ID: 490868
Sample Name: 6LkjS4JhAl.exe
Cookbook: default.jbs
Time: 16:50:27
Date: 26/09/2021
Version: 33.0.0 White Diamond

Table of Contents

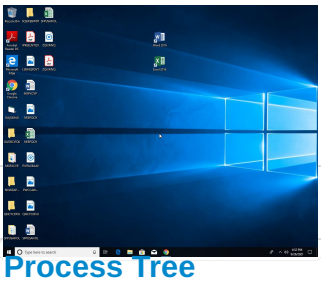
Windows Analysis Report 6LkjS4JhAl.exe

Overview

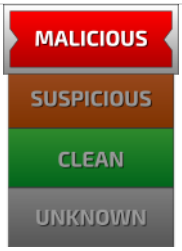
General Information

Sample Name:	6LkjS4JhAl.exe
Analysis ID:	490868
MD5:	4aeb49bf7e23aab.
SHA1:	a9a80ec2e9ea80..
SHA256:	d11342ce9c7550..
Tags:	exe Neshta
Infos:	

Most interesting Screenshot:



Detection



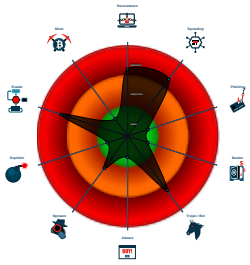
GuLoader Neshta

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

Signatures

- Potential malicious icon found
- Yara detected Neshta
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- GuLoader behavior detected
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Hides threads from debuggers
- Infects executable files (exe, dll, sys…
- Drops PE files with a suspicious file…
- Tries to detect Any.run
- Drops executable to a common third…

Classification



Process Tree

- **System is w10x64**
- 6LkjS4JhAl.exe (PID: 6508 cmdline: 'C:\Users\user\Desktop\6LkjS4JhAl.exe' MD5: 4AEB49BF7E23AAB664DE914DF204664F)
  - 6LkjS4JhAl.exe (PID: 6580 cmdline: 'C:\Users\user~1\AppData\Local\Temp\3582-490\6LkjS4JhAl.exe' MD5: C666C22685D135C1EFE709CBEDD0EB6B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
6LkjS4JhAl.exe	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] y ours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 1 5 FF 15 34
6LkjS4JhAl.exe	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
Click to see the 221 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.506546365.0000000000409000.00000004.00020000.sdmp	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
Process Memory Space: 6LkjS4JhAl.exe PID: 6508	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6LkjS4JhAl.exe.400000.0.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
0.2.6LkjS4JhAl.exe.400000.0.unpack	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	
0.0.6LkjS4JhAl.exe.400000.0.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0xa0e7:$x1: the best. Fuck off all the rest. • 0xa1a8:$x2: ! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas] • 0xa108:$s1: Neshta • 0xa113:$s2: Made in Belarus. • 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
0.0.6LkjS4JhAl.exe.400000.0.unpack	JoeSecurity_Neshta	Yara detected Neshta	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Spreading:

Yara detected Neshta

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

System Summary:

Potential malicious icon found

Persistence and Installation Behavior:

Yara detected Neshta

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

Drops PE files with a suspicious file extension

Drops executable to a common third party application directory

Boot Survival:

Yara detected Neshta

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

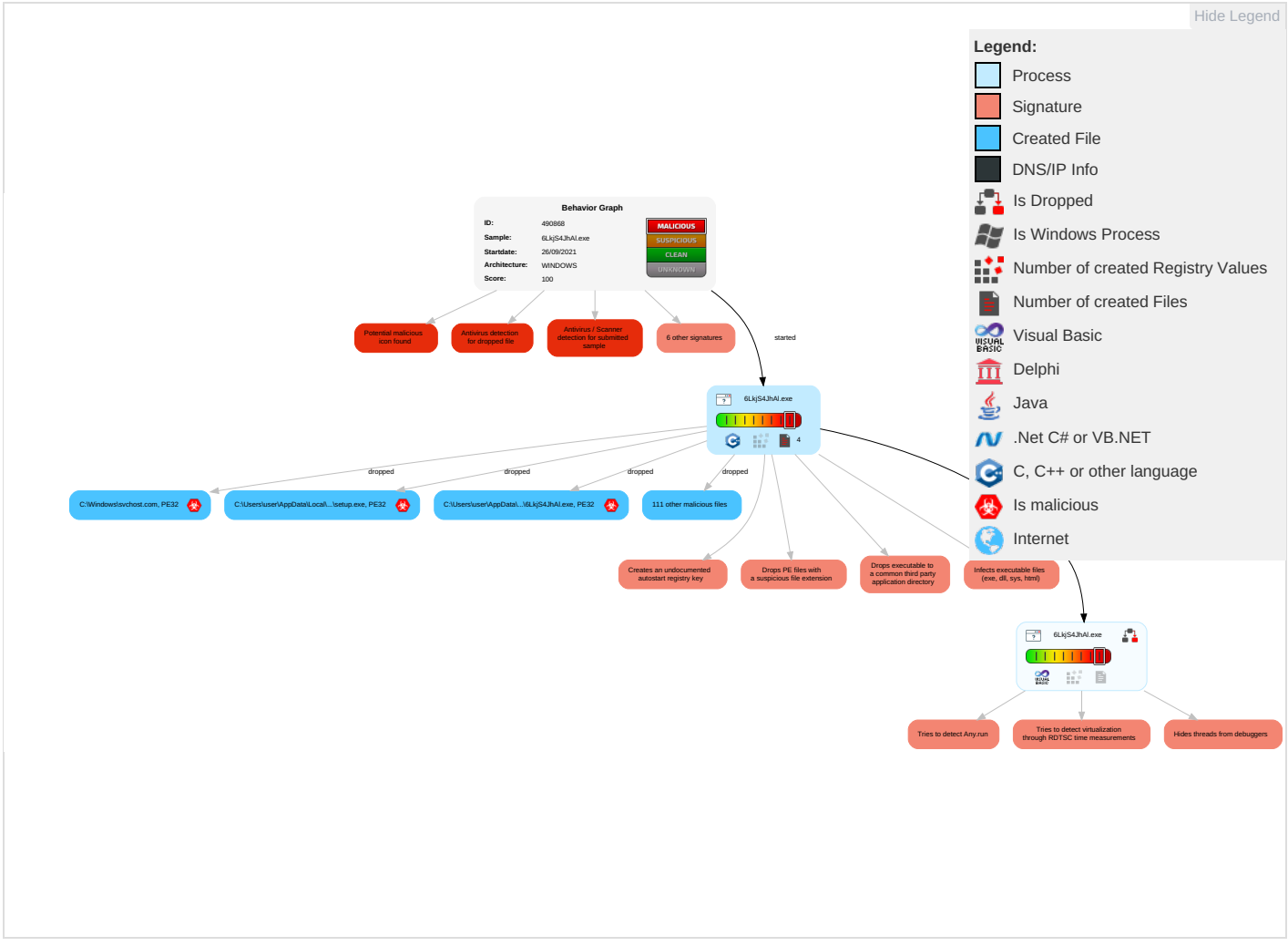
Yara detected Neshta

GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 2 2	Input Capture 1 1	System Time Discovery 1	Taint Shared Content 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service

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
6LkjS4JhAI.exe	85%	Virustotal		Browse
6LkjS4JhAI.exe	100%	Avira	W32/Neshta.A	
6LkjS4JhAI.exe	100%	Joe Sandbox ML		

Dropped Files

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

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	96%	ReversingLabs	Win32.Virus.Neshta	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	96%	ReversingLabs	Win32.Virus.Neshta	
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	96%	ReversingLabs	Win32.Virus.Neshta	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.6LkjS4JhAl.exe.400000.0.unpack	100%	Avira	W32/Neshta.A		Download File
0.0.6LkjS4JhAl.exe.400000.0.unpack	100%	Avira	W32/Neshta.A		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490868
Start date:	26.09.2021
Start time:	16:50:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6LkjS4JhAl.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, 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
Detection:	MAL
Classification:	mal100.rans.spre.troj.evad.winEXE@3/114@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 49.6% (good quality ratio 47.9%) • Quality average: 82.8% • Quality standard deviation: 26.5%

HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	09876523456789.exe	Get hash	malicious	Browse	
	Y4pMlX1fO2.exe	Get hash	malicious	Browse	
	B513104971C9E0C5B6721A523C9475701A67BB368A74F.exe	Get hash	malicious	Browse	
	1J5sT000kJ.exe	Get hash	malicious	Browse	
	ij99opH1kI.exe	Get hash	malicious	Browse	
	McAfeeStingerPortable.exe	Get hash	malicious	Browse	
	javaw.exe	Get hash	malicious	Browse	
	javaw.exe	Get hash	malicious	Browse	
	Lw6h2Z5Lg5.exe	Get hash	malicious	Browse	
	Shipping documentsProforma invoice.exe	Get hash	malicious	Browse	
	je60o4s3gS.exe	Get hash	malicious	Browse	
	8doUcc9Dn2.exe	Get hash	malicious	Browse	
	y9pE5n5u9D.exe	Get hash	malicious	Browse	
	wVdurpHHFa.exe	Get hash	malicious	Browse	
	smHWkWDwfX.exe	Get hash	malicious	Browse	
	dVUslZmrvk.exe	Get hash	malicious	Browse	
	wIAWmUGebs.exe	Get hash	malicious	Browse	
	lAFVkA8CLk.dll	Get hash	malicious	Browse	
	PgIBHusOv7.exe	Get hash	malicious	Browse	
	IepvPME9Y3.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.278258254187173
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCctJ77qzWk6AM2oS/xePB:sr85CctdeKzC/y
MD5:	E47F8A2ECDC2D4BFBBB6328B1391F1CC
SHA1:	A633C3106A89C083014FC9F29D559B70E93D6D69
SHA-256:	8FCB4C541BDDA7D5CDA8124B48BECBAFBAFE2D82116BD6356D16FF894E1D83AD
SHA-512:	6A9088AA04F3BC6F57AAFDAC45B3C52A0668431CA373BA6E8C034717FEE10BE90B2E7F806178A26151D040B3087F708A08219AAC3B2F4553AA5D84E36BE86EC6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: 09876523456789.exe, Detection: malicious, Browse • Filename: Y4pMlX1fO2.exe, Detection: malicious, Browse • Filename: B513104971C9E0C5B6721A523C9475701A67BB368A74F.exe, Detection: malicious, Browse • Filename: 1J5sT000kJ.exe, Detection: malicious, Browse • Filename: ij99opH1kI.exe, Detection: malicious, Browse • Filename: McAfeeStingerPortable.exe, Detection: malicious, Browse • Filename: javaw.exe, Detection: malicious, Browse • Filename: javaw.exe, Detection: malicious, Browse • Filename: Lw6h2Z5Lg5.exe, Detection: malicious, Browse • Filename: Shipping documentsProforma invoice.exe, Detection: malicious, Browse • Filename: je60o4s3gS.exe, Detection: malicious, Browse • Filename: 8doUcc9Dn2.exe, Detection: malicious, Browse • Filename: y9pE5n5u9D.exe, Detection: malicious, Browse • Filename: wVdurpHHFa.exe, Detection: malicious, Browse • Filename: smHWkWDwfX.exe, Detection: malicious, Browse • Filename: dVUsIZmrvk.exe, Detection: malicious, Browse • Filename: wIAWmUGebs.exe, Detection: malicious, Browse • Filename: lAFVkA8CLk.dll, Detection: malicious, Browse • Filename: PgIBHusOv7.exe, Detection: malicious, Browse • Filename: IepvPME9Y3.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.3372362912074625
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCpbQILFkbeumIkA39xSZW175V7UZQx:sr85Cp8LRkgUA1nQZs
MD5:	10075707D5C79CDACFE09DEF9C6D4985
SHA1:	7D1DD5FB7DBBCC8563911BDB3C40B244FD03C634
SHA-256:	3D49D6B3360EB03FDD43A4C926213F8B348ABEDE3A5D8B7A4530BF8ED4AE1B72
SHA-512:	C31030085A5D2C15DCE1B9B5EA1727CF36CC4F3AC71A5F5715086342669D9E3E2D0BA213ECC00D9A18D792122332BB6DF2EE05B146CA83AF279E3C4CE80B82D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	moderate, very likely benign file

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

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

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.220006974675465
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCbO/DiMgT0O8ahUMJD/dt7:sr85CSPm8aVJD37
MD5:	F447C4B446D5889225A9D9082145AD88
SHA1:	A1A380F3D3402F243E1A213C39E969D2C24CA99E
SHA-256:	C34D1F919C306D2F2959C932CAC15FBED433AD465F71C50270DA27803952B829
SHA-512:	E62F7E4F3E7EDE368CA0ECB242BF9AD12124AE92A61AF9BD97CA47E1457B842D84BC16105EE84EC201B948C31E613046F92DA4635EF2061638BD40EC797435A B
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.356945716242827
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC8xXHWVxZs58xP3RFA+8j/Em8kjkO:sr85CHVxZo8xP3RFA+m/Em8St
MD5:	DE64003856A8B74AEAF33E247AF9424B
SHA1:	912E6F9C6B1103AAFEC7F30FE3B0F9C3F55D6650
SHA-256:	A39859FB4CB6693CDB686B3501C0178DFF81D27375C0086805F09ABF45284F64
SHA-512:	4D2B92577F21183B5BF72DDA2DA4750099F198AA086FD68DDCCB43C686E1A8949E834E72D8E7FEAC05DA4F080D54C12BC1A7A5E2DEE36DFF3B92A4931BF1FE 8D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.486359083061706

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJw0L11g2ncA7932EDoh3hG2xS79o5kUt:JxqjQ+P04wsmJCt2ce3ExA89/I+b
MD5:	D972E8BC4F221D69D9DF89999B74C311
SHA1:	3A43D069389EFDBA178DCF16EBF4A45A8B09F0F9
SHA-256:	8E0F471BC8BAEBB5FBC3C65A9C6C75B3F23B4E94AC4C07054DAD643CEBDCA103
SHA-512:	DDA8C29088E907E0B429E560CC21FD2B5C7EF0736456A30BAA3FF08AC85C73487471E6164CE8872AFA7E7B8604AE6A5882A748140B4ADBA142EBB0CC6560E7E6
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.5232250585402545
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCdkLMxpXEZnDJussJ/ngE:sr85Cos4uBJYE
MD5:	F648557D5287EC8C3677DC5B57E1C6AC
SHA1:	B04F7B7273C97B1E56FD2B0BE2998D93A7327E75
SHA-256:	647C4669A29D3D650AE1B750B2DDCFA312FA4AA64552C1D53867B6DDA6A72C73
SHA-512:	033E2C729A89F75AD4B198A4FC7431C8763F386B5993265F2A16B0B4591CEAB88803CAF4D5952A27F074651988F1FCB09B12EA6CEC2932CD429015DE0ED0B95
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.186107093668235
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCFhUpMPub5+G92qoooZVq/LF:sr85CTqSwgHVqDF
MD5:	67059EAECEA081CE3E6426BCE980BFF0
SHA1:	C1EDD7FD96E1C367A0403DD7A8DDA32AA3E13601
SHA-256:	BC0FBF0B4739B4ED148D96B64308CD8815EAD686DE4400BBBA49E5B90BD7D21D
SHA-512:	5E3BF07788443B558FBDBA88B41AAAA548D20697FBECF8B31F2CF1D4AC965A858100160ADAC30B7662EE2CBBFF17B3CEFA7A100623DB13C66C8735C5D70DE84E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.667436230875162
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCi3rlNE0YMqYCka4KltvntyHi:sr85Ci7LE0YEKlhtl
MD5:	E13741E87379B8A0130CCB0F24B56D1E
SHA1:	C1DF66670A0370F44E9F7BE15FCB60C580992D1F
SHA-256:	CEDC7E901AA1E9FF96BA749A3239542AD29F62B1C08EA392B721CD28D0D298C8
SHA-512:	F299C2732A09B5C7870CB9AAF5CAFDFD3DC41A0B81C6102B53962A1E3EA4A2BBC12C20FB788849612B6FEEA2B9571A2BA28A748FAE32BA58281A3C320317710
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.461209967778202
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCl8H777b4o4yre0zlbTzqYOeg9lZdKMOZo2:sr85Cl8Hn7b4o4kbT93Kxj2
MD5:	72EC370FCAB5AC9E14C7DE1B93C0B954
SHA1:	B2216AE2B03F902878D852F9D52FFA704C76F61F
SHA-256:	DB205349D14EA35D6081598FBDE492AB12BEF4A39555EB9B4F4020C5B492E039
SHA-512:	6046A04E192C329D56FBC11118269DEEA06053D6C0C41FF5E6225938476B54969A03345D3B46F84B54D7B5262230584218466651E7B4ADDAA0E642AF3CF4F6F2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.302303877870808
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCeJ8cSLgpA3hKwYPRvGdIab:sr85CncSLgpG88b
MD5:	B41F70A22F31E1DA8FF057AD47499F3E
SHA1:	15918D00F2C8DE480C4D3749D5317468C1B14DA0
SHA-256:	8860EEA648A0CD39281639D27B1B9C981568ACEE9C3DBABDC5D862534F70946E

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

SHA-512:	5F0C77A4842BA7FC53CECA4F641FA906EA0D26652876406B52158DC6BC3D36ADCC3A63E6FDA5B226073320ED301A21A6AFC87B930ED4D5B91058172727AB47A4
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.261294291615621
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCmwGqE9qLa7QoIG5fIIXBB8C:sr85CaqcVz5fzsC
MD5:	F25F4BF1D71532CE97C90BEEC7A56FBC
SHA1:	337C45D81469B760EB7ADA0316AFC262FE4C3721
SHA-256:	B24831A423AFFF5E65032A7673D7BA4E35192C43C365FCDE75D678CAF4605F33
SHA-512:	5AEDA5CCD0F38392FEF3F14AD49EAC63D03ECBFDDC89D326DFE0ED03A225A1E7496B02D5F983168D1D7C96448F90718B6975A8D58EAAA6DF9626C27D4AF96AC
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.423139673646388
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCULKBHLLkRkjuXi65D5mFv1:sr85CU0LFjAiGI
MD5:	C4CA362C5EF952BAF96EF61B59D8355D
SHA1:	5DEB0DAE7262FF31BD9B2C2205D55D2E5D012CEF
SHA-256:	A679F4131244485FD10E274A510C2B76DF545838B8562E579C9805269834355E
SHA-512:	49261B804AB74A90DCE657FD7C4FE87F42505F673847C143C42A4CF89E2BF3226C329630ECCBF19FB584071FC4E7DAFFA7725F66A7E7936DC8CDF4A3E73425E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	
Size (bytes):	82944
Entropy (8bit):	6.355719905315724
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCdjrXDyO4zkm8dbHVLokF8iJTwRH0n:sr85CVrMzkm8PL3Eo
MD5:	A42467B5C21814776277B4CE3456D716
SHA1:	B01DD2412ADA123EF3D6317F839826D37C6A27D4
SHA-256:	B1A5063A32CB8AFD591C57AAB1A679137EE29A886AF77849A13C26537A100AD9
SHA-512:	62D2AECABE4892E0E25A9787A28898EC989A4AA54A66CDB7DE65EB48A8634E0274EB6515722EA1FA580C848E1AD683C75CE26F6AB7D7F7E48A5DD064DD1B3A24
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.228109838185618
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC3uireklhKsikOkCWfNU:sr85C+ilU9xL
MD5:	B9A06C8C07B4BC86001ABCA5835AEED2
SHA1:	5EA2F32AD6F1642498CDE9F8CA74D8A70DE376E0
SHA-256:	1531CA6AD23335F3F93231D153CB9DDEE40580A5A82D502AD6F7B54C8328D8B4
SHA-512:	79C9F72832E53AED9E50C680F0146E6F971D77299E192DD61500E8B91117E19373C7EC92B84A31B2934FD65CD6090E9613BC6F62A2337A1313E7E52A1041B04E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.26326337462311
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCFbIJyoI91593nKMd/VHT:sr85CFboI9133K+HT
MD5:	7C2E8C0527C5CFF276FB2FFA314D455A
SHA1:	6B6FD014B9C295838E0F1F2D563C185A0004C028
SHA-256:	41AEBB2A2B6175595684D20DF5F7B8AB8FEB2B5662530F6593287F9F72777296
SHA-512:	2138731F6006CB6DF13821E05DC16EDEBF7F70777906AB03271707A1237DBFD8859ED43795F36A87901D63BDAA4CC738E46B9D2D0D6361546FD64A2AE56EB65
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

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

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

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.079745714518026
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJCBF45im0N0l9U96lOQ7ABFPXdLtZqWn:JxqjQ+P04wsmJCJ4wNlu9HQIXsW/44
MD5:	E6A82ED5EA7010F781B63E30C2377BEE
SHA1:	1829EE1E5E5B34C9721F4EB51E3AD09F7A13DCE2
SHA-256:	E02365CA739F356FE66B4F49C4D11EC156B0BB512211A177A813FC7D8B0C2DFD
SHA-512:	2FD5BAF35A018DFF7FCA19A4C118E781FC9D03F9DDED1CEE8F2A5E9E6E41F1C99D984F24E5AB3E60AC2FFBD1B505F728410203D11234197D109BFDEC728ED 0D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.352749197508949
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCZti/kCXBIvpnJXCFgyf:sr85CzgkC+Jt6gA
MD5:	E784AF0ED9D53B2A29B2EBBDDE7E470B
SHA1:	203533AB59D90155BE6EC83B9E7FD643869FBA9D
SHA-256:	D8B35FBB5A6A4E3069FF8E60BB9F35670DEEB5B5933820CCC4FC9D9D4148EB78
SHA-512:	A2C77DD2CB33815273C4730892FB45F2EB086853CE7544890FA970F666249FCA61AEDFB826109293066C2F615B95CAE48E9C28F96B0C59D6EA0423B337BDF291
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.395396839059979
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCBBTfrVijfDZaoXFdP+aWYEsPnBEbfOjBvX5zjjSbE51E6AoAV9:sr85CnfrV5EAVMczsELz7Vz
MD5:	B4E63C549366CFCDA2363E35C197D41C
SHA1:	10E1078FF8D1FD5FF2080FCB659A012630FD07E8
SHA-256:	68BE6B2F5E8181E4E36DB6F370E3110C43D702E6953735FE6843D230FA6E7A37

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

SHA-512:	FB0B06847F459BA7D439D20608C3A098AA01B18FEBBF3D014536A3CF21353EC0524922056BF151B3A0F66E00E758C36CDC49B44A59C81F78B6249E93B535C893
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Check.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.509452568334581
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCXl/TR5SDQQfzSlOOc1c:sr85CXFR5StHe+
MD5:	A7D23C329BAABBA8B883C9B0EACCE4A5
SHA1:	0E2B51FF3DA7806D0F5DCB403222D06637B08738
SHA-256:	C2521122926A26FFDB7E9D56EE6E24682F1C76B573BEE8765E9E287CB1DCAE89
SHA-512:	22116FE8362AA86EDBD268EF90A415B4E204416C39AB0312EFFA6E3C2C7C6AB85B000A642443DA071F61E3C370398D6C018E8F4582E9E854BAF2B3BCAB7E5D3 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.476428579556002
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCzbdrFQAj9UlJZ4PAZav4RLRLK:sr85CfQO9UKRGRLK
MD5:	02879251FEBD3B13DFA84C0DBB3B9387
SHA1:	D2226312A4460980B036C0CFD3B7BF95752145D9
SHA-256:	28C72711975DEA1917D0B4C996D93E945F0487DFBDEB1A0B298E9A724F6E8937
SHA-512:	864BF0149EBBF033306C7B0FBD168D696DFFFEE012B61991C5F0B4D35F82ECE7FE276EBEDE901BF30E22529D8EDEDF3EE3FF64F9D18A411624DB3188ABA45E 4E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.520333669037674
Encrypted:	false

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	
SSDEEP:	1536:JxqjQ+P04wsmJC32EQwB3BsLsWIGihj58u9otwqtOk:sr85C325wztj5xiv
MD5:	32C22D658E9A54E56C54B1A2AFE1D817
SHA1:	E1DA8AA26A509BC23A761EB25267DCE9F8A7EF92
SHA-256:	C957D33A54BD308948E37F020C3FD23DCBE4762DF1143EFAE8109433342DE76C
SHA-512:	C669F6999EA0ABC48D7AEFB32CD067F37B2894C8EDB1EC538063ED47B719A4597C5BFB770C821DE0D0384FE3B4AC212368B629284D8740E8855D7281A84590C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.481287941039048
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCrwiuLWf6G/YemcUCYY8AZqQwOp9yQeRoL3:sr85C0iuVAYemcUCN8AwhOpCoL
MD5:	9C8E99E8AD1568B91CBC2A9FE09304A8
SHA1:	DCD08E9FE8ACFEF7F194CF0E6759F5468FA028EC
SHA-256:	A33D6E9432C5D3E83EE5CFEC260EB5C1396982EFC713DA6C5B31F67712272B41
SHA-512:	68270258389E3EC950F6E1535D2EA7271611A57268B7897E4C76237122DF2B7E15884F4F110C11DFB711BDF42F80F682BC0D81D62E16C954EB7AE0EC43DEF349
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	7.2906774035349695
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCloZCsdndoviDl47IcIyh3e01pxDQOF:sr85C+Z1noWILcIys01vQOF
MD5:	9B9601BFE0B0E353A4AB8B3FA54F7540
SHA1:	BFCC868475761DB126FBCE6D36A8F3696C00FD3F
SHA-256:	289C2D7F33C2ACB203D47A677ABEBC41A6D4D580BFBB3E80A4AD65D35DC65AB8
SHA-512:	AC65B689940E9CA2A02CFE07F7D53C024B3E612621CCA202DAAE1E37709D66C713C7865C336DBCF8248FC42A55776B3327F9B2AA71C7FAED2F547AFFC4DC15EE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	
Size (bytes):	82944
Entropy (8bit):	6.586052312714495
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJZe5EaY1O/TqX0YpwD3nwBoX0M12Pnhq:JxqjQ+P04wsmJC5QOgVKnwBvPlnJml5
MD5:	934C8B78754C1FB79DF08EF114600899
SHA1:	5A50BBC6139CF24D3785A1AC5BC1303087ACCFE6
SHA-256:	12A68206D1263D798EB284C9A6EF654E4ACFAD20310AFAADB092B54A20358A3A
SHA-512:	DFF08DAADC807CF170FDC13D4C2EC20D0567B6B4F91D1853F737A6B57ECBBD332EC98D237EF4705E77693361AC3027D0298F194BD10472A2AFF9338616B8C4D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.529393382316189
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC34bCTNhZYt+zphjirUcYkzzaOvo:sr85C3MCR74+/+YcW6o
MD5:	B6BA74867ECBA5541827551FEEC46F7A
SHA1:	62AFF9292E306BC442F46D8835CDBA2F777A0BF1
SHA-256:	8D6A0F83B4FB84B8670BB9C103071B4D40CA433876242B476DB83BDB683FC446
SHA-512:	850385B0D7ECF20BEC4406D0EFB1AB0A01D9B42E2011FAFC94A8DDB49932FC3B2EB0F6D486903B84D72518928567E96BAE638891F578B9C7CD32C0CEFAC0524
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.7205787223638
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCA75/gWXq7+8aTaI/dBKvFBvqNm48fnRV2B:sr85CA0a8aTaI/dMrvkL8fnR6
MD5:	29BAF7AE561A3CCC4EF6A6988D57324D
SHA1:	B2D3512E166A5F9E10FAA4E461F6EB5A6B926531
SHA-256:	0B607DF09D9876EC9A80D77B9F2E20267B611A75DA95962FD2DACFF286E00F9F
SHA-512:	A8CF29B616CF505F8A52E0775F0B3859F29A56181F3E1D5B16B86B40FD4E5BA0ECC5DD81098AC1024A32A1CA4575CD9B7F9F6FB2D22C75F808FE32A12406501
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\AutoIt3\Uninstall.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.52588514314363
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCWCrRRPYqa5pic6jXFdL2KiMceCry:sr85CWCrbPA6jXFN2MceCry
MD5:	DF57A3FC85CD6B6CFB31C52714E2D79E
SHA1:	D4DA4DA44C58BB9B818CAF22C7A578FF1EDECF26
SHA-256:	E660F04725795D12A67A796BA9A96889216C2CAE4A6ADA2459F7948428136BC1
SHA-512:	14FBDFFF9E7689A2800A150FB3EB7F50E12A25DEBBC7CF18ADADCDAE925A72DE8E942F5A1AC0023D419C965E2DF9684217D13A95A1AD6C1FF2B61D1B2B814F70
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\AutoIt3\Uninstall.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.5042461329985075
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCmGhFAlQY7rMdInNwUdROnIDh+vE6YjhmnCu26W:sr85CAlQGrkInNwUPOnWh+vEzEnCh7
MD5:	A5EA90AC4FC049DF79D7DB1814B9B326
SHA1:	1AE4394BAB6F0CEB3F1EE611B460C0FD632E87C5
SHA-256:	61B25B74A7126A96A87A8D313B850CEAD18B5AB5389E9FF2B2C9A164927A08D2
SHA-512:	DC6FBDEB7D79AEDB4479A4D8742D15AAA4BEEE97892715406D58E0C5E1511073C85D91B287E7CA75DE376C0C9A6BC2A307115A646600261EDDD6DD287D5AD36
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.384524945408535
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCmG2kHtSSHuzUfuNAGt1Uv1JwsxtD:sr85CBNrOEuNAsWJwsD
MD5:	D0B62E96259230D26E500B5D2F6E2488
SHA1:	86DA8E18DCCD893874C398FDB41EEE85D766A4EC
SHA-256:	1E2BC4A5441F740B2E9838EAB3964123A2D358B62E1F124C5F1E8BB4E5AB2319
SHA-512:	BA4E224F4D5C8A5B5E626A7EEE6F35688528244BD7F9323CF74AF219BFA2AAFBB947DDAFD8ED815F564EDE0403B09CDBB1DEFB0A9CE9753A75C8A1C5E912FAFE
Malicious:	**true**

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.210368811104495
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCed9fP4LXRxQyEvzDmxvuLX+:sr85Ca4dOyEv/mxmLO
MD5:	27D5B0E45DB81F836CF687549F844753
SHA1:	4EE8AF1DE81163B66C20D4D4C652250D3B116544
SHA-256:	365857D447BD640AC5A1BA7F32AF69211AD8F7C3AA0345C925FADCD6635D8C44
SHA-512:	42BC2AAE4F5371F7F6E21CA25A28578929C160C7B0DD629239BF1C1F47C1E59AC5E56E1E33C8C1B074FE5393A88076F214D73729074E72A2AF1F6F83386A573A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.599158686971261
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCKhp8N3YERomt8JCeToWZmKbt1H0jKWo:sr85CKn8N3YEuTofE1H0jKWo
MD5:	294D120414736A7579445CCCA78F505C
SHA1:	4DC265A2FC75AF686DA3EC830BF9C0072AF14581
SHA-256:	AF7E482890D77DAD13F0D5A1377DEFA83CF2D802DC1444A69FD17A464C4A446C
SHA-512:	8DC9F174875DD7012030EC6FE1624AAA99E068DD464BE4AEFDBA9699C39969DF0E52214B90BC46ACE204D2505DDD69C46D674DE39A6BFAA3DE213DFCA66ED 196
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.6085003171859364
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKN/MZzagYK5o2IQJ/rVSgvV:sr85C/qA/WadUDFBZz9
MD5:	89DC2A4E5290AE1297C2281B5CD35068
SHA1:	1D091812669D1D0CF0293B9D495599BF257434D9
SHA-256:	5116F46AD2BE5B402FAD8B89350F671576D995ECCF91863D827984AE42319596
SHA-512:	2CECAFADFE911CAEF8F735192F7F1D60305BBBA6A390E13CDB4B5055413D931B75F276086F18AE36E32FEF31DD3B37FDDECD1FDB9F4EC12938B1EFABCD6D7E07
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.62851477500423
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCsrkFN/GjcAShJITZOG8i4e53hS5PobC:sr85Csk0cA6JITt8cXbC
MD5:	61694544EA704A28532F4EC0319AC735
SHA1:	F6ED53FF2792797D40ECA888567873F0570698E6
SHA-256:	4183F6849773F9EED9279D5237C93719511F605276F0EB9BF2E8B2258BBAED09
SHA-512:	5004069D9A41811B63CD84A049757A2F2CB061D1D6999FAE9EC083C4AE3C850BAD9D59112B452118A0AA231A4F07145D03C62FDB699074F4610D4899A662C922
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.653521772684421
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKEs2WzzIR++tGuPkNoAvBFbq6DAcBDjFsb:sr85C/qLWos+tGEkBbq6D3Bdsb
MD5:	50B7F8BD51D8BEA4542C8B6FB7046568
SHA1:	46FE9571A136EEDD3DC35089F096D47B32EA74C8
SHA-256:	86A782FF58F3B5F1736EF23051833E340FD56A77C1EDDDBA8ECC5A507BA47EE0
SHA-512:	87A46E55F78299DA53343B832D84C81C230D46AEFB71C603998DA5F6D0BB3FFE6FDA5F825F5731F7B810E21C1EF8E9812278D07E7402BB3913AF6DD66DD43CE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.656070779362061
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKKKajo+iKndnTdkCE1A6n82c6jbs2:sr85C/qo0o+iwdnP6ngIs2
MD5:	60628C314BCF2A97CCFA9CB4241A2DAB
SHA1:	6EF748A1568A9AE0D541C5CDF0F74430A59E4DE5
SHA-256:	FD8BD222DB055C39D6050A10F91EEE576ADDFC37CE78F585ACC48F96E222FA90
SHA-512:	2AC9ED50008A13A4255ABB338C675D53688D321E6086B6DF17B02A3F89896051F60E8565001CE0B7BCEBD0CD211DED9B9574347BC95A05922700C20806EC93E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.6397427450636055
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKHLgwHz2xi03XxQy012eqZwE:sr85C/qMsc2Y03BQz2eqZP
MD5:	7132D6785E73B1159F3AC9AC5DE71A1C
SHA1:	0EF8C262E63E3776662064D00E5C4264D0213C8B
SHA-256:	629945249C52DDB4108FF5C239D4E2C79C92A545ECD25DAE395697831D648A5F
SHA-512:	804BD2E14C52D226F1D470D0C73B3DE7945EA24EA4554D916FF796E24F6C7C6B5A21284396C6359CBD94ACCE87517D19984F207FEED537AE9DDE8C29D04D2A E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.529062771218018
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCPQ5vyh0tYhgw2azkO8rn85GF:sr85CPQ5vyhvcOQn2GF
MD5:	2FECE9074EC51CAA91DDEA7FBB4FFC54
SHA1:	35BD848191A5C14897883B9A11BECC6DB522A88F
SHA-256:	B4D954F33DDFC952FDD208E3EFFCD6A1E442DE8D07C9148C4771986F781C294F
SHA-512:	F9C3249A39CB4206E495EED2A5C6130CCB04874FBFCB9D0D3D854B6625791E88C2BF29A7AE6C5E57B2B5C4EF25F39AA7BAA4B8C989A3A62D9FCFAF9116417A EB
Malicious:	**true**

C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.4112170834310565
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCUN8aliPc8ZbyHVftptXvVWi6N8rKca:sr85CU6i/XtXv7+8rKca
MD5:	BA5A5D15C15E1143A35B5ACB9DA43F23
SHA1:	BE948D6A40AE1221B2E093B6634D695EEDFAD323
SHA-256:	075242C15AEF5CC590E716651ED3F1F53A8BD23A37CFA60F827DBE60B7DA8918
SHA-512:	3E36FA618DF02872C1F5043318A8F945912FC5162F8C9ECE7FDA323F7D8AFD53157C00519E50DA9899DA6BF3117CA82011757B987726F968C3B7B5A632066EDA
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.374994892226591
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCrNsxigdJqueeYUOc1wxNXI:sr85CCnneeVV1
MD5:	BED5A0265D4F2739606BD0C79DB41BDB
SHA1:	0EAE9CA564CC3B83B4B7CAAF64FED47567C8A6D1
SHA-256:	713E2E20A467272CF5E174DFF81954001170C7F92143A5F34C2FFAE9B85BDC04
SHA-512:	FAD8C0A7ED8FBCC7BC9704522B2A35C2BCEA68DE3A614009D49DE7F8C8B35F06DA12E5DA78EF8E96FF72983C33268046521C190C0BD0F8A644887A65DA44B2B8
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.305732261424221
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCWdVJe84MtsqXZhbkALEwcyj3Y:sr85CKVYpqeyDY
MD5:	3A6E83146F925E67FD9BD350F823858C
SHA1:	030EF0512034AE6FFA06C7B42041252A56613799
SHA-256:	494DC48B1892964FB6D5CBB19DACBE990434EED9DEE1BD64D9E74D14681717F3
SHA-512:	F06ABB303461C6F016470C343DBDACB154C2575095B67B0A2620DBF6E7F799BEC18A6F5E3C678DB107F98764701DE33C75C1E6FC08ADD22FF6D486164DC173

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE	
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.375840229458048
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCUK78LyRHC/T5ICzzKgHiTs33fSQ19uk:sr85CUdGS2gHN3aQ1p
MD5:	8D7C662937FFE3C3AA129DD3BA7B887F
SHA1:	F67F3B5C32BF6CC3DEA744DAAB16177DD86DBFF6
SHA-256:	656ED573131580248ACC968FABBA2197657EAEE8DD6D0BA533A50DD34E74B603
SHA-512:	71235707D208BEA37FA95A5BD5EF10F768740621008A50B3E440C70B86039AC2428E8B7105A93921DD8DF659AD35C36BB4BFA2C922335680CC1660B48FD54B4A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.461871956296466
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCqi4IvHjjWhQmgBhtV+mLtiqdSo:sr85CqThgpLTso
MD5:	CE04DA14A0724F9E950D41F9B2CC1643
SHA1:	EFF607BAD3A4CB05CC38065E45DC61555618A060
SHA-256:	D90265A2653E732290DD6617ADD54CA1B2981481AE6B6C18C570D4552C84E826
SHA-512:	6E548630AF301C8F472BACCB487C31E7E4092E3B25F439D585F36F0A24846C6C0F4A3AF34BE25389D9B9FDF6C1A03A9A8106F9FD777BFB4D1F824A29844E5803
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.119504084682648
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJxqs0y0gqotvngnYkJZZZZZZZZZZZZZz:JxqjQ+P04wsmJC2L4Y4YkvJt
MD5:	EF92B40044CB210120E9889CA1DC1D5C
SHA1:	EEDCB5BA7F70F04C3D25AD321C93F978E5E1C7A8
SHA-256:	016D35F82750ECF792D64A6CFF5D376DB69F2BA1D30BEF80978CCBE84ACFFD0B

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	
SHA-512:	DBB2EC69392CFFA9ABC8EB0E2C979E5CD4F6A806E14D53F87E8D041E7F0D25816D13363FA66F97FB93DABA8E5CBB17D617029A87BBB31CDECE9A48745E321062
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	4.799951544005101
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJbR+QDxQPcfwBOB6ZZZZZZZZZZZZZbJO:JxqjQ+P04wsmJCC+WxQ0lEJRaCA
MD5:	7078371E0D358B86D46D6CF87987C8CD
SHA1:	6F58E6F33BB9242034F7C6CDCF17B637C060C8BA
SHA-256:	2DE937273CBFE6AA5909EFD083FFE477DC7CF37739F12923E2B2FB1B1B6E17B1
SHA-512:	13449BFDB7AABDC75EC51F1FCB5FE95761C22E3F9E4D1A1CBB5BFC0A3F8FE2AB2FDC3ACD0BAA0D5BADDF0CD0DB390788C60B9C664C3E3FDCC29537347B83E4EF
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.05148718063145
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCPkMrdYJnRQV6J4tuw62roH5lL1u:sr85C9rsRQIouwjQlL
MD5:	D4B144B9963B3114F1D938F44200AE62
SHA1:	F14C2F8BD9BD0CAC7A682D453C58B99858D6C0CE
SHA-256:	CB49C8EA020EABA89BB5032060928901AA90BA2530CD5D5467D15AAB489747DA
SHA-512:	80D70AAF806C46388447A4BF0DF9A98C7DBC211E290A60F3A30C560E09BF12BBDCDABB4DA0B945A8144CBE8D2B22CD4F0D9AFF4DBC33E8FBCB7DAA8244CEDA95
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.365915780903398
Encrypted:	false

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	
SSDEEP:	1536:JxqjQ+P04wsmJC+rie7lHfYdCtBzNKxmtshDucWs/7VOb88sirz:sr85C+rN7btBAxm2Z/ps/rz
MD5:	43B8EBCCF6312172AF0638D6EA2E9A4B
SHA1:	C628EBF5D72FDA6B9BE07CB69312472906E1143B
SHA-256:	B42F96D408CFDB35545C5900EC0E8AE72B85FC960DC4BDBDEFD0B6A4BF3A49C3
SHA-512:	773A5C800CA9EE738A6152D0B9B6F1CFC410407F95CA84D72951C4D8BFE914659FD66892A927174278BA77B5190BF74B98B806E6A78AAAE2D70277345AEAFC4
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.420838658743323
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCVNAa6ZUmWtWHpy7+OAqbrefMSy8A:sr85CVNB6zLy79b8A
MD5:	58473BD19292BBBB9CE1C6BFAE872648
SHA1:	D9B5084A65CF3C039D51AE4F1C39C7E5DD83DBCC
SHA-256:	328E9B6CE1A7D1B4B8B602F1A2D61C56BF85CEC9293C55C047584937C9390C3D
SHA-512:	E0A19F3C91BC3433D5AD83C78135346769889BA06EB56F92AE3137CB7769582BA5F6139524EEFFE238B67CDA3BCC8854F2E59283E60D23BD555DEB6152310872
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.364257425575085
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCRtWit2d+BkpzTscsot7h:sr85CRtWo2Q+ycsAh
MD5:	9180D3CEE013A6DE40DD963A16951734
SHA1:	18E74AD691F4448AA451FBE5AB7D374F24CB07B4
SHA-256:	299E81E2FE407A151C56B24E904AA2B0B9C18F712A0B43E704034939AAD1B564
SHA-512:	DBDE2F6EED630ADADC7F58FFA269DCFE2749F499B8C5DE0927DE47EFF55FB7B6A185B1323DA55307228D117629B79152638B129D92562ACCA208555E7105F9E F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	
Entropy (8bit):	6.435519044418047
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCxKZg7inyp+gsnV3SNjDBII0DNC:sr85Cx4g7Ky1p7
MD5:	E7868326F5EF4E85A0FBAEC678D13A2C
SHA1:	7E57578EA08482DA52474EEB3960CD4407225A59
SHA-256:	D702CB2F33424FDBCE4EF3CB5B2C0DA789758F4EA6A4AB772591F110369F90F4
SHA-512:	F56B049C81F2433875840455C18FF972C848C4AE0F04CCFD5BBE5C2222A26680AF3B86A301F9886A84C8D4EAC8861786AAEE224278E96F85B999BF4DA7E3306D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.278417014765199
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJBr+YKB8MXTVul6YekIfQzbL2Vo8/nXS:JxqjQ+P04wsmJCUyYKBRXM6PaGxZCP
MD5:	4C6732F9F7CF89C1BC807F26552F0592
SHA1:	9790303D2B8FD2C4DEC80D34C7E7D61081DDB03B
SHA-256:	16A32ABF53E0246C49D984F31FA56B612A818BFA4FFF7681196DEC4F6343F19F
SHA-512:	56D5EDE482CFE2DEFEE022CEB66EF839E9B47F33D8A270E060A729D70FF03F74A8C1699492C8C2BFB88B70483153C79A5890B31FEB3C7B3BCDB0AFC9D4FE59 A7
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.254081989191424
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCbblZ1PNq9uCUOFVSiHdq+sxneZ:sr85Cbbr1Pg9uCRFRzsxeZ
MD5:	C2C98501C8C0A38CB3B3D89B1CD09C67
SHA1:	8D8469485BD3995DE34512BAC18DA482A31B5DC2
SHA-256:	EFB24F3670542E6B491E3B9092E31E5068EDC2068C986F4D96E9F8176F6DCF26
SHA-512:	10A42C069528EE8D55BE2106F2851B9E26AFEA5311D63D1CEDE860DB6B8E0252C3875422B047A9C6D35FC3D3F8409771A682B67C85CACF0A8D8A9352491FC3E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe	
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.565853286242963
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJPwnvIu/+HCidGL0RYfqJfj+0xUYfQ76:JxqjQ+P04wsmJC6cQZo0xUFGh1SNcs8
MD5:	2BE98153912196C9044AB31250DEAF28
SHA1:	18487088B298B9E6B5E7FBDD00D5C37F2ED6AA78
SHA-256:	47164473C9E34EC71472CB3516C4575D1C8A4484BE1308DD69AAD38CB84D03AD
SHA-512:	20DB7DFC73249CE140DC3764D8A304A0CE080E9421751CA394829D0A57962D19A86C2A799CD0650DE14CD0CCF56BE887B63E696A9FB0F2D12994DDAB410CB6 2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.517183428602308
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJPgOCegc5f3E/lwvSHazYLO0K/rdiiA9:JxqjQ+P04wsmJCznxUOoQXALA
MD5:	10CA92590C0A328CD9DD6B232AC5B97C
SHA1:	CA9C9D94ACA6666E7655B9A7E3E11EAA23D84119
SHA-256:	D6E3584260FE9CC093D4E7A33A66C201059296D5BBE30DFDFDD3AD76584192CD
SHA-512:	5D78BA107880C8D8FACF61EA5C097705E6410C8D2AF8D6D49540B19FD2DDAB9177080B6435D30B9E3448C81DA4C85943456F93A4F3F549DEFD0794AFE85CAD
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.31341198420156
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCMw0wAh3A5sWBMcdSJ+L94ltGTxv5ou:sr85CMuAt2Sk2m5ou
MD5:	C5CBA627E9C4F07BF06013E2E19A2ADF
SHA1:	B8678C954DE42C8D686384179EB1835E378C19E3
SHA-256:	0215077B4DAAC5B17314C2A55673E2416ADAD7CD34E8C33AE748AE22C59A2CC5
SHA-512:	234455B1C396B38DF98C569584C85CE153423CAC75E9E0DBCB724D9A0795FBCBE6D116185017535CC23ABAC49DCE9C77A9D8F470BE7B899E80C7C7E5086EE7 F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateBroker.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.571220400525005
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC85J2AeSh8/J7YGzhc299YX:sr85CRgh2Bh1c27YX
MD5:	2CE4DFB3663A6C0B5EA20EA10DECE139
SHA1:	A9D39DDD39D9419D1B0A836E9110BC5E7CE071DA
SHA-256:	006DC11C857D8EC872D4ECFB6CF70FB1BAB5C95AF8773BBEC11E07C2E0BEFC27
SHA-512:	0F25FF89C156ED21AFB55F07BE74C8B290C9E42710A3AE3917CE2FEAEE3626FA20E26F1088CF47CC487B18C69E3A1A3B560A321F63EAAB9A3F478822B2B0F904
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateBroker.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateBroker.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateComRegisterShell64.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.35638621946935
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJ1jaG5lO8Ao+MJo1So6lSvUpRGaCJ9K7:JxqjQ+P04wsmJCwNbRu+2Hdt5yG10x
MD5:	9AC378232CF66E98AC476EE00ACD8A6B
SHA1:	ADDECA30D06C773A5C6D209646EC64DC0CDF3039
SHA-256:	F3C6416304690DD5950F44E4721CE140B8932BE7C130204DEE2A623998F0F716
SHA-512:	F14621706EF7E9E480A13E17B3A0764B93AE06EC6507C2401FC57D29D565397969A98091E373DF06A169C3005537A8E635610F1091AED5B64B8A22D9D253B46E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateComRegisterShell64.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateComRegisterShell64.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateCore.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.572547877647106
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCBeljakK11t5rL6Tfr/sVKQ7t:sr85CBkjtQVrY/0
MD5:	FDB7DA820D2F539A317A598BA31067C8
SHA1:	C9D147B854A2BB03D782A3BA1C645C525DA0EBD8
SHA-256:	2D98E44BE09EDB2627AAB1A7AC69FF72CC7C06E24CA77B9F4C14A602B5DD78BB
SHA-512:	6195C603856129DB9310484D0FD09AF788FDACFC468EC21C3F99E6BE7718AC491D6E001048492C3A67F811EABC062432DCF0EAAE175489B1A63A6CED1E8D865
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateCore.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateCore.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateOnDemand.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.571346004771877
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCjpJaUWSZknGE7YGzh82dlYX:sr85CSsZmGkh182jYX
MD5:	5BC82420D22E028C2481B8150AD4F793
SHA1:	9DE41D3BA5DBF3DC259110C5C34E216315DFD327
SHA-256:	2CAAF2C35A46F53327B11B7EE33B34E1DB112D5C83798BC1B1FEB11A7DD38DD1
SHA-512:	61A5207DAFC38941A87EBB47B835F212C4D4581F2E3EBE5FE2AEAA7E1D51221DD1805176B0925967B4934754092B364A1A40DEEB778E6817B6BAEC533B367D1A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateOnDemand.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateOnDemand.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateSetup.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.5964179831347325
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC3GoO5OLmk1uFQfI5367Kd8:sr85Cnm5Wi3h8
MD5:	49108FC1C6FF24CD49C200E2D7A44B86
SHA1:	E79038C6363781BF92D4487BD77A4A770352E948
SHA-256:	06197B71B98A7C4FC08B2B354B6B5DE011BA11CF958827BEE3438B170A27F17F
SHA-512:	008A7A84B3BC2337AF59260348076CDEE1F3C507AD2BF4D2C567029E1F12594555D2BDC4B9BEB2AE77B29E07F7F02158806DB196BB1878D9018E34E7A7757FA
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateSetup.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateSetup.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.653521772684421
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKEs2WzzIR++tGuPkNoAvBFbq6DAcBDjFsb:sr85C/qLWos+tGEkBbq6D3Bdsb
MD5:	50B7F8BD51D8BEA4542C8B6FB7046568
SHA1:	46FE9571A136EEDD3DC35089F096D47B32EA74C8
SHA-256:	86A782FF58F3B5F1736EF23051833E340FD56A77C1EDDDBA8ECC5A507BA47EE0
SHA-512:	87A46E55F78299DA53343B832D84C81C230D46AEFB71C603998DA5F6D0BB3FFE6FDA5F825F5731F7B810E21C1EF8E9812278D07E7402BB3913AF6DD66DD43CE
Malicious:	**true**
Yara Hits:	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.330325009255707
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKMmG2haDkdWIJ7OkUVS:sr85C/qzE+bgOkIS
MD5:	47848F50CD963815CF2894B7C284095C
SHA1:	8F8E03058352E172E9158782BC8E315D026CD720
SHA-256:	115C7F82BED3C1779F50CE53273248152587D8F9421B933C10534B84E16E7815
SHA-512:	9D692E732A6E0F673A2A4ACC6E7877976FCB2901A874D696ADF2A16EB55C08AB738744811AC9A6AFD5673F2FE272E2C6663B6EB123049F41FA5C1E68EBCD5A8E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.656070779362061
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKKKajo+iKndnTdkCE1A6n82c6jbs2:sr85C/qo0o+iwdnP6ngIs2
MD5:	60628C314BCF2A97CCFA9CB4241A2DAB
SHA1:	6EF748A1568A9AE0D541C5CDF0F74430A59E4DE5
SHA-256:	FD8BD222DB055C39D6050A10F91EEE576ADDFC37CE78F585ACC48F96E222FA90
SHA-512:	2AC9ED50008A13A4255ABB338C675D53688D321E6086B6DF17B02A3F89896051F60E8565001CE0B7BCEBD0CD211DED9B9574347BC95A05922700C20806EC93E
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.6397427450636055
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC/rmKHLgwHz2xi03XxQy012eqZwE:sr85C/qMsc2Y03BQz2eqZP
MD5:	7132D6785E73B1159F3AC9AC5DE71A1C
SHA1:	0EF8C262E63E3776662064D00E5C4264D0213C8B
SHA-256:	629945249C52DDB4108FF5C239D4E2C79C92A545ECD25DAE395697831D648A5F
SHA-512:	804BD2E14C52D226F1D470D0C73B3DE7945EA24EA4554D916FF796E24F6C7C6B5A21284396C6359CBD94ACCE87517D19984F207FEED537AE9DDE8C29D04D2AE
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.346606571165856
Encrypted:	false

C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	
SSDEEP:	1536:JxqjQ+P04wsmJCOLIFaIz9SEhJyurf6S1TWfavAd3VbB:sr85Cb7hfFTkd33
MD5:	95ED8DD6C4D471F68911840679CA1F9B
SHA1:	5BDD0A4778F72B6AC95FEEFF108F74E342981690
SHA-256:	82B98FAF27483CB4C8957A2BC6306C47D59559046C8DCDC03C708C77C36E2417
SHA-512:	581BD049EDCEC4E330FEC670AF7B2980F1B338FC8588B596555803A43B0BE4232A3376CB314C8F3C9DC615D892D80746EB2E1C60766BDB7E046515DB9751DD8
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.107296013528715
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCWnoDdvhQBW1kqanjaYt6Zs8:sr85CaEQQhanIZs8
MD5:	4141A0DE0BCBE19FA9E93DB323462679
SHA1:	88F7E506A247D882C4F4E924D1E3DAB0FC077387
SHA-256:	3CD849C610540723B3785865DFCC8F65B820003251B39ED6594A8A979F20E948
SHA-512:	940ED87A4C20AE138D388D2324AEBCCA2FC4C93B8D8C2443E91EB382937F79B55BDAD03F595C4EF3FA94D0EC087EA3C228ABB143BBCB79C554E5C3FA38CA754
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.242980084696127
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCZqO55PvVT4zHu+wLZ8qU:sr85CIO55PvV8HVwLZ8qU
MD5:	18E80CD6901FFDEDD81B44D0526240D4
SHA1:	640A66FC69235A0B3677A010376FC607CC2B50E6
SHA-256:	3A70FBA9C369E6FC2DB35AF45D1201833ADEB33B1ACE24603A582D2BACE6ACDF
SHA-512:	4F62E2168BFCFD0329F12F93FB5783B9D70989852CF9C12339FDED1ACC5C984FCC847555DD223C6EE2C3CEF64DD95F580DB31138F9D2F47E68FF2F6106A3BE3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.2705620011183765
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCFtwbWR/v1o/G42UR9whwRrcUTR9EhhBhc:sr85CpnD9UR9whwtvTRMBy

C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe	
MD5:	F56F560D473A7660D3AD44E731930A06
SHA1:	B71090C328FF4234B213D76689591DE15DEBD0F3
SHA-256:	9B7384DC0D5DBA8C5161DB5C42D3075A4281716F741F10DEF974C5C680308CD0
SHA-512:	0134B6C093C053343177A83B81A23EEE54BF4C655958906B854B221B85097D633FA96953B83343F6C207BE5A15919017EA26C05DD3B46193618FC26510C6E74F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.110851138659397
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCIbgvgvwvEvFvwYF57LoW8dwhFz7Oos8iwiFT7XMvNvev0vUvZo:sr85CIbMMc4ZTTfRyKFifVlt7wx+oIVg
MD5:	4DA76295D7246E94AC917F192A2ACE84
SHA1:	58964579A019BEAB01488F1B1FD0A83C4A38B0CB
SHA-256:	D1D94327BEFFD6F453E862BFE9B715C980B20F33F38C8825AA2B2DF1DF33F9A5
SHA-512:	8811B0CC2BDE08B9354AC1F84F441F7E3D11A31D7E5D25139E53DA4C2C2E99645A1F37FAA7FD043B4FCC1169DB59FF4F7BA8EAC9CAC14CD455B3CCD34B6BA AD2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.46960810763993
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCwMkBExFhpgLTGlrFBbeEOCr:sr85CJ7uTGlr3iE5r
MD5:	3AE73C8D42CF093E893717A04A20D5F8
SHA1:	96384CCD613D795E953BFD876250C86007EF74D6
SHA-256:	BAE7AFCEBAEF2A3BB243EFAF1305AED127D21B978D7C4335109F2A403A4C2CE1
SHA-512:	C90A74241A93652AB10BD6E1D476D89C995C7749938B83877C14A8F9496959C8868F21239DC6C468629852D154621E310CA76FB4C50DF8C02626560D48F96E07
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.448388258977007
Encrypted:	false

C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJZyKcXJKtm61b0fth1uvh/NYANLOT9j/:JxqjQ+P04wsmJCRXJQm62t+vTaT9jxd7
MD5:	8BA32D4C4C59A22D2A5A1BEAB8B004C7
SHA1:	AA91417C5BA67F09E743A7740662EED65C4873EA
SHA-256:	2B0E0FBC461BED861EAF961F5058A18252A8A517008660D46063A1DCDF10DD02
SHA-512:	07B9A4827EFDE249FBD6953ABE3559A589500534E8DBAFF12C65EAD40FDE51395822BD265AE48D271ECB825BF6EDEC3D7CB7D2D96FFCBB3AA167FF7FC1A64AF4
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.285196024262785
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCVJQEW8SSfaU/VEwdwzfnuktR9KJMkW:sr85CbQE2SkXFKJMt
MD5:	2355BC5DCE8E63203BD523F6A3EF11C9
SHA1:	06E09B957EC99F2635D39BD9D3EF6FB8C26FDD8F
SHA-256:	37D5B62049B2ECBAC53E3126E68E2FA0416A2E220C97E9951BD71FFF52E514A9
SHA-512:	71BCE642EDC4355E8CD217442EE6AEB1AA536069FAACA69633EF3B508A6E523FA2386A7EF841FC84F9EAF475725368DCC2CED0C0D4C13B170EE789A69FFDD6D7
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.72011826313205
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCa9IKr1BRo+SYZMuIb3eJG53B:sr85CaDr1BRo+SYZMuW32GhB
MD5:	BD61FF1B20A7530ECF797894EE1316DC
SHA1:	A9601D8B56C247B801E5D5A89377EEFA6FF37FA2
SHA-256:	29F10DE4B67C8BF585A581AE8893069FA52214A18CC4444D3E207A7A657EBD02
SHA-512:	CD91235FF8ACC7D8263EF05028E728E0BBA90D9459B3FD86568C7149DFF55F1E3E010C5234C234DA87B2CBFBE7B8C71DFEDD9E8C5BB326146579CA9EAD9005F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.169493808225336

C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCslMDFepJnQxbMwwNOhO8WSnWR0Oj:sr85CsaeYyiL7WR0k
MD5:	8F4A79DC0DD71E8CA092D84C0260F92D
SHA1:	CEB13BACFAE68CFE94561487FC6E0AE0464C6A58
SHA-256:	2480D138EE436D182337435EF36F9A895ED9A98DA620C752976D575C08ECD390
SHA-512:	A100A527B654FE476672B7809A4C73F8C523C2620815476CF8D994E1553A344CFE4191FDF8641719D52B29743D625574A9287EF51BBF343B5D8FDD428FE68D33
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.3186383734960625
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCDnCgs1pSd8MvYMRLWjqov/M:sr85CD+4DFLWjlXM
MD5:	B4F5C898517A6B40402611BF65397423
SHA1:	F6E1F64CA7C05131682153B67E5EF5C54533F1DE
SHA-256:	E634A7EECA5A30B359DD622BA3A3BDBF5729173A416C86C962647B2B7A1F286C
SHA-512:	C510990B72E1FCD1007B38B0A9F4A28280E909D2AC81AE08F106EC482423927EE13081B89DA316D44EDC6FF684C3C3FB93E898705D6D7E7640612560C494E5C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.392056642854633
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCjCTi/Y5cIzwdi9Jo5wJ8RNjRmBF2XFAkrfkGj:sr85CGT/5Lz8RNIBAXFdrtj
MD5:	77E4E96AC817B6D2DCC671C75B3AF7D5
SHA1:	2B3C254A156F9CD60BD9EF5B5832C7BC8F7FF9E2
SHA-256:	657B05CB38BED57B93383818722F9058FED9966D1CDA1AB5A00034CB0F6E9A0B
SHA-512:	F4F835B4004C5BF7C7ECB7DF6179EEF8DDDF277B13609A4ABE5AF4A748AD27A6207020E6A9E5301C89C0FF689CFCD99234245BB621CCC94A3E2A9B930DA63E 0F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.496755886640026

C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCJ5SSe4emv59S7OJvwgUQn73bPrI3SZ:sr85CJte4eK58i6gUQ7LL
MD5:	C5ECA751B54F507CCB797556E24D9EDA
SHA1:	30949D80A7FC4778ACCD14FA9A35B3910F0C96D2
SHA-256:	8F2BF3E7F90A0A85C2B121E448BF1C0BD8B5C8B860E64C1ABF64DBBA8C20111C
SHA-512:	AD1B5E374C615E92EFFD6E789BCFEB99D7DBECBCBB4DA4ABF013DE911E5BA8B6B14F836836EA8EC949F1652ABB29A32204FF5B9BF843C85ACC1453DCAB162C64
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.268163712816429
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCdi4v7jFil6gu4ayPdTTFDiopJLN:sr85Cc4vHFs6gu4aCdPFDi2
MD5:	1EF797E5E199041B8A0EB41A50E73185
SHA1:	2D059C707E2738DD623FF8E4D336D8B90B482451
SHA-256:	0BB888F08C57AD222A544EB3A73478B4747059277A80F21A03E5655FA21CE119
SHA-512:	3B08845C01002AF7B35A5BCDCA1D984D7D019EE117F0CB761E3DA608329314067DA1A16ABEBC8AA3FCB602EC58EA77D0F1EE3FC288142DDD0F44970BF431B(77
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.201681837230837
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCpSsTITDBkt+ETGBaORneubkuJ:sr85C7IvibTCaOFeubks
MD5:	D528E65D0A3CFF610803965BAB5D42EE
SHA1:	A01448DD0C03BAF9B1E287BCB87A58450084BFFA
SHA-256:	C82DAD16438E79EE2ABC34D1B405F09DE3844FDEF99F9115B58E7D1F7C90C4E9
SHA-512:	4A0C3C8F49CE25A4D5D06359683DE444EDFC6B49E09323D10F675E5029D584135A80F89A04FE77CB58D4B9BC6522F7E2DC359FC8D6EB8A55F981AB4CC07B913
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t..*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.352529349012904

C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCkb7zbeu8L16Ytx2XaRSX2qA4i:sr85Ckb7Heu8LSakmP
MD5:	2249CAFC0B359EA41F137AB87DC151FA
SHA1:	DABA42EFF4B9D3251E409CFD98A2BD3B9A672ED3
SHA-256:	3478297533C741CBF62D8FA8F2D820089E3777EBFD6DCDAD50F8FBCF93FB6304
SHA-512:	D0684A20BD7449D97323DBBE93467148F7E63DB79EC1BD3AC2E90D1350148EDF6F31E7BBEE1F32773D169CD04E1D11FEF03AE2E2C5637A89288FFB08C8115D5
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.46773744909196
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCxvuAvYalUpgotzYIlHkHwt7//Qt:sr85CqaBotvHkHwK
MD5:	F3279F5053B3112B5299C08136AE58E9
SHA1:	5B4C8EA82DC1E296CB31EC7B439B8B6E52795995
SHA-256:	1A1E7090747C3F600989939E12DA73BD2E85FFCAD10159E7AC52D374DA11874A
SHA-512:	86A355429C9358EEC0FE6B95623DC26FE7879684CDDB6AEAE293276FC5D604CC37DE64FC520F0EE749A3F6A15E9D5FB53852F9B444A0B3DE1374077578A9956
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.4135504331115705
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCC+MHzv1nArfoWBgJCSTgHyyf:sr85CDuv1nqQ2zSESy
MD5:	A937F48D8198AB59DF93A63E834C4AAF
SHA1:	4DA8ED9F7A886A8437562470A199744DF6E88F24
SHA-256:	CA2CA4A45AB550D894AA4B16919FF38ABB7784E532C327891DF71645AB845C6A
SHA-512:	490CDFC2D7AAF7142889398D70DE668CCCD8D4A52AF7C5FA9D64540CE2740F09A481293F4DFFED1ECCED9827148313D2296CC9BFC9716A88814544930C9DE5
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.344917752925491
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCDt+pejhS5enb1o24/tmIY514oZFt4s:sr85CDt+pGQ5E1o24VmIYX4oZP4s

C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	
MD5:	EA546BBE947027BA147DE2719F53D051
SHA1:	38B150F5A8BE8E19B5D1F2824F8EDE784DE2C6E6
SHA-256:	930F29A1D4152D23CB5F1E60693191F2865F56EA5474BF720BDC286D518CD9C1
SHA-512:	D456962B5511F76AF309345C22FCB20EDB120CF4EC3388300FEE1864B13859C605C40B6E86357E698DACA5AED60F56B59DFF1655E3059A9065B9550A7A3C9E1E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.464347380493513
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCSGNDd85lS8adLs4XK9OtiRk+7mLpNKahE:sr85C9NDS5lS8D0K8tMk+7ms
MD5:	072EDD1A5D3A99C26EA9987890989B31
SHA1:	6ECC5A3EBEB7EC6EEBBEF28CEB67079A92F57107
SHA-256:	598CA2D9EB855C5D53C9C19374AFFAAE2E4A6A9C9EBF1F46D2B025B5BD8731B4
SHA-512:	D11D018159148C9926450A3047B207484D1B31B80BB975B435D6E0FEB497F60625450273C1D834FFAD74C7C581A80224898FDCDC41BB9D3BD799E70AE8EF838E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.4498443082331764
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCLddbrls2itD1NrBOTe5IfY2X36Be:sr85CjbO1OTqcX36Be
MD5:	187B658322698CB74D48476EB2ECB171
SHA1:	3C4371425F833F6C7643E09BEBA5762B67081611
SHA-256:	7460BB6E5A2E43F3C737730FE5F9FC5E199072C61B870C07FF35207F333EE496
SHA-512:	3013808486F1445457BC00B919AFDCC46297B3F167A876EE5F028D50456EBE582C05882D99A0E677531C9FD3796F574AD88AB48FBF394A124F425894F841D636
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.336782734218808
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCEbf/h1xmGzUiVZd0p813HmTJhM3:sr85CMfJ1xmzsHmTHM3
MD5:	A3977FA0A7C20B05EC69FADE4F852D71

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	
SHA1:	FE2C747F4DA1C5C85C55EB755CA32D59B0B1EC43
SHA-256:	1F3B9AB4F318C962967E9418DFEEBF251EF610A0ECE5570E166D84B6A730A932
SHA-512:	CD8082F275380F4CD67BA08904C116E921C428D8D6BD8BF411A93B42CA9276332AB6E7F46EEC05C697662A98CC70841D12AD3EA6A3DE54EB575DE11BF2A0A12
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.531432224892055
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCN5Ss6w5T7tIc+9KLSifgpM5:sr85CrSsp+9KSM5
MD5:	A651847108A83A8B2A3B75A66403B0DC
SHA1:	EA7CFC3C984B676C322578E80DCD78DDA75E5A2C
SHA-256:	A1616D454E5EE365285A3E03455CED1FD70D8EEB682D47A8379EB08CF801D325
SHA-512:	0B97CD6F46A4660C27E99F140D07BA7F0F380E32062D5F9AF550C161E0191332EB27A196C5CAEFEB94A091CF9294FFEE91604D0FEF329260F768D9669591E2CE
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.556968630457308
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCVFFlJhOo/ovdHk4h6zeXVv:sr85CVFFlJhOoGt66F
MD5:	FB0697C512E65305CF24EFA18EC58086
SHA1:	B924F5AFE1A14163E20DB2CDCE980017C1461D1E
SHA-256:	CCA73F1C0206BBB9D6567616808D4BADAFAB7796ED40FC86097032802F2381D3
SHA-512:	FA3AD9699129E24AEAC778B38EF1B6CEBA11B226E6636635224FCB9019036D9E11726F11F50A9D1D531A8A6F08B5D3A3B650E7416655113284B63412C01B1F60
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.131108501135707
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJaFFlJhl7XC0dHPgzh263DX:JxqjQ+P04wsmJCVFFlJhlLDHmdzX
MD5:	2DCEF042EE374AC5BA2307EE6D97FFAE
SHA1:	3E39AD4F60367BAFB47B3759253064F7BA57A92B
SHA-256:	C83153D11C1D63FF5C330035DD66A958BF19EC465969D82DE87351A2C5F7A99D

C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	
SHA-512:	9319A16EA4B3D49FC1CFC4FE9E5890E2DDAA3E5D1523A150C77E0201C727EA0580E0B2D79CD4914968305B037B987494D57604E4792790069E992EEEE3D5324E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.254281392784178
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJrBE27rCNzU3GLCAAhUSCr1HkueFNUx+:JxqjQ+P04wsmJCKEJzbmAoDucEMQnF0
MD5:	D7BF211CED7D30A27312CE4DA2487EE1
SHA1:	CE664FBA8F5BEAA728CB7EAE107C5ED3810A5DDF
SHA-256:	9266432725D9466253A4F1F609C9A2DD85FC82B3A0E3A6C43FCB1A267C976265
SHA-512:	260EA864A9512B243DD18EC3C4D6CA7782DD3ED117AA553E6C30F3249655EEDB3768AC190432CBA66078F93C83F8B05CAB352B254FB58C3586EF56F2C3482EE D
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.369176164130001
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCmmgFboVWAfMOD9nwcP4McxAF+V2r9Q:sr85CmhFbG5n7vcxAwVIu
MD5:	E883EB6C4D29614F1887EDF6A2412659
SHA1:	33DAF7D41A5C6D4D8AB1C91160F775D9810E10F9
SHA-256:	BE47F38C1D1A3806AD27867DF41BF62AFB77FADCAD4F00CF3B68FD469E1B2154
SHA-512:	EF18F22EB51AE378651FD7421E56EC682BE64AED01D79FDC1E3366459690AE52E312B4BE3A70C50653EC98C261EE2557C4B4F908AC8254E47B96F7268847F665
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE	
Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.694866680260046
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC5wI4PqxgWvwG+TUawK:sr85C5wslwG+TUawK
MD5:	A851E7A4D035C32FCB2830718B34F01C
SHA1:	6D89FD230ADE8F14971A600591A8B6FAF67CD770
SHA-256:	73610C44EE38B1785E018C2BC869052729D56C65545F52EE5D2AB89C8C7B6DCE
SHA-512:	77726930C4BFE2DF33FCADA1A4A493F8DB8B3A5681C5D79DC51F9625C4110680DFA50C44CA272B71E46175FF56954B1583B9771B73412D25D06954AF8AAF81E
Malicious:	**true**

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

Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\SETLANG.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.511827025814232
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCHz6xccTu/YnwN9+ko47VGsKkfrwayHd+f:sr85CT6yHYn+o4Jrn
MD5:	2DBF9767B1524319753ADE899740500C
SHA1:	D684A9E8CC28A5185CF477554DF2065D73126877
SHA-256:	14143B435D60E49B251E80E37857E98D36088EB0CBE02C4C630F381E37BA8F0B
SHA-512:	A7B9EA44485796E0AA8C51A2A762EA95640EE34FEA51C3F043A5EC37E99EE95054F610C8FB72C445609F90B6EBFA5590036294B8E4770BD483E8926B38C7BDB3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\UcMapi.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.361986604416892
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJC4QTS8CYtvYSi+GAqeqCifxUajaQ:sr85C42S8/caAUSaQ
MD5:	8F8291D79A298A9B071864C651BB0794
SHA1:	F7614B1E0D476F1CBC75B5D698711F9DF460F773
SHA-256:	E9562B1B83495930753D145E9834CCA9128745E3163C060A4AA3D7DA62AA468F
SHA-512:	160D10672400D32BB10A059CC2AF3CA79810A9D0FDB88B79F6E0BB208DA26F973965853A429A7D9D4CD30570E015F17EB458DF6C6311BB89394AF46ED8B189E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\VPREVIEW.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.56237653560924
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJ/MyzuDxqDq2m1eHwSFdrdAHZY:JxqjQ+P04wsmJCOxzuDxqDsmwSFbuY
MD5:	2CF8F2ECEB42B70A5493D1EAEAC6B20A
SHA1:	B411993C6352F4B026153AE4010A6C2D7B1ACE3B
SHA-256:	A85EB54DE3BE548DBE89BC47098B417F4C1029BA084D0B15F75687D0751EF44E
SHA-512:	8D2514F16C8D47CE668397B6DEF1A59A4D2C7B7E4A8E7613865C4833BE0B882D87AECB02C049B7496D633CA740DEB33A59DE6D0488F21C26109C89F8C511570
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE, Author: Joe Security

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

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

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.388189611386593
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJ/jWSlFQQoUmydAHZk6:JxqjQ+P04wsmJCOjTlWFauk6
MD5:	62A21A597FA5F5C489D266A87694FE61
SHA1:	8A9C326ABA5638F6B91BA8DD18D258998CC9D25B
SHA-256:	D35B0D2411B6D5CDE4F61E5EBD70BBB1644AAE5E95EF417E3E885B20C194DE49
SHA-512:	F4F9F7C8BDCDC7CAC1D491E528E88464A78F6254F44F2C3758860B495E188B607EA2FB2B292CCD82829F1E462EC07BFDD5F0F1729F7083C9FA398FD7EC133E2
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\WORDICON.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	82944
Entropy (8bit):	5.131620925268659
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJDK2sNTXC8cEGV6GskwTO:JxqjQ+P04wsmJCOKZxXk6GskwTO
MD5:	1F414E9B0D1C3584418658367EC9242F
SHA1:	5D11420BEB0507F3A71925E2A0A2DC36EA1265DF
SHA-256:	CEB5DB2FF4B04E0C3683D039DB97ACC145C5FB9DD026A7DC9B84F12D424E9488
SHA-512:	1AE9A3653B774AACEA8A2CD24ED9BAAD8245967E16122F53099A8A640D6BF5C055651C50B5D83C4EBF962060FE021A274EDBFB818093A783884C9AC6DB822D 3
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\XLICONS.EXE, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.4980851403396676
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCHJDYG7YSUhCD8TanIVayX0TfC8cvB11lV:sr85CpDDkSQCfLy0fk11lV
MD5:	D4811ACDE0C5F48DACC1BBC3E310E8D8
SHA1:	06F814E81524B40587E503E32B8865D66A8383A6
SHA-256:	3B5D056392B165F9001BF785E6F91187B75A67F0209E5C189AE0764A66FF3E10
SHA-512:	6BE82945EAB1E9FD9BA507045B6B45799AFD11F5A3A30949E03FA100F93750DD0ECEBECABDB1883B764C90791ABED09EE191588BB8A8241AC6A6AFAAA120C 169
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Joe Security

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

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

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.57605386644689
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCMfSoIt2ZzzV9uc1EshwMDkEcAv4i+:sr85Cnkz//1DgEcAv5+
MD5:	100E15577B28178663E63AB854D28B4A
SHA1:	DC7D931ECDA8C09D0D2B43988E6D689A20E080F1
SHA-256:	238254BCE07446426D478897AC3DE27DE2B9606B2E8477F7DDAF8A20A2999FC4
SHA-512:	5F5A2C7F553B747A9A1811E9D4D3A0BDA525D5977D5BB709F65164308E020B31A7EC0029C435D8F05E46E737242BB5F934D0094728841F6C545E15C625444C47
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	4.744720269791172
Encrypted:	false
SSDEEP:	768:eyxqjQl/EMQt4Oei7RwsHxyP7nbxzOQdJozp/q4:JxqjQ+P04wsmJCV/Z
MD5:	316C81CA54C5FAC241D16CA25E7B341C
SHA1:	9E1199BCB359EA9146EAD52E765F3913A791CD7A
SHA-256:	9CE3D752106B78CBB5CF3DF574CD084177C4CF97FF35CC6E983EAD6F4A3F6CE1
SHA-512:	CEC15054D8351322566F67B46B333F11064CB650D4ADDCDBC9174C66EE4E4D4F1C3400FDE6BBDCD3B632ED051C92E898C5170B1A6504BB11A771230D4EA15D F
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

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

Process:	C:\Users\user\Desktop\6LkjS4JhAl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.422024969420582
Encrypted:	false
SSDEEP:	1536:JxqjQ+P04wsmJCjMnNFZnBeGI9cKm8q3+i2PPvfKLD1D9nwt:sr85CMBeLsOBXiN9nwt
MD5:	62F99051442ED97159B8D9CC03BBF8DC
SHA1:	E22CF810217DFC5700C2C629162EF37CA672C957
SHA-256:	C83C04BB7EBAC75F623938C167AD7F09606F2E0B786A1CCAFA12E080F9455E9A
SHA-512:	FE259BC5D8C12884C403B4F08E00272DEBFEECEDF5F9230F8B0A3B6DE100D58AEC610B849DFFD94568A44389FACAF7B55B1631F9AA51BD91B7C1F3C9140861 A
Malicious:	**true**
Yara Hits:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe, Author: Joe Security

C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....t...*.....@.....@.....P..d.....p..... .....CODE....,r.....t..... ..`DATA.....x.....@...BSS.....|.....idata..d....P.....|.....@....tls.....`.....rdata. .....p.....@..P.reloc.....@..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.213524537555061
TrID:	• Win32 Executable (generic) a (10002005/4) 97.38% • Win32 Executable Borland Delphi 6 (262906/60) 2.56% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	6LkjS4JhAI.exe
File size:	123392
MD5:	4aeb49bf7e23aab664de914df204664f
SHA1:	a9a80ec2e9ea803aa8db80aac266826304916dbf
SHA256:	d11342ce9c7550e129e455126cb6373145ea86ae5ee777 a652205541ef4cec2c
SHA512:	494bb1b3b713ca9592568dc58b27696f64b727dbdcd03f6 46f3a57235ffbe5a6ffde659bcef7fa13b7ebd854fd67ba8d d5fb0e23c1bcbf2d661896ebc23bf57e
SSDEEP:	1536:JxqjQ+P04wsmJCVB5IdO5w9VRvk/wDK0TJxxcR TQhxdpIElh:sr85CVnw9fvk/weJqxdpIElh
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4080e4
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9f4693fc0c511135129493f2161d1e86

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x722c	0x7400	False	0.617355872845	data	6.51167217489	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x9000	0x218	0x400	False	0.3623046875	data	3.15169834056	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0xa000	0xa899	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x15000	0x864	0xa00	False	0.37421875	data	4.17385976895	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x16000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x17000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x18000	0x5cc	0x600	False	0.848307291667	data	6.44309346589	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x1400	0x1400	False	0.1548828125	data	2.05936459375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 6LkjS4JhAl.exe PID: 6508 Parent PID: 4888

General

Start time:	16:51:17
Start date:	26/09/2021
Path:	C:\Users\user\Desktop\6LkjS4JhAl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6LkjS4JhAl.exe'
Imagebase:	0x400000
File size:	123392 bytes
MD5 hash:	4AEB49BF7E23AAB664DE914DF204664F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: 00000000.00000002.506546365.0000000000409000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: 6LkjS4JhAl.exe PID: 6580 Parent PID: 6508

General

Start time:	16:51:18
Start date:	26/09/2021
Path:	C:\Users\user\AppData\Local\Temp\3582-490\6LkjS4JhAl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\3582-490\6LkjS4JhAl.exe'
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	C666C22685D135C1EFE709CBEDD0EB6B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Code Analysis