ID: 526553
Sample Name: TR0398734893 50601251.exe
Cookbook: default.jbs
Time: 18:41:25
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

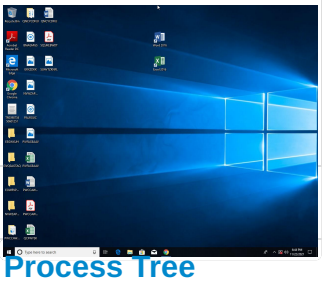
Windows Analysis Report TR0398734893 50601251.exe

Overview

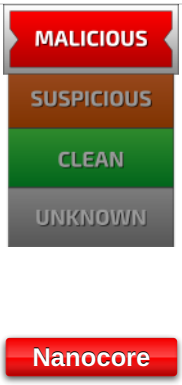
General Information

Sample Name:	TR0398734893 50601251.exe
Analysis ID:	526553
MD5:	f245cb3e4ecc54a..
SHA1:	71ff34129913ac8..
SHA256:	8371daec5ed076..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

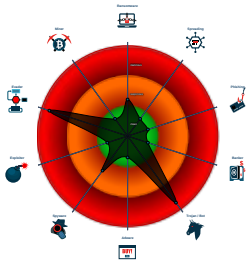


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…
- May check the online IP address of …
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- TR0398734893 50601251.exe (PID: 6612 cmdline: "C:\Users\user\Desktop\TR0398734893 50601251.exe" MD5: F245CB3E4ECC54A0883371B525EB0BB1)
  - powershell.exe (PID: 6952 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\bLtzKqfzc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6968 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\bLtzKqfzc" /XML "C:\Users\user\AppData\Local\Temp\tmp20D5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - TR0398734893 50601251.exe (PID: 4260 cmdline: C:\Users\user\Desktop\TR0398734893 50601251.exe MD5: F245CB3E4ECC54A0883371B525EB0BB1)
    - schtasks.exe (PID: 6648 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp85D3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6712 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp8F69.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- TR0398734893 50601251.exe (PID: 6488 cmdline: "C:\Users\user\Desktop\TR0398734893 50601251.exe" 0 MD5: F245CB3E4ECC54A0883371B525EB0BB1)
  - powershell.exe (PID: 1936 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\bLtzKqfzc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2944 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\bLtzKqfzc" /XML "C:\Users\user\AppData\Local\Temp\tmpC245.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - TR0398734893 50601251.exe (PID: 7024 cmdline: C:\Users\user\Desktop\TR0398734893 50601251.exe MD5: F245CB3E4ECC54A0883371B525EB0BB1)
  - TR0398734893 50601251.exe (PID: 6984 cmdline: C:\Users\user\Desktop\TR0398734893 50601251.exe MD5: F245CB3E4ECC54A0883371B525EB0BB1)
- dhcpmon.exe (PID: 6812 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: F245CB3E4ECC54A0883371B525EB0BB1)
- dhcpmon.exe (PID: 3516 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: F245CB3E4ECC54A0883371B525EB0BB1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000000.375316696.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001E.00000000.375316696.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001E.00000000.375316696.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000009.00000002.528150611.00000000057D0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000009.00000002.528150611.00000000057D0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 60 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.TR0398734893 50601251.exe.57d0000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
9.2.TR0398734893 50601251.exe.57d0000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
9.2.TR0398734893 50601251.exe.5b94629.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
9.2.TR0398734893 50601251.exe.5b94629.9.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
9.2.TR0398734893 50601251.exe.5b94629.9.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 75 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

May check the online IP address of the machine

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

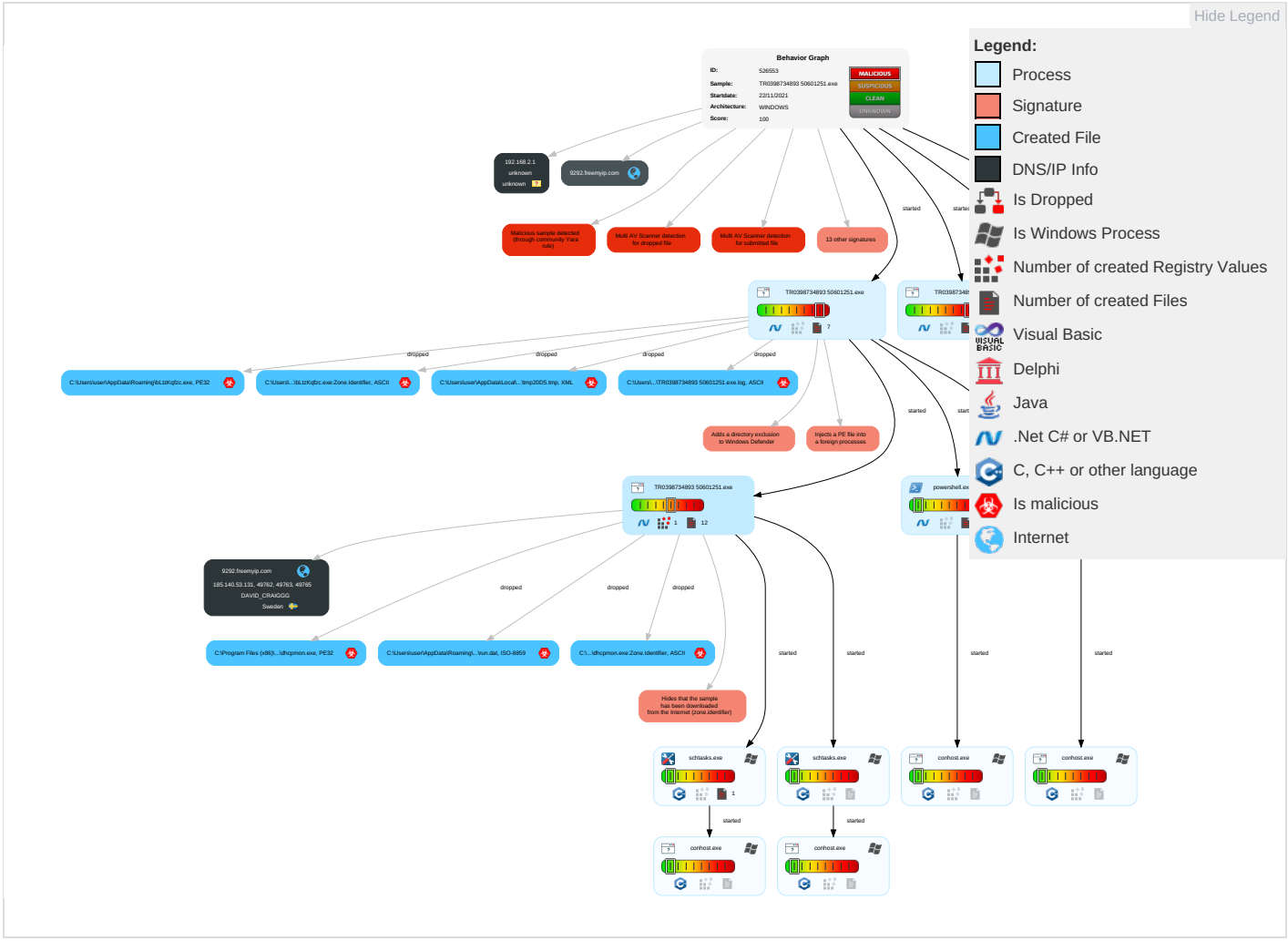
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

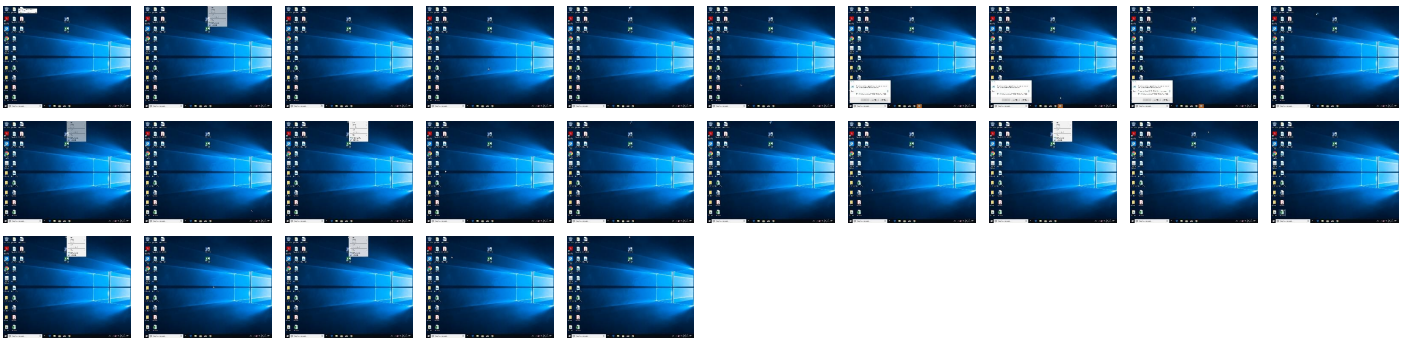
Behavior Graph



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
TR0398734893 50601251.exe	28%	Virustotal		Browse
TR0398734893 50601251.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	
TR0398734893 50601251.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\bLtzKqfzc.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\bLtzKqfzc.exe	28%	Virustotal		Browse
C:\Users\user\AppData\Roaming\bLtzKqfzc.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.TR0398734893 50601251.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.TR0398734893 50601251.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.TR0398734893 50601251.exe.5b90000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.TR0398734893 50601251.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.TR0398734893 50601251.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.TR0398734893 50601251.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.TR0398734893 50601251.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.founder.cV	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn5	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
9292.freemyip.com	185.140.53.131	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.131	9292.freemyip.com	Sweden		209623	DAVID_CRAIGGG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526553
Start date:	22.11.2021
Start time:	18:41:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TR0398734893 50601251.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
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@28/16@12/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:42:30	API Interceptor	807x Sleep call for process: TR0398734893 50601251.exe modified
18:42:38	API Interceptor	59x Sleep call for process: powershell.exe modified
18:42:49	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\TR0398734893 50601251.exe" s>$(Arg0)
18:42:50	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:42:52	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
18:42:55	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	693760
Entropy (8bit):	7.310160824686315
Encrypted:	false
SSDEEP:	12288:BmsTtD00GPFzPtmeQzDYoO863iRWl91tMgTq:BmsTC0GNJmeQfYT3iRWf1yYq
MD5:	F245CB3E4ECC54A0883371B525EB0BB1
SHA1:	71FF34129913AC8A924A28C7523885F11CA44A1C
SHA-256:	8371DAEC5ED076CAA1CFDAC1CE0AB350744DE7D71108AE5EFDA80E4C54AB1D0E
SHA-512:	EDC01E12E62A2A127209E22D86BA647BEC26726CAF0C19ECF8F72C8D02277A6DF5FCA94E98C86377DCAC2C0C0A020F62FA59983AB959373E1F10D0F0C0A2009
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 28%, Browse • Antivirus: ReversingLabs, Detection: 24%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...OG.a.....0.....>0... ...@....@.. ....@...../..O....@..... ....H.....text...T.... ....`.rsrc.....@..... ..@..@.reloc.....@..B..... 0.....H.....xj..LG.....k.....(~.....b..}.....}.....(,.....*r..}.....}.....r...p(,.....**...(3....*...|7...%(.....{....X(.. ....|7...%(.....{....X(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*....0..A.....B. ..%...%...%...%.....%.r...p.%.rM..p.%.r[..p.(.....+..*^..}.....(.....(.....*....0..,.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TR0398734893 50601251.exe.log	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TR0398734893 50601251.exe.log	
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22268
Entropy (8bit):	5.6039199473406995
Encrypted:	false
SSDEEP:	384:zhtCDURZHX89PGKpCRYSBKn0jultI2DpaeQ99gtfpSx+T1MarZlbAV7KWD25ZBDW:zD8dGyL4K0CltZFat8tVCSfw0VW
MD5:	A8FC0D308EE9DAC3FC72B4F6BE60F60B
SHA1:	4EF8A31D28B4ABFA7E6F55A5E18F3C70B7E7FAE1
SHA-256:	C27116B6EAA7BD5DE8C8F226ED3D02913665E57E3EFE47E571C3DA363FD9381F
SHA-512:	387539BA110D128DCE17A9E97027F560A2ABD2DE1863D7DB4574A81D75E26FA58C0FAC187D4FA169464D65902AD66041FDB5F7B5001D5B63F7E2849E18F591B
Malicious:	false
Reputation:	unknown
Preview:	@...e.....v.....C.Q.=.=...T...,r.....@.....H.....<@.^.L."My...::.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5gkkyk2a.4bc.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5gkkyk2a.4bc.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sq4dvbwi.034.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(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmp20D5.tmp	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	5.138222953452563
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtCxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTGv
MD5:	D0F8ABDCF7855BE5F44D41001BC8B4B9
SHA1:	F0491430B13410A02307F0F7BBC8801E10569759
SHA-256:	A534BD817D80EF08E0134EB64A31FCFC730E9A8856B813F9736A1AFD4A65EC5E
SHA-512:	D0E18C0D5D548627F72C5F7CF8F91FD4D5A3EAAF8C14D435A0BA767BB061D77472F710CEB5E85593C55C9D0656025A34FF21AD02C26BD8628ED08F39AFD017 F
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Local\Temp\tmp85D3.tmp	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.15107733589013
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK09r9xtn:cbk4oL600QydbQxIYODOLedq329j
MD5:	475679C76B7A902D42BD17BF990EF85B
SHA1:	30D575A6ABB5C510673E64B023D421106BBFA8B0
SHA-256:	A47745504B38190742287EB75F6498FF062CC4FF37B133F5D4357D98CF9B68E8
SHA-512:	AEE89FE7DD3B6F536DF7D06927481BCA118E542B735E72524540588C57A00152D7867B4B8DE673FB429562E0A9F764781A45FE21A0D9439FD13EA6DF0181B868
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp85D3.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8F69.tmp	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpC245.tmp	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	5.138222953452563
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtCxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTGv
MD5:	D0F8ABDCF7855BE5F44D41001BC8B4B9
SHA1:	F0491430B13410A02307F0F7BBC8801E10569759
SHA-256:	A534BD817D80EF08E0134EB64A31FCFC730E9A8856B813F9736A1AFD4A65EC5E
SHA-512:	D0E18C0D5D548627F72C5F7CF8F91FD4D5A3EAAF8C14D435A0BA767BB061D77472F710CEB5E85593C55C9D0656025A34FF21AD02C26BD8628ED08F39AFD017F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:1G8:b
MD5:	F194EBA2A5B030A89E0924B2723CFFF3
SHA1:	D3770575989A6A60508D6C459BB7613885AAD7AA
SHA-256:	5D3911ED91DB035F88564D64E1ACD3253D8EDABC0EFB50B83A13BFBBB8F84B46
SHA-512:	790DEDC3AD650CE7EAFEBF38E78A27E37F2821EC416D892BE4AE163309BA348ABF36FE732456FAC8E32DAFCCAA6E88FF077CA8B4038A71B7D08B98181CD3590
Malicious:	**true**
Reputation:	unknown

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.678912497395635
Encrypted:	false
SSDEEP:	3:oN0naRRx3VMW7n6Gn:oNcSRTX76G
MD5:	6D23CA5B932A39B404EAABECC2D3282E
SHA1:	C403AB90DD6ACEF2299F0B1CC626A8E16793D11C
SHA-256:	3CA34E26F5DB3A21563A5CE3FFA753ECFF055E9CF0759AC815CA01EDD2954561
SHA-512:	CD10A79389291E31A57C0EC68848E44E0766DFE679C5E86FDEC4C85973C2B4F4E1661B1A82FC0970D19A196B2D5DE59C27ACB69542463CF984FAD6C3C8D4A38
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\TR0398734893 50601251.exe

C:\Users\user\AppData\Roaming\bLtzKqfzc.exe	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	693760
Entropy (8bit):	7.310160824686315
Encrypted:	false
SSDEEP:	12288:BmsTtD00GPFzPtmeQzDYoO863iRWl91tMgTq:BmsTC0GNJmeQfYT3iRWf1yYq
MD5:	F245CB3E4ECC54A0883371B525EB0BB1
SHA1:	71FF34129913AC8A924A28C7523885F11CA44A1C
SHA-256:	8371DAEC5ED076CAA1CFDAC1CE0AB350744DE7D71108AE5EFDA80E4C54AB1D0E
SHA-512:	EDC01E12E62A2A127209E22D86BA647BEC26726CAF0C19ECF8F72C8D02277A6DF5FCA94E98C86377DCAC2C0C0A020F62FA59983AB959373E1F10D0F0C0A2009
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 28%, Browse • Antivirus: ReversingLabs, Detection: 24%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...OG.a.....0.....>0... ...@....@.. ....@...../..O....@..... ....H.....text...T.... ....`.rsrc.....@..... ..@..@.reloc.....@..B..... 0.....H.....xj..LG.....k.....(~.....b..}.....}.....(,.....*r..}.....}.....r...p(,.....**...(3....*...|7...%(.....{....X(.. ....|7...%(.....{....X(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*....0..A.....B. ..%...%...%...%.....%.r...p.%.rM..p.%.r[..p.(.....+..*^..}.....(.....(.....*....0..,.....

C:\Users\user\AppData\Roaming\bLtzKqfzc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TR0398734893 50601251.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211122\PowerShell_transcript.226533.DYqwUES1.20211122184236.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5825

C:\Users\user\Documents\20211122\PowerShell_transcript.226533.DYqwUES1.20211122184236.txt

Entropy (8bit):	5.396902799265613
Encrypted:	false
SSDEEP:	96:BZi6/NaqDo1ZJZv6/NaqDo1ZEaMyjZK6/NaqDo1Z1TCC5Ze:8
MD5:	F33207262F5C04CE12B6D75FF00124B7
SHA1:	57097622FABDFC7810D70F2868496E62C9386306
SHA-256:	C3995E9A0E243E0D6E579B1BAC4421A37E1900DC57B31A9FEA2B4577CC0380F4
SHA-512:	F915154122F5E6653F4167A9E35E3727F1F3ACA24580319DF83A14998A490828532D28EE445E1ED5E7136BA221419F61F2C1FF6B90ADB066E227D968BA6CE38C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122184238..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226533 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\bLtzKqfzc.exe..Process ID: 6952..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211122184238..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\bLtzKqfzc.exe..**********..Windows PowerShell transcript start..Start time: 20211122184550..Username: computer\user..RunAs User: DE

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.310160824686315
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:	TR0398734893 50601251.exe
File size:	693760
MD5:	f245cb3e4ecc54a0883371b525eb0bb1
SHA1:	71ff34129913ac8a924a28c7523885f11ca44a1c
SHA256:	8371daec5ed076caa1cfdac1ce0ab350744de7d71108ae5efda80e4c54ab1d0e
SHA512:	edc01e12e62a2a127209e22d86ba647bec26726caf0c19ecf8f72c8d02277a6df5fca94e98c86377dcac2c0c0a020f62fa59983ab959373e1f10d0f0c0a200b9
SSDEEP:	12288:BmsTtD00GPFzPtmeQzDYoO863iRWl91tMgTq:BmsTC0GNJmeQfYT3iRWf1yYq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...OG.a.....0.....>0... ...@....@.. .....@.....

File Icon

Icon Hash:	d4d4d4d4d4c4d4d4

Static PE Info

General

Entrypoint:	0x48303e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619B474F [Mon Nov 22 07:31:27 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x81054	0x81200	False	0.846968023959	data	7.71324859014	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x27fe8	0x28000	False	0.066162109375	data	4.88686576028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 18:42:56.064798117 CET	192.168.2.7	8.8.8.8	0x1739	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:02.829432011 CET	192.168.2.7	8.8.8.8	0xdd3b	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:09.085760117 CET	192.168.2.7	8.8.8.8	0x9f4b	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:30.819693089 CET	192.168.2.7	8.8.8.8	0x825b	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:37.544235945 CET	192.168.2.7	8.8.8.8	0xc074	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:43.264965057 CET	192.168.2.7	8.8.8.8	0x41dd	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:04.800498962 CET	192.168.2.7	8.8.8.8	0x2c58	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:10.916512966 CET	192.168.2.7	8.8.8.8	0x3f66	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:16.413800001 CET	192.168.2.7	8.8.8.8	0x9ff8	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:36.836651087 CET	192.168.2.7	8.8.8.8	0xf7ea	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 18:44:42.118063927 CET	192.168.2.7	8.8.8.8	0x4949	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:47.401452065 CET	192.168.2.7	8.8.8.8	0x20dd	Standard query (0)	9292.freemyip.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 18:42:56.250201941 CET	8.8.8.8	192.168.2.7	0x1739	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:02.850032091 CET	8.8.8.8	192.168.2.7	0xdd3b	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:09.271630049 CET	8.8.8.8	192.168.2.7	0x9f4b	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:31.003617048 CET	8.8.8.8	192.168.2.7	0x825b	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:37.564265966 CET	8.8.8.8	192.168.2.7	0xc074	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:43:43.284579992 CET	8.8.8.8	192.168.2.7	0x41dd	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:04.982683897 CET	8.8.8.8	192.168.2.7	0x2c58	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:10.935914040 CET	8.8.8.8	192.168.2.7	0x3f66	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:16.434004068 CET	8.8.8.8	192.168.2.7	0x9ff8	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:37.021974087 CET	8.8.8.8	192.168.2.7	0xf7ea	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:42.304447889 CET	8.8.8.8	192.168.2.7	0x4949	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)
Nov 22, 2021 18:44:47.421081066 CET	8.8.8.8	192.168.2.7	0x20dd	No error (0)	9292.freemyip.com		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TR0398734893 50601251.exe PID: 6612 Parent PID: 5368

General

Start time:	18:42:23
Start date:	22/11/2021

Path:	C:\Users\user\Desktop\TR0398734893 50601251.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TR0398734893 50601251.exe"
Imagebase:	0xaa0000
File size:	693760 bytes
MD5 hash:	F245CB3E4ECC54A0883371B525EB0BB1
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: 00000001.00000002.300853554.0000000003DC9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.300853554.0000000003DC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.300853554.0000000003DC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.298209102.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6952 Parent PID: 6612

General

Start time:	18:42:35
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\bLtzKqfzc.exe
Imagebase:	0x1110000
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 Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6960 Parent PID: 6952

General

Start time:	18:42:35
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6968 Parent PID: 6612

General

Start time:	18:42:36
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\bLtzKqfzc" /XML "C:\Users\user\AppData\Local\Temp\tmp20D5.tmp
Imagebase:	0xb00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 7072 Parent PID: 6968

General

Start time:	18:42:37
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: TR0398734893 50601251.exe PID: 4260 Parent PID: 6612

General

Start time:	18:42:41
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\TR0398734893 50601251.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\TR0398734893 50601251.exe
Imagebase:	0xd80000
File size:	693760 bytes
MD5 hash:	F245CB3E4ECC54A0883371B525EB0BB1
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: 00000009.00000002.528150611.00000000057D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.528150611.00000000057D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.292483199.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.292483199.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.292483199.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.294328099.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.294328099.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.294328099.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.293437788.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.293437788.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.293437788.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.525426883.00000000030E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.291833438.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.291833438.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.291833438.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.527129280.0000000004129000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.527129280.0000000004129000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.528651363.0000000005B90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.528651363.0000000005B90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.528651363.0000000005B90000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.516249872.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.516249872.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.516249872.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6648 Parent PID: 4260

General

Start time:	18:42:48
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp85D3.tmp
Imagebase:	0xb00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6600 Parent PID: 6648

General

Start time:	18:42:49
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: TR0398734893 50601251.exe PID: 6488 Parent PID: 1104

General

Start time:	18:42:49
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\TR0398734893 50601251.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TR0398734893 50601251.exe" 0
Imagebase:	0x770000
File size:	693760 bytes
MD5 hash:	F245CB3E4ECC54A0883371B525EB0BB1
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: 00000013.00000002.384186174.0000000003DE9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.384186174.0000000003DE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.384186174.0000000003DE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.382218948.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6712 Parent PID: 4260

General

Start time:	18:42:50
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp8F69.tmp
Imagebase:	0xb00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6440 Parent PID: 6712

General

Start time:	18:42:51
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000

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

Analysis Process: dhcpmon.exe PID: 6812 Parent PID: 1104

General

Start time:	18:42:52
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x830000
File size:	693760 bytes
MD5 hash:	F245CB3E4ECC54A0883371B525EB0BB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000016.00000002.330253981.0000000002CD1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, Virustotal, Browse • Detection: 24%, ReversingLabs

Analysis Process: dhcpmon.exe PID: 3516 Parent PID: 3292

General

Start time:	18:42:59
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x750000
File size:	693760 bytes
MD5 hash:	F245CB3E4ECC54A0883371B525EB0BB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000017.00000002.341866745.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis