ID: 500304
Sample Name: dUzAkYsvl8.exe
Cookbook: default.jbs
Time: 22:27:55
Date: 11/10/2021
Version: 33.0.0 White Diamond

Table of Contents

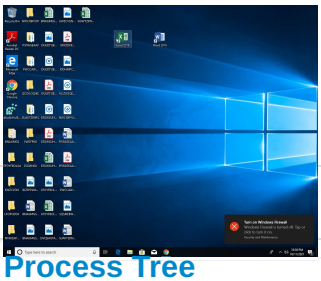
Windows Analysis Report dUzAkYsvl8.exe

Overview

General Information

Sample Name:	dUzAkYsvl8.exe
Analysis ID:	500304
MD5:	9a4a8643db95a8..
SHA1:	c6beb75cbc168f9..
SHA256:	b4e2d864ec0394..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

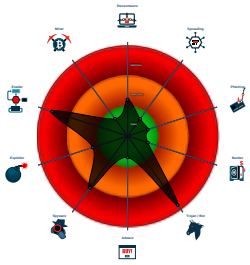
Nanocore

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
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Connects to many ports of the same…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- dUzAkYsvl8.exe (PID: 6428 cmdline: 'C:\Users\user\Desktop\dUzAkYsvl8.exe' MD5: 9A4A8643DB95A8C0FE52AF8675A5D1B1)
  - cjlaro.pif (PID: 5028 cmdline: 'C:\Users\user\77066510\cjlaro.pif' txoxpdjc.qnr MD5: 279DAE7236F5F2488A4BACDE6027F730)
    - RegSvcs.exe (PID: 6364 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 5252 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp1EC2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 1240 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2720.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cjlaro.pif (PID: 2132 cmdline: 'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr MD5: 279DAE7236F5F2488A4BACDE6027F730)
- RegSvcs.exe (PID: 6748 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6836 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cjlaro.pif (PID: 7152 cmdline: 'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr MD5: 279DAE7236F5F2488A4BACDE6027F730)
  - RegSvcs.exe (PID: 3676 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 3460 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\77066510\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - cjlaro.pif (PID: 3016 cmdline: 'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr MD5: 279DAE7236F5F2488A4BACDE6027F730)
  - cjlaro.pif (PID: 4504 cmdline: 'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr MD5: 279DAE7236F5F2488A4BACDE6027F730)
    - RegSvcs.exe (PID: 4968 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 4580 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.560410383.000000000611 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000005.00000002.560410383.000000000611 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000001B.00000003.383284019.000000000478 A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xfddd:$x1: NanoCore.ClientPluginHost • 0xfe1a:$x2: IClientNetworkHost • 0x1394d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001B.00000003.383284019.000000000478 A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001B.00000003.383284019.000000000478 A000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfb45:$a: NanoCore • 0xfb55:$a: NanoCore • 0xfd89:$a: NanoCore • 0xfd9d:$a: NanoCore • 0xfddd:$a: NanoCore • 0xfba4:$b: ClientPlugin • 0xfda6:$b: ClientPlugin • 0xfde6:$b: ClientPlugin • 0xfccb:$c: ProjectData • 0x106d2:$d: DESCrypto • 0x1809e:$e: KeepAlive • 0x1608c:$g: LogClientMessage • 0x12287:$i: get_Connected • 0x10a08:$j: #=q • 0x10a38:$j: #=q • 0x10a54:$j: #=q • 0x10a84:$j: #=q • 0x10aa0:$j: #=q • 0x10abc:$j: #=q • 0x10aec:$j: #=q • 0x10b08:$j: #=q
Click to see the 180 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.2a67f10.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40a6:$x1: NanoCore.ClientPluginHost
5.2.RegSvcs.exe.2a67f10.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x40a6:$x2: NanoCore.ClientPluginHost • 0x4184:$s4: PipeCreated • 0x40c0:$s5: IClientLoggingHost
5.2.RegSvcs.exe.3a807ce.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
5.2.RegSvcs.exe.3a807ce.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
20.3.cjlaro.pif.48ce458.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 118 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 submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning 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:

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

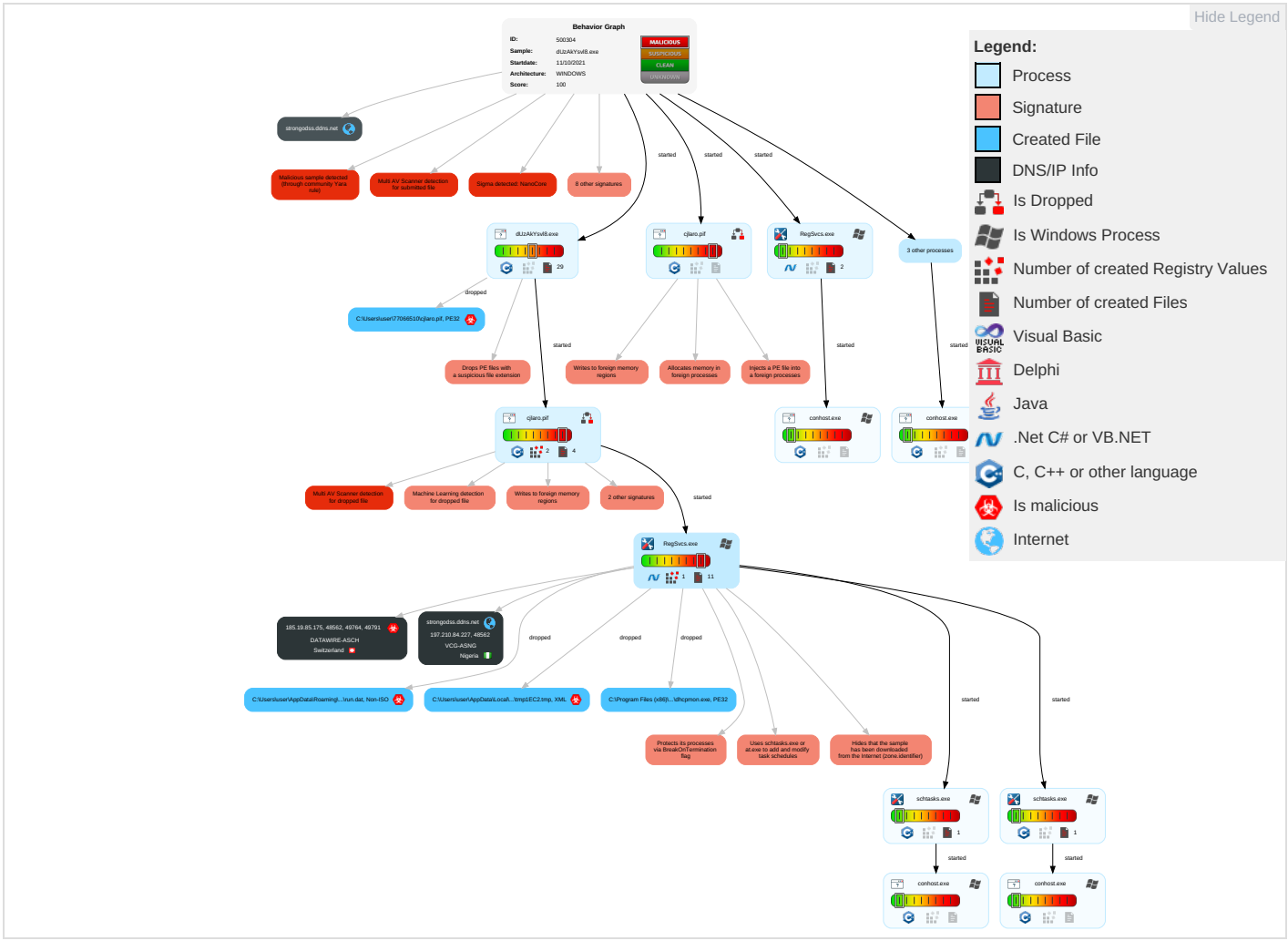
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Valid Accounts 2	Scripting 1 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 4 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingr Trar
Default Accounts	Native API 1	Valid Accounts 2	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 4 1	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Valid Accounts 2	Scripting 1 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non Port
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Access Token Manipulation 2 1	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Rem Acc Soft
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	Software Packing 1 2	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits	Non App Lay Prot
Replication Through Removable Media	Launchd	Rc.common	Scheduled Task/Job 1	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	App Lay Prot
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	Con Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wet Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 2 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

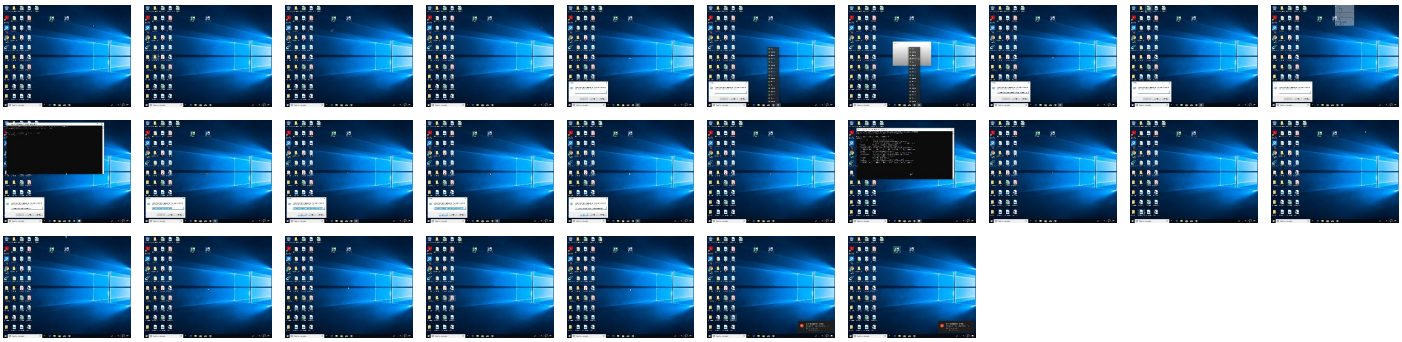
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dUzAkYsvl8.exe	52%	Virustotal		Browse
dUzAkYsvl8.exe	56%	ReversingLabs	Win32.Trojan.Lisk	
dUzAkYsvl8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\77066510\cjlaro.pif	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\77066510\cjlaro.pif	37%	Metadefender		Browse
C:\Users\user\77066510\cjlaro.pif	56%	ReversingLabs	Win32.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.500000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.RegSvcs.exe.61b0000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.onnodb.com/aetraymenuH(	0%	Avira URL Cloud	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://crl.micrH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	197.210.84.227	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
197.210.84.227	strongodss.ddns.net	Nigeria		29465	VCG-ASNG	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	500304
Start date:	11.10.2021
Start time:	22:27:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dUzAkYsvl8.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:	45
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.spyw.evad.winEXE@26/37@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.3% (good quality ratio 16.6%) • Quality average: 77.7% • Quality standard deviation: 26.3%

HCA Information:	• Successful, ratio: 80% • 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
22:29:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\77066510\cjlaro.pif C:\Users\user\77066510\txoxpdjc.qnr
22:29:12	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\77066510\Update.vbs
22:29:13	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
22:29:13	API Interceptor	839x Sleep call for process: RegSvcs.exe modified
22:29:16	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
22:29:21	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
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\77066510\Update.vbs	
Process:	C:\Users\user\77066510\cjlaro.pif
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	107
Entropy (8bit):	5.002783808669296
Encrypted:	false
SSDEEP:	3:FER/n0eFH5OWXp5hCM/XKaDc1WXp5hCMQXBPcU7n:FER/lFHIWXpJfpDeWXpJc0U7
MD5:	D7D163335F9D1CCBAB796BC5C8E03BDD
SHA1:	9CEF3FE22619FAAE680C3920F62B4A89847E929F
SHA-256:	CAA9D279E13AA7ECB9A786A680BD62A6044758623744204324 4DA003C6DC0C61
SHA-512:	9ABD835B48875A2196D9720977444D32DD791C6A4E6EB7091E97AB1F6966F7E79982C981406E1AEBB1D7DCAD33F2AEA5A05D7CC3995932AA3EA3FB3BC6A72D E2
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\77066510\cjlaro.pif C:\Users\user\77066510\txoxpdjc.qnr"

C:\Users\user\77066510\agvlvr.cpl	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.429702104548591
Encrypted:	false
SSDEEP:	12:xgRsRrAtZPIlB7Y4HUERSRdlCiMRwCShdzhWmeTDbeorLCU5+WopwlKVBH:xFJAv47/HXRadlCiMRpShdzz8bfrWi+B
MD5:	45CE434F3827D00D9C3AB67BD7079AE8
SHA1:	80C5FB40633B0BCD55516F89523251E6B5E3A809
SHA-256:	F3370937C56AAA052CFF38BC4DD87ED6590C53E5C12F134C509CA67AD248B808
SHA-512:	2A90270A6CA572788ADF9A61F9287FA71322F0F77BADE789B11ABDA146495E061B63ECA9052BD360B9FA38CFCAA7A7C90FCE37E61739431C4E794AC5A0EEBD CC
Malicious:	false
Reputation:	unknown
Preview:	H35179kJvnA8K5839O2q..9R1Dv6Gx04P63Cz4G873YUM64f18L10eA3BVkM0TGr5377E4qZ2K392Wb821V9Q9v65i..0460b32OWz45wkzoJVQp05u4Hq0W4772C1yjIa 0X77yy9..F85JDq5wK9806r1366hCr17B9311q8205H5f7gve977afL75j8723a60630F65O707JfAUtRsCZ5792z53VcP0s449a97BTC3o6123Fg13W51v59X48Kd3kLC 392nlAA53XX51RJ0187JQt4RM128w0lY5QF1hD0rqM1Z67a386Vxl0jv1XNu62eT835526p440..TYL15RA8466j02Z56o19Otx681Rx450eFB4ob7rSkeR4n5r8V378K8 d3p74p9n89e812WT1Yb3H221Dxp4c20vun937796k5..F9sW35p8Er9449lynCR1VK148TE7fE88b27lM0S054QOf7n8521CfW0B4198iz9..LytE23n2TB84ha97H3A89 91L2BL167l816f23K7y7C404qYxm6sS04512z0y26Uvy2pFM9m50I9oDXsS6809ZM110u2Jr7109l0957f448l063t..

C:\Users\user\77066510\aravnorhp.pdf	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.5024278614068125
Encrypted:	false
SSDEEP:	12:5YOA/nxL4RlHbcZCVtuJ7p6zPl50DnsvNthFo7OFQXqsIBHeKVZ:5Y9pOcZZJ7pYPD0Ds17Fo7ZqsGR
MD5:	B661EA9D0EE79FC8D6ABDC292228A94E
SHA1:	747EC3AE658432133137C847A997460D2ACCCB31
SHA-256:	8D0D086264BE5B548B5C71591F97D2665F27BE763EADCBA958EEF49B4BC1F490
SHA-512:	4EE3927EA43037719F21704D3BAF53C6344165AEC5C726DF54AC9D199498B1C849FB3047E93C08F188E4AF397F3276AB7C43FBA16CA5A9D2721FF5C085D9FE1(
Malicious:	false
Reputation:	unknown

C:\Users\user\77066510\aravnorhp.pdf	
Preview:	6W0g980A5N1Ex6S56i54U7Fen7Q8L4239VK5r33AZVJfMH2t9Z25ep9463YO38aR38t94B0K235436J3..K6707so05XaK2R3py71NTbs6SO1a0293E9eXv7K19U3K2677 j7Gljp9A621L72L53oA13Jt2g8D774PY57NMW08dpz0TM751uXgQ453u606..n51s4WxHu7Lbt8qb06L346232hhiC..sJV3EJ2RU5wkNp990S806GA90593n80oB4xPDG SXD63657XLo7g1I98fOY06b2v6Xu3oU14K73f3OPo..6B35V5K2..gfk85m70N76626G7kZleR1F8CN2469as755iY7q4wF8C4..8p05Xn2625c87q65Qk7N34eH956G97 49225afj0JlFAfEDWX40Ld5M800S5GQb6q2Dg7wsK973AJY9a6wWJGf25TmL98Ks5846c82C8a03ETLMRqK94vxieLR5S4x854WEpLe5jux81L41WQ2X16Hk 87F9U69C8SQFFtk12206QhIYG87H02pi9I2a9Qok25..

C:\Users\user\77066510\bvjuru.dll	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.550150501825932
Encrypted:	false
SSDEEP:	12:dtryVYKWnNoxxOc5MaFbeJCxlsQocvSfnRmlFOX1RU/e5NeWfot:dtrT6xAcSaFbeguySfnRMe1Ogen
MD5:	AC41F1ABD1FB73EB627E9A41861CB963
SHA1:	A6997F25AAA3622B5A0485AA266E0AA43F1BFA2A
SHA-256:	848DBD0A158E01F158874EE4F573A5109AF3FAAEEF5B31FC192E3896909B46DF
SHA-512:	4268492CC123118AD90F5A42E2BDB4C417341256C4510AD34A4CFB0C49F8A7830A26F43797CF3F875D3741D000DD51D9043989DC57FB00940B5FE53C3E72CDC
Malicious:	false
Reputation:	unknown
Preview:	Q540942QUf4Dbp1nL7915N08T89t89N5jn5G6pR0vZS9998MN7r7J63093JF5S3uTtIw818m84CY2mq8tl2..428F0cL71p1..f8JdD4qL090e3vVj97gMb7kkKe87bZ25 3KXKZ86b9QKn8yV0t88E6z47VFuLDs4YZq281mO5wY89YhM929b4s2..on4C0321p2kX7Ldb32xsXG8P0lV87Q4U1..L2aq4Sn9HZb53auPFCFn99ly1t6EUt174b8e0su hT2Ze6LlFWew55Q30w56imc9LQRV4uf8MyZf1Kxz7H9qDy7zy55926T4517rT32H2XQJ2011p31u4X9DHL9..44ar1B35D8p44YN54y2uqVUVsu670D48dRO013RtD90zw 65hb0RX05S1mst2wGQ5tU06fj08lEP76T34R3dMSGc11065lf2A0OIg5pkLJQ180s1k8V2..1G1QQ16118d3E01..087MeWs97C85zQeN97690t0j5Q9562mLXQNK2R40u 691J2GBCUPSy6117G7794ZRD0A9IzG5B5AO3QLJn065973n..

C:\Users\user\77066510\cjlaro.pif	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	776432
Entropy (8bit):	6.353910854155555
Encrypted:	false
SSDEEP:	12288:qBzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4aKie5DGDt2:kcneJVBvXAvwRJdwvZ5aKie5DGR2
MD5:	279DAE7236F5F2488A4BACDE6027F730
SHA1:	29A012E5259739F24480CEDFD6D5F2D860CFCDB3
SHA-256:	415850F2706681A6D80708FCA8AC18DCF97E58B8F3FDC7BC4B558AB15FC0A03F
SHA-512:	B81276FC4D915A9721DAE15AA064781A1DBA665FF4864CCBDF624E8049C1B3C12A2B374F11CFFCF6E4A5217766836EDBC5F2376FFA8765F9070CBD87D7AE2FI 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 56%
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....."....d..... ....@.....0.....Jg....@...@.....@.....T.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...D.....@..B..... ....

C:\Users\user\77066510\gmbvs.ini	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	596
Entropy (8bit):	5.49650466783217
Encrypted:	false
SSDEEP:	12:nXNTQQhmCFkEOimlfljPLsd3JXyNRGleqcY5+9fkgCbyHgzhyEhhN7:XJQQ9kE1mlBPAdZXDeqcYgiQHgzkih
MD5:	D24E6E36CA0380D9AE91B95956A2B495
SHA1:	C9AC0D0AABB8FDD8775FE54958DE809E481731F1
SHA-256:	154AF62E924559C5FE675B816B6B2E327D5820CA76409DCCD2CECBB15A48C1D6
SHA-512:	CB6133F7BE480C557B6F42495284AE6394B67D0833105E3555DB091749093D689E4B13B98B9B46DC83BF0E993F9257FF9D9A8D68FA389488EB2D23815C621AEC
Malicious:	false
Reputation:	unknown

C:\Users\user\77066510\gmbvs.ini	
Preview:	490bF9417QYc193z68dr35847c3..gZ99Ne7N5500ZAx70515Y9T86ubw7NiBn763z30Q6s9rKZm82G4W6zU35Z2A19b8L6CP0Hf3Y398O3UW33hWl86z3314..922q0gu 8TmBW928Uv9w30T..u417pM11y5X9E10BhQz6K32q6L74T0uliFaR95lNT73Fi0Dvm75Z6P5562c9wfU0397n829zMg15o5012G422ZS0Hgg1778YS218Obs54o913V1V9 0c1H1795GC7828GM6Hl0r33u2D7pGY752dc4HA3dak3EhK3..61d8O294530ILFNeT20Ox32j7yJ8LwkX5w694lN8f..2DCz32Kb99o487ztlFh9871F2Jm952Q5A85w8q J555F5JRa2BQ9OM0X..1Ft7cMc1Pk147jZGh7Na07Yi..3L3D5c60Xz6rD1X358nn1dgi1kHXa0j1aQ7q48vZBQ685..1eCU62..T09430nQQtd2asG2q1aIz86q5292lT 4tWkxy37gJyS3g89TB8BO74R3ay61Kl5HZ1y591lb863lw0R8P4517m9E3319987oQ4e33Xp87..

C:\Users\user\77066510\hrennftnds.cpl	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	65398
Entropy (8bit):	5.57926760107341
Encrypted:	false
SSDEEP:	1536:ZeWsPd1VFU1Jj5pTkp8x0AMrqTok8Jb4C4m/le3ma+VBxo1yotcuG:ZH61VyJbxt2Hnbf03mvTxVyG
MD5:	51B278BB20BA6B5C39B96E40B19A591F
SHA1:	CCF1834F98327A25B1404EF9D679B9D8A29D5330
SHA-256:	B68324E9D8A2669F261B06AF1F96DA4CD8360CEF79F76E2AF45EA7E423F96C2D
SHA-512:	0C7B27F4227069385D57CC4983A40DDF55A782DCE47A7BFF2A484C1AE92C0C66FCC7804B7AB25CA175939A6F4816B6E769D69229052F01D94E8EE7D8EEFC4D 1
Malicious:	false
Reputation:	unknown
Preview:	44oa3..n1j49a94W8usBOZ4N2i9yT7SG03Q7W80R418EQ8QlG4Vsz9N7Tv..336f2TeAh1NBx79EeYf183bA9VBH4B9z93Zr1m8j135Pky6w..4176InN5u4bPg50242Bu 1LK6BY56B49O9403m9..78FK17b2123U3C8c35A6OtMO4H0vKyA49P7501d16bz9..xus3U448h8W0w7F0F3OKD0VM8967a4P977PA96E8YQ4plfg7f7uG8..ak48DtA1m 76ydl46o55j157BXClQmzH76w2792xy57j6RT79aM9L049ya54Y21x5H327BH0L01k9BQ..4k4TDJ7Wv0Dmam0NJ8fD3bJ4..X52DL84LxY26L0401Q4Q3R16M933bEP8P gU9052JAh1Dk06B0rVJ..2Xy9536r9m67OB4b0PN55J252874K0WUJ9198341xV3885V93lqG856Yt6f96y5IijQF11F1Q7374185m2212w6Org09..lbJLr65849y11si Cxq7O07Y8mdZH4a85n8x2rXF3bS978oL2LTOmkw4462f6u5Iqu631o2BrAGo27i87A602m1D64W4E1l8..fuCK32619UE02o6A5ffHfRVflyy0a5QL96KSsbx2M2611of7 3yzc705F8..6K4E0AE6U3hA27a7o0C1ao2e86n79iAvWy1..55H2Ua12c7GMF85qQafa65QW5w856AzM6B7nj9b38aQuq1e1r0h710vq4Hf13BAi9QLWdts90..NLd38qW 42RuN7X5MURKG9WCQI7P236G0T41P8FHev6V10glh338JD2e32..G4703kFbjOQDo2825W406811675J4cO..7ghZ9918R32957987ll4w551HHz98576z5D518r4P7Kib 412GH01..Ehrk0q3922dA3qFN5u8P78od37Kn5036..qPDFHK2i2klYwqa8duBu7A7cNw5HnX3Vd97r856m94sm5nB

C:\Users\user\77066510\ini	
Process:	C:\Users\user\77066510\cjlaro.pif
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\77066510\inprv.xl	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	5.424929682839166
Encrypted:	false
SSDEEP:	12:YuTQZItykUeGyjxyGhKzLUtIPtIsyvdVSBwKK+X2bO7nTy:LQZC5xhKzmrsTlNlTy
MD5:	FE93C18D9F3135D1657E5C1EC1738AA6
SHA1:	D4112EA632172366F983DFA963C702CB234F79EF
SHA-256:	04317DBF1CC693EC693A13A0E6A242C1C04B185A73FEE1E689768D354AF48F11
SHA-512:	0ED13CE0171DE1FE5BCD99073A34F1A45630C5140C821F715F280AA21B8912CF5DAFD42B080061AAF25799383370A68C6CD77F2A391CCFABA3923219CA55D76
Malicious:	false
Reputation:	unknown
Preview:	v6Ui6zPK6xh02mgFgXp0pcl194503sdm00576PYX525M3zT8492qb1964Xj777Gv003ez10u6mv199XvQY1m55O935fSj917vmUt..57Fl7C9E2dAsg087Q398gU8gDC6U 70P0VUe1eL5S6MB46l0979G689o4uf92..454999Bto5..y0J16Xt5..97W3g95t4Q5c77j32b42wm2E66gq68m1gF9sAz4oVEvTr3V6847l6996a822e5z8S96Xt..021 13N28J1sd346lSA35W17Su16eFj219M2lStKS20MgC21S3yQJj6gS70t3Vi838RotN7842532z1u91Fc665572..0lv87212406iC9o2Abqm7v84ade65i2tn8..v3zU0J G9O5br0DtQXjnO896t9F20UAlZt7o9JbWz2kLLw256697iNJRj99RRLh06QFc52..W7p2cE757b30t66v05A5tf28V524g1T234KnNio51f521665YiOE14LSx5068i8r8 2d12Fz947MN1bvC6878Ay6D043pqo6QyR08aMh08Pw85o4..

C:\Users\user\77066510\jbxbxjeb.dll	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.469755934931095
Encrypted:	false
SSDEEP:	12:OAObNzhqrQKrMrxuHqTbSQV8hNyfFysMeRxs:dO5g5A4OjV83yN2e7s
MD5:	C80239502806F958F12FAA39BA84560E
SHA1:	F7C7780C5E5EF39C93E397CB5FEDCC3179CE0546
SHA-256:	D26440B3C6DD42923630C4E5732D635B13F50765D813527D6DCA9725D3B00811
SHA-512:	3B99D9DE4E189C567184F6AE8CDE55090E7E53CDC81B3CCD0B0DE35E5A81E1AD2E266DF739C079CBDFC53CBEEFDD662014011113081423 82BB9392D81374F B8
Malicious:	false
Reputation:	unknown
Preview:	0hs56692t9Tc55KQd84E9440S018S47n69h53U..B0qQ3007A5Bqd80M0gfP09d441ck80040PEd95JB5Ml094bll087nT8OY782b1E5aYzYuH2yM4k42FY74T86H8U8O4 22667G5O25g..c73uUH0A496009PK0oE65PY24w37..7lY0L05299Kab4amvh36w3V6Dmmi2815N0V8HP1xXONbaHgSnO3893g66B5181P7IBUeT85s09265mRr1f6a83V 3j0Y4ojlf4cf1oY9p52hoCSyuQpN61m5K8I..o62LY554zX2Kb2B42XJe229W161HQQDb348SnqFO20L20Xg2z5e7Z9S66Nowa5056U9YWM835ON49F0K553lhAG8ug8R2 90aks634h37q96934HZ09zu950WG330IB7w32N2..6v7lqC8S451zg579y42y19yTVv7x7neev6017Z3PCJ76759tZ0ILb7pT8e2D0U711J30..

C:\Users\user\77066510\keksbhxmev.ppt	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.470587495063201
Encrypted:	false
SSDEEP:	12:bnEjM0hglXLpsw6TczgUO2iqWjX1AsqAcnsLGRzEmoB+NMVX1QKgeR:bnEjMgglbpspAxqjX1aAcsym+NMZawR
MD5:	85845D8C48A5A553F765E4B356CD3911
SHA1:	E4616CDD21D9534F30D4DF68A1FB72EEB31169B6
SHA-256:	ECCAADF73B9B6258B128FBB8EA6D09D818F13272DB3FFE93ABD2EBCEF1B0F78C
SHA-512:	6A5E9FE1EAB4168CFCA7A922E62037BD850354BB3B495C6B409DC9FB8DD8E7534173AFC4E38D412F859B8BC8EB86C3E57A2756D3BCCAEC79A853ABED4FCD 210
Malicious:	false
Reputation:	unknown
Preview:	9q4f6wGoX5d7wBAnv2Or6t85hu0NMZ4JA39ai45vdpX6P01y0v9G5y125hks85925519OO8os49536x5rm..KDY25hyEu05ld0543z797747Fp919f4z51yD0TYJc92h08 457u605v1Hpe31va93852n72n4kPayRgYtgJ58DQ7Ww76Di37Nt7bxXMrc37FPI8t0960e4P2543O7958H668992pU9E4TEB..8J013Q75A3M83Pw3gH5ccVL0rE7r4q2Z g4yFY5h34Q6PkV93t7I24i8298037i30q9z90GKg508XXT1f4rjH94Vryh8KzU4Avw5dzUp9m4..b68l81C32p0884qX0Vs7rw4H16a08dc7Wa86Zc4QF9G0x02lM84mH3 T596YuBxNPMHU796Y3nb769..3l09422mF4QU85TkV21TIs3824463zAO90q2q55W4Cb89B3nR2nB1895U2V79Q8O5u14E610222QM7750Yo654pgOaWX6..

C:\Users\user\77066510\krrapb.bmp	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.401172365993664
Encrypted:	false
SSDEEP:	12:43hqymOySBOJcbJKrD0qloPjd/0Zi7Wrhu5ZoJoQeETVMx:4INOXBOJcbJe0quPxsZMouXNEZMx
MD5:	0DE8FCFC411FF1F85AC8EF2FE25B2F58
SHA1:	1B7181B6451FBABC502369B9532E8CB16AC58540
SHA-256:	899444AB8E592CD0D5C8BC9051E4B45BA02FE317FA78512FA2531A8B8C655A8D
SHA-512:	F1CFADDC269703C88A258ACE052683D29A5C90335FBBA95F563FDD872C3BCE0CF973945C077F51DC83C885A24FD16A380E657CFA608E6D784DFDB5D30430D 3
Malicious:	false
Reputation:	unknown
Preview:	Gt45978X2N80A7qq8VY7ha7405M4ai7kW5d08TK8Q3W728o84Cq9J4M983c98V728ae3E1912Wd2zUs3l880..7Pg9d36698l6x19hBU3G70lz097A64L..72h85c410qK 0171p9l1rs4b83N6V0w9AG108udn4L60H064750513Pj8I0v2K6Hug86hcG6Pyq3r3h61g3Wb31gO2q8HCJ09gJ394XqQlvOM14N9P8ZQ9r97SjJ54d74rY5EC1B..D464 3wG66ddN87X134w62C067O7L328O7S76290QmVZu01146bndmf3045Au9V13966596y094so226F08P5svi5u9o2656oGSJgD9Zv4764qAR9W0D5x3wd87NlfYg5u674qZ N03F85UhVh8Aq26322XhOmMnc17pG1F76919W8TA..8Qn9132984T6fDKJHo0l5n9F3YGv69j5Yt7PflQT7eR6CQ90964Dfz7V3kHVm706of4871014Fg75c6a74661PPS 10M9M3HE1728D325p41849h8E31VU..

C:\Users\user\77066510\lmaqspuvfs.txt	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	575
Entropy (8bit):	5.478714072804598

C:\Users\user\77066510\lmaqspuvfs.txt	
Encrypted:	false
SSDEEP:	12:Q2PLgImEyURredpVS8kyCUrXYQ/xXaCGUPN/mD5n0qs0S78f0RaR:Q+gxrgVMSXYS5GXTRSJy
MD5:	2BCB8D5803ACD40E750A3EACE6FFF142
SHA1:	B9B7AAFD67D2E7F7172525D00C387F745EC5718B
SHA-256:	5FCA30CF19F3F3C6A69FFA2F61C8101E883B450731748AFAF82C8ACC7B629A70
SHA-512:	5325C49DB64ED84A27DC93CE737F2DF8A52AE5AC7D473205D1864DEE0524F1674C77A21F85A631566399C5714C35DADBF65F7553C8EB673572E8A1372055E58
Malicious:	false
Reputation:	unknown
Preview:	6ut297243s5zr61VV9hDAn759sN03zlBYyJ03aXQr5R52K59W8Er6269Xth2u2460R4552475U0mvsh99jHVD549D4c75nKi7g60Ko8wq0w85251265K73k05586C160H5 DPbMviTB56k758pOORrZY391431e9..gS0j6nKx8q450p61135CX5U4E03dQ7sPNJyW817x1K880z5FQvJCAf19P7mL9K02a1766mM6T4x5Y13447XD5373c5D885G4uD5 QhD1231v0r1278mpr63..zy77JZ1wQl7461e4KIf4w14l9081416986555RD6WVS5l781pgb..Iv06c4S8O7..38l2752J6x06GxR399y0z04yVR4NXJCD0cc3E7ZHF1ce0 4X41R6CW2t01U8kwZST920nnjqh162Z68Kj0O63M57UV87K02YwJ4caewym..F15G841Ir8WI3YHOIc619Q58y229X1HP..I3kV8u88lM30u0U410wJ8lM9m207BJa3Q71 R3E9om3i89g173bqxYXXCUrU0wr408onSJ67m173qGVrF9C4A28K6..

C:\Users\user\77066510\mbchmfnast.lfh	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	430098
Entropy (8bit):	4.000008896555934
Encrypted:	false
SSDEEP:	6144:XtApp0ELYvuadbIZLjE5rfqN6CtwJYlF2b7SOXssuseskMe8:XtApBcvuCbIxaWN6CFIhcXsre8
MD5:	FE4F919F7FD004D0D1C5C89BCF638D11
SHA1:	11AF89C8ED4069E553FA20F204D1C8C78C60505F
SHA-256:	BF5E0A807796017B22886D1C734D579DC22CDD47A2A26560960908BB05BAA6B8
SHA-512:	87CB95067DA0E57DEA4E853E3BB23AD7DF79489A570C0182271461FF7512BA889497A756F6B1DF33561BEC569AD6D7AA171BB8E2FD7940A21470960C84265B49
Malicious:	false
Reputation:	unknown
Preview:	58395FDA4BB3F8001A1403B0D188A2834EE36D5E40FE650F891D48B3CDDCDACCE1721234A9B602F419379B7AD42AB46D2C6D187AE8D8EE10794BA2E5 04803EE1ACA14DB680B85211097E8BE1088295F49B8914E3FECA38128D86BBC869CD321DE7368BC07CFC53C637C7552DDC94B0BF2C6518E33096E92A 7138811F9C0C4224E6156D52293B93603F1B728B93A6F9A4736063C28700FB16F2B2D0280E1A2FC11A45E42CE6BC86DA1EE1FAA42996CD4506D489F7 BFAA3AEE5B8C9348F283F364858BC459CA5751A58DD9F7C1B6497A4D40AFEB5FF7C34CD4B9E65F86217F21263D32BF551E85D54CA2A17B144EE4D140 654AF7FE85FC35D6D5FD10E181C85E9232A921B9AE38FA426E7B517C3A639D525CC9985BFF072D4E65C8652D956CDCF66B613D1C815C6874CB702C45 A73A29494460F3A49CB22C03EA3DD67248F959320143D89B83CF9B883D6A9769E205020E1D3D9319AA9D1E3DE4DC5F048030080001D6A4FD8ED7C0AA E01E14B2F5531BCBD56E77D4D168A1D01C6A9F5E7FC234E4A17EA7166070E67DCF7A672F983DF6DB42D2FABD48B6DEF887EF2BF01A35202A4ACBF160 5E40AF06C587C0C809AC7A1319964749457B109AF6C193942449D202DD3C727CD1BAAF7B34FA967F7F00DA7B38D0C99AF5497CA3441668A7B1F646FA 949CE873AFFD9711BF18314E0FDB2A34839BE5DE

C:\Users\user\77066510\mirwsqtlk.dat	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.519787882016756
Encrypted:	false
SSDEEP:	12:6yKcEjor7VW5bFYovesJt9YdBCwr1rdVKo9ZQ+nAuJf:PworMFYovTtaBHrhdVKGNnAuB
MD5:	8CC56D133A86B8D76CD01C98D1FA3A93
SHA1:	30122115E8C39A622CAFFCD2F5C22F5F824CC60F
SHA-256:	7B51963066C3E05A695E929E5B128BC9A08F1819C775FF55BD60278C6189EB25
SHA-512:	DDA706FF378A7A5F51ACCF33C5FADB2D6E52BC885434F9E69C26B868167C40CC196DE47C95CDDF4B1E9C8AFD1696CAE5FF287275CFDA48E483A53C7093134 53
Malicious:	false
Reputation:	unknown
Preview:	4z50XUwCpa010uu2815Mh00YH30j6t58cvO3kj6a9N2Gj9B45J9mPljxw0628vwE7NU57ui070944C57F126d7IVFH843Ou57..3C0pI9cv036360PsWNp9P38O47oMe23 11x70174b4x36h89mi8v5jn62u2t26o9o84m89qWK8A64qY2t454C7qcDf8Hf8661ky0J7KmH..g6156y4J2ENLw47881f6542716fkT76UHV3QfvA17k11859221O568e oqtpGlb03cm..C77hqwaYdMd72VF06ilLpoU16Qok93q3820M9TI76V8Yu24A216655e1T7NnD30f06lOg78D08pUq3MJ9v9Odt07e6OJj5XdFT2cqP428I1dWrt38PPQW e0Z..BYml38xJEdBDB559Lu1gNl59RX87A15Bdn99LMoF7z8m054902E37a3J13493n6uL511RVm4d50uZ30lg63yX5FmmUy76K8p3dZ5Q398fSJA..

C:\Users\user\77066510\msowiig.bin	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	619
Entropy (8bit):	5.492545476252811
Encrypted:	false
SSDEEP:	12:G4RShxcOTwcG24qT3Xrz/ysneuE0X6RZaMDAg7VLBkL1zPN830djQWINJ4:GgsxcOTwv24qT3XnllslFnkL1D63qjew
MD5:	D4B853315AA3430917FFE7B653D81946

C:\Users\user\77066510\msowiig.bin	
SHA1:	2494B995CE6B89E533CB7D39EEAE2AC14257324D
SHA-256:	F8B28942BA82E32A875FF7974006932286F5FE1CBDF860423090EF257E0D0D06
SHA-512:	0E30D3A44668287A1449FAA5FE6E64E819A2CAD14B825252CF13B30E44D8174128F29740E21D9CC937FAA781B474C8B739373A5C763EE5C42E0B0AD1A46FF54(
Malicious:	false
Reputation:	unknown
Preview:	2P467iUI44C73iaoX4m8w868aW7Q5qB78FC3CB479r1ePc04uA2H17f3j37p3BvYd616oOH21BabC7X91Y9209YV11..47094eL6S5m2nwyWvJGkHUW12772k96v1d28s2 3m02e4W284og1mS6ZDQ2n85acDl1WPX59u687008..J0ftvhi463..l59c197X5xbX63284fK2vDho0J6S9r2p5gG59907Z45l9029EFCJA16ykWN19tk0NxuO1hsapx51 8oClrlT937v852i19wc1m9Jd2MGNU134KV1a0992w3nZi2deIxHJxg8782kw4Mq153kJd423R108835v..6Z710pUj70hk90X7734zu320l7yJj546xmV9Sf6o9219677y 0kR998rdBcZKlp289k52JEdos7pz41Q69q0yY59Q46A34328..JJU99vt4t3LsZQkNhj985nVsV2w3Hf6tg..8BFD664R1Z9GjbI1er3OO2j0T7oKRm7uz12944iz71217 0VQ6uS47p5B81Cm9xW457306zC980872wDEp8234n4jq36Z680p6d62339WL43H6Qy4mO9rn7pd7n436H304r18z5534Q97x3..

C:\Users\user\77066510\oaeobeseuI.bmp	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	526
Entropy (8bit):	5.470896728928171
Encrypted:	false
SSDEEP:	12:jY1q0ykCR66FNR9hBif9fYNcjGY2ohQsQ80SSh2n95DRUUW62l:rwJ6p9hBi2NSUoqs2SShKZwl
MD5:	4B682E2CFE8733C3FBC05909A49EB6F9
SHA1:	13C089692ADD164CD19BB3E6503ACE3CE62A240C
SHA-256:	8D878D2A5CE42C36802B75F854156A6885677F2970B8ED61AB3593013EAB3B83
SHA-512:	C62F9BBB28056F391FC735A691C130AEBEDC2D0E977B9454237CAF5D8468A6B07C218BE32783E00C9E526A15AE08FB0ACF0BD8DBC7F69151582D0CF49014EB 1
Malicious:	false
Reputation:	unknown
Preview:	u31U6ySzFC7iMO3pNrvG35wT2dg1cu5s70E7s74v82Xw4sa6n..18xhv53D0W923..gN92l94S1b2M6815oe8193Bm2v3q9W0Gu0r31S4zE09i4284t..a0s9347HaW024 2ehh870Z33Y1z4E9QE79xN062Q6W3MsF1N00k299YM49m98z2cyf8025tf6kCGNR3mj570k03k2BDK505y81bZzq2qvNK4952Jg161993bKt5t5L1u4G..10Rq6Kwfju7q 59FpbtdP39531G23AEz84VB21Elt1e326y9IXp96653Qp678Sx1WcfU7G3c8m0z0106j7WA8Yt78KI6C94p10Nv63Z046949vtbOesyNI5Ek30b3j6Jd8093l5X..Z6OP2 495N2P84859UAHg0a599J7sFV32U41mvR35b8vIT1dJy118559qWOdI4MMxg803Wy0c8Te15s36E811p7O13HD48t5b80S80Uu250ytQ86OI8q780k6T8SDTbY1010nGv0 bMU8..

C:\Users\user\77066510\oeobxhkbe.xls	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.43675555101191
Encrypted:	false
SSDEEP:	12:0VE7CIEcVHdUb8rmhaUMixFfbkNTAbyecENQQxTrHLf2Fg:0VmVCcm88cvdQxqFg
MD5:	A412CE7422B902168C9D9D0069B2BD73
SHA1:	5ACE613E2FE2D8DE9A78825ACA7EF6C8DB271885
SHA-256:	63F1F9AA632314FE0177F06317530365AACAF728C21DC03A208E1109B5784E1D
SHA-512:	42A9CE52EED8DA9E756FEA877C25F70D4CB92E5B9B13FFF7D15446A0AE68381E25B8E1FBB022701CFEDFB100F8045FA584E851D6DEE32E9AA7219140BEB450 F1
Malicious:	false
Reputation:	unknown
Preview:	9B6o76o7HZ7GD73943Bu9pj47R06jJC0l8mH52ZEdXn2023i577t20651p6LW..9K3j6036LvSz0T61321U52S2V2s9j0g163n5A6374O7p7DK5u41390jm62v6zQX5m03 eW6Y9bA72N08N66b1ywF9vLR7l9YCS3f..17wQN48d09F83h16ges4917847Mi8pYx2IHN79e8184qdkae4RIOu6I00vQ3j7zuQ72l4KY4u27uBH0l50Mv09FT9t..eoGv gM7766Z86iR77GH253ASV8158e9rvB583..284Y1k846C4A24c6CjV53Q13F2Z7Q11Gf5930a168JZ9285v60RY8lL0c45ci0Cl1y62wD1bH7gL6Dcb7817Dn6579o48C3 ka60056GKh58X9k31N0115701Om481O2s22h7j1DDq..320h06Mhvbvx7TN47lwO7t5o48CK16R1D5oqVk92WkkF7i1J140Dg5y8T8U287C4sv4v70Q6Z2rZI34p5L986l eOF666Ch4ts36TO1Fgfw..

C:\Users\user\77066510\omrq.cpl	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.498311572387548
Encrypted:	false
SSDEEP:	12:xFFdWUIP+oniolYaDrJTCzj/cb4yvcnN0IxtXhelY2EaGiZ:xFFYJT2CJTCzj/biwtxtYlYaZ
MD5:	A0421E014197E3AB334AC3588A5E91A1
SHA1:	BAF987222C5925251A6567528E797FD63CAB3A92
SHA-256:	D27CDAFD99E19C474BC1BFC89334DD828C9089E44B0D3E043D3F0EAF2950F6EC
SHA-512:	411C0994EDEE07DF1F3140F85504C4F08534D41C3B6DF1502732491CBD5931D7597A7B08072986D6E5709B0817FF3384FB0E71F684274244875A6B1B46A122C2
Malicious:	false

C:\Users\user\77066510\omrq.cpl	
Reputation:	unknown
Preview:	6w48PegnK941ic7PHZcf0r1NP5..76ifu6842f61B7590D4I1AZWSA27pcAc7gGZ5w065h3oo6ukzQlvaLo1P8g2b77m181U1X3bO6ntm1n7u3R20B052AN210En2Vl58. .Rv351f2y7641Q666jp012mb3k9jN3psg10kj679lm5865hm010eX52Lng089K431q3D9p9vA6567j71..82Y41S4810Z723G58qZUD2zxWZkX4ehRu240j4aic0oL1E5o 27hQWj5H0f3QqLU7V7..X6vc0k95F6T9E0A84ttwQ59FQadq8d1Oauoke82Luv2U31p87V22U7gN500x921707l8504D4oL470jKTX03C82gP8615fJQ8lMH4G9GC3vMdr f1C86rf9057988863623nm5etj72LHg46Hch7xV2us77Vq..ZgO5X4500TAo1c0GP67t9Zz9t9k5641522aAWV4n5D67z0FmxW6aEC6H5Yne029b21V071is3Z6F26..

C:\Users\user\77066510\psrsdcrs.ppt	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	535
Entropy (8bit):	5.460228697655972
Encrypted:	false
SSDEEP:	12:qmPLn4doIG2hU8Q9O1gOT98GsoYE3WMIvteVVx2i8:qmiG2Cn9O1gOTyQYIs+m
MD5:	06617F07B96ACD92F7B97E6968FE12C1
SHA1:	A5651BBA9A8F5B7BF7BBD579E5CAA790C81518FD
SHA-256:	D9CF772CBDB83A3DBA9EE767AC14BF1CCFE30FFFD41121EBB01C6D4D4799F792
SHA-512:	A4137B9F09A467218388A7272859B438B45C65BC3DA9DDDBB2FD5822DFA676C567C5ED3D4F30F6F334DB9578B8D8EE8CCA9E2405485D941CBB0242AD2BAAB5 9
Malicious:	false
Reputation:	unknown
Preview:	0i87hcn7zq38Ud0M6O..7e15N4eJ3K5X1aJu25V8zYH6hv08uX1Tl39KJk5Dbt9G0S1s5ljav7Z47V9094006655j4b5Hl3Kt328479TsS6y34pB6LmzzVdOX6DT7B9D0t dFs069532nx7xK30jPG538nOo5l1fZ776Ma98n46rxUh8QeyJ21lM3Cv027K2110O7iH640y441544B0..sZvj9C5l0244v9BcC8568Hp549jHoiF4061V6R8K46Yph334 a1C378O878rP0S186B02X6UB25896J1yT..7lh13r84g3zpSg2wR570v9pKs20ALzWa2439jDm67689DY99IqB6..n236g95825254793218230Br45e6bD2871PuAlaFS 11I880e9MRlZ6wqY6K9099qn27JD822..124g48r34433f2C6Pj420GAnT0M0CNW6237J4gz4d26dWFH43i00N0335A3Io1x4A12x60Zjv85nlROSEU6ZLt51i96tH0X3r 29FwZs20i29tE..

C:\Users\user\77066510\rIller.xml	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.494842699274943
Encrypted:	false
SSDEEP:	12:Ih0PfU2+AQOW9QR3wU4uWavcRAI/7umzYVxBmUXOuC:FtQ59Q4HaIAczYVxBZC
MD5:	03818248A8B6BAAB709E4957BE26D1A6
SHA1:	77221C21787284A0891AAD0F918046E6EA8D209E
SHA-256:	D6825227D0376E6F9704C6213D61B3E324473CBB44987CEBB645D7458D8A1322
SHA-512:	C74D82DE930B544C9E1D6C51CF6C56FE3640D23C1C39B0A6FF4F0924EA905A093C85943C6002454558CB43E76558CE5773375D124809B62C39D2BDEC1B7C35C
Malicious:	false
Reputation:	unknown
Preview:	u8N053k31p6j04MT87Q69ij9Y9EF94WV..ji3v3gt0282dZ2Gw1H2s55U4047ec0y1..c8T1E8Z183E68D50XASx26481t28I7gE6TLr16328O91YT3hKTji9sr35hpWeN 9mvYvS29M2123D3699V532F5517wD45h9884Z0I80F..02VK5U80q8P6Wm4Z73tk2R77CTOtIEPLj0U5m50KUL65qqs4WYbI0DGT019p3Uht504Hn9C6833x1fZ228eNM. .Y0jP62js65265W24Og96Z19Q9U8sfnIc6zr5Mf91qtwVX1MUQ7z2049Nq28K276dvjg73gl0R0e4Zp8K81r226JC4cAW2cK2Gj79m0B9eY9560nvo399G7o6QCiHrcfQ3 rP762O7972c7P1zIKGL7o299..VS25TV1L5Tn4725Bp81m7v0oqDB642Z0FsU58d4LR4LHtc66692sM39inGE6Y35i0v78TVvxq24r693pCNK657vn5Q3QRd917159Zs7U S6RbuVb59V..

C:\Users\user\77066510\tcodw.xls	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.491533496757466
Encrypted:	false
SSDEEP:	12:UJhER91CU87mCTa/V0TDZ0vOjWrMNltukGSAtP6gv5xLTsyaUt:ChI1C75TBefMNltbUTvvLTXa8
MD5:	026F110A0C817D206247DAABE85734B6
SHA1:	F7A4A3054513E2BC1E3DE9F4AD628E642BD0965E
SHA-256:	478020C98C3533DDBE747DC2285F4B9743BC5C3476C53D28CBC1E10A861CCD71
SHA-512:	E5A65B33A297B5C58226E0DFEF7B30E3A4F440BAE0FADB7EECADC968B3CCECB3D26A7F43208BAC1AFCFCA5F9F775A855EA677EC87516FC378F6B363006C2E DCC
Malicious:	false
Reputation:	unknown

C:\Users\user\77066510\tcodw.xls	
Preview:	f7sO4yc6zm04pV5JL2quHc8e9T0C22BqPv21F5N746705..074Oq3bpPRGYa3l86905Y0T544F527Fbl59U06q..a6Tl488L9bQhe7ih3C2YT06w235R0G6u7l950873f1 000Y3T6IU7LfyjhT8a672E625B6P4f14H15g6F683D6XuZ1hTT8M27O8..14S18JaNArK515zH53770n7fW27xWuvUHxXI8M39N7e1yN77P78Qy8e6dog8262jil..1rSJ 7KLCB5zC9u87UggY962B39U24rU11bmnBuSHC93C29042K..697S57s1z00b139B1L081zwC1..a74R17v1O08BB7pVg58c02053H93h95GM34107VO01j25..T66ozm13 411vL6iUX34bk037Bn35WLyf303j442FQFQ16S25h9h8B54BQ4Zc79607JH1X201Mz4KMQE4znmFC72j9U6u7tD7BO093W3B..XH8jBlY4xk4rTv8F207s7Ei81bM35P63 5o1g2962q66PCjgESH75341o0vifI1OLB4U116shk6FU1ctxvC60735x6VK5c0pdqAi9ei586..

C:\Users\user\77066510\tstvjpwaw.ico	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.487676269826994
Encrypted:	false
SSDEEP:	12:3VuARexgiBiiM1Yc1NUAgaJRXYcLS184svKxiXkHFymlE4X:jReWiBiimy+zYd1EUdX
MD5:	7E48DF6BAA951ECAE39B524CF001FCCA
SHA1:	454836998D2510CF79377EA16077922CC5AB2C13
SHA-256:	6AA7A35C0628AAFB3851BE715525F94323972C5B468E70FA9E77C98A17893ED1
SHA-512:	F56C16D18C3B9FB9F7F2421E66103E1D7A901F1C9160480C732AA303A29F71CE040B0A90DDEDAD68F210FC9A2ABF50CE9A4AF15112796D73EA97817A1984712
Malicious:	false
Reputation:	unknown
Preview:	O9E6963gB9N6aN1Nid2wW67R5z9dM799v9SV3cD8qy57k6z3d7MUHGH1F35RdQ1c1p12C..CH43X5q99yA4Y816C07NKAf63TfsJ09..C51iuMERi8xMX53pwoKd8gl986 6s47oS1i42435YhQC33Zmn8b26SV6bEvk850Qb5x8467K8QdP92l37zS3OB46Qi98w47r3W6Px028t9K1Li7vKxS23F3xg..e54kX0nz77Gdj5y46SOqe7602jhWMR5125 3641Va121251r7b94V369w0gz21k9llU8J1110Y..3i7vAoK08316V5227N824VsS0Dm165DTTj926I2F124833ftC4TtX1570h88400Wz66951q5541O0Td4Hk683Fv61 jSCHHy8A83Z..w1WQ6S0pV0TZh6BYGIr663Lj54eK6613M3dB6qJ0npq6Ec555RezV680EvF84p8QKG20Yj6S28..3m2bR0079106p0IiC629m398186yZ2v4yXn37T11n..

C:\Users\user\77066510\txoxpdjc.qnr	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	data
Category:	dropped
Size (bytes):	96502020
Entropy (8bit):	7.090532095529658
Encrypted:	false
SSDEEP:	98304:mnLDOE6//KHPJqqs2C7slJ1+UdhsPQ36hX7jWcW3b3Mr0O1dElqhA1GJNkAL84Oh:3
MD5:	A6B5973B2AB8621E18DE5325194D4217
SHA1:	AE4F38F9D99FE7CAA0DFD1A8C20F9A8645C1AD19
SHA-256:	9F205B1613138A4CEB7942223C7654D575062ECB54D3CF54CDF1BB3E56BC2A6E
SHA-512:	938CD33CDC47F8BF9E588C9C2D4D9DF17C3866D69CD44527F08003CC1F50A96BDDDE7AD268D4FF3B5CDDEBAEAC44C9A888433172D5747B3AB419283D57414 E6
Malicious:	false
Reputation:	unknown
Preview:	..;.=.....w.d]M.7.(.....{uS.....#.c.s...@..M...IMU..*[D.;..dx...1....J..$....Rv....o.$Vx....q.d+.[...._.@J.+.....8.8.V.k.X.b.1.O.6.t.4.U.6.4.X.8.0.s.y.0.J.p.b.J.r.E.3.6.U.9.r.2.E.3.f.Q.M .W.O.9.6.a.....9.a.K.0.1.O.a.4.8.6.a.X.2.3.K.F.8.N.7.c.5.4.V.3.g.9.Q.S.w.f.0.8.f.1.0.....>..X..U...D.M..uy...er:.H..p.....u..(Z@.yDU,...P....y..L.o8..w..g..@1.&%..S..]e.K.E.:.. G$.....9.Z...bMo.fHVo?...,}...#.....#2;.A..V.>.zg]...A..G..v.^~..|....I....3.2.1.2.4.Q.s.M.S.f.n.....W9qRk.M....2o.R.T.~.q..<..$D.R...O-.Wc.m..B.....m...xo.}..$...S.2.?s...A5.9..... <.O.s..k..}.....W.5..... ..e.a...^7q^py.F9.+.$ef..4.xO...n.....EQ.#..)[.-.....qcO...+.!V6H...GYd.we./...I.....<.....f.G1q...G..\X;.+n.)h.....-.tL.J.O.[.....j^M..J..o...!.W.a..ug.Z.J.d.. .....1..wZ$.y..P..Y...W.u.&.....z,.gD9.f.1.*./....3...mdq..y.Y...^.....*q...U.'..T.xh.!l&n.{#.v._.....N....LD.....N.....F.1...}u/.9.u.S..2."8#./.3..^.Vw.....\..,!-dr7.p..".....P.KD..%.j..`.#.. (..._f..Z

C:\Users\user\77066510\vdxnbnfvi.pdf	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.496370279162565
Encrypted:	false
SSDEEP:	
MD5:	F35202D8C9FD1328ACF1397B5D6E9BF8
SHA1:	8F86894D08EF2AF26E3A3B4EAD2FBB4135FFB2AB
SHA-256:	5E088E5B883EB50CF8BB1820B6003D8B82DA35969DEB5A9BA8F606AB1E5F6DF6
SHA-512:	3C53300A425281738AEB6DF03D6B20E59A7BBF10B7695D8A8B2C91F9FA428D48F874DA546E9D78F65D55CD0ACE5E6225F00DDBD7A993FACD2131F6F9391513C 7
Malicious:	false
Reputation:	unknown
Preview:	R3PxX43qOZ6h9N0tl61tRS1zgm5613195k971wU9yt9H869R52Jo00jJ2aQm4l7KOBp5F0kp54PX23R1237A1LYF5cJ48Xs07Ru96QA5395KEm338f6tO2U1A2h7i117Ux 669wC8C3V94822mdor4p1mk..545F8uK74aqb377nRXmA4831jfo04K6jFIu110Hs6Ff2S8120424079q6z70mx24zq09911IDpt1..B8ipPqOgkg67Fj70492GPqSzm3M wKM0i9URKN73p5jtO49M4ZB4g623z9xY7dq490X20fEv23w1uy9CB6Nws4Aw317xhfSbV95BLN..KOt86Zqzh435E0W1R4c69uc9K2us56T7bq0Gv3L52AK2k038ONG7K1 7WQ2725Y..4078A0..x4ZCb29C800F227t9ou94GAg876eV4tQP2iUQPW1n..Nylcy1k2MW7..9405528E76s1L72oN539h5W29z6H4f33V4cc6JQZN8xc4M263371R035 9511Vv91BYO9xvY8916fS8zzj4L423915mB9BQ66L8fjzf385..

C:\Users\user\77066510\vdxnbnfvi.pdf	

C:\Users\user\77066510\xfjtfdxub.cpl	
Process:	C:\Users\user\Desktop\dUzAkYsvl8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	546
Entropy (8bit):	5.4988646271397466
Encrypted:	false
SSDEEP:	
MD5:	F04CA2A967FC764A36FAA9308CF33F48
SHA1:	A5C2DDB13912B1C5EF46B0BDDA7CC76031377CC9
SHA-256:	9343D1C8FF4B8D5D2B9FDA129AC44AA61F7B07BC5681C68088B997EDE440CFEA
SHA-512:	7B324450F41166AB33C26466DC8BFBAD1C84AE8B66CE38FF8C37ABD365A083738B3E8E9D1E5F05D68514B071321B29D45ED6E7D2009D4B13EF27F7876E937D0
Malicious:	false
Reputation:	unknown
Preview:	M493C155X97O876a58tcFb29B51297QOnbu322ar50o2q0Qqt6b2Nw7e117I05m2Qn38F06yYOl98..gc19QC66as81v853Wz6456Yp4lwl7x1LPo7W6tlyM63u2Av050g In32444T76..2cxJ7214JH9077dH92Mf18N6m4x1g86v3w9vGa9383T3sxqaV471e1WAa68de8qb36Hd57RGLHRf5TuuQXjAEXK319C6300Y2Fu9l248e13Px2fiOVBz0Y 2749h0hJ27Mw0587Jhz9LlVww7uK24pPlr2x5j32XY43xc104WLgqw66t1H6W348cYg0xm5A..822zg47hKqnh43Ss94E4BB9Km2yaX23vz472M9b34r2Fb42Yj336R2Yi 6z11N9097032p9dq1z955uCq76oLg28t..6Q36fg0a4yJ8plKm9e80Np01H66S2WZ8Zu140lS50fe8A98V79V8ejnC3NX7mf3437c19614l0j570OV751HLZk40m6STWSO T9dS80Np0E2a98wY18Z9Z6b3..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	
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:	
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\tmp1EC2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653

C:\Users\user\AppData\Local\Temp\tmp1EC2.tmp	
Encrypted:	false
SSDEEP:	
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCBF
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\tmp2720.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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:	F6112EADAC856DAAE9732D589993F43F
SHA1:	0DE653A9EA324DC51954C5FA1E58331AC7B8038C
SHA-256:	AD578EF8FC5B61D19BB496C0720C05E1FEF5D5B5EA8EBC40390D3D4C336DC4F8
SHA-512:	184F1EDB675AE8829090176439A63AA69E9CCF1B7040BD23938EFD3C6245C5DDAF019442F8D567E71CB4D9BB5E50DE74E0536121817E36C0C2E7D7670D8C6CAF
Malicious:	**true**
Reputation:	unknown
Preview:	.s.5A..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Reputation:	unknown
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\temp\hrennftnds.cpl	
Process:	C:\Users\user\77066510\cjlaro.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	82
Entropy (8bit):	5.0087305542018905
Encrypted:	false
SSDEEP:	
MD5:	EC8A6D0D840B97981D8DA9935499D168
SHA1:	002DCDC5B737749AEAC14B1B1F50DC83B05429AA
SHA-256:	2A33D572C8D852E5B135B7AC9F521FCF1E8CA030DEAF672594C180A7845017FC
SHA-512:	17D47FA260D6C06B9106EEDD92759B99DDFB3DF417D070B9BC28CB84FCCB69F258B350C5249D428595057AED972588D29558606B9611D43319B97736015E2201
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=Chrome..Dir3ctory=77066510..ExE_c=cjlaro.pif..

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.823508667946661
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:	dUzAkYsvl8.exe
File size:	1021780
MD5:	9a4a8643db95a8c0fe52af8675a5d1b1
SHA1:	c6beb75cbc168f9224ace74c0dcfb29df6197e82
SHA256:	b4e2d864ec03943310548bfbc963a0848bd08e088429c5ce05759face5d380d2
SHA512:	05d404c9422c2da367135f616a8b61b6adc68dc3f8f0b3a070f2071ec01de8c2aeafe5a63aea6e306fdfd299c43ef792efcfd9b555dcda9b3ff9e44872a8b4c0
SSDEEP:	24576:rAOcZEh5lwWkAZ5HrNUWTq6ai0bagi7vzJV:tWWbL1Tq6d4a5vT

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.../y..#...&...._....._..'...._..'...._..'..

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

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
10/11/21-22:29:37.142185	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53910	8.8.8.8	192.168.2.3
10/11/21-22:29:55.963084	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52130	8.8.8.8	192.168.2.3
10/11/21-22:31:05.092278	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	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 11, 2021 22:29:16.670052052 CEST	192.168.2.3	8.8.8.8	0xcd37	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:29:37.122045994 CEST	192.168.2.3	8.8.8.8	0xbdd8	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:29:55.940438032 CEST	192.168.2.3	8.8.8.8	0xbfba	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:30:30.033157110 CEST	192.168.2.3	8.8.8.8	0xda86	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:30:47.756072044 CEST	192.168.2.3	8.8.8.8	0xa386	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:31:05.071070910 CEST	192.168.2.3	8.8.8.8	0x8eb	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 11, 2021 22:29:16.686587095 CEST	8.8.8.8	192.168.2.3	0xcd37	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)
Oct 11, 2021 22:29:37.142184973 CEST	8.8.8.8	192.168.2.3	0xbdd8	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)
Oct 11, 2021 22:29:55.963083982 CEST	8.8.8.8	192.168.2.3	0xbfba	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)
Oct 11, 2021 22:30:30.051671982 CEST	8.8.8.8	192.168.2.3	0xda86	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)
Oct 11, 2021 22:30:47.775213003 CEST	8.8.8.8	192.168.2.3	0xa386	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)
Oct 11, 2021 22:31:05.092278004 CEST	8.8.8.8	192.168.2.3	0x8eb	No error (0)	strongodss.ddns.net		197.210.84.227	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: dUzAkYsvl8.exe PID: 6428 Parent PID: 5144

General

Start time:	22:28:50
Start date:	11/10/2021
Path:	C:\Users\user\Desktop\dUzAkYsvl8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dUzAkYsvl8.exe'
Imagebase:	0x1f0000
File size:	1021780 bytes
MD5 hash:	9A4A8643DB95A8C0FE52AF8675A5D1B1
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: cjlaro.pif PID: 5028 Parent PID: 6428

General

Start time:	22:28:57
Start date:	11/10/2021
Path:	C:\Users\user\77066510\cjlaro.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\77066510\cjlaro.pif' txoxpdjc.qnr
Imagebase:	0x1130000
File size:	776432 bytes
MD5 hash:	279DAE7236F5F2488A4BACDE6027F730
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:

00000004.00000003.315424551.0000000004EA3000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.315424551.0000000004EA3000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.315424551.0000000004EA3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314549221.0000000004D88000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314549221.0000000004D88000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314549221.0000000004D88000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.315994973.0000000004E6E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.315994973.0000000004E6E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.315994973.0000000004E6E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.316144236.0000000004E6E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.316144236.0000000004E6E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.316144236.0000000004E6E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314585596.0000000004E06000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314585596.0000000004E06000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314585596.0000000004E06000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.315927794.0000000004E06000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.315927794.0000000004E06000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.315927794.0000000004E06000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.316303784.0000000004DD1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.316303784.0000000004DD1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.316303784.0000000004DD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.315764008.0000000004E3A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.315764008.0000000004E3A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.315764008.0000000004E3A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.316393189.0000000004D88000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.316393189.0000000004D88000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.316393189.0000000004D88000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314529331.0000000004E3A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314529331.0000000004E3A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314529331.0000000004E3A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314683885.0000000004EA3000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314683885.0000000004EA3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314683885.0000000004EA3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314613880.0000000004DD1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314613880.0000000004DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314613880.0000000004DD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.314455197.0000000004DD1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.314455197.0000000004DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.314455197.0000000004DD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 56%, 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: 6364 Parent PID: 5028

General

Start time:	22:29:02
Start date:	11/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x120000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.560410383.0000000006110000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.560410383.0000000006110000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.555314514.0000000000502000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.555314514.0000000000502000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.555314514.0000000000502000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.560490990.00000000061B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.560490990.00000000061B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.560490990.00000000061B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.559058243.0000000003A79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.559058243.0000000003A79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.560258652.0000000005630000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.560258652.0000000005630000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.557771680.0000000002A31000.00000004.00000001.sdmp, Author: Joe Security
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: 5252 Parent PID: 6364

General

Start time:	22:29:10
Start date:	11/10/2021
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\tmp1EC2.tmp'
Imagebase:	0x10d0000
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: 6612 Parent PID: 5252

General

Start time:	22:29:12
Start date:	11/10/2021
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: 1240 Parent PID: 6364

General

Start time:	22:29:12
Start date:	11/10/2021
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\tmp2720.tmp'
Imagebase:	0x7ff70d6e0000
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: cjlaro.pif PID: 2132 Parent PID: 3352

General

Start time:	22:29:12
Start date:	11/10/2021
Path:	C:\Users\user\77066510\cjlaro.pif
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr
Imagebase:	0x1130000
File size:	776432 bytes
MD5 hash:	279DAE7236F5F2488A4BACDE6027F730
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 6432 Parent PID: 1240

General

Start time:	22:29:12
Start date:	11/10/2021
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: RegSvcs.exe PID: 6748 Parent PID: 664

General

Start time:	22:29:14
Start date:	11/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0xf50000
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: 6828 Parent PID: 6748

General

Start time:	22:29:16
Start date:	11/10/2021
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: dhcpmon.exe PID: 6836 Parent PID: 664

General

Start time:	22:29:16
Start date:	11/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd30000
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

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6816 Parent PID: 6836

General

Start time:	22:29:17
Start date:	11/10/2021
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: cjlaro.pif PID: 7152 Parent PID: 3352

General

Start time:	22:29:18
Start date:	11/10/2021
Path:	C:\Users\user\77066510\cjlaro.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\77066510\cjlaro.pif' C:\Users\user\77066510\txoxpdjc.qnr
Imagebase:	0x1130000

File size:	776432 bytes
MD5 hash:	279DAE7236F5F2488A4BACDE6027F730
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: 00000014.00000003.359982101.00000000048CF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.359982101.00000000048CF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.359982101.00000000048CF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.363952559.00000000048CF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.363952559.00000000048CF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.363952559.00000000048CF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.363022584.0000000004938000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.363022584.0000000004938000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.363022584.0000000004938000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360137256.000000000489A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360137256.000000000489A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360137256.000000000489A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.364780852.000000000489A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.364780852.000000000489A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.364780852.000000000489A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360433850.0000000004903000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360433850.0000000004903000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360433850.0000000004903000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360821611.000000000496B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360821611.000000000496B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360821611.000000000496B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.366099101.0000000004902000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.366099101.0000000004902000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.366099101.0000000004902000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.370237585.0000000004831000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.370237585.0000000004831000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000003.370237585.0000000004831000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.369728872.0000000004866000.00000004.00000001.sdmp, Author:

Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.369728872.0000000004866000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.369728872.0000000004866000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.363076349.00000000039E5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.363076349.00000000039E5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.363076349.00000000039E5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360037831.0000000004831000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360037831.0000000004831000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360037831.0000000004831000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360563466.0000000004903000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360563466.0000000004903000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360563466.0000000004903000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360697455.0000000004938000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360697455.0000000004938000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360697455.0000000004938000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.366655070.0000000004902000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.366655070.0000000004902000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.366655070.0000000004902000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360273834.0000000004866000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360273834.0000000004866000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360273834.0000000004866000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.360354824.00000000048CF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.360354824.00000000048CF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.360354824.00000000048CF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.359604202.0000000004866000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.359604202.0000000004866000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.359604202.0000000004866000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: wscript.exe PID: 3460 Parent PID: 3352

General

Start time:	22:29:21
Start date:	11/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\77066510\Update.vbs'
Imagebase:	0x7ff63d490000
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

Registry Activities

Show Windows behavior

Disassembly

Code Analysis