ID: 612101
Sample Name:
xgnxoS8HWxonNHl.exe
Cookbook: default.jbs
Time: 15:13:32
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

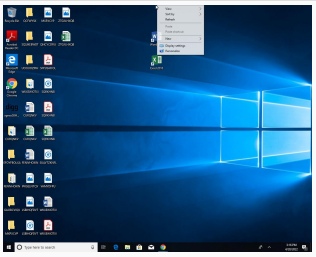
Windows Analysis Report

xgnxoS8HWxonNHl.exe

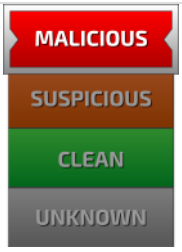
Overview

General Information

Sample Name:	xgnxoS8HWxonNHl.exe
Analysis ID:	612101
MD5:	56e4a7420f9a9fa.
SHA1:	31595356f12725..
SHA256:	12811d59e06901..
Tags:	agenttesla exe
Infos:	



Detection



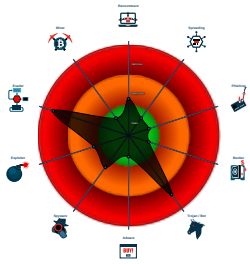
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains very larg…
- PE file has nameless sections
- Queries sensitive network adapter in…
- Contains functionality to check if a d…
- PE file contains section with specia…

Classification



Process Tree

- **System is w10x64**
- digg xgnxoS8HWxonNHl.exe (PID: 6420 cmdline: "C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe" MD5: 56E4A7420F9A9FA987ABA56B6F91FBCB)
  - digg xgnxoS8HWxonNHl.exe (PID: 6736 cmdline: C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe MD5: 56E4A7420F9A9FA987ABA56B6F91FBCB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "umut@ormretsan.com",
  "Password": "AGjluYt1",
  "Host": "smtp.ormretsan.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.410042576.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.410042576.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.417603219.00000000041EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.417603219.00000000041EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.409181519.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.xgnxoS8HWxonNHl.exe.422f518.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.xgnxoS8HWxonNHl.exe.422f518.9.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.xgnxoS8HWxonNHl.exe.422f518.9.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2edfe:$s1: get_kbok • 0x2f741:$s2: get_CHoo • 0x3037b:$s3: set_passwordIsSet • 0x2ec02:$s4: get_enableLog • 0x33276:$s8: torbrowser • 0x31c52:$s10: logins • 0x315ca:$s11: credential • 0x2e023:$g1: get_Clipboard • 0x2e031:$g2: get_Keyboard • 0x2e03e:$g3: get_Password • 0x2f5e0:$g4: get_CtrlKeyDown • 0x2f5f0:$g5: get_ShiftKeyDown • 0x2f601:$g6: get_AltKeyDown
3.2.xgnxoS8HWxonNHl.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.xgnxoS8HWxonNHl.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 28 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

System Summary

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations
- PE file has nameless sections
- PE file contains section with special chars

Malware Analysis System Evasion

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Stealing of Sensitive Information

Yara detected AgentTesla

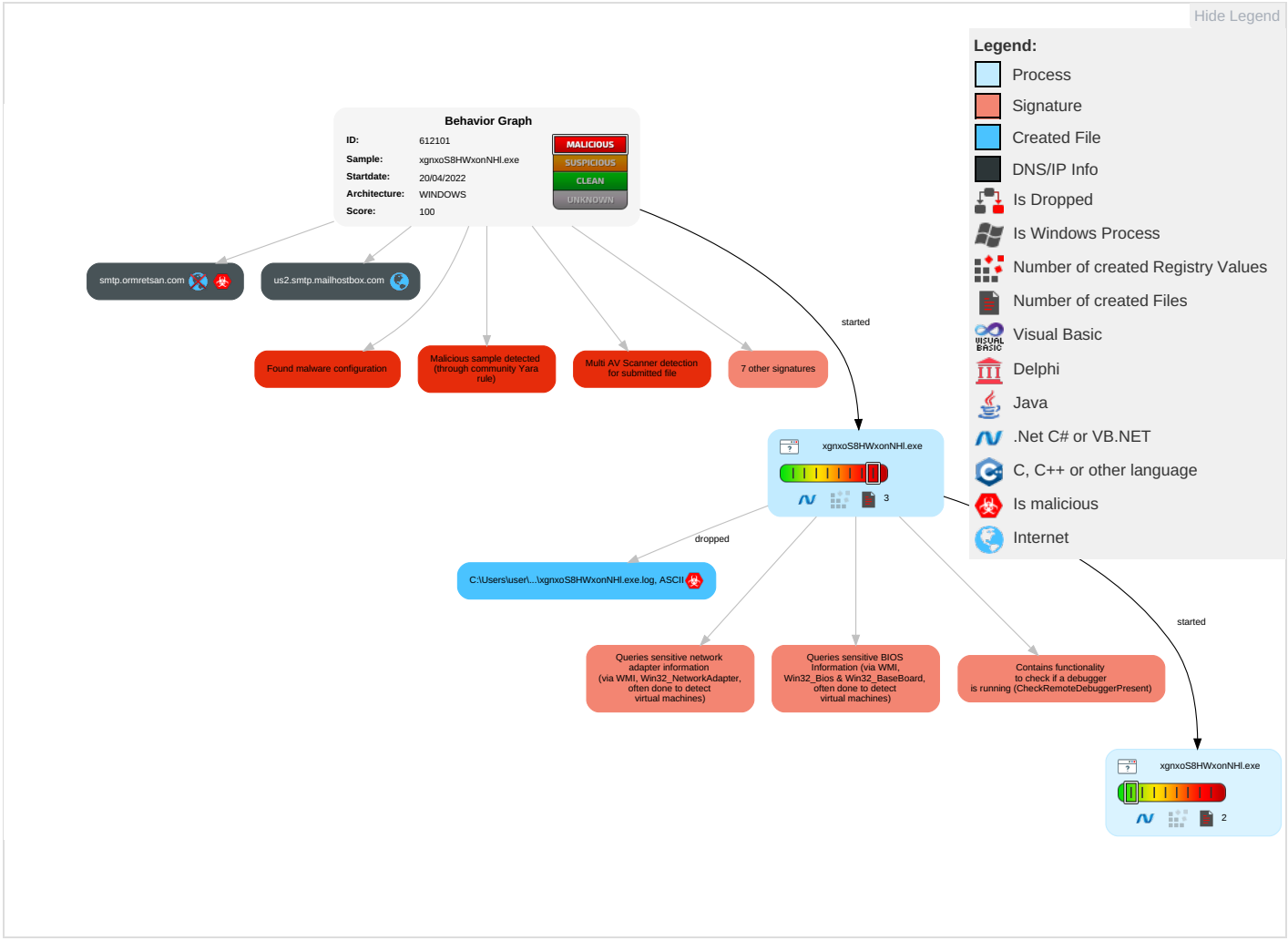
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	1 Input Capture	3 2 1 Security Software Discovery	Remote Services	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	4 Software Packing	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

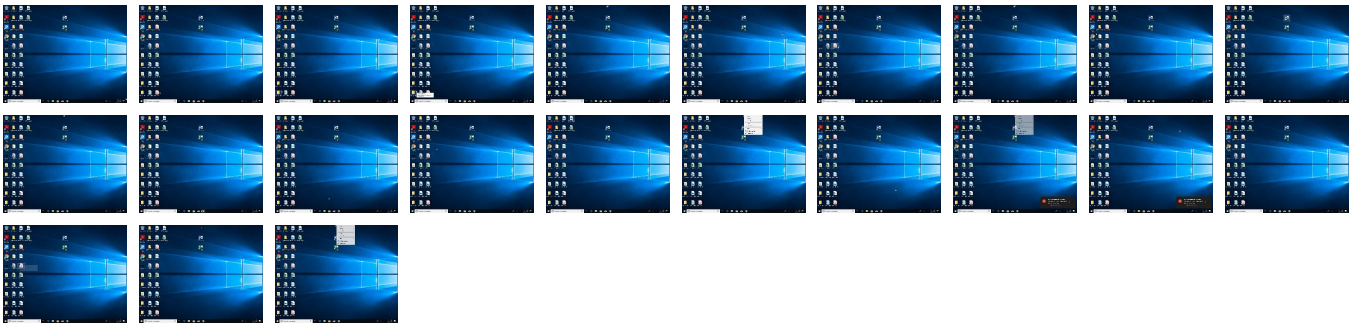
Behavior Graph



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
xgnxoS8HWxonNHl.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
xgnxoS8HWxonNHl.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.xgnxoS8HWxonNHl.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.xgnxoS8HWxonNHl.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.xgnxoS8HWxonNHl.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.xgnxoS8HWxonNHl.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.xgnxoS8HWxonNHl.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.xgnxoS8HWxonNHl.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comC	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnttp	0%	Avira URL Cloud	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.fontbureau.com4	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comX	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	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.comldTFM	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.fontbureau.comd~	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comz	0%	Avira URL Cloud	safe	
http://www.carterandcone.comily)	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comalsS?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cna	0%	URL Reputation	safe	
http://www.galapagosdesign.com/3	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comurs	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.comi)	0%	Avira URL Cloud	safe	
http://ATRZqY.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	162.222.225.16	true	false		high
smtp.ormretsan.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	xgnxoS8HWxonNHl.exe, 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersB	xgnxoS8HWxonNHl.exe, 00000000.00000003.376447774.0000000007AB8000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.375942088.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersY	xgnxoS8HWxonNHl.exe, 00000000.00000003.377813742.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.372072274.0000000007A84000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.372094133.0000000007A8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	xgnxoS8HWxonNHl.exe, 00000000.00000003.376637617.0000000007AB8000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.384487951.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.376696263.0000000007AB800.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.375942088.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comC	xgnxoS8HWxonNHl.exe, 00000000.00000003.368566801.0000000007A83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comasF	xgnxoS8HWxonNHl.exe, 00000000.00000003.376341670.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersP	xgnxoS8HWxonNHl.exe, 00000000.00000003.376447774.0000000007AB8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnttp	xgnxoS8HWxonNHl.exe, 00000000.00000003.371366282.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.368156883.0000000007A82000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.368566801.0000000007A8300.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	xgnxoS8HWxonNHl.exe, 00000000.00000003.379946625.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.379889262.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com4	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.377363480.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comX	xgnxoS8HWxonNHl.exe, 00000000.00000003.368566801.0000000007A83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersc	xgnxoS8HWxonNHl.exe, 00000000.00000003.384487951.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	xgnxoS8HWxonNHl.exe, 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fontbureau.com/designersv	xgnxoS8HWxonNHl.exe, 00000000.00000003.376069831.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	xgnxoS8HWxonNHl.exe, 00000000.00000003.373879871.0000000007ABB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comldTFM	xgnxoS8HWxonNHl.exe, 00000000.00000003.411742228.0000000007A80000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000002.419351318.0000000007A80000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	xgnxoS8HWxonNHl.exe, 00000000.00000002.417603219.00000000041EC000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000003.00000000.410042576.0000000000402000.00000040.00000400.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000003.00000000.407935315.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerss	xgnxoS8HWxonNHl.exe, 00000000.00000003.377813742.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	xgnxoS8HWxonNHl.exe, 00000000.00000003.379889262.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNS	xgnxoS8HWxonNHl.exe, 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcomd	xgnxoS8HWxonNHl.exe, 00000000.00000003.377363480.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	xgnxoS8HWxonNHl.exe, 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/i	xgnxoS8HWxonNHl.exe, 00000000.00000003.376341670.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comd~	xgnxoS8HWxonNHl.exe, 00000000.00000003.377363480.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.comz	xgnxoS8HWxonNHl.exe, 00000000.00000003.368156883.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comily)	xgnxoS8HWxonNHl.exe, 00000000.00000003.372641423.0000000007A8E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.coma	xgnxoS8HWxonNHl.exe, 00000000.00000003.411742228.0000000007A80000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000002.419351318.0000000007A80000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.372641423.0000000007A8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	xgnxoS8HWxonNHl.exe, 00000000.00000003.371988138.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalsS?	xgnxoS8HWxonNHl.exe, 00000000.00000003.378171280.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371387468.0000000007ABE000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371615251.0000000007ABD000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371351820.0000000007ABD000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371440220.0000000007ABD000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371503172.0000000007ABD000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.371366282.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cna	xgnxoS8HWxonNHl.exe, 00000000.00000003.372478173.0000000007A8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/3	xgnxoS8HWxonNHl.exe, 00000000.00000003.379889262.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	xgnxoS8HWxonNHl.exe, 00000000.00000003.377363480.0000000007A85000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers%	xgnxoS8HWxonNHl.exe, 00000000.00000003.376510155.0000000007AB8000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comurs	xgnxoS8HWxonNHl.exe, 00000000.00000003.368156883.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	xgnxoS8HWxonNHl.exe, 00000000.00000002.419789394.0000000008C92000.00000004.00000800.00020000.00000000.sdmp, xgnxoS8HWxonNHl.exe, 00000000.00000003.377016385.0000000007AB3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comi)	xgnxoS8HWxonNHl.exe, 00000000.00000003.373157693.0000000007A82000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ATRZqY.com	xgnxoS8HWxonNHl.exe, 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	612101
Start date and time: 20/04/202215:13:32	2022-04-20 15:13:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xgnxoS8HWxonNHl.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:	18
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@3/1@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.7%) • Quality average: 42.4% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, sls.update.microsoft.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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 NtOpenKeyEx calls found.
- VT rate limit hit for: xgnxoS8HWxonNHl.exe

Simulations

Behavior and APIs

Time	Type	Description
15:15:00	API Interceptor	516x Sleep call for process: xgnxoS8HWxonNHl.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_v4.0_32\UsageLogs\xgnxoS8HWxonNHl.exe.log

Process:	C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzu
MD5:	36C0A7F32E757FCBECED4EB6FC3C922C
SHA1:	939BED45186769E4D878B9A44420CE140445F2CB
SHA-256:	C85B76D06B14DE0D203F30A03BA1D26F17BA9970FE8491AB00A1ED1C0DEC9989
SHA-512:	F0C308E83AE3FB61E9A7AA68E2CA54D9D48027DF1E8D8092C1FA61600555005675063F377C50572C34A39E8CC77FC044EAF2BC31D5C08DC46446C38F4433DF1
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.923008451625047
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	xgnxoS8HWxonNHl.exe
File size:	707584
MD5:	56e4a7420f9a9fa987aba56b6f91fbcb
SHA1:	31595356f127256829e137be2c28ab6f4788e76e
SHA256:	12811d59e069011b7a1249365e515c8b63f21dd480cd955e2ec027aa2e3b80d8
SHA512:	db8da513d2de747f9e75294952e9c4087b0f5d3c0aa3dfc2735022f784a4205d2eacd78e15c192fda19c344d352bc7d3181fb5bc71dabcab898bcf77324d0824
SSDEEP:	12288:d1PHUMvd+OT+Aooafb45NmrNm2+oMFYlY2BUV3vIr9yhDS/PUn3It9DIi96KASyx:dBU2oAqk/hYR0/IIhDSk3o9R6KASe
TLSH:	42E4F19C326032EFC86BC076CEA86CB8EAA574BB971B57039417059DDE4D987CF150B2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._b.....0.....,..... ...@... ....@.. .....@.....@.....

File Icon

Icon Hash:	0000000000000000

Static PE Info

General

Entrypoint:	0x4b200a
Entrypoint Section:	
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:	0x625FC909 [Wed Apr 20 08:49:13 2022 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 [004B2000h]
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
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	0x14870	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0xf78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	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	0xb2000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x14000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
=hsS2-	0x2000	0x118e4	0x11a00	False	1.00042941046	data	7.99707331021	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x14000	0x99918	0x99a00	False	0.920395456164	data	7.91748293352	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xae000	0xf78	0x1000	False	0.5673828125	data	6.3429053765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xb2000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae130	0x8a5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xae9d8	0x14	data		
RT_VERSION	0xae9ec	0x39c	data		
RT_MANIFEST	0xaed88	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	Telemarketer
Assembly Version	0.0.6.0
InternalName	WindowsRuntimeBufferHel.exe
FileVersion	1.0.3.0
CompanyName	Telemarketer
LegalTrademarks	
Comments	
ProductName	Visual N-Queens Solver
ProductVersion	1.0.3.0
FileDescription	Visual N-Queens Solver
OriginalFilename	WindowsRuntimeBufferHel.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2022 15:16:58.594237089 CEST	56758	53	192.168.2.7	8.8.8.8
Apr 20, 2022 15:16:58.798269033 CEST	53	56758	8.8.8.8	192.168.2.7
Apr 20, 2022 15:16:58.803100109 CEST	62381	53	192.168.2.7	8.8.8.8
Apr 20, 2022 15:16:58.821592093 CEST	53	62381	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 20, 2022 15:16:58.594237089 CEST	192.168.2.7	8.8.8.8	0xe33	Standard query (0)	smtp.ormretsan.com	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.803100109 CEST	192.168.2.7	8.8.8.8	0xaf7f	Standard query (0)	smtp.ormretsan.com	A (IP address)	IN (0x0001)

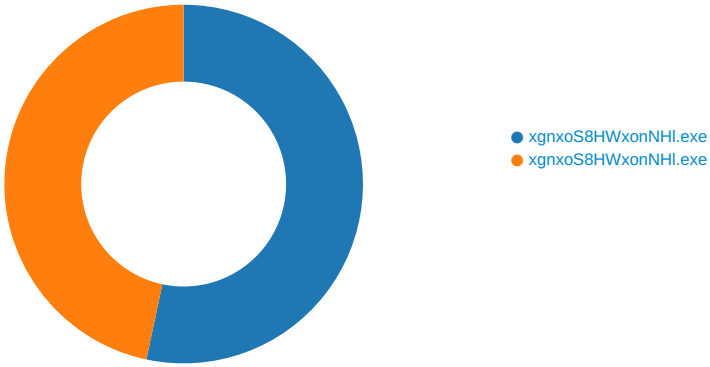
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 20, 2022 15:16:58.798269033 CEST	8.8.8.8	192.168.2.7	0xe33	No error (0)	smtp.ormretsan.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Apr 20, 2022 15:16:58.798269033 CEST	8.8.8.8	192.168.2.7	0xe33	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.798269033 CEST	8.8.8.8	192.168.2.7	0xe33	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.798269033 CEST	8.8.8.8	192.168.2.7	0xe33	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.798269033 CEST	8.8.8.8	192.168.2.7	0xe33	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.821592093 CEST	8.8.8.8	192.168.2.7	0xaf7f	No error (0)	smtp.ormretsan.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Apr 20, 2022 15:16:58.821592093 CEST	8.8.8.8	192.168.2.7	0xaf7f	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.821592093 CEST	8.8.8.8	192.168.2.7	0xaf7f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.821592093 CEST	8.8.8.8	192.168.2.7	0xaf7f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
Apr 20, 2022 15:16:58.821592093 CEST	8.8.8.8	192.168.2.7	0xaf7f	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: xgnxoS8HWxonNHl.exe PID: **6420**, Parent PID: **5740**

General

Target ID:	0
Start time:	15:14:48
Start date:	20/04/2022
Path:	C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe"
Imagebase:	0x270000
File size:	707584 bytes
MD5 hash:	56E4A7420F9A9FA987ABA56B6F91FBCB
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.417603219.00000000041EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.417603219.00000000041EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.413129137.00000000025A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDCCF06	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	6DDCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xgnxoS8HWxonNHl.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xgnxoS8HWxonNHl.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 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	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",02,"System.Windows.Forms, Vers	success or wait	1	6E0DC907	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	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Analysis Process: xgnxoS8HWxonNHl.exe PID: **6736**, Parent PID: **6420**

General

Target ID:	3
Start time:	15:15:08
Start date:	20/04/2022
Path:	C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\xgnxoS8HWxonNHl.exe
Imagebase:	0xa70000
File size:	707584 bytes
MD5 hash:	56E4A7420F9A9FA987ABA56B6F91FBCB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.410042576.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.410042576.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.409181519.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.409181519.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.407935315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.407935315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.408520132.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.408520132.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.627732273.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.627732273.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000003.00000002.629133048.0000000002E31000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6DDCCF06	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	6DDCCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Disassembly

No disassembly