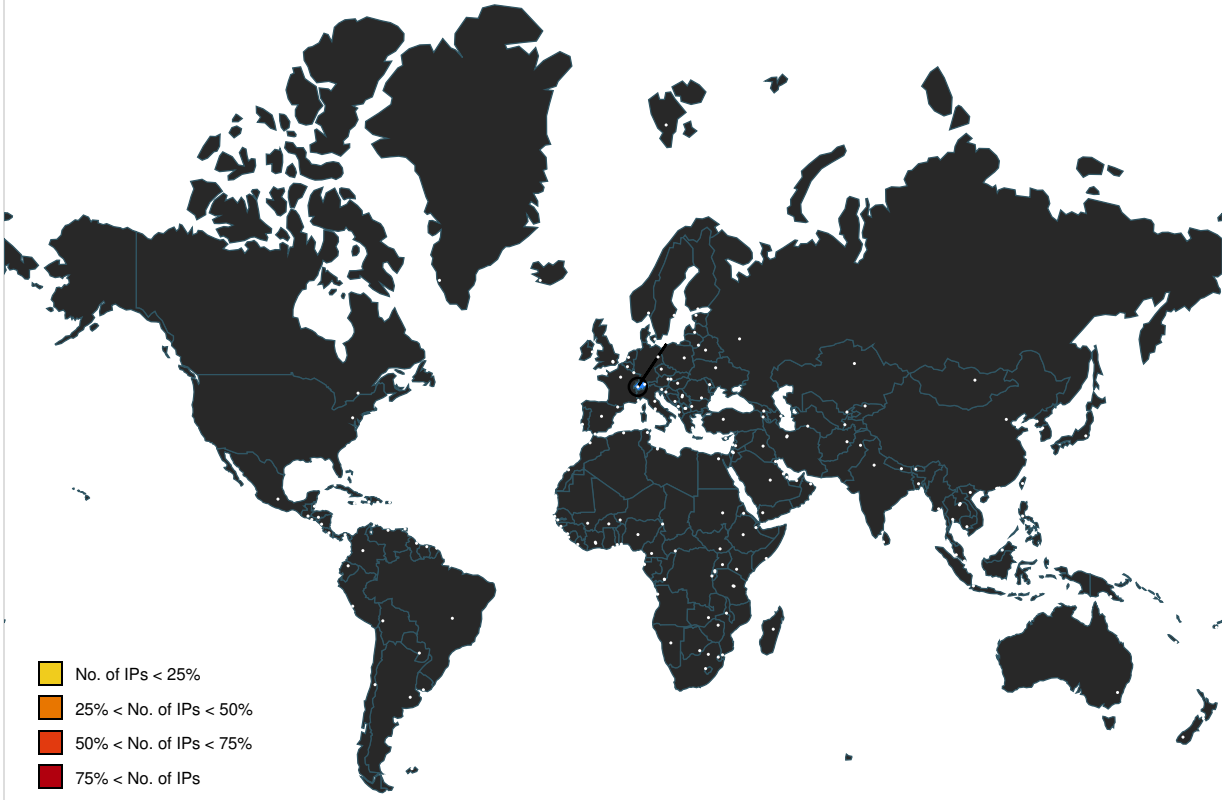
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googleusercontent.ddns.net	79.134.225.25	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
googleusercontent.ddns.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.25	googleusercontent.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877850
Start date and time:	2023-05-30 05:01:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	IntelCpHeciSvc.exe
Detection:	MAL
Classification:	mal100.spre.troj.evad.winEXE@6/118@21/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Execution Graph export aborted for target IntelCpHeciSvc.exe, PID 5760 because there are no executed function
- Execution Graph export aborted for target IntelCpHeciSvc.exe, PID 6824 because it is empty
- Execution Graph export aborted for target dhcpmon.exe, PID 4728 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:02:58	API Interceptor	684x Sleep call for process: IntelCpHeciSvc.exe modified
05:02:59	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	244400
Entropy (8bit):	6.5189732112846555
Encrypted:	false
SSDEEP:	3072:sr85COzMPySe8DnpeIPipoHbKvXWXz9LRnsaJUS+6wPXD3fxNW7gq5yGgA9SBtdv:k9OeySe8AlqpoHbnDns1ND97deKzC/y
MD5:	CC9086282AEB0488C6F400AFBF477D65
SHA1:	2086A61C1F68C0E36C0F9017C68528F2E2E866D7
SHA-256:	C2D2D8A74C726957A9DD578DCC0ED1C8B86B400822477B50FB2518923065E229
SHA-512:	564924ADF4BCE14AEB6EACAED8A2CC9D809CDBBDAC257EBA7B3AE19EA4A419619B20B67AA4675FC81558B76F210C6ED6EE3FE4E27F8A08D6782BB64D2E5E2078
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96% • Antivirus: Virustotal, Detection: 93%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278208
Entropy (8bit):	4.147085013209047
Encrypted:	false

SSDEEP:	1536:JxqjQ+P04wsmJCy0UjsWpcdVO4Mqg+aJRaCAd1uhNRBo+XrbQILFkbeumIkA39xb:sr85CyFGVO4Mqg+WDr8LRkgUA1nQZs
MD5:	CB74FFCED758250840C0BF149835FF35
SHA1:	8641E256AE71E51374B4BF24E317BDD64F3F26C8
SHA-256:	4EACD1204E4856AE01D64D58C93E7D45D8CA825C5A5AD1D998576A01ABFFAB8F
SHA-512:	47DE98059B44F7D2C98503FEF3BFADA075C0A25F3480A435B25A505CDB6D63D6969563A5BA0EA2005B6884A93EB3E7D4A293860D75921518D4FC5C33324E197
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	180272
Entropy (8bit):	6.296469804776402
Encrypted:	false
SSDEEP:	3072:sr85CjcYN0KD42sN7UGMovkIJ1jJ7LxcUUPm8aVJD37:k9jLN0K0NsjM7Lx5rJDr
MD5:	DBF433D30B00C342CDDA474F1E5C3551
SHA1:	F69AC3300AE37D7F60D5417525C9B33D4AAF6F2F
SHA-256:	F4160ECB4F7213BECFCD77518CCBB6DC05F8524CC9E6BEFBFC0F5546F1E9F134
SHA-512:	58BAAEF31A40E1530AEAA4021F1AA42EA21DAD1A525F9044A8D25AFA188E5F36E829B3312A81216A4F5500219E09D0A9F0072F50A925E6331A332FFD746BD67E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	340528
Entropy (8bit):	6.5900810039009725
Encrypted:	false
SSDEEP:	6144:k9jZAyHK0TcC+TKfVM7ZoL3czvPOU4MZY7TZoopFAdEm1t:2ZA2TcC5ko8aVoWAdEmT
MD5:	D2EB72B886C0E4516AD92D182472D3BE
SHA1:	760158C1460813FEB54EFF98E4C91D83EFBCB436
SHA-256:	F2A6D42CE2B2A77F3425D7259F0C3DFA0ED725C953D8D562DD0882591D2BA484
SHA-512:	2AF8D00EFA617937A160F2E1EC0B30411736B486835ED1368C07D6A8A3247B236C8E5D9CB7CAB8472A72294C44BDAD8BD9266661D313E12B612D902BE68384A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9516592
Entropy (8bit):	6.938557564832647
Encrypted:	false
SSDEEP:	98304:vDrMXEU5YPx01Dz2JhT1SbST3fX8ommgE6FWecuhd91h32zNX3CG9M:cEI2JhT1SeD/8BmgE6AkhdLh3QNd9M
MD5:	6469E2741DF733E5988971D908D1CB85
SHA1:	EBA742ED0EA23763C146377C0CF5464ADAD125D6
SHA-256:	1E9CCFA853279C8F8653ECD1BB17FAE5CAC2DE950E32B2EF61D24D9503184A78
SHA-512:	5F3D36CC3F6BFBF2687B4EB46A0332FD9915F2477565A09BDBB7879A1B88760FEDBCC8707C68B76B9CD5F830B91382D50BC3E328E86E2A66C011C2A3B654322 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2612784
Entropy (8bit):	6.11140851325999
Encrypted:	false
SSDEEP:	49152:+5j15HcNnCCZjaDpiA6E4O8b8lTDnlC+u:+5j1KCC4Dt
MD5:	5F33B528035F5DF3D4DEE014B93925F1
SHA1:	95AA78A7CC348A0A675FF9E3E21912413D90D8F9
SHA-256:	B1FBC7B6394735885586EF3FFF94154FA426A65DA37EFD994AB495026A7D7E77

SHA-512:	9497DD0976E9C967169BEC3BAC5EEFA3ECE164338AB6FCFC1E734204229FD6C1C3EBE3F7917E2517675DDDD514801B6843135DCA8CE4C46AD34177C14A144 8A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	90160
Entropy (8bit):	6.34072613745348
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCQhUpMPub5+G92qoooZVq/LF:sr85COqSwgHVqDF
MD5:	FA7D79A2CF553CBFA0EB56C0DA7FBD02
SHA1:	1CB1B005CA1D42860C4D9CF7A5335651AF796D91
SHA-256:	BC90A5650BA265C27CB5881FCF46D278D77184BC73BC1E1B2D479848BBF58674
SHA-512:	45CA0A5A793F4AC1EF57C5A55073FAC75F22ACA8BF83423E49491EB4ED16CF0A2C109B178276433CB1E4513744EC3974256E1BBC809F1309E1E233BBDDD4C4 7
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6152240
Entropy (8bit):	6.6006137058553
Encrypted:	false
SSDEEP:	98304:kzWaiDMRWPaefvGQCB97iKezm9GIlsgCDlFXHhoswt7HPe8U:k+Ql9CzWr3Ws6PpU
MD5:	B4560A6288B179EC9DCA7A98C3FD7E8E
SHA1:	74D52D67CF2B54947D4390419E7F7EF3A10B48E3
SHA-256:	8FCFC6FDDB85BEB3B6C6482437DF418692A9601A8967FA129C6870E19AA954BE
SHA-512:	5B6D5E587D5F63CD6EA237CBCF1BC15FC378ADDA2E39C5E2348E9BB5D20DCA8384CAF8D0260BB5584CD248BA67EE7222A8CFECAC66B18ED703FE64F63B52 56C6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe, Author: ditekSHen

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	190512
Entropy (8bit):	6.576815762637232
Encrypted:	false
SSDEEP:	3072:sr85Cl8+4lW4L7c3BG7THxRvyAgnz8n3Nn7b4o4kbT93Kxj2:k9h4l/Lg3ovHxAcb4oJbNKxj2
MD5:	EF4F52F25DA99ABE7221141D567472AC
SHA1:	4CAF7D4FA8D3F6D759AAD9BAABB6F1DCBCCB397E
SHA-256:	7F116252DBF7798B76729BB155508174EC21A2FDC9E9E176374E0CF57BA5B0AF
SHA-512:	09114CB1242B1B06B531EB83D229BD6415BEBAA278CF63D72FACBE32C0D34B797784239BA788721CDCFDC128E522B95365CDF5C476667E2221336D0934FF5B8F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	140848
Entropy (8bit):	6.306221506765706
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC7ULU8+mFfaz1llPN5gWCP19NJ8cSLgpA3hKwYPRvGdIab:sr85C7ULomFfWlF+WCP1icSLgpG88b
MD5:	6B829BD673B03FB5D32E6A102BD00C54
SHA1:	409E57A015E4B1E2D359D2DB8EF576CC13748AFE
SHA-256:	C060AE6CE05CE15128F614480DF559671338E950AB8E5C6F425331B1F1C07634
SHA-512:	792538C3A821F0D66E5963228B672EF8AEBF95891473146E375E9BF22C171739A90B7BDD89552BF502802B22FBBA94BE6E6530406C420203F3164DD014F19AB9
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	260104
Entropy (8bit):	6.384747990341208
Encrypted:	false
SSDEEP:	3072:sr85CYl4dsOc6v2vTzwU+Pho86meq+FaSoB2+vSHr8qcVz5fzsC:k9r3PiY+Fa7BdvG1cT7
MD5:	4DDC609AE13A777493F3EEDA70A81D40
SHA1:	8957C390F9B2C136D37190E32BCCAE3AE671C80A
SHA-256:	16D65F2463658A72DBA205DCAA18BC3D0BAB4453E726233D68BC176E69DB0950
SHA-512:	9D7F90D1529CAB20078C2690BF7BFFAB5A451A41D8993781EFFE807E619DA0E7292F991DA2F0C5C131B111D028B3E6084E5648C90816E74DFB664E7F78181BC
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	395344
Entropy (8bit):	6.40974219406537
Encrypted:	false
SSDEEP:	6144:k9W3n0dK2NP0RHx8D98WTBPW8fF8oABm1nKZ0RsrI:WKhHSDeWTRW8fdebmqI
MD5:	8C753D6448183DEA5269445738486E01
SHA1:	EBBBDC0022CA7487CD6294714CD3FBCB70923AF9
SHA-256:	473EB551101CAEAF2D18F811342E21DE323C8DD19ED21011997716871DEFE997
SHA-512:	4F6FDDEFC42455540448EAC0B693A4847E21B68467486376A4186776BFE137337733D3075B7B87ED7DAC532478DC9AFC63883607EC8205DF3F155FEE64C7A9BE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	128160
Entropy (8bit):	6.34354996662028
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCWM2D57Kykf8d/R8Tyr5J5is7MDjrXDyO4zkm8dbHVLokF8iJTp:sr85CCQw/STyr5Jks7MvrMzkm8PL3Eo
MD5:	CCE8964848413B49F18A44DA9CB0A79B

SHA1:	0B7452100D400ACEBB1C1887542F322A92CBD7AE
SHA-256:	FE44CA8D5050932851AA54C23133277E66DB939501AF58E5AEB7B67EC1DDE7B5
SHA-512:	BF8FC270229D46A083CED30DA6637F3CA510B0CE44624A9B21EC6AACAC81666DFFD41855053A936AA9E8EA6E745A09B820B506EC7BF1173B6F1837828A35103D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	146416
Entropy (8bit):	6.360093562607092
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC9S7UmwuBLAefbVH8x+FOI31EmkIY2d5J6WUghEuireklhKsikg:sr85Cs7HN9fN8sFOE1Z5Y2966ilU9xL
MD5:	92DC0A5B61C98AC6CA3C9E09711E0A5D
SHA1:	F809F50CFDFBC469561BCED921D0BAD343A0D7B4
SHA-256:	3E9DA97A7106122245E77F13F3F3CC96C055D732AB841EB848D03AC25401C1BC
SHA-512:	D9EEFB19F82E0786D9BE0DBE5E339D25473FB3A09682F40C6D190D4C320CCA5556ABB72B5D97C6B0DA4F8FAEFDC6D39AC9D0415FDF94EBCC90ECDF2E5136A31
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	285168
Entropy (8bit):	6.108456726369133
Encrypted:	false
SSDEEP:	6144:k9P1UKupTu8ffMb0/GxsZfcJtqQ1UBZ6g:jK+HMYcytZh
MD5:	12C29DD57AA69F45DDD2E47620E0A8D9
SHA1:	BA297AA3FE237CA916257BC46370B360A2DB2223
SHA-256:	22A585C183E27B3C732028FF193733C2F9D03700A0E95E65C556B0592C43D880
SHA-512:	255176CD1A88DFA2AF3838769CC20DC7AD9D969344801F07B9EBB372C12CEE3F47F2DBA3559F391DEAB10650875CAD245D9724ACFA23A42B336BFA96559A548
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95216
Entropy (8bit):	6.254186124080135
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC66w8MghW4wNlu9HQIXsW/44:sr85C66w8oFlKwW//
MD5:	176436D406FD1AABEBAE353963B3EBCF
SHA1:	9FFDFDB8CC832A0C6501C4C0E85B23A0F7EFF57A
SHA-256:	2F947E3CA624CE7373080B4A3934E21644FB070A53FEEAAE442B15B849C2954F
SHA-512:	A2D1A714E0C1E5463260C64048BA8FD5064CFA06D4A43D02FC04A30748102FF5BA86D20A08E611E200DC778E2B7B3AE808DA48132A05A61AA09AC424A182A06A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	152112
Entropy (8bit):	6.146727203548715
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC9Mqf1X/8cxsNsWUd09dlwxiBLSPLQ7eti/kCXBIvpnJXCFgyf:sr85C9Mqf1XEcxJMciBx7mgkC+Jt6gA
MD5:	7E82408281FA552ECF495EF0711EA163
SHA1:	33AC8ACCCDD372B80174C0F64CF619D1FE62D07D
SHA-256:	7746601A09FABE22EDA2203402B7060640DF699E26F16534CE4726AF65A5040C
SHA-512:	C1CBB428FF3FDB1A6D15CE0FC59BC5AD0B8EA86FCA232FE43DCAF94C620907B314ED82BC018137DEFD51C744106BF55D5938253D675E7CE2C2BFA6DC6079B28
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Au3Check.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	238776
Entropy (8bit):	6.175509697860494
Encrypted:	false
SSDEEP:	3072:sr85CrpTjGuX7GVdw3ELPU5+WYPwmsDx5T4XT3CAOA3GeilfrV5EAVMczsELz7Vz:k9rtjGFPy8wjNADHrLEoznVz
MD5:	80E793F8DD96C3F7255E2A9BDA94C7A7
SHA1:	65BDD000FE4E96E53F6CBEDE262E2E899AB7370C
SHA-256:	1B813E873416521371C8CF5478BC29E7261EEB358EACCCC8AE19B073E7A9C2CA
SHA-512:	CE9AFCEE60708A4038FEDBC71E113A41FF0D9328737184C6E1D89863185F148CA8DAF8CEF53846391C7B6033734207D9EC4AE30B66F945ADB849CFDB0830B7E A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Au3Info.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	197808
Entropy (8bit):	6.521212414216342
Encrypted:	false
SSDEEP:	3072:sr85CJv5cyOZyW6RRWy4ZNC6ZraL3mU3FR5StHe+:k9h5tbXWBZw6ZraL3mh
MD5:	3C43C01C22830EA3151F6772436933DC
SHA1:	F4E5C82240FE2810D7C1490DA4C6F40FAC5DCB66
SHA-256:	309EF2E6F16A0797E02F5DD1B53540F2BB4BD5D5BDCD635663A2486FCE9EA1DB
SHA-512:	A88C3AB6D1CF9323581B84A98081D4DE5CE8DF6EEDE53131A902EFACCA7068214BDAFDB5ECEC43763EBAFE14BD79BBB6433326A07871DD8F74507DEB54DE 9DCA
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	217776

Entropy (8bit):	6.279671702068234
Encrypted:	false
SSDEEP:	3072:sr85CpHThgfQMdmFDCwpcGr/yryldXRWy4ZNC94QO9UKRGRLK:k9ZTOfZdmFDNS2aOpBZw9xKaK
MD5:	2D7B5026E966B9F095EFF2F6AB724367
SHA1:	6C0C7F22F8B40CFB1A1E14142E8C54A233AFF1A9
SHA-256:	8154E59A9B387176D020F6144254BE5FBD69351014AE64002F560CE744E48A5E
SHA-512:	8E7F5B9422A081D6AF1EBA221D413370EE42B6B5722B152DCB0BB5B7700F435359DC4484A725F2177FF6F3CA8840605EF6F78BC0A7411E333F418E84546F91CE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1377456
Entropy (8bit):	7.492762950137599
Encrypted:	false
SSDEEP:	24576:E0RJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNnGw:p89+ApwXk1QE1RzsEQPaxHNGw
MD5:	984FD2F9964FA1C220E32004FE066F12
SHA1:	94D45F3B036F6FBAD72F3F2350BF641F746725C0
SHA-256:	3C665DAB78B5F613D40A620957D493B2D133C3F37AF6D7ACBAD1F05CE6EF91FD
SHA-512:	63538A12B7B1CD06CA06EF498CC0F8813277CAD50A4F7D8B5D821D3FD93D04FBFC03918C6195825EF05B003A29C5D17FA2FACDE78ECC3060E0AC7AB0FAD79C5
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1418416
Entropy (8bit):	7.424737019812187
Encrypted:	false
SSDEEP:	24576:dBCnx+QJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNn6uioL:duxw9+ApwXk1QE1RzsEQPaxHNks
MD5:	97155B2E1EE1B3FD0EAA1EC515B180EC
SHA1:	41C5258AE0E982FBC20812B3738E4C58F6F4FE41
SHA-256:	FECD867EB0E79F6810F4E0748AC35BA0C0C8C605000A5284FA7F6D98F3E38EAF
SHA-512:	F997B9E8506A20DE2A2F80DB44E212C4BAFB4421869EA308F15DE9CA1639588D6E84A0F357001A7D2D4D27125E004F535B97B25F861039420E00A66F8ABA8FA0
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346624
Entropy (8bit):	7.904139028422803
Encrypted:	false
SSDEEP:	6144:k9ypXDXz7yIrozs0WuNd3ojusBdgnNW6r4F53ttuGENGFdVCLEYnPO1D7YYoSyZV:V9zGlmAjJdcH4j3ttzFdVCLNSfHoSWCG
MD5:	4D2A6099D369E478E6B97ECA38DF66FF
SHA1:	F8A2EFB513BC22A550E1DAADB7765D3691795D05
SHA-256:	E8657C5096C1D6059D7862D842C93EE9D7C16331EFBEC02C99BECA1ACEF0E4D7
SHA-512:	7BC01CBF7A591AAC71439A126940D1374B6BB49A3109651EB9525026EAB22AD70558FFB8723838C33830467D1B7DBE72E76BA84925BFECD405E10B83FFDF8A45
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160424
Entropy (8bit):	6.10165663615367
Encrypted:	false
SSDEEP:	3072:sr85C5y0L5hQCbIJqC3CJyoDjyYB78UAwBvm5:k9LgLk1B7XBv8
MD5:	F1C9F5DEE11DC9DBE65CFF99DB035B96
SHA1:	1E0736C1890BC81AD146FCDAA0A7B3481CA02CAB
SHA-256:	C20A680F2DEC0F5D917ECB0F72E8609BB30B3632AFD719969A86347C06D048A2
SHA-512:	B0782B2D3E830250A9CC782F6F90FB82B6AF99EBDF3FFB447C9AFB20F4971F4BCF48A2A562C107C1470A2854998116D6392FE59670773781F6AF1D02D9F9A25E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1055400
Entropy (8bit):	6.4225736655610195
Encrypted:	false
SSDEEP:	24576:dmUFhNcmLFj4svqaShRsUiTfjo5ya8j8s8:vGmxj4svqaShRibza8h8
MD5:	3E5A05A68FC9D6DF26689AC8A26C00FD
SHA1:	323355134CA0C548C774766C0D11C13E8A02FA21
SHA-256:	E200098DDDCB591E14643A48E8528C9A1790770D61FD4FA38D4A34C472E735DD
SHA-512:	54D90B22C330A6FB935BA844AAD8193DB2BD2F41360BF66CB34F3851E54F97E40EA406B9DE1C585F3115869C299D913CB1E4473AF3B9F3D7212EF386391B268
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1298432
Entropy (8bit):	6.68752077269718
Encrypted:	false
SSDEEP:	24576:3h7dtrjrICw9XuXo7beSTdt5xbX02uvfTXfBxrj3d5E/jKQvVj4YpdjYY0td7ktW:3ftnrICSooGSTD5xbX022fjBxrj3MA
MD5:	4D90BC4B9810CF47BE47D6C9DEC20FEB
SHA1:	3A78D864C9917DA386142FBA5CA7FA1342431B79
SHA-256:	F7247AB5D88EED3BA0CF6EA41E55FF75873FE7A9DE5C85E6A32C620E76F9D01C
SHA-512:	0D5C6F60E54B2F9D8380B712959585DAB9181072A3322591417C6E44F348347DAB37CB10C5CAC7BFA5668848E6BD40F2CD0B421E8DC2F9B0C45BC414DAC574 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Uninstall.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	108903
Entropy (8bit):	6.7724162065172395
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCWCrD5iTfMEgaGySODDvRit2RPYqa5pic6jXFdL2KiMceCry:sr85CWCrDI11VDDvBPA6jXFN2MceCry
MD5:	2F9A43267EEBE21AC9F33B334433234D
SHA1:	08FEBD231E86E54CFDEBFCB03204314209397CB5

SHA-256:	6AADAB36A7040EDD91B13CAEC0097C643A71FB2F09940E8F9FE303E1CEDC1D0C
SHA-512:	C4CB3299BAE2979C22BFD2A825DD3D68B2A93234E78DB60572BA5FAECB525FD0F088703FE055E316835A3A8908D126F641CB5DB830EF7D21387373E3CB5B52(6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	464936
Entropy (8bit):	6.360683839248502
Encrypted:	false
SSDEEP:	6144:k9DQcslnC3znG+xfbMgyGn7LiJdKkAtyKuskePvX2Zp7DmuXYvr6ys/pJYCf:PlnCxjMyn72/KkAtydem3nM6BHYo
MD5:	6A02DFAEE140217151427D7301E61289
SHA1:	793B86D11BD13C12BB8D60E01F36A21A3CE2F728
SHA-256:	7F474C8C7643AB7A5AA9CDB27A93ECB7CA3F23ED8AF916CB7FC5905F572CF732
SHA-512:	A4E21A104CD9C772799AA84632EE821A0B0CF859721F6C3482BC532221DFFFDA8186888BBB9B52391E3E9F472631F3C5320A7DD4976ED49674F8BF322E4A9DA(
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	125456
Entropy (8bit):	6.243532552718445
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCV66hOAsu3ocbxghFd9fP4LXRxQyEvzDmxvuLX+:sr85CkkOAsu3v44dOyEv/mxmLO

MD5:	72B958CB9CDCD8F788037A5E9F226F91
SHA1:	F0452F038280AF6E832B89D53228499806B84774
SHA-256:	650B8F0A205CE0C5A8EFC661F8105BC2C6AE5371DE6ACC482E6858B95531BF81
SHA-512:	1CB545931288E5D4C19BF1D710807B7ED661247EDF33CC63AFE4149A687FD0AA9D120A953D8237BAEFC293E55A532A6FFAC0DEE182CA7F9245FE1D0A3BC05D F3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	472912
Entropy (8bit):	6.5565215741761556
Encrypted:	false
SSDEEP:	12288:wnFwHDxPuHqaTWl/jFucTsoY7BN3Hti0jKWo:wnFwHGiILFucTO7BN3H00jKWo
MD5:	D18639427E57710E5DFF1D1CC15993EE
SHA1:	1F34D641139878D1C07511448D6A4F7B5D751DFB
SHA-256:	F03903002FE82F426A6F63BF70E75CE389023F061575707AF553B78106F1948E
SHA-512:	38740928C49154A960878F12E330C65475A65EA48A83516D16004F1E67196CC96D2BF31D9B669FA59DC3F0E14C872F90EE2AA477A21AD80B7D57E1A852C02713
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1001296
Entropy (8bit):	6.464835172745815
Encrypted:	false
SSDEEP:	24576:75UFBBhPT+1Gl+B66TmUC5bx0HnBJlxCN:GrhQwW5Ts5KJAg
MD5:	73AF30D83FD52846075C21A68959FE56
SHA1:	D41B47F559B859045111DA74E8EFD20EC2B70330
SHA-256:	6C6C71C1DCD90546442085B853450922DFA0E71747D3DB8BD984D8918FA4905A
SHA-512:	CEC40FD370886A5A76FFDF0595B818523573ACFE9D3825413F0EDC3E3700D7D1EC6F0ECE465EA5A885556821E50A7C69AA69F0F367B13DCEF3306E0E5101433 F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: ditekSHen

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	686928
Entropy (8bit):	6.657086665651869
Encrypted:	false
SSDEEP:	12288:yxy7dFtEB12w2w6Ahk7Re42UZuy/XlLTsiW0h73OZ+PY7wGPXiCR1bC:N7ftE2y6HFX2UAy/XlLTHW0YwPYEGPXw
MD5:	7A9EC6152E71BEF30EED406A5784031C
SHA1:	0A3D8F9EFFB6F9C0C3B098F234555E36A2A1A279
SHA-256:	E42D06BBE346703D9AC8F28A98AA1D334E088785EBF43203AC51B4BF3881AACE
SHA-512:	5118CC0BD11884DE1DB4380646376F52DC2E6874B9AAAAEDED4F69566BECFDAF6D7B48D6EF98E70FBAC0C32B0668D5392E74C9A8F3EBF0A0F31E4A63D2109051
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.74977503731175
Encrypted:	false
SSDEEP:	3072:sr85C/qeRM5xzgglg8S7UnatoTBf3bmjZqMNT2rIWDTWos+tGEkBbq6D3Bdsb:k9/Rezdlg8S7watoTB2vi9jspTq6Ndsb
MD5:	4F29AC6A10F97FB23E73FC4EB09B299E
SHA1:	4998AB461B66DF8CF435D435AA47BF47BC8DB9E5
SHA-256:	1BF2384B3E4A9F4A95B7FB0B4D03F36A658936F4DE4ED569E137D16069730EDD
SHA-512:	828B210C801F90A6CD1613A74B1020B5A2A447F0AEEFDD8F10AF72EACCE59C32CF46DEE82A335C3A0F77CF62EF02E8E395B4AC401DA010F273CA53EA78583E96
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.753407460087031
Encrypted:	false
SSDEEP:	3072:sr85C/qgC18pVwUM0NldXnSsohU4TBfHqKjZqMN6wVzQQS0o+iwdnP6ngIs2:k9/hCYwUJzdXnSpU4TBdvD2QS0eg6Zs2
MD5:	7664868B3587C8A92E797C9B6A948C4A
SHA1:	AC2CEFF0C1B898A3A3B8CDC524BDE3B2C2401E59
SHA-256:	EA7B9E779DF726F99906E96C1A65804C60840C31D240FA65B164CBE5CFECF0A5
SHA-512:	5D3F983D244C114FBCA962E808DC773D5D3C5E05453363A88238BE54ADDBE35068229A545364412C5B48BEFFCDFD0058F66BAE75DF6C30E92F3CA7DE3B1FA 5A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341880
Entropy (8bit):	6.494451078546094
Encrypted:	false
SSDEEP:	6144:k9//edYNAMeo/0/3/A//FE/FzdXoktv/Pu29mYx:GGmNAMeo/0/OtE/F1tvtFx
MD5:	7E0FECA66B63B24125A4382E4BCCF851
SHA1:	867EE4E9CA574FC1872473AA7D81650C242C63E5
SHA-256:	18DA8ACE9C2524D10A4FBC65C1BD0CF842C81974947139094A6B6B3391C0249E
SHA-512:	65A2011D14979E443E3F62DF858675EB80D49FB42B13E50F0D4125A769D98A6A44E70834D5C3E99911C0D10A0364B54820F6F4AEB60C1382B32EC01978935452
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: ditekSHen

Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2628816
Entropy (8bit):	2.679593361098342
Encrypted:	false
SSDEEP:	12288:iQFsiEt5LODS6RcvRtd+sGum6QHArfePms//bV5cOXPMiCSmRZQkEKFF:XFA5LODZWvT4sGz6QHVN3bcOhfmRqkf
MD5:	9C0D6AC2E466E889E3942F657F2A9722
SHA1:	5A1FAB3A4D953930EE67B31306CE71C94F3DCDF3
SHA-256:	E1DB281AB5D39731EB3A7C44B27928E21FC8D89F2D2B99D8B6D9B6187D412ED5
SHA-512:	50FE3D1BD42615388B7B2395AC645DCF44AC8E0C0B8EE9C5A8C57A1B1E089757B4EDCC4A60E70B7BF136E91022CA474F5E3D3CF2E8724B516DF518F738D5D(BE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	225512
Entropy (8bit):	6.411549382704613
Encrypted:	false
SSDEEP:	3072:sr85C8gYp/OAWLTIKE4Vw2v6HXPoYvtT1mxho19K/rEs59s6i/XtXv7+8rKca:k98gYp2ARNQYm+1WllgXtj+eC
MD5:	B45E235D4600D4A75C90D037D9D5C208
SHA1:	994614F1A7F8D7E7423A46781FDB72AD6469835C
SHA-256:	F38C4B7F5604C3D047A1DFA76A0987C6C13FEDD97155DC5633DE38269787AB49
SHA-512:	86050D6F26FFA4999BE405A6F2FD7050436E3C8AA8507A37DDD1BA84F731D6DE547E640C121382AEDB6E6F9D81FD0DE4B34A6A49D1EA44607DA078E705916B 7
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	5434136
Entropy (8bit):	6.306403224869207
Encrypted:	false
SSDEEP:	98304:Hd4rAkEDQUKrXhluiA7i/9kl0DQW/dq9s2/v5OC5Ca/oz6g1PbxL:rkz/Z/9k6DQW/dq9syBB8L
MD5:	241A771AD01F3E181B8930F36DBDCE45
SHA1:	942B1601C5985DDD2DF5E96BBE1993318E17F382
SHA-256:	4C586D3F7AD0945D75EC3F51F46431483E118A6CD811A7D1EF35126832936147
SHA-512:	551A9D772DC1E03EBD66AD320659DE515B7F091A3D157FB6CBE2AFCA74A0E553D3AECB7EEDEC6487E6C2600BB792ABDD35F39C56A3703A4924E983E14F7AE163
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	148832
Entropy (8bit):	6.402312332234301
Encrypted:	false
SSDEEP:	3072:sr85CVrGOTPVJb+dW0wnbP1EfEDVYpqeyDY:k90FdW0wbcEDm/yM
MD5:	8D5273AB369F21CE9AE8DE3617F1543C
SHA1:	2AEC6177549D024BCB3B6F4DA45E31B41F4512C4
SHA-256:	B45246D66ADDD0242CE68F6188DC73A7B1C6A16B6A316E80494092E28346F8AA
SHA-512:	72FD33191470348A2D61CBBA4726374052D0CFAE3596049E37A2B9ABAD2B02902AAFCD059A8F3887C49E3DD25A5AFCB87EA4070FD2579E3D9A162B6A079420E2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	325808
Entropy (8bit):	5.5226016140596625
Encrypted:	false
SSDEEP:	6144:k9ULqmJHCJMgenwBOPhloudkpkSuULGD5NlKrGS2g1aQ1p:WmJHCJMgf0PhPdkCzU6D3ZSh0Q1p
MD5:	5136D87E5AF05DCA5F150225AFACB2B6
SHA1:	04EEC23E8B08E97BD8106EC4F0EB43C1DC6D661B
SHA-256:	F91DD439569B16AB39E348DC0CA7FFF74E6196E53E32D6260AEE5BBE0635C6FF
SHA-512:	FFA6E93116FB8CE90B83A3227DC8D7E448822DDB8EF4DE862448D3521799D4718327DCAE3732D91E6D251F8A1C48467C27A07FF21117A5E6C027F0B2B319C1A
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	366288
Entropy (8bit):	6.48929995153674
Encrypted:	false
SSDEEP:	6144:k9gV7oJKtEsCZQ9BMHmD1tYFLqY/W5R02qO7VKCy7KIxanso:MotEsCa9+aYFLq3ny7KYo
MD5:	679EF460120D3C4038D12BE232F20CDD
SHA1:	C4CE1629658BC812383107DA694BBC0C49BC5E9B
SHA-256:	6AD6C4BFB89F876BFAA332917FAB8DB2572A6A785AAD54C2D85A7BA9FAAA6B12
SHA-512:	7B59B45B27A958291844C1455D89DD62A25CE263E8A5BECEF21477A39A02A213506D7CA75CB6FE804A8AC47ACC90A0A3395FFCA0FC431803CD1808425C9A67F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	657064
Entropy (8bit):	3.618030662317966
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCGaCAd1uhNRN04gi0o0AdA/AZQJSShpuL4Y4YkvJt:sr85CGd04gi0ouuL4Ytkv
MD5:	A16A6EA47B7C467547C4A70ED1410B69
SHA1:	A09526746160F238704443E171A171BEF915E104
SHA-256:	4C3903394275D2888CF5A7B1252A3DC4D9E1ECE80C29EE713D2D19EDFF824233
SHA-512:	9C24B6937CAB50CF941C5FDD0CB03502A4D82A2C77B31B061355EB162A599B5F8FA7CA3EA06E53063D3D359CD45DDE4F9EC506F41CAD1A4448B35BAA4A8E7AF5
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	222904
Entropy (8bit):	3.461165007131812
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCt1uhNROY+WxQ0lEJRaCA:sr85C3vWtI
MD5:	4C6E4AE5E8D23BCFD573180D5D0C1CDD
SHA1:	83F2EDB37645A354E99D6EFE2656E1E194D4B88C
SHA-256:	4271DA8BA28C34CB0D2577201C2BEBB00472BCBEE5CF27687AA3F1F2E3539D6D
SHA-512:	9FABF050FB69C6DC2B0B2633BBB4BD406A23EF94EE73033A2801441EB00502671D2178E2E7BEDB2195E10B3CE701A4ED32D332E7476BE43C4999E75ABEFBDC B9
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	262344
Entropy (8bit):	4.108554712470892
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCzRaCAd1uhNR0Ga1vRdbwzkMrdYJnRQV6J4tuw62roH5lL1u:sr85Ctk9v/0xrsRQIouwjQlL
MD5:	B9BB6908286044951C1219CB6D7ED627
SHA1:	FF716B938C49D21C28C14A6FEC573153354EDCF1
SHA-256:	1A4DE2B1BDCA2768D92B817B4E79CC884564CA8835C42F4EBACC186620EE576F
SHA-512:	DAAA7A6FD5B4064BF38F74D9E4992AC4D2CD58EA946587D7F14433830CC5A3663C1F93F47F5620FE0A52AA664B6CFC49B3690C86F43C418A9A10E61FE6EB9B 2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	166104
Entropy (8bit):	6.252331629815344
Encrypted:	false
SSDEEP:	3072:sr85CWenbUaOU1IcODjnhyAf98rN7btBAxm2Z/ps/rz:k9fIUjEwEGDAxm2Z/m/rz
MD5:	5AA9BF8620B1540F8696BF4158B49F36
SHA1:	B6C53F173A497567AEA6D745048B45C2CE46F63C
SHA-256:	9A55AD87E0E8A200C7B5A6E4AF520B17E06781692CB96527AA3332CF943AA1A5
SHA-512:	EFC589FD4343761B3A51154734AE41A6C04513731573B84C01AF50B7365292888CDAA0DD3E040093A6C1E5CA73B193059292F837708337B629D379070CC99561
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	244944
Entropy (8bit):	6.5104370398950335
Encrypted:	false
SSDEEP:	3072:sr85CZRqkGhC5v+1Z04e4qOPBRzIN/yvdyVCKtUoBx9KrKeQk1bUpyNB6zLy79bL:k93qkGhCM1fqOPHkN/ylyU2mPUOFL
MD5:	CAD74221846597826D04754CDB9DBA4B
SHA1:	9824F68AB0005B1C3B14415085A20AAFCB0F478E
SHA-256:	9DDF22F1422C16EE910A9A7F3588C9A8E25B1596A548B8D523D828FE3F2BAC7D
SHA-512:	9D41DE4C02B9CFDCB126EC0ECD3A3091A2AC80D62D91B067F49FDADC5FDB7FAD344A3C0B32BF6C4661097E5D5CC593FE6AE8F899821119 02F4A248CC0FB5 48F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	589976
Entropy (8bit):	5.336385030490749
Encrypted:	false
SSDEEP:	6144:k9D4aeA+WEnGH1NCmWR5FJYUJupxFdYqIVz:2eLWEnONCmC5Vuzrb6z
MD5:	EF2793ABFD4E043F63B1CA873F237C2D
SHA1:	FF5457BD00F86D79F819F00678FD8AC30F367388
SHA-256:	16C5983B4C61A079E59B24462BE18FBF0E63857FA69F793DE36E74F9BB7A2A82
SHA-512:	5C4D478A4E543E038F9AD52E6B34F9B01B0284C8E634E61014B15E41D4EC49304A0C9308E379867D0FD944B38942203A5D2FF53B3D327B70604093752E421499
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	673304
Entropy (8bit):	5.441697637615724
Encrypted:	false
SSDEEP:	6144:k9aua5qijR4ZTvC7yPA1ikaY1xA1VurX6hOI0MjEVQTzfKfle6lZuy7:HvqijR4g7h1ikByX/OVE8fle6lZuy7
MD5:	BCFBF50E51399487EB4DBE3EE4E19C31
SHA1:	2E765B3801F6FA24C237674BE5F474593FC51D8B
SHA-256:	CF2CC5B6DF6A8FF7FC0AF8AC395106C2E486297B14C74275229FB6E242A2CF57
SHA-512:	BB167373C6CA5E53018AC2A86116439BF387A4FA4DF1FC6B38A42B55B759CAB1F34CACCA2D0A4400D409A15FD0D2167FB8F410459708E546CC934C6FDDB85E34
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	255168
Entropy (8bit):	6.581428824084993
Encrypted:	false
SSDEEP:	3072:sr85C6zcMqiGhz/fA96A9L45vxfq4qzqD27eIyUX3cM74E5S4uNUx9y1RXMUaGY:k96ctXc9L4PCqCz10/Dz1RXMTD
MD5:	5E6B5C0D0846BB3838F629F211229109
SHA1:	B340BBA8A255C1EC362F2BB10C69E71F785462BF
SHA-256:	BD4835C66C6A39D9E15714E3CBDD1DA980B6C81F8F6B5DF3325893CE03E8261A
SHA-512:	7B5353F8B5A55179769546102350B7743C0356BB84E0D14CC513E7DC37F336CB1B498C0AFD8C6D5BF3664EF37852EB46DA27C614CA7F06B908B30408453238C

Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	124136
Entropy (8bit):	6.283326852264287
Encrypted:	false
SSDEEP:	3072:sr85CqPo10JOSdBlrbr1Pg9uCRFRzsxeZ:k9qg1MOcxPmRFJs0Z
MD5:	52A62AAF5FB24EB66FC6580781659B53
SHA1:	F905E2B869462A12A3D57088B2E9F8AF1A822134
SHA-256:	64828A7C1BFD29B45B595E62AFCEF39D808CD286A1C31A7524E2BC7D52B64F2D
SHA-512:	4FF9DDE47D88D2A9AF53B499CB3E5F6E30CAE3A7D6A2370A3AEF95C9000B5821D6F0813363CACDE5B8077EEB718FF8C9C5751F6CE11B6F89C172FA63FA659 EF
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348344
Entropy (8bit):	6.672872121878769
Encrypted:	false
SSDEEP:	6144:k9NADu79SiirlTeeGyfgCA/j6FyAO/Hsumwc4+Qx+jeZAVlpTpPXQ:QAvroeGyfgMy1Hs/wtx+je6VlpTp4
MD5:	D100DD451243D803BEF2A6C40B0020C6
SHA1:	A69D07CB6149AB858DA10C4AA9925309F6EEC20B
SHA-256:	AC302270468E2CF49F96CA3EEAB7D5CD20782A9CB92E8553D3530643FADD47E5
SHA-512:	5BE451023E11185B1F3B16FBC950F51EACD2CFDDCBD2957EF8E2F0BD645270E638C3F875C9580418CCE05631940D6127BC7CD6D64B9F9481BED6A2CD9F2834 B6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	447160
Entropy (8bit):	6.42308894643679
Encrypted:	false
SSDEEP:	12288:WjPOEv2zUM2WJoROZApostp4oeTYvwDz8Ox+aCC:Wbn9ostp4Tcvwf8OxdJ
MD5:	BD676ABC8497C82307D92843F54E85B9
SHA1:	8B3EFBF8B25647AF14F57F95502E56AEDBDACB69
SHA-256:	F9F636B05C5C01CCF4BA39B35EA15FD6F5C51E6134BF27486042167337288AE1
SHA-512:	BB62F6201891A9EB77F2AA71F860E2647AE077E3CEE91A1F3CFC256C39EF76A4FD00029558BD709A3C987BEE754A1CB0EA0D5441996E38E5650537F61CA2309 5
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	210104
Entropy (8bit):	6.199615239624141
Encrypted:	false
SSDEEP:	3072:sr85C8aKavT/DvbEvK9aobNI2B+hlsfni3YGByThXKBZkZN4GhQ2eRZh+/bJSeoz:k98aK2h9H/B+rwYtiPC
MD5:	E2F2AA47EC5A4AAE63FBA8AD40691B9C
SHA1:	09C83FC458BF3AFAE15756D18681C34141870A22
SHA-256:	5691228B9C00336C0157D99C799DBF03089E6E22EA51395B81DB9F93E8E6C9E6
SHA-512:	5803FB556A8C941C026876F485421A1EFD9DF79AA5DBEEC2F19FD4AD338EAF3A682BC5783951FC7B9350AF7C6CFDE2604D374389A4BE23400F875ACC57B94B 8
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	156344
Entropy (8bit):	6.583491683345372
Encrypted:	false
SSDEEP:	3072:sr85CV4vzT+PXZpsB+KR+EOQC8m9WMxJ7Rfp8K172YPrp:k9zpsB+w9t1MH7cCxPd
MD5:	23DACF6F9722D3C34B89656E9D8CC7D0
SHA1:	C82795EC367614E155F3FB8353AA6E035B4210BF
SHA-256:	31224B24C740F5840570A0A9FBCD77B920081021C48EBCA50C0639A9F26E18CB
SHA-512:	9E6599301F7A47F589B3CB19BAD6516B0ABF220F6EAEEE27ABA4AB88A45E7832F529D35217C477309E9DC0849F4B620BA0AF0B242659F9E4F841524C54C14515
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233656
Entropy (8bit):	6.293668636600837
Encrypted:	false
SSDEEP:	3072:sr85CvySAcz4hp9wuzkHUYqWEybmoY46+WbOURHqDVC8O1uZXVS38yXLiQ:k9vySAcz4hUmA0ohMv2GSXVS31GQ
MD5:	BE1CC21C0A86B4978B9437E16DE1A420
SHA1:	C19C4DD66B04C9BBB14237F352C9D94D4356D31A
SHA-256:	2A33F58E2E6D8A1ED1D7DD65035CE467C4C1DB9003EA9A8F05455B19408244E7
SHA-512:	BFF4EC3B7D070009DFC7CA9A89DE1320242FE9445AA69631FCB79745556E76A2EA59CF07F2F64F621A57D46B95D972A6BB568FB6CE9895D9859ECC1B07E7CC C6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	268984
Entropy (8bit):	6.685634979954
Encrypted:	false
SSDEEP:	6144:k9zXqsTk90qC1AOb7Yswf1Px+efD83zgiC4p:WXqsTkiR7zwRx+AD83ciD
MD5:	CE3093F256BDDD46F1825DB8E5FA7F06
SHA1:	B61613A8BE5BF1A849379378F8BAB64A8F723CE9
SHA-256:	241CC17CDECEEAB568EF77A6E0A1A617740E19D1F37B61155ABF3BF420CF3205
SHA-512:	BD5F002AB1EF384F212ED23BDF5C17FB9920D2CE9CC82D1BBE6E43ACFBF3B062F1BCB725BC6E05AC4D5AFD7731E8B7B74AE416ED9C2ECC7484E147B2C7C4 4755

Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	156344
Entropy (8bit):	6.583159899761365
Encrypted:	false
SSDEEP:	3072:sr85CZ4qR8v7ZksB+KRdqkC8/BtER5AhC48S1m2YPrZ:k9cksB+wYktEXAe6QPt
MD5:	B24BCA7D2B19E941E63EBDD573781A21
SHA1:	D646BED25DFB3B3B452334A761E739F23EFDB572
SHA-256:	26D0C08FADE4FE2FA81B5A250CBBB23DBA5F637160CE11E50B13DA4932DBC769
SHA-512:	D48432AB5DAC45F9DFDFFE84B619695F78D7A3377C34D9F6649E94818B4469208A11E8E795626D161B22430776C5B80A6BFBAEBB8398F1A3DAE74AA30040D5DE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1456072
Entropy (8bit):	7.903360864050763
Encrypted:	false
SSDEEP:	24576:wKH/B1FBgDXZNFfZoWe0KVIC9ClKa5IrykTHhQ5NoRyftZZriXWzr6pfKuItwy:wK51rgXteP3Vz9oI2mhoNosVDP+fXq
MD5:	9B1499751A0BD2028744637F1D3943C6
SHA1:	606351B3371F637F8E52E7A67F0088AF4D9CAEBA
SHA-256:	EC1DB30D9847A367AB8D76842674CEA2071989D41FD655F8687E126BB338F1FB
SHA-512:	F1C120969BD7A8AE8A1130DB6C0A5CA771ED9DBC3D852B7D0CC094813CAFC8100BA20B16C3169A27AFF7AF34BDE7A77C8AF6C434EEACAF449D42D6A5FE5FE8F3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\Download\{430FD4D0-B729-4F61-AA34-91526481799D}\1.3.36.132\GoogleUpdateSetup.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1456072
Entropy (8bit):	7.903360864050763
Encrypted:	false
SSDEEP:	24576:wKH/B1FBgDXZNFfZoWe0KVIC9ClKa5IrykTHhQ5NoRyftZZriXWzr6pfKuItwy:wK51rgXteP3Vz9oI2mhoNosVDP+fXq
MD5:	9B1499751A0BD2028744637F1D3943C6
SHA1:	606351B3371F637F8E52E7A67F0088AF4D9CAEBA
SHA-256:	EC1DB30D9847A367AB8D76842674CEA2071989D41FD655F8687E126BB338F1FB
SHA-512:	F1C120969BD7A8AE8A1130DB6C0A5CA771ED9DBC3D852B7D0CC094813CAFC8100BA20B16C3169A27AFF7AF34BDE7A77C8AF6C434EEACAF449D42D6A5FE5F E8F3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\Install\{3560B2D0-8C42-4C08-AD8B-F3DF39FC149C}\GoogleUpdateSetup.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1456072
Entropy (8bit):	7.903360864050763
Encrypted:	false
SSDEEP:	24576:wKH/B1FBgDXZNFfZoWe0KVIC9ClKa5IrykTHhQ5NoRyftZZriXWzr6pfKuItwy:wK51rgXteP3Vz9oI2mhoNosVDP+fXq
MD5:	9B1499751A0BD2028744637F1D3943C6
SHA1:	606351B3371F637F8E52E7A67F0088AF4D9CAEBA
SHA-256:	EC1DB30D9847A367AB8D76842674CEA2071989D41FD655F8687E126BB338F1FB
SHA-512:	F1C120969BD7A8AE8A1130DB6C0A5CA771ED9DBC3D852B7D0CC094813CAFC8100BA20B16C3169A27AFF7AF34BDE7A77C8AF6C434EEACAF449D42D6A5FE5F E8F3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.74977503731175
Encrypted:	false
SSDEEP:	3072:sr85C/qeRM5xzgglg8S7UnatoTBf3bmjZqMNT2rIWDTWos+tGEkBbq6D3Bdsb:k9/Rezdlg8S7watoTB2vi9jspTq6Ndsb
MD5:	4F29AC6A10F97FB23E73FC4EB09B299E
SHA1:	4998AB461B66DF8CF435D435AA47BF47BC8DB9E5
SHA-256:	1BF2384B3E4A9F4A95B7FB0B4D03F36A658936F4DE4ED569E137D16069730EDD
SHA-512:	828B210C801F90A6CD1613A74B1020B5A2A447F0AEEFDD8F10AF72EACCE59C32CF46DEE82A335C3A0F77CF62EF02E8E395B4AC401DA010F273CA53EA78583E 96
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116088
Entropy (8bit):	6.487271937371817
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKB7qjh3rmKPNdTB63hvdmG2haDkdWlJ7OkUVS:sr85C/qJjZqMNdl2dE+bgOkIS
MD5:	0BD4255ABD473ED8E64592BF071499FF
SHA1:	52B8A7784CF87B3DF00BBD47335F74726653C398
SHA-256:	CB944C36D2BD9E4C2948B738C6983E1F280DC2F01E7268F6CCFE3E812F4533D7
SHA-512:	A360FD171158346BF65A4BAF15AA9ABC08C2AFE748C5A7007CDB8A12FBDFF54111688F68C5E91113AF9F730099E752E4C4C5C35A3BC43DDF324755D09E9C66 3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.753407460087031
Encrypted:	false
SSDEEP:	3072:sr85C/qgC18pVwUM0NldXnSsohU4TBfHqKjZqMN6wVzQQS0o+iwdnP6ngIs2:k9/hCYwUJzdXnSpU4TBdvD2QS0eg6Zs2
MD5:	7664868B3587C8A92E797C9B6A948C4A
SHA1:	AC2CEFF0C1B898A3A3B8CDC524BDE3B2C2401E59
SHA-256:	EA7B9E779DF726F99906E96C1A65804C60840C31D240FA65B164CBE5CFECF0A5
SHA-512:	5D3F983D244C114FBCA962E808DC773D5D3C5E05453363A88238BE54ADDBE35068229A545364412C5B48BEFFCDFD0058F66BAE75DF6C30E92F3CA7DE3B1FA 5A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341880
Entropy (8bit):	6.494451078546094
Encrypted:	false
SSDEEP:	6144:k9//edYNAMeo/0/3/A//FE/FzdXoktv/Pu29mYx:GGmNAMeo/0/OtE/F1tvtFx
MD5:	7E0FECA66B63B24125A4382E4BCCF851
SHA1:	867EE4E9CA574FC1872473AA7D81650C242C63E5
SHA-256:	18DA8ACE9C2524D10A4FBC65C1BD0CF842C819749471390 94A6B6B3391C0249E

SHA-512:	65A2011D14979E443E3F62DF858675EB80D49FB42B13E50F0D4125A769D98A6A44E70834D5C3E99911C0D10A0364B54820F6F4AEB60C1382B32EC01978935452
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134008
Entropy (8bit):	6.497362587068476
Encrypted:	false
SSDEEP:	3072:sr85CVRJdaMTcOmFk2W5OX8e77hfFTkd33:k9pdLcOlk24OX8knkn
MD5:	84C34888C9A51FB01DF63C0CC0B7C7CD
SHA1:	32A7CBB932FB78BA7D923FBB0552EF161B6B3E30
SHA-256:	566EEBF5BE25EFE8141FBF5FB7AADE83FE071D796B8B1AF954E65AE61F8E3852
SHA-512:	3F6A09924EA6DB56FA45534389A40A3A52B9AF57BB8A3B7F57E5CBFD3E447D7DADF1943874765DCA6F0616FAC4DAE803859DB8E8038B71292026D0A202E6C95 8
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	99192
Entropy (8bit):	6.3128286006573395
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCtOxg2Zz2hf3hOkqnoDdvhQBW1kqanjaYt6Zs8:sr85CtOxBZz2GREQQhanIZs8
MD5:	9DC560AE62D70ACECEBC7FB453F8CC3D
SHA1:	3B54D928E4FE60CA6FD5996F71E2B91243572AB6
SHA-256:	46431DEF5888434940751F24EE0376E6BF2E7A0DC1D6F36CF19C01FB26E33607
SHA-512:	F84807CEEE685F384B8742A82CB0CB9BCAAA53696442C685CC7D2865B561D936B8E2B53D2FB1CF846CEB3F0B9A0BA45404BD1BEACE3CA37FFD9A4555F8E6B F72
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	202616
Entropy (8bit):	6.134213889875678
Encrypted:	false
SSDEEP:	3072:sr85CTpl0EAWfL4JVDTBfveag9zQHvIlsSvO55PvV8HVwLZ8qU:k9T20tsL4jTBneag9zQHvCHVqZc
MD5:	91055112AF610F32A9BCD4C75BFB9714
SHA1:	D44A43CAB74C059AE53C557535B1969263BBFB85
SHA-256:	7FE29B3117AC85E958780A679E837037E3AD2524E1715E201E40FF5C14CA12E9
SHA-512:	711A8D1DAA1B4CEFED7B0B49E6CF95353F12909E321AFEDCC0794160A919DE8EF7DFB5164232C05E5BAFC2223B21844F99628E89E5642689D6394F0E7C65E07F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	136880
Entropy (8bit):	6.108883505091151
Encrypted:	false
SSDEEP:	3072:sr85Co3Bpj4+gLS8eUxkaenD9UR9whwtvTRMBy:k9o3Bpj4/E5RUNKBy
MD5:	21375F8643D992CD28FE2A43D43FD910
SHA1:	77846ECDCD2AD0F99215194D62D8C30CB0D76A00
SHA-256:	49FAA1C43FD5692B74F615ECE02E84FD846903821652E8F66F13481BE177AB70
SHA-512:	C9C08476BB0985650427AB868BFB4DC67080F08F6F5F44F21D5E91A417C7C4515FACFA4CDC49B5325CD394288326F0ED3B1AA2ABF28FB3DF77C068B82DD658E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3790504
Entropy (8bit):	3.576026782794367
Encrypted:	false
SSDEEP:	12288:el5td2vvvvvEvvvvvqb5Z6ziw812i4Qog6SerHqE7sLaMqkh:u5ty5Rw8Dog6RrKas
MD5:	044107F1653DC74AFB34823473EE46E2
SHA1:	22494F099C7C71EECF0A2C91B59599CD78518F98
SHA-256:	583AA7E7504D5C1F6826A2E8024AB2362B9C3CD168A3431290E032AE6E3CC04B
SHA-512:	02BA64056F1C3EA8E3BF671835C6548713F6B9A3E928D2DE4D5DFBE510FEE532504A98FC1BFF322A0F4DD58CEBD2942F6F60DFD2686E720129B800F942F5D4D3
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92664
Entropy (8bit):	6.635062455271286
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCECbkMkBExFhpgLTGlrFBbeEOCr:sr85C37uTGlr3iE5r
MD5:	2EAB2215D9C2A45D666A37903ED98BA0
SHA1:	89BE64137D65CA5CB36A01A990A6DC4A1D0C05F7
SHA-256:	9F8A3B5CA9E1E687937FEF9D07614CD8781C094F0E92A39DC4A20B3B8BBF3AB1
SHA-512:	3EF4E92834A8C53D21E02433ADA7D23CF4D593FA5DA399F6985F052EA58D152CDD1E9DACDA6059F41DDEFCE827707136E45E55F6B421EFEC984CF2314DF2A 59
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	413888
Entropy (8bit):	6.013317343594466
Encrypted:	false
SSDEEP:	6144:k9qd8/cXscXt7E1S4yRSZxqZboxNJ6XeJh:Fd8/cXsS7OS4yuxqpUmeJh
MD5:	D9C03C891BA40A1727DAFB3FAABF3981
SHA1:	C3263DADF7982468BDA720D47B79446B1F842BEE
SHA-256:	F64D6492DE5ECFEC963203FB749E0E98998DBA2208268ECF6058CDEEDDD33ADD
SHA-512:	08152AFFA3D37853AF5FA70DB71D20A60DFC77BB3B34A59E4352FE56CD31B1DC4C831D94734165ADD2D6733A802F2669A3BC9B6EB9DC100B6702D6A0F1E673 F1
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	217896
Entropy (8bit):	6.197146251739616
Encrypted:	false
SSDEEP:	3072:sr85CZiPMhRRhO40LIs5L6YrGioAPKhjah2QE2SkXFKJMt:k92Gn0kE6OrfQs2xt8FKu
MD5:	CB390C1C1680D4DE4E755204084540F6
SHA1:	56F3FA46168726FC6B21BB96281701CF34DBF398
SHA-256:	A56A8D8398D2B9D0421EE034BD32EC6E4B3F4700749563A0A1926E66A5C5AECC
SHA-512:	47044C594474816DD0478F1355173B469626BE9AEE60AC7987E00AA003AEEC6C46A4B2B605A616C349061203EDFFE534661D2BE80177F6C4F77A74B848D198A9
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	226656
Entropy (8bit):	6.404425291839694
Encrypted:	false
SSDEEP:	3072:sr85CuvMQ/58sNZ2OZ2Oe2T8sXF9xDr1BRo+SYZMuW32GhB:k9u0lsNhgs1f/1BRo+SYZMj2GhB
MD5:	556849FD8DC0825231C2BD774B530A44
SHA1:	E1B0E16F1646106353B6B3018A6D8BA4C2D24791
SHA-256:	80EA049A3B5D6A1036E1416658EC37BBAD73ADCDCEE7F614060A0E17BB15D069
SHA-512:	540B6E41F732D086C59F617707C25AFEBC531D1EE0D200AF76ABEAC101C218384E842C658CECEA68CFEC38B1B22F6F4C6DBF60D01EE04E6BB8C9C334B2133 3A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	496320
Entropy (8bit):	6.672915426345178
Encrypted:	false
SSDEEP:	6144:k9aDcmdCI6BHAlSpFG/+Ls3ze30xLs+bz0YTirzhafYyf7Pvm7M80yzyiL7nk:XDcmd/6JAB/6N30xQWhRvm7MIDnk
MD5:	90CF1CD64775478C1557AEB644225F48
SHA1:	F44436465D291ECAA558A9AB2F1289BD38A92347
SHA-256:	48FE31CB988AF311DBA1889CF7238F36010905119A7406E867B7B1DE9F768120
SHA-512:	0E12D4123A430FEC8427B525C11C12B48C5EB2122D61FCA7790888407006D83E9E94662C9221163AF32B92901285FD0AEB947986173EA44929D6446764652A78

Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	284864
Entropy (8bit):	6.433547487808304
Encrypted:	false
SSDEEP:	6144:k9PWQZIn91zska8o8dfu7hjBjobCUqJXGSOjKCkVWjlc:eE91zhTdfu7bU+DkKCkoy
MD5:	0BF7F314B38096114127763942C90D2D
SHA1:	030FBE240815DA96BC215BE9E44C416F1A93B194
SHA-256:	ED3E3235CD221A28CA04A62BD23CF3B751D75F2F669378BA3713A16C5AB2DD3A
SHA-512:	310A87A78DEF4C48B225B8F9951BAB74A7B4884EBB58EE4F5155C418906799FA44E29724F9E9895BE79E7887FBF7EADE915DF79477DB0FF497FF484ECDD30D88
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	813344
Entropy (8bit):	3.593320257597669
Encrypted:	false
SSDEEP:	3072:sr85CN6zI4fTT9loKYIAE8SM+mkzT4vo6d7FZzSsFinsietwZTtcihJibnqtaKRx:k9N6zNf9laluQoSSBHSUdb5LpB8pN
MD5:	471BDD50CAED8E9F629648ECA3C43767
SHA1:	0E4E1421BAC9E68581A43D1DBCE9D4DFD81DEDF0
SHA-256:	01C7F5CCCE86104C24DB562B7FF360D091917E66F927AFE32BB7B76EA158DCAA
SHA-512:	CFEF6E2669063B6D6B53DB3C7C6342093258212B2331F13784529CBCCE7E4BD299AB25978F2E322448C09B01C9F57BBB11EDF8655E8EF7537A04966825F243E0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4461400
Entropy (8bit):	5.950158976548802
Encrypted:	false
SSDEEP:	98304:FphXvapxXCk1JgTN6Yidt0TGwdp7JJK4AjXYwK/nF+TXx:zhXvapxSk1STN6+JK7jXG/nkrx
MD5:	D45CA170523B3F9E1CCA2BE57DFBC28D
SHA1:	2FDC4351383F23C91BBF168CAA91C5DECDA1A960
SHA-256:	A631289492580379DF23A1B73084768E510BDE0016A484268347B7392755ECAC
SHA-512:	E3A30E9305EB0A8AE6F0137D83C09FA4E9C479C39652572ABB81845B1C8B13A96B41FD595C211C54CFF45F52CA2747B276568E01E1573F5D35DFCFE7A40C77BE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	244160
Entropy (8bit):	6.516351495265726
Encrypted:	false
SSDEEP:	6144:k9QJ4mjSBzUzdiR5CpmCYvwg76HStzaCd9i2:EqB85C0CYteH6aCbi2
MD5:	3883FF97376691682D004A440DBF6612
SHA1:	252A3C24866C4C3049BE71F450D51C4636640E28
SHA-256:	A61E54F2829B464EFD831F2F00A2F8F99CF58E71E8C905676BDCC7EB77154ACF
SHA-512:	F508BEB028C9594FB8CE50890ADBB660763E9EDD6F210840C81D5869C3DAF1568219FC053B95C311505E8FC613D5EE4A4EFB7DFCEC758E43F1203CF77B6D6BE2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	118976
Entropy (8bit):	6.281459880554557
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC58F/3Oqm3yJFn7DyPSsTITDBkt+ETGBaORneubkuJ:sr85Chh3yJFn6dIvibTCaOFeubks
MD5:	CFAA62E8E09F71AFDF11535BB7C77370
SHA1:	7056433195ECEA9AF6473B5AC746BD1E139FE627
SHA-256:	617203C62C241DCC2D3D6FD4505DDFDDDDEE870AA4225E154BB244B6BE5BB8D4
SHA-512:	F0175CFACB3BCEED78983CB95F221416C29F77F17F43CB14145293AA6985571FD68AAE8EA9C4F5829A53092E0C42D8CF695389F4C0F062FEC02F0743095437A1
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	216264
Entropy (8bit):	6.312569617561015
Encrypted:	false
SSDEEP:	3072:sr85Cck7EhKG9e5aSUTrWT6ALhWYURNwqMb7Heu8LSakmP:k9R4DqaSOALhW9n0bTeuWSaN
MD5:	30D3A67F3058F2997FE70917E0CF6BF0
SHA1:	64A5048DDACCA55E4223D835ADC431C80839E3AC
SHA-256:	A65FE96E42DA1E3A01DF59A412612E7F2358CABC4E906F80270A76268479A229
SHA-512:	4A326CD77AE23AAEF77E97E4CADAF679C0B5A9C7254D29CBADD6F5344C66E4F7427F074CD065DD68411822F6E7D7241B6D95312E553CCEDC82C0C91170C18CE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	508160
Entropy (8bit):	4.204812044084468
Encrypted:	false
SSDEEP:	3072:sr85Cxjs2S6bj7lZ6C6zvahEghKaBotvHkHwK:k9xjs363SfShKaBo9EHwK
MD5:	E982EB0F53AE3406388700AF6E61F280
SHA1:	18A7CA63A6FAB57771C8B72B763C76A5F77841BA
SHA-256:	3F4CFFEE48824B2801B399A7E1C0599699B887ECDE7946C1234BD2F5B00478F2
SHA-512:	9DF082B861445A660E64AE47973AEF25168314A8949C17AE42904F3B402684EC31FE372BAAF42C8773F1CC7814A2BDA028A446254645DAC967F6799A2A8231D3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	564984
Entropy (8bit):	5.7343127030699925
Encrypted:	false
SSDEEP:	6144:k9wYRNgcg+u0BY1QeXBSb+9ZUKyHHzxGBcnYLsFpyHP63/OElEQyqy:EmP+uZ1QeXBSs6QNM/O55
MD5:	A0DFA53959740DDBC5691348F9E11762
SHA1:	D864CFD05F58C0D1CC4472294358DEB3CAB9150B
SHA-256:	AA2A99F1B257875D66C581873298DE290CBB8B95628DF81B594BA3CDE0395B8F
SHA-512:	C06B995A585F60CD3936E5AD80AB77F15AE25806569DE16DB787ED6735A7329A6A2B826616055866341D777CC6CFE0DFB0DCC9689753DE8D7EDB12127474FA(D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	747680
Entropy (8bit):	6.563860785698071
Encrypted:	false
SSDEEP:	12288:siut5wMRQrM5U7GYIiV7WApd8uGk0O3mMYvvmzTrdeM0fsyc/DKRGYP+4hNMyiVf:sTzwMREM5U7GYIiV7W28XO3mM7aTMyiF
MD5:	1026AE3D4904BFDD219A6A3A51EF2F75
SHA1:	6FD36AD56057979B413475E9050C7D4D3FC83BF3
SHA-256:	572EDB50457A36BF22652FFA0E5D9390BB52B83FB64E138ACA308FAC2EF22AC7
SHA-512:	865F1316167D48DEC187F6A71AA5A8481913AC5DFCE21084AEE757284CEE4BFAEF55CE7BCF93B2410C6287945FBD04CB66DE6D34C65EE3C64C4B3F0197BE01 2E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	153392
Entropy (8bit):	6.481711842686246
Encrypted:	false
SSDEEP:	3072:sr85C9NDS5lSsOjTFa1mr+fkT77NDS5lSu0aD0K8tMk+7ms:k99NDS5lSsQa1mr+fmfNDS5lSuLD0KDp
MD5:	E17B04C89921BEA5ED5D0F7842F52BF7
SHA1:	424596B0BB2DFAC4FC9D668A850DC3A9D1DFD436
SHA-256:	ECC3477F55109CA316317523C0B122D684749F90A67FBF685EA4A37F32513A1B
SHA-512:	48C7B1B8DE281BFB9F2620D8213351D07C8BE9B4BA93878F1C616FE5933FCCDC46D5533B04B0EF4D8A0599605F667E228E0A20087C8AF22D1EFB32C314C8593
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1717544
Entropy (8bit):	6.016143912072138
Encrypted:	false
SSDEEP:	24576:DWOXuaQ8eUXyfYvgn2lmMjbDowM1BNCkQ3aVremRRo+hQbzPNywi947QsawN:Al8NXygvgn2KgzEUrhQbzPNyR9lsa2
MD5:	DA312AA05912AB40E3B5B80D4CB7FBC5
SHA1:	3318B5631E71F36E254F4007F0EDDB5C08E5E31E
SHA-256:	E581BE40CDC473C3819132F9FA2942FD1D9FE1C91FC469E19712CC7F0C6B0BC9
SHA-512:	82B38CEAA442C5120224A8D17D21D464B167B81C44542E44B4E09C3AA3CDD33D5D2FC4B36BF8A35C5686C1566D2D6C7C85C572A5E6BA253B7B5BB39718B81E 34
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199344
Entropy (8bit):	5.596364836421844
Encrypted:	false
SSDEEP:	6144:k9qWnuOvOYOhODOXOYOzODOaOpOxO1O3OvOJO8O+O/ONOHO4O1ONOyOjONONO8OI:ze6xmI
MD5:	C59940D8865E47ED2C1F7A6F86A3C0DB
SHA1:	3A0F4F1F8EC5A9A72C4A587FD310539FDCA6208F
SHA-256:	6B11A9D79F0363C55A34BEDB7B4BCE9E9FC4487DA5ED53C7E2C0E10176486386
SHA-512:	304038168F61055ADB963C199DF5C09C97F46ACC712321BE14BD4C0B97C6A4AF60918A260F07275B1B258797DE70897B5EB013719D617CE43B14E41D0DBDBF1
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1598352
Entropy (8bit):	5.64057466441852
Encrypted:	false
SSDEEP:	24576:/V2ohJid8Uy2iHlu2w7NbV+D/KTO6lTDMx:wyiuUynHYZVa0OkDMx
MD5:	477F62B58CB896ABD7CB8613C34143B0
SHA1:	70398A72EED1BA70EB2E2ADFCC893091131D695B
SHA-256:	47952850C4B12894327205CA518F29760F747714BFC32B66EA60355596062BF1
SHA-512:	E76F842C10FCFAB081C30B9FD8869120D12FCE96D06E6868C7A8A53CB2BBCC8D9F6FF5C6B2133B2601E968F30BE06C20E721404E0E2728AC1F7458B8978D34A6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1890480
Entropy (8bit):	3.626577416508813
Encrypted:	false
SSDEEP:	6144:k9NT6ZXFzb5Ucyw4T7po25xx2qNcUcMeTOzhc:qTg5Ucy9oexxtcUcMe
MD5:	B4A4064AB06BE46247E26EBB426BF28A
SHA1:	A5E2224B5B64467BCDCFDFA1468DE7E7B0A59E16
SHA-256:	7331BAD015B2AB4CE324FAE45B79C955BACE66C7C268BDC90C2A11D82CD8649D
SHA-512:	CFD0D147E4649F0CFF5853EEAD1C547C22A0EED9553E78F3CD818F088CC73F725D24B696B35420F7ABAAD88EB81C74C7010F863D51CFC1228DEB575F2D7418AA
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3551912
Entropy (8bit):	3.3573232593996556
Encrypted:	false
SSDEEP:	12288:F0knX9Y5Ucy9oexxr5UcykDuD7fcUcMeV:FxLe3kD0Q
MD5:	A117007C4C779978A6C5D890B847BC98
SHA1:	0AB6D80AD953B8C2152AFB304EB4648B21648465
SHA-256:	686262AC34622190CBCA444A152CDED2E8D626C4F7E0B9045A0FFAF1A2F1A60E
SHA-512:	D0632F9C2B50A2F9EDD51820038B4F9F3193BCEF88AC827343840031D419B1F59D59ED17824E238EEFEFB7EBA704706A0B7859EFCD5C2B29B99531A52DC302A8
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	97072
Entropy (8bit):	6.543326517338806
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCtvNuEJzbmAoDucEMQnF0:sr85Ct1uUlbMt
MD5:	DF65F71CC8759F86441E0F07A3623256
SHA1:	652DD618FC30E7BC77D2B31CC02FCE7C77322B71
SHA-256:	EC77869B45D62D729EECA9EE20F7116126C6BE9D6D5798717C2A89C7186F68B3
SHA-512:	991FF8B6F6BA4A651B40479D2C7B1A96DB6A99E196902B67C654E0AE65015909B1A2EFA0EE23BC5D8DF939CFF5F115AA788A873C4210A859FC778BF850B9F20E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	401112
Entropy (8bit):	6.187772596269455
Encrypted:	false
SSDEEP:	6144:k9dDppHQA0GZHU0MQdtmutQqrvMcHe6Gg1WLu+ffCvkV2hriVFRG5pcGBvcxID:U/CGN+9qrvMciMiCaI8D
MD5:	442BA7D148A5B05DA25B6136812C399B
SHA1:	6AC7A8CE93C8AF8C1B8589AD06C1CC319A18A293
SHA-256:	B459320677D5C8DB1A82B89355B1DE323DA47C87CCA408153F9EECB6F862B7A8
SHA-512:	969599FF2B64D857AE8E91FA0D3E2D431B2866928E4883E3F1A101D0C58052926387E2F43775DAE5F7AE850A3EEDD37F137AAA421FFB0FCC4AC27F35137FC19
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	97496
Entropy (8bit):	5.941949021977476
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC5wM5RpEctMF4PqxgWvwG+TUawK:sr85C5w00callwG+TUawK
MD5:	08C9EFE747D52B7C97EBDAA7616C8271
SHA1:	7474EDC076F64726324CB1405E1C65B47DB6E17B
SHA-256:	CE4A6A2DED14AF0BB753103EA5C16FBFFAA03773A4B180A6E9289CC9046EAF0D
SHA-512:	DA444A2520031C0BF4401BB201E34E121A556C42838D8925C53B2FC83FBA8505CF346D3AF26C2A30DFB96D87BD7441AB45CAC96879FAB0369C1ACB48280D7E E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 98%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1119024
Entropy (8bit):	4.825577989169068
Encrypted:	false
SSDEEP:	12288:yW5pS9L2k8TsUz71UL9DuNvdbsA3syoWh4Jr:yWDSRK71A1uNmnC4Jr
MD5:	BEA2AD6850108169F81A818546C0C1EF
SHA1:	8AA4608188E4484AACB7973F85425A0660F80D23
SHA-256:	0606DC5D058414B632FD717DDEFF2D794A9C7D9DF77F6B550E92B4E67360AE0C
SHA-512:	EA8FD6B5D21ADB98E4FC5AFE64D3A58F145B0B090AC256F92F618DD84F89E3187996572BAE2CB4642B03421A94EED83D8941A3EEB35705D3D3F27D40D68AB7 78
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	345288
Entropy (8bit):	5.604022763849136
Encrypted:	false
SSDEEP:	6144:k9sPeJiOSJeUC2AI01h7OD2+gVmW7y36RaR2S8/KaQ:9FJeUCzI01hY9Aj7o8W
MD5:	F4D74A3E2C454B359EBCE229E03D6D15
SHA1:	B388806ACBD5C61C493EDF5323852CF72CD385EE
SHA-256:	793D263EEAA4B383826E838A14C5B68C8159E81DA428DB2531F4615380EEFB76
SHA-512:	15600E3D199233DFB84A0733DCD01736B4318FF086CA5888823F18419B95741B5B2A83B4D268446174C7BFE7552BB8046D992F4E853FF2000A3AA4A7BF8DBBD4
Malicious:	**true**

Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1979160
Entropy (8bit):	3.8393367118042114
Encrypted:	false
SSDEEP:	6144:k9G23FukA1kAb0rEbrESZU8wFjNHsNurY:q3E790rEbrECNiY
MD5:	82F1E75BB8C77982089DE6994CEF7CB6
SHA1:	A4A4F80C3990F6A4723D13155B13406F0FF0A035
SHA-256:	44E9598558628F634A0EA8D30C5AD19BE75265C5208D1C997FA01CCF14B36B96
SHA-512:	DB59F5449A6B21507C79D1D052AE70CDA0A859E35D7500FE61E14032DB0C9A3790725EAECFF2736AFA699F1F46158A99AA55A89DB3E8F86168B53EDEF078D5D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3057832
Entropy (8bit):	3.4614725617151314
Encrypted:	false
SSDEEP:	6144:k9fcZUNrfkrfzMwFjNVtZ9EYDEWs3cKrFYWKKnKK02NqTlaX:hRtZ2YDEWs3cKrFYWKKnKK3ocX
MD5:	CB31D8C2DD93637FB0191D70014DE6F4
SHA1:	DB5687E6C66ED4E47133F30A77DF572B3EF287E4
SHA-256:	B578A27ECFB0189254C00BDF37A198659721AD6340781BFA3001EF6E89FE62D5
SHA-512:	7FEA9BC27DC0F26FAA2CE1ECECF6563CB59D1AC38F1A1F4C82AC2347BC146728174C758C8BB467F1F3587656714D5CA927996898D1DDF8AFDA61D02B172BD54
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 97%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	3728040
Entropy (8bit):	3.366413518949862
Encrypted:	false
SSDEEP:	6144:k95DYJniVbgn0Cuc6evCvAHfOXYdrqtAhoGfufLN1Z7:yDYJnQYgSXMR19
MD5:	B1F52E736ACFF704E3D272B4E5FE21D3
SHA1:	7F1FAFAD77B555FE9BCF743B6AB287B2F5C18903
SHA-256:	5FE59FF4D80FC714063DB7381A7E9E88D303BCB22B2BD73F73071CBA3B2544B3
SHA-512:	DADB2CAC72AE69EFA9350893FAF2E9160B772F2DFBF967A72E00EEBDA425CB791225CD76B0B49A2F080A780F2F1B20B525C4C8D924CAAFAB8E73ABDA3E46EB06
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	779568
Entropy (8bit):	3.908021969671963
Encrypted:	false
SSDEEP:	6144:k9gkYNiTF7BjXnhMKNRneNMToeGYAXLMDpQCfhmLV:fkHTz9cRLMdQYWV
MD5:	8C3B0E435921E204224DDCAA4C449F55
SHA1:	E8E9EDE55C9FF8F0CC6AE3F344698068F475518E
SHA-256:	A65D99A7B630A8078788CC3212019015F435F25A5C1E50881E931B4C72797681
SHA-512:	495999B69450D7E0B69CE54FD1AE388D6B4B1F4A9123BE8A3F043B94E26A78E101D358DE9303F260C6FD4EB5184CCF2F3664962F529E5786BAB208F92E1EF92E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9384960
Entropy (8bit):	6.481029897216704
Encrypted:	false
SSDEEP:	196608:Kcs45Kb0KuviDnYatO4HbnvVa73gRT3BWziGis9qhSfpmL:KNb0KuvenYiOGTV03GxWfis9qhr
MD5:	4DFAB259E8E581428A857AACB9726D0F
SHA1:	C3566A0D65B101F42D0A41C93A37C4CD4526A836
SHA-256:	F183E033C94F5E4CDD73C96B7C7562C371CCA2109ED0BBB029DC780E0FDAFA83
SHA-512:	64E288C445D3BAE532170642CABE1D3339913614A7ABA82521E7EF97E3F6989B09E34174245B6D0BCFF80CCCC723EA0C592807E2BFE11019AF7004BDAA166075
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe, Author: Arnim Rupp • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe, Author: ditekSHen

Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\misc.exe

Process:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1069224
Entropy (8bit):	3.692305981725916
Encrypted:	false
SSDEEP:	3072:sr85Cco4TUawK1uT040i0ougmQmJDJnJ+20FxPlJPPSSPJ/Z:k9N243xmQm59UtUSxh
MD5:	DE1BDD8AFE5C15AA550F72FE0AB41724
SHA1:	D0B444BEA8EEE42F873CF1D1CA16BCCA731FD4F3
SHA-256:	4B41036D99636462320122BDC38CF6B4BD9F4371AE8BBDFEB8FC9C7F826590C3
SHA-512:	0345A2FFCBD21C90714D293A675EC64082B24475F5B28FB5F93931197DB23BAC127F4A0235A42900D6D301F02CC4C81B0CEF3FE494D303C64B8677AF8410D1D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.339754709472576
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.32% • Win32 Executable (generic) a (10002005/4) 49.28% • Win32 Executable Borland Delphi 6 (262906/60) 1.30% • Win32 Executable Delphi generic (14689/80) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	IntelCpHeciSvc.exe
File size:	248832
MD5:	6b4a5a412e90721fba5170a25caefbd4
SHA1:	7796314ed7b9b9472b98d6efbb93164e44877c34
SHA256:	62271e4b8eeb27837dda10e85fb4b4a8f0c54b319ea06d28ffd56fab022d6f18
SHA512:	d17175feb0eb585f8a8e82dcd31c1b44b9c80e13d5ea9aaeeb9685af7d4e0b799b34a94112cd2e719b0e9d68f208443a7112b1962429461dd639655f090c8d30
SSDEEP:	3072:sr85Cd1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HInQT9cx77B7aqetQ0XdeMBma1uT:k9dta6dtJmakIM5Qx79PEQ8QVPkLV6h
TLSH:	DB34C055B7E4893FE29E46BC611252128339D2E3ACD3F3EE28D455B69F263E0060B1D3
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4080e4
Entrypoint Section:	CODE

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9f4693fc0c511135129493f2161d1e86

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
add esp, FFFFFFE0h
xor eax, eax
mov dword ptr [ebp-20h], eax
mov dword ptr [ebp-18h], eax
mov dword ptr [ebp-1Ch], eax
mov dword ptr [ebp-14h], eax
mov eax, 00408054h
call 00007F2320AC6737h
xor eax, eax
push ebp
push 00408220h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
mov eax, 004091A8h
mov ecx, 0000000Bh
mov edx, 0000000Bh
call 00007F2320AC9881h
mov eax, 004091B4h
mov ecx, 00000009h
mov edx, 00000009h
call 00007F2320AC986Dh
mov eax, 004091C0h
mov ecx, 00000003h
mov edx, 00000003h
call 00007F2320AC9859h
mov eax, 004091DCh
mov ecx, 00000003h
mov edx, 00000003h
call 00007F2320AC9845h
mov eax, dword ptr [00409210h]
mov ecx, 0000000Bh
mov edx, 0000000Bh
call 00007F2320AC9831h
call 00007F2320AC9888h
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F2320AC7172h
mov eax, dword ptr [ebp-14h]
call 00007F2320AC7706h
cmp eax, 0000A200h

Instruction
jle 00007F2320ACA927h
call 00007F2320AC9E06h
call 00007F2320ACA619h
mov eax, 004091C4h
mov ecx, 00000003h
mov edx, 00000003h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15000	0x864	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x1400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18000	0x5cc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x17000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x722c	0x7400	False	0.6173558728448276	data	6.511672174892103	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0x9000	0x218	0x400	False	0.3623046875	data	3.1516983405583385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xa000	0xa899	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x15000	0x864	0xa00	False	0.37421875	data	4.173859768945439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x16000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x17000	0x18	0x200	False	0.05078125	data	0.2069200177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x18000	0x5cc	0x600	False	0.8483072916666666	data	6.443093465893509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x1400	0x1400	False	0.1302734375	data	1.296744017426327	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x19150	0x10a8	data	Russian	Russia
RT_RCDATA	0x1a1f8	0x10	data		
RT_RCDATA	0x1a208	0xac	data		
RT_GROUP_ICON	0x1a2b4	0x14	data	Russian	Russia

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, GetThreadLocale, GetStartupInfoA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, MessageBoxA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegSetValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	WriteFile, WinExec, SetFilePointer, SetFileAttributesA, SetEndOfFile, SetCurrentDirectoryA, ReleaseMutex, ReadFile, GetWindowsDirectoryA, GetTempPathA, GetShortPathNameA, GetModuleFileNameA, GetLogicalDriveStringsA, GetLocalTime, GetLastError, GetFileSize, GetFileAttributesA, GetDriveTypeA, GetCommandLineA, FreeLibrary, FindNextFileA, FindFirstFileA, FindClose, DeleteFileA, CreateMutexA, CreateFileA, CreateDirectoryA, CloseHandle
gdi32.dll	StretchDIBits, SetDIBits, SelectObject, GetObjectA, GetDIBits, DeleteObject, DeleteDC, CreateSolidBrush, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, BitBlt
user32.dll	ReleaseDC, GetSysColor, GetIconInfo, GetDC, FillRect, DestroyIcon, CopyImage, CharLowerBuffA
shell32.dll	ShellExecuteA, ExtractIconA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Network Behavior

Network Port Distribution

Total Packets: 71

- 53 (DNS)
- 54984 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 05:03:04.241796017 CEST	49701	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:04.265069008 CEST	54984	49701	79.134.225.25	192.168.2.7
May 30, 2023 05:03:04.800154924 CEST	49701	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:04.823407888 CEST	54984	49701	79.134.225.25	192.168.2.7
May 30, 2023 05:03:05.487658978 CEST	49701	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:05.510993004 CEST	54984	49701	79.134.225.25	192.168.2.7
May 30, 2023 05:03:09.814769030 CEST	49702	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:09.838552952 CEST	54984	49702	79.134.225.25	192.168.2.7
May 30, 2023 05:03:10.394373894 CEST	49702	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:10.417825937 CEST	54984	49702	79.134.225.25	192.168.2.7
May 30, 2023 05:03:10.988148928 CEST	49702	54984	192.168.2.7	79.134.225.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 05:03:11.011717081 CEST	54984	49702	79.134.225.25	192.168.2.7
May 30, 2023 05:03:15.180689096 CEST	49703	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:15.204330921 CEST	54984	49703	79.134.225.25	192.168.2.7
May 30, 2023 05:03:15.738518000 CEST	49703	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:15.761953115 CEST	54984	49703	79.134.225.25	192.168.2.7
May 30, 2023 05:03:16.441720009 CEST	49703	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:16.465014935 CEST	54984	49703	79.134.225.25	192.168.2.7
May 30, 2023 05:03:20.523221016 CEST	49704	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:20.546850920 CEST	54984	49704	79.134.225.25	192.168.2.7
May 30, 2023 05:03:21.129595995 CEST	49704	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:21.152993917 CEST	54984	49704	79.134.225.25	192.168.2.7
May 30, 2023 05:03:21.739033937 CEST	49704	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:21.762600899 CEST	54984	49704	79.134.225.25	192.168.2.7
May 30, 2023 05:03:25.813194036 CEST	49705	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:25.836783886 CEST	54984	49705	79.134.225.25	192.168.2.7
May 30, 2023 05:03:26.489481926 CEST	49705	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:26.512829065 CEST	54984	49705	79.134.225.25	192.168.2.7
May 30, 2023 05:03:27.098850012 CEST	49705	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:27.122178078 CEST	54984	49705	79.134.225.25	192.168.2.7
May 30, 2023 05:03:31.211497068 CEST	49706	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:31.235635996 CEST	54984	49706	79.134.225.25	192.168.2.7
May 30, 2023 05:03:31.802465916 CEST	49706	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:31.825779915 CEST	54984	49706	79.134.225.25	192.168.2.7
May 30, 2023 05:03:32.489943027 CEST	49706	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:32.514102936 CEST	54984	49706	79.134.225.25	192.168.2.7
May 30, 2023 05:03:37.066646099 CEST	49707	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:37.089844942 CEST	54984	49707	79.134.225.25	192.168.2.7
May 30, 2023 05:03:37.631010056 CEST	49707	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:37.654295921 CEST	54984	49707	79.134.225.25	192.168.2.7
May 30, 2023 05:03:38.240475893 CEST	49707	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:38.264163017 CEST	54984	49707	79.134.225.25	192.168.2.7
May 30, 2023 05:03:42.316741943 CEST	49708	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:42.340038061 CEST	54984	49708	79.134.225.25	192.168.2.7
May 30, 2023 05:03:42.943941116 CEST	49708	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:42.967350006 CEST	54984	49708	79.134.225.25	192.168.2.7
May 30, 2023 05:03:43.631505013 CEST	49708	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:43.654850960 CEST	54984	49708	79.134.225.25	192.168.2.7
May 30, 2023 05:03:49.448380947 CEST	49709	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:49.471637964 CEST	54984	49709	79.134.225.25	192.168.2.7
May 30, 2023 05:03:50.073642969 CEST	49709	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:50.096999884 CEST	54984	49709	79.134.225.25	192.168.2.7
May 30, 2023 05:03:50.600856066 CEST	49709	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:50.624227047 CEST	54984	49709	79.134.225.25	192.168.2.7
May 30, 2023 05:03:55.844918013 CEST	49710	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:55.868120909 CEST	54984	49710	79.134.225.25	192.168.2.7
May 30, 2023 05:03:56.492001057 CEST	49710	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:56.515204906 CEST	54984	49710	79.134.225.25	192.168.2.7
May 30, 2023 05:03:57.101468086 CEST	49710	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:03:57.124826908 CEST	54984	49710	79.134.225.25	192.168.2.7
May 30, 2023 05:04:01.860733032 CEST	49711	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:01.884084940 CEST	54984	49711	79.134.225.25	192.168.2.7
May 30, 2023 05:04:02.448404074 CEST	49711	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:02.471786976 CEST	54984	49711	79.134.225.25	192.168.2.7
May 30, 2023 05:04:03.039407969 CEST	49711	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:03.062695980 CEST	54984	49711	79.134.225.25	192.168.2.7
May 30, 2023 05:04:08.062824965 CEST	49712	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:08.086141109 CEST	54984	49712	79.134.225.25	192.168.2.7
May 30, 2023 05:04:08.602433920 CEST	49712	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:08.625761986 CEST	54984	49712	79.134.225.25	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 05:04:09.290117979 CEST	49712	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:09.313275099 CEST	54984	49712	79.134.225.25	192.168.2.7
May 30, 2023 05:04:13.558610916 CEST	49713	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:13.581857920 CEST	54984	49713	79.134.225.25	192.168.2.7
May 30, 2023 05:04:14.102895975 CEST	49713	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:14.126240969 CEST	54984	49713	79.134.225.25	192.168.2.7
May 30, 2023 05:04:14.634191036 CEST	49713	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:14.657601118 CEST	54984	49713	79.134.225.25	192.168.2.7
May 30, 2023 05:04:18.721616983 CEST	49714	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:18.744879007 CEST	54984	49714	79.134.225.25	192.168.2.7
May 30, 2023 05:04:19.259565115 CEST	49714	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:19.282850981 CEST	54984	49714	79.134.225.25	192.168.2.7
May 30, 2023 05:04:19.790879011 CEST	49714	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:19.814150095 CEST	54984	49714	79.134.225.25	192.168.2.7
May 30, 2023 05:04:24.419668913 CEST	49715	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:24.442877054 CEST	54984	49715	79.134.225.25	192.168.2.7
May 30, 2023 05:04:24.963188887 CEST	49715	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:24.986629963 CEST	54984	49715	79.134.225.25	192.168.2.7
May 30, 2023 05:04:25.494482994 CEST	49715	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:25.517893076 CEST	54984	49715	79.134.225.25	192.168.2.7
May 30, 2023 05:04:30.657922983 CEST	49716	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:30.681288004 CEST	54984	49716	79.134.225.25	192.168.2.7
May 30, 2023 05:04:31.198075056 CEST	49716	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:31.221323967 CEST	54984	49716	79.134.225.25	192.168.2.7
May 30, 2023 05:04:31.807533979 CEST	49716	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:31.830872059 CEST	54984	49716	79.134.225.25	192.168.2.7
May 30, 2023 05:04:35.911439896 CEST	49717	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:35.937855959 CEST	54984	49717	79.134.225.25	192.168.2.7
May 30, 2023 05:04:36.524955034 CEST	49717	54984	192.168.2.7	79.134.225.25
May 30, 2023 05:04:36.549006939 CEST	54984	49717	79.134.225.25	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 05:03:04.193967104 CEST	50835	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:04.220006943 CEST	53	50835	8.8.8.8	192.168.2.7
May 30, 2023 05:03:09.763631105 CEST	50505	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:09.799726963 CEST	53	50505	8.8.8.8	192.168.2.7
May 30, 2023 05:03:15.148186922 CEST	61178	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:15.174299002 CEST	53	61178	8.8.8.8	192.168.2.7
May 30, 2023 05:03:20.493885040 CEST	63926	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:20.521481037 CEST	53	63926	8.8.8.8	192.168.2.7
May 30, 2023 05:03:25.785439968 CEST	53336	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:25.812330008 CEST	53	53336	8.8.8.8	192.168.2.7
May 30, 2023 05:03:31.181466103 CEST	51007	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:31.210273981 CEST	53	51007	8.8.8.8	192.168.2.7
May 30, 2023 05:03:37.036231995 CEST	50513	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:37.065052986 CEST	53	50513	8.8.8.8	192.168.2.7
May 30, 2023 05:03:42.286479950 CEST	60765	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:42.315392017 CEST	53	60765	8.8.8.8	192.168.2.7
May 30, 2023 05:03:48.027374983 CEST	58283	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:48.056211948 CEST	53	58283	8.8.8.8	192.168.2.7
May 30, 2023 05:03:55.814769983 CEST	50024	53	192.168.2.7	8.8.8.8
May 30, 2023 05:03:55.843626022 CEST	53	50024	8.8.8.8	192.168.2.7
May 30, 2023 05:04:01.830446959 CEST	49516	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:01.859366894 CEST	53	49516	8.8.8.8	192.168.2.7
May 30, 2023 05:04:07.995629072 CEST	62679	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:08.031418085 CEST	53	62679	8.8.8.8	192.168.2.7
May 30, 2023 05:04:13.533860922 CEST	61392	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 05:04:13.557497025 CEST	53	61392	8.8.8.8	192.168.2.7
May 30, 2023 05:04:18.690506935 CEST	52104	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:18.719341993 CEST	53	52104	8.8.8.8	192.168.2.7
May 30, 2023 05:04:24.381665945 CEST	65356	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:24.417123079 CEST	53	65356	8.8.8.8	192.168.2.7
May 30, 2023 05:04:30.628102064 CEST	59006	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:30.656935930 CEST	53	59006	8.8.8.8	192.168.2.7
May 30, 2023 05:04:35.869673967 CEST	51526	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:35.909228086 CEST	53	51526	8.8.8.8	192.168.2.7
May 30, 2023 05:04:41.106550932 CEST	51139	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:41.127481937 CEST	53	51139	8.8.8.8	192.168.2.7
May 30, 2023 05:04:47.337800980 CEST	58784	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:47.366252899 CEST	53	58784	8.8.8.8	192.168.2.7
May 30, 2023 05:04:53.208657980 CEST	57970	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:53.228923082 CEST	53	57970	8.8.8.8	192.168.2.7
May 30, 2023 05:04:59.529512882 CEST	64608	53	192.168.2.7	8.8.8.8
May 30, 2023 05:04:59.558573961 CEST	53	64608	8.8.8.8	192.168.2.7

DNS Queries

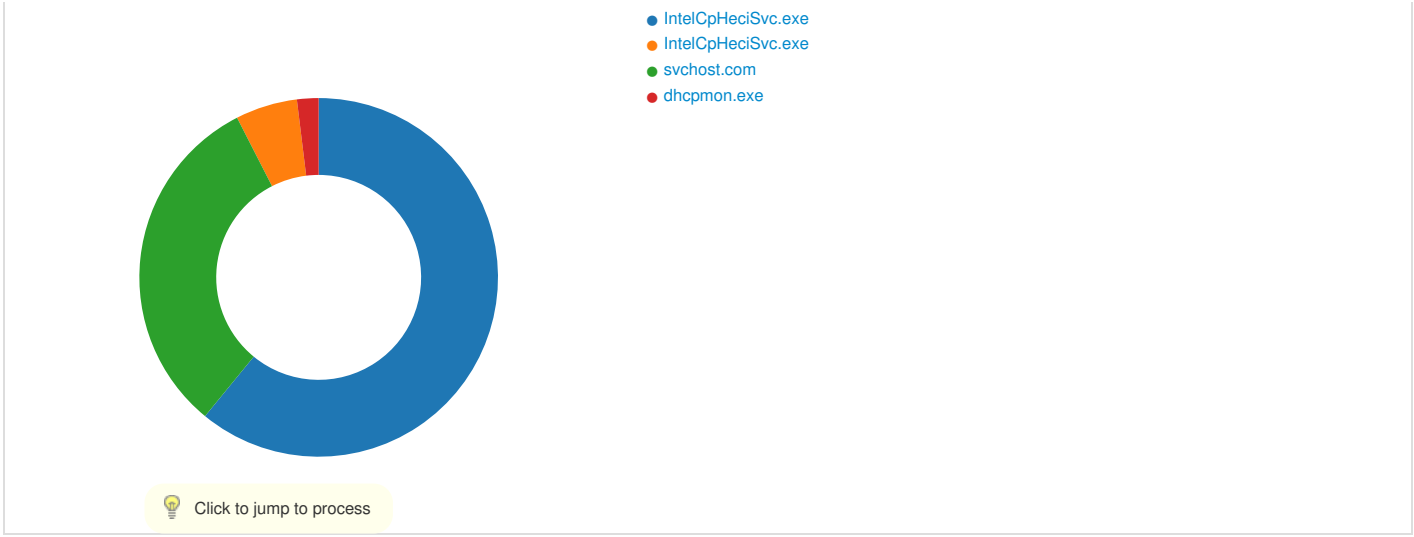
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 30, 2023 05:03:04.193967104 CEST	192.168.2.7	8.8.8.8	0xcdb3	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:09.763631105 CEST	192.168.2.7	8.8.8.8	0x4e43	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:15.148186922 CEST	192.168.2.7	8.8.8.8	0xb3e7	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:20.493885040 CEST	192.168.2.7	8.8.8.8	0xbcd9	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:25.785439968 CEST	192.168.2.7	8.8.8.8	0xb60a	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:31.181466103 CEST	192.168.2.7	8.8.8.8	0x270c	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:37.036231995 CEST	192.168.2.7	8.8.8.8	0x307	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:42.286479950 CEST	192.168.2.7	8.8.8.8	0x3f35	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:48.027374983 CEST	192.168.2.7	8.8.8.8	0xcf64	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:55.814769983 CEST	192.168.2.7	8.8.8.8	0x670a	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:01.830446959 CEST	192.168.2.7	8.8.8.8	0xbb1a	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:07.995629072 CEST	192.168.2.7	8.8.8.8	0x1d1	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:13.533860922 CEST	192.168.2.7	8.8.8.8	0x12ef	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:18.690506935 CEST	192.168.2.7	8.8.8.8	0x60a9	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:24.381665945 CEST	192.168.2.7	8.8.8.8	0xfedd	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:30.628102064 CEST	192.168.2.7	8.8.8.8	0x7369	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:35.869673967 CEST	192.168.2.7	8.8.8.8	0x4b7f	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:41.106550932 CEST	192.168.2.7	8.8.8.8	0x9e63	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:47.337800980 CEST	192.168.2.7	8.8.8.8	0xf877	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:53.208657980 CEST	192.168.2.7	8.8.8.8	0x9c82	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:59.529512882 CEST	192.168.2.7	8.8.8.8	0x6791	Standard query (0)	googleuser content.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 30, 2023 05:03:04.220006943 CEST	8.8.8.8	192.168.2.7	0xcdb3	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:09.799726963 CEST	8.8.8.8	192.168.2.7	0x4e43	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:15.174299002 CEST	8.8.8.8	192.168.2.7	0xb3e7	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:20.521481037 CEST	8.8.8.8	192.168.2.7	0xbcd9	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:25.812330008 CEST	8.8.8.8	192.168.2.7	0xb60a	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:31.210273981 CEST	8.8.8.8	192.168.2.7	0x270c	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:37.065052986 CEST	8.8.8.8	192.168.2.7	0x307	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:42.315392017 CEST	8.8.8.8	192.168.2.7	0x3f35	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:48.056211948 CEST	8.8.8.8	192.168.2.7	0xcf64	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:03:55.843626022 CEST	8.8.8.8	192.168.2.7	0x670a	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:01.859366894 CEST	8.8.8.8	192.168.2.7	0xbb1a	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:08.031418085 CEST	8.8.8.8	192.168.2.7	0x1d1	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:13.557497025 CEST	8.8.8.8	192.168.2.7	0x12ef	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:18.719341993 CEST	8.8.8.8	192.168.2.7	0x60a9	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:24.417123079 CEST	8.8.8.8	192.168.2.7	0xfedd	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:30.656935930 CEST	8.8.8.8	192.168.2.7	0x7369	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:35.909228086 CEST	8.8.8.8	192.168.2.7	0x4b7f	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:41.127481937 CEST	8.8.8.8	192.168.2.7	0x9e63	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:47.366252899 CEST	8.8.8.8	192.168.2.7	0xf877	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:53.228923082 CEST	8.8.8.8	192.168.2.7	0x9c82	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false
May 30, 2023 05:04:59.558573961 CEST	8.8.8.8	192.168.2.7	0x6791	No error (0)	googleusercontent.ddns.net		79.134.225.25	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: IntelCpHeciSvc.exe PID: 5760, Parent PID: 3320

General

Target ID:	0
Start time:	05:02:54
Start date:	30/05/2023
Path:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IntelCpHeciSvc.exe
Imagebase:	0x400000
File size:	248832 bytes
MD5 hash:	6B4A5A412E90721FBA5170A25CAEFBD4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.341781141.0000000002184000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.341781141.0000000002184000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.341781141.0000000002184000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.341781141.0000000002184000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: 00000000.00000002.609863549.0000000000409000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\3582-490	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	404EC2	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404B8D	CreateFileA
C:\Windows\svchost.com	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404B8D	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	0	41472	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 60 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'T` @	success or wait	1	404BEF	WriteFile
C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	41472	165888	0a 02 7b fd 00 00 04 fd fd 28 fd 01 00 0a 16 02 7b fd 00 00 04 02 7b fd 00 00 04 6f fd 01 00 0a 1a 28 5e 01 00 0a 02 7b fd 00 00 04 fd fd 02 7b fd 00 00 04 59 02 7b fd 00 00 04 06 59 28 fd 01 00 0a 0b 02 7b fd 00 00 04 02 7b fd 00 00 04 02 7b fd 00 00 04 02 7b fd 00 00 04 6f fd 01 00 0a 06 58 07 28 5e 01 00 0a 02 7b fd 00 00 04 02 7b fd 00 00 04 6f fd 01 00 0a 07 06 58 6f fd 01 00 0a 02 7b fd 00 00 04 02 7b fd 00 00 04 6f fd 01 00 0a 2d 12 02 02 7b fd 00 00 04 02 7b fd 00 00 04 6f fd 01 00 06 2a 02 01 10 00 00 02 00 39 00 1a 53 00 07 00 00 00 00 13 30 04 00 20 01 00 00 fd 00 00 11 02 6f fd 01 00 06 2d 01 2a 02 7b fd 00 00 04 1d 2d 23 26 02 7b fd 00 00 04 1a 2d 1c 26 02 16 15 2d 19 26 26 02 16 7d fd 00 00 04 02 7b fd 00 00 04 2c 21 2b 0d 0a 2b fd 0b 2b fd	{({{o(^{{Y{Y({{{{oX(^{{oXo{{o-{{o*9S0 o-*{-#&{-&-&&}{,!+++	success or wait	1	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\svchost.com	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	404BEF	WriteFile
C:\ProgramData\Adobe\ARM\S\11399\AdobeARMHelper.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Adobe\ARM\S\1977\AdobeARMHelper.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows Defender\Scans\MpPayloadData\mpengine.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\ProgramData\Package Cache\{49697869-be8e-427d-81a0-c334d1d14950}\VC_redist.x86.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\ProgramData\Package Cache\{f4220b74-9edd-4ded-bc8b-0342c1e164d8}\VC_redist.x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Users\user\AppData\Local\Temp\CR_14C6C.tmp\setup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTe xtExtractor.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeC ollabSync.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTr ustNotifier.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\AutoIt3\Au3Check.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3 \Au3Info.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\AutoIt3 \Au3Info_x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3 \Aut2Exe\Aut2exe.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\AutoIt3 \Aut2Exe\Aut2exe_x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3 \Aut2Exe\upx.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\AutoIt3 \AutoIt3Help.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3 \AutoIt3_x64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\AutoIt3 \SciTE\SciTE.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3 \Uninstall.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHe lper.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10 .0\VSTOInstaller.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_tar get_885250\java.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\ Update\1.3.36.132\GoogleUpdate.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Google\ Update\1.3.36.132\GoogleUpdate Broker.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\Update\Download\{430FD4D0-B729-4F61-AA34-91526481799D}\1.3.36.132\GoogleUpdateSetup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Google\Update\Install\{3560B2D0-8C42-4C08-AD8B-F3DF39FC149C}\GoogleUpdateSetup.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROL SERVER.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE	0	41472	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	2	404BEF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IntelCpHeciSvc.exe	unknown	41472	success or wait	3	404BD4	ReadFile
C:\Users\user\Desktop\IntelCpHeciSvc.exe	unknown	165888	success or wait	1	404BD4	ReadFile
C:\ProgramData\Adobe\ARM\S\11399\AdobeARMHelper.exe	unknown	256	success or wait	40	404BD4	ReadFile
C:\ProgramData\Adobe\ARM\S\1977\AdobeARMHelper.exe	unknown	256	success or wait	40	404BD4	ReadFile
C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	unknown	256	success or wait	34	404BD4	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Scans\MpPayloadData\mpengine.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{49697869-be8e-427d-81a0-c334d1d14950}\VC_redist.x86.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{f4220b74-9edd-4ded-bc8b-0342c1e164d8}\VC_redist.x64.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe	unknown	256	success or wait	23	404BD4	ReadFile
C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	unknown	256	success or wait	22	404BD4	ReadFile
C:\Users\user\AppData\Local\Temp\CR_14C6C.tmp\setup.exe	unknown	256	success or wait	24	404BD4	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	unknown	256	success or wait	3	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Check.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Info.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Uninstall.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\MSInfo\msinfo32.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	unknown	256	success or wait	4	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	unknown	256	success or wait	4	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	unknown	256	success or wait	4	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe	unknown	256	success or wait	3	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\Download\{430FD4D0-B729-4F61-AA34-91526481799D}\1.3.36.132\GoogleUpdateSetup.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\Install\{3560B2D0-8C42-4C08-AD8B-F3DF39FC149C}\GoogleUpdateSetup.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ExtExport.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ieinstal.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ielowutil.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\iexplore.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	unknown	256	success or wait	3	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE	unknown	256	success or wait	3	404BD4	ReadFile
C:\Program Files (x86)\udTcqoJlaRJvKnVbqSgKaWbTRdPRcLGHClOOvPvUxdYuiyOpcPlbZVFLVcydZFXEpZQNkEt\dupxdxKTvx.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Mail\wab.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Mail\wabmig.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\setup_wm.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmlaunch.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmpconfig.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmprph.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmpshare.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\windows nt\accessories\wordpad.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Photo Viewer\ImagingDevices.exe	unknown	256	success or wait	1	404BD4	ReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command	NULL	unicode	"%1" %*	C:\Windows\svchost.com "%1" %*	success or wait	1	4057BC	RegSetValueExA

Analysis Process: IntelCpHeciSvc.exe PID: **6824**, Parent PID: **5760**

General

Target ID:	1
Start time:	05:02:54
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user~1\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe"
Imagebase:	0x6c0000
File size:	207360 bytes
MD5 hash:	7F00E9819E4B205654B46E0090E6763E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.629221700.000000001B800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.629221700.000000001B800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.629221700.000000001B800000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.629221700.000000001B800000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.630261931.000000001BD60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.630261931.000000001BD60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.630261931.000000001BD60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.630261931.000000001BD60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.630261931.000000001BD60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000000.342421463.00000000006C2000.00000002.00000001.01000000.00000004.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000000.342421463.00000000006C2000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000000.342421463.00000000006C2000.00000002.00000001.01000000.00000004.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000000.342421463.00000000006C2000.00000002.00000001.01000000.00000004.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.619633331.0000000002DB1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE22358147	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE22358147	CreateFileW
C:\Program Files\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE22358147	CreateDirectoryW
C:\Program Files\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFE22358147	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE22358147	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE22358147	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd 45 fd 05 61 fd 48	EaH	success or wait	1	7FFE22358147	WriteFile
C:\Program Files\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 60 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'T` @	success or wait	2	7FFE22358147	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFE221C5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFE221C5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFE222E5AF3	ReadFile
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFE2228DA53	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFE2228DA53	unknown
C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	unknown	4096	success or wait	1	7FFE2228DA53	unknown
C:\Users\user\AppData\Local\Temp\3582-490\IntelCpHeciSvc.exe	unknown	512	success or wait	1	7FFE2228DA53	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFE221C5C7C	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	7FFE221C5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FFE22358147	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files\DHCP Monitor\dhcpmon.exe	success or wait	1	7FFE22358147	RegSetValueExW

Analysis Process: svchost.com PID: **7040**, Parent PID: **3320**

General

Target ID:	2
Start time:	05:03:08
Start date:	30/05/2023
Path:	C:\Windows\svchost.com
Wow64 process (32bit):	true
Commandline:	"C:\Windows\svchost.com" "C:\PROGRA~1\DHCPMO~1\dhcpmon.exe"
Imagebase:	0x400000
File size:	41472 bytes
MD5 hash:	36FD5E09C417C767A952B4609D73A54B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: 00000002.00000002.580407779.0000000000409000.00000004.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: C:\Windows\svchost.com, Author: Arnim Rupp • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Windows\svchost.com, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Windows\svchost.com, Author: Joe Security • Rule: MALWARE_Win_Neshta, Description: Detects Neshta, Source: C:\Windows\svchost.com, Author: ditekSHen
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\tmp5023.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404B8D	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5023.tmp	0	8	65 fd 5b 6c 0a 26 41	e[l&A	success or wait	1	404BEF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\svchost.com	unknown	41472	success or wait	1	404BD4	ReadFile
C:\Program Files\DHCP Monitor\dhcpmon.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	unknown	256	success or wait	1	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Check.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Info.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\AutoIt3\Uninstall.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\MSInfo\msinfo32.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	unknown	256	success or wait	2	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdate.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateBroker.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateComRegisterShell64.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateCore.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateOnDemand.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleUpdateSetup.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\Download\{430FD4D0-B729-4F61-AA34-91526481799D}\1.3.36.132\GoogleUpdateSetup.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Google\Update\Install\{3560B2D0-8C42-4C08-AD8B-F3DF39FC149C}\GoogleUpdateSetup.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ExtExport.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ieinstal.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\ielowutil.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Internet Explorer\iexplore.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE	unknown	256	success or wait	1	404BD4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\udTcqoJlaRJvKnVbqSgKaWbTRdPRcLGHClOOvPvUxdYuiyOpcPlbZVFLVcydZFXEpZQNkEt\dupxdxKTvx.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Mail\wab.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Mail\wabmig.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\setup_wm.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmlaunch.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmpconfig.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmprph.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Media Player\wmpshare.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\windows nt\accessories\wordpad.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\Program Files (x86)\Windows Photo Viewer\ImagingDevices.exe	unknown	256	success or wait	1	404BD4	ReadFile
C:\ProgramData\Adobe\ARM\S\11399\AdobeARMHelper.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Adobe\ARM\S\1977\AdobeARMHelper.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{49697869-be8e-427d-81a0-c334d1d14950}\VC_redist.x86.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{f4220b74-9edd-4ded-bc8b-0342c1e164d8}\VC_redist.x64.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe	unknown	256	success or wait	2	404BD4	ReadFile
C:\Users\user\Desktop\IntelCpHeciSvc.exe	unknown	256	success or wait	1	404BD4	ReadFile

Analysis Process: dhcpmon.exe PID: **4728**, Parent PID: **7040**

General

Target ID:	3
Start time:	05:03:08
Start date:	30/05/2023
Path:	C:\Program Files\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\PROGRA~1\DHCPMO~1\dhcpmon.exe
Imagebase:	0xfd0000
File size:	207360 bytes
MD5 hash:	7F00E9819E4B205654B46E0090E6763E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.403891013.00000000134B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.403372406.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.403372406.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.403372406.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files\DHCP Monitor\dhcpmon.exe, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE22198527	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE224E6147	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE224E6184	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 53 79 73 74 65 6d 5c 31 32 30 31 66 32 36 63 62 39 38 36 63 39 33 66 35 35 30 34 34 62 62 34 66 61 32 32 62 32 39 34 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 62 31 32 62 62 63 66 32 37 66 34 31 64 39 36 66 65 34 34 33 36 30 61 65 30 62 35 36 36 66 39 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",03,"	success or wait	1	7FFE224E61CE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFE221C5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFE221C5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFE222E5AF3	ReadFile

Disassembly

No disassembly