ID: 881357
Sample Name: HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Cookbook: default.jbs
Time: 04:41:06
Date: 04/06/2023
Version: 37.1.0 Beryl

Table of Contents

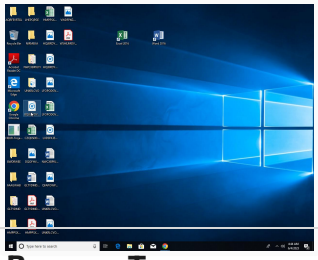
Windows Analysis Report

HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe

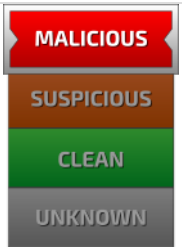
Overview

General Information

Sample Name:	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Analysis ID:	881357
MD5:	81b7988b523fb..
SHA1:	9d14022defd13..
SHA256:	1617174ffdba5...
Tags:	exe NanoCore RAT
Infos:	



Detection



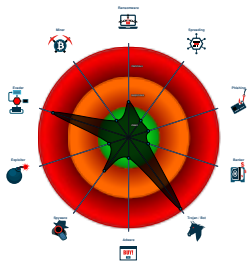
Nanocore

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
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…

Classification



Process Tree

- **System is w10x64**
- HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe (PID: 7144 cmdline: C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe MD5: 81B7988B523FB109B834C76E7F0FEA10)
  - schtasks.exe (PID: 6060 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAqpXXDLkkJ" /XML "C:\Users\user\AppData\Local\Temp\tmpBEA2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe (PID: 5756 cmdline: C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe MD5: 81B7988B523FB109B834C76E7F0FEA10)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "8016d6d7-9a9c-4266-8244-58d40eab",
  "Group": "Mba-Month",
  "Domain1": "podzeye.duckdns.org",
  "Domain2": "",
  "Port": 414,
  "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": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x10a5d:$x1: NanoCore.ClientPluginHost • 0x10a9a:$x2: IClientNetworkHost • 0x145cd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x107c5:$a: NanoCore • 0x107d5:$a: NanoCore • 0x10a09:$a: NanoCore • 0x10a1d:$a: NanoCore • 0x10a5d:$a: NanoCore • 0x10824:$b: ClientPlugin • 0x10a26:$b: ClientPlugin • 0x10a66:$b: ClientPlugin • 0x1094b:$c: ProjectData • 0x11352:$d: DESCrypto • 0x18d1e:$e: KeepAlive • 0x16d0c:$g: LogClientMessage • 0x12f07:$i: get_Connected • 0x11688:$j: #=q • 0x116b8:$j: #=q • 0x116d4:$j: #=q • 0x11704:$j: #=q • 0x11720:$j: #=q • 0x1173c:$j: #=q • 0x1176c:$j: #=q • 0x11788:$j: #=q
00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x10a5d:$a1: NanoCore.ClientPluginHost • 0x10a1d:$a2: NanoCore.ClientPlugin • 0x12976:$b1: get_BuilderSettings • 0x10879:$b2: ClientLoaderForm.resources • 0x12096:$b3: PluginCommand • 0x10a4e:$b4: IClientAppHost • 0x1aece:$b5: GetBlockHash • 0x12fce:$b6: AddHostEntry • 0x16cc1:$b7: LogClientException • 0x12f3b:$b8: PipeExists • 0x10a87:$b9: IClientLoggingHost

Source	Rule	Description	Author	Strings
00000000.00000002.375141713.0000000002C14000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.50f0000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
3.2.HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.50f0000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
3.2.HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.50f0000.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
3.2.HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.50f0000.5.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
3.2.HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.3c8e434.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 57 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26 −

Timestamp:	192.168.2.3192.169.69.26497084142816766 06/04/23-04:43:12.068942
SID:	2816766
Source Port:	49708
Destination Port:	414
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

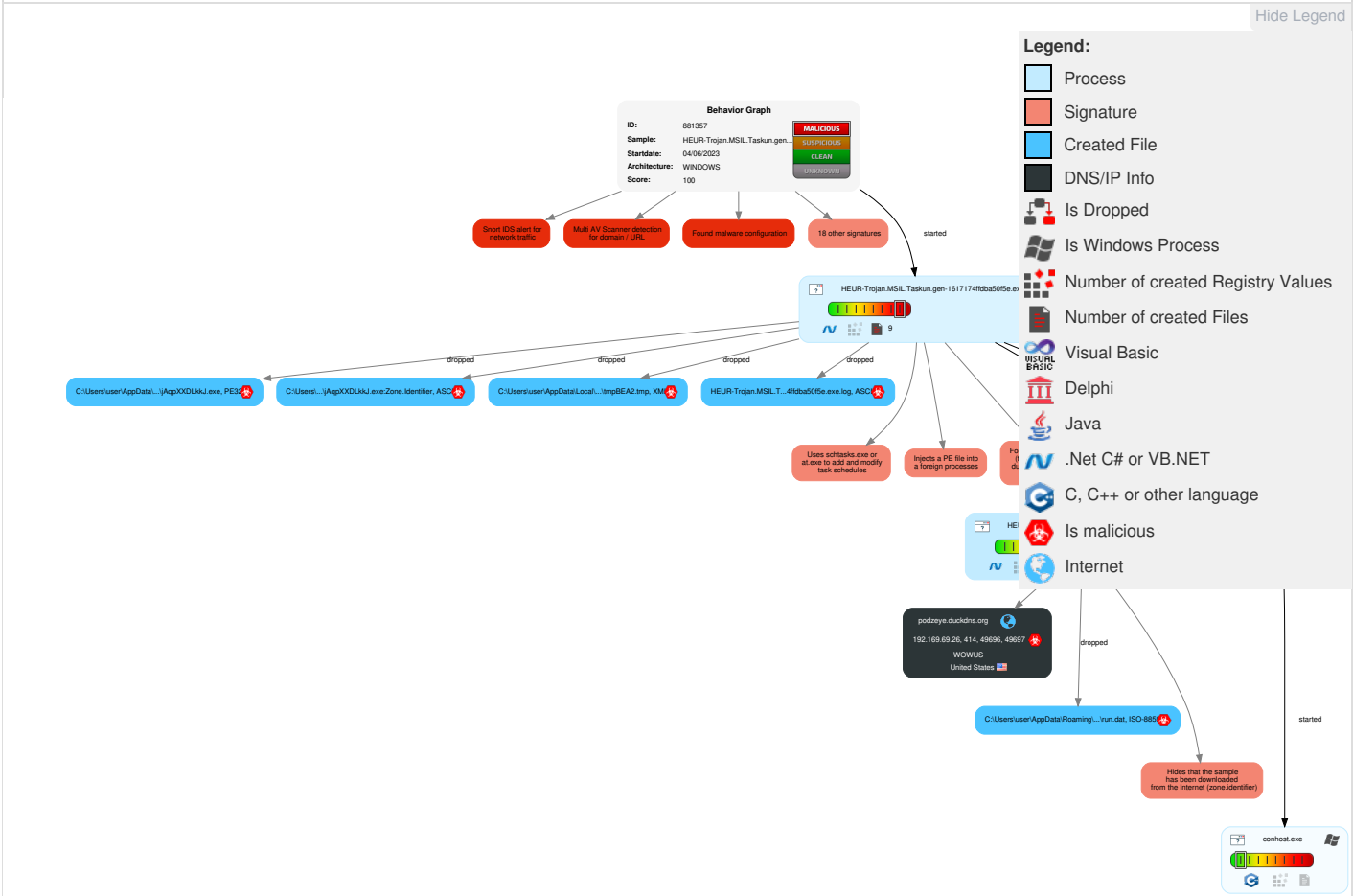
Detected Nanocore Rat

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	1 Masquerading	2 1 Input Capture	2 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 2 Process Injection	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 2 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	65%	Virustotal		Browse
HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	100%	Avira	HEUR/AGEN.1306098	
HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jAqpXXDLkkJ.exe	100%	Avira	HEUR/AGEN.1306098	
C:\Users\user\AppData\Roaming\jAqpXXDLkkJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jAqpXXDLkkJ.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
podzeye.duckdns.org	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.fontbureau.coml1	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	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comz	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.tiro.comd	0%	URL Reputation	safe	
	0%	Avira URL Cloud	safe	
http://www.sakkal.comrmJ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/=	0%	Virustotal		Browse
podzeye.duckdns.org	16%	Virustotal		Browse
http://www.t.	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/=	0%	Avira URL Cloud	safe	
podzeye.duckdns.org	100%	Avira URL Cloud	malware	
http://www.fontbureau.comldno	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
podzeye.duckdns.org	192.169.69.26	true	true	• 16%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
podzeye.duckdns.org	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

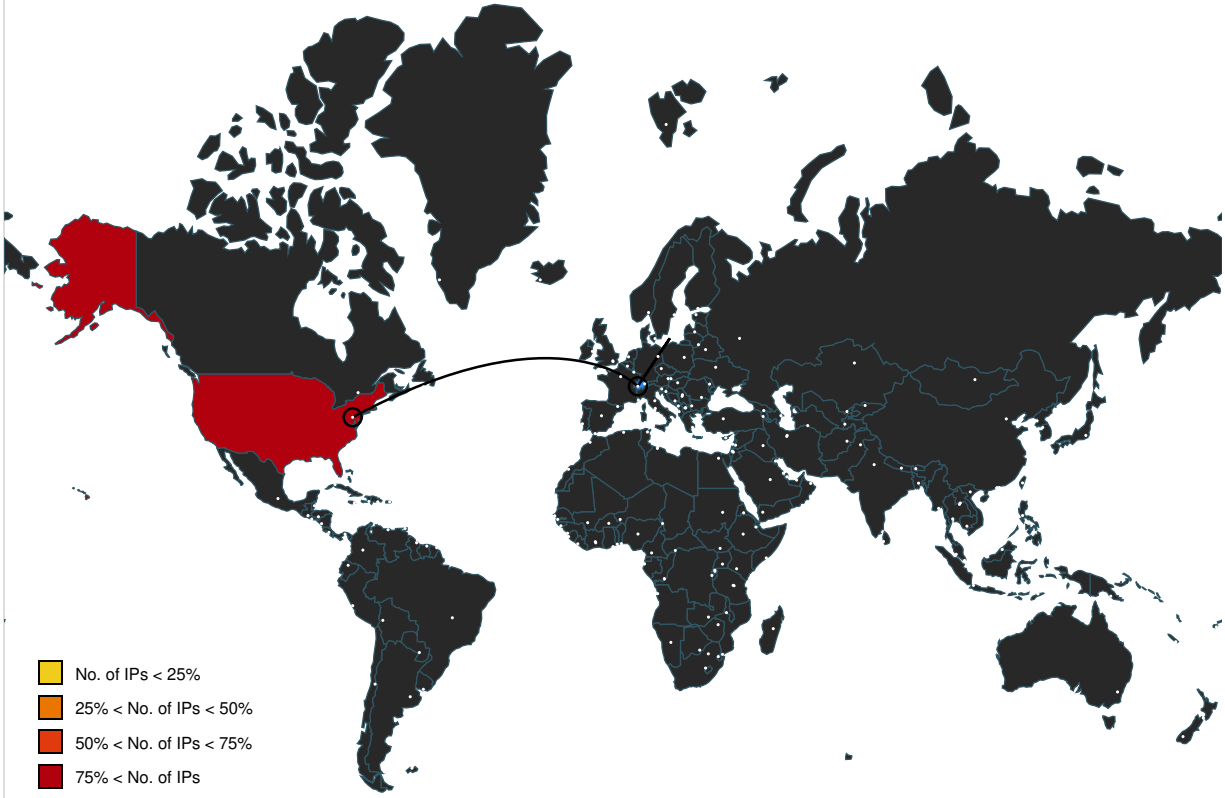
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.374035218.00000000055A0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.368418627.00000000055D6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/=	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.368418627.00000000055D6000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.tiro.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365340286.00000000055A2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.374035218.00000000055A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365534017.00000000055D6000.00000004.00000020.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365581213.00000000055D6000.00000004.00000020.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365600611.00000000055D6000.00000004.00000020.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365617649.00000000055D6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coml1	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.374035218.00000000055A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.0000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.363939571.00000000055BB000.00000004.00000020.00020000.00000000.sdmp, HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.363954268.00000000055BB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.comrmJ	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.366069273.0000000055E1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.t.	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365340286.0000000055A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comz	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.367096675.0000000055A6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000002.378015829.000000006782000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comldno	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.374035218.00000000055A0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comR.TTF	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.367096675.00000000055A6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comd	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe, 00000000.00000003.365340286.00000000055A2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.26	podzeye.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	881357
Start date and time:	2023-06-04 04:41:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
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
Sample file name:	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@22/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile 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
04:42:02	API Interceptor	856x Sleep call for process: HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe.log

Process:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	895
Entropy (8bit):	5.267807484859312
Encrypted:	false
SSDEEP:	24:MLF20NaL329hJ5g522rW2a2+g2s26K95rKoOz2T:MwLLG9h3go2rx9+g2X6oG2T
MD5:	B3E077F49443B4E3033A37748D818FC6
SHA1:	6C06565EF8ABD974E8D34BFDBC8981CFC67562E4
SHA-256:	D1118A0BBCF7AF4819F9678314431A418D3B77767312FA6436A6564EB0F9FF83
SHA-512:	2E55D43B305984CE230BE4E00220CC51FFB358592D9D010A77174A4E27E18D7D9F32A826D3E780AAA423A380999E50F84E6C43328162F8B2917CE00E1EFBD338
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Data\ 27ab8d047396db374abb803b446b76f0\System.Data.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c 619a3e1d3\System.Xml.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configu ration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpBEA2.tmp

Process:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.205337193730257
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBHs2tn:cbh47TlNQ//rydbz9I3YODOLNdq3aA
MD5:	E505E84B7674DD82695781E85F907F55
SHA1:	004AAAE57BA1FF6213D3A279CCC95446EDA68849
SHA-256:	173CD7A8C1F06287BA9251A4201C98D3F02886BF785B4AC0726421EA6475CB14
SHA-512:	46D364899919CC21EF4AD6B82A67762EB87A071381A3E4639B679B46E3FACA073C73B8A8BDBD8A4505F13AA6C734EF7CF4F472D44FF3777CEF07B761EC13D1E A
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\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:DSn:DSn
MD5:	6168249EA05B80227B36364801A82F6E
SHA1:	87AB76476E06A4A980558870F8DABEA3D81FE1EE
SHA-256:	FA1CB67CC9EFFA397D609F4F7B758E5FCFD80E545D979018AD9F4F6EE7314AB4
SHA-512:	2EDCC0B25F7C8D848965D35D89C707CC9AC1C0A4DE6D6B53764DCD73EDEC090E2349993D25398D2E347F2A89169A7F7FFD9D721CA15D48AAF6F09369DB418AF
Malicious:	**true**
Reputation:	low
Preview:	C.:..d.H

C:\Users\user\AppData\Roaming\jAqpXXDLkkJ.exe

Process:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	546816
Entropy (8bit):	7.516638880644476
Encrypted:	false
SSDEEP:	12288:FKk4DbF53e0IUFLuEEfrrmdQ5S/eMGXZLfJOSq7Ls9:F0SEwrmW5PMGVJOSCL
MD5:	81B7988B523FB109B834C76E7F0FEA10
SHA1:	9D14022DEFD1373971A2892B1A5B5BBE830280CE
SHA-256:	1617174FFDBA50F5EFA07C53E0FFB0D765F35CBE821173BDA7CD96C1F5CFE5CD
SHA-512:	17E6BA0DBCA1CFD06D684F6A512CD6C45CA4ED161289FC14D5C5AC4244E33A55657DF85AC249EEDD2031E7DCF29FE4C5478D28EA7A4CF8D621530E1EB633ADF
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 68%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....?a.....0..@.....^... ...`....@.. .....@.....]..O...`..... ....H.....text... >... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....V.....@..B.....]....H.....d.....2...hH..X.....0..P.....(.....s....}.....++...+...{.....s....(.....X.....-....X.....-.*.0.....{. ....+..*&...}....*...0.....0...2....0.....+.....r...p..(.....(.....(....o.....,.....r?..p..(.....+D...o.....+...(.....(.....(....o.....(....-.....o.....*.....d.+.....0..".....~3.....9.....~ 4.....o.....+.....+.....X.....-....X.....-..-

C:\Users\user\AppData\Roaming\jAqpXXDLkkJ.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
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):	7.516638880644476
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:	HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
File size:	546816
MD5:	81b7988b523fb109b834c76e7f0fea10
SHA1:	9d14022defd1373971a2892b1a5b5bbe830280ce
SHA256:	1617174ffdba50f5efa07c53e0ffb0d765f35cbe821173bda7cd96c1f5cfe5cd
SHA512:	17e6ba0dbca1cfd06d684f6a512cd6c45ca4ed161289fc14d5c5ac4244e33a55657df85ac249eedd2031e7dcf29fe4c5478d28ea7a4cf8d621530e1eb6331adf
SSDEEP:	12288:FKk4DbF53e0IUFLuEEfrrmdQ5S/eMGXZLfJOSq7Ls9:F0SEwrmW5PMGVJOSCL
TLSH:	42C4BE203DFB5119F1B3BFB65EE075868A6FF6332A17E45D104503864B23A81DE91A3B

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....?a.............0..@...........^... ...`....@.. ....@................................

File Icon

Icon Hash:	8e65656565a5a581

Static PE Info

General

Entrypoint:	0x485e12
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x613FEAC3 [Tue Sep 14 00:20:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
sub byte ptr [eax], al
sub al, 00h
sub dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0x85dc0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x13b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x83e20	0x84000	False	0.8557406338778409	data	7.526269053088037	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x13b8	0x1400	False	0.549609375	data	6.174184576615129	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x86130	0xd0c	Device independent bitmap graphic, 32 x 50 x 32, image size 3200		
RT_GROUP_ICON	0x86e3c	0x14	data		
RT_VERSION	0x86e50	0x37c	data		
RT_MANIFEST	0x871cc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3192.169.69.26 497084142816766 06/04/23-04:43:12.068942	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	414	192.168.2.3	192.169.69.26

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 04:42:08.593722105 CEST	49696	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:09.072313070 CEST	414	49696	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:09.073271036 CEST	49696	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:09.246226072 CEST	49696	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:09.575026035 CEST	414	49696	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:13.826567888 CEST	49697	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:14.075243950 CEST	414	49697	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:14.075371981 CEST	49697	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:14.076153040 CEST	49697	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:14.581448078 CEST	414	49697	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:19.022104025 CEST	49698	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:19.563606977 CEST	414	49698	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:19.563736916 CEST	49698	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:19.579202890 CEST	49698	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:20.068938017 CEST	414	49698	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:24.265559912 CEST	49699	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:24.578030109 CEST	414	49699	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:24.578366041 CEST	49699	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:24.579011917 CEST	49699	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:25.069581985 CEST	414	49699	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:29.295825958 CEST	49700	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:29.573273897 CEST	414	49700	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:29.573376894 CEST	49700	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:29.573837042 CEST	49700	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:30.069685936 CEST	414	49700	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:34.268313885 CEST	49701	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:34.573151112 CEST	414	49701	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:34.573282957 CEST	49701	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:34.573657036 CEST	49701	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:35.068526030 CEST	414	49701	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:39.284648895 CEST	49702	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:39.576230049 CEST	414	49702	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:39.578665018 CEST	49702	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:39.579507113 CEST	49702	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:40.069488049 CEST	414	49702	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:44.197591066 CEST	49703	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:44.578819990 CEST	414	49703	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:44.579087019 CEST	49703	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:44.579682112 CEST	49703	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:45.071170092 CEST	414	49703	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:49.353243113 CEST	49704	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:49.573173046 CEST	414	49704	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:49.573282957 CEST	49704	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:49.605051994 CEST	49704	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:50.070497990 CEST	414	49704	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:54.453860998 CEST	49705	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:55.065051079 CEST	414	49705	192.169.69.26	192.168.2.3
Jun 4, 2023 04:42:55.065272093 CEST	49705	414	192.168.2.3	192.169.69.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 04:42:55.118761063 CEST	49705	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:42:55.573617935 CEST	414	49705	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:00.431969881 CEST	49706	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:01.064155102 CEST	414	49706	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:01.064308882 CEST	49706	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:01.065073013 CEST	49706	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:01.568650961 CEST	414	49706	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:06.146394968 CEST	49707	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:06.574738979 CEST	414	49707	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:06.574925900 CEST	49707	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:06.575464010 CEST	49707	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:07.072035074 CEST	414	49707	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:11.383093119 CEST	49708	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:11.571010113 CEST	414	49708	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:11.571146965 CEST	49708	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:11.588933945 CEST	49708	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:12.068942070 CEST	49708	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:12.070327044 CEST	414	49708	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:12.571326971 CEST	414	49708	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:16.366458893 CEST	49709	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:16.574939966 CEST	414	49709	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:16.575073957 CEST	49709	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:16.577032089 CEST	49709	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:17.070564985 CEST	414	49709	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:21.192884922 CEST	49710	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:21.573195934 CEST	414	49710	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:21.573338032 CEST	49710	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:21.603037119 CEST	49710	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:22.070581913 CEST	414	49710	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:26.181845903 CEST	49711	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:26.572562933 CEST	414	49711	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:26.574724913 CEST	49711	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:26.576728106 CEST	49711	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:27.069644928 CEST	414	49711	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:34.509677887 CEST	49712	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:35.065113068 CEST	414	49712	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:35.065305948 CEST	49712	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:35.065699100 CEST	49712	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:35.570178032 CEST	414	49712	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:40.214036942 CEST	49713	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:40.576226950 CEST	414	49713	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:40.576329947 CEST	49713	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:40.582603931 CEST	49713	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:41.069681883 CEST	414	49713	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:45.923980951 CEST	49714	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:46.568640947 CEST	414	49714	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:46.569830894 CEST	49714	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:46.593607903 CEST	49714	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:47.075848103 CEST	414	49714	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:51.273710012 CEST	49715	414	192.168.2.3	192.169.69.26
Jun 4, 2023 04:43:51.575884104 CEST	414	49715	192.169.69.26	192.168.2.3
Jun 4, 2023 04:43:51.576004982 CEST	49715	414	192.168.2.3	192.169.69.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 04:42:08.461453915 CEST	52387	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:08.584316015 CEST	53	52387	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:13.804982901 CEST	56924	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 04:42:13.825361967 CEST	53	56924	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:18.991372108 CEST	60625	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:19.019965887 CEST	53	60625	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:24.148152113 CEST	49302	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:24.261750937 CEST	53	49302	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:29.265285969 CEST	53975	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:29.294018984 CEST	53	53975	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:34.246910095 CEST	51139	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:34.267290115 CEST	53	51139	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:39.262290001 CEST	52955	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:39.283380985 CEST	53	52955	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:44.172225952 CEST	60582	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:44.195631981 CEST	53	60582	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:49.229825974 CEST	57134	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:49.352425098 CEST	53	57134	8.8.8.8	192.168.2.3
Jun 4, 2023 04:42:54.336741924 CEST	62050	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:42:54.450535059 CEST	53	62050	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:00.401382923 CEST	56042	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:00.430135012 CEST	53	56042	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:06.116441965 CEST	59636	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:06.145123959 CEST	53	59636	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:11.264379025 CEST	55638	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:11.382052898 CEST	53	55638	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:16.186063051 CEST	57704	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:16.313746929 CEST	53	57704	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:21.163583994 CEST	65320	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:21.191978931 CEST	53	65320	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:26.157421112 CEST	60767	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:26.178278923 CEST	53	60767	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:34.487503052 CEST	65107	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:34.508172035 CEST	53	65107	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:40.115076065 CEST	53848	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:40.144586086 CEST	53	53848	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:45.902225018 CEST	57571	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:45.922760963 CEST	53	57571	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:51.144181013 CEST	58691	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:51.269069910 CEST	53	58691	8.8.8.8	192.168.2.3
Jun 4, 2023 04:43:57.385121107 CEST	53305	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:43:57.499840975 CEST	53	53305	8.8.8.8	192.168.2.3
Jun 4, 2023 04:44:02.610562086 CEST	59433	53	192.168.2.3	8.8.8.8
Jun 4, 2023 04:44:02.639483929 CEST	53	59433	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 4, 2023 04:42:08.461453915 CEST	192.168.2.3	8.8.8.8	0xb877	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:13.804982901 CEST	192.168.2.3	8.8.8.8	0x5851	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:18.991372108 CEST	192.168.2.3	8.8.8.8	0xe43e	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:24.148152113 CEST	192.168.2.3	8.8.8.8	0x19ef	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:29.265285969 CEST	192.168.2.3	8.8.8.8	0x3894	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:34.246910095 CEST	192.168.2.3	8.8.8.8	0xb827	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:39.262290001 CEST	192.168.2.3	8.8.8.8	0xeca7	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:44.172225952 CEST	192.168.2.3	8.8.8.8	0x21c2	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 4, 2023 04:42:49.229825974 CEST	192.168.2.3	8.8.8.8	0xd1f	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:54.336741924 CEST	192.168.2.3	8.8.8.8	0x706e	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:00.401382923 CEST	192.168.2.3	8.8.8.8	0x8b26	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:06.116441965 CEST	192.168.2.3	8.8.8.8	0x3ccb	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:11.264379025 CEST	192.168.2.3	8.8.8.8	0x76f0	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:16.186063051 CEST	192.168.2.3	8.8.8.8	0x21fa	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:21.163583994 CEST	192.168.2.3	8.8.8.8	0x6884	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:26.157421112 CEST	192.168.2.3	8.8.8.8	0x8134	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:34.487503052 CEST	192.168.2.3	8.8.8.8	0x198d	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:40.115076065 CEST	192.168.2.3	8.8.8.8	0x686	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:45.902225018 CEST	192.168.2.3	8.8.8.8	0xaba2	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:51.144181013 CEST	192.168.2.3	8.8.8.8	0x8ad3	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:57.385121107 CEST	192.168.2.3	8.8.8.8	0x720d	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:44:02.610562086 CEST	192.168.2.3	8.8.8.8	0x682b	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)	false

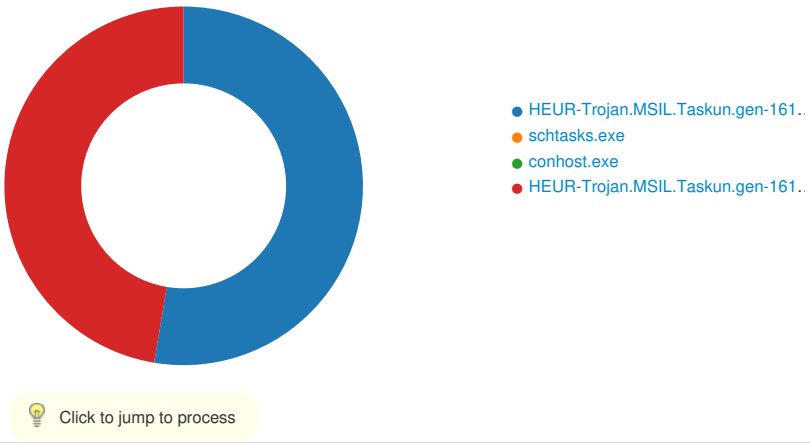
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 4, 2023 04:42:08.584316015 CEST	8.8.8.8	192.168.2.3	0xb877	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:13.825361967 CEST	8.8.8.8	192.168.2.3	0x5851	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:19.019965887 CEST	8.8.8.8	192.168.2.3	0xe43e	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:24.261750937 CEST	8.8.8.8	192.168.2.3	0x19ef	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:29.294018984 CEST	8.8.8.8	192.168.2.3	0x3894	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:34.267290115 CEST	8.8.8.8	192.168.2.3	0xb827	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:39.283380985 CEST	8.8.8.8	192.168.2.3	0xeca7	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:44.195631981 CEST	8.8.8.8	192.168.2.3	0x21c2	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:49.352425098 CEST	8.8.8.8	192.168.2.3	0xd1f	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:42:54.450535059 CEST	8.8.8.8	192.168.2.3	0x706e	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:00.430135012 CEST	8.8.8.8	192.168.2.3	0x8b26	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:06.145123959 CEST	8.8.8.8	192.168.2.3	0x3ccb	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:11.382052898 CEST	8.8.8.8	192.168.2.3	0x76f0	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 4, 2023 04:43:16.313746929 CEST	8.8.8.8	192.168.2.3	0x21fa	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:21.191978931 CEST	8.8.8.8	192.168.2.3	0x6884	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:26.178278923 CEST	8.8.8.8	192.168.2.3	0x8134	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:34.508172035 CEST	8.8.8.8	192.168.2.3	0x198d	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:40.144586086 CEST	8.8.8.8	192.168.2.3	0x686	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:45.922760963 CEST	8.8.8.8	192.168.2.3	0xaba2	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:51.269069910 CEST	8.8.8.8	192.168.2.3	0x8ad3	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:43:57.499840975 CEST	8.8.8.8	192.168.2.3	0x720d	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 04:44:02.639483929 CEST	8.8.8.8	192.168.2.3	0x682b	No error (0)	podzeye.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe PID: **7144**, Parent PID: **3452**

General

Target ID:	0
Start time:	04:42:02
Start date:	04/06/2023
Path:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Imagebase:	0x2a0000

File size:	546816 bytes
MD5 hash:	81B7988B523FB109B834C76E7F0FEA10
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: 00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.380153441.0000000009E78000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.375141713.0000000002C14000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.380153441.0000000009D51000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.380153441.0000000009D51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.380153441.0000000009D51000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.380153441.0000000009D51000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: 6060, Parent PID: 7144

General

Target ID:	1
Start time:	04:42:07
Start date:	04/06/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAqpXXDLkkJ" /XML "C:\Users\user\AppData\Local\Temp\tmpBEA2.tmp
Imagebase:	0x8f0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6088, Parent PID: 6060

General

Target ID:	2
Start time:	04:42:07
Start date:	04/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe PID: **5756**, Parent PID: **7144**

General

Target ID:	3
Start time:	04:42:07
Start date:	04/06/2023
Path:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe
Imagebase:	0x460000
File size:	546816 bytes
MD5 hash:	81B7988B523FB109B834C76E7F0FEA10
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: 00000003.00000002.640270105.00000000050F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.640270105.00000000050F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.640270105.00000000050F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.640270105.00000000050F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.631138634.0000000002C41000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.635994119.0000000003C84000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.635994119.0000000003C84000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.635994119.0000000003C84000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.628751592.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.628751592.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.628751592.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.628751592.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.640443999.0000000005500000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.640443999.0000000005500000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.640443999.0000000005500000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.640443999.0000000005500000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.640443999.0000000005500000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
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	6C8760AC	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	6C8760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4EF0D15	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	4EF0E0F	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	4EF0D15	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	4EF0D15	CreateDirectoryW
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	6C8760AC	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	6C8760AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe:Zone.Identifier	success or wait	1	4EF10B5	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	43 fd 3a fd fd 64 fd 48	C:dH	success or wait	1	4EF0FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C8A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C8A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C8A8738	ReadFile
C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	unknown	4096	success or wait	1	6C94BF06	unknown
C:\Users\user\Desktop\HEUR-Trojan.MSIL.Taskun.gen-1617174ffdba50f5e.exe	unknown	512	success or wait	1	6C94BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C8A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C8A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4EF0FC7	ReadFile

Disassembly

No disassembly