ID: 501919
Sample Name:
ameHrrFwNp.exe
Cookbook: default.jbs
Time: 12:14:37
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

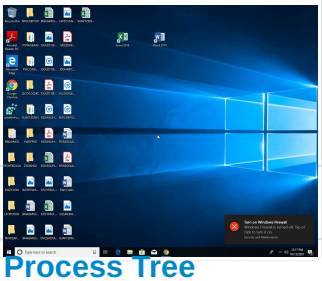
Windows Analysis Report ameHrrFwNp.exe

Overview

General Information

Sample Name:	ameHrrFwNp.exe
Analysis ID:	501919
MD5:	1f221e6e2a07d55.
SHA1:	0cd7541409f63dd.
SHA256:	2d2f62269797be7.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

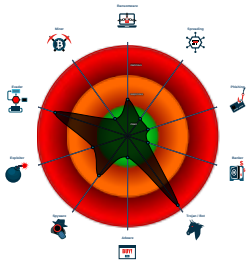
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Creates multiple autostart registry ke…
- Connects to many ports of the same…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- ameHrrFwNp.exe (PID: 5216 cmdline: 'C:\Users\user\Desktop\ameHrrFwNp.exe' MD5: 1F221E6E2A07D553E3FCF5BDB5874B2E)
  - bspmflqee.pif (PID: 3836 cmdline: 'C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif' ewdsxu.ije MD5: 8E699954F6B5D64683412CC560938507)
    - RegSvcs.exe (PID: 4644 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 6764 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8F04.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 4336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 2352 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp94A3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 4868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 2148 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- bspmflqee.pif (PID: 1048 cmdline: 'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 3560 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 5076 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 7032 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- dhcpmon.exe (PID: 1504 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- bspmflqee.pif (PID: 3032 cmdline: 'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 5572 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 6664 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- bspmflqee.pif (PID: 4732 cmdline: 'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 6540 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 5104 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf1e5:$x1: NanoCore.ClientPluginHost • 0xf222:$x2: IClientNetworkHost • 0x12d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xef4d:$a: NanoCore • 0xef5d:$a: NanoCore • 0xf191:$a: NanoCore • 0xf1a5:$a: NanoCore • 0xf1e5:$a: NanoCore • 0xefac:$b: ClientPlugin • 0xf1ae:$b: ClientPlugin • 0xf1ee:$b: ClientPlugin • 0xf0d3:$c: ProjectData • 0xfada:$d: DESCrypto • 0x174a6:$e: KeepAlive • 0x15494:$g: LogClientMessage • 0x1168f:$i: get_Connected • 0xfe10:$j: #=q • 0xfe40:$j: #=q • 0xfe5c:$j: #=q • 0xfe8c:$j: #=q • 0xfea8:$j: #=q • 0xfec4:$j: #=q • 0xfef4:$j: #=q • 0xff10:$j: #=q
0000000C.00000003.423204049.0000000004A4A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9ed:$x1: NanoCore.ClientPluginHost • 0xfa2a:$x2: IClientNetworkHost • 0x1355d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000003.423204049.0000000004A4A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 231 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
32.2.RegSvcs.exe.3a2e6b0.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
32.2.RegSvcs.exe.3a2e6b0.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost
5.2.RegSvcs.exe.48bb041.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x2874c:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x28779:$x2: IClientNetworkHost
5.2.RegSvcs.exe.48bb041.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x2874c:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x29827:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x28766:$s5: IClientLoggingHost
5.2.RegSvcs.exe.48bb041.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 292 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Multi AV Scanner detection for dropped file

Networking:

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Boot Survival:

Creates multiple autostart registry keys

Creates autostart registry keys with suspicious values (likely registry only malware)

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

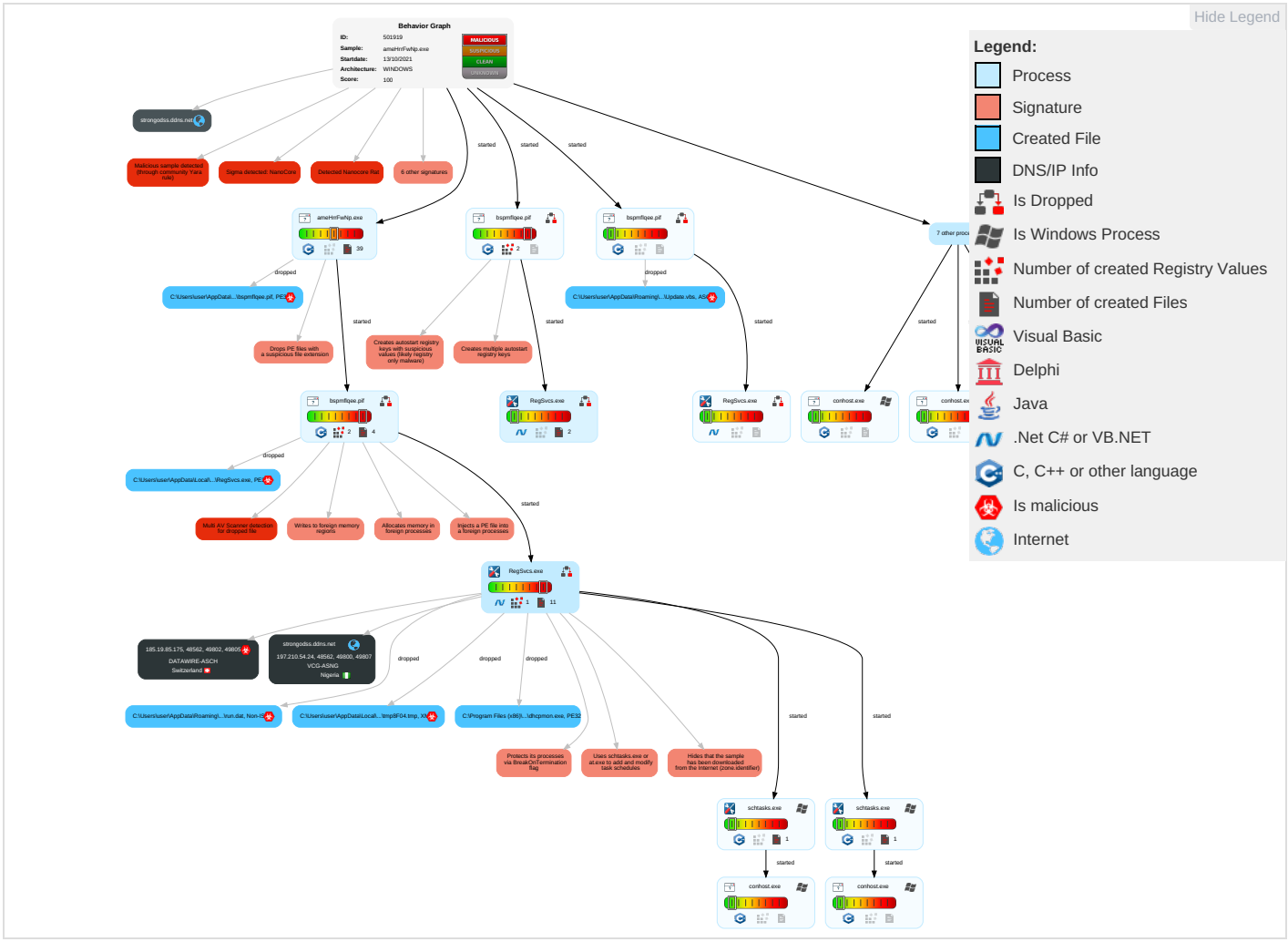
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Native API 1	Scheduled Task/Job 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-St Port 1
Domain Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 2 1	Process Injection 3 1 2	Scripting 1 1	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remot Softwa
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2 1	Software Packing 1 2	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

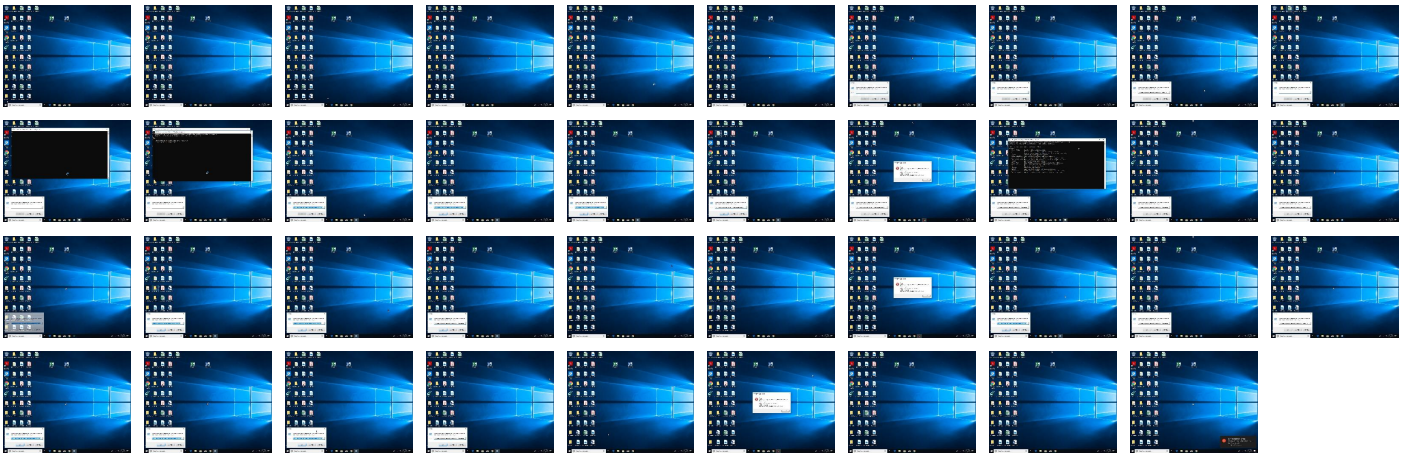
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif	32%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
32.2.RegSvcs.exe.1300000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.RegSvcs.exe.11a0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.RegSvcs.exe.500000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.RegSvcs.exe.6fb0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.RegSvcs.exe.1300000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	197.210.54.24	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	unknown	Switzerland		48971	DATAWIRE-ASCH	true
197.210.54.24	strongodss.ddns.net	Nigeria		29465	VCG-ASNG	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501919
Start date:	13.10.2021
Start time:	12:14:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ameHrrFwNp.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:	37
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.troj.evad.winEXE@29/48@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.8% (good quality ratio 9.3%) • Quality average: 76% • Quality standard deviation: 27.7%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:16:19	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
12:16:26	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
12:16:27	API Interceptor	624x Sleep call for process: RegSvcs.exe modified
12:16:27	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Roaming\98025414\Update.vbs
12:16:30	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:16:35	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:16:44	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
12:16:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Roaming\98025414\Update.vbs
12:17:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
12:17:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Roaming\98025414\Update.vbs

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,..P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

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

C:\Users\user\AppData\Local\Temp\tmp8F04.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.107159514403738
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0akxtn:cbk4oL600QydbQxIYODOLedq3Bkj
MD5:	211C08A48B92E556A855FB90EE4B0942
SHA1:	4E3ECFBEA0CCA0EE2743C0E23ED3FC79EB2E282A
SHA-256:	21F529F720EE77AD03AFD3CFA4CE04EBAF243C3E752F14C268529665CA936146
SHA-512:	B65C55C05249DFFFD0B52DF66DBA692CE21B6D447DEA43E93DACE718E40ABAC069A6BD2DC4CF0BC3F979A327BB7896BE6A3A36540916A33E0CDA8B974E295 5F1
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp94A3.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\98025414\Update.vbs	
Process:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	556
Entropy (8bit):	5.3119498211809475
Encrypted:	false
SSDEEP:	12:+R/vdHKmIHKEy4/vdHKmIHKEy4/vdHKmIHKEy4/vdHKmIHKEi:+R/4EEB/4EEB/4EEB/4EEi
MD5:	7C6769F8DEA687E698E0E84E195F6E06
SHA1:	478CBA334C07493F5D68AF8FF6BC7AFA68159178
SHA-256:	DCBB3D6D5B7937BD42F6030F54ACA188A2D9190D529F69A0745B66A46AF99151
SHA-512:	A594B79392A9F8DF2BBBD5390012DF29FC357E31DBECB100D6E55CA6A23C3A59AA6C7E4B793374C38E6BCC651DD3696EA30E0F5AD50CEDAC4460307A6C319 BA
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Roaming\98025414\Update.vbs	
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije"CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije"CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije"CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije"

C:\Users\user\AppData\Roaming\98025414\bflqi.xls	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	527
Entropy (8bit):	5.4581934236982255
Encrypted:	false
SSDEEP:	12:SGaK3cHsPchSllqdGJuaCx3La0ycUDTg1wstW8RKWd2nRcvyfe:cU6sElmoJuT8zetW84Wdyeie
MD5:	BB7B044C1869889E106DCCB7565B8A79
SHA1:	3F53639B4C01B9F0CCB939E84F2ACDD8806CAF8B
SHA-256:	26765B3A200C88B51579C1117DCBC7A590C9786510080A2347BDC3996F7CE006
SHA-512:	7EBBB130B0BD459F08F33380AA1071B5C0F1B8562AE640271EC33301E80EC575886258932EAB08A23C5DA0FFFB53910318576066C0E068093B0123B5CF95A61F
Malicious:	false
Reputation:	unknown
Preview:	Z2vs5Ug368bTu39207m350VS2O6pmT2nIs2MGo1978AW7A76fk712U239197U2099d89v25clB2y7p16v2PP3J7078V10Kwj5s04IX76Ugi9kD4c2759Hm4S83c78R3v25 1Y7Q177Ij72Qqe43..opC7A7379k818pO80r46TsHI0W93xe304HyX89VUH031xO5U7t0t6l0F6lO982k584j84Z4M359Fs6bK4YbSa1s9m629NAuy8P2l631xrZ60C103 45REH4u2154..R003vD..QiXxy6r42svB64fP2H78cub5w4TeSM53ViU895737J8917ee8Miu90zxbc06K1y403JPs8i35ZZ0p7378K8a76s419E92PPXH2H47PP321948 ..606vpEl2swF6va3MU198Lh6e8DYw1vB6o1ei0344518SO5O69n077w2LFU9Fa4KQ3Li0Wf3610K06upT5v44..H06U..b439ozR7JzjlhnLILipVbS6uaw5Q337L9fd24l74d..

C:\Users\user\AppData\Roaming\98025414\blqfwrfoe.xml	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.4555675690576315
Encrypted:	false
SSDEEP:	12:fB3qwHA1TFFN4rS9QrFfOP2r9BVX4AAceC4mWVI6NmWDWy87:JNA1nOG9wFcQBXTe5mWa4S7
MD5:	C7E2B6FDB655F30530C26D2C2EDBF84B
SHA1:	BCB902E52BD04D58FC562C90E6AACDAA0A7610BA
SHA-256:	D8A2F1D6A56838F7E83E4CB382D3B3F7A33AAB415E23E4AE5B8603B1346E0BCD
SHA-512:	CC0484A163A4698B96AD7F397E37A8661CD853A3C32B56C75D4D7040C9A4DC27DDCCAC3BDB06B92CA0B6AEB1CE33A34044D18C7C396977E11ECCD16E4E37 FA
Malicious:	false
Reputation:	unknown
Preview:	Z0935C13S2e9FxXSo8YkCsT7G8uIU9001OraNEg06JWF2lc3z666T83R2522C537h45q15278c8yptw85T668U661zsdg886k9f5G0l8FzCLZ7Q05N0t47Q6190Pe2NjlV 6O4m01kKVH0ruJ49Uk77850K8Y1yzE9Fo9u46w399O7Y94m54988..O0Q989hN66ahTLmTsu74Ce35RZ387f5pOWJW4i3a191240swt..17Sf32ATh135..185r2945486 944590l7K..Hq1qYr302z5c14369C7f6pN..3U24d99wt8q1D8pNHI12C0TPi5..3ol3l4Vq00i6C2O1756iyY0lzj8637oN4um5LrFXV512u2BM99Bu14v..5HBLD5167903xHK6xi4 10D0aNOpM698a288818lfx6y02e0Q98FA80w2826Q82D7C8721954w231rg6368o88303SI6zYz1nKBwUp5CDWp..Id531qzp00f3GmhOejU8D2i7u8GIH2Qhi2SY61Y6x gk75uh98MSkS8QL96Bw99D..

C:\Users\user\AppData\Roaming\98025414\brlfpdix.pdf	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	608
Entropy (8bit):	5.463531236483358
Encrypted:	false
SSDEEP:	12:zlklMEv/lEh29bNm/A72vvGr30woQpSoLwaM5D7yoH75VSVmB84B/1cJRgY+R:5KMOdEhahmbiEwo1oEa4Oob54UltcJny
MD5:	66459F672BB19399A82836CEC9189482
SHA1:	7F08BA22A59C1FD19E0579505CF9016DD1A8AC62
SHA-256:	8F7C37DF3613E2F87AD7A1478C3C7FACDD058A19283C87E40F065A7F830ED8DD
SHA-512:	8B097C70D159D6D8514DB803227C9D2F34752C1C5A86B5563FF210D6E8E05D4FC4B99F7F6CCA0509394E2E1862C83E6F7F0A018D33226D7E4962F9D6A0DD6CE
Malicious:	false
Reputation:	unknown
Preview:	l09eQ22e4w0HFc26yw13Gs11D209j84C81k9AN8zBUS4J38l8U6l903T0385i3BwM713J12T03Bs25XE1a99faANR84eT2iy3V53tx18OU6924nYpGfx43v..CN27u40Ta 757RY2690B..8Mn65m1pSkz6UAWhW8iZ501Y881478vu7PcFGz7RIr244jl236F96G0E44K2vAT8Uy7K7Eb48D7R5G6NQvbhn4b4M45VSn6ho6v95z9zoFf55n341RzX0. .b44A44W99k75744090B08851ci9VTKB3NpJRz..77Aj12XvpM3350V61017264eRS4dykKp2JZA2VyZv7D1P2xV..X1Wizblp06..5J2CZD706570L99HBiiY385v1956 8Ps..96Y621zW911Y6115cQ4y22b29x9dy3298Gl4420631E0Ch54bN1042k1oi70X43Lvthi3TaR38lL6454N69l75tcr139..768410VK7701MuYs9Sc09MMt0c91S56 6kt6hS5fmXnOpcs4S0mc69d3ekedeUb6B918SmKM40v757154166QJ713g2474535H1Y50HhxDIz3u32d801M9..

C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	777456
Entropy (8bit):	6.353934532007735
Encrypted:	false
SSDEEP:	12288:aBzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4akiP5DGDt2:0cneJVBvXAvwRJdwvZ5akiP5DGR2
MD5:	8E699954F6B5D64683412CC560938507
SHA1:	8CA6708B0F158EACCE3AC28B23C23ED42C168C29
SHA-256:	C9A2399CC1CE6F71DB9DA2F16E6C025BF6CB0F4345B427F21449CF927D627A40
SHA-512:	13035106149C8D336189B4A6BDAF25E10AC0B027BAEA963B3EC66A815A572426B2E9485258447CF1362802A0F03A2AA257B276057590663161D9D55D5B737B02
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q....y.....i.....}...N.....d....`.....m.....g....Rich.....PE..L....%O....."..... ....@.....0.....@...@.....@.....T.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...H.....@..B..... .....

C:\Users\user\AppData\Roaming\98025414\busn.exe	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.425509258170051
Encrypted:	false
SSDEEP:	12:P6PegCZnTYJE/odBmRQjZefXoNSmwS9Nx9KMf948kBStsh:P4GZQnjZqoR9zYMVeh
MD5:	6D176D6A6F1603BD9AD991DD89E63973
SHA1:	8E36ABB26A0D08950FE840296A486BF6E134FED9
SHA-256:	C556539176F1992F60A16ECABBD6DB2CBDF6CCA450C5DD572F50F0F71AC6D965
SHA-512:	E40D27789F3AE814B2193DED6E6CAABAF1A86575660FEE4048C318572D77966B74EFC93A551268E2433145AFB4F9F42167BCC2C2A79BFFC91169BCC1A8FAEF80
Malicious:	false
Reputation:	unknown
Preview:	87P0y2u7C29M3V5165651J212Wnc0P66d50427k53wBoZ892T72r439vYi8Yn1G2v3K2N57f415cZL0X0ya17nz18F3LmeUl..C5251Z5013H58r9680..4nu97J49sZ423t6tg0p25Chyap6awiK7qHMZ5l01Vl8D3Jf99870SCZ1B13lZkITGrB4563113yj5T5300T84T55U98959440ePk..0rqV9854ws622jY15T3A8BV18p70yt4p1bq554CA4rq195M7Q6822n5SU7UD2711K3U09190J7CU8622lw1s1ujw27fce0B2Tq535j3B90p4703tbl3U7tY5Y959Z4I498wdqGaDO3de1ZU5..UHw47k8It404I6Tx0e5t2wMN68m0raPk2oU668o3Z7Q228H1Ij2ZA82cOR2h1Kk2N9nHE0G2NQ6Oz46iZ5q3H1821PsgFZ94xi9..20561R62wLGq5rR031Xz826736N4oFyX6573h8b5ae9qU34Rf2X09x22hmT7lylL90wH7Y..

C:\Users\user\AppData\Roaming\98025414\ckrnnsvtob.ppt	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.447687369660329
Encrypted:	false
SSDEEP:	12:j4na1Wnf8+dCjctDznzfFZR87oA3N0PZfdVcLuGgrHXImpC:jfcnf8+dCgtDHNZex3mPZfdquNYmk
MD5:	C81632CBA7BAFBF7F39779E2EE21C702
SHA1:	97DBBF0044C476A4CC1FE50438A235CBBC0D714B
SHA-256:	8FA5B087D394BC6BC9AF27DFF9396963F3A195BFFB132272D1B4875F848427C2
SHA-512:	93D78B9101005E0E460839FA9546EC4DB50409D32B1516E747012F19489B8F9E158A485A9E9B1D2E59D1FD580AE590665A815D18BFB6B73BE38AE05DCC773196
Malicious:	false
Reputation:	unknown
Preview:	3Qlqj10tD0138W4OP57RM9r09L6fp66M694qjEF09M685h5518Nh5w02467H41QU14AnF45711q09y9855E8SK0b505f..42jULc5wl5l43wS163u6548C4er625fozFk28Ll8m0NmbE0t5fw515Y59C514b3u7Wy924YZ65ul790769ZA0I9664w27u114BXyvVUyAnY5x..G16ST8rs9JIp47T52X99KJL04n9v1c603eSV41rVeUze836f6i8Z371AC4o4R293F4096NuQjW32M659KWJW0h9PTWUbSa0O2XV..50I1NYE1904s62j4MPPrp6Y9zo95jY9V70Vy7328650BvT3oG0t1O61qv7e5kF2UE8Y69Uk64K8..88K8S5t7L856pLDI4099g6363g9r5YN0F03T61P72F59WdNvc539Ce10O3WxP2673x20189dJdxGuO1Qk..AW9AWok02Fp3Flb06gH5022U0S65bu8nIo4fXYA6U5a7750s60oK3GQcx484I6DEP959963m825754m9077u8Z70M3YZ590Ri1g43U599i7QNxll1K3W175N1JJ70O7m22r6CW1h15662S8y..

C:\Users\user\AppData\Roaming\98025414\csmggk.xls	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	564

C:\Users\user\AppData\Roaming\98025414\csmggk.xls	
Entropy (8bit):	5.520444876236276
Encrypted:	false
SSDEEP:	12:GeetdQLf3qr2jDzG0dNaYahIXZzc/a6M7YVu+LZq:GOWGDzGcQ/hIXZzc/a684u0Zq
MD5:	4638BA44BC318D643950700C106EC3F4
SHA1:	029AE95014C50F9C719238FDF6023B5F154F2697
SHA-256:	319C18E5DCDE9660C5E8DE43361E0ADC7B69893390F4FFB62E651F7542341C63
SHA-512:	C51B81BBE87BC1EE66D577E43BCFB90F55A8610373D3BF1EBF131DF8A52E5D57259C56B42F9B14F976A136527C137DDFE1D613951E8D6AF028FD18640C7786D
Malicious:	false
Reputation:	unknown
Preview:	03231T8..5KyXClC4A1f2y1626..g9n73EomHy12jy8c4Bq8At6n27110dEs9LhtOG1v454p02721938Ew4559o6CV08R0u5NJ127nSnz3C62bT0XAmFlI43MCh56jl69R OY04x82RR98608589Y74b1M3v985Yf70xu1r4a9T89i68Yrs3BFy..B17VBO9D10nWE4OO220whYO705G97359Cf77NZuUFp8d5JGf3R7AlQ83k9e6Sw7Fe46x1dt6PH2n VkVLQNK777lcRR1tFg6k0R6Uhj0JL0609FIP3e5xDrnR1N9368Y0ZEl347713b8ks42o98..w7FAkk08sj396OyC159JMdAm0370kj5d9ka03764x4ST..V0T4227L8k7S 6..r8Oa64DmG92l87aqG7N2I3gpM6S2B9b106AU10q2129phi573Tz94b9rH7O536NJ8S4sF62444uTH1G8586g7IrQ060YT0aRz70M48X1H8f9681AtntL7q19HVyx5Lj QLN21y2Mox716z2n0g77Oh55RA54Q3v8z9hh2622Z7..

C:\Users\user\AppData\Roaming\98025414\ctifihmq.xml	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	527
Entropy (8bit):	5.474619117448956
Encrypted:	false
SSDEEP:	12:P6iG6mBbUy9I1vv11i77MNH3JRVRYttyHYZRX2oyp5Lo2MwZ0:P6J5Uy9I1v907MN5RVRYby4PupenwZ0
MD5:	9942C89348AE4E9E2B8E2AF6FCA87877
SHA1:	3034AED7F77A1CF65D3BE80AD3CD027BB45C2E3C
SHA-256:	5C43BFFCA850084A560A387DE5B9CEABFBCE925885CC2B4D862F1CF11B486009
SHA-512:	232B73D9BA7D2AEA9E40B3B4748FDE5F7CD72BF18FDACE72DF97C95F179F1682D531A957EBD7A026FC4033887312CD039D09C604EB28E644B9376E75282956E
Malicious:	false
Reputation:	unknown
Preview:	68hoS4b7CAM3gj68006r490n54UmSO4B52eBh4Ym6qy8605i2241Y906HV4LJ0H5p0768E5N18F6bT2618m2S72420xQdK1qG1d067LX1pqY748XZxr56AR57ZP28pZ6.. 9m238r48d1T0D0863fu4e152856aC3R930v..44150t7z80xs4t88XHw899Fv31705rvVJC74jC8r08yL79330w3cN1A987DsE746..AewA7S7W6J188XV9J49D..BFGY9 666LEAg5k6I7lvC45w3M14B..12ypq93LCYOE7b2273841J7u8yFQ28Ib6w4bGuM9bB5Hw67KSJ98775k2lXwRc91Op24hb76q4k7Sc8173paE2SgKAe1V0OMhG5g960Ab J75I..A6537PCoJMu55YNG2P24E19Kat1o03l0q60U65752a4780Zq9vO95F44l6Va98NcgFSi87t41NcMDJ9276QL4y2009..kXAJ79baw1s443r0efs4J3lO12xnil6DU048X..

C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	139971984
Entropy (8bit):	7.061995429082689
Encrypted:	false
SSDEEP:	98304:6l5lllNlqlgluIhlhl+lJlhlTlOl+l4lCl2l1l4lclDlXlql1l/lLl4lhlklJluq:i
MD5:	88A7B78373EEDC7C838AB5ADE9628B9D
SHA1:	122A17B6E6E9FD2EEB875CABBE673A0886BA67BE
SHA-256:	B10B2A020300A668E155CAAAB629532793C4D0FEBE401B4B71B05025DFFC2C1E
SHA-512:	96D3C826353048F3F32AB9646A227E6E9B27EE879FF963587CB8D50C25423EEA2E9AA8B824C642E08F7B6886856E7E858D81392D116838E0E675FE8ABC941BC6
Malicious:	false
Reputation:	unknown
Preview:	..;.n.;...j.....2S*!..[.si.....}.....YEJ.....zw..r3=..\A.."....Yw<.Z..$.....h`..;.K...G.=.....#.c.s....'J..q.....D.@hPm.....9.O.3.T.e.2.5.F.3.3.9.0.J.5.j.y.s.1.3.T.l.S.4.l.7.f.0.9.Y.u.o.8.....C .o.!d.._nK.-.zW.....tX.b2..w., ...?.!.@`....c.QlZv..}.u4.....qf....P.W..)}.:.(."8..hEQ....H=..9..q>".@..A.....I.7.t.2.1.4.0.3.9.C.f.3.N.2.7.0.O.9.8.8.6.j.5.c.Y.....>.v.b]i...A\.'4y.M_..... <.....9...B^...V.....W..\&.....U...2c~.qFY.\...E...}..4..}.U&....`.32D.....%.Y>...:.bWs...7...i..Km..Y.h..L0..f....Q.7.6.3.2.0.X.n.4.4.w.y.9.R.5.O.9.5.t.g.w.n.5.g.n.1.z.V.7.7. G.3.s.A.R.3.M.9.z.5.2.Y.....(G..5A'....H.p..#..QE.\.l.?.....N.?.*h...r.]:...<.[....nj..@.J...;D7.....z.....a....u?.N.#p,.Y.....r.=.....jg.}(...e..0{.e.H..6r.@LP..TLD.~...!.X..i.Q.....9.6 .3.6.P.U.5.X.8.z.0.1.G.1.h.U.r.H.r.Z.9.g.z.8.3.....x.8.R.J.3.6.0.b.b.Y.F.3.g.M.E.D.0.3.k.3.3.2.I.7.M.2.Z.v.....f.8.4.8.Q.m.I.B.3.S.Y.I.P.Q.F.7.6.C.5.5.h.8.8.L.6.0.6.X.8.r.8.2.U.4.L .Z.9.r.m.N.9.7.2.Y...

C:\Users\user\AppData\Roaming\98025414\febjvuw.dat	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	544
Entropy (8bit):	5.592971064447333
Encrypted:	false
SSDEEP:	
MD5:	8C28CAE7D76A0E9BA170B1D8A07CB3A2
SHA1:	33DF8C30A51652F6F1A3F8D0F7F31DED7D5AC4DF
SHA-256:	5DA6F6FA8CAC485E57FB44DA5F118B591F11911C2C2155255D7D16A23D9A8507

C:\Users\user\AppData\Roaming\98025414\febjvuw.dat	
SHA-512:	00C2E88A73D5FCA0D8997200160DE7E73195CB3D8EB9D81638968EEB7D7C3E28D854A77A92723E70BC8DD6D84A083B005AA9D6903CA2EBED9D2DA538AECA1C3
Malicious:	false
Reputation:	unknown
Preview:	8Q3X227q2657f721b1x0c1Nctbl2wD8101VU1i7yaCnB8fX842905YkkUG8HjG56Uhh16j6817W4T9d9R7Z31g2FBUtA9r..49ig826B4CQ4o80437Z086067H1B9I8D996fBo0M610..9p9yaGoq359bBLi6sekeT4Fk4s3FUT55x7zp1dWzQd22t5OJu5A84136DCQ2KQx4Me7218yEw8qw7D5WD57K9Kv6D1t0f75JW1z972v..5569A508JZGLYj3y2zw16s312Oegt47o818n212b81782O13oV09iLq63zhh9zM2J47FV679836v997RG104eK70mcj..iN87X3DH0..0va2qNWG865Eu7Pr5rYdnQf4Z9Q6S6ZxR0TeTL44X03629RN2yhwz43G6x0Y4425..oe6Sokn36pV0nz0567..0zg3B60d2oKD2I88OcfO9AvE5SY06Wy0e3..888tpptSJXx4fNhTHma1Av1Yc7l0R794i872e94w80Eehne9dk3QIDJbgB1rnf3X72rPPa..

C:\Users\user\AppData\Roaming\98025414\hdokdhg.xls	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	553
Entropy (8bit):	5.43819133165135
Encrypted:	false
SSDEEP:	
MD5:	F854254AE5B91A5EE6860E6606E4ABDD
SHA1:	3AD12991CF1063EA3FBBE52DE491A22F533F454C
SHA-256:	887EFCC748AE6203142D47A31680FEBA0BA35837F57B2278C467169DFAED7201
SHA-512:	21FF7D5710C27905DCFF1BB49006469F80A52E604A32F01B38AA1933FDD4A6B6974ED1C7F66A319761F8AC2BE06B9C20FE32ECD077B693BACB83BD5E3E1B0575
Malicious:	false
Reputation:	unknown
Preview:	T4cuB54w1V16U54m3v4gQ6F3pF24088zo5390j339J8HG7y246fD0t33yFNd25g6BQ36wBCO8SjwOi13JXf37456v83c90N287xsVa6tD42289o..I2W9h6v9RjJ0b94ZWIsUDdV461mR0285jY71w37206E9t6i59h442z9s2205s1F26BJM8h45LI3q7..aJ2U620iZHr81856z4j54yt2249c5pmHO3k1169gR8nr9d469fy05rA306YO37Q35n73ijv7m7q0n2W7nNC03Ex1I5crJ7bC3dY8maa9c3..404W0E72fqSQ5wg42ZGO5a6zM5f6l6O2192Ke69OQ971o6EXiw4..2j8018FJz22ga5VG039C55D3qj30dLm08K4w153k685sl3vgLgA85959268k3rO98..u0s3IT4625bcf405s1pau5E57H5Y78I56UErG8rS0Mhk8YpN4YJ57twi0894677wI22231Yvn6u0jIMAl1g2V0FpT16h48a132769C643755403B7b4Z0S7FCm6M2w50z5L..

C:\Users\user\AppData\Roaming\98025414\htlvxqr.xls	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	5.474360030920562
Encrypted:	false
SSDEEP:	
MD5:	69746D70CF5A58B5414006066932B19F
SHA1:	9CA236FD260ABD86017FEA81A8DD119D4C27E55C
SHA-256:	C25254FCC6420125C8953BF723B0ABC03B45DB22F23B687FC561C42569E75E59
SHA-512:	26F2C98B5AE5D6848476E9F5D085E2BFF38B20849FF7A26022FE0E51F7670210A8C68D1990BF82642CB7D3224A3AFD5DADA5FDA15A0EEFCF2622E6EE2F36E9E1
Malicious:	false
Reputation:	unknown
Preview:	85lJ4D3U9r1igqB7yTL8s9y8G5kCYWNX47Prrr68Ye6199072eN4i7jtr25E9440AM3d02h9909Fu4..rm5w84d49..Q8n3cm88PltXrmzP04im3y738F372L3Bgm87F01hwn08xH17d12w699ws9uG2B0p4OpXpMR8..1L1068T2883Q7a33Z7ouE31c89r1ScY8324L8Q04q57iU59wr783F09BgH9..2qW8mGTj..N82048Y6pU8g6by8838N223Z51S73P1k2n5r1aRfT170lmvN6Yjl04..ki79SCPa9766387486lcgtce8w9P8Us8A5H49Fc2l8koskx5a3Y71EnI494G21tl1Bq7XLWdVY64eYy8ruB3Im216F7Bc3dUFJ..ssr4zV88nWnNa7Zs357Jp468W840iu8M1w2007r58ej87R360E2472e994o83lPCx80XROs67b98pwJ4h2b5aRf2B52s11A2Ca5B442G4rWCVb4e7X698s3i..

C:\Users\user\AppData\Roaming\98025414\ienaksfo.xml	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.452143550049103
Encrypted:	false
SSDEEP:	
MD5:	330402BEFCAD78C4ACB9EB5BFEEE5A71
SHA1:	D1A9852684D3263E3EF0958AE1C920101AD5FBE9
SHA-256:	A39F85A348D1825A70FCF20A777330E44370A1824620A631EFFBB3E0CC0C7D88
SHA-512:	4F20C7D60E82CA6C5C6AF99148093A7285FF669D2A69791A3A72C9F3F4EB22EC7944A7EFEA714C4EFF9DA9978BB7F77A3B00FD6A2A1005DA117A7C037362A07B
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\98025414\ienaksfo.xml	
Preview:	4804819fqjpwmi2402C66495Tc0Sg81q390V1jF57aIap1h1870QFlXA4OK5I2dQqM090559a3W01iZ4972Hj199O28iJBY96Ol711n0F92V4wg0Oz86pji3O3Q21y6KG1 2aS8W408w35J1602A5ELGo1..3g5F3z25A739CD3ZW7nS87rz9wgq0D9SE05pB4915u..6q179wk36i5bG6U3971I2svw555D5tTAc1bN1Xexk46o68bk7V2MSs63wgNmR 893q399TS27wX35Lt700989k1za1438E794d53J6m982XA5499e6U2f908mG27gAA672edb4hp6Oe0tC38Ac491X22Q..2SV24..ojs5vvkJO61iXx7AAP5hRzcE9hAB8J Aj10BB776QP36a7Z1t9bLY98..46w0917q99Q7k06H0Q9sfp2j284Zo6538L49Uc58BuWwe0iB5A94u6OK8ldLCX11M73S96937vsz52ez6xAdORxN333b55uG0h09H0N3 Ku4ko0625599B0N6RK3s18j913V..

C:\Users\user\AppData\Roaming\98025414\iiaowrwd.dll	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.439584995584582
Encrypted:	false
SSDEEP:	
MD5:	0E1695E9123308A70A62DF019A5515EC
SHA1:	C9D8F2E76CA90D07715B82CC68F0B2A693459B5B
SHA-256:	699DBC802FE6C8C549E2410FC559E2452A95E53DF83D8E1E2E5B2D44BC362521
SHA-512:	E0E1F3E22FEE85D2F6B5DBB4A12A0EF03C9F1FEC2EE217F1C166303665A7712DB986EDE8A885BE9B5C1FFFA0A0F19E46F9BDE3EA044C4108EE78B5D020A8AD52
Malicious:	false
Reputation:	unknown
Preview:	s71Y13FT2T88zWd9o5Y95h75xsXDB01lEs908P53efs104C76B477Ut14529xvvww3J1FE4A6..dc08k2g8396kS05j29qDwh78dhLTr9VD6X5333dJX4P2ZOk03Du6pQ5 86o4so9y0W8a74Y6EMkf3yhDZKM424V5584441bA859i04903GRAPp538pG4S9k0737P68k9aO8D45996v5py47S9S9mr0hd79ejEE7y04M78Pyb4W2xvfT35..88oa3x9 G1Kx73m9V1q239Q9848y41420662176ao3Xl3S2ns01pNV0779Zev1F2uL15..7B8219K0alWV7czsf9R7qw2020S3359Z7AAlCBu56j0fL57vH331N55636P69bl18Y91 83OF5x8JB0t5Pu7B40695480..0C1v07mrsB3px547N2492Qga2B2ha480hx1rXqmn07eu35H0iC14n5037A80f636qdcgI1tGY3z16E675k70b316Txv8FD8C3fFu181x sE1b53yl771Y3J68a1pv7A6i6Ytw8150qync..

C:\Users\user\AppData\Roaming\98025414\jbsuoiq.pdf	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.47056014552393
Encrypted:	false
SSDEEP:	
MD5:	92A265C207FDACF9957288342633A912
SHA1:	EDF7EE5A544ED5C5A9645FF24BE9EEA56C1EDB6B
SHA-256:	BAC80E516FC686F9A2B51EABA2D7A5BAAA5C224F2EEAC6C973B5A1754859739D
SHA-512:	8DE85E2241BC6F5AA66403FAA58AB46096186FC89ED0A181774B58C0FD75461D864FC803ADF7F76224AECC85DA9633DCB1EC531D8552D9A618D23BE2500394
Malicious:	false
Reputation:	unknown
Preview:	4tC5B43433nb21OLp8z5j10925zFSN..t968ZOn0802xT11RVv68Kyr8bf1E5fh450d595Ul9sC1NYazA419Kb4xB6H5UV4U2Oe68w93VJ323yin1jo7iTj..O787H141x jS9VzkV21p2qV2730871917fAULaO37c3SK4DlA3Da77F51m77037F596NPjI9bF7..58A37vi700s1c6421UuU342PKM6hh36Cn8446T4d3028Y6TuW87K4Tfx5wT..45 D5a50w4a47W051N28A18Rp2q9j99jXDtbm7972a4l1Jj28R6foTR..9ES2Ad..a79P6OV9729f5k34V93059329fBG7wZgR4A66OW2G3m4vpRc88T63xoZ7d4Cd385v744 1I6w9W4BzXm5xmB7Jg3A4H3On7U59f953Q3qq10KX42P2a9..N353IS67dg6383P0ZyV988405g1sJ7hS388C4Xf5y45IZG9n3b1DsL90n61FPxjX7p30z9Le2T020BmZw L2894T380HgPIP82TK5..

C:\Users\user\AppData\Roaming\98025414\lbclgn.bin	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.354414729209349
Encrypted:	false
SSDEEP:	
MD5:	4C3F53A6ABA2D6FB46A65026D303EC8E
SHA1:	7404F51E971E8F1646AE90973037B586FB52851C
SHA-256:	66A7B8FEC97B40D1B088A17094A8088A32FBBEE9B617CC6CB1E5E0346BF63ECE
SHA-512:	70D0486B33988DDDAB43C4611EB814E7D418ACDB67C8D1F843718C17F9A618169F45CB4816CF52B0DCA2236DE59473FB3168AF9DBD9DCFD6F64082B20823115
Malicious:	false
Reputation:	unknown
Preview:	067TG2LBz4766iJ903E922P9yu51I4J6xE21m52i0578P77TN0Y39e98X06Y6Dh12wR986R0J0367p386E6l891V86u2R20tg0685Xx39806eqU5..93v14ndtH6cBz6q9 bzM3MgpV70ZssN9645X5Yy3BQRmmq7449vt33N5PuXgu2R1bZ405YIvol8100J46075m..7Y3b1791o2e6ro7539F8511O0613W0H14833i56sTw9B54cP3010NtoW14b0 Ml1owg2H5Ftu59EemdT57O2948v013XRtw15535E46GBM1p73m5e357j1cPYF9oqNPc8PqJ4E..lH9SSdqHeNo6Mn111Hi8i6x52F87Ds60N3Yr47126J14NvV12lmyJS0 1C0Tn73G0a61X3N80216R286dhmB1..6b47533Qc5D223403wu3Sp1TQ274F85B36o2E39GYp1hF5828JVop888x2B347S01n1U60875j84..Gm998BGLlV60BqzZ08K02 b5I86x117E1KLt2l751t3X8193tSj..

C:\Users\user\AppData\Roaming\98025414\mjvxdifm.dll	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	526
Entropy (8bit):	5.50043966440634
Encrypted:	false
SSDEEP:	
MD5:	133CBAC508BBF9665C26D4E6DA1B286D
SHA1:	A5333069551B4B2C95D3BDFC804D45012975C0BD
SHA-256:	F117C0903111C6DF6583D8FB5CD054CD6100047201B54FD004F94B24250DCE9E
SHA-512:	0DDF80DEC2CED7DFB7032341649B5040BE4DD67FC9FF380709AB210F5FE41CA6C9CF23AC88ED479FC6B2020B68D26FEB976B7794AECA986180E623F4EA803E6E
Malicious:	false
Reputation:	unknown
Preview:	0K464Gns2FwCmt04Ps72X1731FcPM8N0DK5KWZlS33U0729a65nOg928WaDFV59gnQ1u6LS2CEdz63EQQvCM38CWxc56i0Oozy2A5ghAOzm87k071d..q7o0 267..90dUn1F6s5YO7W1G958054663q65z740S640h748HZ646e787yU175dl3I99O5Qm8P53Va5x510K3cF554U1AR4IAKMe1CW4Qc46J6606p7n8U2N2BE GP801N1l4O550d1tA247E3Neq538D..0g95pq9XWv58b23S1w4akZix80dc268h8ruX4S13Y37tM31nA7633I08Y90381..0839wRlc8T174Qu1s6E1k599077bvz9T86v 6q4268B8Col77PQ2L5CneAEa2EP19bN69t33i5EU4z38bx798Fg92qJtoZ3m05yQN8I2D..hQ44E81Hc481wHiL9WXj0su978TQjUweKHbA8gRkKWD4t66E00E14bT98wI 524404UY0sV99EN3k7872q0h..

C:\Users\user\AppData\Roaming\98025414\natddbtsa.jpg	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.4231692739732225
Encrypted:	false
SSDEEP:	
MD5:	B8BBDBD611FDB5DBA061770CBECAD795
SHA1:	AF6D610EF38F4B7D33CE5409D8917C9201E3DF74
SHA-256:	92C040F48196F6F6C690520365489C97CCC269A67BE0318F1FC4BD9F42BE9AC1
SHA-512:	E82C35BFB1100D785C0443E28AFE2C8ED4906339B0BF80F465BE88EFB6FF9F02334FD778C29D34DB196A26D7C07E632145E5B8CF6410B8B0F58725C2CB5AB46
Malicious:	false
Reputation:	unknown
Preview:	16A37CTF4M40IP2h677Xlup9v5oZVo0w16OXA5q9798PVRW1911K0STTw35xM7h1vGX895c51054V4w19buNA9N1u58S1x5985bU93c9WRPk89HK2W03h639 797xv6dDnp575U5r4Gf46252KGD4e5834729315Dk7zn860O3K69L..Uez91P5v0106638VJLP5DMFL87u495HyTlwx4MGg6Q2E6J1678x4ePK7z6E2uw176q6b2E5xkr9 Q94Q22654II94U09tZ01u651H27S5l4G8gz8iOWxV3yh8k5JQ4790..E0E5FM6p019j915E2qc053i60w8WJkM74Q348qiR34X6DGx8O5hZ46038Gf2N677..08f73gA50 UV67lR2xH2V02n1112ZE6pKe49D1z0wP4xcWl0832lHrP91FT5MLg..1LVjN288TA6LdZ5M01mX9F7lzIDZ37fKEY0f139KqwA373Jr6577U906q356Kl1AVY9212K51qx g63B06uhbyA8i593DCQSx5v520l..

C:\Users\user\AppData\Roaming\98025414\ntwe.mp3	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.455094475691125
Encrypted:	false
SSDEEP:	
MD5:	A0823581838A89D7D4CCB8622FD92180
SHA1:	DD31E9F5376C4A75854D704A5F5DA734FD75BF07
SHA-256:	3B0A80F0BFF75190CA95F80B60628C72843382E885375360C6E8D955CEA298FD
SHA-512:	6448148DD91F86C31BFADEEA97B71AA7F7463BFCBF29DBE6415A66BA621F1157D4B860E912118B35ACB77B87024A02708FD765DFFEE5F96282D57579948BE18
Malicious:	false
Reputation:	unknown
Preview:	zwL6pRe5875KtrBhS71N4x70RwG72474kW7n0n947X56E65DkRc6WY35PD3cR2740..7M315Z9sWM3J3..42L3bWF5A8990J8vg1ihHKNh52ts21ZoG0em102mP65l2Su5 8CbM10c..L5Ged96hmC22VRG7LF08ClA6fKZT09Al435dk6881b37d89374e1cVG1054hBdPz6Y3m8YVtP3bV30Yn17c7e536f2Jb..45x81sZ2F98O2B0J0n10961yD57 8873QO3b57G3K9zq72j9NAI8TU668md53FnbS62Q968d9..43Z1s6U234zOg265H96C67JByIF35Q9B8l2oP15V642i856P5H93d5LL22eXmo80FzR9hAN8..e94Q28N1B 00Y73G9VXi0180lKYa44K2553IIZU6u1e847Z038kF433f390Sr4J975kz37dQ9Pl06HYvK6a05xrq03t..5j5700575O2UOCDD86cb9qE1z6bU97O8E2J9A16245j18jD 4Ir8pOmo9f128P5GZKk96fF7kz0d45D6v40457oo80FA2Iy67957164fQsi674y79A547ep9t3Z9A572E1287L622e75D..

C:\Users\user\AppData\Roaming\98025414\ouvrjba.ppt	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	634
Entropy (8bit):	5.565796365658858

C:\Users\user\AppData\Roaming\98025414\ouvrjba.ppt	
Encrypted:	false
SSDEEP:	
MD5:	D2C08AD9B40C6395904420C7F97242A3
SHA1:	087A9FBDDA0C08802B331172F018B60949E4AAF0
SHA-256:	6FBA2B94D2E47266D6CEDA55469D339D3647322AFC7BE420C8617DEADC3EF115
SHA-512:	2BA4315F61E5B50A24893D217A8EC193564885DEA2E40444EE1B999860828F06F7C0F247E311447C1024DC5FD23F4F5FAE0A5DCB131CAB2038DF0306AE3CA83
Malicious:	false
Reputation:	unknown
Preview:	vEq570C058N4538ZMp815S36I1IE7Da9MD5d93Y41VUg0p4yxGi0ML7e482R..93Xq3qB4OzS3YXd770AVUEu305ivoW8GXesYG0qBT189BeA02U..C9FYIX qb2N94aum5Xb4Yj042iG34zsS0Rvfy7MJJer5..x32sFR22Ds2DK520704Lko9bSlz7w9h06E7E2ymTtP2f16tq85f4zfiBzsk6XM3z039428w4d56f32S5546elYd0531 4TA80e192CTAL65G2PQhM3mt..7799gwbj92oi4g2Z9l6w28081R090e832N0G0g0V9i5pimgnY00X791C53VAl1yk72O1..3jjTZli21311627e2..8ZSVu1f8M9bQ60h 227Gkby1B3Y6ni9HS8gqLW4137UH00Z65OmtB6621A307NGTj6BM21jM638pQEf71S..S4201D5GXh24a5wQ7t45hQ70v6SP28gh0yxIuiIyi2M350s3R259PH40Wy3L46 3f3QCbTxC2ECzf0431Ml3v5T8N2W0QUNYs6S2UWXz40s69Fe02KDS0YTFlu582dEXNTVq9LRZ7p3768Q4U5lyJ1350r51y7j31q3870S5z59aY7c3aC7Ig56X3..

C:\Users\user\AppData\Roaming\98025414\owxpr.pdf	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	56976
Entropy (8bit):	5.579376667471237
Encrypted:	false
SSDEEP:	
MD5:	04A33F4AF4AFF3027A40B095DAD04A99
SHA1:	9387782276CAEEF4B3D43DD9E9C6D3BDF968077D
SHA-256:	1249B35F3978F85E5496EAEB12FAB950BEE9820B42DC84A3B99588B6669DA073
SHA-512:	A4510FAF84E4A57C18EBEEE1A7BD31BCD27B1169FDBE88263583C81C9F9037D3CE2FF9A3EAC6F5B1E881CCCE8265438F9BA458BB7CF164CC841D66CC2A44C FBE
Malicious:	false
Reputation:	unknown
Preview:	A0Zn65j448xdAX3muo530824365sEz1qzY3k0..VUf1555063T8t0505lQ121z70..9sO60OW7211J63r3AWZ6Q8B2sK073MEA96wsPt95i863d4w0414HY45KG81p..h0 LoD5uaKQ9Isy4I5191983X039wJYi5P2P1R47T0C4z19s0lZ4qn99cA8NE676u6l90xZO52684qQW9e7n7160KRr7e..7q48cg0RQu59po5627VibCHaK7qZZn89PglV76 2..9iLr83cdtD7yH1lv230D9C8VA1Kj4NIB6Z9..Cp57baaj431UXw94333g2T3688926i18..y36MJr9510g52TBF21W5X42Q368c7206G226XG7v58K9QvD3Ipg90IkJ 9Z79..36953n2g4pS5b50x61y20H8ge0o0w56180L0tV3E5a5OnS1IYEdEPTcz0YA2u7408666145Zvh915kPv5i3J4g..uY60l7cwH3BR1g75441rhioH8t43I3q03QJ3 fP1JF5927jHNv07..DF13480eSTF62E8zuT4Sq3lAa6a02uqj0Ef1WCTe0701ct4B..HmoAmT7sdbO41wS3EM947s196wRUND7Kz..gA5a1fSwQ7w3wM1r829N15FEz798 73A0E12o8mZ1D6849G5568E8i66m6Y29F52Q9544x6d96Ac..qo929l99G7h0910416SdG..Z045sg7695L631n6EG3TzW7521C9iQ8U08dF3Rzid6978u..6uVQ04e3xS 6bOdJT8y6361P26O7..Y6E40Ml22u2iT9S755134542P93vZa7y4ktj32pOvosEHlY19ta3GoD85026..48g2X6R0l8hH95teT4Cz..181841807AOdh7A5RVN1r003820 H8H..1Y9v3HuRQ2AfMtO3WXh49b42J3WGFS25839072R83g713f3Qdu..01E11Fs2e3Q702bnWl3E0J4628Q18E1B9

C:\Users\user\AppData\Roaming\98025414\pfoqpoutwu.ppt	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	526
Entropy (8bit):	5.484669489916625
Encrypted:	false
SSDEEP:	
MD5:	F5675772D77448A1FBC20304851AA52F
SHA1:	CA6E108FD12EAE6E2913144E2957857691BDCCE4
SHA-256:	DEA7FBB80E83FEF7F62FD1174A2B72507A5B373C57B450E815D1B8465F3C44E6
SHA-512:	14D798FD2AEB6991DE19A28C503A46E0C8DF0D18ABF84B2FEB47E1BFBE5305121111E9A5DD399D83422C04C620CFB01C507C71E876D2878F8018E7158BDEDE A
Malicious:	false
Reputation:	unknown
Preview:	cE1r9020016D2bv8pvje3vl8w9L84xq43k1Q9579..t5blL58xKixE7y5EG6RK8A166Ps9R0m36X0e3wh..aI02FN2c8sbB7Fr139VhRQe5KA547PxrZe557IDf35143Gc 47r2k7aE070QRW4U30072qbrp1j..3GOu94j51..1O3d2B0582a74gB3javkgT4kP7fKR304r2Qi6K3q725w8NK37w..3S34h78J8wx0J5Uj00H..Y2R6lj75vK1k6W8q7 3722I89c196a6Y309A6Hp94I8qH12sa8E..42018399Ow79jf9y2hej8x2..OTPN0hPT51uhY529148..3l8L5548BD3Zho0HnAv52g7hjV48Z11Jp27Fi9LAv80668a6N q57Qz00Z9n2iw0Mp125j9JR9NmFi3T..8l8odFBe4Nn8521s879NXsJt83Br90Uh825735mY18h02QnfTlqpQ2JV4942h2m355jF4do55q1b025sSTY1h2177CPQW14142 vf28..

C:\Users\user\AppData\Roaming\98025414\qustvis.buq	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	430098
Entropy (8bit):	4.000009446322543
Encrypted:	false
SSDEEP:	

C:\Users\user\AppData\Roaming\98025414\qustvis.buq	
MD5:	C1D0F02492CC355266EE04F0F2C17C24
SHA1:	DA8C0302F4877A9B10D263A43E970D8EA7EDF57D
SHA-256:	416505C75142609A8D79C3DC94260CB74942E1731FA1E198855EF8BAEB166D3A
SHA-512:	64E808C1581F5D41879B421447003E32D3CA81B2578E29F2177928E1B4E858310B3C0F202C4BE426275F5FAB5917A592616CAF4090725469C47728E57562E859
Malicious:	false
Reputation:	unknown
Preview:	E23BDBA134B3755E861BC1DD8025A44827D468BA63A752515A0E85D143E6D2D7592A17FEEDBE410E7475D87ADED47D5B1096AC1A6059CDFEC51DB460 7DB991085D6F55AB550177F2759E24CA0E88D20E5885951B88143FB6F19591B314EEA607C4A831647BA5DFD150602DF0E7A1FDDB2A73B0DFB399CFEC 0CAE1597E23EC821B4E56DD99AE57AF5624A498CDB65CA2A8D680A28BEA65BEA381F7053D6F4584356081A6FCA50BB47B2C501682E7A82D2D805A779 0301F82398BF0FB337FBBE696B69CB93445F288973704E01329B5F11A58D328AE8BE2129FFB3ECC875EEDA74804DEBC5E304F4DD0CF4B5225841F788 4FEDC5BCF2FD58B0CB3D9DC78DDE19A5C78DADE9A7368B3845AFB01F152BE9133358F94BCC1B19B3264DD89CE3D14D9355F5D594548B2BB6FD8A3B74 47085B0ED08C366D76DA08DFB388515DF80F5C1D943C9F61468ED607727EC869BE10543516B34FBA3537BAD08D3B68E4609C0169805C2608C9AECEB8 CDF649E8944E73EEF1F0E039F68538922F105D92813E86D171AA36981FF1D2D69B887C52D892A2B4274E1331A45F14C712111C24E34E0E7422935F6E 5014B7FED5D347B46AF13A3EB0864A755815125E8AB4111A327CF2D8E47973F7FED00AAE07AE4172742282BB95E767453D067C7FD7A7C74D77D27ABC E8C0AF4862AD2354339CDDD71EA504CC5246FD37

C:\Users\user\AppData\Roaming\98025414\srajj.xl	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.4555981206233986
Encrypted:	false
SSDEEP:	
MD5:	CF602EDC2787D24922C837094DF1DF90
SHA1:	CA799EABC72026E72EB6103E2899542C8DCCD2F5
SHA-256:	30131414A5B20B89B4CBE48585A63707CAB8EF234DDD489D0545EE80DABC6C65
SHA-512:	870F8AB4D225F54AD92DA6A1CF08555A6BBF8EBAB0A23BA3AFDCC9D192C4035563FF701ABCEC042846E7035173E1DB888460B9EF5351B86E8922A1C76EE22B F7
Malicious:	false
Reputation:	unknown
Preview:	n93Ajd9V4D527CGbDd1527q2DuR749uM397U3a3kFpu1W75phktU4E32EVg097r4Ln326X38Mf8212k5lk5386D689081F8ym08405C5G3Y45B7QG2SCs41J..7jF7PCQ2 GqmQ989MUi5687n796h474Y19q740d139772CFP241ye27U9441988Rx3h27P83fsRHD31..Hn6w295R2sJ309SVED1Qq6c6rFr5kU63CsK751fr3MmB4l0s7m41062286 I93ID5xSl900572tZQD80C6..SKC51Z5WxST7o803gsiAPD75wat9t442fYk18sT3nU1i04vFtQ05q61Y20PC28S8tlyjT4q89ux8PctmIqCk36cgcYX64m8w74S8808iM 8P974i91vRn..10oF72B39J8B3wyuPGIR3f6sqN0xK689QO24143TF96u3p..x1N03L26xj3v8B91OD3127942qDJ59jrQo2O6e562ustD7Za307O3DGD1ju4pPbkab83854..

C:\Users\user\AppData\Roaming\98025414\ukxkuctlug.cpl	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	543
Entropy (8bit):	5.4842104066745705
Encrypted:	false
SSDEEP:	
MD5:	20B1F75F8C77F57AEBE2F0FF9B2CCA4E
SHA1:	FE7C73EFCD0B43EB7338ED5CBB9336A72E695DAA
SHA-256:	C4E306746ADEE64B0696798F25BF5FB7EC810D4D33AA606B74D8DCC7F0FB925D
SHA-512:	9C4BC3C8CA837F4789D6764461CD022B13DF105298CFD8363A8AF9A47AE3C2DB2F422C343EB1C5E0F1E6C8D2D7EF0A62538936282BDDD0989FFA7B4DDF6F7 C7
Malicious:	false
Reputation:	unknown
Preview:	427q203Uo30757k19c5ux..1l51C3541U1Ue3G7R1S2Q6E998S7p0R9T030HzjfVb112F7dp520Wv103lLF9B1LP2Cvx312YS6tRNX4Sc3dS2fOuOaS5V83487hIc22MN4 Sx892rmAY..c6c15J7UQ38tD7Ek8v206y7jW3fi140O065WPZ9DRi7g41BdF9wN6hhkp7W7xv9LS042cCh048HX59533AZ97yeF89463..t3Y389H540908y0Z0bP48Usa y96yCjl6at9873zRRL642nm5qwd21606030d..6PXg9f656gHmv211X5689W12P6497pnCKI52C974dONU9dy426l4EHbWH..GIcQ2y02996hAy028fmSRsj79W0jg031e INV6LT9nY15..1cAk9eJbu5gE41L7Zp4we6xO4003h28Y6A40WW28Urq38x5F515iwu996r57A7hs37e50N260t0L56hJCCv10p..1eQ0uw90884S006N9573U0L5u3R7B 9B003vftu098bXQY7TSk8..

C:\Users\user\AppData\Roaming\98025414\uvixt.docx	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	582
Entropy (8bit):	5.570793472253881
Encrypted:	false
SSDEEP:	
MD5:	E8CB1CC9B7433E8551DB5BA4727FB2BD
SHA1:	8928338BBC9A44E4DEC09437FABFFB970A8DE8C3

C:\Users\user\AppData\Roaming\98025414\uvixt.docx	
SHA-256:	A1AA8322744F441E37FD70A289C8868B532B985074E6EAEBE79DE2B18D8C158C
SHA-512:	3B979A8038DD484B2AD9C073D8CB9614E07AFB1B216E9E70D82E17256EC4BB38970B04BDA90352E848CBC315EECE350E5662199616DB7CE84F05BC03FB0A61E
Malicious:	false
Reputation:	unknown
Preview:	019aMn4Yk42yLqZ8Q41yO58pUxI0tU074E0NT2Q54Zx066PgO..9U56348920ShfLO56iCo14Vi6LS3e2Zu65F8OV2Z35784aH5d0It4Ixz18N5YGsh71kd5H7k9Z4f8WQ 8YB45b9Ja3194O4cvX7x8h5c3B8lvaHs98r6k6Z..8L3UfIWFW500nEf41WY5Bt6643G1XV2AqU4rNuIfeCW1cY2023Wc3qtUzU67J005055E30y743X4rXXTTrmeH3YJi 8Yod916hK8cD12M71FT59RlVQ0lMJzkz595B1hd13jQ56Uf..vAZOp5biL1wL398LSK0696wZP15mA0u3351T357G2v7J4r1sma88F81A90pBUrB55ZQ6Ft96dG5LpdL28 TJJTW257DtLRHZa1q907N2314JGR46..fR8F9KvY2ARb51932696s6589672N5..MD27twO9ib..69LeL5eQU9zT77..70iu041S01D09OzS5Sg5268xhgPu5tSq4d3Y2o 261mZ6W528YMt223Fh044iRXE25rGSnu8899571if36ZBJ15184o6M1g5M7Y..

C:\Users\user\AppData\Roaming\98025414\vcmtqv.bmp	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.4838784565098475
Encrypted:	false
SSDEEP:	
MD5:	832F4C49FB169973E403DF1ED1DCC661
SHA1:	37727A10227528D6532C1C63470B35B3CD30A4DF
SHA-256:	3CA859E061E3A124ABD1202D753E237921D67CDF4A697B9018954A9A740EBCC5
SHA-512:	EE59E5ADFAA8E4271F70314A41781266717EBA24C7DBC0BBE2F625A466C8BF4EAB07CEF84E73F9C288A4A42AAFAB492C4A5C460352507BCB0CE18A2D5E11E21F
Malicious:	false
Reputation:	unknown
Preview:	M451b3HNo0Q8M8958fszU897U202RXQKtM5N286GNu5ZrJ6L35JFdaZ2JI9bq0P6F2x0759i3071n313i2N54vLjFo3cief6IrUoTYDM2pG51K91f069EH86l42i086IPp M6W4IMn69twaBri92h7G085akr4d0o885545h80o61299XH..UH5tw8v11zDh1K628Y5b06H9s9Hi369995Xe93T1y591X9SQ24gFb2yXIeFAI0t091vdIA2e5q..Fm145 E2r19eC47D5zF72C30FGv4Xkw3V5wx520oR0dL5Vd6k29Zqp87u6cYpiASxt25E03Kc66p062412646XXc0QD299803o4SM66rY3044b99d4j02Y..uxE7zZ6Q63MG8Ij2 9IpL2Y91U5U4XUqiKfgElx552cS61o5Mls623293l8c4B14qALv6L63g7WQ5Y9Fv3Z0..H2cq38n23dA436R736624z7nV9t136609Yh5K3v581j4K60opf85N1KiuG4kn 8u2sx97ur5Jdzf9j17c3..

C:\Users\user\AppData\Roaming\98025414\vlgkcgiqnf.icm	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	5.495839634849947
Encrypted:	false
SSDEEP:	
MD5:	64D5CF423451AF267F5E81DDD99D8916
SHA1:	74B07CFA81679B04EBB0D35BF624F507F4E61A5D
SHA-256:	C3B2BC273DF1EE4C3A3912BE250F7117E6489EA97799EC7E85D421FEE5683158
SHA-512:	6A77196CFEDF3E3AB2375460EE6CAFD052EFF0F0030F3E21CA238ABE4EE4DE7BB1B88C1C16808C156A71728E4A50B418C30241B7F63D4CE4F9639AEBE809EF33
Malicious:	false
Reputation:	unknown
Preview:	S73keXb4MhWV39e75s3x452LfWT2u4T00tB5EiF6R38jo289k0k4Y8pk4Uw5qn2497a2M540Jz..612MtO598IGcFo0y9d558772GhO6PHr24Q2Y48w33Mz7932fc74c76 y36oA74Rk3L120w23WI816315566O1PNV502N6Ln494f5KjTb55F637h..0643Ga9NV2IN2Vz66jk858H82552yURFUjm23FJI96jH9m04iaGy55X7..FeWITCl935J1N1 d19qn3Z0q3420314p7Z3r6764..UFE300I48Zv30948Y4vt221s4871NoUL9Y9w3P5499EeIfmRU5LfR27megTLUK18Bc537810M7K46mY57be60VAt8H5..49942ijPk0 49gf812mZ012dLV9jeCIgkFsSZbR0x4Y0O03Fko6o3C6X751YVp8CfL15DPA1P2070080677eJ252YK435eiW6Qj..4iK20..67h06700N2i01ND19A4969686CAMOHLGq PVyry5028D80353aPi69V9j76VPWA57B5Bn710p4F03poJsOIlWth088OQ41j9Y73F5m6J8x9RSEjA2Kq8374999Q7016wnK9Dg48o1lu9lXCxKD8L93153qX02qf880cH dcqH6e1B6a6653jlW2z..

C:\Users\user\AppData\Roaming\98025414\vrmksemwed.exe	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.489232019943575
Encrypted:	false
SSDEEP:	
MD5:	219895927D4CC80B6D14975F461D3404
SHA1:	DDBD21228FC6EFD4E9B13785E5B23F58C491A0F7
SHA-256:	4F70F361AE4100A16FC25DD630145FBC9DA3B81007D861DE4E7DEAF216EF4295
SHA-512:	2858C479987F178F030D60AA92B2B3111ED577EF6AB3817769156DC1FD819D9D6230452BFD6C27E49E133CB47ECE63906832A4C6B94F948D9940D3DFF7B89C77
Malicious:	false

C:\Users\user\AppData\Roaming\98025414\vrmksemwed.exe	
Reputation:	unknown
Preview:	5365578BD7Q3Su0U34xT7974QG526B4fQnA522MCn4V8z61t6..p4sfQo839542ca6Ytz95073961SrIIz8N775..0W1c9YTBo4gaESAQ54WU7110731d1l3T2AO06T69f o29gl5B2X7f2M8Idi5LhvtnYG038Y9y0X9qE172b1..h82KVs4Oh3tD77V51Ja6P2E51SZ1020L7q900wt25N26a919417Mnkg6r23h3LbD6LBU39w50..ZjaVfMmOaf80 hcj7HNrWTRJ0Ig2Hekvv0SH0..0tDcd2126RCf289ihe0466a56369rX7V713K6R5P2695T64n27FxnB8W4N09zewax4J367bDoPltP2f45y91E1g4aU03f3K4cuU3nz34 Om19js210G910X23..1u9I4t78G8hVq48W4I55f54K05RnXeb7875741K76R50de7y286522RVuG81I9H4yLW64383z5pK48c2l993C2Ap479..

C:\Users\user\AppData\Roaming\98025414\vrxipgjwdt.bmp	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.456361205166428
Encrypted:	false
SSDEEP:	
MD5:	F44351B6BD604752BC14594FA4F52AD7
SHA1:	517F43BBBC91A655486C2E5722C92531E5B0EF50
SHA-256:	73D4587E93D12CBDF2A50E9C025B61D32390D0313F150C816CF7BB05C1E0BF09
SHA-512:	A160784736AC0257CD4154922FA572E2D5877835B89A6895FF11320D3D74DEAB4135DC90EE23FF762701FC86D86AC615D283747C2959357D358C9022CEE40D4A
Malicious:	false
Reputation:	unknown
Preview:	8Eo5Qp0K7KC37U5HtS3PnpdmC2D4yb831j5d95036M9o0KVL4T39arHM1ya1n58a2613FPe109X9161LY0OV9Gat41Eo0d8mTm6if06YbA40..deDfMq32542u9b24nGyz 541d77Y4p9847ydM3TWf4K..3tUkx0MgT39pyNO13792ug26yvPEDsa095KxV9Al3b3tl45157j26C..g86drBI95Db18IO689Q719U7s8960D83BKqHsWC340DWawb851 6u1b339566925ybEUy0BJt840o6YM57H52oH04M4O2188259q8M0ay89316fWVai33Qy8B4ify0dz7M50H0fzukJM0435b3l..22985vN2J4oH42fP5s770V6568r2r59R 502P5vv9787..39436cw2OD6k34688V3Qtf858ZcM859x0728xVe7803g1WcTLUi0cji7y4LMKFR648h59l9350SpJrj05BFC8w340K5M5wMfesD..

C:\Users\user\AppData\Roaming\98025414\vtvpu.log	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.503797988329663
Encrypted:	false
SSDEEP:	
MD5:	E0D2C5AD21C810301A3136E0157E6DD6
SHA1:	9BFF387143948E49D09D8BF252BBC5694FDB9D1E
SHA-256:	2168C5FDF28545AE869775600825C77EF04BFE80F658CC1255224D58129FA051
SHA-512:	E03508B3282075D70B95858A0475361CBAC93F6A644B0B155C74E25239D33C699195EFFC22CA3E6B682E7163269439263210FA8494CC16315EE92787951BA37D
Malicious:	false
Reputation:	unknown
Preview:	1F563i6R1W9R7D324..K173e99x9i8X6A59ZZqp3..Pzq5pCGQNT2m2a7x2RUl0Z2ET67N57S9M8njW63240r..3442Ed9kh02MT40Qk3714vOL38n4k4pzt70613WvzXT p10V377U15z5yBNZDI17Nq0x7k58xvc3A78zC16j05x7P586K93I..D3287S4W43k27vQ11zOockjBPg9qzFlG4NucpTuRJO39hy89M718tScNh5242F0nEn1N82wZma34 WElX4C1ZHKc0lv79K4N6c..BUiG5GN571301VI7R9ca03o7F1132Z9oKKzVbW62u4h43900jS94565038wLL99T5694ccN5A7iwY61qzU68t5E6x87150F..2i2xFZP215 f32A1Gz9o8N836f9r55K..i6YXdwVA7Dq4ggbfpQM7q007L2P3D73X5Y9P3CQO7WR0904A39WN51d157Wx714xNq256vvE1714yIs551w8co3f..

C:\Users\user\AppData\Roaming\98025414\wqpf.dll	
Process:	C:\Users\user\Desktop\ameHrrFwNp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.444720181233763
Encrypted:	false
SSDEEP:	
MD5:	344250623AC0BA8B7225B5D6A90F3724
SHA1:	A1C3AEBCE08F3F950FF0FC7834897D7E18944C4B
SHA-256:	41B6EBEF5FFF31F33DBBCD71B34ED67443D6B2E9A1AB483D2D6F21925FA9E34A
SHA-512:	0E2C7E81F9A54197805723D3DAD2057BB5607E3EBBBE290651C773F820CA0657696DEBF8F92FD7EB8AF2A6D74D3332B8DF79587671805C50C24D372A7538E101
Malicious:	false
Reputation:	unknown
Preview:	9C74ey5wL32uaD08017685v8uGqZtRI0e04F229T4Q662V5IFrr559s0363UBKaQE2CZt0j89482366fs455r9r1n7d18lV89i9q6K59m1DB79MrAs0O72vrU7l86J88lO 1CH92ga4q1..kMH7cdk38nb0Sve967WGbJ4i04EiUW105e80F71vAKA..01095f8rZ9i36K833S7552z7W4Ia3FdS6x973Y5qMTglhhrdykXTPx2q1IX0ly1pbLFnH66u9 Nc622G3tdC336208B1Oa9Ng7z0a423607154JYoxUcaU..S1318227f..9V72M33yB24me61794HsX1Uwn528f554..0H9R523cTOBG0804UW48a2057Vch3..eq98keW9 7G7424hZsuXO6QrE2epSt178nEo60F7B7H919564LO0fx9q3cl83M0567Y5u80L4Kf3687RRN2sy584j6074Ym..Q7O6g032q6lI..9M75t31tt8qk18841387936JSY03 JH6K076e8Fec311y891S5w2mt18F08i19455dQ6445EU0119K19Eg9FI49489J86637..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	BD8766BA1722A2A636D519BB2B64FC26
SHA1:	48F583F5ADE38ADC3E34A726F9AD3EFF6B3C7BF8
SHA-256:	FF3B6D253DCE757D1D4C4EFBB47322BE3FE9E9DC4F383AFBF6ED320F4355ECDB
SHA-512:	7D606ACBD66C7305B53A88762CEACEAEEC5E49875FCD7816E2DC7476110E015A5EC94586BA407E30604BF739EF7896FB1437E864E4F9623984B89EE8DC763BF2
Malicious:	**true**
Reputation:	unknown
Preview:	.*..}..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.4112044189276585
Encrypted:	false
SSDEEP:	
MD5:	4879007AC97C3DF41896D937852ABBE7
SHA1:	05A8C8638A4C8157216EF4AE24B43D3A4E750F00
SHA-256:	18B03E2D9F5F5E7E26686848D71049AC56D06500A2AB420A3A01CA0ED6C7AD18
SHA-512:	03C80EC22591301B32EB0310A188B1C4C24DC16BF9E2E25B22A95AA6E36E9B7002196B13A522F36D9AC64C38A98D6BA06C3387DBBE7CB3319E45BC43359A6C3
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\owxpr.pdf	
Process:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	81
Entropy (8bit):	5.107152824712226
Encrypted:	false
SSDEEP:	
MD5:	980CF6AB3F834CAADC71AFDC5FE23036
SHA1:	9D30B5465D73385F2D8D26D0D8AFD928F8F499DC
SHA-256:	949B481B9C161702F6A85DFA8646C9BCB465935BE68FC5DACA072205A3057C46
SHA-512:	114132750DE9BF5F4AF871D4A72D41115A7DBBA4964B2376B6BD3B6FC8C5224A93AD506E419EC903844AA48C86E41C7882FF6CD2C3E79C9C75E8E1CA8E77326
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%appdata%..Key=Chrome..Dir3ctory=98025414..ExE_c=bspmflqee.pif..

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false

\Device\ConDrv	
Reputation:	unknown
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.829741962910898
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ameHrrFwNp.exe
File size:	1068179
MD5:	1f221e6e2a07d553e3fcf5bdb5874b2e
SHA1:	0cd7541409f63dda3781d18c61bdcd74782192e6
SHA256:	2d2f62269797be7ef763ac2da37e4c190381cfba8798e92e73ee9aa2084386f1
SHA512:	6ba7d89395d226a8d11ade5be491d5d98ab7d64c4d27d8ccab284bbdd007bb9d97cd13c21010d2f54a05c75da7af349c79ddd00f16671016daaa5c4da1b6be63
SSDEEP:	24576:rAOcZEh4lkCwJlOZIafXiba6TPY5I7nT1RMwazk:t6SCuKfXb6c5IzTXM7I
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y..,.../y..#...&...,...._.....'.....f.'...._..'..

File Icon

Icon Hash:	b491b4ecd336fb5b

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.589268410853	data	6.70021125825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.455030487805	data	5.23888424127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.368272569444	data	3.83993526939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.12166381533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x4c28	0x4e00	False	0.602263621795	data	6.36874241417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x67000	0x210c	0x2200	False	0.786534926471	data	6.61038519378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-12:16:31.658754	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52130	8.8.8.8	192.168.2.3
10/13/21-12:17:07.382116	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50728	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:16:31.639177084 CEST	192.168.2.3	8.8.8.8	0xae48	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:16:49.931766033 CEST	192.168.2.3	8.8.8.8	0x6fa	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:07.362140894 CEST	192.168.2.3	8.8.8.8	0x6e23	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:40.308571100 CEST	192.168.2.3	8.8.8.8	0x2318	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:51.160240889 CEST	192.168.2.3	8.8.8.8	0xd40e	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 12:16:31.658754110 CEST	8.8.8.8	192.168.2.3	0xae48	No error (0)	strongodss .ddns.net		197.210.54.24	A (IP address)	IN (0x0001)
Oct 13, 2021 12:16:49.950122118 CEST	8.8.8.8	192.168.2.3	0x6fa	No error (0)	strongodss .ddns.net		197.210.54.24	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:07.382116079 CEST	8.8.8.8	192.168.2.3	0x6e23	No error (0)	strongodss .ddns.net		197.210.54.24	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:40.326713085 CEST	8.8.8.8	192.168.2.3	0x2318	No error (0)	strongodss .ddns.net		197.210.54.24	A (IP address)	IN (0x0001)
Oct 13, 2021 12:17:51.180282116 CEST	8.8.8.8	192.168.2.3	0xd40e	No error (0)	strongodss .ddns.net		197.210.54.24	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ameHrrFwNp.exe PID: 5216 Parent PID: 5092

General

Start time:	12:15:37
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\ameHrrFwNp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ameHrrFwNp.exe'
Imagebase:	0xd70000
File size:	1068179 bytes
MD5 hash:	1F221E6E2A07D553E3FCF5BDB5874B2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: bspmflqee.pif PID: 3836 Parent PID: 5216

General

Start time:	12:16:13
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif' ewdsxu.ije
Imagebase:	0xf90000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386724490.00000000042F6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386483303.0000000004393000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386483303.0000000004393000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386483303.0000000004393000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.384746745.00000000042C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.384746745.00000000042C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.384746745.00000000042C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.387003815.0000000003526000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.387003815.0000000003526000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.387003815.0000000003526000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386831922.000000000435E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386831922.000000000435E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386831922.000000000435E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.384936448.00000000042C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.384936448.00000000042C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.384936448.00000000042C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.384792516.000000000432A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.384792516.000000000432A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.384792516.000000000432A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386582858.000000000432A000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386582858.000000000432A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386582858.000000000432A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.384816077.0000000003526000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.384816077.0000000003526000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.384816077.0000000003526000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.385533357.0000000004393000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.385533357.0000000004393000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.385533357.0000000004393000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386935348.00000000042C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386935348.00000000042C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386935348.00000000042C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.386760974.000000000435E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.386760974.000000000435E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.386760974.000000000435E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.384853009.00000000042F6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.384853009.00000000042F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.384853009.00000000042F6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 32%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 4644 Parent PID: 3836

General

Start time:	12:16:20
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Imagebase:	0xdd0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.572913306.000000000489B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.572913306.000000000489B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.567098678.00000000011A2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.567098678.00000000011A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.567098678.00000000011A2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.570251514.0000000003861000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.574999029.0000000006440000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.574999029.0000000006440000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.575657153.0000000006FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.575657153.0000000006FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.575657153.0000000006FB0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.575569142.0000000006F90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.575569142.0000000006F90000.00000004.00020000.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6764 Parent PID: 4644

General

Start time:	12:16:25
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8F04.tmp'
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4336 Parent PID: 6764

General

Start time:	12:16:25
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2352 Parent PID: 4644

General

Start time:	12:16:26
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp94A3.tmp'
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 2148 Parent PID: 664

General

Start time:	12:16:26
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0x6f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4868 Parent PID: 2352

General

Start time:	12:16:27
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6892 Parent PID: 2148

General

Start time:	12:16:27
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: bspmflqee.pif PID: 1048 Parent PID: 3352

General

Start time:	12:16:27
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
Imagebase:	0xf90000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423204049.0000000004A4A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423204049.0000000004A4A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423204049.0000000004A4A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421938786.0000000004AB4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421938786.0000000004AB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421938786.0000000004AB4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421415700.0000000004A7F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421415700.0000000004A7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421415700.0000000004A7F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423042439.0000000004AE8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423042439.0000000004AE8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423042439.0000000004AE8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423278623.0000000004AB3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423278623.0000000004AB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423278623.0000000004AB3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423077125.0000000004A7F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423077125.0000000004A7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423077125.0000000004A7F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421689539.0000000004A4A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421689539.0000000004A4A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421689539.0000000004A4A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.422088669.0000000004AE8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.422088669.0000000004AE8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.422088669.0000000004AE8000.00000004.00000001.sdmp,

	Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.422141219.0000000004B1C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.422141219.0000000004B1C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.422141219.0000000004B1C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421763189.0000000004A16000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421763189.0000000004A16000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421763189.0000000004A16000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423525061.00000000049E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423525061.00000000049E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423525061.00000000049E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.420907021.0000000004A16000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.420907021.0000000004A16000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.420907021.0000000004A16000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421847119.0000000004A7F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421847119.0000000004A7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421847119.0000000004A7F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.422029126.0000000004AB4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.422029126.0000000004AB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.422029126.0000000004AB4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.423356287.0000000004A16000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.423356287.0000000004A16000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.423356287.0000000004A16000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000003.421567836.00000000049E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000003.421567836.00000000049E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.421567836.00000000049E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: dhcpmon.exe PID: 5076 Parent PID: 664

General

Start time:	12:16:30
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x940000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5096 Parent PID: 5076

General

Start time:	12:16:31
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 7032 Parent PID: 3352

General

Start time:	12:16:35
Start date:	13/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs'
Imagebase:	0x7ff6d16a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: RegSvcs.exe PID: 3560 Parent PID: 1048

General

Start time:	12:16:37
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x100000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.450398182.0000000003B99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.450398182.0000000003B99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.450263245.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.450263245.0000000002B91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.446552957.0000000000502000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.446552957.0000000000502000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.446552957.0000000000502000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 1504 Parent PID: 3352

General

Start time:	12:16:44
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x720000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1376 Parent PID: 1504

General

Start time:	12:16:44
Start date:	13/10/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: bspmflqee.pif PID: 3032 Parent PID: 3352

General

Start time:	12:16:52
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
Imagebase:	0xf90000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.471749969.0000000003E23000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.471749969.0000000003E23000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000003.471749969.0000000003E23000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.468945390.0000000003DEF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.468945390.0000000003DEF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000003.468945390.0000000003DEF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.469891641.0000000003E8C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.469891641.0000000003E8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000003.469891641.0000000003E8C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.469212700.0000000003E24000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.469212700.0000000003E24000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000003.469212700.0000000003E24000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.472098835.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.472098835.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000003.472098835.0000000003D51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.469336157.0000000003E24000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.469336157.0000000003E24000.00000004.00000001.sdmp, Author: Joe Security

- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.469336157.0000000003E24000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.471685199.0000000003DBA000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.471685199.0000000003DBA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.471685199.0000000003DBA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.467883620.0000000003D86000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.467883620.0000000003D86000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.467883620.0000000003D86000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.468798612.0000000003D86000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.468798612.0000000003D86000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.468798612.0000000003D86000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.468698040.0000000003DBA000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.468698040.0000000003DBA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.468698040.0000000003DBA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.469466887.0000000003E58000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.469466887.0000000003E58000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.469466887.0000000003E58000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.468029326.0000000003DEF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.468029326.0000000003DEF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.468029326.0000000003DEF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.471893908.0000000003D86000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.471893908.0000000003D86000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.471893908.0000000003D86000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.471520869.0000000003DEF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.471520869.0000000003DEF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.471520869.0000000003DEF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000003.468116768.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000003.468116768.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000016.00000003.468116768.0000000003D51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: RegSvcs.exe PID: 5572 Parent PID: 3032

General

Start time:	12:16:59
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xf30000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.493660606.0000000003711000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.493660606.0000000003711000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.492519775.0000000001302000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.492519775.0000000001302000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.492519775.0000000001302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.493877285.0000000004719000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.493877285.0000000004719000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: wscript.exe PID: 6664 Parent PID: 3352

General

Start time:	12:17:00
Start date:	13/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs'
Imagebase:	0x7ff6d16a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: bspmflqee.pif PID: 4732 Parent PID: 3352

General

Start time:	12:17:14
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\98025414\bspmflqee.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\98025414\BSPMFL~1.PIF' C:\Users\user\AppData\Roaming\98025414\ewdsxu.ije
Imagebase:	0xf90000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513759179.000000000437C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513759179.000000000437C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513759179.000000000437C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513522579.00000000042DF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513522579.00000000042DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513522579.00000000042DF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513627931.0000000004314000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513627931.0000000004314000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513627931.0000000004314000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513035581.00000000042DF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513035581.00000000042DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513035581.00000000042DF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513434193.0000000004276000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513434193.0000000004276000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513434193.0000000004276000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513576200.0000000004314000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513576200.0000000004314000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513576200.0000000004314000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.516238923.0000000004313000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.516238923.0000000004313000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.516238923.0000000004313000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513192668.00000000042AA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513192668.00000000042AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513192668.00000000042AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.516361406.0000000004276000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.516361406.0000000004276000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.516361406.0000000004276000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513666767.0000000004348000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513666767.0000000004348000.00000004.00000001.sdmp, Author:

	Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513666767.0000000004348000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.516187648.00000000042AA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.516187648.00000000042AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.516187648.00000000042AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.515810065.00000000042DF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.515810065.00000000042DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.515810065.00000000042DF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.516555865.0000000004241000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.516555865.0000000004241000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.516555865.0000000004241000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.513089293.0000000004241000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.513089293.0000000004241000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.513089293.0000000004241000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.512868270.0000000004276000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.512868270.0000000004276000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.512868270.0000000004276000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: RegSvcs.exe PID: 6540 Parent PID: 4732

General

Start time:	12:17:19
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x7ff6ccee0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.539250856.00000000039C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.539250856.00000000039C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.539382391.00000000049C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.539382391.00000000049C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.537091542.0000000001302000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.537091542.0000000001302000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.537091542.0000000001302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: wscript.exe PID: 5104 Parent PID: 3352

General

Start time:	12:17:22
Start date:	13/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\98025414\Update.vbs'
Imagebase:	0x7ff6d16a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis