ID: 500301
Sample Name:
1FB6ncJ5XP.exe
Cookbook: default.jbs
Time: 22:22:54
Date: 11/10/2021
Version: 33.0.0 White Diamond

Table of Contents

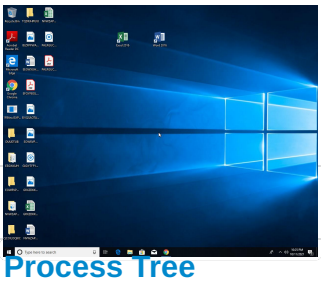
Windows Analysis Report 1FB6ncJ5XP.exe

Overview

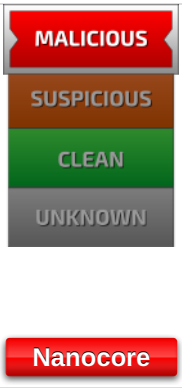
General Information

Sample Name:	1FB6ncJ5XP.exe
Analysis ID:	500301
MD5:	e90d3150b729f9e.
SHA1:	08f865e0f25ca9f…
SHA256:	b96ae4aab134c7..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



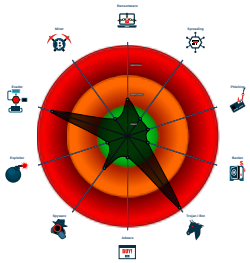
Nanocore

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

Signatures

- Found malware configuration
- 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
- Connects to many ports of the same…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- 1FB6ncJ5XP.exe (PID: 6448 cmdline: 'C:\Users\user\Desktop\1FB6ncJ5XP.exe' MD5: E90D3150B729F9E9F8271ED964DA0D14)
  - schtasks.exe (PID: 7156 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QLpzxrlNoQJN' /XML 'C:\Users\user\AppData\Local\Temp\tmpCE1C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 1FB6ncJ5XP.exe (PID: 2832 cmdline: C:\Users\user\Desktop\1FB6ncJ5XP.exe MD5: E90D3150B729F9E9F8271ED964DA0D14)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "a34ced25-fb8b-4570-a6e3-066f7f9b",
  "Group": "AAA",
  "Domain1": "ella666.duckdns.org",
  "Domain2": "mikeljack321.ddns.net",
  "Port": 31829,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "ella666.duckdns.org"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.573289700.000000000564 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000007.00000002.573289700.000000000564 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000007.00000002.573397352.000000000578 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.573397352.000000000578 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000007.00000002.573397352.000000000578 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 20 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.1FB6ncJ5XP.exe.5640000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.1FB6ncJ5XP.exe.5640000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.1FB6ncJ5XP.exe.3d6ff64.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.1FB6ncJ5XP.exe.3d6ff64.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.1FB6ncJ5XP.exe.3d6ff64.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 31 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

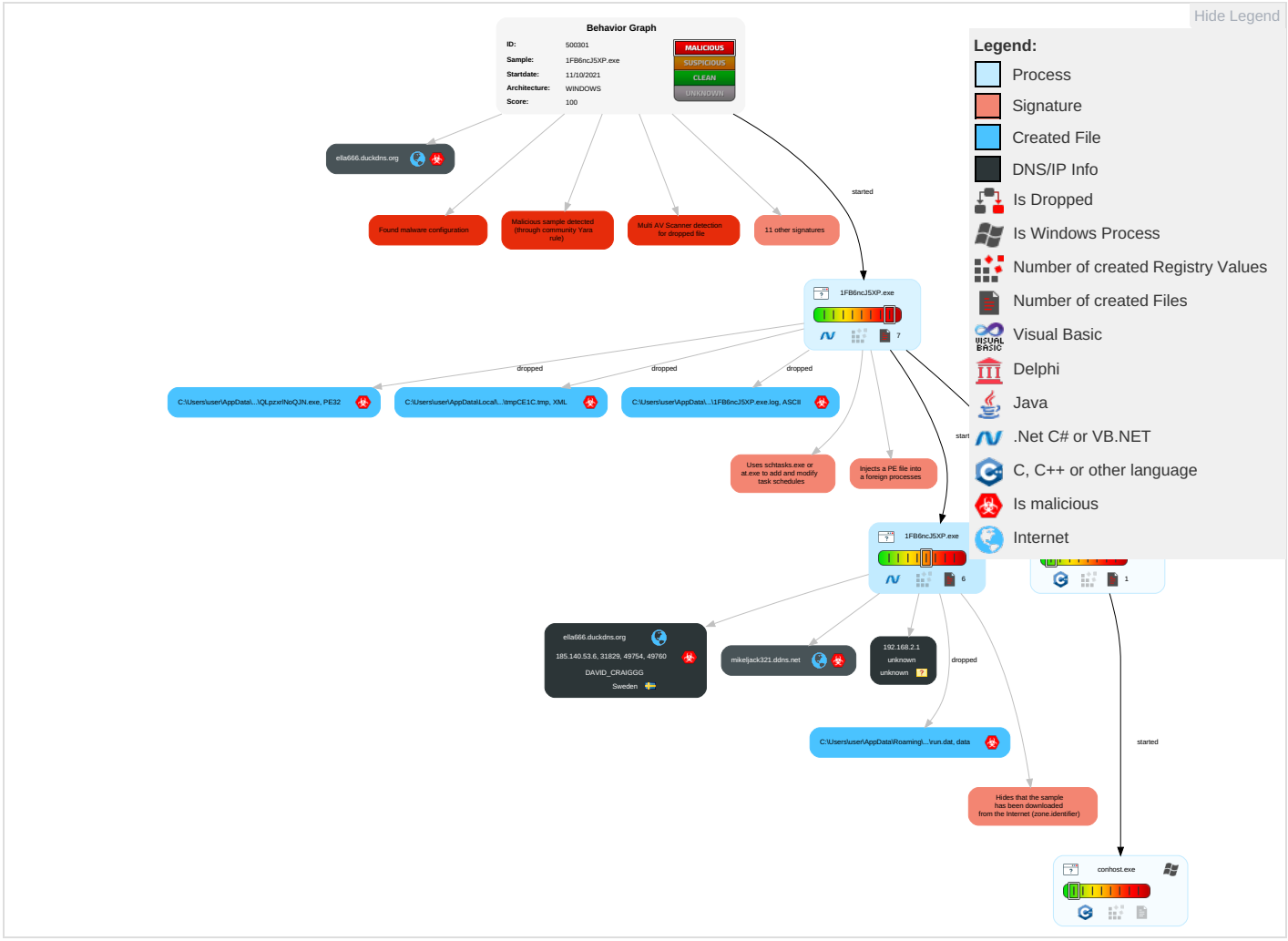
Detected Nanocore Rat

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	Netw Effec
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls
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	Explo Track Loca
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 (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
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	Down Insec Proto

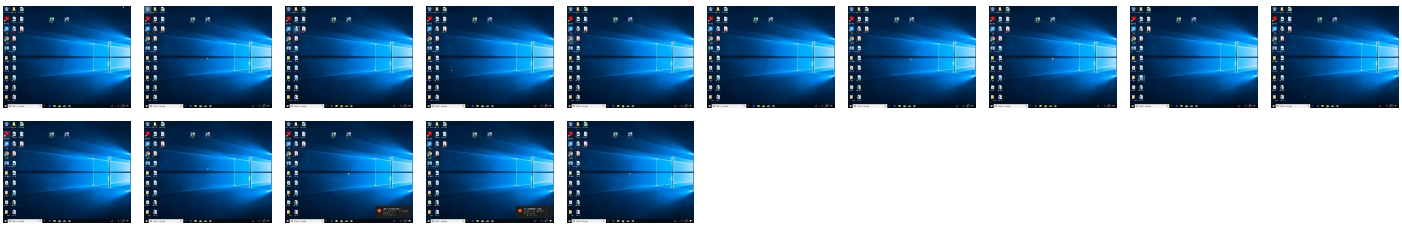
Behavior Graph



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
1FB6ncJ5XP.exe	37%	Virustotal		Browse
1FB6ncJ5XP.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.DarkStealerLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QLpzxrlNoQJN.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.DarkStealerLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.1FB6ncJ5XP.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.1FB6ncJ5XP.exe.5780000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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.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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
ella666.duckdns.org	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
mikeljack321.ddns.net	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mikeljack321.ddns.net	185.140.53.6	true	true		unknown
ella666.duckdns.org	185.140.53.6	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ella666.duckdns.org	true	• Avira URL Cloud: safe	unknown
mikeljack321.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.6	mikeljack321.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	500301
Start date:	11.10.2021
Start time:	22:22:54
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1FB6ncJ5XP.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:	20
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@6/5@21/2
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
22:24:10	API Interceptor	921x Sleep call for process: 1FB6ncJ5XP.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.6	d1IaoX0mpm.exe	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	DeKjb2fKJT.exe	Get hash	malicious	Browse	
	MT103 tek M#U00fc#U015fteri kredi aktarma kopyas#U0131,pdf.exe	Get hash	malicious	Browse	
	DEKONT,pdf.exe	Get hash	malicious	Browse	
	PO 001077 - CS#000310.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ella666.duckdns.org	DeKjb2fKJT.exe	Get hash	malicious	Browse	• 185.140.53.6
	6cg2ZIoAHQ.exe	Get hash	malicious	Browse	• 79.134.225.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	DHL_101121 recibo de la compra,pdf.exe	Get hash	malicious	Browse	• 185.140.53.136

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	noZPwMIh7e.exe	Get hash	malicious	Browse	• 91.193.75.133
	Memorandum from the Saudi Embassy.pdf.exe	Get hash	malicious	Browse	• 185.140.53.8
	RkPJvCnCuJ.exe	Get hash	malicious	Browse	• 185.140.53.133
	AWB # 2617429350,pdf.exe	Get hash	malicious	Browse	• 185.140.53.133
	DHL_100621 de documentos de la compra,pdf.exe	Get hash	malicious	Browse	• 185.140.53.5
	DHL_119040 de documentos de la compra .pdf.exe	Get hash	malicious	Browse	• 185.140.53.5
	Nouvelle commande 983765_2021,pdf.exe	Get hash	malicious	Browse	• 185.244.30.19
	#U00d6DEME TAVS#U0130YES#U0130_PDF.exe	Get hash	malicious	Browse	• 185.140.53.232
	TEKL_F VE F_YAT TEKL_F TALEB_PDF.exe	Get hash	malicious	Browse	• 185.140.53.232
	Yeni Sipari_ #86-55113,pdf.exe	Get hash	malicious	Browse	• 185.140.53.133
	OMNH11mXX2.exe	Get hash	malicious	Browse	• 185.140.53.3
	FZJCUwvp0s.exe	Get hash	malicious	Browse	• 185.140.53.3
	Naujas u#U017esakymas. 141.exe	Get hash	malicious	Browse	• 91.193.75.173
	SWIFT.exe	Get hash	malicious	Browse	• 185.244.30.252
	Mts#U007e00037363673893-09387633783876337.exe	Get hash	malicious	Browse	• 185.140.53.9
	W3vlt7fcaD.exe	Get hash	malicious	Browse	• 185.140.53.14
	J5K18S6C5V43.exe	Get hash	malicious	Browse	• 185.140.53.3
	RFQAP65425652032421 urgentes,pdf.exe	Get hash	malicious	Browse	• 185.244.30.19
	Scan0005936148.exe	Get hash	malicious	Browse	• 185.244.30.68

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1FB6ncJ5XP.exe.log

Process:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
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\Temp\tmpCE1C.tmp

Process:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.199228582576025
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBatn:cbh47TlNQ//rydbz9l3YODOLNdq3W
MD5:	F3CD74A20FE323A5FC1F90249DE26602
SHA1:	F802CF5462A0D068F577F3B31E6A5D3ED7D53CE7

C:\Users\user\AppData\Local\Temp\tmpCE1C.tmp	
SHA-256:	CA606E21DEFDB5A07862C1D48A4DE79699EFA24F466CEAACE13F1463329B14F7
SHA-512:	D69C54F4D5F7B3AE06157D1FB53855C632828F960D0C170B140E64FA9B473319CDD087C5F174DEF6A6E3EB7A93E2727FF72BA389DD3A49EBC77735845555052E
Malicious:	**true**
Reputation:	low
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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ct:c
MD5:	407C6F1A0FAD16CAB6817B9EEA8F0868
SHA1:	861B00F6BC9BD070317ED8A146D379BED7A451F3
SHA-256:	03894C3F20DAA7ED0F45203344BF70510CFA7207B54B528EAE004C894D42419F
SHA-512:	3CB51C0E9C03AEE25BBAD42779A9DD1AC758920979FA9DF6FD91C90EA4C27D1ACDCB1E89C3694F6202A7176ACFFE9F05F61FE7C68D3D5F3B18C87EF28262605
Malicious:	**true**
Reputation:	low
Preview:	.v..@..H

C:\Users\user\AppData\Roaming\QLpzxrlNoQJN.exe	
Process:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	7.380179159495352
Encrypted:	false
SSDEEP:	12288:O7hv6UDSuTG2T9BGQ7KhQ5w8vdw3e1FH6pBhc7UfGxmn0:iiUmuTG2JahQ5bw3eaVc7xIn
MD5:	E90D3150B729F9E9F8271ED964DA0D14
SHA1:	08F865E0F25CA9F7E19F04E8D437214F924C3BB8
SHA-256:	B96AE4AAB134C7612BD21311EE76A7B0B0DC14AF7B2E10713564E50FC739967E
SHA-512:	E60900A239117FF9959F3BED2E889814527A814FB1D00041E09C9E589FE017CF9F0F43CD54A75F5CEBBBBF384EC4F0001CC94F10999A9BFCD43269D67FDBA63
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 42%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ca.....0..t.....~.... .....@.. ....@.....,...O.....T..... .....H.....text....s... ...t..... ..`.rsrc...T.....v.....@..@.reloc..... .....~.....@..B.....`.....H.....T.....z..../..@c.....^..}.....(.....(.....*.0..+.....,..{.....+...,...{....o.....(....*..0..2.....(....s.....s....}.. ...s....}.....s....}.....s....}.....(.....{.....o.....{...r...p"...A...s....o .....{.....s!...o".....{....r+..po#.....{.....8..s$...o%.....{.....o&.....{....r9..po'.....{.....o.....{....r...p"...A...s....o .....{.....s!.. ..o".....{....rK..po#.....{.... .....s$...o%.....{.....o&..

C:\Users\user\AppData\Roaming\QLpzxrlNoQJN.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\1FB6ncJ5XP.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:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.380179159495352
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	1FB6ncJ5XP.exe
File size:	622592
MD5:	e90d3150b729f9e9f8271ed964da0d14
SHA1:	08f865e0f25ca9f7e19f04e8d437214f924c3bb8
SHA256:	b96ae4aab134c7612bd21311ee76a7b0b0dc14af7b2e10713564e50fc739967e
SHA512:	e60900a239117ff9959f3bed2e889814527a814fb1d00041e09c9e589fe017cf9f0f43cd54a75f5cebbbbf384ec4f0001cc94f10999a9bfcd43269d67fdba631
SSDEEP:	12288:O7hv6UDSuTG2T9BGQ7KhQ5w8vdw3e1FH6pBhc7UfGxmn0:iiUmuTG2JahQ5bw3eaVc7xIn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ca.....0..t.....~.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49937e
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:	0x6163E5E2 [Mon Oct 11 07:21:06 2021 UTC]
TLS Callbacks:	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x97384	0x97400	False	0.76508910124	data	7.39359374162	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x654	0x800	False	0.3349609375	data	3.52727036159	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/11/21-22:24:18.095895	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
10/11/21-22:24:23.876499	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
10/11/21-22:24:29.226553	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49572	8.8.8.8	192.168.2.3
10/11/21-22:24:34.714834	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3
10/11/21-22:24:40.104285	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63297	8.8.8.8	192.168.2.3
10/11/21-22:24:45.272642	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50728	8.8.8.8	192.168.2.3
10/11/21-22:24:50.980931	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53777	8.8.8.8	192.168.2.3
10/11/21-22:24:56.492230	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60352	8.8.8.8	192.168.2.3
10/11/21-22:25:12.191345	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64367	8.8.8.8	192.168.2.3
10/11/21-22:25:22.606841	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	8.8.8.8	192.168.2.3
10/11/21-22:25:33.092754	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58540	8.8.8.8	192.168.2.3
10/11/21-22:25:38.249210	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55108	8.8.8.8	192.168.2.3
10/11/21-22:25:43.411922	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64432	8.8.8.8	192.168.2.3
10/11/21-22:25:48.709933	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49250	8.8.8.8	192.168.2.3
10/11/21-22:25:55.885208	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63490	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 11, 2021 22:24:17.984097004 CEST	192.168.2.3	8.8.8.8	0x8497	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 11, 2021 22:24:23.762837887 CEST	192.168.2.3	8.8.8.8	0x8a71	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:29.112129927 CEST	192.168.2.3	8.8.8.8	0xc4bf	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:34.694262981 CEST	192.168.2.3	8.8.8.8	0xb4f	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:40.084264994 CEST	192.168.2.3	8.8.8.8	0xe2de	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:45.252636909 CEST	192.168.2.3	8.8.8.8	0x51dc	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:50.867288113 CEST	192.168.2.3	8.8.8.8	0x27b8	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:56.376194000 CEST	192.168.2.3	8.8.8.8	0xaa0d	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:01.844786882 CEST	192.168.2.3	8.8.8.8	0x30f9	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:07.003144979 CEST	192.168.2.3	8.8.8.8	0x1814	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:12.170744896 CEST	192.168.2.3	8.8.8.8	0x4722	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:17.326965094 CEST	192.168.2.3	8.8.8.8	0x431c	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:22.491801977 CEST	192.168.2.3	8.8.8.8	0x3064	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:27.745096922 CEST	192.168.2.3	8.8.8.8	0xa45f	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:32.977087975 CEST	192.168.2.3	8.8.8.8	0x9656	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:38.228058100 CEST	192.168.2.3	8.8.8.8	0x7bae	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:43.392096043 CEST	192.168.2.3	8.8.8.8	0x2c60	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:48.689290047 CEST	192.168.2.3	8.8.8.8	0x32bf	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:55.771222115 CEST	192.168.2.3	8.8.8.8	0x6bc4	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:26:01.238878012 CEST	192.168.2.3	8.8.8.8	0x3609	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
Oct 11, 2021 22:26:06.354088068 CEST	192.168.2.3	8.8.8.8	0x6ce0	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 11, 2021 22:24:18.095895052 CEST	8.8.8.8	192.168.2.3	0x8497	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:23.876498938 CEST	8.8.8.8	192.168.2.3	0x8a71	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:29.226552963 CEST	8.8.8.8	192.168.2.3	0xc4bf	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:34.714833975 CEST	8.8.8.8	192.168.2.3	0xb4f	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:40.104285002 CEST	8.8.8.8	192.168.2.3	0xe2de	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:45.272641897 CEST	8.8.8.8	192.168.2.3	0x51dc	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:50.980931044 CEST	8.8.8.8	192.168.2.3	0x27b8	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:56.492229939 CEST	8.8.8.8	192.168.2.3	0xaa0d	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:01.862924099 CEST	8.8.8.8	192.168.2.3	0x30f9	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:07.021365881 CEST	8.8.8.8	192.168.2.3	0x1814	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 11, 2021 22:25:12.191344976 CEST	8.8.8.8	192.168.2.3	0x4722	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:17.345349073 CEST	8.8.8.8	192.168.2.3	0x431c	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:22.606841087 CEST	8.8.8.8	192.168.2.3	0x3064	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:27.761207104 CEST	8.8.8.8	192.168.2.3	0xa45f	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:33.092753887 CEST	8.8.8.8	192.168.2.3	0x9656	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:38.249209881 CEST	8.8.8.8	192.168.2.3	0x7bae	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:43.411921978 CEST	8.8.8.8	192.168.2.3	0x2c60	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:48.709933043 CEST	8.8.8.8	192.168.2.3	0x32bf	No error (0)	mikeljack321.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:25:55.885207891 CEST	8.8.8.8	192.168.2.3	0x6bc4	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:26:01.257261992 CEST	8.8.8.8	192.168.2.3	0x3609	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)
Oct 11, 2021 22:26:06.372297049 CEST	8.8.8.8	192.168.2.3	0x6ce0	No error (0)	ella666.duckdns.org		185.140.53.6	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 1FB6ncJ5XP.exe PID: 6448 Parent PID: 720

General

Start time:	22:23:56
Start date:	11/10/2021
Path:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1FB6ncJ5XP.exe'
Imagebase:	0x9c0000
File size:	622592 bytes
MD5 hash:	E90D3150B729F9E9F8271ED964DA0D14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.339237051.0000000002D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.340496644.0000000003EE2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.340496644.0000000003EE2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.340496644.0000000003EE2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.339659740.0000000002E7E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.340027547.0000000003D59000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.340027547.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.340027547.0000000003D59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 7156 Parent PID: 6448

General

Start time:	22:24:11
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QLpzxrlNoQJN' /XML 'C:\Users\user\AppData\Local\Temp\tmpCE1C.tmp'
Imagebase:	0x60000
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

Analysis Process: conhost.exe PID: 4008 Parent PID: 7156

General

Start time:	22:24:12
Start date:	11/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000

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: 1FB6ncJ5XP.exe PID: 2832 Parent PID: 6448

General

Start time:	22:24:12
Start date:	11/10/2021
Path:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1FB6ncJ5XP.exe
Imagebase:	0xa40000
File size:	622592 bytes
MD5 hash:	E90D3150B729F9E9F8271ED964DA0D14
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: 00000007.00000002.573289700.0000000005640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.573289700.0000000005640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.573397352.0000000005780000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.573397352.0000000005780000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.573397352.0000000005780000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.566743292.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.566743292.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.566743292.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.572012572.0000000003D69000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.572012572.0000000003D69000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis