ID: 877862
Sample Name:
P05jmXYKpr.exe
Cookbook: default.jbs
Time: 06:21:06
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

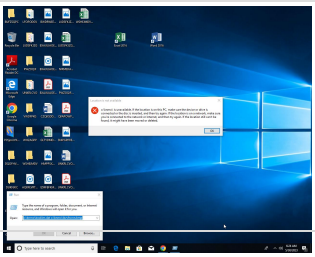
Windows Analysis Report

P05jmXYKpr.exe

Overview

General Information

Sample Name:	P05jmXYKpr.exe
Original Sample Name:	db555a9de355…
Analysis ID:	877862
MD5:	db555a9de355…
SHA1:	07534d501252…
SHA256:	fb25c8a64c09f…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

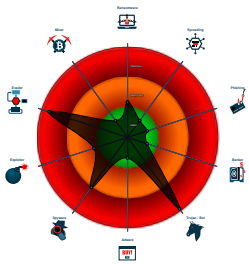
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…

Classification



Process Tree

- **System is w10x64**
- P05jmXYKpr.exe (PID: 7296 cmdline: C:\Users\user\Desktop\P05jmXYKpr.exe MD5: DB555A9DE355C70681E2E5F9ED38A335)
  - wscript.exe (PID: 7360 cmdline: "C:\Windows\System32\wscript.exe" Update-ta.l.vbe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - cmd.exe (PID: 7412 cmdline: "C:\Windows\System32\cmd.exe" /c ipconfig /release MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 7420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - ipconfig.exe (PID: 7480 cmdline: ipconfig /release MD5: B0C7423D02A007461C850CD0DFE09318)
    - cmd.exe (PID: 7432 cmdline: "C:\Windows\System32\cmd.exe" /c boaliim.dat ikvvfncnn.bmp MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 7460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - boaliim.dat (PID: 7512 cmdline: boaliim.dat ikvvfncnn.bmp MD5: D70543055E19B63641C7D5CB908EAEC7)
        - RegSvcs.exe (PID: 7772 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
          - schtasks.exe (PID: 7796 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE45C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 7812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - schtasks.exe (PID: 7852 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpE586.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 7860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 7620 cmdline: "C:\Windows\System32\cmd.exe" /c ipconfig /renew MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 7628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - ipconfig.exe (PID: 7660 cmdline: ipconfig /renew MD5: B0C7423D02A007461C850CD0DFE09318)
- RegSvcs.exe (PID: 7924 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7940 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "72ec1ea3-16bf-4e76-a7cf-15ed5e2a",
  "Group": "Marcello",
  "Domain1": "december2n.duckdns.org",
  "Domain2": "december2nd.ddns.net",
  "Port": 61715,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x227f:$x2: NanoCore.ClientPlugin • 0x2205:$x3: NanoCore.ClientPluginHost • 0x2295:$i3: IClientNetwork • 0x221f:$i6: IClientLoggingHost • 0x223e:$i7: IClientNetworkHost • 0x1f9f:$s1: ClientPlugin • 0x2288:$s1: ClientPlugin
0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2205:$a1: NanoCore.ClientPluginHost • 0x227f:$a2: NanoCore.ClientPlugin • 0x29a0:$b7: LogClientException • 0x221f:$b9: IClientLoggingHost
0000000D.00000002.651409238.0000000007B00000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 110 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.RegSvcs.exe.3850378.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
13.2.RegSvcs.exe.3850378.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
13.2.RegSvcs.exe.3850378.3.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x2d96:$x2: NanoCore.ClientPlugin • 0x2dbb:$x3: NanoCore.ClientPluginHost • 0x2d87:$i3: IClientNetwork • 0x2dac:$i4: IClientAppHost • 0x2dd5:$i5: IClientDataHost • 0x2de5:$i7: IClientNetworkHost • 0x2df8:$i9: IClientNameObjectCollection • 0x2e1d:$i10: IClientReadOnlyNameObjectCollection • 0x2bce:$s1: ClientPlugin • 0x2d9f:$s1: ClientPlugin
13.2.RegSvcs.exe.3850378.3.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2dbb:$a1: NanoCore.ClientPluginHost • 0x2d96:$a2: NanoCore.ClientPlugin • 0x6758:$b1: get_BuilderSettings • 0x2dac:$b4: IClientAppHost
13.2.RegSvcs.exe.7b00000.27.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 259 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049703617152025019 05/30/23-06:22:55.049348
SID:	2025019
Source Port:	49703
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049705617152816766 05/30/23-06:23:09.678894
SID:	2816766
Source Port:	49705
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049704617152025019 05/30/23-06:23:00.991147
SID:	2025019
Source Port:	49704
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049704617152816766 05/30/23-06:23:02.678231
SID:	2816766
Source Port:	49704
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497006171520250 19 05/30/23-06:22:37.625556
SID:	2025019
Source Port:	49700
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049703617152816766 05/30/23-06:22:55.907026
SID:	2816766
Source Port:	49703
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	
Timestamp:	192.168.2.3212.193.30.23049705617152025019 05/30/23-06:23:08.061417
SID:	2025019
Source Port:	49705
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497016171520250 19 05/30/23-06:22:43.112445

SID:	2025019
Source Port:	49701
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 212.193.30.230 - Destination IP: 192.168.2.3	−
Timestamp:	212.193.30.230192.168.2.361715497032841753 05/30/23-06:22:55.906759
SID:	2841753
Source Port:	61715
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.2649699617152025019 05/30/23-06:22:32.082582
SID:	2025019
Source Port:	49699
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	−
Timestamp:	192.168.2.3212.193.30.23049702617152025019 05/30/23-06:22:47.971581
SID:	2025019
Source Port:	49702
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 212.193.30.230	−
Timestamp:	192.168.2.3212.193.30.23049702617152816766 05/30/23-06:22:50.317410
SID:	2816766
Source Port:	49702
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file

Networking

- Snort IDS alert for network traffic
- Uses dynamic DNS services
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to modify clipboard data

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM autoit script

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Starts an encoded Visual Basic Script (VBE)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

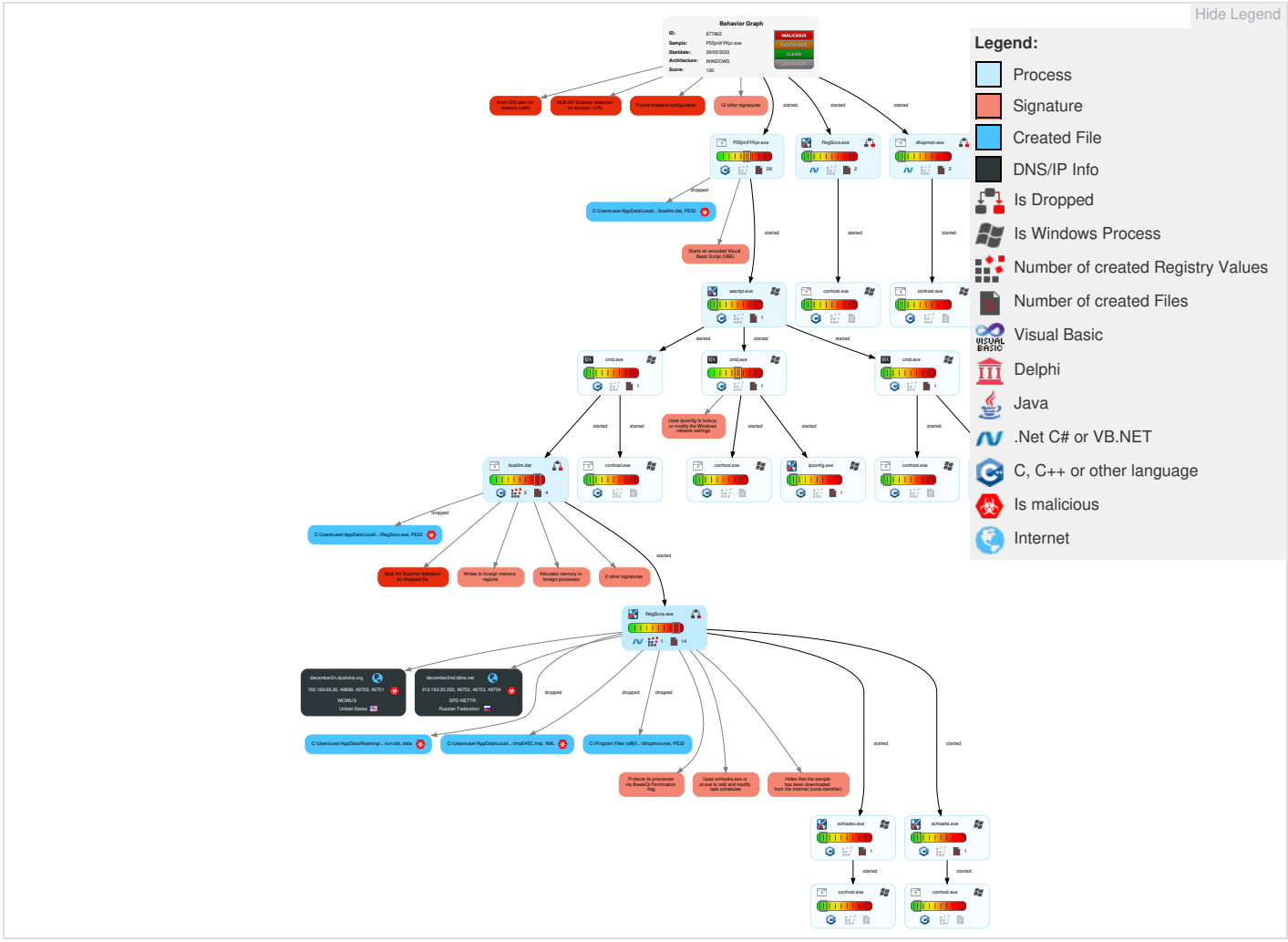
Detected Nanocore Rat

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
2 Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 1 Disable or Modify Tools	4 1 Input Capture	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 1 Scripting	2 Valid Accounts	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	4 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	1 Scheduled Task/Job	2 Valid Accounts	1 1 Scripting	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	2 1 Access Token Manipulation	2 Obfuscated Files or Information	NTDS	3 7 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Data Encoding	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Scheduled Task/Job	Network Logon Script	3 1 2 Process Injection	1 1 Software Packing	LSA Secrets	2 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Remote Access Software	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Scheduled Task/Job	1 DLL Side-Loading	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 Non-Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	2 1 Application Layer Protocol	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Valid Accounts	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	2 1 Access Token Manipulation	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	3 1 2 Process Injection	Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Hidden Files and Directories	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

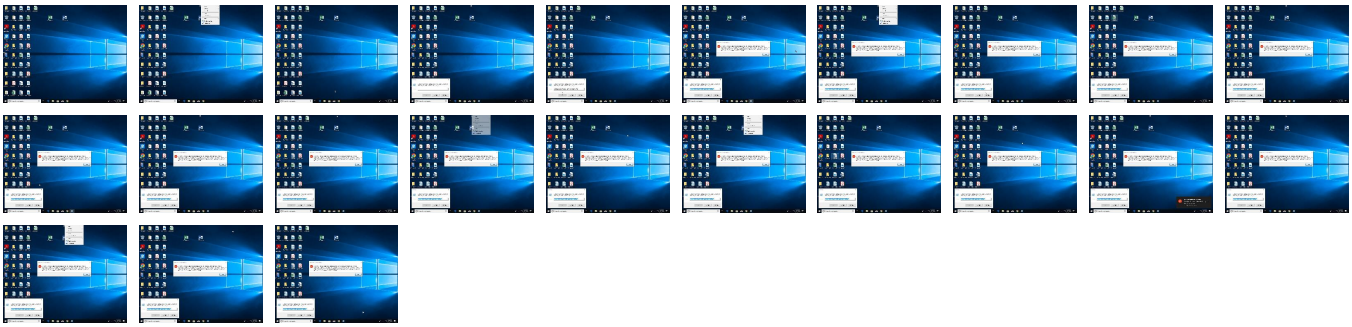
Behavior Graph



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
P05jmXYKpr.exe	70%	ReversingLabs	Win32.Trojan.Leoncem	
P05jmXYKpr.exe	68%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat	53%	ReversingLabs	Win32.Trojan.Leoncem	
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	17%	Virustotal		Browse
december2n.duckdns.org	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
december2n.duckdns.org	19%	Virustotal		Browse
december2nd.ddns.net	100%	Avira URL Cloud	malware	
december2n.duckdns.org	100%	Avira URL Cloud	malware	
december2nd.ddns.net	17%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	212.193.30.230	true	true	• 17%, Virustotal, Browse	unknown
december2n.duckdns.org	192.169.69.26	true	true	• 19%, Virustotal, Browse	unknown

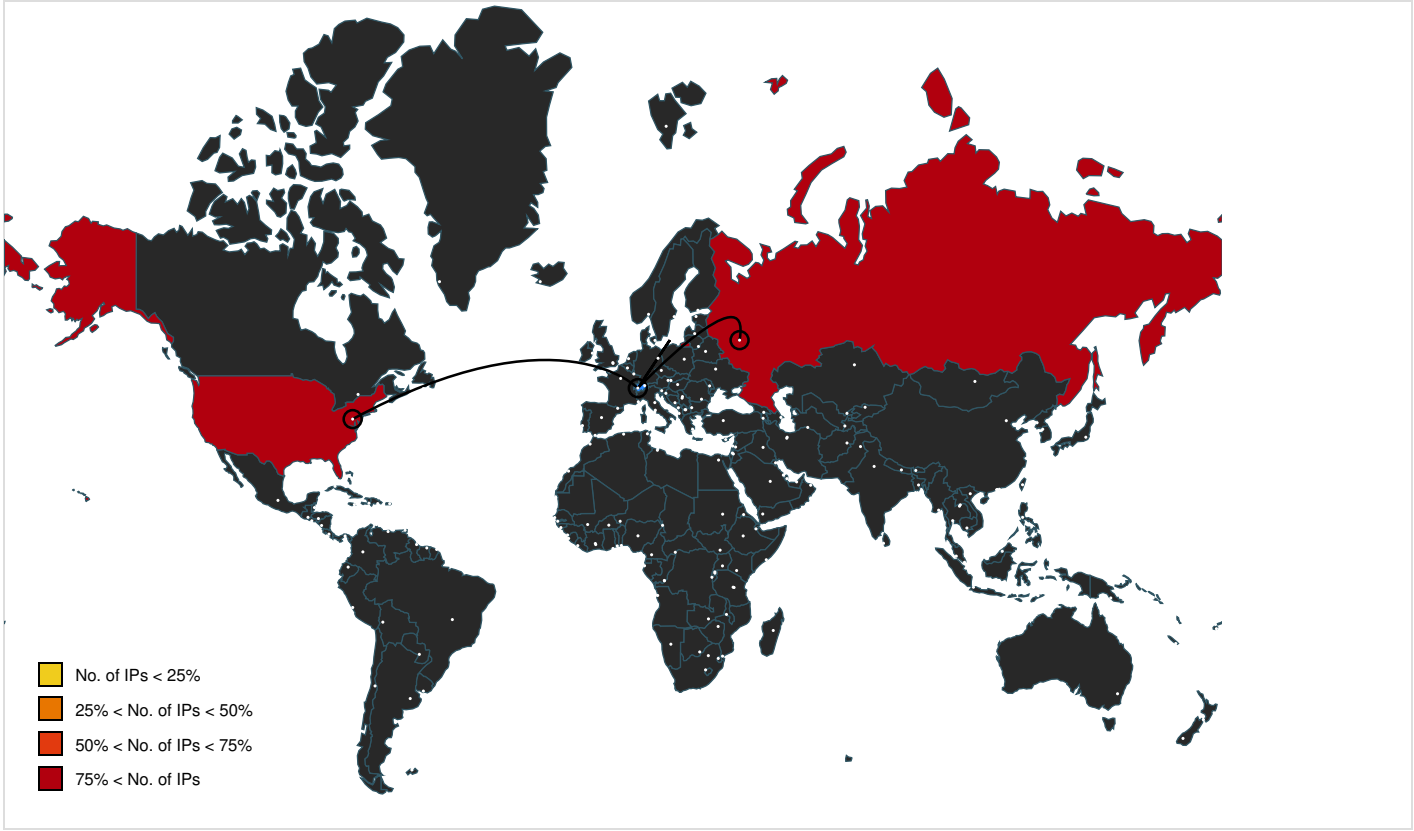
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
december2n.duckdns.org	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	RegSvcs.exe, 0000000D.00000002.636564713.000000000383A000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000D.00000002.643242754.0000000004AEE000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000D.00000002.651236156.0000000007AD0000.00000004.08000000.00040000.00000000.sdmp, RegSvcs.exe, 0000000D.00000002.643242754.0000000004977000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.autoitscript.com/autoit3/	P05jmXYKpr.exe, 00000000.00000003.377814211.0000000007236000.00000004.00000020.00020000.00000000.sdmp, boaliim.dat.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 0000000D.00000002.636564713.00000000037C1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.230	december2nd.ddns.net	Russian Federation		57844	SPD-NETTR	true
192.169.69.26	december2n.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877862
Start date and time:	2023-05-30 06:21:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 7s
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:	24
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:	P05jmXYKpr.exe
Original Sample Name:	db555a9de355c70681e2e5f9ed38a335.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@30/36@16/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 99.7% (good quality ratio 92.4%) • Quality average: 78.9% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 98% • 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, audiodg.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:22:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome c:\knmo\boaliim.dat c:\knmo\ikvvfncnn .bmp
06:22:30	API Interceptor	856x Sleep call for process: RegSvcs.exe modified
06:22:31	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
06:22:31	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
06:22:32	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate c:\knmo\Update.vbs
06:22:52	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\RarSFX0\Update-ta.l.vbe	
Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	34862
Entropy (8bit):	7.091025192719944
Encrypted:	false
SSDEEP:	768:QOD33OD3gOD3WOD3vdOD3iOD3EOD3vTOD3w:J6dT7EXZ7qs

MD5:	998B0027EB59F3283BFBC0E95979CABD
SHA1:	8354C76C835B137935DC8B8576F1902F8670E868
SHA-256:	44F0988D28CF5474A366DEB9CEC3B2BE6AB506AE55656D16A9E826DB5980257D
SHA-512:	8A0912145D4D43D3E20606F6DD6E9EE83BE73C369DFC15999CE0E3BF57E38C4773E11293B7B564DF6381DCA8EAD775FCC7F2639420A6F4DA391E604442570D9
Malicious:	false
Preview:	..'.K.M.Z.4.O.Z.9.4.8.f.Y.f.b.a.V.P.C.o.p.W.6.2.v.b.i.2.3.y.9.0.P.g.c.....'.H.o.1.3.4.z.9.a.8.7.b.....'.w....._..9.>.0.8e].,.=`^.....p=.:.jL..i..c..k..MKU..}...9$.|.*.{.8..3.....>.X.q....'. ..._4O..`%.M....9.FT..C./...:3)Y.v..T...zI..#Wh..f#.9.oy@z.3...d..s.LW..pd.."......1.:..)8...*.)Iw.p.16..p....R...M..%.....yu..'.....'..np.u..3.F..t.W.....T..Z.J.;...fK..E..q.....w.E. YsGz...i....._...2.y....mh`../.U0z.20F.&..#...`S..KR.,....Sp.f....V...n.-.VE.4+...-..0.|(?.....k<.....|.'*.\:$hvJ..A+..v!.7.\h0.....'.j.4.x.3.2.1.P.2.1.9.E.S.4.8.2.h.8.1.2.9.b.3.O.P.P.1..... '.2.0.0.j.3.y.....'.1.3.8.k.1.1.z.V.o.d.A.7.Q.1.F.W.7.....'.....T..}...)......u%Yxm.P.v.v..Q...{.4..`.%.....Bm.)K.....!.K7.k.nO....Z...9.....[..^.\...I..(....-0..])O%...?s..R~ .|.....D...7y..... ..K...G.(./.;..+u2.J.ph..J.....Q.....'.....3.....'.L.9.G.v.6.F.I.O.8.4.U.Y.9.A.t.i.q.8.Z.m.U.7.a.R.....'.....tc.Z.c" "~P...c<....'.).YE...y.h.O.e._E.....q..mo;.....8...\.b2.?.B.....c.

C:\Users\user\AppData\Local\Temp\RarSFX0\Update.vbs

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.7227105278432004
Encrypted:	false
SSDEEP:	3:FER/n0eFHEBi/JMMItf5OdPTTQoVH:FER/lFHd/PIt5oPoIH
MD5:	4B6F1A54F2823912817EF376AF2CB300
SHA1:	5DA8FDC368156CE4DBBAF8FC8883AC3D0D1CEF62
SHA-256:	2D77855D782CC56D8C74ECA587E851483F9869AF112A830B1FBDA9FE1FD808D3
SHA-512:	A154C1B1CF86F7239308A77B8548B8BCA1E62E261F04C8BA53CFD74B08B7FA5F4FF3A140AC20E5745FBCD1F48CB56BFF3352E2F3AAB1AA46529C1816F42B1C29
Malicious:	false
Preview:	CreateObject("WScript.Shell").Run "c:\knmo\boaliim.dat c:\knmo\ikvvfncnn.bmp"

C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	909912
Entropy (8bit):	6.602467450731382
Encrypted:	false
SSDEEP:	24576:sYgAon+KfqNbXD2XJ2PH1ddATgs/u2kaJml:s37+KSbq5e1diEnHaJo
MD5:	D70543055E19B63641C7D5CB908EAEC7
SHA1:	C4CE358B96ACCF34B885B56E49F242B847FBDC6B
SHA-256:	CFC03A739220BEF4F9BDE940B1CEEA4E3041DD7C1129C72F0EACC25CD76D0106
SHA-512:	34CF463ABD0ACD0B2B2E324A46B2506B8313FD7A5DBD9BFB23B0FA24D1FEBFC5586D804A7289CF6C0CDC64B6282EE6ED6910A7FC5BA33468F38969F8AB353BBB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 53%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..h..h..hX;1h..hX;3hq..hX;2h..hr..h..h...i...h...i...h...i...h..Ch..h ..Sh..h..h..hl..i...hl..i..hl.?h..h.Wh..hl..i..hRich..h.....PE..L...).(c.....".....,.....@..... .....s....@...@.....@.....|....P...E.....X &.....Pv.....C.....@.....text...|..... ..`.rdata.....@..@.data...lp.....H.....@....rsrc....E...P...F. .....@..@.reloc..Pv.....x...D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\cjeugvqj.txt

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40183
Entropy (8bit):	5.582554582462828
Encrypted:	false
SSDEEP:	768:2MGYLiMUg9lcJ1aLds6i5YhFUbh+IOsdaLJuwd9B4rRJ8oLfzBz:2M/iMUrJydsMUMI5daLJuwjB4QoLzZ
MD5:	FDA288802056526936033992B8E7F65
SHA1:	5BA9FB1FBEE9FCEF4D09781EB246F560BC2D4A55
SHA-256:	90AED0CA38C37473AC9761508F946E730391F00CCB01CB71B9573D2E64E9418E
SHA-512:	EB0E12F8A4310B7899B27F2D3E62639AA3E6AADCBBA575A9DA9B708EE11B0798FADF99F9125AE4E1AA7D04D76727BE8446A3A93D768F35243DCE3A4B4238D924
Malicious:	false

Preview:	c781v4D85p06Kjqmq6XJ93aN1ED3u24fOrrQ6HQO..02Mj8S2p1E2n5BvYo5lWH43g9o6..090tTE22508D7V3341F6gtx3669qFw43C7g8r9091y85h0YL13eo680GoVy 0MR..2Vzfrt8654ercc7P3NNx4sG81bU6XD91P..8i7q6SRYkKg3PrS3U209agZ0mqmr7uy424LpAPT862CQZ7a59Y1h8iXZG3GgdfEK..12Ja2d4oX9a1q0f84K9tKPV7 12l0S8AMqf..11233936cor1YN1MN5jt44PEYW50N36267e8U9Q4Xh680722L3g9O871r9Xt51AZu4j43n5l1..5XMowR58B1055UWnhltiE7OM3SiZg1tQtf469b88j4H 33U3E7W1dNb98cpM2PTAtP1bM57813U0u9Cs42S2..ATK7j775uGj2p11NXc17Y3G23Ped1iz7b5hm5912l541008Cd263uZUdVt0228N..8PFE42843692n3RCY4UV97g lBPzS9317I0lZQM4us1l6w22345E3B756gBri5l643v55sCu7gw8..87pHuk6HW2LAto2516Ba9T9A5x17l4d0jid4r6G552U89s6L2vE8A..74ShQ9sFzftQtQG6r0BV3 123gJw64VOQSX1JD4h6b81s926A1qO1t37WhsE5g2YWr21v6Nu6857..8f85bq521103ltYlZ..jW1901qk337r36MX97RT838U74i4bIeiuD0531a48Z3p4l4Zc38Ti32 b2H6vSG3..9r2PrAI73VpnD7F4479h359d6Nr3w0zPM0192N4060ESBAS80nci..4xT889U635Q658o975l741Y029E24ZS25s8WJp55pS76yX3iGVVGpkyMKpf16k..99 0K1oqYb4C0Rq3b0UeF61u6Q8eMV32L42975C5x825n1J..030E5d6y74D6l88mYgG2kT7275r2p8g77a5J..835Pn5

C:\Users\user\AppData\Local\Temp\RarSFX0\dnggql.bin

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.677861047219423
Encrypted:	false
SSDEEP:	12:/uwIGN5v3xSQUTM/LLdmGj+H2Mz5S65Ne3ukruxwMXJ9Hj+34mhXKmv:mwl25v3xSTo/1jLMAk83rlHY9Xfv
MD5:	CCBEF5AB9429D5D0A42C1291DF553332
SHA1:	29C9B657160C76AB7DE342CD64118E16EACC516A
SHA-256:	6DEBB303DD0986A0A24FF2D14FBF69D5B776E88AD5D69BEF457D9FEB0584C4AB
SHA-512:	7E39BDD65F7FE68A6D8FFAD49FDA60410663B526A6D355C8BA8BC253BA7E5A26ADFA3E7556F816AD14EA82FDCBE0596AEB6733B921A5325930A79B2D6A7685 23
Malicious:	false
Preview:	3w0Z55i499Kj690aj..StructureConstants ToolTipConstants..l3u5Pk49fs64D3725OQ06nr650P718iS3YROq29weh68N1SJ1M04B6TE27e75g8M7l25568L2wX0g090T71x c3tpqwk3j8AiGBXLDf0636KH9EU62w5WX0bcz379ml6571gN3esB0vGTWLuC19V8b93nA9..ToolbarConstants BorderConstants..8C65YBuln3TPyM7oKWW25WTS 6GxpiXR3368fHJ10Apx9W94ni2770t288771703Qj7x3JLT1g1q5..FileConstants DateTimeConstants..LCR2UbH22Ua20s176bs2BU57m1Ws70G8237ih0A28w2 rDn8230JO9L644o79618KG1wjy65q9V8325w62Uo7w2RV352c4RCtqhS..ButtonConstants UpDownConstants..L7444zw64SO3XzWXS82E417wQI84Qq3j965DO6l ZLn041k7f3B3GZ2v8Z2qgvvW9pc350yx489chaHY53xr14J1OdCws201082fb4115gB6UT3QA707ZiYM1m59a6o5200IDmC14n9f4iz08u6NF0FcG8k9q180SFo8xMmm.. GuiDateTimePicker GuiDateTimePicker..

C:\Users\user\AppData\Local\Temp\RarSFX0\draovqnp.ppt

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.61420691526579
Encrypted:	false
SSDEEP:	12:QyqJyPevEK2hHQgXpUPUW40LmKpl5H0WFmTzBo:QRJqK2hH9Z1W5bpl5fF7
MD5:	2464923D96F4CCB9E514843726D4699D
SHA1:	0E59D7286245F567E91B4BA826CB19015F807C91
SHA-256:	979CEE496158E406A273787C20B85C747B42371FB2C0B7C391EC39FF1514614E
SHA-512:	AFD9DBCE1A847EF45E3296092AF01E7D83E10D19700BEE81C25168743D664D17A77A3B41574C5DD71EBBB6487FA56B12CA2EA1E912617397EADF3B11E5D1A0 0E
Malicious:	false
Preview:	Q9c04788C2zb6652vJo37gJ9fKP10W36CAHF3W4hB348al5..TreeViewConstants DateTimeConstants..60guZ5Oaq4pjL8N2Y4438Kj1AU90t66wNc1B4m7021L4 40486fk756J5r750pVr..GuiDateTimePicker FontConstants..89oeN1540l8HEID2v6uqGA8KTLiRNma065957h0Z4vS6J55W6zvM29641tQKB0Qj8Z6827h150l2 4pRDK7qq3lU05100ty2XR97KW26V..ComboConstants FontConstants..f69U5675278rZ7Z5560i9568SPpTM6osdel4518u1Pi29WN3JuwWL2D760l92D82310Q1Z yhXE9J8y4h454c7g7C3433ea2X87l5X4iK66V6k39Px89ttkNG5y2T7oI73Ci3L032jr7RD98QSRb35hyTu5n5q8DM93pi4x..UpDownConstants FileConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\ggqkqbgc.xl

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.545663580105036
Encrypted:	false
SSDEEP:	12:8uKixHe/LqK69cMfFyrSRnCR0RCc3KTV3qyNIoOQQ0Py:80pe/N6DdyonC0RCdwyNIo/W
MD5:	BF23A7ED26731B18D7922F9E6EE71B8D
SHA1:	D7A835667E4CFDA4B92DC012CCD2B8AB58EA11B2
SHA-256:	FFC2B93B6811894CA06BD693F2D6E05404871C24A0C4F49E262739BA2B84B28B
SHA-512:	53BE801DC9F1111030C012ECCB546DE4EAD7B3528414223292D2499C954699512E3BDCB596E188E88FD525B732C8D10E26E3B99BDC3965CDA7E79FFFB7415D 7
Malicious:	false

Preview:	v0b9R571RO6rU84SJ60TI7Mg61n7J85d61570H1hP1XQY5Ww240SjAu0mmZIVwV15628C3xUU50165B2YV2c2Q9362whk7c36Z9VC59h8jw6FaF3311p8bJ0 4689Ljwo030PdMgC82325Z76p..ColorConstants ButtonConstants..09ZUV0tj3iBs057F96d307MW932X3e3YQLk07yJv7W26O3Haf9E63Aj4m1d023gK4v48o12 ..ColorConstants StructureConstants..aq4u89X4T7N787tGNzm1S028eJ5q383654M3Q225v5QVa74Mu4NoW36G..StructureConstants FileConstants..04Fb6c3324r K6J99zC5702U3mg0Dh1Lf3Ge9tUb0c8t668M5d484R0..ColorConstants ToolbarConstants..8ksLYhr221823o03z19N54xBzf73kT7x4N38o6nfav0q4rK9t31Ff2541f2xlw n7477i59737mp5F3Eif2..TreeViewConstants ColorConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\gmbxvlkihm.msc

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.507584372742505
Encrypted:	false
SSDEEP:	6:TMyFUfsqSrVpiXFU0rxCrNtKM7FbGQ2sq0n/UWWSQNUQDdz+H7PWJQo9d/SpX+hk:QdfspaS0r8rDZBiSqgUJU7PEQpXSDF2
MD5:	099A4822E2671902FC6CE161F8DA4ABA
SHA1:	526560B54C15AA7FF768303AF92F13FC18C5F7B6
SHA-256:	CF28AFC0668594A95AFDBC78BEA31BED8B6F1B0EB15EFEB695E67B4CBE00C24D
SHA-512:	4FDA30C82B680D9A15A96CCADD9086063B6B61854470F65DA6E85314D026C9FC85DF9A6C843175C4F7CDADE462C8100F3A38CF1159A98CAB52D91AC2530D9(D
Malicious:	false
Preview:	4P09361P4G11P0Aw8X5736fk1O150e92onveU00p361586X7c140yg0Om3p..UpDownConstants GuiDateTimePicker..Td980D839002K089t56hty62k5jC4B4154 QvX8y23Ms7l3L4Dkv415cN0n401vETZ5OCO24s3HQW322Q9a4T5B38RV6Yg61b5HD97Q041bRZR1r0E7Kj714ucPSjjRp36rpn88K55xafz97100q33..FontConstants ComboConstants..3a0sr5R6911iPl0rkyWc53C7l8Kb127Va75Kk7b55J7WsYdYKemf1EcDuMB7520..ColorConstants UpDownConstants..u62vZ42540E3coHJsDpESt0241 52211700Q6Bs38X2523Mr2mS2807R9QM6897N34745t2kcn34a6fK80r846OT827F83..DateTimeConstants ButtonConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\gsau.dll

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	5.607689829507894
Encrypted:	false
SSDEEP:	12:A758NcycAF8Q/PqjmIUrJYJ/QYrumfbKQaxbsuXW0:o8bcAF8zlJGQaz+ZbJW0
MD5:	9A7680A212F373D14BFABDB65B2E0E24
SHA1:	C6C6C05B6F02D5BD75D8D6D2F36688697F44A16F
SHA-256:	AFE60D1645A8A9326C30A79B3673FCCE74EA88E9E17EBFB159641E45E6DA62BE
SHA-512:	61DCFAAEA010725523FE800B7E3DFAA594184E0A798A41E454C4C0A9C5BBEF231F85865214E1C97080762D63C478206A0EE2D90270B96F7E00EAD9C2E36A8EE 2
Malicious:	false
Preview:	758qz81Jm36k95w11MSl1rQ7..DateTimeConstants ButtonConstants..4336i4784C2g4792j9c85883ffi21Xr9uBUA971dw3x..ComboConstants ToolbarConstants..9 i7785G1849866j6D7F777O7kcs872A380v9Dg51x10kgJ249kzzq2L1J20R7Z4Tr5E5DZ5Dr22YSNYA2E..TreeViewConstants GuiDateTimePicker..h62YT..ToolTipConsta nts DateTimeConstants..1Gg67MIG1ckf2XLK3cP09rnb2gy69Q15JkwX1nS20O86U4K61s678dk3807Ak332LjV48624nl4hw9rUou7828S085K652r54Gn98Mm0sO9 l380XAwv7yPP99Q4H..GuiDateTimePicker GuiDateTimePicker..b2ZWUv8u0fTR2ilY341QBu0aKG7M5J06R8C8h1o2AJqv2B1h72qtrPT5RRnL85pC1LY4693w3k i6v10Z77fp6Z14i4MDZVf8ne281T..UpDownConstants BorderConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\hsfcsirb.msc

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.627465718803386
Encrypted:	false
SSDEEP:	12:3imE4mXcsaHlumLFQARaVT7c3UptnHEh6NKjXyPq:SmEhXcsabmhlRaVNtHEhqeV
MD5:	ED8B39554FA55A099A30D463C71E38BA
SHA1:	1A16C296614A7E57A3E7B92C06B6BD36734BDE2A
SHA-256:	E1403D1D1E752FB0CD4995B103DE41CC354070AC460EC2FA63CCAC5DE9380A20
SHA-512:	022CC1963D9ECE650ED7746094CB0A6682561E5386E4F452A5756635B0B191F50C33A6422F2969E115C13F8BB0B976E3C89F7125D6D3C9590C34975FC43D1ACC
Malicious:	false
Preview:	hx5B0631wz37BquqfC6a50Wsk78787018U5..GuiDateTimePicker GuiDateTimePicker..gZRe8kv937LNLLHixq42h1NHF358T71365CN9U4OxPK06C58rP9E41at 8QnM3z0RAl1qN3eO31OuLFJD0Dcn3ilK8x3064qMZLPu4o2355512VEKt04CBv4g71tacHN2AUR5F3Q8PkId7j55Hm5U7l88f4L72D346W740..GuiDateTimePicker B orderConstants..8op5Y993dPup1631mn0Yy97BQ59khKH8..BorderConstants DateTimeConstants..2GIVi8eDq2X762N6722u6Ub..ButtonConstants ColorConstants ..8U30w40Ou1j040G5A2W79d0I721r51I8Q2t5c501p4pBE69a8uO3g3jR3p103gG3q32qv27R33U9O6C9CX254We8i766L12Sa119..TreeViewConstants ToolTipC onstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	data
Category:	dropped
Size (bytes):	98000414
Entropy (8bit):	6.980315985645683
Encrypted:	false
SSDEEP:	49152:gORNTfuVImlH1cy2R3YL1wEKGB+3cOyKztb2629q1Tw4igHsuI78IdZS34thfhFV:O
MD5:	224353FCD92D49B9DFC259E1DC19A5E9
SHA1:	1EC921E5F5F2C5577F0633F83EFF1D315DB013F3
SHA-256:	209F04E9B26AA11D09821B11FB325D6D52989AC730369DAD2FB25464BE48B5D9
SHA-512:	3DFE8A57AADA00291528DCFF3716E8BE7D8FC893FAA8CE00C8FB6E4A9F553CDAA68A51762881333B605B3E4E18685DB93CC6B5C2368B2BB4D9C16864D0D93F8
Malicious:	false
Preview:	..;..&;L.2.I...v.TR8.z..k...).#...`.7.F..&.^P....#.c.s...ka....PS....~nG.VqD..v.|[n...^..p+&#...w.....E.4.l.4.h.7.d.T.B.6.5.q.4.q.4.O.7.N.6.1.4.3.1.0.2.2.1.1.z.l.....2.....#**....(.~T)..V.....R..I8...@g.$....=..w\|._.<.....j.....f.@..{;...6,X.....n.....JJ..p...w...o.....z....1.5.v.K.O.x.x.o.r.D.H.s.q.Z.n.v.9.R.7.5.6.C.x.3.8.1..... ...a...B.m.....#).gz.d....J.m.....gR..q.e..8..tuOJ.QCb.#...#..s..D.f.=W.....MN.@.!"rU.9.{+..8.aF..$.z.AF..X.p..u\k>.....).I.(.Jq..3$.B)IYF2..g.m66"...@V.....y...A..F.x.....t<.....M8.....d..O..".a.H.M...g.;.FCG%..ye%\..WZ .....T.....=c!j...~.,..,%..... .sQ.4{.bN...:\Uz.f..,$.,.!.B..q...E...p..{U&$..W..`.$.....,L'.@.cRH....8.....1.5.b.4.n.3.n.c.D.l.0.l.O.v.F.7.5.p.7.8.7.3.0.5.s.7.c.9.h.l.t.j.6.Y.6.b.4.3.R.1.b.1.2.0.r.....l.Y.r.Z.8.3.9.6.v.0.f.0.3.p.1.7.c.f.q.x.s.w.R.9.5.4.B.R.3.2.S.r.1.t.U.T.9.6.7.9.5.J.3.6.5.4.p.7.6.....#3.a...)..#...8...yq.t....$.9.r5..Ie..#xq.s5<~..0.C.T.iK..... ...I...J.CA..|o..n

C:\Users\user\AppData\Local\Temp\RarSFX0\jqdgnhnhre.xml

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.562755778898995
Encrypted:	false
SSDEEP:	
MD5:	F6C7C5A49B0EADC97C63131991202F58
SHA1:	0F3D4CA96FE7DF872A4353BEC03C349AA889C869
SHA-256:	60311BCA5CB7E4011CF68AB3A5923BC834ADBD79C0840290C443E019C4188FCE
SHA-512:	615F823CDC596C4DD0EAF874C94252BB378899097A1F55C9B06B26B449EAC22B802605F633993006E6F815C30AB348272D9D2511EC0BD4C064B963601D456C19
Malicious:	false
Preview:	7L6j364418U232q31YZOv9r25MM34594xti0K78fz316XM206n44U75342i187AF25m0aUGuw1qE0M9J923jT577Ng8t859w50Z6V98VW0g1w4413s025754t4jX4l..ButtonConstants UpDownConstants..jQ03V062ei560BV39SSp44VZ1g8UY0Rx14YC5o617V480s01hwR3a78ex9l18I736n38S880wtd3C93k79f9w578Y8P1DvQ8G8n1BU3mzY3WKrvr4v6Z73PGfR4N38TBm47tod..BorderConstants StructureConstants..857gT34164X404z7R798Wt4Pvv4Sc8P7q2G7Bb67x390Fd9h1V1g84QzkXd804l7827Y1351zol981Oe6P2col1fBseKDv95Hy339bPwA957K70SSX56O4f594J0kukn7B51eNjx8yPg6h8t1T09v2V60N580v9SOr3..FileConstants GuiDateTimePicker..

C:\Users\user\AppData\Local\Temp\RarSFX0\nhoxu.docx

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	512
Entropy (8bit):	5.529365166129993
Encrypted:	false
SSDEEP:	
MD5:	D4E1AAB6991C0C1AF02C7F16D6EB9458
SHA1:	A047C8DC248DE5E857F0A4039D24D53485B27350
SHA-256:	FDBAA2EDC1087277362099CB493A000A48D285AC598933A9828909F025F40280
SHA-512:	50E9C09AFFE24A3011519550B1898672214FDEDDCC1B6CAE71C940079FA83BD6DC2D15C10026D24B9553B56B8FB99DA27F3977BB31E798CFE2EB0551C256504
Malicious:	false
Preview:	12u32Q9X52S2p9Y2c6123KxSre30971429y3S75D60862p0p5q9E90vub17m..ColorConstants StructureConstants..JO1T760x9f020WSwUjzl6H0TVpy7rJi436Rg859IYz5o67RXE7QO14sLU189l4..TreeViewConstants FontConstants..N63480TxjK89W8z9dL9jDL6H4375L..ToolbarConstants FontConstants..1re2t31a3Dzv4H6N924uw0gkSq4sZ1laWl4u5O4cfcdO879Z5i3Z9t92N17A76zmb13u6tbUQ7U4pp45..FontConstants FileConstants..01B80N7pWXjl0nj484N8Oq6Xz0h15D9gNtHe0Ol1G92l5J..UpDownConstants BorderConstants..n47vPs18vdimC7Ky85GkAgoNwP00c8..ComboConstants ColorConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\nibh.ini

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	596
Entropy (8bit):	5.634463495541907
Encrypted:	false
SSDEEP:	
MD5:	09E859F88E268DE999BAC15B79120559
SHA1:	FE05846EA36F415C9E9E3F073926FF312176A820
SHA-256:	63D2909F815AD46DCA32B9617BC285172ADA6FCEBEA29DA8653F7FCF1657CBA0
SHA-512:	58C9DEFE228984257C38C1F21E90024A162DA03C8958A5ACF54C8C7CF9E10D71F1A1FF42637A21938FF10CDD6CE0CC46C229DC8EEF5AD38837FC9B0BB96A4E3
Malicious:	false
Preview:	1LBieO772d0x2BBr99180eII61X1P1u4KS0zMNQ77nW24BN436695op616jA3d..UpDownConstants StructureConstants..8322w12f981DxY547Rg08lI13a5T3h j11HT630nHymD8k9CP79861Rvac50Oq11Usx8VJ42Lm04wsz2uSf7BR9ypTw82Vhu4iny4O8Zykn557q088D3v7EfX68bE6o65c3Bp5904J5ZB11St46967EA6C34qz67Y 85tDd7869e7t58049..DateTimeConstants GuiDateTimePicker..30KD3G7nGZ042AcY105e2O47wU11x4F1Py336f73hHaPA0H1pET314xw2q02Z6c4A9225t6165 CV5SsW8NJ4Gt0CYh4IjGy5494X1K19..StructureConstants UpDownConstants..l2N52680k26O8vBT659qqLYkB9s0VSHl2t71G7e49z65wqp44753b821MOmDl1 1C5hylQalg8s5Kv2n9CA1C2E3U0aM97l91W8FfKI..DateTimeConstants ColorConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\prkwlrpwug.bmp

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.404161121920393
Encrypted:	false
SSDEEP:	
MD5:	3350E3C8E8DAEB531E07F846AC0F142F
SHA1:	8C72765CC982F476D3ED953EE4297B4187937F3B
SHA-256:	4A7517DAFB3C2AE545585328B979B09C7663E1264C80501DA23295D6220EA063
SHA-512:	AB3817A279CE9DAB4922059900E9799E0B84EA0C39DD8B797DDF9826628196FBA47A0F44DA9FFABDE3C6B334EF8ABA26DA8B3411437FA224338E9F2C8EC35AB0
Malicious:	false
Preview:	9b4D917H353..ToolbarConstants ToolTipConstants..04X5146l3QG85s79P8m9XwRD6g4l8Fw3c22z8ePhd3cmM42YYn46d0G7Gkr6M8YG7U86y2f91D10f1K550 03SG23H32w954W3T51Z5s324U64m363Bf60yG94482C1r6ZX9D13hQOu21Z411o8H2679P16tdXBY1k646M55..ToolbarConstants TreeViewConstants..1e04231 8sFE6722iDVboe458X8ZqT7xl4k0T1D7G0863526CQ42Mw..ToolTipConstants ToolTipConstants..pa1xUlvH6b03I7880kTFXN54Z98s1b24..ButtonConstants ColorConstants..463Pq89n2Y23424Y0eMI9879dU2y39Uhf6Cm30qU24645i9ma541N562ViB734uo9HY554Cinaq83r46Y..ComboConstants BorderConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\qbjxqxvrm.ini

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.547005218041853
Encrypted:	false
SSDEEP:	
MD5:	0787094CCB9A5E8D7D2E294B14719444
SHA1:	0C4C9DE4B550461B3F5D80D1E8FE9CEE6F3F912E
SHA-256:	C09D173EC6444B7428B92EB564C62C5FFE2281DF63EC084B3188C539521DA1E9
SHA-512:	176C19DBAA297863E00AC0F08FDFB41C05EDBAD3F1C67FB5F63FEFF3E01CE5E327734BC96999E8B4D1A33F904DFEE2CCF5CDEB8B50ACC754B7C935BFE14B7D2B
Malicious:	false
Preview:	gdWv210gq9cY6Ra4N34a3yj4lV11p161t51VW0e1uk70H90NfU73yt70ro6829784F56bVnPvt3yX5Xv8U3xXz1c1AJ36r3v5O0329B557W0TWu39N70x3bfZ48b761cm1 Z1v920FXo73740Tc882D9lN44586261CS6..ToolbarConstants ComboConstants..taq12bZ417Bl4cyp0CM781285m8304f79R7eiKoDP01U83560BwC351k691k2 05l3NhdMd2PMU3230vJY0e1VzyXHA1Rx9v51l28mb48C06g9XNYL0O1nIW8k289YQe13vyA6M26de2Bo34R62ql8z07mN968889Dzla7a8Ty7126k3m6n622929..BorderConstants TreeViewConstants..RKQs6r7cunNUbqZ71759x5U736t4Kz1K9Ffc376bfwH5D0..FontConstants DateTimeConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\shjgtph.kmt

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	407523
Entropy (8bit):	4.048835164908167
Encrypted:	false
SSDEEP:	
MD5:	C652D22B20629DCD29146B09FF90C5B7

SHA1:	FC05A29D60E34ED153BF5C5B257460B85967BD0F
SHA-256:	8245A77BC68A9B141B318066C6BD305825AA175823D7BF6A6D1B79DB198A328F
SHA-512:	614A92E3529E9A1B3C8FB9AB9F93DF734A47F4ADF527FB9659A4D579CB23ECDC32D5A649061308C50C13AD3D215A71BD9F99E29789021CA1F71544C02451153
Malicious:	false
Preview:	0x4D5*9--3---04---FFFF--_8-------4----------08----E/F_*0E-_409CD2/_80/4CCD2/546869732070726F67726/6D20636/6E6E6F742062652072756E20696E2 0444F53206D6F64652E0D0D0*24-------5045--4C0/03-*/27E954--------E--E0/0_0/06--C80/--7E0/-----92E70/--2-----2---4--02----2--04-------04--------*-3--02------02-----/--0/----0/- 0/------0/----------038E70/-57----2-2-787*0/------------------02-0C----------2---8----------082--048----------2E74657874---98C70/--2---0C80/--02---- ---2--0602E72656C6F63--0C-----02--02---C*0/------------4--0422E72737263---787*0/--2-2--7C0/--CC0/------------4--04----------074E70/-----48---02-05-E4D6--54/-/-03--- CE0/-06CCC4--/8/2----------/33-3-5/---0/--//026F35--0*/82E02/62*026F36--0*/E2D0*2606/69//F0*2E332_030*2_F406/69/20*C---330E06/79//F 0F3/0706/79//F2032/606/69/20C---0330*06/79/20*8---2E02/62*/72*---033-9-45-------7337--0*/92D28267338--0*/72D26267339--0*/62C242673

C:\Users\user\AppData\Local\Temp\RarSFX0\siwhtkxo.txt

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.52295939542178
Encrypted:	false
SSDEEP:	
MD5:	471D3AFC0D2E98211F74B782365D9CFE
SHA1:	6061119FFEEB9B3E2494C768C5645A2309264EEC
SHA-256:	D8422D1C7730CFCABBEF0BE0938EA1B4426407F2A3174B109BAFDE30B1325882
SHA-512:	564A36C01D4D2CD923705ED84FF1561DD53B118853B6878B3D61D2AFC7498D67FDB9158A20445ADD501B18AADD09AA4B49C10CE7E874F6DC9EEC963E57BF9 80
Malicious:	false
Preview:	Q5csJ04..ButtonConstants ComboConstants..3R5287f8ITsh5QaUP57m133QD8Q79B2E5TdGu80RWE5yV78931qF1Cy51YX6N97904WL8GBn3v135fs59AlMvJuvf 4P8p14U90o99938g1kP94W5Dc5Lr2p8LUZ240VkR5323D..ToolbarConstants ComboConstants..8aB6WEzo8Y5S611C212Z9801G0..ToolTipConstants ButtonConstants ..g8voP8n02p5N9006QNB9Lg919CW8GUA58V90II32S9y7l2s09pc..UpDownConstants StructureConstants..981426703j3H96w608Nsp5zq5Pm895j9A80b761 6ZlXf2ACNHM09SeLx037A58r9Pr7k9RwjQF4aO713bw2P99057B39D..GuiDateTimePicker ToolbarConstants..T7oS0fzp6xDQ3Noh1h037V9mnkF013MGh7RP5G U7r6R11..ColorConstants ToolTipConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\tsxgodcl.msc

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	583
Entropy (8bit):	5.643721449601676
Encrypted:	false
SSDEEP:	
MD5:	C673799ABFD1A91853D69D6E538C94A5
SHA1:	5B7DBEF81362B2CA98D652B06480D1F3A6EF0AB8
SHA-256:	D32CE2F369FBDB301993F7EC754DD25BA7D55DEF3DB224EEC986B2D795EE5162
SHA-512:	9DF64ED6626D74D584324C6C062C307AD62ED79C9717ED163116E3C64CABA6A04105923828908687F024B32B514EAD8DEB12F45909B42EBB2FCFC80C45FB195
Malicious:	false
Preview:	OI4391186M32yl87Bu1OW783bQH1271BE6y89uOC042kj91635p12T601k9..GuiDateTimePicker FileConstants..1ixR49Pa024lK0d4251teiwI2S4M52WF4N84 33x180WaCV8Jo7K1O62e7sG226Q5gsL..UpDownConstants ComboConstants..0ec5Yg5V7Z251sub95VsJ6A1i024OjU6kkr3562BB332y7sM3H50f53fxU68C55OT AL6i985gR5c9BM13jSy4y8crg564p6J85943365YVk9k02doHMx6U740k431V4075K3zh..FileConstants ToolTipConstants..Cg29TUN145429hNGZc6Ofkaa43T 7ed57880d4RmBL8gF8SC0B4DTn04274hG6Nq2J8kR1BS9Q8y25eUGyF399h49BZpUKx2m07l297U1f7u4140NzK9488F0qc090G5CZk1M21r6Oa666HgCfE5 H173DGJbyD68df6u2ZMj6B89E0kdj2vmL..StructureConstants GuiDateTimePicker..

C:\Users\user\AppData\Local\Temp\RarSFX0\vmxmpsfs.msc

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	599
Entropy (8bit):	5.5610985457723245
Encrypted:	false
SSDEEP:	
MD5:	4165825E78065EEDC9C64FA7575876E0
SHA1:	549C00FFC79FDBF22121BA54D4B01C68126488BF
SHA-256:	7804BC05082A390CFFC4EF8C8F0856C5190BE6D85912241A2197CB9D17114130
SHA-512:	6B738AEAABE7BB55CC8A31BD51CE255A3565613E8BFC0DDC77D0E8EBF152FC80B1D55EAD4FB0B2E451D6CFB0495789A5D8546416D7A4756081AF8F221F34E 266

Malicious:	false
Preview:	vNeTT512l..DateTimeConstants FileConstants..M5pWL7820T25O1181FHqA10418bH9E9Jw850p329oO64H4qeG4L6po5W37lj7t83e08K8Bq0I2E5Lt334JN6SV02..Button Constants FileConstants..SX821272fh17zps6u5k12..FontConstants GuiDateTimePicker..346SA57K87X104493SClH14z7tb9p3k6rk8zJ5W09t0C519g18rrUq9G4Q3 nMKy72j81Da80kasZ5J7606F102v77m7s43589m8w8O6R9I5220GM83m2fJt91X95uRn15J93iAv877kpT1F80V69De59X8850w7QO9j9x4RBm3N1a4218200T0TZ688y0 cxywd..UpDownConstants FontConstants..2gqjb4n736f570y4vVVg7A48RgIX0941lewP77k43O36EsCBjYSM47U47tfj492L42gxX3a8jy4870P6g447H6B5q437468pPIT1g5 B30oP432Q8hqe..DateTimeConstants ColorConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\xivqfmq.pdf

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	599
Entropy (8bit):	5.621645197014055
Encrypted:	false
SSDEEP:	
MD5:	F711A97BE2732B8D02C95737C854A938
SHA1:	A5470B5154C2000D77D444AAD7E19939FC171DB5
SHA-256:	4EBFEB846ED6CA27AC4CC8529EF902C9A56FB71B06E14E1514D96A21BC41D959
SHA-512:	481EF16C01259D7A0D830643320428A21ABDF975B2058E11C508CB1BD54DA59F7683435CDFBE692792B9C57A0BDBB506788AA949C504B0CE4E1DA1A51F12391
Malicious:	false
Preview:	9G4i6X85bS88NE854LU09H6aTTC474F17645r40L6d8iHY9298b2i50h44012..GuiDateTimePicker ComboConstants..Y99f8895r2M8SZMm9Rx06W5sRv9E4y7I7 7Us55LBq67F33gs0alp7q6YVIzlwOm201113991kX1M1QH5Xl39W4StlW779RGv4v41GyK65807yW416..ComboConstants ColorConstants..U1E6QS9Szq78F9e94 0j3B4vsgTp9600ohHF8qGAS4u4hgA816vC931u6dwga8ygv372y7fjRZ56151h72F35S9H2P1wkF0hDNXn9dnwksq98V317mxi8947759Qa2dg18Pw586YIVqq91..GuiD ateTimePicker ToolbarConstants..nr30BC955..FontConstants DateTimeConstants..ltWd6ds591z30t80fQzrBX9g9X89t6EOXt2X3t3A5C44b94F0RPzbb1Xz4973pWQ s3b5az4a158Ul314jnVnqpoVIfPi7wzW..BorderConstants DateTimeConstants..

C:\Users\user\AppData\Local\Temp\RarSFX0\xwmakcb.docx

Process:	C:\Users\user\Desktop\P05jmXYKpr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.56446671260521
Encrypted:	false
SSDEEP:	
MD5:	05A03ED5B3120B420092518601CC840C
SHA1:	8AF644D3093E0E6E1A81E3F0A2F478F0D4387D2B
SHA-256:	DE18135659C53F7025CCE0FA6778B7397D83DA4CAAA9804AD311C6D67EC6FB23
SHA-512:	4E015A956FC8820ECC8CA4C950DA7A525EF8A33543B164C6A5FEBB5E37B40269B90051700587EBE72C8E92B41D618DC106DB2053C3464BF8D685357B8D7B737 2
Malicious:	false
Preview:	wk259a6FU8wozV726nR252VH7oo5SLk4ZEYy9Jn9B0hDwO74B5Aler6X20W4db89..FontConstants ButtonConstants..Wc1SvX7948Xq27P811NWou6y4R4UFu608 8l67O9V0uw55D4589QW4u89D1824WH8h1H7Vj9TTBc5y011Q3WJ381hext79750Tu4Q1359848O27a60P9eD4jH093b0..ButtonConstants GuiDateTimePicker..7 eqW6E2vff344xpIe3t6815A1V067kw00zR9C3xZs69oNj7619E7rw0R2kA5988n8m9R9yMT8oAG9vb7GQE6a3138850247PYy37177ldFR477Z2..ColorConstants St ructureConstants..aPp562Hh7QkP6h8edG6fRD8593aT4e3BP5DB0obEzR6106N669Q5l729UiF0l1u90FvO2r2id0228k2pvG58Syn6v88E0Kc53Z6j7628h73834Iy 80l8a272kz1bdQq943d91H86186ype8566462qZR60I2O9q3o57Zc495c..BorderConstants ToolbarConstants..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D 6B42
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o"....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Temp\tmpE45C.tmp

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.107159514403738
Encrypted:	false
SSDEEP:	
MD5:	211C08A48B92E556A855FB90EE4B0942
SHA1:	4E3ECFBEA0CCA0EE2743C0E23ED3FC79EB2E282A
SHA-256:	21F529F720EE77AD03AFD3CFA4CE04EBAF243C3E752F14C268529665CA936146
SHA-512:	B65C55C05249DFFFD0B52DF66DBA692CE21B6D447DEA43E93DACE718E40ABAC069A6BD2DC4CF0BC3F979A327BB7896BE6A3A36540916A33E0CDA8B974E295F1
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpE586.tmp

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	
MD5:	061E700FE27D852034A5A44BF5985CCF
SHA1:	15B072DE6D6FDD92AE36F074345FA41985833E8D
SHA-256:	4BBB88AF530693EB4A710B0591D4BAF585837242C5690F5A821BF2FC9CC587CD
SHA-512:	CF6C5458AB50C859740490985D1E7E887D1116F3FA947FF2EC49AF9997A42F3402C63EF42B93498544195D9859FBB19CCC295966564B30F5ADB4A36D4E8886C6
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L....A.t...F.{....C.|&.w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	C423895161CCF32B983D88DF7E278B61
SHA1:	945D1ECC89886799DC030BC511F5F8A1567CCE27
SHA-256:	7FB989D7AB4EB7CD91C1448524B0734E5CB57B07D06C8A9F8350EE2D961A461E
SHA-512:	3EDAFCAEB7A7E61C32DDCF2867C31399D9F81205D211BEA5908D3D0C7024FBCED4DE9AAEB8B0716BC302D92CEF1967F25855ADC8842F941F9081A5D291DCE EA7
Malicious:	**true**
Preview:	M|h..a.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	330240
Entropy (8bit):	**7.999409395730101**
Encrypted:	**true**
SSDEEP:	
MD5:	0CA9956E5967CBD48189498803097888
SHA1:	6B0E6770D94C66479A57A0741CE2D4A582C544BA
SHA-256:	535452B987718279A4606B726A3DB76C48C74D8D5D4D08D10272511CBC7EB756
SHA-512:	D6FD9F69E0B402E6227131C7663753211DAC622FD3673218C5E1928686E6F1800081F28094EC7E13B9C08936791BEF304B346C578DF8F8B3D9284542AFF40911
Malicious:	false
Preview:	^.H.X8O.....z.....@u].....}.... ...jr.M.6.....v.3P6...._.xh.ku..A.~..!..6N)R'.....u1!....5..F...C..Y.&.A*.pd-..c.A.8`...|.)@...r..`.;...UPM.....B...a.O.y....4..Z....?[..Et..:..`.....k^?tR]..".IY.. ..9..^M..VW.j...i.0-.....B.|.PW....;mG.V...6&.<G..Ri.qo...l.`nW...Q.'.....xJ.....f.. ..Oh/xt.k.1.c..496..[=.lA8.X.JM.a.....G.S"."3).C3.\J..3^..$d...k..m...R....0.@.>N.]...Zt.x KDF~....5...H.y...'#Q...h.cp...I.9'..@..u.0.9..ZY.[k...^..^a.=..1.P..8Y.r.Y..e...V..b!#o.r...kz..a..].~yU.A..hPx..U.U.x...;..xb.o.f..._q..-=.*..8.b.....;..8R|0i.....<....0i...}A..-.:#3..\.....-.../!..#rH..A.2.h.O..)`1..#.\..8.5.k..=,..;|.....Mvk..h.....".e..y.l..Y...@.`.s?..c..p.).a..%.g;0....R.n...K.h.\z9..@p1..O...j3x.;>Z.....sy{.f.x..N.:..l...w.sPR....LN..-J><..'...3.j...".w'... 9P0C.T..T..kK@.P]SmB<.~.....)h....J.U|%..I...:_.3.y.....b..g..`.....Z.....;.QM...A...:.....}...=).1..(.=4.O...}..8.r8....#.I_b*..D..&.....E.kH...B.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.4112044189276585
Encrypted:	false
SSDEEP:	

MD5:	4879007AC97C3DF41896D937852ABBE7
SHA1:	05A8C8638A4C8157216EF4AE24B43D3A4E750F00
SHA-256:	18B03E2D9F5F5E7E26686848D71049AC56D06500A2AB420A3A01CA0ED6C7AD18
SHA-512:	03C80EC22591301B32EB0310A188B1C4C24DC16BF9E2E25B22A95AA6E36E9B7002196B13A522F36D9AC64C38A98D6BA06C3387DBBE7CB3319E45BC43359A6C3
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\cjeugvqj.txt	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	69
Entropy (8bit):	4.818760421130472
Encrypted:	false
SSDEEP:	
MD5:	05F06C28F5D955691BED4FBDC37385D3
SHA1:	0DFAEC0DDEDE341CDF6896BCBF8A6F710FA28E9E
SHA-256:	9C8BB284A5642CEF5D7A6B4BAB1606D8E444B5D33961EDA0EB6A6D53E09A35EA
SHA-512:	593B88B8E2E1FD59430DD3D6DB7890DD08939B04D69E88BD59C31C4A62CF0A339DAB3E555BED257EF331C4445A75FF71A7A8BE61064C2EF9E184866BFE60654
Malicious:	false
Preview:	[S3tt!ng]..stpths=C:..Key=Chrome..Dir3ctory=knmo..ExE_c=boaliim.dat..

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	215
Entropy (8bit):	4.911407397013505
Encrypted:	false
SSDEEP:	
MD5:	623152A30E4F18810EB8E046163DB399
SHA1:	5D640A976A0544E2DDA22E9DF362F455A05CFF2A
SHA-256:	4CA51BAF6F994B93FE9E1FDA754A4AE74277360C750C04B630DA3DEC33E65FEA
SHA-512:	1AD53476A05769502FF0BCA9E042273237804B63873B0D5E0613936B91766A444FCA600FD68AFB1EF2EA2973242CF1A0FF617522D719F2FA63DF074E118F370B
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....The following installation error occurred:..1: Assembly not found: '0'...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.7997542721005315
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	P05jmXYKpr.exe
File size:	1115860
MD5:	db555a9de355c70681e2e5f9ed38a335
SHA1:	07534d5012526f6bdec5314a4d140de5d94672ea
SHA256:	fb25c8a64c09f9c4e8c586b94d5cda1dc69be203b786ea297f9293d7bd7b8b30
SHA512:	909caea1efe9ce4bfe357a2f987774c83f4b3be060b4d4b8337dd7f3ff939e615eccbb95a3e9e6ce4bd80f4172c39258c196cef42875a4dd32b9fbb315e4b9a2
SSDEEP:	24576:QTbBv5rUvUaHOI/dnZ5Tm0mGbQKomFGa6mFWqSRA4Q1Kpg6:CBUw85QX7A4Q1Wg6
TLSH:	AF351202BED184B2C5621D326A76BB21A93DBD301F758DCF63D00A2DEE715C1D635BA2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<>.....1>.....>.....$>...I..>>...I../>...I..+>...I...>..5F..7>..5F..;>..<>..)?...I...>...I..=>...I..=>...I..=>.

File Icon

Icon Hash:	163e3a121624633e

Static PE Info

General

Entrypoint:	0x41f530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6220BF8D [Thu Mar 3 13:15:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	12e12319f1029ec4f8fcbed7e82df162

Entrypoint Preview

Instruction
call 00007F193CFC0B7Bh
jmp 00007F193CFC048Dh
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F193CFB32D7h
mov dword ptr [esi], 004356D0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004356D8h
mov dword ptr [ecx], 004356D0h
ret
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 004356B8h
push eax
call 00007F193CFC391Fh
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F193CFC061Ch
push 0000000Ch
push esi
call 00007F193CFBFBD9h
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F193CFB3252h
push 0043BEF0h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F193CFC33D9h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F193CFC0598h
push 0043C0F4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F193CFC33BCh
int3
jmp 00007F193CFC4E57h
int3
int3
int3
int3
push 00422900h
push dword ptr fs:[00000000h]

Rich Headers	
Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3d070	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d0a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x19fe4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7e000	0x233c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3b11c	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x355f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c5ec	0x120	.rdata
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
.text	0x1000	0x31bdc	0x31c00	False	0.5909380888819096	data	6.712962136932442	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xaec0	0xb000	False	0.4579190340909091	data	5.261605615899847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x24720	0x1000	False	0.451416015625	data	4.387459135575936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x63000	0x190	0x200	False	0.4453125	data	3.3327310103022305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x64000	0x19fe4	0x1a000	False	0.8160494290865384	data	7.348244743499026	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	0x233c	0x2400	False	0.7749565972222222	data	6.623012966548067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x646d4	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6521c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x667c8	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152		
RT_ICON	0x66e30	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512		
RT_ICON	0x67118	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128		
RT_ICON	0x67240	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors		
RT_ICON	0x680e8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x68990	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors		
RT_ICON	0x68ef8	0xf268	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x78160	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x7a708	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7b7b0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_DIALOG	0x7bc18	0x286	data	English	United States
RT_DIALOG	0x7bea0	0x13a	data	English	United States
RT_DIALOG	0x7bfdc	0xec	data	English	United States
RT_DIALOG	0x7c0c8	0x12e	data	English	United States
RT_DIALOG	0x7c1f8	0x338	data	English	United States
RT_DIALOG	0x7c530	0x252	data	English	United States
RT_STRING	0x7c784	0x1e2	data	English	United States
RT_STRING	0x7c968	0x1cc	data	English	United States
RT_STRING	0x7cb34	0x1b8	data	English	United States
RT_STRING	0x7ccec	0x146	data	English	United States
RT_STRING	0x7ce34	0x46c	data	English	United States
RT_STRING	0x7d2a0	0x166	data	English	United States
RT_STRING	0x7d408	0x152	data	English	United States
RT_STRING	0x7d55c	0x10a	data	English	United States
RT_STRING	0x7d668	0xbc	data	English	United States
RT_STRING	0x7d724	0xd6	data	English	United States
RT_GROUP_ICON	0x7d7fc	0x92	data		
RT_MANIFEST	0x7d890	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3212.193.30.23049703617152025019 05/30/23-06:22:55.049348	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	61715	192.168.2.3	212.193.30.230
192.168.2.3212.193.30.23049705617152816766 05/30/23-06:23:09.678894	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	61715	192.168.2.3	212.193.30.230
192.168.2.3212.193.30.23049704617152025019 05/30/23-06:23:00.991147	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	61715	192.168.2.3	212.193.30.230
192.168.2.3212.193.30.23049704617152816766 05/30/23-06:23:02.678231	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	61715	192.168.2.3	212.193.30.230
192.168.2.3192.169.69.264970061715202501 9 05/30/23-06:22:37.625556	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	61715	192.168.2.3	192.169.69.26
192.168.2.3212.193.30.23049703617152816766 05/30/23-06:22:55.907026	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	61715	192.168.2.3	212.193.30.230
192.168.2.3212.193.30.23049705617152025019 05/30/23-06:23:08.061417	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	61715	192.168.2.3	212.193.30.230
192.168.2.3192.169.69.264970161715202501 9 05/30/23-06:22:43.112445	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	61715	192.168.2.3	192.169.69.26
212.193.30.230192.168.2.361715497032841753 05/30/23-06:22:55.906759	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	61715	49703	212.193.30.230	192.168.2.3
192.168.2.3192.169.69.264969961715202501 9 05/30/23-06:22:32.082582	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	61715	192.168.2.3	192.169.69.26
192.168.2.3212.193.30.23049702617152025019 05/30/23-06:22:47.971581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	61715	192.168.2.3	212.193.30.230
192.168.2.3212.193.30.23049702617152816766 05/30/23-06:22:50.317410	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	61715	192.168.2.3	212.193.30.230

Network Port Distribution

Total Packets: 50

- 53 (DNS)
- 61715 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:31.131561041 CEST	49699	61715	192.168.2.3	192.169.69.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:31.605544090 CEST	61715	49699	192.169.69.26	192.168.2.3
May 30, 2023 06:22:31.606998920 CEST	49699	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:32.082581997 CEST	49699	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:32.593255997 CEST	61715	49699	192.169.69.26	192.168.2.3
May 30, 2023 06:22:37.036273956 CEST	49700	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:37.593662977 CEST	61715	49700	192.169.69.26	192.168.2.3
May 30, 2023 06:22:37.593805075 CEST	49700	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:37.625555992 CEST	49700	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:38.099855900 CEST	61715	49700	192.169.69.26	192.168.2.3
May 30, 2023 06:22:42.733571053 CEST	49701	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:43.111396074 CEST	61715	49701	192.169.69.26	192.168.2.3
May 30, 2023 06:22:43.112071037 CEST	49701	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:43.112445116 CEST	49701	61715	192.168.2.3	192.169.69.26
May 30, 2023 06:22:43.604094982 CEST	61715	49701	192.169.69.26	192.168.2.3
May 30, 2023 06:22:47.673362017 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:47.970376015 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:47.970663071 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:47.971580982 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.247226954 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.259541035 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.490556955 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.515604973 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.886370897 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.886584044 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.886869907 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.886950016 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.887016058 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.887078047 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.892366886 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.892452955 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.893244982 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.893294096 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.893306017 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.893353939 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.894494057 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.894558907 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.894566059 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.894632101 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.895184040 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.895242929 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.895243883 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.895298958 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:48.924403906 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:48.924628019 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.100361109 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.100428104 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.100476980 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.100496054 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.101037979 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.101102114 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.102283001 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.102328062 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.102385044 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.103725910 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.103775024 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.103837013 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.103981972 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.104088068 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.104147911 CEST	49702	61715	192.168.2.3	212.193.30.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:49.105066061 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.105113029 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.105159044 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.105200052 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.105202913 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.105254889 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.106223106 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.107091904 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.107141018 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.107165098 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.131263971 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.131875992 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.133136988 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.155262947 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.155368090 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.294261932 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.294420004 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.294507980 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.294727087 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.296103954 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.296150923 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.296163082 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.296705961 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.296766996 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.297456026 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.297605991 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.297669888 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.298506021 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.298548937 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.298615932 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.299462080 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.300280094 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.300343037 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.300405979 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.301075935 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.301135063 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.301282883 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.302018881 CEST	61715	49702	212.193.30.230	192.168.2.3
May 30, 2023 06:22:49.302081108 CEST	49702	61715	192.168.2.3	212.193.30.230
May 30, 2023 06:22:49.303183079 CEST	61715	49702	212.193.30.230	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:30.992628098 CEST	52387	53	192.168.2.3	8.8.8.8
May 30, 2023 06:22:31.116616964 CEST	53	52387	8.8.8.8	192.168.2.3
May 30, 2023 06:22:36.918315887 CEST	56924	53	192.168.2.3	8.8.8.8
May 30, 2023 06:22:37.032358885 CEST	53	56924	8.8.8.8	192.168.2.3
May 30, 2023 06:22:42.609644890 CEST	60625	53	192.168.2.3	8.8.8.8
May 30, 2023 06:22:42.731828928 CEST	53	60625	8.8.8.8	192.168.2.3
May 30, 2023 06:22:47.643842936 CEST	49302	53	192.168.2.3	8.8.8.8
May 30, 2023 06:22:47.670588017 CEST	53	49302	8.8.8.8	192.168.2.3
May 30, 2023 06:22:54.712057114 CEST	53975	53	192.168.2.3	8.8.8.8
May 30, 2023 06:22:54.741142988 CEST	53	53975	8.8.8.8	192.168.2.3
May 30, 2023 06:23:00.715585947 CEST	51139	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:00.748215914 CEST	53	51139	8.8.8.8	192.168.2.3
May 30, 2023 06:23:07.733160973 CEST	52955	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:07.753385067 CEST	53	52955	8.8.8.8	192.168.2.3
May 30, 2023 06:23:15.454030991 CEST	60582	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:23:15.482513905 CEST	53	60582	8.8.8.8	192.168.2.3
May 30, 2023 06:23:20.963572979 CEST	57134	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:20.992204905 CEST	53	57134	8.8.8.8	192.168.2.3
May 30, 2023 06:23:27.025173903 CEST	62050	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:27.045439959 CEST	53	62050	8.8.8.8	192.168.2.3
May 30, 2023 06:23:33.817295074 CEST	56042	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:33.852931023 CEST	53	56042	8.8.8.8	192.168.2.3
May 30, 2023 06:23:39.982450008 CEST	59636	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:40.005990028 CEST	53	59636	8.8.8.8	192.168.2.3
May 30, 2023 06:23:46.009864092 CEST	55638	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:46.030122995 CEST	53	55638	8.8.8.8	192.168.2.3
May 30, 2023 06:23:52.003278017 CEST	57704	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:52.038084030 CEST	53	57704	8.8.8.8	192.168.2.3
May 30, 2023 06:23:58.118482113 CEST	65320	53	192.168.2.3	8.8.8.8
May 30, 2023 06:23:58.153744936 CEST	53	65320	8.8.8.8	192.168.2.3
May 30, 2023 06:24:04.627254963 CEST	60767	53	192.168.2.3	8.8.8.8
May 30, 2023 06:24:04.654015064 CEST	53	60767	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 30, 2023 06:22:30.992628098 CEST	192.168.2.3	8.8.8.8	0xaf79	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:36.918315887 CEST	192.168.2.3	8.8.8.8	0x339d	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:42.609644890 CEST	192.168.2.3	8.8.8.8	0xc42f	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:47.643842936 CEST	192.168.2.3	8.8.8.8	0xaf9e	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:54.712057114 CEST	192.168.2.3	8.8.8.8	0x36f3	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:00.715585947 CEST	192.168.2.3	8.8.8.8	0x69a5	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:07.733160973 CEST	192.168.2.3	8.8.8.8	0xf441	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:15.454030991 CEST	192.168.2.3	8.8.8.8	0xf0d0	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:20.963572979 CEST	192.168.2.3	8.8.8.8	0x2736	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:27.025173903 CEST	192.168.2.3	8.8.8.8	0xe04b	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:33.817295074 CEST	192.168.2.3	8.8.8.8	0xbe59	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:39.982450008 CEST	192.168.2.3	8.8.8.8	0xedab	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:46.009864092 CEST	192.168.2.3	8.8.8.8	0x4b6d	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:52.003278017 CEST	192.168.2.3	8.8.8.8	0x76a7	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:58.118482113 CEST	192.168.2.3	8.8.8.8	0x1919	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:04.627254963 CEST	192.168.2.3	8.8.8.8	0x9f7a	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false

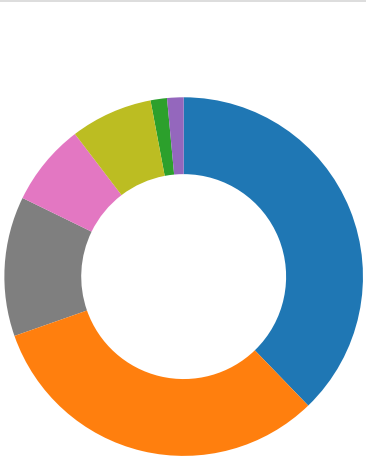
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 30, 2023 06:22:31.116616964 CEST	8.8.8.8	192.168.2.3	0xaf79	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:37.032358885 CEST	8.8.8.8	192.168.2.3	0x339d	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:42.731828928 CEST	8.8.8.8	192.168.2.3	0xc42f	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 30, 2023 06:22:47.670588017 CEST	8.8.8.8	192.168.2.3	0xaf9e	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:54.741142988 CEST	8.8.8.8	192.168.2.3	0x36f3	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:00.748215914 CEST	8.8.8.8	192.168.2.3	0x69a5	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:07.753385067 CEST	8.8.8.8	192.168.2.3	0xf441	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:15.482513905 CEST	8.8.8.8	192.168.2.3	0xf0d0	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:20.992204905 CEST	8.8.8.8	192.168.2.3	0x2736	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:27.045439959 CEST	8.8.8.8	192.168.2.3	0xe04b	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:33.852931023 CEST	8.8.8.8	192.168.2.3	0xbe59	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:40.005990028 CEST	8.8.8.8	192.168.2.3	0xedab	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:46.030122995 CEST	8.8.8.8	192.168.2.3	0x4b6d	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:52.038084030 CEST	8.8.8.8	192.168.2.3	0x76a7	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:58.153744936 CEST	8.8.8.8	192.168.2.3	0x1919	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:04.654015064 CEST	8.8.8.8	192.168.2.3	0x9f7a	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false

Statistics

Behavior



- P05jmXYKpr.exe
- wscript.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- ipconfig.exe
- boaliim.dat
- cmd.exe
- conhost.exe
- ipconfig.exe
- RegSvcs.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- RegSvcs.exe
- conhost.exe
- dhcpmon.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: P05jmXYKpr.exe PID: 7296, Parent PID: 3452

General

Target ID:	0
Start time:	06:22:03
Start date:	30/05/2023
Path:	C:\Users\user\Desktop\P05jmXYKpr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P05jmXYKpr.exe
Imagebase:	0x950000
File size:	1115860 bytes
MD5 hash:	DB555A9DE355C70681E2E5F9ED38A335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: wscript.exe PID: 7360, Parent PID: 7296

General

Target ID:	1
Start time:	06:22:11
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\wscript.exe" Update-ta.l.vbe
Imagebase:	0x350000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7412, Parent PID: 7360

General

Target ID:	2
Start time:	06:22:17
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c ipconfig /release
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7420, Parent PID: 7412

General

Target ID:	3
Start time:	06:22:17
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 7432, Parent PID: 7360

General

Target ID:	4
Start time:	06:22:17
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c boaliim.dat ikvvfncnn.bmp
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7460, Parent PID: 7432

General

Target ID:	5
Start time:	06:22:17
Start date:	30/05/2023

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ipconfig.exe PID: **7480**, Parent PID: **7412**

General

Target ID:	6
Start time:	06:22:17
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /release
Imagebase:	0x1a0000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: boaliim.dat PID: **7512**, Parent PID: **7432**

General

Target ID:	7
Start time:	06:22:17
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\boaliim.dat
Wow64 process (32bit):	true
Commandline:	boaliim.dat ikvvfncnn.bmp
Imagebase:	0x250000
File size:	909912 bytes
MD5 hash:	D70543055E19B63641C7D5CB908EAEC7
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: 00000007.00000003.419593137.000000000192C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419593137.000000000192C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419593137.000000000192C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419593137.000000000192C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419481281.00000000018F9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419481281.00000000018F9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419481281.00000000018F9000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419481281.00000000018F9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419137772.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419137772.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419137772.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419137772.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419113322.000000000192D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419113322.000000000192D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419113322.000000000192D000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419113322.000000000192D000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419304447.0000000001964000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419304447.0000000001964000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419304447.0000000001964000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419304447.0000000001964000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419527075.00000000042A5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419527075.00000000042A5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419527075.00000000042A5000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419527075.00000000042A5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.419176316.0000000001995000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.419176316.0000000001995000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.419176316.0000000001995000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.419176316.0000000001995000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 53%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2BDADF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\RarSFX0\Update.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2959A8	CreateFileW
C:\Users\user\AppData\Local\Temp\RegSvcs.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	2BDA78	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\Update.vbs	0	77	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 2e 52 75 6e 20 22 63 3a 5c 6b 6e 6d 6f 5c 62 6f 61 6c 69 69 6d 2e 64 61 74 20 63 3a 5c 6b 6e 6d 6f 5c 69 6b 76 76 66 6e 63 6e 6e 2e 62 6d 70 22	CreateObject("WScript.Shell").Run "c:\knmo\boaliim.dat c:\knmo\ikvvfncnn.bmp"	success or wait	1	2BD4EC	WriteFile
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0	45152	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 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 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 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.$PELzXZ0dV @ "`	success or wait	1	2BDA78	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	65536	success or wait	1497	2893D3	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	8192	end of file	2	2893D3	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	65536	success or wait	1497	2893D3	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	8192	end of file	2	2893D3	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	65536	success or wait	1	25B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	65536	success or wait	1457	25B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\ikvvfncnn.bmp	unknown	65536	end of file	1	25B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Update.vbs	unknown	65536	end of file	1	25B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\shjgtph.kmt	unknown	65536	success or wait	2	25B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\shjgtph.kmt	unknown	65536	success or wait	14	25B0B2	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	Chrome	unicode	c:\knmo\boaliim.dat c:\knmo\ikvvfncnn.bmp	success or wait	1	2DD017	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	AutoUpdate	unicode	c:\knmo\Update.vbs	success or wait	1	2DD017	RegSetValueExW

Analysis Process: cmd.exe PID: **7620**, Parent PID: **7360**

General

Target ID:	8

Start time:	06:22:20
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c ipconfig /renew
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7628**, Parent PID: **7620**

General

Target ID:	9
Start time:	06:22:20
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ipconfig.exe PID: **7660**, Parent PID: **7620**

General

Target ID:	10
Start time:	06:22:20
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /renew
Imagebase:	0x1a0000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: **7772**, Parent PID: **7512**

General

Target ID:	13
Start time:	06:22:28
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xd20000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651171603.0000000007AB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651409238.0000000007B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651409238.0000000007B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651409238.0000000007B00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651409238.0000000007B00000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651594442.0000000007B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651594442.0000000007B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651594442.0000000007B30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651594442.0000000007B30000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651096129.0000000007A90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651096129.0000000007A90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651096129.0000000007A90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651096129.0000000007A90000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.633014703.0000000001102000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.633014703.0000000001102000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.633014703.0000000001102000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.633014703.0000000001102000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.649689117.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.649689117.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.649689117.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.649689117.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.650948551.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.650948551.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.650948551.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.650948551.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651288244.0000000007AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651288244.0000000007AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651288244.0000000007AE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651288244.0000000007AE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.636564713.000000000383A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.636564713.000000000383A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651206131.0000000007AC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651206131.0000000007AC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651206131.0000000007AC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651206131.0000000007AC0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.648734115.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.648734115.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.648734115.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.648734115.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.636564713.00000000037C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.636564713.00000000037C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000003.511336975.00000000074D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651471493.0000000007B10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651471493.0000000007B10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651471493.0000000007B10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651471493.0000000007B10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651756992.0000000007B60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651756992.0000000007B60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651756992.0000000007B60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651756992.0000000007B60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651236156.0000000007AD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651236156.0000000007AD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651236156.0000000007AD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651236156.0000000007AD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.648908774.0000000005F60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.648908774.0000000005F60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.648908774.0000000005F60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.648908774.0000000005F60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000003.511098071.00000000074D7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.643242754.0000000004829000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.643242754.0000000004829000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.649506775.0000000006D10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.649506775.0000000006D10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.649506775.0000000006D10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.649506775.0000000006D10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.649506775.0000000006D10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.651126783.0000000007AA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.651126783.0000000007AA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000D.00000002.651126783.0000000007AA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.651126783.0000000007AA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.643242754.0000000004AEE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.643242754.0000000004AEE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.643242754.0000000004977000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.643242754.0000000004977000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.643242754.0000000004977000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Antivirus matches:	• Detection: 0%, ReversingLabs

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	7299CF06	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	7299CF06	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	717EBEFF	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	717E1E60	CreateFileW
C:\Program Files (x86)\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	717EBEFF	CreateDirectoryW
C:\Program Files (x86)\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	717EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE45C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE586.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	GetTempFileNameW
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	717EBEFF	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	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	9	717E1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE45C.tmp	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE586.tmp	success or wait	1	717E6A95	DeleteFileW

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	4d 7c 68 fd 10 61 fd 48	M|haH	success or wait	1	717E1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	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 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 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 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE45C.tmp	0	1308	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	45	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Users\user\AppData\Local\Temp\RegSvcs.exe	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE586.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	248	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 5f 66 fd 5a 23 fd 7c fd 11 fd 40 48 6b 47 10 1f fd 31 47 fd fd 4f 2a 56 2e 15 0e eb fd 1f fd fd fd fd 70 7a fd fd fd fd 22 fd 0a 07 fd 72 fd fd 10 77 26 26 7c fd fd 63 fd fd 33 7d 7e fd fd fd 1d fd 7e fd f6 fd 6f 73 fd fd 66 fd 05 fd 12 fd fd fd 34 12 fd 31 fd 67 4a fd 27 fd 64 22 fd 4c fd 0b fd 41 fd 74 fd c7 fd 46 fd 7b fd 2b 14 fd 43 0c 7c 26 fd 77	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLfZ#| @HkGGO*V.p z"rw&&|c3}~~osf41gJ'd"L AtF{C|&w	success or wait	13	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	330240	5e fd 48 fd 58 38 4f 0b 02 fd fd fd 1f 7a fd 11 0f fb 1c 40 75 5d 01 fd fd fd fd 7d fd 1b 00 fd 20 fd fd fd 6a 72 fd 4d 06 36 fd fd fd fd fd 76 fd 33 50 36 fd fd fd fd 5f 38 78 68 fd 6b 75 fd fd 41 fd 7e fd b9 21 12 fd 36 4e 29 52 27 fd 01 fd fd fd 75 31 21 fd fd 5f fd 35 fd fd 46 fd 3c fd 43 14 fd 59 fd 26 fd 41 2a fd 70 64 2d fd fd 63 fd 41 fd 38 60 fd fd 03 7c fd 29 40 fd 10 fd 72 fd fd 60 fd 3b 07 fd fd 55 50 4d fd fd fd fd 02 fd fd 42 fd 86 12 61 fd 4f fd 79 fd fd fd fd 34 fd 14 5a fd 10 52 fd 3f 5b fd 09 45 74 fd 94 3a fd 0e 60 a7 0f fd fd fd 00 6b 5e 3f 74 52 5d fd fd 22 fd 6c 59 fd 11 fd 1c 39 19 fd 5e 4d 12 1e 56 57 fd 6a fd fd fd 69 fd 30 2d fd fd 17 10 fd 42 5f 7c fd 50 57 03 d5 fd fd 3b 6d 47 fd 56 fd	^HX8Oz@u]} jrM6v3P6_xhkuA~!6N) R'u1!5FCY&A*pd-cA8`|)@r`;UPMBaOy4Z? [Et:`k^?tR]"lY9^MVWji0-B|PW;mGV	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 4a 22 fd 43 3b 22 61	9iH}Z4fJ"C;"a	success or wait	1	717E1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7295D72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	4096	success or wait	1	7295D72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	512	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7295D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	717E646A	RegSetValueExW

Analysis Process: schtasks.exe

PID: **7796**, Parent PID: **7772**

General

Target ID:	14
Start time:	06:22:30
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE45C.tmp
Imagebase:	0x150000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE45C.tmp	unknown	2	success or wait	1	15AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE45C.tmp	unknown	1309	success or wait	1	15ABD9	ReadFile

Analysis Process: conhost.exe PID: **7812**, Parent PID: **7796**

General

Target ID:	15
Start time:	06:22:30
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **7852**, Parent PID: **7772**

General

Target ID:	16
Start time:	06:22:30
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpE586.tmp
Imagebase:	0x150000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE586.tmp	unknown	2	success or wait	1	15AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE586.tmp	unknown	1311	success or wait	1	15ABD9	ReadFile

Analysis Process: conhost.exe PID: **7860**, Parent PID: **7852**

General

Target ID:	17
Start time:	06:22:30
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **7924**, Parent PID: **1080**

General

Target ID:	18
Start time:	06:22:31
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xba0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	141	141	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a 31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	186	45	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'.	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile

Analysis Process: conhost.exe PID: **7932**, Parent PID: **7924**

General

Target ID:	19
Start time:	06:22:31
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **7940**, Parent PID: **1080**

General

Target ID:	20
Start time:	06:22:31
Start date:	30/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x140000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	141	141	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a 31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	186	45	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'.	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile

Analysis Process: conhost.exe PID: **7972**, Parent PID: **7940**

General

Target ID:	21
Start time:	06:22:31
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly