ID: 800437
Sample Name: gNrfORqjCV.exe
Cookbook: default.jbs
Time: 13:54:09
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

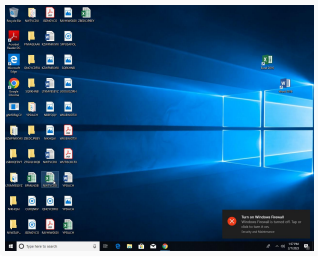
Windows Analysis Report

gNrfORqjCV.exe

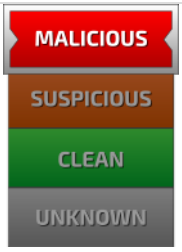
Overview

General Information

Sample Name:	gNrfORqjCV.exe
Analysis ID:	800437
MD5:	60c8d91adfa30..
SHA1:	f8460389f3434...
SHA256:	5707c702f70cc..
Tags:	exe
Infos:	



Detection



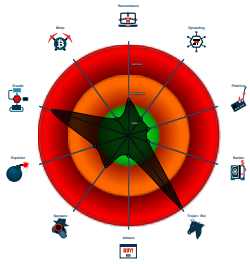
Nanocore

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop...
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- .NET source code contains potentia...

Classification



Process Tree

- **System is w10x64**
- gNrfORqjCV.exe (PID: 5240 cmdline: C:\Users\user\Desktop\gNrfORqjCV.exe MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
  - powershell.exe (PID: 492 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\gNrfORqjCV.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1544 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5936 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmp78F4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gNrfORqjCV.exe (PID: 5320 cmdline: C:\Users\user\Desktop\gNrfORqjCV.exe MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
    - schtasks.exe (PID: 5256 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp2556.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6016 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp27D7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- GzGmImHFmOq.exe (PID: 5000 cmdline: C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
  - schtasks.exe (PID: 5660 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmp389B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - GzGmImHFmOq.exe (PID: 5544 cmdline: C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
- gNrfORqjCV.exe (PID: 5248 cmdline: C:\Users\user\Desktop\gNrfORqjCV.exe 0 MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
  - powershell.exe (PID: 1252 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\gNrfORqjCV.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 400 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5684 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmpEAF8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gNrfORqjCV.exe (PID: 1324 cmdline: C:\Users\user\Desktop\gNrfORqjCV.exe MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
- dhcpmon.exe (PID: 4544 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
- dhcpmon.exe (PID: 4720 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 60C8D91ADFA30A60AFA2F5437CE7D041)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "cb7cb109-a06b-4fd7-8d0e-5290e77d",
  "Group": "MOFASA",
  "Domain1": "nonoise.duckdns.org",
  "Domain2": "127.0.0.1",
  "Port": 6060,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "",
  "BackupDNSServer": "84.200.70.40",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfcf5:$a: NanoCore 0xfd05:$a: NanoCore 0xff39:$a: NanoCore 0xff4d:$a: NanoCore 0xff8d:$a: NanoCore 0xfd54:$b: ClientPlugin 0xff56:$b: ClientPlugin 0xff96:$b: ClientPlugin 0xfe7b:$c: ProjectData 0x10882:$d: DESCrypto 0x1824e:$e: KeepAlive 0x1623c:$g: LogClientMessage 0x12437:$i: get_Connected 0x10bb8:$j: #=q 0x10be8:$j: #=q 0x10c04:$j: #=q 0x10c34:$j: #=q 0x10c50:$j: #=q 0x10c6c:$j: #=q 0x10c9c:$j: #=q 0x10cb8:$j: #=q
00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xff8d:$a1: NanoCore.ClientPluginHost 0xff4d:$a2: NanoCore.ClientPlugin 0x11ea6:$b1: get_BuilderSettings 0xfda9:$b2: ClientLoaderForm.resources 0x115c6:$b3: PluginCommand 0xff7e:$b4: IClientAppHost 0x1a3fe:$b5: GetBlockHash 0x124fe:$b6: AddHostEntry 0x161f1:$b7: LogClientException 0x1246b:$b8: PipeExists 0xffb7:$b9: IClientLoggingHost
00000000.00000002.350708235.0000000002AAE000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 57 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.gNrfORqjCV.exe.398062c.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0xd9ad:$x1: NanoCore.ClientPluginHost 0xd9da:$x2: IClientNetworkHost
23.2.gNrfORqjCV.exe.398062c.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0xd9ad:$x2: NanoCore.ClientPluginHost 0xea88:$s4: PipeCreated 0xd9c7:$s5: IClientLoggingHost
23.2.gNrfORqjCV.exe.398062c.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
23.2.gNrfORqjCV.exe.398062c.4.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xd978:$x2: NanoCore.ClientPlugin 0xd9ad:$x3: NanoCore.ClientPluginHost 0xd96c:$i2: IClientData 0xd98e:$i3: IClientNetwork 0xd99d:$i5: IClientDataHost 0xd9c7:$i6: IClientLoggingHost 0xd9da:$i7: IClientNetworkHost 0xd9ed:$i8: IClientUIHost 0xd9fb:$i9: IClientNameObjectCollection 0xda17:$i10: IClientReadOnlyNameObjectCollection 0xd76a:$s1: ClientPlugin 0xd981:$s1: ClientPlugin 0x129a2:$s6: get_ClientSettings
23.2.gNrfORqjCV.exe.398062c.4.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xd9ad:$a1: NanoCore.ClientPluginHost 0xd978:$a2: NanoCore.ClientPlugin 0x128f3:$b1: get_BuilderSettings 0x12862:$b7: LogClientException 0xd9c7:$b9: IClientLoggingHost
Click to see the 137 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

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 AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

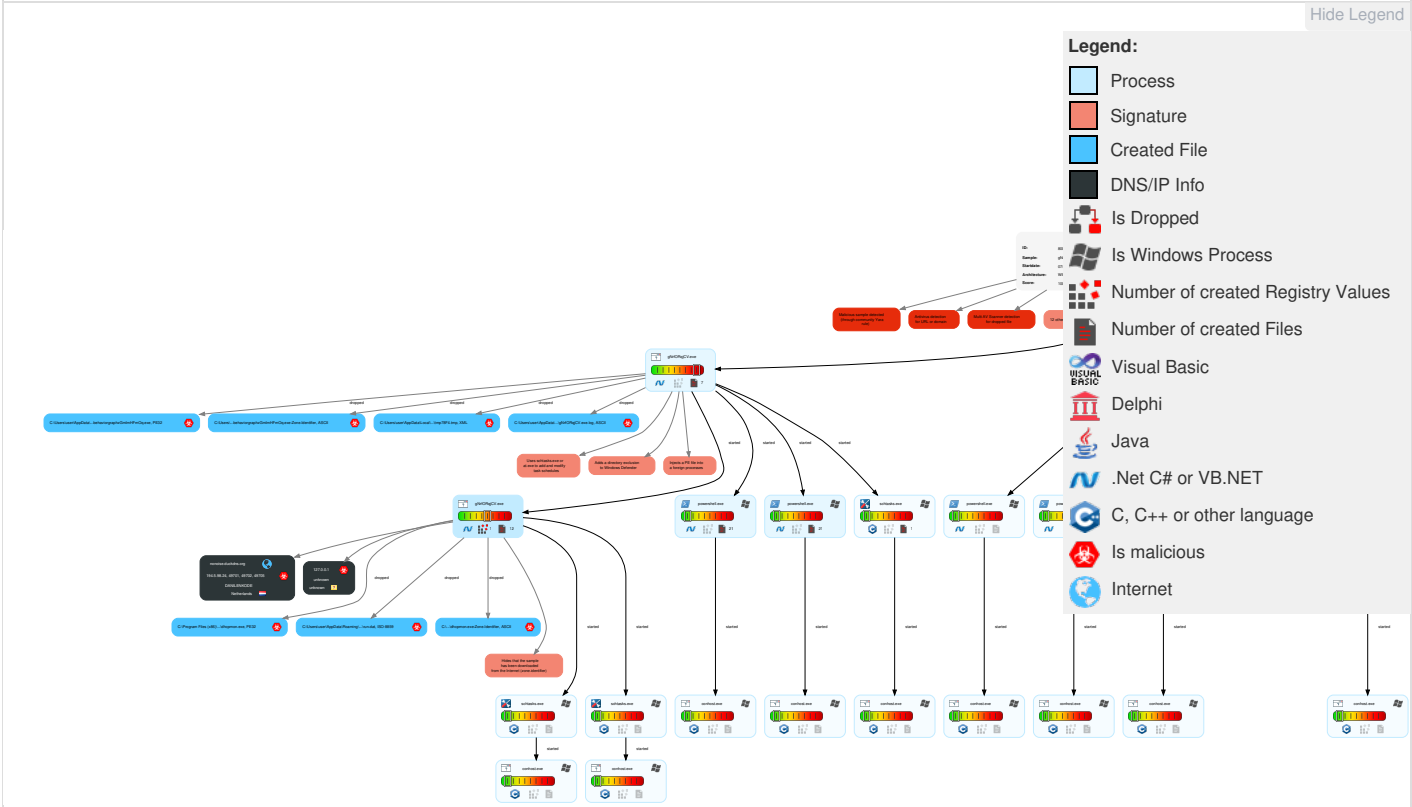
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	1 1 Input Capture	2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

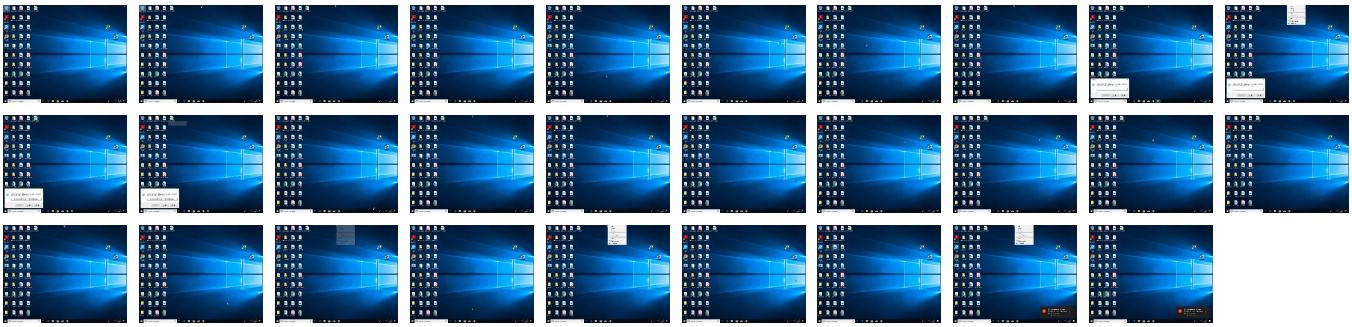
Behavior Graph



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
gNrfORqjCV.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	
gNrfORqjCV.exe	59%	Virustotal		Browse
gNrfORqjCV.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
23.2.gNrfORqjCV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.gNrfORqjCV.exe.5a70000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
nonoise.duckdns.org	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.fontbureau.comalso	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.fontbureau.comd$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/-	0%	URL Reputation	safe	
http://www.founder.com.cn/cnicr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	URL Reputation	safe	
http://www.founder.com.cn/cna-e	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/kurs	0%	Virustotal		Browse
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	URL Reputation	safe	
http://www.founder.com.cn/cnno	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.comony	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/g	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.fontbureau.comessedQ	0%	Avira URL Cloud	safe	
nonoise.duckdns.org	100%	Avira URL Cloud	malware	
http://www.fontbureau.comalsFu	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kra-d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/kurs	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krX	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/u	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cntra	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalicS	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cni	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnani	0%	Avira URL Cloud	safe	
http://www.fontbureau.comuevo	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.T	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnlg	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t-i	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCH	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/n	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.p	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFH	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/de	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnde	0%	Avira URL Cloud	safe	
http://www.carterandcone.coms0	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/Z	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comlg	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comde	0%	Avira URL Cloud	safe	
http://www.carterandcone.comego	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsb	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nonoise.duckdns.org	194.5.98.24	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nonoise.duckdns.org	true	• Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kra-d	gNrfORqjCV.exe, 00000000.00000003.297489904.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd$	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305929656.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305990317.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305838770.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305713164.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306618063.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306685172.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306515905.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305767077.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312116348.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304821209.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	gNrfORqjCV.exe, 00000000.00000003.304376908.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304218382.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304586978.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304481831.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/kurs	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300626397.00000000057DC000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsFu	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306515905.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	gNrfORqjCV.exe, 00000000.00000003.294783811.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krX	gNrfORqjCV.exe, 00000000.00000003.297489904.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297537163.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/-	gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	gNrfORqjCV.exe, 00000000.00000003.301383146.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalso	gNrfORqjCV.exe, 00000000.00000003.305608628.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305713164.00000000057E2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298672055.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	gNrfORqjCV.exe, 00000000.00000002.350708235.0000000002AAE000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.350708235.0000000002831000.00000004.00000800.00020000.00000000.sdmp, GzGmImHFmOq.exe, 00000007.00000002.454001802.0000000002AAF000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000008.00000002.561827065.0000000003059000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 0000000E.00000002.418053715.0000000003046000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790404.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300055029.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300121923.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessedQ	gNrfORqjCV.exe, 00000000.00000003.304720200.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304656866.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304821209.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0/u	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	gNrfORqjCV.exe, 00000000.00000003.307562749.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cntra	gNrfORqjCV.exe, 00000000.00000003.298397850.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298272672.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298235609.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298328560.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298175941.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298051431.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomd	gNrfORqjCV.exe, 00000000.00000003.304586978.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/H	gNrfORqjCV.exe, 00000000.00000003.300626397.00000000057DC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersno	gNrfORqjCV.exe, 00000000.00000003.312116348.00000000057E2000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/C	gNrfORqjCV.exe, 00000000.00000003.301848813.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301817563.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301964183.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301489951.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301383146.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301753239.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301721274.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301610181.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.302024144.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301642038.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.302116093.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301545636.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301786090.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	gNrfORqjCV.exe, 00000000.00000003.296515775.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296396139.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cni	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298672055.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	gNrfORqjCV.exe, 00000000.00000003.297575248.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFu	gNrfORqjCV.exe, 00000000.00000003.304720200.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304937014.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304656866.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305239978.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305277458.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305453770.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305332327.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305058105.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304821209.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305393745.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	gNrfORqjCV.exe, 00000000.00000003.304656866.00000000057F4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304586978.00000000057F3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalicS	gNrfORqjCV.exe, 00000000.00000003.303190287.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303341407.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/u	gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/t	gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300626397.00000000057DC000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/-	gNrfORqjCV.exe, 00000000.00000003.301848 813.00000000057E3000.00000004.00000020.0 0020000.00000000.sdmp, gNrfORqjCV.exe, 0 0000000.00000003.301275522.00000000057E3 000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301817563. 00000000057E3000.00000004.00000020.00020 000.00000000.sdmp, gNrfORqjCV.exe, 00000 000.00000003.301964183.00000000057E3000. 00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.3014 89951.00000000057E3000.00000004.00000020 .00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301383146.00000000057 E3000.00000004.00000020.00020000.0000000 0.sdmp, gNrfORqjCV.exe, 00000000.0000000 3.300916137.00000000057DE000.00000004.00 000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301753239.00000000057E300 0.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301721274.00 000000057E3000.00000004.00000020.0002000 0.00000000.sdmp, gNrfORqjCV.exe, 0000000 0.00000003.301610181.00000000057E3000.00 000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301642 038.00000000057E3000.00000004.00000020.0 0020000.00000000.sdmp, gNrfORqjCV.exe, 0 0000000.00000003.301335862.00000000057E4 000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807. 00000000057E1000.00000004.00000020.00020 000.00000000.sdmp, gNrfORqjCV.exe, 00000 000.00000003.301545636.00000000057E3000. 00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.3017 86090.00000000057E3000.00000004.00000020 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnicr	gNrfORqjCV.exe, 00000000.00000003.299416 168.00000000057E8000.00000004.00000020.0 0020000.00000000.sdmp, gNrfORqjCV.exe, 0 0000000.00000003.298397850.00000000057E8 000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298730476. 00000000057E8000.00000004.00000020.00020 000.00000000.sdmp, gNrfORqjCV.exe, 00000 000.00000003.299600985.00000000057E8000. 00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.2997 90040.00000000057E9000.00000004.00000020 .00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057 E9000.00000004.00000020.00020000.0000000 0.sdmp, gNrfORqjCV.exe, 00000000.0000000 3.298272672.00000000057E8000.00000004.00 000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298235609.00000000057E800 0.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00 000000057E9000.00000004.00000020.0002000 0.00000000.sdmp, gNrfORqjCV.exe, 0000000 0.00000003.298448695.00000000057E8000.00 000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298328 560.00000000057E8000.00000004.00000020.0 0020000.00000000.sdmp, gNrfORqjCV.exe, 0 0000000.00000003.298175941.00000000057DE 000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298516176. 00000000057E8000.00000004.00000020.00020 000.00000000.sdmp, gNrfORqjCV.exe, 00000 000.00000003.298672055.00000000057E8000. 00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.2988 49689.00000000057E9000.00000004.00000020 .00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057 E8000.00000004.00000020.00020000.0000000 0.sdmp, gNrfORqjCV.exe, 00000000.0000000 3.299112643.00000000057E9000.00000004.00 000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E800 0.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00 000000057E8000.00000004.00000020.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com.T	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/g	gNrfORqjCV.exe, 00000000.00000003.300626397.00000000057DC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersF	gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304218382.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comuevo	gNrfORqjCV.exe, 00000000.00000003.312305827.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312179725.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312571385.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312116348.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377294989.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312473392.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	gNrfORqjCV.exe, 00000000.00000003.305608628.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnani	gNrfORqjCV.exe, 00000000.00000003.298397850.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298272672.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298235609.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298328560.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298175941.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298051431.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cna-e	gNrfORqjCV.exe, 00000000.00000003.297957541.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298027129.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comFH	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnde	gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298672055.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnlg	gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298672055.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	gNrfORqjCV.exe, 00000000.00000003.297685163.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297575248.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297537163.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300055029.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300121923.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/de	gNrfORqjCV.exe, 00000000.00000003.298397850.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298272672.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298235609.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298328560.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298175941.00000000057DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTCH	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300055029.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/:	gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301489951.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301383146.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301610181.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301642038.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301545636.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersT	gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnno	gNrfORqjCV.exe, 00000000.00000003.298051431.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/~	gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301489951.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301383146.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301610181.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301642038.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301545636.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersR	gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.p	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comony	gNrfORqjCV.exe, 00000000.00000003.305453770.00000000057E2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	gNrfORqjCV.exe, 00000000.00000003.307784164.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	gNrfORqjCV.exe, 00000000.00000003.295899082.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296138391.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296240339.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.295949444.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296360113.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296039310.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296275045.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.295980858.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296109893.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.296305097.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/n	gNrfORqjCV.exe, 00000000.00000003.307562749.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/t-i	gNrfORqjCV.exe, 00000000.00000003.301275522.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersl	gNrfORqjCV.exe, 00000000.00000003.303341407.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.comC	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comB.TTF	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305929656.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305990317.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305838770.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305713164.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306515905.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305767077.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/g	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305990317.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerse	gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersb	gNrfORqjCV.exe, 00000000.00000003.304720200.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304937014.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304656866.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304821209.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fonts.com	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	gNrfORqjCV.exe, 00000000.00000003.297685163.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297489904.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297575248.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.297537163.00000000057E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

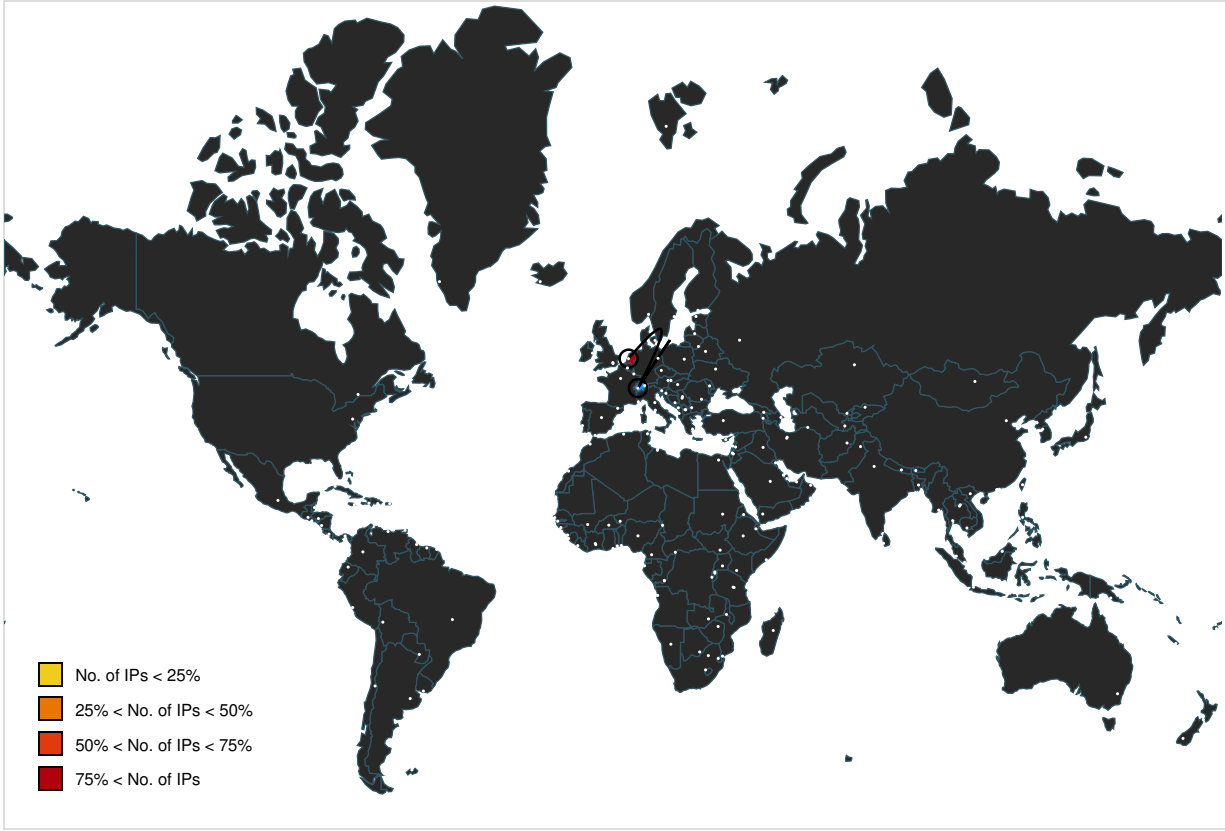
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersp	gNrfORqjCV.exe, 00000000.00000003.305608628.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305713164.00000000057E2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.come	gNrfORqjCV.exe, 00000000.00000003.294783811.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coms0	gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303683488.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	gNrfORqjCV.exe, 00000000.00000003.298516176.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	gNrfORqjCV.exe, 00000000.00000003.306269906.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305929656.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305990317.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304720200.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305838770.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312305827.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305608628.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306376678.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305713164.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304937014.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303190287.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304656866.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.305239978.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303341407.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304376908.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306223458.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306133463.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306459708.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.306044876.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303683488.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.comTC	gNrfORqjCV.exe, 00000000.00000003.298730476.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300055029.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300121923.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdy	gNrfORqjCV.exe, 00000000.00000003.304376908.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303683488.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304218382.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304481831.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comego	gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/Z	gNrfORqjCV.exe, 00000000.00000003.307562749.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comion	gNrfORqjCV.exe, 00000000.00000003.312305827.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312042266.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312179725.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312571385.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312116348.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377294989.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312473392.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comde	gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/u	gNrfORqjCV.exe, 00000000.00000003.300626397.00000000057DC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	gNrfORqjCV.exe, 00000000.00000003.300916137.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300843664.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301610181.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301642038.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301335862.00000000057E4000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301052807.00000000057E1000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.301545636.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	gNrfORqjCV.exe, 00000000.00000003.304376908.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304071114.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303960292.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304218382.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.304481831.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.303851330.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comlg	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299600985.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299790040.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	gNrfORqjCV.exe, 00000000.00000003.298175941.00000000057DE000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298516176.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377796505.00000000069D2000.00000004.00000800.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298672055.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298849689.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300055029.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.300121923.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298912231.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299112643.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298027129.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.298051431.00000000057E0000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299908418.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comf	gNrfORqjCV.exe, 00000000.00000003.312305827.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312042266.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312179725.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312571385.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312116348.00000000057E2000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000002.377294989.00000000057E3000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.312473392.00000000057E3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comsb	gNrfORqjCV.exe, 00000000.00000003.299416168.00000000057E8000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299451966.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299359743.00000000057E9000.00000004.00000020.00020000.00000000.sdmp, gNrfORqjCV.exe, 00000000.00000003.299189314.00000000057E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.24	nonoise.duckdns.org	Netherlands		208476	DANILENKODE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800437
Start date and time:	2023-02-07 13:54:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	gNrfORqjCV.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@37/23@20/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.8%) • Quality average: 67.6% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:55:12	API Interceptor	731x Sleep call for process: gNrfORqjCV.exe modified
13:55:20	API Interceptor	148x Sleep call for process: powershell.exe modified
13:55:22	Task Scheduler	Run new task: GzGmImHFmOq path: C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
13:55:31	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\gNrfORqjCV.exe" s>$(Arg0)
13:55:32	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
13:55:35	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:55:40	API Interceptor	2x Sleep call for process: dhcpmon.exe modified
13:55:42	API Interceptor	1x Sleep call for process: GzGmImHFmOq.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	941568
Entropy (8bit):	7.676646011154186
Encrypted:	false
SSDEEP:	12288:77S45nJrTmHkFrVoaqnS/pjpkH7PRNNiJTp/cuP1FRkkYy27YBp7HwcBVw:nS4PkkFr2QJ6HdaTp081L4y2Qasw
MD5:	60C8D91ADFA30A60AFA2F5437CE7D041
SHA1:	F8460389F343481D7420073AD1DA2F90DDEDC696
SHA-256:	5707C702F70CC5BF864E10AAAB48F9300E3BE0A7892D8FAA1810145F0AF93D2D
SHA-512:	38DE4CFCD5A1E75AF8E730B7F459D545108306BCFE06C2D315FB70B72DD75F550F21E0078F7AE4214D03BBBC5FDD4A3DE8500254534842E6EB8321693F5062C0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.c.....0..V.....>u... .....@.. ....@.....t..O..... ....H.....text...DU... ...V..... ..`.rsrc.....X.....@..@.rel oc.....\.....@..B..... u.....H.....K...B.....-.....{....*..{....*V.(.....}.....}....*...0..C.....u.....6.,0(.....{.....{....o.....,(.....{.....{....o. ...+..+..*. ...U)UU.Z(.....{....o....X)UU.Z(.....{....o....X*.0..b.....r...p.....%..{.....%q.....-.&.+.....o ....%..{.....%q.....-.&.+.....o ....(!...*&.(.....*.0..V.....(.....}.....}..... s"...}.....+&...+...{.....(#.....X.....-....X.....-.*...0.....rG.

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

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GzGmImHFmOq.exe.log

Process:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gNrfORqjCV.exe.log	
Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21748
Entropy (8bit):	5.600772758637283
Encrypted:	false
SSDEEP:	384:LtCRLq0gJcKuAax0rq/3ISVxyjulrItiiJ9glSJuyzSv0ZqbAVrdJQBR3BT+inY8:0KuAaxgUxyClrSSlBBs4wXoY8
MD5:	13AAEA93CDE8136DA48D5BF09ADF3B60
SHA1:	0450C3870498BB682CE4010CE9F85A1D6DC8774C
SHA-256:	C68305D299D55E533CD4DFA704D41EF40C81EB455BE38414FC6458A777A8C0F4
SHA-512:	460B8B08B988E680BDFD0869B5EB0E862A89099BB60A146F7A3EFA55CA9BDE803028C18FCFED4A5B154955C9A7ED42BD9B8801CD6AAC230E4F072B2CFA6155C
Malicious:	false
Preview:	@...e.....d.7...b.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1j2kljyl.nvz.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_amg03k4b.ntk.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fkpvekda.sks.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ilozur5r.kfw.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_llqraot0.bne.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_n0npb1fb.bd2.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oj43ruk0.xkr.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p15ocwwh.bio.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2556.tmp

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.111180834949932
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Pcxtn:cbk4oL600QydbQxIYODOLedq3Scj
MD5:	205A4E2EE65AB288C6B92DB204349ACF
SHA1:	2F645852F3AB280F7FC170545EDBC557356DE80E
SHA-256:	5FBCDCDB9CE1FDCA116227AFE38D307CEA461D64D653BD23F20BA3872EA85B72
SHA-512:	77550160EAB85A1B52DBCB26F4D6DA3C4BED08DB7E220AC320937EEABFEA3755C0EA0354D691C803CBF8100A96BB67B06C9C30829876BC5EFA7941A02E3331 A5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp27D7.tmp

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

C:\Users\user\AppData\Local\Temp\tmp389B.tmp

Process:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1602
Entropy (8bit):	5.140535559819237
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNt2xvn:cgeCaYrFdOFzOzN33ODOiDdKrsuT6v

MD5:	7249F2169DE65C5704FB934EEAF9D7BF
SHA1:	6A0CB99EB5C1D4ABB0F5A8A6993ABD92DAAC126A
SHA-256:	A8E9843BC4C116B227EF3AD89E1BE8CB9C501370421504FEB5E82C66C8879247
SHA-512:	64D47BBC462F714DE847F49C3FF66F0B9880CFBFB0EB8DE3FC8FE657FF12F9922E256225A91EED819A82B97BB5408053B7FBCB7F7889065C535C281F8B9DD82D
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmp78F4.tmp

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1602
Entropy (8bit):	5.140535559819237
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt2xvn:cgeCaYrFdOFzOzN33ODOiDdKrsuT6v
MD5:	7249F2169DE65C5704FB934EEAF9D7BF
SHA1:	6A0CB99EB5C1D4ABB0F5A8A6993ABD92DAAC126A
SHA-256:	A8E9843BC4C116B227EF3AD89E1BE8CB9C501370421504FEB5E82C66C8879247
SHA-512:	64D47BBC462F714DE847F49C3FF66F0B9880CFBFB0EB8DE3FC8FE657FF12F9922E256225A91EED819A82B97BB5408053B7FBCB7F7889065C535C281F8B9DD82D
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmpEAF8.tmp

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1602
Entropy (8bit):	5.140535559819237
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt2xvn:cgeCaYrFdOFzOzN33ODOiDdKrsuT6v
MD5:	7249F2169DE65C5704FB934EEAF9D7BF
SHA1:	6A0CB99EB5C1D4ABB0F5A8A6993ABD92DAAC126A
SHA-256:	A8E9843BC4C116B227EF3AD89E1BE8CB9C501370421504FEB5E82C66C8879247
SHA-512:	64D47BBC462F714DE847F49C3FF66F0B9880CFBFB0EB8DE3FC8FE657FF12F9922E256225A91EED819A82B97BB5408053B7FBCB7F7889065C535C281F8B9DD82D
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

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

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:KF:KF
MD5:	84F57A2CCBF5202D84064D529BC5F7F1

SHA1:	48D0C7CADD8EF77664087CAF8474E57C77FAB1AA
SHA-256:	BC484715C0A8CFC52127533FEFB1FE211599F6FD7CAC1183A15C1449E255DBFD
SHA-512:	B4AB763748F3F445E55CCF2A85A9684BF392E5903F4F8253C4F61637099419469895DB23C92EF5C9BC0138B325D57A40F75153C638BF371D41EE79AB0DED11CA
Malicious:	**true**
Preview:	.pV.V..H

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

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.405822250285692
Encrypted:	false
SSDEEP:	3:oNUWJRWCfqGi4A:oNNJACfq6A
MD5:	2C464CA33435236989E7B48201539321
SHA1:	BF6ED3B301DE5F4AE68C17E4CC826C70DE058248
SHA-256:	E8D74AB7595A22F57A930F896093E42870EFCF9CC6FF801D97F0E31073B03D28
SHA-512:	45E51DC7DCDD94F0EE2011AD5AE05A88E3D14825F0F4C46E9B8C55F19C7ECA4D096E28727D0BEA57590E9D02E030F12B001A4C4E53B382671084CA3CB51B73 27
Malicious:	false
Preview:	C:\Users\user\Desktop\gNrfORqjCV.exe

C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	941568
Entropy (8bit):	7.676646011154186
Encrypted:	false
SSDEEP:	12288:77S45nJrTmHkFrVoaqnS/pjpkH7PRNNiJTp/cuP1FRkkYy27YBp7HwcBVw:nS4PkkFr2QJ6HdaTp081L4y2Qasw
MD5:	60C8D91ADFA30A60AFA2F5437CE7D041
SHA1:	F8460389F343481D7420073AD1DA2F90DDEDC696
SHA-256:	5707C702F70CC5BF864E10AAAB48F9300E3BE0A7892D8FAA1810145F0AF93D2D
SHA-512:	38DE4CFCD5A1E75AF8E730B7F459D545108306BCFE06C2D315FB70B72DD75F550F21E0078F7AE4214D03BBBC5FDD4A3DE8500254534842E6EB8321693F5062C 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.c.....0..V.....>u... .....@.. ....@.....t..O..... ....H.....text...DU... ...V..... ..`.rsrc.....X.....@..@.rel oc.....\.....@..B..... u.....H.....K...B.....-.....{....*..{....*V.(.....}.....}....*...0..C.....u.....6.,0(.....{.....{....o.....,(.....{.....{....o. ...+..+..*. ...U)UU.Z(.....{....o....X)UU.Z(.....{....o....X*.0..b.....r...p.....%..{.....%q.....-.&.+.....o ....%..{.....%q.....-.&.+.....o ....(!...*&.(.....*.0..V.....(.....}.....}..... s"...}.....+&...+...{.....(#.....X.....-....X.....-.*...0.....rG.

C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\gNrfORqjCV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.676646011154186
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	gNrfORqjCV.exe
File size:	941568
MD5:	60c8d91adfa30a60afa2f5437ce7d041
SHA1:	f8460389f343481d7420073ad1da2f90ddedc696
SHA256:	5707c702f70cc5bf864e10aaab48f9300e3be0a7892d8faa1810145f0af93d2d
SHA512:	38de4cfcd5a1e75af8e730b7f459d545108306bcfe06c2d315fb70b72dd75f550f21e0078f7ae4214d03bbbc5fdd4a3de8500254534842e6eb8321693f5062c0
SSDEEP:	12288:77S45nJrTmHkFrVoaqnS/pjpkH7PRNNiJTp/cuP1FRkkYy27YBp7HwcBVw:nS4PkkFr2QJ6HdaTp081L4y2Qasw
TLSH:	82159D5119AB43E6ECF98D7832B8E61826A28CD2476D9D3EBC863D7A8CF370F4451711
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.c.....0..V.....>u... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e753e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63C94CB9 [Thu Jan 19 13:59:21 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe74ec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x3a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe5544	0xe5600	False	0.8197239015667575	data	7.680692465060209	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x3a4	0x400	False	0.3837890625	data	2.942309763240296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

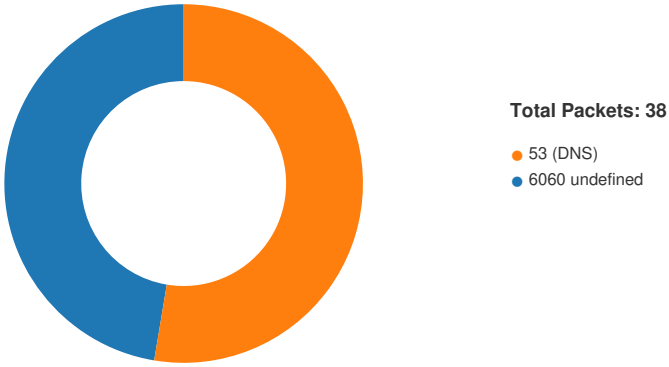
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8058	0x348	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 13:55:35.385148048 CET	49701	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:35.746256113 CET	6060	49701	194.5.98.24	192.168.2.5
Feb 7, 2023 13:55:36.263089895 CET	49701	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:36.502480984 CET	6060	49701	194.5.98.24	192.168.2.5
Feb 7, 2023 13:55:37.060009956 CET	49701	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:37.292237043 CET	6060	49701	194.5.98.24	192.168.2.5
Feb 7, 2023 13:55:45.062972069 CET	49702	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:45.285547972 CET	6060	49702	194.5.98.24	192.168.2.5
Feb 7, 2023 13:55:45.967027903 CET	49702	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:46.183325052 CET	6060	49702	194.5.98.24	192.168.2.5
Feb 7, 2023 13:55:46.764082909 CET	49702	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:55:46.995682001 CET	6060	49702	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:08.145855904 CET	49705	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:08.364366055 CET	6060	49705	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:08.953275919 CET	49705	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:09.165040970 CET	6060	49705	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:09.765851021 CET	49705	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:09.983294964 CET	6060	49705	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:39.798890114 CET	49712	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:40.003993034 CET	6060	49712	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:40.518403053 CET	49712	6060	192.168.2.5	194.5.98.24

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 13:56:40.723225117 CET	6060	49712	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:41.228743076 CET	49712	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:41.443243027 CET	6060	49712	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:54.732409954 CET	49713	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:57.188936949 CET	6060	49713	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:57.863878965 CET	49713	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:58.096165895 CET	6060	49713	194.5.98.24	192.168.2.5
Feb 7, 2023 13:56:58.598249912 CET	49713	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:56:58.812616110 CET	6060	49713	194.5.98.24	192.168.2.5
Feb 7, 2023 13:57:02.917262077 CET	49715	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:57:05.326845884 CET	6060	49715	194.5.98.24	192.168.2.5
Feb 7, 2023 13:57:05.842473984 CET	49715	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:57:07.717140913 CET	6060	49715	194.5.98.24	192.168.2.5
Feb 7, 2023 13:57:08.230956078 CET	49715	6060	192.168.2.5	194.5.98.24
Feb 7, 2023 13:57:12.010140896 CET	6060	49715	194.5.98.24	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 13:55:34.256066084 CET	60649	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:35.317756891 CET	60649	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:35.370954037 CET	53	60649	84.200.69.80	192.168.2.5
Feb 7, 2023 13:55:44.998558044 CET	51441	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:45.034903049 CET	53	51441	84.200.69.80	192.168.2.5
Feb 7, 2023 13:55:53.838025093 CET	49724	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:54.828720093 CET	49724	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:57.980149031 CET	49724	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:55:59.984153032 CET	49724	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:04.031718969 CET	49724	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:08.101353884 CET	65323	53	192.168.2.5	84.200.70.40
Feb 7, 2023 13:56:08.142416954 CET	53	65323	84.200.70.40	192.168.2.5
Feb 7, 2023 13:56:31.261082888 CET	55039	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:32.283844948 CET	55039	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:33.328063011 CET	55039	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:35.691873074 CET	55039	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:39.746449947 CET	55039	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:39.797384977 CET	53	55039	84.200.69.80	192.168.2.5
Feb 7, 2023 13:56:45.474669933 CET	60975	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:46.489002943 CET	60975	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:47.535037041 CET	60975	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:49.536046982 CET	60975	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:53.621021986 CET	60975	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:56:53.668188095 CET	53	60975	84.200.69.80	192.168.2.5
Feb 7, 2023 13:57:02.882363081 CET	55068	53	192.168.2.5	84.200.69.80
Feb 7, 2023 13:57:02.916222095 CET	53	55068	84.200.69.80	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 13:55:34.256066084 CET	192.168.2.5	84.200.69.80	0x9980	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:35.317756891 CET	192.168.2.5	84.200.69.80	0x9980	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:44.998558044 CET	192.168.2.5	84.200.69.80	0x64c6	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:53.838025093 CET	192.168.2.5	84.200.69.80	0x4229	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:54.828720093 CET	192.168.2.5	84.200.69.80	0x4229	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:57.980149031 CET	192.168.2.5	84.200.69.80	0x4229	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false

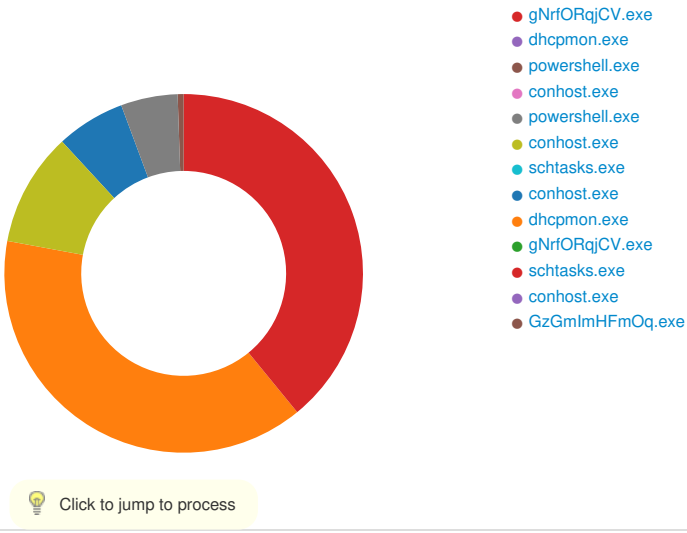
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 13:55:59.984153032 CET	192.168.2.5	84.200.69.80	0x4229	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:04.031718969 CET	192.168.2.5	84.200.69.80	0x4229	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:08.101353884 CET	192.168.2.5	84.200.70.40	0x8c8	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:31.261082888 CET	192.168.2.5	84.200.69.80	0x790f	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:32.283844948 CET	192.168.2.5	84.200.69.80	0x790f	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:33.328063011 CET	192.168.2.5	84.200.69.80	0x790f	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:35.691873074 CET	192.168.2.5	84.200.69.80	0x790f	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:39.746449947 CET	192.168.2.5	84.200.69.80	0x790f	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:45.474669933 CET	192.168.2.5	84.200.69.80	0x7de9	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:46.489002943 CET	192.168.2.5	84.200.69.80	0x7de9	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:47.535037041 CET	192.168.2.5	84.200.69.80	0x7de9	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:49.536046982 CET	192.168.2.5	84.200.69.80	0x7de9	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:53.621021986 CET	192.168.2.5	84.200.69.80	0x7de9	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:57:02.882363081 CET	192.168.2.5	84.200.69.80	0x8867	Standard query (0)	nonoise.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 13:55:35.370954037 CET	84.200.69.80	192.168.2.5	0x9980	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:55:45.034903049 CET	84.200.69.80	192.168.2.5	0x64c6	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:08.142416954 CET	84.200.70.40	192.168.2.5	0x8c8	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:39.797384977 CET	84.200.69.80	192.168.2.5	0x790f	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:56:53.668188095 CET	84.200.69.80	192.168.2.5	0x7de9	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:57:02.916222095 CET	84.200.69.80	192.168.2.5	0x8867	No error (0)	nonoise.duckdns.org		194.5.98.24	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: gNrfORqjCV.exe PID: **5240**, Parent PID: **3324**

General

Target ID:	0
Start time:	13:55:01
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\gNrfORqjCV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gNrfORqjCV.exe
Imagebase:	0x430000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.350708235.0000000002AAE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.356107386.0000000003E97000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.356107386.0000000003E97000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.356107386.0000000003E97000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.356107386.0000000003E97000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.350708235.0000000002831000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7117DD66	CopyFileW
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7117DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp78F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71177038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gNrfORqjCV.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp78F4.tmp	success or wait	1	71176A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4c fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 56 0e 00 00 06 00 00 00 00 00 00 3e 75 0e 00 00 20 00 00 00 fd 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELLc0V>u @ @	success or wait	4	7117DD66	CopyFileW
C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7117DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp78F4.tmp	0	1602	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	71171B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gNrfORqjCV.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7253C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71171B4F	ReadFile

Analysis Process: powershell.exe PID: **492**, Parent PID: **5240**

General

Target ID:	1
Start time:	13:55:13
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\gNrfORqjCV.exe
Imagebase:	0xf00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_amg03k4b.ntk.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ilozur5r.kfw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_amg03k4b.ntk.ps1	success or wait	1	71176A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ilozur5r.kfw.psm1	success or wait	1	71176A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_amg03k4b.ntk.ps1	0	1	31	1	success or wait	1	71171B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ilozur5r.kfw.psm1	0	1	31	1	success or wait	1	71171B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 13 00 00 18 00 00 00 fd 0d fd 04 fd 08 fd 08 fd 08 00 00 64 00 37 00 05 00 62 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@ed7b@	success or wait	1	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 35 26 40 01 37 26 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BM@D@mE@EM@q@q@S@%@n@4&@5&@7&@	success or wait	11	724F76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72211F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7221203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	95	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile

Analysis Process: conhost.exe PID: **5684**, Parent PID: **492**

General

Target ID:	2
Start time:	13:55:13
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: powershell.exe PID: **1544**, Parent PID: **5240**

General

Target ID:	3
Start time:	13:55:14
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Imagebase:	0xf00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	710D5B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	710D5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n0npb1fb.bd2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p15ocwwh.bio.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n0npb1fb.bd2.ps1	success or wait	1	71176A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p15ocwwh.bio.psm1	success or wait	1	71176A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n0npb1fb.bd2.ps1	0	1	31	1	success or wait	1	71171B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p15ocwwh.bio.psm1	0	1	31	1	success or wait	1	71171B4F	WriteFile
unknown	503	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7209EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 13 00 00 18 00 00 00 fd 0d fd 04 fd 08 fd 08 fd 08 00 00 64 00 37 00 05 00 62 0d 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ed7b@	success or wait	1	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	724F76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 35 26 40 01 37 26 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BM@D@mE@EM@q@q@S@%@n@4&@5&@7&@	success or wait	11	724F76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72211F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7221203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	104	71171B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71171B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71171B4F	ReadFile

Analysis Process: conhost.exe PID: 4720, Parent PID: 1544

General

Target ID:	4

Start time:	13:55:14
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5936**, Parent PID: **5240**

General

Target ID:	5
Start time:	13:55:14
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmp78F4.tmp
Imagebase:	0xcc0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp78F4.tmp	unknown	2	success or wait	1	CCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp78F4.tmp	unknown	1603	success or wait	1	CCABD9	ReadFile

Analysis Process: conhost.exe PID: **6036**, Parent PID: **5936**

General

Target ID:	6
Start time:	13:55:14
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: GzGmImHFmOq.exe PID: **5000**, Parent PID: **1084**

General

Target ID:	7
Start time:	13:55:22
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Imagebase:	0x530000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.463703676.0000000003F1F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.463703676.0000000003F1F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.463703676.0000000003F1F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.463703676.0000000003F1F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.454001802.0000000002AAF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 64%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp389B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71177038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GzGmImHFmOq.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp389B.tmp	success or wait	1	71176A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp389B.tmp	0	1602	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	71171B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GzGmImHFmOq.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7253C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71171B4F	ReadFile

Analysis Process: gNrfORqjCV.exe PID: **5320**, Parent PID: **5240**

General

Target ID:	8
Start time:	13:55:25
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\gNrfORqjCV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gNrfORqjCV.exe
Imagebase:	0xbb0000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
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: 00000008.00000002.571677772.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.571677772.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.571677772.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000008.00000002.571677772.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.574171475.0000000005A70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.574171475.0000000005A70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.574171475.0000000005A70000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.574171475.0000000005A70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000008.00000002.574171475.0000000005A70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000008.00000002.561827065.0000000003059000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7117BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7117BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7117DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7117DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2556.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71177038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71171E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp27D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71177038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7117BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7117BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2556.tmp	success or wait	1	71176A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp27D7.tmp	success or wait	1	71176A95	DeleteFileW
C:\Users\user\Desktop\gNrfORqjCV.exe:Zone.Identifier	success or wait	1	710F2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 70 56 07 56 09 fd 48	pVVH	success or wait	1	71171B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4c fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 56 0e 00 00 06 00 00 00 00 00 00 3e 75 0e 00 00 20 00 00 00 fd 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELLc0V>u @ @	success or wait	4	7117DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7117DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2556.tmp	0	1301	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71171B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	38	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 67 4e 72 66 4f 52 71 6a 43 56 2e 65 78 65	C:\Users\user\Desktop\gNrfORqjCV.exe	success or wait	1	71171B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27D7.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71171B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71171B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\gNrfORqjCV.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\gNrfORqjCV.exe	unknown	512	success or wait	1	721ED72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	7117646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **5256**, Parent PID: **5320**

General	
Target ID:	10
Start time:	13:55:30
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp2556.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **5228**, Parent PID: **5256**

General	
Target ID:	11
Start time:	13:55:30
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6016**, Parent PID: **5320**

General	
Target ID:	12
Start time:	13:55:31
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp27D7.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6108**, Parent PID: **6016**

General	
Target ID:	13
Start time:	13:55:31
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: gNrfORqjCV.exe PID: **5248**, Parent PID: **1084**

General

Target ID:	14
Start time:	13:55:32
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\gNrfORqjCV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gNrfORqjCV.exe 0
Imagebase:	0x820000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
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.00000002.425767553.00000000042E7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.425767553.00000000042E7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.425767553.00000000042E7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.425767553.00000000042E7000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **4544**, Parent PID: **1084**

General

Target ID:	15
Start time:	13:55:32
Start date:	07/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x740000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.394849296.0000000002F5E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 64%, ReversingLabs

Analysis Process: powershell.exe PID: **1252**, Parent PID: **5248**

General

Target ID:	16
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\gNrfORqjCV.exe
Imagebase:	0xf00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5244**, Parent PID: **1252**

General

Target ID:	17
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **400**, Parent PID: **5248**

General

Target ID:	18
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Imagebase:	0xf00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **1640**, Parent PID: **400**

General

Target ID:	19
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5684**, Parent PID: **5248**

General	
Target ID:	20
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmpEAF8.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6036**, Parent PID: **5684**

General	
Target ID:	21
Start time:	13:55:43
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4720**, Parent PID: **3324**

General	
Target ID:	22
Start time:	13:55:44
Start date:	07/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xc10000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: gNrfORqjCV.exe PID: **1324**, Parent PID: **5248**

General	
Target ID:	23
Start time:	13:55:50
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\gNrfORqjCV.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gNrfORqjCV.exe
Imagebase:	0x4e0000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
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: 00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000002.436230882.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.440525605.0000000003939000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.440525605.0000000003939000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000002.440525605.0000000003939000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.439566387.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.439566387.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000002.439566387.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5660**, Parent PID: **5000**

General	
Target ID:	26
Start time:	13:56:04
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GzGmImHFmOq" /XML "C:\Users\user\AppData\Local\Temp\tmp389B.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5260**, Parent PID: **5660**

General	
Target ID:	27
Start time:	13:56:04
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: GzGmImHFmOq.exe PID: **5544**, Parent PID: **5000**

General	
Target ID:	28
Start time:	13:56:07
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\GzGmImHFmOq.exe
Imagebase:	0xc50000
File size:	941568 bytes
MD5 hash:	60C8D91ADFA30A60AFA2F5437CE7D041
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.476397038.0000000003191000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.476397038.0000000003191000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000002.476397038.0000000003191000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Disassembly

No disassembly