ID: 501918
Sample Name:
gNFfZ1w8E6.exe
Cookbook: default.jbs
Time: 12:11:21
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report gNFfZ1w8E6.exe

Overview

General Information

Sample Name:	gNFfZ1w8E6.exe
Analysis ID:	501918
MD5:	664d73b23eddfcd.
SHA1:	36fa060dbc14677.
SHA256:	e88b591e50dc77..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

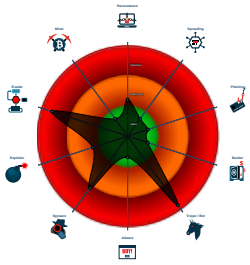
Nanocore

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…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- gNFfZ1w8E6.exe (PID: 5500 cmdline: 'C:\Users\user\Desktop\gNFfZ1w8E6.exe' MD5: 664D73B23EDDFCD0227786B9D0F5D022)
  - ahmrqkljvd.pif (PID: 2116 cmdline: 'C:\Users\user\70020325\ahmrqkljvd.pif' iwqnllkpjb.jam MD5: 8E699954F6B5D64683412CC560938507)
    - RegSvcs.exe (PID: 6244 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 6304 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpEBDB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6420 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpF755.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6428 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ahmrqkljvd.pif (PID: 6560 cmdline: 'C:\Users\user~1\70020325\AHMRQK~1.PIF' C:\Users\user~1\70020325\IWQNLL~1.JAM MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 6696 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 6572 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 6716 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user~1\70020325\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- ahmrqkljvd.pif (PID: 6796 cmdline: 'C:\Users\user~1\70020325\AHMRQK~1.PIF' C:\Users\user~1\70020325\IWQNLL~1.JAM MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 7128 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.534249648.0000000005D50000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
0000000E.00000002.534249648.0000000005D50000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9ed:$x1: NanoCore.ClientPluginHost • 0x441f5:$x1: NanoCore.ClientPluginHost • 0xfa2a:$x2: IClientNetworkHost • 0x44232:$x2: IClientNetworkHost • 0x1355d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47d65:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf755:$a: NanoCore • 0xf765:$a: NanoCore • 0xf999:$a: NanoCore • 0xf9ad:$a: NanoCore • 0xf9ed:$a: NanoCore • 0x43f5d:$a: NanoCore • 0x43f6d:$a: NanoCore • 0x441a1:$a: NanoCore • 0x441b5:$a: NanoCore • 0x441f5:$a: NanoCore • 0xf7b4:$b: ClientPlugin • 0xf9b6:$b: ClientPlugin • 0xf9f6:$b: ClientPlugin • 0x43fbc:$b: ClientPlugin • 0x441be:$b: ClientPlugin • 0x441fe:$b: ClientPlugin • 0xf8db:$c: ProjectData • 0x440e3:$c: ProjectData • 0x102e2:$d: DESCrypto • 0x44aea:$d: DESCrypto • 0x17cae:$e: KeepAlive
Click to see the 179 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
21.3.ahmrqkljvd.pif.4612068.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
21.3.ahmrqkljvd.pif.4612068.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
21.3.ahmrqkljvd.pif.4612068.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
21.3.ahmrqkljvd.pif.4612068.5.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
21.3.ahmrqkljvd.pif.45a9c50.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 202 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

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

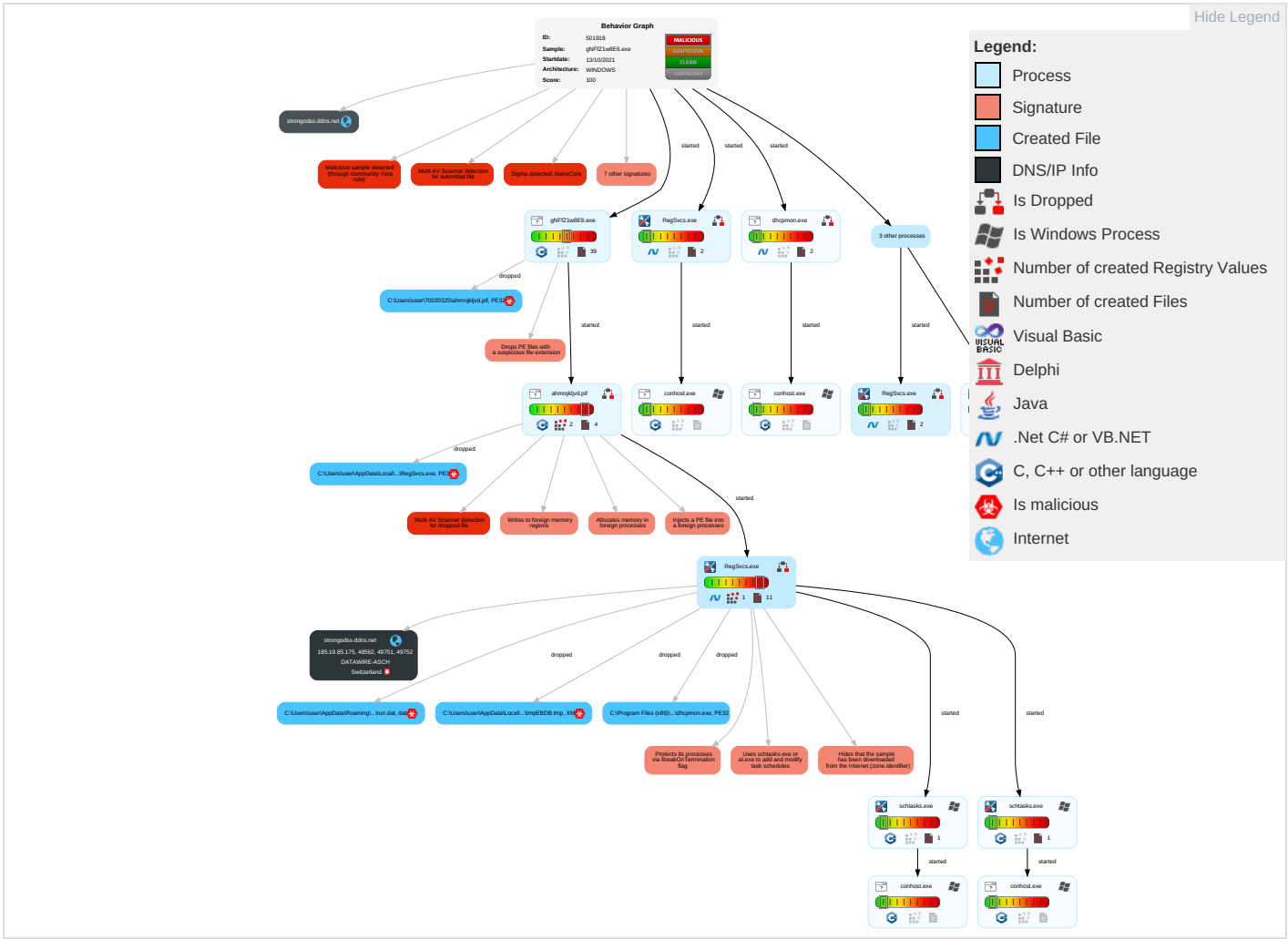
Yara detected Nanocore RAT

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 2	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	Query Registry 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	Security Software Discovery 1 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	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 2 1	Network Sniffing	System Owner/User 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	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
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

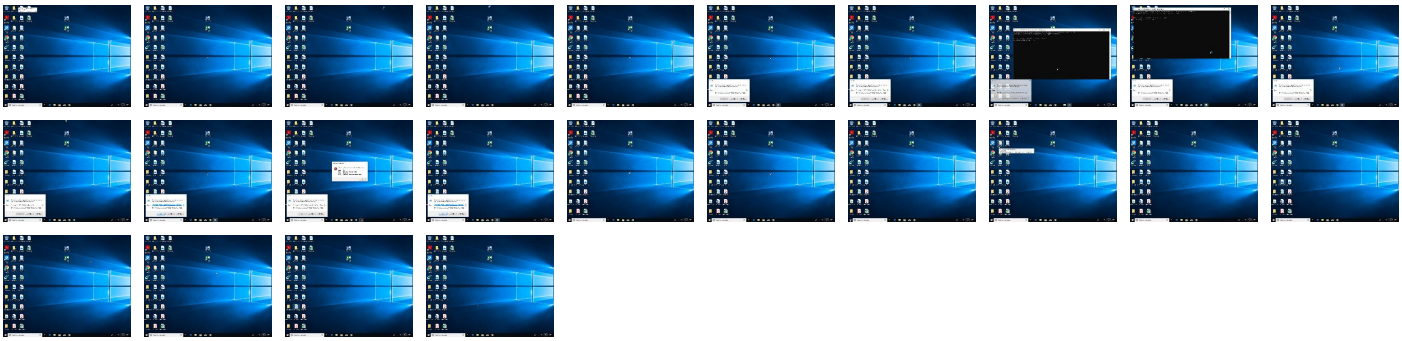
Behavior Graph



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
gNFfZ1w8E6.exe	44%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\70020325\ahmrqkljvd.pif	27%	Virustotal		Browse
C:\Users\user\70020325\ahmrqkljvd.pif	32%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.RegSvcs.exe.6c60000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.RegSvcs.exe.900000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.2.RegSvcs.exe.d20000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.RegSvcs.exe.1020000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.microsoft.cFF	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	185.19.85.175	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	strongodss.ddns.net	Switzerland		48971	DATAWIRE-ASCH	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501918
Start date:	13.10.2021
Start time:	12:11:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gNFfZ1w8E6.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:	40
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@22/48@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.1% (good quality ratio 19.2%) • Quality average: 74.4% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 61% • 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
12:12:50	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user~1\70020325\AHMRQK~1.PIF C:\Users\user~1\70020325\IWQNLL~1.JAM
12:12:57	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
12:12:58	API Interceptor	745x Sleep call for process: RegSvcs.exe modified
12:12:59	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:12:59	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user~1\70020325\Update.vbs
12:13:07	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:\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
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D0B42
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • 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\70020325\Update.vbs	
Process:	C:\Users\user\70020325\ahmrqkljvd.pif
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	345
Entropy (8bit):	5.308151029035932
Encrypted:	false
SSDEEP:	6:FER/lFHIe36iUrNe3yrr/lFHIe36iUrNe3yrr/lFHIe36iUrNe3yro:+R/ver/ver/veo
MD5:	7D1DECD7AC1B792B4FAD2D52C1E1C197
SHA1:	C4DF85F5B61896AAD894123867134ABBF7E03E3E
SHA-256:	72594DCCD9AD5823C2782950CC655278398866E85EABEF119136A42972D80C4A
SHA-512:	BC17FEF1C7A8039430C73BAD5F802D8E910D65BFA2EDB08764B1082747718CBF17533E9396FA43B7B22E2C61BB0BC1CD51A9F2690BE21BDD2A7970047D72B1EC
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user~1\70020325\AHMRQK~1.PIF C:\Users\user~1\70020325\IWQNLL~1.JAM"CreateObject("WScript.Shell").Run "C:\Users\user~1\70020325\AHMRQK~1.PIF C:\Users\user~1\70020325\IWQNLL~1.JAM"CreateObject("WScript.Shell").Run "C:\Users\user~1\70020325\AHMRQK~1.PIF C:\Users\user~1\70020325\IWQNLL~1.JAM"

C:\Users\user\70020325\adkv.docx	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.467807598701544
Encrypted:	false
SSDEEP:	12:AIWtH60J3/4JIR0K5rytcEAkfk4teIRsVcNEAxKuMC6n:yJ3/4Jl+kcEz87CNxHMCk
MD5:	B9288284091790 85F1FE218BFF33B175
SHA1:	FC25671245A6E8B18178D61A00B266DC5A3235E1
SHA-256:	9017D3DF294B41F9CE4DF9D7FE9A2CAE165AE574AD3FDAAD02800D0EF26D5EE3
SHA-512:	BE6AD99EB8D3EB35E6A83183FD04F8364301A0CB55A8888820DE16F99B75DE146D2FD1D14E003A72959835549D534A0840EC4EAC25490BCF9D1B84CDDA3C268
Malicious:	false
Reputation:	unknown
Preview:	u00C194921e85351Ze7k3814K64Q1P8220030Qb1tm..iu04i355hZE96069h2BmwQJ29IE204L085nk5MV5KQ1m6i9WUol2H1lJvKFL09x4Q8c2f77f2W551F1fl56l1S5xr6AbFYUFeI4..74J4kwOoeldHOgO10n2jNcKU709s00q8Z0T211827Q632Olh005T81G76GG2T4w6Qq3D6G4T3y996kVhPcKm4e434481T8mp48h2LZTC937x5jfE6oU08a094TH357CoHk525ZFh70YA7..265v25LCrIQ8vi79VA45011Ku10bw547FGG8a3H4uryLQ72g31M8HaxIxq47uF961L7A2K..84C3n65P4Q4D5Kl0R485Sj79bu5D6c6T512aY63h8R045OKGj2o17ddg34f93I7U95I1V2qCiZg6598VzW6DF8Q7s65Z742T7wuy84L81EGn2nMm1W2fj49V50A1s4U..0O6D9Qo2A5ty6q2c..

C:\Users\user\70020325\ahmrqkljvd.pif	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\70020325\ahmrqkljvd.pif	
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: Virustotal, Detection: 27%, Browse • 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....."..... .....d..... ....@.....0.....@...@.....@.....T.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...H.....@..B..... ....

C:\Users\user\70020325\aqdgdw.bin	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.509016351124897
Encrypted:	false
SSDEEP:	12:SPQVtjPUI+A4UbNPnsUxw000Znso/AaGlsEd/k:vPUYZWBxH0aak
MD5:	E72413DA62FB434DB9693AE96AE2AD95
SHA1:	AADDDD4B5E894AAEB4C2C67BBEEEDB8F818F7B0F
SHA-256:	DC18B800AE763C9B92D198A763138EC9001D1EF07E97A207DAE3F572D71F954D
SHA-512:	E1900A1BEE8F3D7FEC7C42F1CF384C89E99B9EE489A082D19EF4D4A4C2F7B8F7361D199C963EED4DC2F1E3945EA82D7D49D32F13BE383777202BC3582FADF7E
Malicious:	false
Reputation:	unknown
Preview:	681578N7fr61kZxKd2IwPBgpQ73639Q3Y3B47156QiZt17GFK308CkR09vL2..eOJN32050R4FMP7En7W86BR6XIu032HX5pyf1B4TM2J50nB03BvX11lN6k9Ic24fx482 L87XeLn03W5566R37H..1r92i03EGbD4Y1y90rgp94ZT6303gT7dSa305A32i8L59w14vE78770xg2V721D3j04AKp13PB4I784b3C7g5Cmn65i76g7334d8q5EHWILn1M O71N5500dgY2uF43kzN9W..hw12528n7Q966q0z3UA0wbLI4p7cTB89YD55896nDmK15H5gFE157bu77Gy8WAPs79y959BC0B47uD1oExe1R4Yemwwo4YJQ6 w4b0C..qM92h0r003O7x10S4pG822Gzz000N3Y92I6o03JP038HspWn4Y80kr641hV5N2uMZmq38Q3O9..XA3865MO77wdeNML27683E9oVM511zC9QRR7fv 51m5xF8IvU9394Yks1953757Dm0qkA..

C:\Users\user\70020325\aqxh.ico	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.521875197418181
Encrypted:	false
SSDEEP:	12:UsHwJ+BlZ7+kQo1rgT2qOjE6xNcdIm9RYNWRDqOEGm1H:U6wslXVcOjHN69Gx3H
MD5:	255A60E333ED4F2B51BC44C621E77D43
SHA1:	4D3518CDD5DCFC42B5E8FF0579BA9C20C7FD1D33
SHA-256:	3C942FE54BEF33704A20B0A1EA6274EEC1FFE107DE5036C8A2635C53E4A978FD
SHA-512:	BE867FED4399919A44030A457F2CD3B553D7AA4249EEBDA19A82E539C8196A949AC3EA32A78060695191190665088F51D4436819CB7E7E2DF1C6D3B5332C1DD5
Malicious:	false
Reputation:	unknown
Preview:	E44Ubl31EBEStZg6fkc2530H0044U6y0BC336z371bAehojl9fPDJ51772i752Zmy349a4h71s32i89kKqV44Lwjx8a75OaZO7u9E0vH2AfJ6317yu5jLyx2kl5Ki92Zvi G64mbdT6Czn6t97..ZKp4dams480t72w8kV66y0zhY21uF83223l7piToHdc2lLRe65Wsf83WTc842SdJk793ky3MmZq1r6X317G86p4J0b03p1c52R1vJ74B168Fp9f75 4sXtEh5A4h753353483zxeI00j8..stY6b8310S5..99wxxh02u0mbR31S3N41jB035500SgNeMCX4A85foW9h1z92Y6u775wWO4Pf8E775304X3U103p..JgcW4f4631B 2v333qmxFI9t19fb36h3Ze3HMALN5U99j40S3M34Hx75aAB263ZoL1Kv8h0Y1n0L84iU73119799c72P42v3P6Whl82UIT..tz3f90dUP142eG..

C:\Users\user\70020325\axdhk.pdf	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	521
Entropy (8bit):	5.515219594640504
Encrypted:	false
SSDEEP:	12:PHUtHsWxVLooUTVNQ3fd13m4+EKhHQqQCpthIBIbch:QxVPUTVIfdXIVPQCmBIbch

C:\Users\user\70020325\axdhk.pdf	
MD5:	7C52B84BA4C7AD8683DEEF42CB0CE98E
SHA1:	E52BE80A81E1F0C4C93248F5D49D1E4E07BD04F4
SHA-256:	DA31F949FB6819B3D3B214D166135BD78BBA020B6C7560D76D8F9FE28A5F1FBA
SHA-512:	C8CDDE75676E75263221F6FA5464B140DB3F0901A5F11F88315470DDB82F5EB8D166A5A27FCEF67CEBA1150D37AE0CFA2CD589C43EA9DB04AB2B41ED3988B896
Malicious:	false
Reputation:	unknown
Preview:	43l9f046YJrr43mAXd8716bTnw1WZq81J7R46M8f00944585..z8Z980kpTjX1..fy968i60K0iA4i2E47zME35aHhLd8t5o30zp647Zs1U1B0I1it1G81F9Gt4IWT7379 4Db0y7cdlH0tjXH6V0UMwe1G0jK5O5933..yV0O46AeY1gX81u8T51X5R2a6nOM1gZnuyjWJo7z6013x81172ab40Jt4DA4ij0R1yFG5Q42c5lG38j521qM5Zr3H..JO89 Z2cRHP0H68t710q70v75oYKrCpN25o35GMRVk7477W32xvMn1p155MtUVw1u..3Ui4ed1b135M9lpTLFgGy47Do21691q1L78Il5959939T4JGT925U64PvGI6xrBE85D8 u108z..u4tjRS023OOj7XD57vS21M8o5f6L5c93CTOd45Eh7X4rjQz38333B5H78626c21X630L43d40246ue1rd3uJrK47Hd34z13mp0Y4P279v4U4quZkt2x7l5T3i7..

C:\Users\user\70020325\bipbwmq.jpg	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	578
Entropy (8bit):	5.510614564463693
Encrypted:	false
SSDEEP:	12:U2muSfA6EhdkOvMTtzlRdxBw4EfovHzGHz46Ci7tQ+/QvTOkpPJO:U2VsGAaMTtzpQfovCH0c7G+YTFPJO
MD5:	B8BFB09FBB1348AFCE8C54BAEE7E325D
SHA1:	22376B584BACD89E4F1F9DADFE1A95C0589F52E4
SHA-256:	68DA8827A627033CC73B52F1FCA453B3F3F552E85BBED31678592D7CC087D042
SHA-512:	C039022744F5ECCCBF3982D409A0662B82411241176963556 88E20DCBEACDF10552B780196FAC466D6C376C3B2A24F687A0E01DB9913121475B181975706F617
Malicious:	false
Reputation:	unknown
Preview:	d4f4465IsB2TJ7c988K5M9OC1607Oa15QLiZaU2NW9969o7Sd34g56Wb5Y1n2eG635C51N6z46R723uMzz89GLy369Ach3XU927OF7880wfa74867102cz8W9..j24qOn7 c0G61ru58CKQBdo86D2i7hVAVP4mPNXi6bnh4N2cGx0897t33705E5MZ3fCOh8l1W7yF4B9v627650KZzJkt7k65c824s74252AB515R20Flz20m79dg013Y2H952EM626 4uT66BzAMv10P0S6VklVkGq5..rFtf6zEO597EH09j3lVgl627UCpE3F4S6b31b8d41211w7P0bN07c62601a08b9JlG3X6XrK7h286Tluk9nQUcI9F60522xQ2G379rI8 JiE0oN3..a52WaT7XX51O40Kvsl72..w5o7Ghg27pwnT9TT47GwdK8L236hU0oiW8G5zv128RN5Q7RBN3352n9f124i28LQi6lk3725L1p2e5Wm6Iv6kqQ3zZp7Q6U4678 354ClM411p418s408a6B6vL4RJPpO22om0sk0v5CJ98114237ZTcBwLM..

C:\Users\user\70020325\eamjsiij.txt	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	5.428296171556631
Encrypted:	false
SSDEEP:	12:lXhjdXg+39nhTafOLycxRMUxnxhbh7tlNBTeEdlWyVc08KnFR0czC:rjNgENhlL3xZhxhbhxbVc08KnFR0uC
MD5:	77138125664D1B6EBF47026EC6C398E6
SHA1:	2773427DB6580C6CAC92C398E9D8636D83F27AD2
SHA-256:	2083F0AFBF98452B3EE24EB7D512BEC0C415AF445055E428949430C962F2827F
SHA-512:	FB76274F580766DE18A7619DE659C01548BD94390169B3BE2A83C94AE246979F5C740F2231FE99B9CA1E58171C6DA1EC2338123C3A72F262A2A5E4D99CDA4716
Malicious:	false
Reputation:	unknown
Preview:	3X717SM2t2779A467iZqq200g6j51wuEUw5IB695b827A5vRvbW7MGX356b7t2H87..41Z22K063xOVeYVZtg5CKJ41AgLfh84CW9Kv4c9l9102D709vF4QA14bQe32505 61IJM5570s59sa94d812T111aC4Cv3xP08kR9824MG3YP4u930Q52w0R2F5s4A9MsAn..z46dT4600tOTypoh208G52W578M080811P891738GzmFA2ca9B84ZTjt94R8. .VZA3B70uAgH45J8CRGBT2h9rU5i825W44J409p56S9Pw9987V467v27995J2K28Y11Dn0uPE964Pk84Wlt7j9h82Qne1238z0J97Et3..54pL..Zj6wn8UqB6hjf867Mz 066A9p3eT5JH1U10T29717g4H2jv5I8m5e1m38l87LF8837E463340G8Tp583m3h2K8xO4Veg72edI374ZRlp54R1zMhMRUon8r..L86l8M492z9X717Kg34dEvH9073vt 23se47cY7n61sE5951G17t9SUmYDBJ7I929v281nM2Tt48..

C:\Users\user\70020325\ellqkdupx.mp3	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	573
Entropy (8bit):	5.549359702680056
Encrypted:	false
SSDEEP:	12:yXV/CSQrJM6HyRABHP3W2Td3de9EvCliF:uV/Cj9MuyuZ3de9EUiF
MD5:	8B6174B8BF54379C012297E9E89068CF
SHA1:	B06BC45A2264F1D83E88395C4D978C1406C3D12E
SHA-256:	1ECF51B93214B63D220BEA83D37156C883B03C443AD00C0A3442944F161EACF5
SHA-512:	E323C5EB438C1674D21E5E3474648D68D39AE3AF1BBD1D4D2587240A2C28F02C0BE60D87E81A1D42B766BB16D50BE5E95CED80282BA7F37E1B41540510750F8B
Malicious:	false

C:\Users\user\70020325\ellqkdupx.mp3	
Reputation:	unknown
Preview:	6Yv85S5iM44ob1UhE3557981z3cU09j76FHOrf3e367T77r..mQfb711kG7668P7op69pk53f8S776..1rv1Hr32CrOV71K6Fu4kxkaGA5t59gHK426Z2L51zl..D53PmD 8h6hn099G8bTVd011Vlf3yR58sYcD6VcZr1WXL869EB7Pnk34F1gc4063h11uK3x8Qz558nO5vLL3NWay6l1NY4314a75xl57x003A6G06xbov3g..j883abcA15G3..8k 8H20OIsO3y..uf2aM7H2SD17C2e459i2d08R0qR977YE4GXwTDgyP1qN5hia8X49hI7244q5864Y0FD1bw71z83u3J89Sny47cabgZ1..4u97E5RI2y5Z193G2Ur3OL5rp p1ULGzmH6v1oDXz4F..pI8h9s80cs4v8560Sz3jIo2KU392L6I2v432L0O63to3IdAVW6v0m3a4y873A9IKS3N46mv0Xs0h98Z7qZd31m0717483349DK44qWxUo10V3L9 78xja3lmwu20763CyB8j496h136c9t213A45967wR10gO0nO79n..

C:\Users\user\70020325\feqe.xl	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	585
Entropy (8bit):	5.389583094307479
Encrypted:	false
SSDEEP:	12:knkvHeHOMppV5BvhUEYGkQBhtEIaFbiRD2xVBMPFK2TnsRej:fH6OUpd5UE7/tEIadiRDMBWFK2IRej
MD5:	7DD966009473E2F50850D079D3469D3D
SHA1:	EBC324512C7A650930A184D7197D5D1454D14CF1
SHA-256:	CCC6652028E048B6C2D64DD5FA0984D86420F4C1C8E34245E81B2B2ED0DA49A2
SHA-512:	2CF672F503616DE3677215AE8D1B8A4E36682A0A33B0A09A7FE69B724979E48E48D53F75E85F36D1BCE18BF91014FACB0D3D88992A321345EE19A5589F45F844
Malicious:	false
Reputation:	unknown
Preview:	726V5g3mQ1..W5O7bj637J33o6452W8C95J5pulU7nQW2Lcy4L58h73L465295xk236C23..qvoDo7z81pC4848DnINOBI7I5243977E36BvOz1r4ll0i93Y4Zw324bWl7 9Ki1POz3u7q97hV942..072o6109V2sH8664NNxWsz874qqWg922UH8IpLUjZB73216Vpn78u0KaVBHS513PG07oM7q973rSKs52l8MnvTS7189v277b4pkXA717..bDrC j51I98Z377ry9980U1Qm83ws1RI2GI72yVk7Q0..KZ5589L8ZN2q515682BMG9pEO6k95f880011V9b7vj2E7IC702UG8O..bO57k07j282y5434h42B50MMvYi06H8385 72856X4732mm9sXvk49d61Sn1832Yh26..869R50531259r9CCfYuxmA08v0A4l37r8xkTan93Bv212DW2Hf95YIt17458h9V0r8M8Xj8c1bB2r28gr1k5y7W9c272008m Ob57f3e5rP3259217244onWCD60oN100C3wS9S46aeD9V277K9cs3705560Z1Ys..

C:\Users\user\70020325\gfic.dat	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.455348901983325
Encrypted:	false
SSDEEP:	12:yCjXsByCjtPqxK9Q35ozzO5h7zgQKVJv1Fxwq+Vk9en:yCTsByCRCYw5P5EJvGq+VGen
MD5:	6651CE63AACAD3553A63BEF115AAA1CE
SHA1:	1DB11D135745230121FAB228D09878B05BD97B50
SHA-256:	3803789A9B12401E983A4D2E3B5BABC791E58D7016ABBF8DCBBA18639811AC67
SHA-512:	9C0CCFB19A8351BBB181F617CB2577EAFF50FE8542332DE5327FA7630EB650345C70704FAD750E086F93D7FC6AEC17F08F3B6B71318BCC3ADC6CF75F0788273
Malicious:	false
Reputation:	unknown
Preview:	034947t5PBs054s38h229N09IXNa273276l774K1534IR1B4SoH3q8YVd1gj62F4Pl373IT5j5Xv43zS4SZ2XBb926MsZ8w4q5..r658ZD6fC3mE37crE7Vs3397Hbf154 6S7E36FR169c910774x3v8677Gx624Iz3GG9Iw62AQ58XcD0f32MABJ80I6559ba37NcKN247QBUa0Y6579MH0WCCAh3ui3196fhA3690547y25Qg506E3rZJ204..29qz a2EQC7yCq34I222kk0bp99i49g77n6g4Ft246..BZ85sY57N834a4R9lbLUkt7s1Q9am74FvS5XB7329zSS7jfoXrGLzLE50Ay26851m02n66309..052e..N84W7OqUvN e823fQQ751D5GqC925tPnLR0x9CZ438UhV339288882eT2u8C0E0cXw4wQs01VsMmyP2B30Y35V8R47q533X9E6GS8a..P6004lfV59z66AQO1E1Tm355dmH7t4hL..

C:\Users\user\70020325\ilkrn.log	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	606
Entropy (8bit):	5.462706321666347
Encrypted:	false
SSDEEP:	12:Akb/FHoqn59litp0iyJZ9Pp3+HgNxygz4SxX+aBYeoCi1r/x4ZVd/v:5N57MJZ1p7ygsSxua1f4C/v
MD5:	7083B5AB02CC094E17A6EB3CB0EC9190
SHA1:	9D7CF2FD6263FE8CA7B6E3BE35FB4E178860BA61
SHA-256:	6407F8DED2BB5071885F2000875E7FFBF84217DE4901CE6FA610A84F5474A6E3
SHA-512:	9AD6394ABCA1686B01EB4F101A8D2893A6E41B0AD162ED846DBF74EADCD3DEA2E1B0BA2D2EFB264C9B0A899F2CCC24D0528A71A7863809287B0A340B805703 B2
Malicious:	false
Reputation:	unknown
Preview:	nw780Lwz6r85259mw1051AE4iw3ul8s303l4vIAc020c70A69657qrD5p37..k0906a26SGq4JS32N..R31W9z236P24nZsX2Xp82Oj3Lo8lr84I96w507M8qMS965kI60 62Wk7l309f47QC1rH355J0c62xQW5m5nY93JC15d7u58349606r05o55IKa12C59Yco3099bxa0a81U78eXv..h7XT0O7n1x881fc2z29844KZ0k3zefuh45Vd381T8N0P e55D9b9437UaOfqrDt467y5z49X9t31r80pw32s517nzs9H4052ak30N9D9i7v4XY0d..km1W8z0hKx904B94g6jR8EGz92w24R15j195sK4V3y76q45..yZAvb1He3Q7T 19E7281Y47VQ91109FXT0vxrBO36N662R8705sdb93W87HD0mL52o01Q..uWMd10Fm5X48kI9IG14128X6906zZ7qV710036o9Kr26S12T21Xl3ifV1p2vKlC5KB8m83M4 CqkDA90eJ544C71K8FG000N13Auz00l47Hr5EL51cw7704N7RO1k19Ktcix315Z45j4lxABUTz5J7wxiXM18..

C:\Users\user\70020325\iwqnllkpjb.jam	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	data
Category:	dropped
Size (bytes):	163580716
Entropy (8bit):	7.07026660273868
Encrypted:	false
SSDEEP:	196608:JDfvcKYrzoj7FoISUgHi2FB0FpNaLmzQVD3/sSkbPbCfKspBiZgl2REVxiu3yGUU:8
MD5:	0FFDEA02D408BDE28E08909C0206C2C4
SHA1:	726F64E817C65918F321FF5E548A2377D5F6EF39
SHA-256:	F2DDEB937A452CE93A1FEE1224573CF31C346B5F77589170DB125B7815EC3C18
SHA-512:	D6B77AAA2C9754F58A7CFAA24D463EDF1E9139F78550F5B8C7615720DCA65E6B059FFD4BE7B468E7A3BD2607A9E410F8B0CF43A286B5F82386BF9AB8E8CDA12A
Malicious:	false
Reputation:	unknown
Preview:	..;..a...oO@..G.,}W.gu.H{...`h}..VEK45YI....#.c.s..i.?.....Xt..B.9.eFJ0.....3....S..#U.....+.._...i.*.Px..0Wnq...H..TK_A.....h..^.}w.....k.,..{P.q.K.Ut..V... 6M...0."V.4...=[.P..Kd^...M..W$.?.*I8.E...$...`. ..1..%.....{Q.j.l...*.."8x.....3.W.d.n.F.W.q.V.o.9.1.4.0.Q.3.e.q.u.0.1.2.8.H.....p.2.nJ.i.e'O.. ...:8..E*.pk...{0.+.....!^.....5.._.x!../...!7..ic.|7...Z5!. .#n.v-...R..3...!.c]._.....:..7...a.._{.8...2.....U.Wn..;b...J. _.%..N.y.....qx....w..M.|WjS.....3.4.b.3.f.6.3.0.h.L.E.0.9.0.9.1.M.T.M.7.U.5.6.m.9.5.l.y.r.J.i.8.6.d.3.3.....8...?o....@-c..,...^.c..%#V'..F.Ek.....\.}`.....0.4.w.a.m.6.s.3.o.8.v.9.G.F.x.8.0.9.....Y.0.k.3.6.c.5.i.8.s.2.7.8.J.1.Q.l.1.6.K.4.T.v.y.p.7.5.3.n.2.O.4.w.6.3.4.....;9svP...3<....[.sN.sD.P[O..4kL.?...X..rN..(..).o...e=^oo"..N.....r'T..H5.Z).K.....S WN..!]..F.R..v....d..>5D(@....^.....La.'\8.t.`.<`.....T.Y.JPV..XMJ....&..f.....?.C...!.fY.N....&.....A3>...C.L.>....4...,.i..d...y....[L+W1op....G....Li

C:\Users\user\70020325\jejniughm.eqr	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	430098
Entropy (8bit):	4.00000785267426
Encrypted:	false
SSDEEP:	
MD5:	2CCF7CA13CB8CF224CCDA4A8CCD5B451
SHA1:	F7D291CFE135DEA0944C4660AF9F24F0EEF588EE
SHA-256:	85C02BE42957AA4639AE6988B3CB6438C9F1AC28DAE0101378BD4E6C63DAA4F9
SHA-512:	D92FBF5922D0EBD7EB04BA2FBDD12768160466E883C8ADCC432AE05D388C5C73A2061C3F06FBC8C988F14E78043993048AE2B8DFE6AB99F2F2308B86D679228
Malicious:	false
Reputation:	unknown
Preview:	C67A7E2611A06FC1EA195A9C924E09069A23901F799C5CCE664790D7DA4F377B988913D06874AA50BDD17592F2A337197B77192D8822697BF3804970 E30C7280D4DCAF2C7CC76471A2A33041C5C130E6AFA5077A86F8499673104B31800EEB2B02566828E07BE200A0B5811FD70C76471D8CC36B7B641CBC C23067C620FC67B9D6FB164BD8BFBDEEC9E39028BC89F987D18CCB70D27049ADF82B355BEDDB7177F0D356F68F7EC11531519FF7EB844B324B3F7150 47AB40C09904480A174EC038AE9624CF1FD1448E6047526DAEA745372705305B6034CDF1DE57C593AED70EF4AF4368B462FD68DCC4BD7FA14019CEB1 A79A5462AF4EF0DE653ACFEF42AFEBEAF9972E15A4BAFB83972716F09882F41F91DB03660D671D08CCAD40EBC109F20C698B449F5D00E3A1FE708BD0 01877075644636D2B28F29171619D7CD41A029B47E7AB3B81B178B523D38F973117457224C4DAE58B8C46990076F8E19C168D464F444D0C4A5A94F01 095101C459BAA047AF3107DCE5B8DA36E09D7E40DECB3DD4F551C85C06048A08A96594D410DD8D20597E41D4F5444390F89216FBC193E3B1BE9C5860 9D79B81153717E252A3F6C7A0082DA6379210D9B49E77410D903B5D1CB4318A8FF72497FFD6779F8711C4556CD9266A3E9109601683B61084867A50A 6120A72118CC7EE79EE21A84508965B193F18694

C:\Users\user\70020325\jhwxpapg.xml	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.504692184009581
Encrypted:	false
SSDEEP:	
MD5:	FCC058F8D3E3A4E977BC1368901E89B1
SHA1:	205C833044A7EB6660592A1A2C83A9533DE62525
SHA-256:	680981B9B3516693531726A2B6BE2CDE400A929AB5C0EA73FB5C3B789BE448B2
SHA-512:	53CD43B06862475E2C6CBF5806884055D0690DAE9F763DE8800D723FA7AF4A5B20836679A688E14FC33871946A4F746C1A2E3C04CCE3F78EAC9363763A524090
Malicious:	false
Reputation:	unknown
Preview:	0345SX058111878gP8Yk651z2yky87eH78HF4b140N7g3PJ531G97a5V2A9y6qDh7851Vyp2Dzd3947s81Fl1l8565N5hN42..53a5LZ7L6993BKsh37d68cd3q57q44p7 oHBHwm790oj8X6UZ0303391039Llpm1Hnmi5A2Ck54248985ARV8DTpg9Rm1lGe23v327iT04xz9v46631Xu71Ap1FKqF7964SXbg85A221xb7Sy9x4d224y24R4F..tun GLEvH7Y5SZ6848HD1j1199u6Z1g9WD14gNKB7dFqSC5F5mgP4i4j76JUYO068Hk77Rm7yEBUhq2MH38t50..iy6032b86MUp3wQ356s0S..99z540rcYl7yqzq6zFKIoe7 mn0I81qq6hFO6vFDQ246Cd5wXAD1r2So998riN3U8H5XAe3yxBu844102Q9x8h58088..SJT6v2bPk2W8e60V3N2R0aQ7VTV3NJ5199juFv66Sy99..

C:\Users\user\70020325\jjdsru.docx	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe

C:\Users\user\70020325\jjdsru.docx	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.4857216904813955
Encrypted:	false
SSDEEP:	
MD5:	D022B01DBA0F2C01AD9D9C9B4BF12974
SHA1:	F0E22A5721DE0AE6005E4240AA40F29CBA6140D7
SHA-256:	9F113C83FFD1028A729EE2030399228CCDBA7BF7421A7AB8894968F4848B8B18
SHA-512:	5C972798EB4DC4128FEF321E4A07932DB831A5FB0B2B7E318AC6EB718943FDA04A5D9236D338B5119C4F07CE7002BBC2CD0244D75133E15B06F94FA9E244B3B
Malicious:	false
Reputation:	unknown
Preview:	Bp2D0FHP14M5871exx36j3Q95BpAE64V15N1JgzbY44S2Qi75IcQ87j101927zugS4TrO9318L9Ucl34r6h13aAC97Tct0TZP1y0kJx505uhN11LGzqS5ZK3lA7n735Wq2 sf08r077D0AC858660z2s9v92s6q508mi3152FU8hy2p47F9..92Hc32E98362g9wc0Y5K65ZFV9Ae3n43S..6p4M2HubG919e4OQ90bdS81K6bA999J11Q8mkh936UDi8 1S0aGtH936D2w95G8bYo4A8a7L358Ks1yS7jrmP3yI00Pn78..q926K0U2L8l4pCHW015Ii2150od10028VduW78..165oy1C4CvM62qlwDl2172A510qU24N31250D9Sw w12zL9iN0rWOM7y2WY6Y40nA4e8639Gyx0..oxmJ6Bs16HO76f66pn4M7D7w9s281p54966536b2C5LDf90371nf2st214p3Lb7i84B7bSa19s01Z39933Q9t8699v1GcP 28pEEsu68xrd7dnm938qlF608civZy4hJr4h8..

C:\Users\user\70020325\jmwbo.icm	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.46955821939074
Encrypted:	false
SSDEEP:	
MD5:	F890BFA477A07A6FF98F587124A9DC23
SHA1:	B15FF1FFFC7157A4971FE62813D4158C66976F18
SHA-256:	FB7F46325D7F063731240FAA32B1AAF1631A4FBD63820FB92888AA4FF61E3F24
SHA-512:	DE221589EBE5AD55F5CE785D812F0B1C65DF84DCF286A576527FED565450692F4246996AA993AFABFC7B65A773C5EB185611479685C19E19E1BDA88F671D1A4
Malicious:	false
Reputation:	unknown
Preview:	248l..5K5l85705q3vnKvL668Et0GlDL8ozQg5Hyp21vVjV2Su322FLI8033USx3j88t2p02rh469l4vqNHl3065ACiO6I0N4ku2MzAoXA27ue1V17cBI0w7J8uCf30xOR 55M..5787FX2T223U5447kI122L8fJ858g0D7XPl6m0X2wx5597JYF376KLOdy0rLL38avY13ra0n1L93gObuE92h061u664ZlCF8a40Z9k0xp498pcJ68C1H3232zD00R 4897oT5Ed0m2Oq6l42842uc30lZd6272Y..ME6v5OJ7Vg3lM2f6533bg25nowgkqx26xKE2042b7O8b27v774uHW52o51N1a7i0xw777181x9sd32Q1g4DZ49j4vQT3g40 89zB73T3J7L76Nb0716137wU376l8..60XexkGmss224nL32Wct68GO34BLM4v4Q..h6U410G6A4E6l17K7Ec0i288O598Aw3uaBxlI131w75AvEq006U1VD22fc6y57a0X..

C:\Users\user\70020325\kgamfloqb.pdf	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	5.504449700018404
Encrypted:	false
SSDEEP:	
MD5:	5558F374B6868560EF5445633B1D5775
SHA1:	359B2FBAD3A9E73D9E11CF927517A71D6BA206E8
SHA-256:	A671047A592E21A62A90DBE88711C32C645DD2B3DA1AB9C9884524F7F9D8BC67
SHA-512:	AABEE3EF5FD11697EBA0D858DE5BD6CEBF727E3C7E329403A5742A3DE3CE95208962DF52FFF4F1FF5D1E217CB9D759522517106A34E36E0267DF2C5F9F24939 2
Malicious:	false
Reputation:	unknown
Preview:	GTczV36Lm4l..1N3w579L7S65Spyl2I9toCA0..3e8bsz1xSuFo4268df47zva7798as3o9y34bDcb9t3oVv3327YuUe73RD6ss5E18B4828XJ443Vla9667il1N6jGjy5 080185x9Ge25QN..G48gzTdJa0t674435a0112CT6730t0lH9JF4alL1141dXV0268WpR47w01A451sg23258CB1..lWbd60OVydsf5v5X9El3w3lb534nCGO9JNNc720a 63UeOYp57tUBAU4t2QF205ig9d2F2u0l1..8g61PPWM992w1V35k134..Pg6F16N918Ji75479k0K73GNA00tr6qpCQ114SzLh052e98PTO3f2Ic3s41..N7z401J5Jakk 02PU2l2U54T3HwoCO000l1l65P..7eys415A78d467VF1r66P5874M3oM25338hj0340YVF477CP8V241S253..Bon9yXu0065eoA8..98GxoM4I0Q4xc7Qcd0l0t8SB1d 25DtfCfSP7h9ca99TzGAw2w84NXrT97ZM6m82N1M62W75o..

C:\Users\user\70020325\kqegmrxnng.xml	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	513
Entropy (8bit):	5.467973173127867
Encrypted:	false
SSDEEP:	

C:\Users\user\70020325\kqegmrxnng.xml	
MD5:	A5EF372946EFA797A272216672239D7D
SHA1:	76A056421F54CEE875659915E2B13519F6ADA6B0
SHA-256:	3EE80A5AACEB6345648B70D53D057FBA2DE140B3E2FF308AD9BBD6BDE074FC4A
SHA-512:	6D38DFEB4355EB776B83013B57CA8E09B0956B9EBA7C39335E1910083FE77C6E32EAB6E05469B9E1B9487AF9008A328DBAF7693E26998E83722696DB5DA42535
Malicious:	false
Reputation:	unknown
Preview:	43400OMMyzi08b6V9703YoQO8U69Q6616959M87088x1uQk61H465e6Q5BlvZ45a3Qmj7H2H1210iZ1M7pX8if0k18fc858ag7W95tu0928eH4G..i90635885UlUw6iCf dpyRY015qdi5U0l0qVy851m547h0Sk3V0s2HC37zs326mO7Z76m0l895A16Hk64z39D2W..17N0Q4c1j820qtmoi2z1788o4w6g0sl6y8N774X2bF35Tg305..hA796W2X qk0ln670Mn7TFr315c7Y1ONaU2hO1RjPl6pp4TmOjv8wxy12izzBK044g23qVO92M6601MM503QDr0zha602i0hEQC6..6v6j90Ed6D567FQSE4Fh9UMFD874944hl1tVb 09kI51tsu18QXl5q2rT9B925B7a1p..WgaNgf7D686La2JS58q968382x3h54PCh0R81R8S6C41f003A139N..A0qc6I0xIF9hE8q2tqH2g4Q5m8023f77EiM..

C:\Users\user\70020325\lexcqxx.xml	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	575
Entropy (8bit):	5.4153101709799
Encrypted:	false
SSDEEP:	
MD5:	7B4DAD6FDD1A31589E3FE50CF20A198D
SHA1:	1BB8FE80A40570209017296DBF75649C072684BD
SHA-256:	E04D7D79E576267523A969565EACF093F7B3C0C9FEDF8A56682A1AED7EBE403B
SHA-512:	97F13319D1E4A0244044BE32C2982D22D77986C3B7B772C376C6A8D9D0FD2E3AF6ACE60425A8B98C09CC844B8DFC9BCDBF8DA9E82E9EDB79F10AF377774C53 A
Malicious:	false
Reputation:	unknown
Preview:	o5X16W9Y0F4f2Dr8Jk8E0SR468e30M1Mv2..5u2ep3N7k396V9Uh1Q349sv1..u3A99443ixHrKF6115Eam7890010m983964i2A4z2jo9VdPX9o0x446..g4AN08m6Yt0 AF7y1F58td8910hN13u618Z45U1VCM05v3Lap683J7gEC85m12J8d4116CM7973..P1z0l4QRh7zk56d58kFY..o9j48dIl4q4B3Mmi2007D90WM527Q8N6K8c630c2L1l YTy6o823w97aPs2d368237191XWOc0X992S5I6zQj88543M7W43Pa7MA37T2bz4015745aV4hx294R81WC6..Jg3D08Ra8AYCn86N9lU38yp3SfeMN8WT3KU15w37r14JI rm3353W3o82lHD58h730N36J2I2lV3I82s4UH128gA3753o464zgUg90S63403xr0T51Ych644J17z4b5J837..eoe0wZAFk5C8T2m19X7noWu4UoCbh3kXEKK43i2M935 2TfL36M788Y845Lv19o191BJ85D4xp5WK39xd76E0f8Dl77L8Q74E..

C:\Users\user\70020325\nahqx.bin	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.415172732444135
Encrypted:	false
SSDEEP:	
MD5:	2751EAB2D7A8B296B2AEA04D97A0CF1D
SHA1:	1FF1A3B69791962D4E432C9FD309E2EA6167B4E4
SHA-256:	1D1633193E8170DE3851D35BEFDD5A6FB44680D69999485A1CAF170058D9E563
SHA-512:	1CFFE2BAE2B6CCA89D8495C2EA77F32540D1FE22968F6B5593453117B381EE9E5ACF1E71E56F6318300C573B0CBA306C8229ED24BE63F375414666CABF3A9E2
Malicious:	false
Reputation:	unknown
Preview:	HT931mN206..xH39a0oE64bTie33Z030BN5p7q0mxm8OY8jJ2ZI7D9621ah6O28550PUOd28dM0005q0ND872az53jB1tE7S546Ag75c5V4o8rJ0g6F99O08PV5AH9v580 UQ56MV2ABkev142P5j6Ivw56ua0033IVT79G1n634b5o8iA..3347HQkY28723C3p91zw0H289pJk55U360GM811q2OPGoG1G6S01wc82156KI79ZQ59..DW66L00Zh3Rt 0l6HN6R0Ow341zSAITg02604jkJTT7283k7j25819fWu2242XpI2Km5YpI63MD7tLQGR4827x87e035W658ny1HeA5T8kTo937x84zJ0K2b19xAT509465KE5yGZ2pKTa1 Dwl93cKl339775J24032i1K69u4J474pK53..J1h1QF..g660nJ1xo0K3E13Fqe8yH94p02phK8dd1261m47493040N1a8oEd5ymCk87m1067521Y1Z8c5CM2qpMhc0660 Jc28D6957492953pg9L35D5mBFDLk5QMzM3K7i465R63a28..

C:\Users\user\70020325\nqmvx.docx	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.500486959913872
Encrypted:	false
SSDEEP:	
MD5:	8B9324745C4E7E035E865443F90558A4
SHA1:	B82C1B535A00447340289D8E1BE05138202139C7
SHA-256:	BA91C0E785B6B63DD61F4FB624198617AF959BF3AEC84E64B60EDF5D3EC1948B
SHA-512:	69BE09AFF28C8FE54759F55738879B8729C5B5CFB2B355FC2E99766F6EA04CEA4E99A9A2685F14A4B081D75538FBB25B3E8C3FA9CD9E4FF8A70896A769F8EE0
Malicious:	false
Reputation:	unknown

C:\Users\user\70020325\nqmvx.docx	
Preview:	D6D3ZXRei086Fa78qu3hO518080hO9a993lM03P4iq2sk981kaiSDIl5qP8l565C6410A5w59Wx4r3u715Cnf97F56xIL71GJf9eBb7U59..Wv1E06gNoJ4XUM7XS3zqTs 0z6ikWQ4K8t609Es801T13j1A14d6e2AtS9Xt66McG82ad08FRl28548p5620..H72f795211N4K6U66V1D4ha60zR63dSC7a0Z35NpH8D319bcAq5v2Nr9690583s3kxF 37F36CVod58m1868W8nhL984UAND2vV824Dg0VpO80F0U6Sl7aMUv4377327358nAmoY31527J702..Y5nsoIy2V8T6W2093E2D6c41bZ12x6X6b5Z9Z4wR5 2obTD6Dt6zVC3350X07B0m370958dX..dkX9lD7y4hd6RK10301w17r3mBrSc187rrK6Tvc..7A03V818B6ahdO1W909tk103whpLBbg66x35mQ62lQG889MT1..

C:\Users\user\70020325\nrajixg.txt	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	5.477318109250144
Encrypted:	false
SSDEEP:	
MD5:	EE1732E73266770BE151820479F86B4D
SHA1:	61ABBE84C2EFAD5D244F84CAC5F4FEA13C4E7211
SHA-256:	0F1A3862727AF183BA4EC31674E274ECCBE17A33B9EA6CA02ED970135252B53A
SHA-512:	FBF3D22CCA81BD9C2496A018FF70A4698F59980BC00281DF6FD7DB0377E57C261128EE48EB8A9B6BCD9759D57C278C29AFD248C96C0D135D330958B8F70542
Malicious:	false
Reputation:	unknown
Preview:	99Kg7206e6B3V7OM42db8aZWR0HbfhLP1h02FV9541724pp8eT890YIs7x0y9z4630CCtGh475V1q9qC..6Tlp189P3693880on5S..0s91..52l4giOj1T8HM3mtAH2S5 872s44ja279KTv01lhWOd570SMVeV66s9517K1073HiX0cSXFG3940m3C7U8Y7CB7122X75u4bgF5UO1010BTO0ZJ4230eV32XcV9Dl07L69rN..3a4707f1d4Y114649d VA6PUY6x82z8uII3c5huUI34RfdO5T7RX7Yf9ma2t8297962u815gz7151i0MFMr3132Q4t1545350493H39Z76zG02198..6684B5LdJsjSc11F802R4M91ox394VG403 8949WxJ4Hu9U2Ka1W..91v9KjA82s3sw60y7r785QZ3NtWC69Yj561r33Ib5TTse63v24P1G9nAk67q5sN5XGXd484l685A3KL7508F0v0..A2RH9eZ20rlGy7wV81003U 45X46uOYB2VA6Ui9S7j5023JkRXlzn2o1uX40dXR5D0A8mgP92b08l283z54FD7f7J5pn0K20x0S4866bLUF2tbVma3Dm1ss17A30QkXZ25482U9r9o..

C:\Users\user\70020325\okeg.txt	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	67081
Entropy (8bit):	5.576541569549301
Encrypted:	false
SSDEEP:	
MD5:	1C9FD8E91BC238FB75B9BAAF24D865FA
SHA1:	F36A4DA77FF16EE761FBD297E7D945EC82F40929
SHA-256:	43C6CA644516EC6AB314DA10812387F3A4057A1DF0D310ACF289D0936385A87B
SHA-512:	97534EDE3662CEF1764376B7F5FB531D9DAD5B7C39ADAFE849AA12EA3EF7DA6F0364C96F6C9EC7927C97C11452CFBA3E5CC174FD696A5EAE86A81CD1508DF 26
Malicious:	false
Reputation:	unknown
Preview:	sSa8DC8OAK2wGByid6vH0p5069zVT5N4qV38X028t9..uz490832716P3ez4NaL6269dYetB2E60RDg550muni1n3lgDFD11ENq153044YHB8p48n3Z35w23CHSD44N9.. 68n988Ownro8zS36AJS0YQ5W244o3457U0a8R2n34qQeB0054urw3u0Fi49q338AM2asd..M2XP3JE583ueHpW44kfj50hCvt51y1j500l4m..13s93Xd9j6iqDt6x0454 9aA9Xyjupkd453208m3XR98xzo26U8A890C8S6C062tcL8tdeU..H7en02vk2w1b8uaE48200F32U693BkMSe3t144l67443J8Tr2sG..cps5pkkYIE6447qwg2g8uYHqt Twv2U2Tw68tP8LVk1k256D1y63rEJtA2Mab92q1I4x57l6aqf..2KPac138d61750vJmaJ12yln4v14617m10WMX4VXS7Hus3EACd6..321B7lA4VyS11u9l76AILnB240 e5dS8e8Zs0Ii42xe8A4079r2N051lw2U5044Oc06qP7ii6Vwu..0Fzj9oA51AvTG0Lo27yes722S3w..25338X0bGj510904qwx03Z9Q2595VJP7TP1947..8pN0r51wS3 99q1E2l318409a7425811TjN5p009..750367YrIHd6NT0p3i457q11X0O5TIScx20vv0N011259aio27I0Ic2Ch9B0445vO7407V1304L2907o1t4kK89l..z1Kr498ZN23R4..Sny1 1O4KSSX0966t0oTZa4xr1I1olY407G0941g4mS4B6040lzy26R16B56PoR9Vw4r43Kv8505ZbsOGh4..25y6b891P4cihec2T944bUGz193LJ00OKCr9059E4OA051p8I1 3E21jt..0eqm0A1Y58dO4208ws586KPI4yEcE143..yx0705187fQZUn3Wn9a40h7kh505365i1j0h23

C:\Users\user\70020325\ppxulrr.cpl	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.46863340146582
Encrypted:	false
SSDEEP:	
MD5:	4D584E4737DADD3DB470374E722C17A8
SHA1:	09F77E0C673F3C4A0850BD41B5921FF8BBCC3CB6
SHA-256:	D575CB8F3BC3BE82090E33A9E0763088D39BE0A68647055695126D89648FF17D
SHA-512:	2216EB59590F2FD2D428D921252742EDB26569AFEBCE85872FFE1B2E8D7E4BC614816F25713EC739D1F716CEEC704F7780360BC7B98A01D310B4D45B245C76C
Malicious:	false
Reputation:	unknown

C:\Users\user\70020325\ppxulrr.cpl	
Preview:	zo744llUL55o9K6U41iWh19RK64L0VJt4v5L5tl7494m55b5S188Rb3PkH233uA9y78s22llGz1H89AZmhi4819Fo6fO..G88S798mi11BIzl5hWX9W536pc4C4VAifa68 4b78479zVVqh0KvJ355mb39q9GU1rO6ER5Z8vEo8E726v63C5RF9RIXes249k21Y2D97MyMH529iZx9E5Ob7Y2K40Eh924fPa3E039N..399GSH1AXwb9292l9a0N0G98l 0B0N952eckBxaa107a71d812W1GQv5..sP1Kj65nu00Qz69h703c965r1nw4r15DC925192Hqi1g67v555V18u9606b21l33..edh13X44C1357S5875lv1Ee70Y0q5F25 k5m19C3OYQb71m3Vmex008l36ruMu9b222vWA814n3B2J6g8h9QB083t8xU9UD02m7G6e9Ci533Zi..p8S2Rz335G..891q06H6x2hYsp48e10910XHkq63M7LsuJN34d8 W150M4..

C:\Users\user\70020325\prcqujmetv.ppt	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.502742284030885
Encrypted:	false
SSDEEP:	
MD5:	6B53C1F97A0509270D934EB1326F69D3
SHA1:	F71CE22AB41F53148A53AD2661E49E51A38024F8
SHA-256:	6E21BAE80A6A1C4100F7BEB325FD3B2695A8B561939E79B44C2381D153B0DD49
SHA-512:	C510B1C6F6181A4ED34B0A81EDAAA15D2EA1747F6CAB25DE16A3C6C7B8CB8C0138CF108011516208F7AA3DDD1622FE33D94CF0B4E84CD010C4E1A92B65AD5 CD
Malicious:	false
Reputation:	unknown
Preview:	p305iizeEu51Tjf87ojau3j73S4V..8O81AMEk4l3fvWk9y51G94q947B6k3MovO4cb1K625k8..l0c16B0DUI03858W127fvaL3Vi7cI123vCbV541D3z796..fV8i47lls5626ufgT T38U1IWmBAyt4M78T77727Y516a1y10Q6ru0d757Eh7hwRaP840cN50z1L24rgM15811hsmR1372BS4E3Pbl7T44Hn4t36m9a4794yS22l07y06W78p..932V1gb29i715 Y17j5CqF90eJ627S6U50tUh664U56o94eWBFe5QYJ727dV6k7h6L024NU67QaC479670cz4tuObk2Gq7aYS809EQkU..33LE050t2324qb179Fg9ZLQ91T33O129gf87qW Q66OJ2B572j7GSUXg76xd8e8QP214MvF6b5cE995y070R917Fno99317v..11k34p5m2080Xry172Hl56fsR86Gr8f9uYjN5mJUkiY39C7Y2d08arO3AoK4lM07B1767av ZK9st6KDWr..

C:\Users\user\70020325\qhqujjxx.dat	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.517675072407982
Encrypted:	false
SSDEEP:	
MD5:	F92DB8F580BA9D9F2CA82E0F94CC4FB5
SHA1:	FED411FB44115349B74404B44A15820D9D9205BC
SHA-256:	666929695D82091361DA40985233C99CD66D1567CFDC114FE8E974207C0B854B
SHA-512:	725C0D8CC4EE78F1F5ACADDCBA96ECADB9A934B3C9F79C9A918EAEA49EEA2445F0165C8D9D3A1182BC1CCE1C8DCA5B7DDD6DED03636518859C2430DC6E9 C4DFA
Malicious:	false
Reputation:	unknown
Preview:	Vk146X47n7Qj89xlo6X15s7uAOw7336Y15kD526xjGy2A8a61c06B6W4xH7JH20nnme30OU720a5cyD303G47bi86md2bobG15x7gBF8Wxb6044K32x..9091AMA6gjyLO 69v3h2gUU3sTx53Ci9v816ME7FP1E4q29186ipa616w605u567Y0mObaVxpNct3Q4626R9Q3i47Q8X7Tm4521DKerfcZ04P83..eOZq16l8C2r754zksQYL96S9J19w48J 2m01q3jgu7cx6u8194pt898uZp12R34Z2ne211x89a716AaT0558kD3uC57Yh3nNyQ03..7x2GnP0O2Q2L1275u5QPG76sA3Oma04E3cUdz64G04v3DMUiM1 SHUqm6RQ3Pg2681971kAj736T5rF33m07C41S8UuFxC1Z5RS08pUF69I4ak1e0886OkE69RW17yD2NOMNq7VGg66S654884JUiz060YW0h6zjdGvGN67..44 98qCjX6t0x24K2T912942q18M94eIT55hI23L8f1842x4xVnY18YdlTpR18x91s..

C:\Users\user\70020325\qtfj.xml	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	552
Entropy (8bit):	5.530452181758965
Encrypted:	false
SSDEEP:	
MD5:	57513C9ACCA55258AD8FB5FF29744D28
SHA1:	1D6251165BF7D8FCE1AF32063CFBA7CE575FF99C
SHA-256:	B14DF6828ACB0618B6CFF3F33638B3713098D7ABC375F4665681A009CF622BB6
SHA-512:	B9F356CF41AC5CD28D96F18D0A7CB71B087537559E62501BC277E22FBE4E9876D0EB00A9976E357AEC27E3C7F8082989694F63B0C9261AC1646EA6521F52291C
Malicious:	false
Reputation:	unknown
Preview:	a320925iNw9zzf6OvkHxkns2BDdc3VUH96bTU0OpG962h7V33110bA664Hm58605KV7wZFivF67uvQkBGy..D2tq8eZ74v1J83Jh445v48N5xORU04tVe0e94Y0u2V696W 7a90..Z079JFKU292V3xeb8l523Em833bsze7Kji9D1oe2e43U70682MI5K36nJ662Fo1f1qVsi26MLY3UVMxLVSSCT9k37ky232914J7vSos5C3u5pvELOhTz6Ax53vQ3 Z24444v58Py..11d12R52T1g180v0GG83364lpgZ1g46964sLXPKc7o975x4x922Avkd0m79s39c3614i4q3sSXCde6137l0cphYD01L7dJamcSE69QS9Z0vF5D9X29rmN Gm55L82tcb656aHJ..hd3m7Y7S4146u76pv43BG0JL4Nt5y6sU508h9maFIc5m0Zje3VCN8l7kr3Yq260n88X4J602mh6t4y8661614R25MW8Hhc20f30X9ol615904m3L trD3cau62c7U3159806ZI62FZ02iT9..

C:\Users\user\70020325\qtfj.xml	

C:\Users\user\70020325\rccvoektgu.pdf	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.546357391593926
Encrypted:	false
SSDEEP:	
MD5:	3384D80BFC65B6632F7305B8210BACD8
SHA1:	40FE8027A281D7D25E3E53D6BF0B12D75BE793F6
SHA-256:	1553A706D36CB99DECEF3117695CA8E1BA0263F2B8C5C69DD77D46085EDA2BAD
SHA-512:	1D3363DDFE7DFE03582F3E8F3839E6CDA1AD3DF6E5DEF0AABCBB734506412B0F94FC0BC70C4EE08AD54E927B1745A3AA5EE64199410736F6D3D8FE04D07D6 23
Malicious:	false
Reputation:	unknown
Preview:	7x6ihufUwq50R7j5H172r16sc43Ed9l59fSz6JS13WH0Ss22TR8aQkX1O91502M3352WVM79253VtzfOA884QlG4gBN3A2pxeG0pFZnQmQ71F53979OdwP5x Wd8902d42vsjf40M292c57izfLvc4xKl949INHuGM88Os2lE8l00am..H19e3G1B4812Wy96a0L9Q5gIKg42XV17y35459H177917Ke6G5ul9u6t1WSRX5126o66bBe9B0 1QLy47MA51z0845h4v0xCe4rYzdX7657ws6kn09k8576534r1QM0Y8U4Lq4A3N9EwK9H9t0ZTFOS1o5Z6Hjp8l6..HAMp7K0MQ859k3K9Bn823xHG2yI5LU0L876e0F1Kh 0YX0vG20O34u31592DewWc5B3t5j0BE69XXm..YIu9YmKHKHo6l8MXWqIXy3Yl754lu11ib23oszQ..4Bt8373Mp5Vk072mn..2W9VPReJ54iPIF65965m0K3Hh336J07s ZQi0pO9gx95lEF1E9ZM150Ki5555WX14oX702Pe0G153wH05R769D7801..

C:\Users\user\70020325\sgfhjno.msc	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.449740555944089
Encrypted:	false
SSDEEP:	
MD5:	922A570F1A69C95A0A06763E52A1F369
SHA1:	4A1D20DF34BE01BD2C796FD44384F5C039EB5351
SHA-256:	822E27241FC0EA6B6AA23E4CFD897D7C5A76E321AFBC4657E86E607FFEEB1F9B
SHA-512:	CC4CDA6989BEBD9C14DB099C5EA716D1F9850A5118B341379592BB6D399CD620D6AF568938A8854133468F93D6A91C2A95814FCE001CA3372AF2D4FB1DA20B A
Malicious:	false
Reputation:	unknown
Preview:	0jq789bw1724R794Z7Ax78bMUHA73X05b424u9cZWQ4C7f60Uc662kT4kd86944485e6T4b7Xsf46Wp768c9ru8P3K0HUkq8N1052Xx6asr364qiW3jY033hXNY88yrOS9 n7hN602tt35n1q806F..90b4Zn6wOG94342uwT1bQ0179F54M2X1DeW6Y795pQ505kTMsu69P51eRYTYjY26Ww3Yh4j4755524Oj4Ma77N01TX3065mLXM998S..PcFR33 ipc8Jz1e9f564LAD5tN55O2j8Bb244f332E7Q741A85G2..7Q4533B0P0vBnq3Lf2..XS2y09Ma97o2J40qbJJ7lXN7oN0j5828006J8S94Id860MO246Bf3UrVU0yf4O8 7u46r0OfwzC19lh78GM48xq5ac3n98n67gEDR4AiIrbZ892VQ3iD44235I2i4km..7E06bl1Y793z830DD4Npz3OGKA70Z1x6O791m476308Bs4404rv00KSj6tPXoZ174 Z02496l849Y4iOSJ5427..

C:\Users\user\70020325\ugvxf.pdf	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	521
Entropy (8bit):	5.530842076552494
Encrypted:	false
SSDEEP:	
MD5:	A28848BA4D166D796861152501B96F8E
SHA1:	09DA575A4F10681C1BFA696D874F54245AC16256
SHA-256:	597D5D3B6F20740B976DAC596B9DA24D222A15916C7BE92ECDB2A4A4192F88CA
SHA-512:	F98E184BF9AEFF25A2CFAE0C9743D478F78462A0321E007A5111D0C129C8F2A5C2656D59110C520922975763EFCCE8BD96CE2076DF1E89D0D6BC100F3EBA928
Malicious:	false
Reputation:	unknown
Preview:	z007C2YHy9tc50a2M70733387235mf2hRNLo6zo37a48e5592Mb379aRUe2Op8RcgBh749SW..6fCl11h8W6rmk9m58nse2UGz9R4331ZuT95no6MY6kW7g72ix4LY494C E..J90Z85q2l472mzqkv0Y1o7319119fv3387z3odw7Q7z02556Jh2Ky8Lj7G0EN9j2G8C823o868UeqjEfAU0oA5S9..4793C672X9H28Et..LuEcS9T97Gv0653hj35m tHF518gOf1C1298KP1FP38xsjFy30A9406uE1FPT67z3LZC728Rri20kK74n0u8vtb7Pf3g5f7858cuScy94s4ix666We382dy6g92f27Q655qldj71dJtZejN2q2741M9 o9NaXOE1z85h5R..q354jNFW44br26bZW6PH9Ox2Ol50M9Vh0Z52xZ2Ke1lA2gJht7..82KqJi6O52976DQdp0016917Srp30scn24x55tr7Yc8EftJv5xXR1381h1i77..

C:\Users\user\70020325\vmrrh.txt	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	527
Entropy (8bit):	5.399887336954362
Encrypted:	false
SSDEEP:	
MD5:	A60830AC3B3C22A62129C6C2291BF341
SHA1:	72FFECE85394BA6539229E1B7E53B2AE687E6C1B
SHA-256:	5F7175BB34D9236CBC10A4981F898AA24B2715016CAA86B7F651774BCA41BC03
SHA-512:	9A73C97C9953E041FC9A13F9E0C94BF5B61B789FBF576EF1D9F7AAC7423D4798D551954C7DBDDFB67DD0E2A2C9FF4B55DD11B56825103D02808EABEAA9D39C A9
Malicious:	false
Reputation:	unknown
Preview:	8979SuD27Pyi921P625502J72esyL1r946u49o37D5e5i75J252N4BG8m5D1O7o9b13NqPO9F55hr8P96K5469WU0C6fL193v13w2zC9B48X2rr647J0PVyM912V70H0eL m43Ur281Y55c64465528H6j4012WU86nAe1..o64736J8T6082pl4gP8k912778v6C3Pejk563P7S567c5z72P936w412s8s496Tzu20g28Y8j62m31l4EB8e2Vld8066v Ai0g8zGF1g0X4g738Z34xaaR603N0A8UlkI8275E..jIHIe1A3xIIb3Zf8W0br7z4u..sK30s15832KKN77Lmf6bc3y6J411mBG0732r7685Kgd3i89E3VP7lNjYd0209N FBg5632863L153otAq0R826..32Zg4Se7vmQv6T71MI13090F13314v742fz8P4I3q2590Jy74jr78..140CDI5xK5J7GisH540EH80AzxBsg954WThLPN7I0oJtWymkt75WZ25..

C:\Users\user\70020325\wbefwjfsun.xls	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	578
Entropy (8bit):	5.421686356571419
Encrypted:	false
SSDEEP:	
MD5:	C2A081370F8349B1F385BC5074B952AD
SHA1:	2EFFA1766FF613EFCA3FB4DE272775773AAC0F0E
SHA-256:	A9F1812730FA4CB3CC0DBBFABE02BA17B9CF862C0A10C14E951C0DFED19635B6
SHA-512:	927BF595991AF84346CA982C7858EF029A1ED61A43F455AF7B22F1B82274724A48903FD180D8397316B3B412B7EA023EF4C9F4F373C5DAE0FF5671A8F4636A62
Malicious:	false
Reputation:	unknown
Preview:	1gUpq655d3EcU176lx7i89lJe9sa311s1qZ3286JWURX11707OXp4270H9..F3K172e214l9h417611223uv737G56m56RZTU1C28ysh52k..455rZ533W67Cw7417315P Nw6X7s8581uAw772r2h2a8ATEcbU932v7Ett51h9YN4215yiLQ464v3xWq70so0LAGmRd96Az0123j8Q6Ds7a4DYth6313K38K614..Gwf6W659ag5EtCr589lT4979037 13i2o5321G4Y0U682172R28alev553..A92bXOnQ23cwVZuS72R2OU09261W76Vxb8wJt097pD938i6318NSN0hnFN2..e452uR3A99rLhP397Y21d5006MS86VJ47..21 BNP54099JNM2kc9e421qf55223T0I6xM242659dB9FgA2E27Zyj67xT7Cu5KM4372P52eG1rf5p2a954jRxL3je358j7l531R78oM8U83agsCz2t81139iQDxcfAQ265CR e620j6V9V378Dk4Ns814C9v2bmxnf4T0Mo203449WK9U7rUR4Q8i61G0..

C:\Users\user\70020325\wnde.bin	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.457737586179863
Encrypted:	false
SSDEEP:	
MD5:	F73FCFDF17752BC29158B17EFFD9E639
SHA1:	503A98A5A0A76E3555309D5512E076687A57B8FB
SHA-256:	57CFC83235D9581CC07DF19A81AA85B83A3964A7EDF05044A11A4B1C0BBFDD3F
SHA-512:	4E65804F13622E53555734FD009D2137533B8F4965EDFBCFC8C8D60E093623952F3DF1D1FAD8E6DBF0FDB18C15B55E4FEBB9A93C1DF960F983D393ECCF2E303
Malicious:	false
Reputation:	unknown
Preview:	77SWup07773qCA2700IXI0g1QmS9f614j75EXu8eg3F3..2cae625A9631Jej12Fi9l43p7W21Jwi2G94r5cY6h6h855232..29195f5k4d97B15ln4OL4H49H5239np8K SLGFiV6FKM8xvjv6L2y8O3P6nx68O313ntz686U3JlHFPCFM61K957R99f3420Ns10L018p26X9S8761n1..HP3A2kgOkL322a6q0e20471q20735QMu10U5D0qQ3d0w3o zv50Hw951B5psIJ1r6x2yz26l739Af55K44P90A0f7P927439gKPxR470BC87b1c9ne4T7Lk4G9Y16G7047302eCC0m40a5B937X4sr205Q673Nv723Z6974n73H5AoH.. j62uW20c03Uwu3t9R78Lh4O779o3k10m4Ov0nrGE9d63I8aC5SJsl19o003nl36BA8W4jj71..1g7h0kXxuEtTp762nw6PED8P72vT42d8O433BE08650T9oI8D0zb0yOw 3Yv26Gt0p7Nw5nFh750g96K2j4F497s147Nf2NZGzhv4..

C:\Users\user\70020325\xphcib.ico	
Process:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.441589733080409
Encrypted:	false

C:\Users\user\70020325\xphcib.ico

SSDEEP:	
MD5:	8E9998AF685EE6B347852A10DBB275A1
SHA1:	B04DA2B1B62488A5CB828B3D308FEC72F3111E68
SHA-256:	416D87FCCC24EEBD4EEE91BF3482C5033194A45C8951AB080D37CBD5DC3ECEEB
SHA-512:	8126EA57C6AB61BFA475541DE57C2933691C8028BAF64EBE14032D441AD7C76267D30BD3D742E1122B8C1099D0E3A64F9B473743E3E7A36C838D20409725BF67
Malicious:	false
Reputation:	unknown
Preview:	818t86a5Sn70nL061Qal59A88555Mye0D2712nLHw2Z14J684CHo99X146319G0x4rU27H8bZr3nXNT0p0OW04upNZy231VG7Hp43OV5T48I..0Cj8G355gj86PDzv2u709S40l354ze95Pa873jZYW3b9hq30x77u2rvRT301Ryz36G526w9iWCk244ZY7aGtj346319V33E1Q78C312X14Yz63by1..133Z6v961490J2o7vQxk8t1082j97gEcU4M96X84H05T8sW02..cCXa0Xs6r8i8AngU90yc6hH8OnhZ9X9409j1hP84gG5Qy4vSZv5K01r25yE3U4u337oA0v3P12IebI7uaL1f3zo57889f8vhq0rNz04c1176X0OJ4lA7kf5m3hlb7525XSmU4359u3qF6U573Fh6k53G0f5635sZ71TH8X31e3o6G1dQ31P1yQv98U9T..HgUw6c83X2x88uq3RAn7117959I6n85I07bgI6Iz59QD7606S15Po0A7x950mWD8308Ys8rnz6f731LZ923oyNF6u72d..

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:	
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\RegSvcs.exe

Process:	C:\Users\user\70020325\ahmrqkljvd.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4DB42
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\tmpEBDB.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):	1311
Entropy (8bit):	5.120237537969728
Encrypted:	false
SSDEEP:	
MD5:	9CC9B31561289BF47DDBEF114BE4B6FA
SHA1:	C901987D5F8BBAD7231B7EE4A65ADB93BB0F56A5
SHA-256:	984AA44429B06B17C290376A8D741A2DAE62FE6F38EEBBF434A0781230686097
SHA-512:	075F148FDD9187FDD6BA56D1CD3D81641FE8D8F9FBA903F98B307463B4BCDC77556B542CFD73C9BC2C34D364245D5B8080DE69DC968DE9070D44FE180741D4C
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\tmpF755.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	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:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	E5D10B0948F9D3181E0C1CC29C697C8F
SHA1:	5EC6635AF3265ED93E966B845BEBA263083C36A7
SHA-256:	6A3C751DA8D6195CF3694F449208C77542F1BD13AB663BA413FF78967B7AF8B1
SHA-512:	BB1EE7184A0287ABCFB3E6CE8BC34A88CA3D97350BE63AF9E3A8F4808B4472A5FECBBE773857713C2384127947DB8A4DC597383996BAAAC9C07A352C550EB303
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Preview:	..it}..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):	48
Entropy (8bit):	4.556127542695029
Encrypted:	false
SSDEEP:	
MD5:	71C86F4534ED6EA4C1E9A785F2EB0A92
SHA1:	D065F0540580FC2E0ACD365784FD5A60F8235829
SHA-256:	DBC475B81DC4AACF70235516B8FB463D4FB170C3E72E647C0BA2A30D3B9EC4E3
SHA-512:	6D97D624C0A2B3D3B8D51A4F2502B8874E59E29538AD0477F1DE32FEEDAE38890F68532B591EEF0FA0DB23CD4929890DB256ACB8E4B73F6F790BB11C1347368
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\okeg.txt	
Process:	C:\Users\user\70020325\ahmrqkljvd.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	5.113845900741421
Encrypted:	false
SSDEEP:	
MD5:	C78630027A0017C87E15C63F5F72A2EF
SHA1:	02849826C91A97C5941B971AB10B61DB34F3306C
SHA-256:	56887C7D292364DCEA51D090D89A45C68E222DDBAFEF7952BA5FF23F521687BF
SHA-512:	5C2D3DEDB897ACC876B90C02E4C8AA22504B303CEEC7F3433CE7E0395FE944E5F7F61D184C91015D8B18B42208BD43A1DAFB49447320627D01A71F22EF229CI 8
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=Chrome..Dir3ctory=70020325..ExE_c=ahmrqkljvd.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):	7.837831519595356

General

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:	gNFfZ1w8E6.exe
File size:	1103092
MD5:	664d73b23eddfcd0227786b9d0f5d022
SHA1:	36fa060dbc146777f54c958e7457096af267e15c
SHA256:	e88b591e50dc770c48156d2c86655923a090ee619753a6028ed857697d21f9db
SHA512:	759eef2e746bb0100637b73f688da001a2a1d91105dc978ba2d69988dd1ec74efe00cfa6146b07e8d1150dbbd6315cb715e70dfe390bd7765aa60abcf553f18b
SSDEEP:	24576:rAOcZEh9dnCceJd8E0S8/ya6TPY5I7nT1RMwazXV:tLd+JdvqJ6c5IzTXM75
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
10/13/21-12:12:59.668723	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60501	8.8.8.8	192.168.2.7
10/13/21-12:13:10.154694	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51837	8.8.8.8	192.168.2.7
10/13/21-12:13:30.658812	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63668	8.8.8.8	192.168.2.7
10/13/21-12:13:41.553181	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60338	8.8.8.8	192.168.2.7
10/13/21-12:14:02.047686	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58717	8.8.8.8	192.168.2.7
10/13/21-12:14:13.312562	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54329	8.8.8.8	192.168.2.7
10/13/21-12:14:44.321951	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51919	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:12:59.648729086 CEST	192.168.2.7	8.8.8.8	0x4d10	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:04.861217976 CEST	192.168.2.7	8.8.8.8	0x8472	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:10.135858059 CEST	192.168.2.7	8.8.8.8	0xda9d	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:30.638804913 CEST	192.168.2.7	8.8.8.8	0x2bd5	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:36.101923943 CEST	192.168.2.7	8.8.8.8	0x3ced	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:41.534449100 CEST	192.168.2.7	8.8.8.8	0x217	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:02.026712894 CEST	192.168.2.7	8.8.8.8	0x4127	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:14:07.730109930 CEST	192.168.2.7	8.8.8.8	0xfe52	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:13.292515993 CEST	192.168.2.7	8.8.8.8	0xb94d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:34.028935909 CEST	192.168.2.7	8.8.8.8	0x1caf	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:39.139225960 CEST	192.168.2.7	8.8.8.8	0xd2a	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:44.295977116 CEST	192.168.2.7	8.8.8.8	0xa741	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

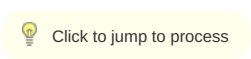
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 12:12:59.668723106 CEST	8.8.8.8	192.168.2.7	0x4d10	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:04.877595901 CEST	8.8.8.8	192.168.2.7	0x8472	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:10.154694080 CEST	8.8.8.8	192.168.2.7	0xda9d	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:30.658812046 CEST	8.8.8.8	192.168.2.7	0x2bd5	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:36.120153904 CEST	8.8.8.8	192.168.2.7	0x3ced	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:13:41.553180933 CEST	8.8.8.8	192.168.2.7	0x217	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:02.047686100 CEST	8.8.8.8	192.168.2.7	0x4127	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:07.748317003 CEST	8.8.8.8	192.168.2.7	0xfe52	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:13.312561989 CEST	8.8.8.8	192.168.2.7	0xb94d	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:34.045557976 CEST	8.8.8.8	192.168.2.7	0x1caf	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:39.155627012 CEST	8.8.8.8	192.168.2.7	0xd2a	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 12:14:44.321950912 CEST	8.8.8.8	192.168.2.7	0xa741	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: gNFfZ1w8E6.exe PID: 5500 Parent PID: 4888

General

Start time:	12:12:20
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\gNFfZ1w8E6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\gNFfZ1w8E6.exe'
Imagebase:	0x1340000
File size:	1103092 bytes
MD5 hash:	664D73B23EDDFCD0227786B9D0F5D022
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: ahmrqkljvd.pif PID: 2116 Parent PID: 5500

General

Start time:	12:12:40
Start date:	13/10/2021
Path:	C:\Users\user\70020325\ahmrqkljvd.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\70020325\ahmrqkljvd.pif' iwqnllkpjb.jam
Imagebase:	0x860000
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: 0000000B.00000003.310008707.0000000004171000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.310008707.0000000004171000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.310008707.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309341352.0000000004277000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309341352.0000000004277000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309341352.0000000004277000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309625586.0000000004242000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309625586.0000000004242000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309625586.0000000004242000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.307456852.00000000041A6000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.307456852.00000000041A6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.307456852.00000000041A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309749923.00000000041A5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309749923.00000000041A5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309749923.00000000041A5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309496574.000000000420E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309496574.000000000420E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309496574.000000000420E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.307635592.00000000041DA000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.307635592.00000000041DA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.307635592.00000000041DA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.308187934.0000000004277000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.308187934.0000000004277000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.308187934.0000000004277000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.307514693.000000000420F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.307514693.000000000420F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.307514693.000000000420F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309384847.00000000040BB000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309384847.00000000040BB000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309384847.00000000040BB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.307678370.00000000041A5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.307678370.00000000041A5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.307678370.00000000041A5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309577630.00000000041DA000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309577630.00000000041DA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309577630.00000000041DA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.309670746.0000000004242000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.309670746.0000000004242000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.309670746.0000000004242000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

	0000000B.00000003.307545225.0000000004171000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.307545225.0000000004171000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.307545225.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 27%, Virustotal, Browse • 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: 6244 Parent PID: 2116

General

Start time:	12:12:48
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xc50000
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: 0000000E.00000002.534249648.0000000005D50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.534249648.0000000005D50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.532878043.0000000004469000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.532878043.0000000004469000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.534985643.0000000006C60000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.534985643.0000000006C60000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.534985643.0000000006C60000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.534717359.0000000006130000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.534717359.0000000006130000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.526048873.0000000001022000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.526048873.0000000001022000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.526048873.0000000001022000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.530600617.0000000003421000.00000004.00000001.sdmp, Author: Joe Security
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: 6304 Parent PID: 6244

General

Start time:	12:12:54
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\tmpEBDB.tmp'
Imagebase:	0x1160000
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: 6320 Parent PID: 6304

General

Start time:	12:12:55
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6420 Parent PID: 6244

General

Start time:	12:12:57
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\tmpF755.tmp'
Imagebase:	0x1160000
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: 6428 Parent PID: 1104

General

Start time:	12:12:57
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xd10000
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: 6436 Parent PID: 6420

General

Start time:	12:12:57
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6444 Parent PID: 6428

General

Start time:	12:12:58
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: ahmrqkljvd.pif PID: 6560 Parent PID: 3292

General

Start time:	12:12:59
Start date:	13/10/2021
Path:	C:\Users\user\70020325\ahmrqkljvd.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\70020325\AHMRQK~1.PIF' C:\Users\user~1\70020325\IWQNLL~1.JAM

Imagebase:	0x860000
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: 00000015.00000003.348386731.0000000004647000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348386731.0000000004647000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348386731.0000000004647000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347308527.0000000004576000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347308527.0000000004576000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347308527.0000000004576000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.349279928.0000000004541000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.349279928.0000000004541000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.349279928.0000000004541000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.348961748.0000000004575000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348961748.0000000004575000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348961748.0000000004575000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.348408088.0000000003859000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348408088.0000000003859000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348408088.0000000003859000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.348700958.0000000004612000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348700958.0000000004612000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348700958.0000000004612000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347385336.00000000045DF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347385336.00000000045DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347385336.00000000045DF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347495097.0000000004575000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347495097.0000000004575000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347495097.0000000004575000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347561842.0000000004647000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347561842.0000000004647000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347561842.0000000004647000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

	00000015.00000003.348601508.00000000045AA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348601508.00000000045AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348601508.00000000045AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347469380.00000000045AA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347469380.00000000045AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347469380.00000000045AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.348802105.0000000004612000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348802105.0000000004612000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348802105.0000000004612000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.347409523.0000000004541000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.347409523.0000000004541000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.347409523.0000000004541000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.348536135.00000000045DE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.348536135.00000000045DE000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.348536135.00000000045DE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

Analysis Process: dhcpmon.exe PID: 6572 Parent PID: 1104

General

Start time:	12:12:59
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:	0x330000
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%, Virustotal, Browse • 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: 6596 Parent PID: 6572

General

Start time:	12:13:00
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 6696 Parent PID: 6560

General

Start time:	12:13:07
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x4b0000
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: 00000018.00000002.369718010.0000000000902000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.369718010.0000000000902000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.369718010.0000000000902000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.370694496.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.370694496.0000000002F51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.370784128.0000000003F59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.370784128.0000000003F59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: wscript.exe PID: 6716 Parent PID: 3292

General

Start time:	12:13:07
Start date:	13/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user~1\70020325\Update.vbs'
Imagebase:	0x7ff720700000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: ahmrqkljvd.pif PID: 6796 Parent PID: 3292

General

Start time:	12:13:16
Start date:	13/10/2021
Path:	C:\Users\user\70020325\ahmrqkljvd.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\70020325\AHMRQK~1.PIF' C:\Users\user~1\70020325\IWQNLL~1.JAM
Imagebase:	0x860000
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: 0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.388913907.000000000439E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.388248541.0000000004407000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.388248541.0000000004407000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.388248541.0000000004407000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385369050.00000000043D3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385369050.00000000043D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385369050.00000000043D3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.389045816.000000000436A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.389045816.000000000436A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.389045816.000000000436A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385181508.000000000436A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385181508.000000000436A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385181508.000000000436A000.00000004.00000001.sdmp, Author:

Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.389087918.00000000043D2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.389087918.00000000043D2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.389087918.00000000043D2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.389217337.0000000004335000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.389217337.0000000004335000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.389217337.0000000004335000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385451279.0000000004407000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385451279.0000000004407000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385451279.0000000004407000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385550231.000000000443B000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385550231.000000000443B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385550231.000000000443B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.389147680.00000000043D2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.389147680.00000000043D2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.389147680.00000000043D2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.384804622.0000000004301000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.384804622.0000000004301000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.384804622.0000000004301000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385237026.0000000004335000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385237026.0000000004335000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385237026.0000000004335000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.384706287.000000000439E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.384706287.000000000439E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.384706287.000000000439E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.384564550.0000000004335000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.384564550.0000000004335000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.384564550.0000000004335000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385312662.000000000439E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385312662.000000000439E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385312662.000000000439E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.389356137.0000000004301000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.389356137.0000000004301000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.389356137.0000000004301000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.385401446.00000000043D3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.385401446.00000000043D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.385401446.00000000043D3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.388536550.0000000004157000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.388536550.0000000004157000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.388536550.0000000004157000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: RegSvcs.exe PID: 7128 Parent PID: 6796

General

Start time:	12:13:25
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x950000
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: 0000001E.00000002.415543191.0000000004499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.415543191.0000000004499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000002.414467693.0000000000D22000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.414467693.0000000000D22000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.414467693.0000000000D22000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.415261342.0000000003491000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.415261342.0000000003491000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis