ID: 712322
Sample Name: new order.exe
Cookbook: default.jbs
Time: 07:35:23
Date: 29/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

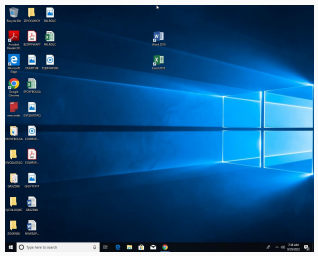
Windows Analysis Report

new order.exe

Overview

General Information

Sample Name:	new order.exe
Analysis ID:	712322
MD5:	450aa1d2ac8e10..
SHA1:	173275f693a10f8.
SHA256:	316ff42588b6cf8..
Tags:	exe NanoCore
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

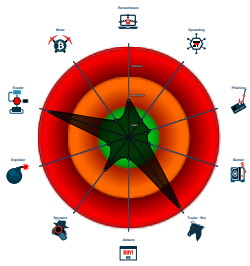
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Connects to many ports of the same…
- .NET source code references suspic…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- new order.exe (PID: 5796 cmdline: "C:\Users\user\Desktop\new order.exe" MD5: 450AA1D2AC8E10A3B8363FE2945462BD)
  - powershell.exe (PID: 492 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - InstallUtil.exe (PID: 2344 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Luqkasd.exe (PID: 1016 cmdline: "C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe" MD5: 450AA1D2AC8E10A3B8363FE2945462BD)
  - powershell.exe (PID: 5636 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Luqkasd.exe (PID: 628 cmdline: "C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe" MD5: 450AA1D2AC8E10A3B8363FE2945462BD)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6a8dc68c-2ae6-4a66-b5dc-80cfa679",
  "Group": "jop",
  "Domain1": "146.70.76.43",
  "Domain2": "",
  "Port": 56281,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 9,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.527779375.00000000033BB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2aa65:$a: NanoCore • 0x2ac25:$a: NanoCore • 0x2d674:$a: NanoCore • 0x2d69a:$a: NanoCore • 0x2d9cb:$a: NanoCore • 0x350aa:$a: NanoCore • 0x2d67d:$b: ClientPlugin • 0x2d6a3:$b: ClientPlugin • 0x2d9d4:$b: ClientPlugin • 0x3456b:$c: ProjectData • 0x2fd3a:$d: DESCrypto • 0x304b5:$e: KeepAlive • 0x2f5e7:$g: LogClientMessage • 0x2dc43:$i: get_Connected • 0x2acf4:$j: #=q • 0x2ad38:$j: #=q • 0x2ad54:$j: #=q • 0x2ad96:$j: #=q • 0x2adb2:$j: #=q • 0x2adce:$j: #=q • 0x2ae26:$j: #=q
00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2d69a:$a1: NanoCore.ClientPluginHost • 0x2d9cb:$a2: NanoCore.ClientPlugin • 0x2d6c7:$b1: get_BuilderSettings • 0x35047:$b2: ClientLoaderForm.resources • 0x2b5d5:$b3: PluginCommand • 0x2ddba:$b4: IClientAppHost • 0x319bc:$b5: GetBlockHash • 0x2dccf:$b6: AddHostEntry • 0x2f5d4:$b7: LogClientException • 0x2dc90:$b8: PipeExists • 0x2dda7:$b9: IClientLoggingHost
0000000F.00000002.527200680.0000000003371000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Click to see the 40 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.new order.exe.412f488.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5044d:$x1: NanoCore Client.exe • 0x50dfd:$s1: PluginCommand • 0x50df1:$s2: FileCommand
0.2.new order.exe.5570000.5.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
14.2.InstallUtil.exe.5e04629.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
14.2.InstallUtil.exe.5e04629.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
14.2.InstallUtil.exe.5e04629.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 87 entries

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

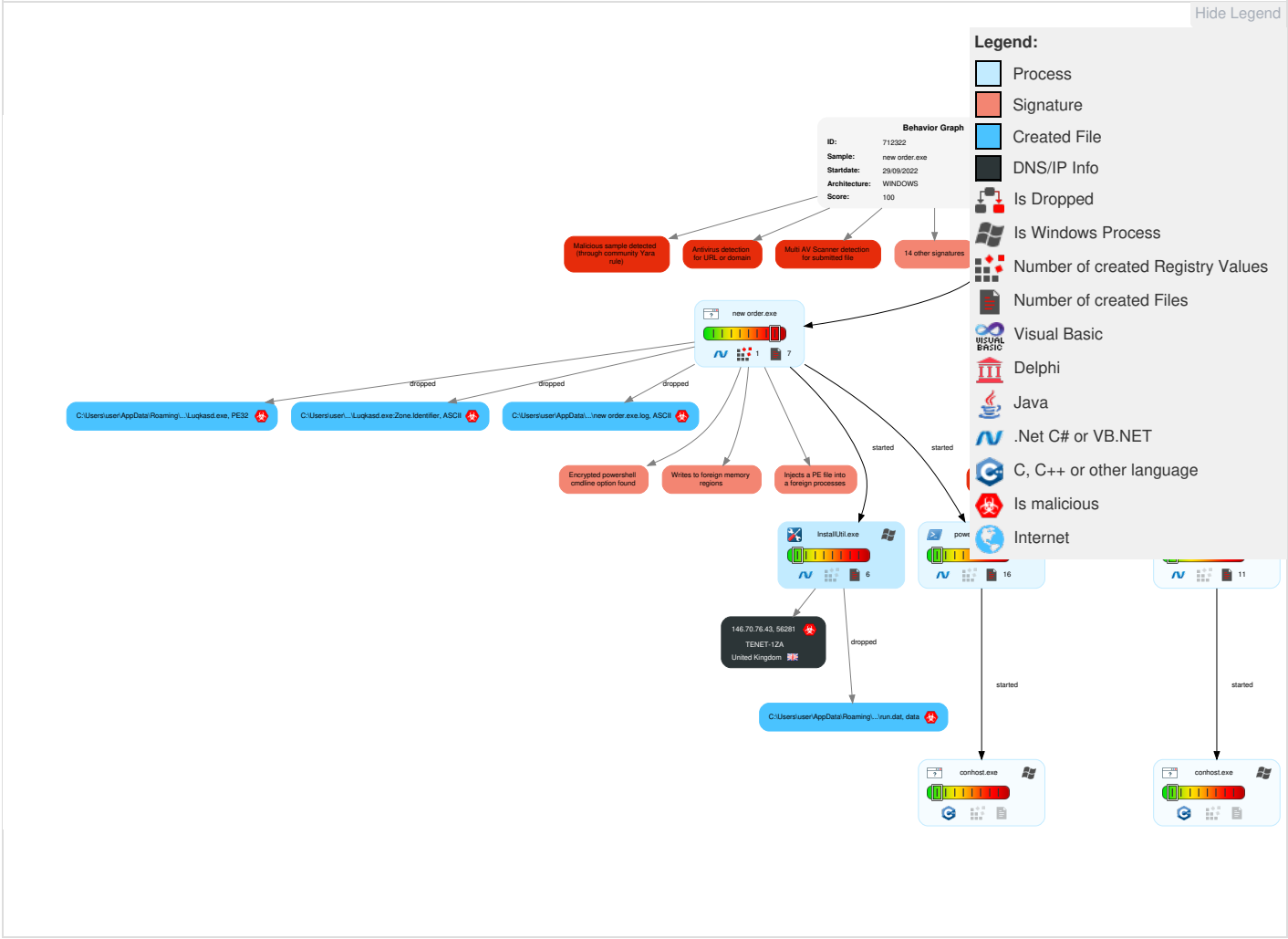
Yara detected Nanocore RAT

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 Native API	1 Registry Run Keys / Startup Folder	2 1 2 Process Injection	1 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	1 PowerShell	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	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	2 3 Software Packing	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 Timestomp	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

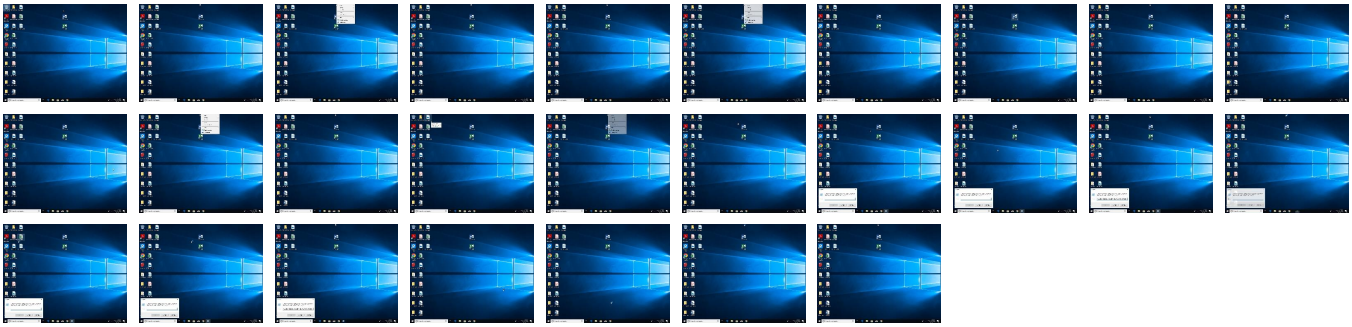
Behavior Graph



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
new order.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
new order.exe	35%	Virustotal		Browse
new order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.InstallUtil.exe.5e00000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.naver.com0	0%	Avira URL Cloud	safe	
146.70.76.43	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

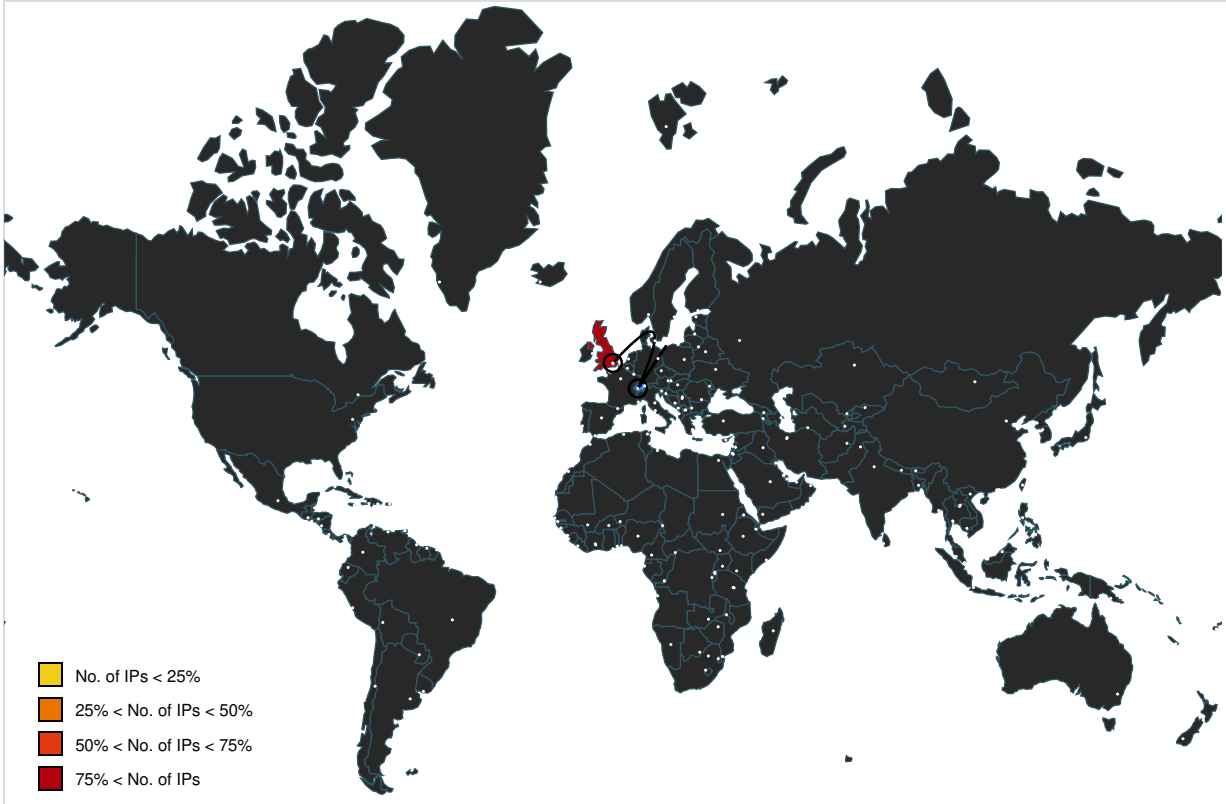
Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
146.70.76.43	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/json	new order.exe, 00000000.00000002.464712592.00000000040FB000.00000004.00000800.00020000.00000000.sdmp, new order.exe, 00000000.00000002.455076504.000000003120000.00000004.00000800.00020000.00000000.sdmp, new order.exe, 00000000.00000002.471486860.0000000005780000.00000004.08000000.00040000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.548140629.0000000004519000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.547142354.0000000004478000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.529612367.0000000003473000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.548137482.0000000004599000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.529846388.00000000034F5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.naver.com0	new order.exe, Luqkasd.exe.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.nuget.org/packages/Newtonsoft.Json.Bson	new order.exe, 00000000.00000002.464712592.00000000040FB000.00000004.00000800.00020000.00000000.sdmp, new order.exe, 00000000.00000002.455076504.000000000312000 0.00000004.00000800.00020000.00000000.sdmp, new order.exe, 00000000.00000002.471486860.0000000005780000.00000004.08000000.00040000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.529612367.0000000003473000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.547137071.00000044F7000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.529846388.00000000034F5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	new order.exe, Luqkasd.exe.0.dr	false		high
http://https://api.telegram.org/bot	new order.exe, 00000000.00000002.453841918.0000000003031000.00000004.00000800.00020000.00000000.sdmp, new order.exe, 00000000.00000002.457661334.00000000032A8000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.527779375.00000000033BB000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.527200680.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.533387647.00000000035B4000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 0000000F.00000002.527732524.00000000033B2000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.528679468.000000000347F000.00000004.00000800.00020000.00000000.sdmp, Luqkasd.exe, 00000010.00000002.527935405.000000000343B000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	InstallUtil.exe, 0000000E.00000002.527475187.0000000002D29000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	Luqkasd.exe, 00000010.00000002.529846388.00000000034F5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	new order.exe, Luqkasd.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	Luqkasd.exe, 00000010.00000002.529846388.00000000034F5000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.70.76.43	unknown	United Kingdom		2018	TENET-1ZA	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	712322
Start date and time:	2022-09-29 07:35:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	new order.exe
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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/10@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:36:47	API Interceptor	44x Sleep call for process: powershell.exe modified
07:37:51	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Luqkasd "C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe"
07:38:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Luqkasd "C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe"
07:38:06	API Interceptor	174x Sleep call for process: InstallUtil.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\new order.exe.log

Process:	C:\Users\user\Desktop\new order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1039
Entropy (8bit):	5.3436815157474165
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhyE4KdE4KBLWE4K5AE4Kzr7a:MxHKXwYHKhQnoyHKdHKBqHK5AHKzva
MD5:	6C24176D343957C767AA6536571797FA
SHA1:	64512F67A49AF75E9A67474DF54FCCD3472905B2
SHA-256:	63AB82B5B458425DB1E0831E1BB8CA642C602D9BCB0762A1E47C7836CACF3350
SHA-512:	D0DFB30B723CC1F0ADB8D9448220AC67A1A21243499B7EB31402CAA0CE9F6A892073E10C52D132E59BF2321F05DBB0973B7E1026023992FC33DE5AB74A6979A4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87

SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E7
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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):	16448
Entropy (8bit):	5.551990926311433
Encrypted:	false
SSDEEP:	384:7Qte/Rq0GSP0xBun3ISBxn2uRRiJ9g2SJ3uzp1sYv:tPkBoY4x2uRp2cuVv
MD5:	2A49B5586BCDEEEF2C02C25542EDF919
SHA1:	5D379D96F470A651A8D0AB3FC1B53472D5562401
SHA-256:	DA695E44D352095F10E2DDF1AFE4FED655008FD354AD949A0E8E8B8E7D6398E2
SHA-512:	19CC7E7C44301A1E27D462CD8C698FAD8852AF2A8E5965CCFD2F4FDD646B15EFEA4CCB494D5456FBC1C1744B01EE3FA2A2707BB5799C0BB847747871A8BF393
Malicious:	false
Preview:	@...e.....9.7.....@.....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_coyhehte.2fz.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_erq5o4m0.rrv.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_jawkttfp.mf4.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_mmo010fb.3b2.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ddVl:ddVl
MD5:	A66EC82C3FF14A24BEB60BCA681BB005
SHA1:	00C5B9BA7A189EF2B13C666788B72081A2719BAB
SHA-256:	A8E642B7C67C3DEC55C98E7AFC170A5E6017C2DC79A0FFF98B67FE52CAEFACBC
SHA-512:	AA006579440262E0FE026413F4135D55316D3B248C147FD725FC996D47FFFF3E1033ABA2CC203D0193BF5F962EDFF29EC801112561378BC4BEF04370506B02CE
Malicious:	**true**
Preview:	...8(..H

C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	
Process:	C:\Users\user\Desktop\new order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	952144
Entropy (8bit):	7.695799414445227
Encrypted:	false
SSDEEP:	24576:q/hlikSs/wzknb6gT3wvFHANcvqpbInfDcvkCqvH:q/eNhYkbQvp8cNnbcsCqvH
MD5:	450AA1D2AC8E10A3B8363FE2945462BD
SHA1:	173275F693A10F8919C45DFB21F8035C7BC45FB6
SHA-256:	316FF42588B6CF8C5A435EFB67D44D08A2D860BAB89612FC3E85EC6E9F4B4455

SHA-512:	C3F95286F4BD09C87DD41ACB12C1279B0CF6A547FED73C7C073C21728503AE8FEC4974BDEC351B9049ACBB3A42F497A9731496073A39CCC6F08234F6DF20DC9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.....0..... .....@.. ....@.....H...O.....n..P.....,..... ....H.....text..... ....`.rsrc.....@..@.reloc .....I.....@..B.....\|.....H.....".....(....*b(....%.o....%o....o....*..(....*.0..+..... .....%.....(....(....%-.&...-.s....z.*..0..0.....(....o....o....s..... ....o.....,..o.....*.....$.....(....*.0..?.....(....t!...o.....+$.....r...po.....o....&..(.....X....i2.*.....-.....~....%-.&~.....s ...%.....s!...*B("...(....o#...*..0..:..... s$.....+..~.....~.....i]....a.o%.....X....i2..o&...%-.&.*V('...r#..

C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\new order.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.695799414445227
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	new order.exe
File size:	952144
MD5:	450aa1d2ac8e10a3b8363fe2945462bd
SHA1:	173275f693a10f8919c45dfb21f8035c7bc45fb6
SHA256:	316ff42588b6cf8c5a435efb67d44d08a2d860bab89612fc3e85ec6e9f4b4455
SHA512:	c3f95286f4bd09c87dd41acb12c1279b0cf6a547fed73c7c073c21728503ae8fec4974bdec351b9049acbb3a42f497a9731496073a39ccc6f08234f6df20dc99
SSDEEP:	24576:q/hlikSs/wzknb6gT3wvFHANcvqpbInfDcvkCqvH:q/eNhYkbQvp8cNnbcsCqvH
TLSH:	2315CED3794E0C81E4521935DDCFCA4F9AA5FACDBF9CF2D5A250C30E833B251A85A486
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.....0..... .....@.. .....@.....

File Icon

Icon Hash:	d8dcc4c4ccdc7cb4

Static PE Info

General

Entrypoint:	0x402e9a
Entrypoint Section:	.text
Digitally signed:	true
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:	0xA395936A [Tue Dec 19 22:00:10 2056 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

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/21/2013 5:00:00 PM 8/22/2015 4:59:59 PM
Subject Chain	• CN=NAVER Corp., OU=Digital ID Class 3 - Microsoft Software Validation v2, O=NAVER Corp., L=Seongnam-si, S=Gyeonggi-do, C=KR
Version:	3
Thumbprint MD5:	79BD3501D2B1064E8CD3559B4E2DB943
Thumbprint SHA-1:	82543FBB1867D57DB13CE1BA7B6C39E115BE010A
Thumbprint SHA-256:	C673653EE4392C9EF3C3F9373213069208EDC0795E53E5F93AEEB8F965CD1430
Serial:	3ABBDAEE0F7C6B3F03437A3C166D7251

Entrypoint Preview
Instruction
jmp dword ptr [00402000h]
push es
cmp eax, ebp
insb
outsb
outsb
js 00007F08D0B4F1EDh
js 00007F08D0B4F20Fh
insd
xchg eax, ecx
xchg dword ptr [ebx+63h], ecx
shr byte ptr [ebp+ebp*2+6Eh], 00000078h
dec ebx
arpl word ptr [eax+2Ch], di
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax+6Ch], di
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax+6Ch], di
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax+6Ch], di
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax+6Ch], di

Instruction
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax+6Ch], di
in eax, dx
outsb
js 00007F08D0B4F1EDh
insd
salc
arpl word ptr [esi-34h], bp
inc edx
scasb
pop ecx
aam 6Ch
and dh, byte ptr [ebp+0510376Ah]
push ds
dec esi
or byte ptr [ecx], bh
or al, 1Fh
push ds
or al, 03h
pop eax
sub byte ptr [edx], al
push ss
add al, byte ptr [edx]
sbb bl, byte ptr [eax+29h]
push es
pop eax
push ds
sbb byte ptr [eax], al
pop eax
and cl, byte ptr [3D222858h]
pop eax
or al, 1Ch
or dword ptr [ebx+63h], eax
jne 00007F08D0B4F1E3h
inc edi
js 00007F08D0B4F20Eh
insd
outsb
js 00007F08D0B4F1EDh
arpl word ptr [eax], bp
sub dword ptr [ebp+6Eh], ebp
xor al, 4Ah
pushad
js 00007F08D0B4F152h
lea ebx, dword ptr [edx+1Bh]
dec ebx
arpl word ptr [eax+6Ch], di
insd
outsb
js 00007F08D0B4F1EDh
cmp dword ptr [eax+62h], 4Ch
jns 00007F08D0B4F1F0h
arpl word ptr [eax-26h], di
popad
outsb
js 00007F08D0B4F1EFh
arpl word ptr [eax+6Ch], di

Instruction
insd
outsb
js 00007F08D0B4F203h
mov bh, 74h
insb
insd
dec esi
js 00007F08D0B4F1EDh
arpl word ptr [eax+786E6D60h], bx
or esp, dword ptr [ebx+78h]
dec esp
insd
outsb
js 00007F08D0B4F1EBh
arpl word ptr [eax+68h], di

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2e48	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x19aec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xe6e00	0x1950	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2e2c	0x1c	.text
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	0xccca0	0xcce00	False	0.8712570069402075	data	7.858504462208288	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x19aec	0x19c00	False	0.07720532463592233	data	3.339326632349292	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd01a0	0xe02	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xd0fb4	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 2835 x 2835 px/m		
RT_ICON	0xd142c	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 2835 x 2835 px/m		
RT_ICON	0xd39e4	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 2835 x 2835 px/m		
RT_ICON	0xd4a9c	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536, resolution 2835 x 2835 px/m		
RT_ICON	0xe52d4	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 2835 x 2835 px/m		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xe950c	0x5a	data		
RT_VERSION	0xe9578	0x372	data		
RT_MANIFEST	0xe98fc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

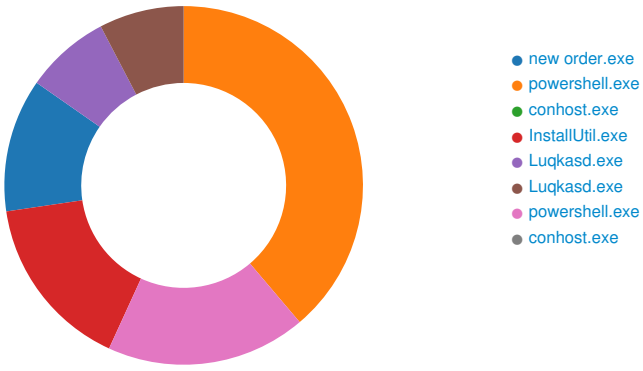
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 07:38:10.310127020 CEST	49707	56281	192.168.2.7	146.70.76.43
Sep 29, 2022 07:38:13.388246059 CEST	49707	56281	192.168.2.7	146.70.76.43
Sep 29, 2022 07:38:19.470930099 CEST	49707	56281	192.168.2.7	146.70.76.43
Sep 29, 2022 07:38:30.191234112 CEST	49708	56281	192.168.2.7	146.70.76.43
Sep 29, 2022 07:38:33.270181894 CEST	49708	56281	192.168.2.7	146.70.76.43
Sep 29, 2022 07:38:39.269511938 CEST	49708	56281	192.168.2.7	146.70.76.43

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: new order.exe PID: **5796**, Parent PID: **6116**

General

Target ID:	0
Start time:	07:36:24
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\new order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\new order.exe"
Imagebase:	0xbb0000

File size:	952144 bytes
MD5 hash:	450AA1D2AC8E10A3B8363FE2945462BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.466623981.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.453841918.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.255565605.0000000004056000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.467477543.0000000005570000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.464712592.00000000040FB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.464712592.00000000040FB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.464712592.00000000040FB000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.466145560.00000000041DD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.466145560.00000000041DD000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.466145560.00000000041DD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.457661334.00000000032A8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.257014991.00000000042E1000.00000004.00000800.00020000.00000000.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	6D64CF06	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	6D64CF06	unknown
C:\Users\user\AppData\Roaming\Znxqmfqxv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C49BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.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	5BD505B	CopyFileW
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5BD505B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\new order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95C78D	CreateFileW

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\Roaming\Znxqmfqxv\Luqkasd.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 6a fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 fd 01 00 00 00 00 00 fd 2e 00 00 00 20 00 00 00 00 0d 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.$PELj0. @ @	success or wait	4	5BD505B	CopyFileW
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.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	5BD505B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\new order.exe.log	0	1039	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6D95C907	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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Users\user\Desktop\new order.exe	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Users\user\Desktop\new order.exe	unknown	512	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	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	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Luqkasd	unicode	"C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe"	success or wait	1	6C49646A	RegSetValueExW

Analysis Process: powershell.exe PID: **492**, Parent PID: **5796**

General

Target ID:	1
Start time:	07:36:37
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANgAwAA==
Imagebase:	0xe60000
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__PSscriptPolicyTest_erq5o4m0.rrv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmo010fb.3b2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	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	6D64CF06	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	6D64CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_erq5o4m0.rrv.ps1	success or wait	1	6C496A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmo010fb.3b2.psm1	success or wait	1	6C496A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_erq5o4m0.rrv.ps1	0	1	31	1	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmo010fb.3b2.psm1	0	1	31	1	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C491B4F	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 0f 00 00 00 fd 0e 00 00 11 00 00 00 fd 0e fd 05 fd 08 fd 08 fd 07 00 00 39 01 37 00 05 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e97@	success or wait	1	6D9176FC	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 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6D9176FC	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	15	6D9176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D9176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D9176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	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 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	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@BMDmEEMqqS%n4&5&7&	success or wait	8	6D9176FC	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	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D62CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D631F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22416	success or wait	1	6D63203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	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	6C491B4F	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	6C491B4F	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	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C491B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C491B4F	ReadFile

Analysis Process: conhost.exe PID: **6084**, Parent PID: **492**

General

Target ID:	2
Start time:	07:36:37
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: InstallUtil.exe PID: **2344**, Parent PID: **5796**

General

Target ID:	14
Start time:	07:37:58
Start date:	29/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x850000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.450018784.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.450018784.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000000.450018784.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.538529652.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.538529652.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.538529652.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000E.00000002.538529652.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.538529652.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.527475187.0000000002D29000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.533662558.0000000003D29000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.533662558.0000000003D29000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.533662558.0000000003D29000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.538073119.0000000005660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.538073119.0000000005660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000E.00000002.538073119.0000000005660000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.538073119.0000000005660000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

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	6D64CF06	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	6D64CF06	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	6C49BEFF	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	6C491E60	CreateFileW
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	6C49BEFF	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	6C49BEFF	CreateDirectoryW

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	09 1f fd 38 28 fd fd 48	8(H	success or wait	1	6C491B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D62CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	unknown	512	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D625705	unknown

Analysis Process: Luqkasd.exe PID: **1016**, Parent PID: **3320**

General

Target ID:	15
Start time:	07:38:00
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe"
Imagebase:	0xfe0000
File size:	952144 bytes
MD5 hash:	450AA1D2AC8E10A3B8363FE2945462BD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.527779375.00000000033BB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.527200680.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.527732524.00000000033B2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.533387647.00000000035B4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D64CF06	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	6D64CF06	unknown

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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	unknown	512	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile

Analysis Process: Luqkasd.exe PID: **628**, Parent PID: **3320**

General

Target ID:	16
Start time:	07:38:08
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe"
Imagebase:	0xf20000
File size:	952144 bytes
MD5 hash:	450AA1D2AC8E10A3B8363FE2945462BD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.528679468.000000000347F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.527935405.000000000343B000.00000004.00000800.00020000.00000000.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	6D64CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D64CF06	unknown

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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Users\user\AppData\Roaming\Znxqmfqxv\Luqkasd.exe	unknown	512	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile

Analysis Process: powershell.exe PID: **5636**, Parent PID: **1016**

General

Target ID:	17
Start time:	07:38:25
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANgAwAA==
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
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__PSscriptPolicyTest_coyhehte.2fz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jawkttfp.mf4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_coyhehte.2fz.ps1	success or wait	1	6C496A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jawkttfp.mf4.psm1	success or wait	1	6C496A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_coyhehte.2fz.ps1	0	1	31	1	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jawkttfp.mf4.psm1	0	1	31	1	success or wait	1	6C491B4F	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	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D62CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D631F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	16384	success or wait	1	6D63203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	6C491B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C491B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C491B4F	ReadFile

Analysis Process: conhost.exe PID: **5648**, Parent PID: **5636**

General

Target ID:	18
Start time:	07:38:25
Start date:	29/09/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly