ID: 356788
Sample Name: WxTm2cWLHF
Cookbook: default.jbs
Time: 16:40:00
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

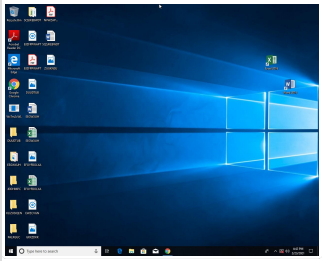
Analysis Report WxTm2cWLHF

Overview

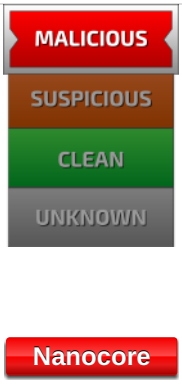
General Information

Sample Name:	WxTm2cWLHF (renamed file extension from none to exe)
Analysis ID:	356788
MD5:	da6d54ef4dd6752.
SHA1:	b88ea4e2bc8929..
SHA256:	6f226cb3268aafb..
Tags:	NanoCore
Infos:	

Most interesting Screenshot:



Detection



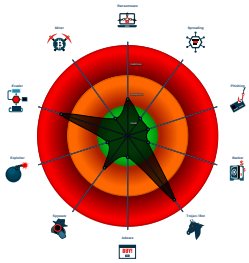
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- WxTm2cWLHF.exe (PID: 5512 cmdline: 'C:\Users\user\Desktop\WxTm2cWLHF.exe' MD5: DA6D54EF4DD6752367FF3F516196B292)
  - schtasks.exe (PID: 6612 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eNEXCeqZvjFuTO' /XML 'C:\Users\user\AppData\Local\Temp\tmp30A3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WxTm2cWLHF.exe (PID: 6664 cmdline: {path} MD5: DA6D54EF4DD6752367FF3F516196B292)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "0875083a-8885-4a01-8069-09c5a276748c",
  "Group": "feb16",
  "Domain1": "amuokuku.duckdns.org",
  "Domain2": "alliedtrade54321.ddns.net",
  "Port": 32114,
  "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": "amuokuku.duckdns.org",
  "BackupDNSServer": "alliedtrade54321.ddns.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.499194196.000000000615 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.499194196.000000000615 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000007.00000002.499194196.000000000615 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.497750745.0000000003F2 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.497750745.0000000003F2 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f15:$a: NanoCore • 0x2f6e:$a: NanoCore • 0x2fab:$a: NanoCore • 0x3024:$a: NanoCore • 0x166cf:$a: NanoCore • 0x166e4:$a: NanoCore • 0x16719:$a: NanoCore • 0x2f1c3:$a: NanoCore • 0x2f1d8:$a: NanoCore • 0x2f20d:$a: NanoCore • 0x2f77:$b: ClientPlugin • 0x2fb4:$b: ClientPlugin • 0x38b2:$b: ClientPlugin • 0x38bf:$b: ClientPlugin • 0x1648b:$b: ClientPlugin • 0x164a6:$b: ClientPlugin • 0x164d6:$b: ClientPlugin • 0x166ed:$b: ClientPlugin • 0x16722:$b: ClientPlugin • 0x2ef7f:$b: ClientPlugin • 0x2ef9a:$b: ClientPlugin

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.WxTm2cWLHF.exe.43e16f0.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0.2.WxTm2cWLHF.exe.43e16f0.3.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:$s5: IClientLoggingHost
0.2.WxTm2cWLHF.exe.43e16f0.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.WxTm2cWLHF.exe.43e16f0.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$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
7.2.WxTm2cWLHF.exe.6154629.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 33 entries				

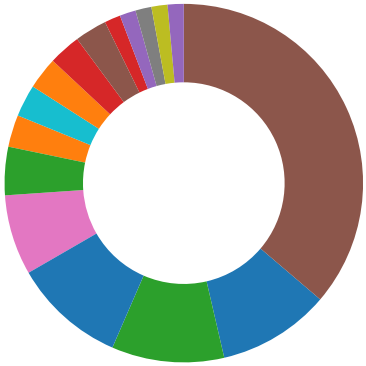
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

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)

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:

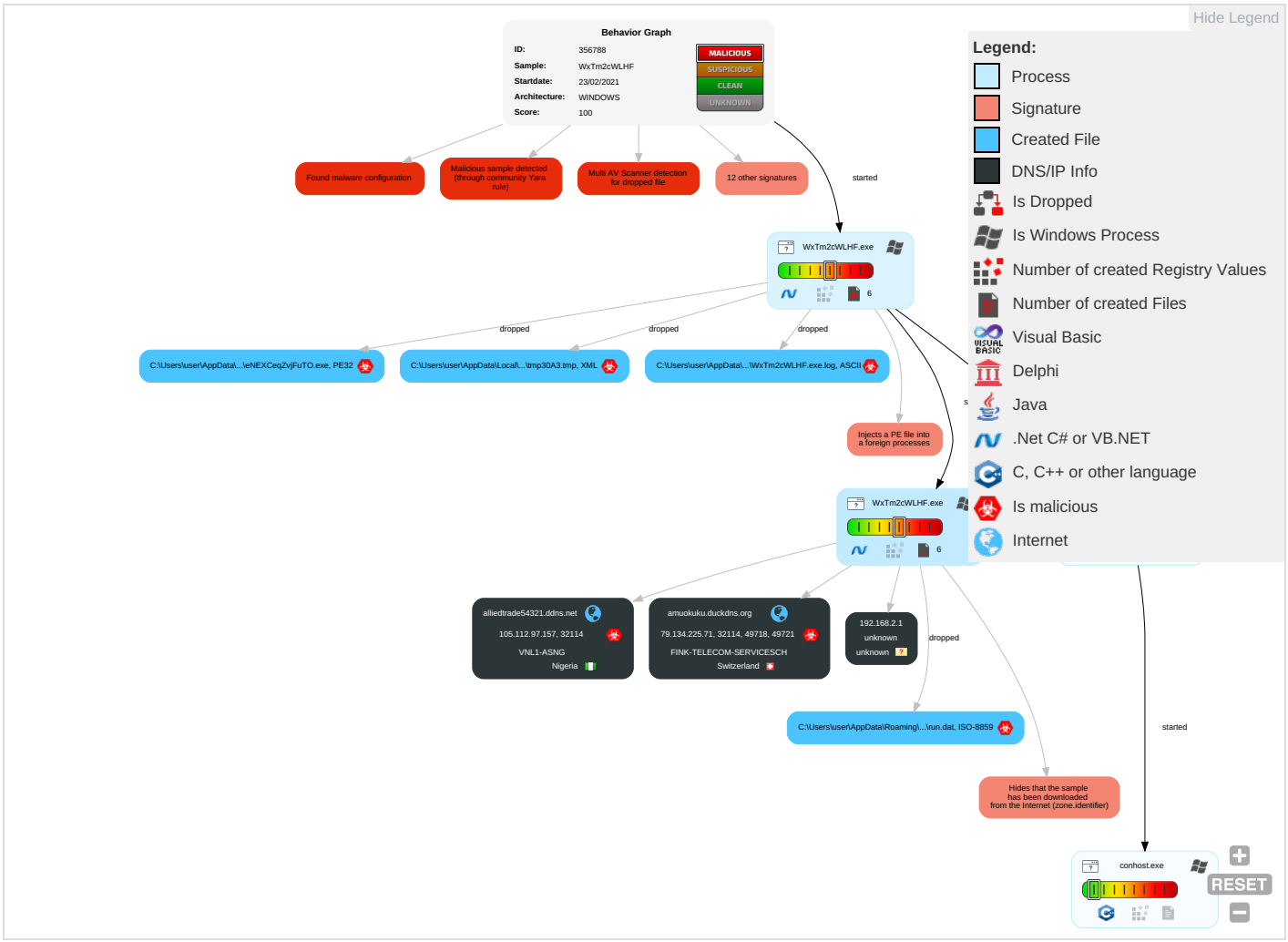
Detected Nanocore Rat

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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1 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	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	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)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	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	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
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	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

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
WxTm2cWLHF.exe	49%	Virustotal		Browse
WxTm2cWLHF.exe	30%	Metadefender		Browse
WxTm2cWLHF.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
WxTm2cWLHF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	30%	Metadefender		Browse
C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.WxTm2cWLHF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.WxTm2cWLHF.exe.6150000.10.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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
amuokuku.duckdns.org	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
alliedtrade54321.ddns.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alliedtrade54321.ddns.net	105.112.97.157	true	true		unknown
amuokuku.duckdns.org	79.134.225.71	true	true		unknown

Contacted URLs

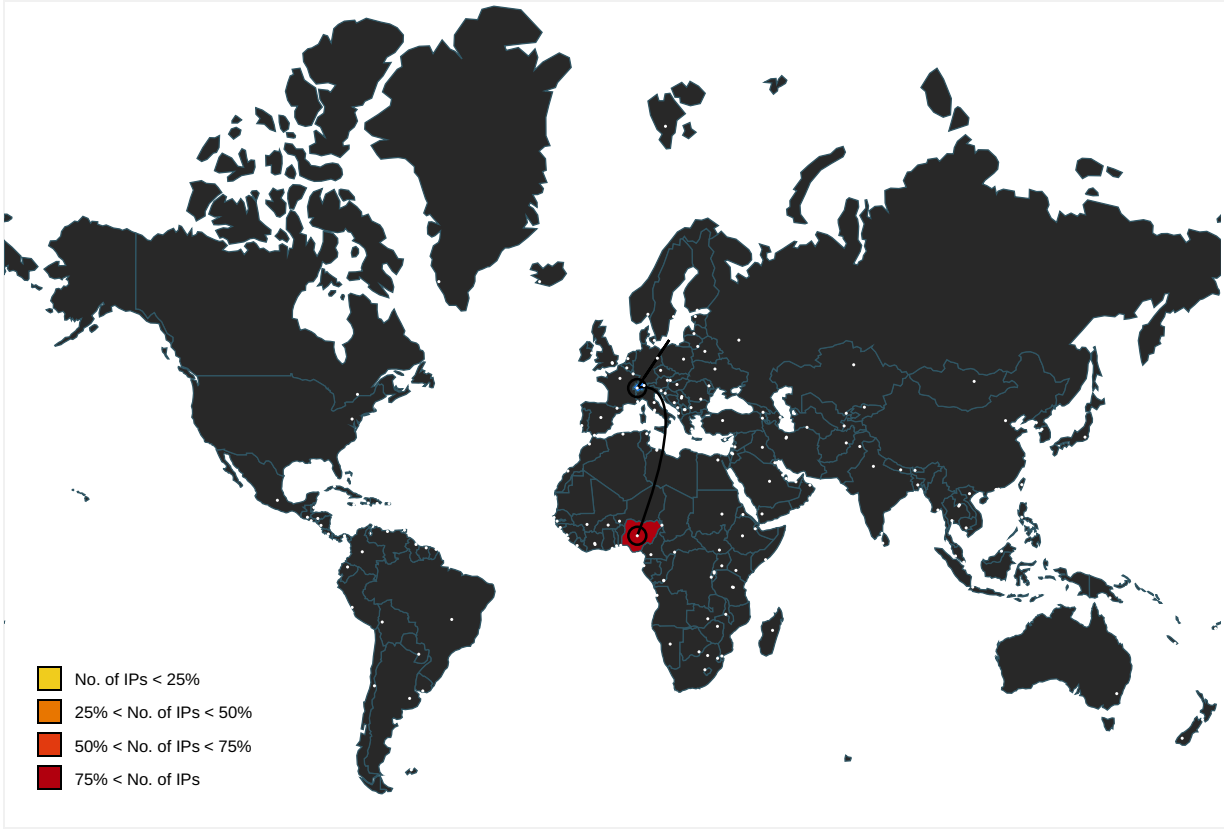
Name	Malicious	Antivirus Detection	Reputation
amuokuku.duckdns.org	true	• Avira URL Cloud: safe	unknown
alliedtrade54321.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.tiro.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WxTm2cWLHF.exe, 00000000.00000002.279546261.0000000002EB1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	WxTm2cWLHF.exe, 00000000.00000002.286567113.0000000007012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
105.112.97.157	unknown	Nigeria		36873	VNL1-ASNG	true
79.134.225.71	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	356788
Start date:	23.02.2021
Start time:	16:40:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WxTm2cWLHF (renamed file extension from none to 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:	23
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@6/4@10/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 51.103.5.186, 168.61.161.212, 131.253.33.200, 13.107.22.200, 51.104.144.132, 104.43.193.48, 23.211.6.115, 13.64.90.137, 13.88.21.125, 184.30.20.56, 51.104.139.180, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:40:57	API Interceptor	856x Sleep call for process: WxTm2cWLHF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.71	uHAHxir7cFIdUqL.exe	Get hash	malicious	Browse	
	Wrcpl1dkib.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	Swift-EUR 28700.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PAYMENT NOTIFICATION.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	fakture.exe	Get hash	malicious	Browse	
	BACK ORDER EXPORT0026254E_DOC_PDF.exe	Get hash	malicious	Browse	
	img_Payment Advice_822020_jpg.exe	Get hash	malicious	Browse	
	Bank Swift_7312020_PDF.exe	Get hash	malicious	Browse	
	LKVQYCZZkBgadMX.exe	Get hash	malicious	Browse	
	aXfA69gLbsTjxGu.exe	Get hash	malicious	Browse	
	22021Item_list_sheet#7292020_PDF.exe	Get hash	malicious	Browse	
	0RY9t35YcXOZNbf.exe	Get hash	malicious	Browse	
	Shipping Document COMM. INV. AFI0147660.js	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASERAL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76
	Orden.exe	Get hash	malicious	Browse	• 79.134.225.6
VNL1-ASNG	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 105.112.108.188
	OXplew3YfS.exe	Get hash	malicious	Browse	• 105.112.39.144
	Y8HGtWidPK.exe	Get hash	malicious	Browse	• 105.112.145.251
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 105.112.106.235
	8Z4Pwqk8E2.exe	Get hash	malicious	Browse	• 105.112.50.235
	Specification lista.doc	Get hash	malicious	Browse	• 105.112.50.235
	Protected.exe	Get hash	malicious	Browse	• 105.112.108.92
	Protected.2.exe	Get hash	malicious	Browse	• 105.112.101.243
	CN-Invoice-XXXXX9808-19011143287989 (2).exe	Get hash	malicious	Browse	• 105.112.109.252
	SWIFT_DCREF98302893884939475988EURO92847 9878364887737487578783 9.pdf.exe	Get hash	malicious	Browse	• 105.112.145.61
	RFQ_Report_19757_pdf____.exe	Get hash	malicious	Browse	• 105.112.37.158
	RFQ_Report_197_pdf____.exe	Get hash	malicious	Browse	• 105.112.39.136
	DOC 20210121__00101094001001001.exe	Get hash	malicious	Browse	• 105.112.101.11
	Purchase order LM20210120991001.exe	Get hash	malicious	Browse	• 105.112.97.27
	company profile.exe	Get hash	malicious	Browse	• 105.112.102.172
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	• 105.112.102.160
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.102.162
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.106.128
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WxTm2cWLHF.exe.log	
Process:	C:\Users\user\Desktop\WxTm2cWLHF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WxTm2cWLHF.exe.log	
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\tmp30A3.tmp	
Process:	C:\Users\user\Desktop\WxTm2cWLHF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.186199962114581
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKButn:cbhC7ZlNQF/rydbz9I3YODOLNdq3S
MD5:	78CF241614E152967085A98389274917
SHA1:	6D5F00D9AC3EA0E74DC7263BD591FA6C88F0CB45
SHA-256:	3FE6A17A16D3E41444BF023F53EBBEFF93E093AF60C0F6ED7E290E5E5E9D8B8E
SHA-512:	3C452CCE63221A6F75BEDEE116DB8DE48A234F0258D90203A077FC47C44E7FB11534CBCEB732624D80CC938D2A582D2ACCFC99EFE190FD25D54E1326AF35CFE
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>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\WxTm2cWLHF.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:iAjPn:iMPn
MD5:	66BE891445F5A78B0583526FF59F4E0D
SHA1:	85C561F403766238C5AADD91FB118AB876100FFD
SHA-256:	371859A54D364B21155F0A3258D151DE8BE5CA14E6585D87ADC9D6B7D5315D20
SHA-512:	F807334D17FAD0E5B2572C7D44FB11A619F63919BF1D8872A6B67E112B9C31A35541A1C5DB45F82A000AF1239DD32947586C453502CFC941221359D0C1D0A8F6
Malicious:	**true**
Reputation:	low
Preview:	.v..\..H

C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	
Process:	C:\Users\user\Desktop\WxTm2cWLHF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	761344
Entropy (8bit):	7.913371093347372
Encrypted:	false
SSDEEP:	12288:hDk0V4mojYDSq0+YWjUW0wQ4g9X/h+ZKAPX9DOr+LLrPBCs+cYv2tasGHW:hIdj9qtYWQWV3g9P4wmOr2tCssutasoW
MD5:	DA6D54EF4DD6752367FF3F516196B292
SHA1:	B88EA4E2BC892980E6E9A394A36CC262178BDBBD
SHA-256:	6F226CB3268AAFBE3FF45D8DAE3655C171AB7E6A0E2069815B761FFAD9E3A7EA
SHA-512:	2B7DFBFDAD286593327FC0A88F8DD6A4AEA478326F0452D78987C223C587A86AB934DF94E59EB2466AA9049EE35268C4587BF719840217185FE2123551A1B06A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	low

C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@.....0.....2.... .....@.. ....@.....O..... ....H.....text...8.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....0`.....X... .....0.....}.....(.....+..%.....+..%.....+....(.....+..%....., ..+.....+..%.....+....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{.....(....o.....{.....(....o.....{....(....o....*...0..... ....,. ....+.. .....X.+....., ..+..%.....+.....+..%.....,...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.913371093347372
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:	WxTm2cWLHF.exe
File size:	761344
MD5:	da6d54ef4dd6752367ff3f516196b292
SHA1:	b88ea4e2bc892980e6e9a394a36cc262178bdbbd
SHA256:	6f226cb3268aafbe3ff45d8dae3655c171ab7e6a0e2069815b761ffad9e3a7ea
SHA512:	2b7dfbfdad286593327fc0a88f8dd6a4aea478326f0452d78987c223c587a86ab934df94e59eb2466aa9049ee35268c4587bf719840217185fe2123551a1b06a
SSDEEP:	12288:hDk0V4mojYDSq0+YWjUW0wQ4g9X/h+ZKAPX9DOr+LLrPBCs+cYv2tasGHW:hIdj9qtYWQWV3g9P4wmOr2tCssutasoW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@.....0.....2.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bb232
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:	0xA6400EE4 [Tue May 21 14:12:52 2058 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xbb1e0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x5d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbb1c4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb9238	0xb9400	False	0.933784845226	data	7.91955251095	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5d8	0x600	False	0.443359375	data	4.25019891341	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc090	0x348	data		
RT_MANIFEST	0xbc3e8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

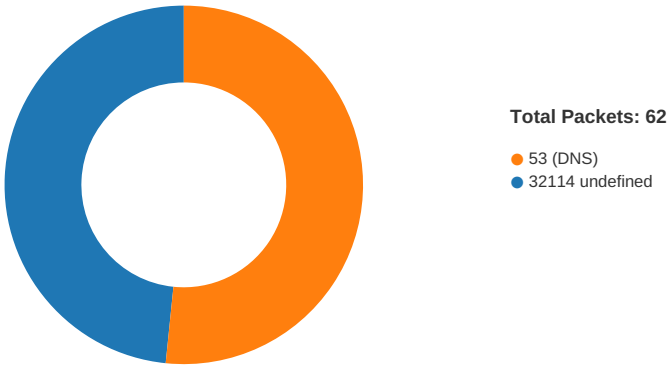
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	4.0.0.0
InternalName	2ygj.exe
FileVersion	4.0.0.0
CompanyName	
LegalTrademarks	
Comments	Neurology Ward
ProductName	Ward Manage
ProductVersion	4.0.0.0
FileDescription	Ward Manage
OriginalFilename	2ygj.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:41:19.342808962 CET	49718	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:19.425188065 CET	32114	49718	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:20.108927965 CET	49718	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:20.194417953 CET	32114	49718	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:20.811820984 CET	49718	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:20.896488905 CET	32114	49718	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:25.697400093 CET	49721	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:25.782759905 CET	32114	49721	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:26.312552929 CET	49721	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:26.397927999 CET	32114	49721	79.134.225.71	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:41:27.015450001 CET	49721	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:27.100970984 CET	32114	49721	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:31.389858961 CET	49722	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:31.475544930 CET	32114	49722	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:32.015906096 CET	49722	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:32.106271029 CET	32114	49722	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:32.703418970 CET	49722	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:41:32.788821936 CET	32114	49722	79.134.225.71	192.168.2.5
Feb 23, 2021 16:41:36.901573896 CET	49723	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:41:39.907102108 CET	49723	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:41:45.907639980 CET	49723	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:41:53.570995092 CET	49732	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:41:56.580395937 CET	49732	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:02.597054958 CET	49732	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:10.246635914 CET	49734	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:13.253674984 CET	49734	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:19.254192114 CET	49734	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:28.394542933 CET	49735	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:28.479233027 CET	32114	49735	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:28.989315987 CET	49735	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:29.072365999 CET	32114	49735	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:29.583412886 CET	49735	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:29.667824030 CET	32114	49735	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:34.024620056 CET	49736	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:34.112453938 CET	32114	49736	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:34.614995956 CET	49736	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:34.702390909 CET	32114	49736	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:35.208592892 CET	49736	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:35.294507980 CET	32114	49736	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:39.586431980 CET	49737	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:39.669121981 CET	32114	49737	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:40.177938938 CET	49737	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:40.264960051 CET	32114	49737	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:40.771559954 CET	49737	32114	192.168.2.5	79.134.225.71
Feb 23, 2021 16:42:40.856256008 CET	32114	49737	79.134.225.71	192.168.2.5
Feb 23, 2021 16:42:45.055721045 CET	49738	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:48.069046974 CET	49738	32114	192.168.2.5	105.112.97.157
Feb 23, 2021 16:42:54.069581985 CET	49738	32114	192.168.2.5	105.112.97.157

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:40:42.037596941 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:42.089063883 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:42.124280930 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:42.183512926 CET	53	53784	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:42.640094995 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:42.681694031 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:42.693265915 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:42.732157946 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:43.767921925 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:43.816921949 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:44.745151997 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:44.795537949 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:45.042634010 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:45.101361036 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:45.734138012 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:45.782907009 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:46.938448906 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:46.987149954 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:52.688620090 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:52.740266085 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:53.715102911 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:53.763701916 CET	53	52441	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:40:54.892847061 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:54.942040920 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:55.900330067 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:55.951833963 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:56.931376934 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:56.982983112 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:58.312891006 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:58.361665010 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 16:40:59.471916914 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:40:59.523488998 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:10.593978882 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:10.665903091 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:19.099385977 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:19.323225975 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:21.875500917 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:21.927145004 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:25.476241112 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:25.695888042 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:31.163094997 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:31.383889914 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:36.837410927 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:36.900299072 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:38.061328888 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:38.113519907 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:40.435273886 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:40.483845949 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:47.697206974 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:47.758457899 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 16:41:53.506145000 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:41:53.566163063 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:00.694535971 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:00.767443895 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:10.186449051 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:10.245104074 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:28.335293055 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:28.392420053 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:33.801003933 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:34.021429062 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:39.336334944 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:39.557692051 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 16:42:44.989430904 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 16:42:45.051445007 CET	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 16:41:19.099385977 CET	192.168.2.5	8.8.8.8	0xe570	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:25.476241112 CET	192.168.2.5	8.8.8.8	0x2e93	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:31.163094997 CET	192.168.2.5	8.8.8.8	0xb18f	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:36.837410927 CET	192.168.2.5	8.8.8.8	0x31a3	Standard query (0)	alliedtrade54321.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:53.506145000 CET	192.168.2.5	8.8.8.8	0x4b08	Standard query (0)	alliedtrade54321.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:10.186449051 CET	192.168.2.5	8.8.8.8	0x7779	Standard query (0)	alliedtrade54321.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:28.335293055 CET	192.168.2.5	8.8.8.8	0xc5f4	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:33.801003933 CET	192.168.2.5	8.8.8.8	0x7dd4	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:39.336334944 CET	192.168.2.5	8.8.8.8	0x997b	Standard query (0)	amuokuku.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:44.989430904 CET	192.168.2.5	8.8.8.8	0x9c30	Standard query (0)	alliedtrade54321.ddns.net	A (IP address)	IN (0x0001)

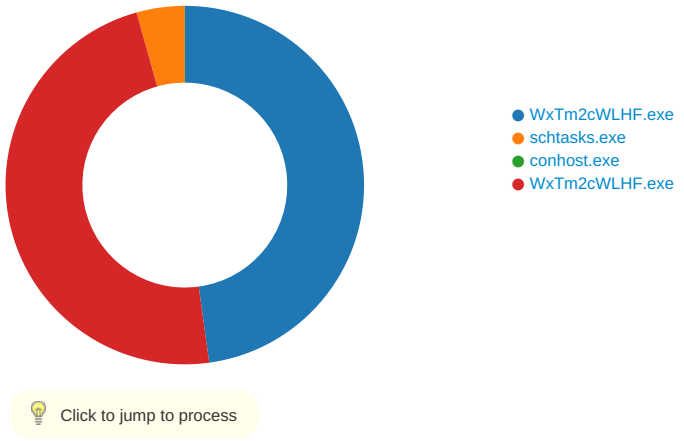
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 16:41:19.323225975 CET	8.8.8.8	192.168.2.5	0xe570	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:25.695888042 CET	8.8.8.8	192.168.2.5	0x2e93	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:31.383889914 CET	8.8.8.8	192.168.2.5	0xb18f	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:36.900299072 CET	8.8.8.8	192.168.2.5	0x31a3	No error (0)	alliedtrade54321.ddns.net		105.112.97.157	A (IP address)	IN (0x0001)
Feb 23, 2021 16:41:53.566163063 CET	8.8.8.8	192.168.2.5	0x4b08	No error (0)	alliedtrade54321.ddns.net		105.112.97.157	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:10.245104074 CET	8.8.8.8	192.168.2.5	0x7779	No error (0)	alliedtrade54321.ddns.net		105.112.97.157	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:28.392420053 CET	8.8.8.8	192.168.2.5	0xc5f4	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:34.021429062 CET	8.8.8.8	192.168.2.5	0x7dd4	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:39.557692051 CET	8.8.8.8	192.168.2.5	0x997b	No error (0)	amuokuku.duckdns.org		79.134.225.71	A (IP address)	IN (0x0001)
Feb 23, 2021 16:42:45.051445007 CET	8.8.8.8	192.168.2.5	0x9c30	No error (0)	alliedtrade54321.ddns.net		105.112.97.157	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WxTm2cWLHF.exe PID: 5512 Parent PID: 5652

General

Start time:	16:40:50
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\WxTm2cWLHF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WxTm2cWLHF.exe'
Imagebase:	0xaa0000
File size:	761344 bytes
MD5 hash:	DA6D54EF4DD6752367FF3F516196B292
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: 00000000.00000002.279715040.0000000003EB9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.279715040.0000000003EB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.279715040.0000000003EB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.281914406.00000000043AE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.281914406.00000000043AE000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.281914406.00000000043AE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6DADCF06	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	6DADCF06	unknown
C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp30A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C927038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WxTm2cWLHF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDEC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30A3.tmp	success or wait	1	6C926A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\eNEXCeqZvjFuTO.exe	unknown	761344	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 00 00 00 00 80 00 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 50 45 00 00 4c 01 03 00 e4 0e 40 a6 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 0b 00 00 08 00 00 00 00 00 00 32 b2 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L.....@........... ....0.............2.... ....@.. ....@................	success or wait	1	6C921B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp30A3.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6C921B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WxTm2cWLHF.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",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_v4.0.3	success or wait	1	6DDEC907	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	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Users\user\Desktop\WxTm2cWLHF.exe	unknown	761344	success or wait	1	6C921B4F	ReadFile

Analysis Process: schtasks.exe PID: 6612 Parent PID: 5512

General

Start time:	16:41:13
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eNEXCeqZvjFuTO' /XML 'C:\Users\user\AppData\Local\Temp\tmp30A3.tmp'
Imagebase:	0xf10000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30A3.tmp	unknown	2	success or wait	1	F1AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp30A3.tmp	unknown	1652	success or wait	1	F1ABD9	ReadFile

Analysis Process: conhost.exe PID: 6620 Parent PID: 6612

General

Start time:	16:41:14
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: WxTm2cWLHF.exe PID: 6664 Parent PID: 5512

General

Start time:	16:41:14
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\WxTm2cWLHF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb40000
File size:	761344 bytes
MD5 hash:	DA6D54EF4DD6752367FF3F516196B292
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: 00000007.00000002.499194196.0000000006150000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.499194196.0000000006150000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.499194196.0000000006150000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.497750745.0000000003F29000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.497750745.0000000003F29000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.491562642.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.491562642.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.491562642.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.494580677.0000000002EE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.498775362.00000000055D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.498775362.00000000055D0000.00000004.00000001.sdmp, Author: Florian Roth
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	6DADCF06	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	6DADCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C921E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C92BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WxTm2cWLHF.exe:Zone.Identifier	success or wait	1	6C8A2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	ba 76 c3 e5 5c d8 d8 48	.v..\..H	success or wait	1	6C921B4F	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	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Users\user\Desktop\WxTm2cWLHF.exe	unknown	4096	success or wait	1	6DA9D72F	unknown
C:\Users\user\Desktop\WxTm2cWLHF.exe	unknown	512	success or wait	1	6DA9D72F	unknown

Disassembly

Code Analysis