ID: 626539
Sample Name: Raeue.exe
Cookbook: default.jbs
Time: 11:39:31
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

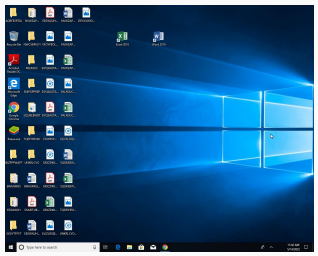
Windows Analysis Report

Raeue.exe

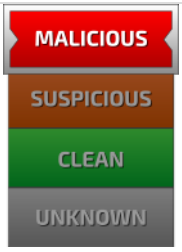
Overview

General Information

Sample Name:	Raeue.exe
Analysis ID:	626539
MD5:	47d09683fc102a..
SHA1:	f64cc824abd880...
SHA256:	848ce511daf904..
Tags:	agenttesla exe
Infos:	



Detection



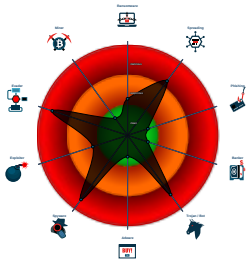
AgentTesla

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
- Sigma detected: MSBuild connects …
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- Raeue.exe (PID: 6964 cmdline: "C:\Users\user\Desktop\Raeue.exe" MD5: 47D09683FC102A85A7DEA2516CA81FA3)
  - cmd.exe (PID: 7028 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7076 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 7120 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7164 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 5812 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5260 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 5228 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6384 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 6436 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6476 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 2972 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 2948 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 4756 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 4592 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 4180 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6292 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 6944 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6632 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 6000 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7064 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 6796 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6296 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 4052 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- timeout.exe (PID: 6464 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 6484 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 5704 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 1532 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 3920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 4856 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 6584 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 6516 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 5756 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 6396 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 3036 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 7000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 6488 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 6576 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 1028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 7056 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 6472 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 6328 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- cmd.exe (PID: 6052 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 6356 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- MSBuild.exe (PID: 4788 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)

- Tyovqojh.exe (PID: 412 cmdline: "C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe" MD5: 47D09683FC102A85A7DEA2516CA81FA3)

- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@metalindus.cl",
  "Password": "metalindus_2019",
  "Host": "mail.metalindus.cl"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Raeue.exe	Typical_Malware_String_Transforms	Detects typical strings in a reversed or otherwise modified form	Florian Roth	• 0x44348:$i2: sserddAcorPteG • 0x44413:$i3: AyrarbiLdaoL

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe	Typical_Malware_String_Transforms	Detects typical strings in a reversed or otherwise modified form	Florian Roth	• 0x44348:$i2: sserddAcorPteG • 0x44413:$i3: AyrarbiLdaoL

Memory Dumps

Source	Rule	Description	Author	Strings
0000004F.00000002.479898674.0000000003A71000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000004F.00000002.479898674.0000000003A71000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000004C.00000000.368773514.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000004C.00000000.368773514.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.382727411.0000000003F92000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
79.0.Tyovqojh.exe.5b0000.0.unpack	Typical_Malware_String_Transforms	Detects typical strings in a reversed or otherwise modified form	Florian Roth	• 0x44348:$i2: sserddAcorPteG • 0x44413:$i3: AyrarbiLdaoL
0.2.Raeue.exe.910000.0.unpack	Typical_Malware_String_Transforms	Detects typical strings in a reversed or otherwise modified form	Florian Roth	• 0x44348:$i2: sserddAcorPteG • 0x44413:$i3: AyrarbiLdaoL
79.2.Tyovqojh.exe.5b0000.0.unpack	Typical_Malware_String_Transforms	Detects typical strings in a reversed or otherwise modified form	Florian Roth	• 0x44348:$i2: sserddAcorPteG • 0x44413:$i3: AyrarbiLdaoL
0.2.Raeue.exe.3f92930.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Raeue.exe.3f92930.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 29 entries				

Sigma Signatures

Networking

Sigma detected: MSBuild connects to smtp port

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

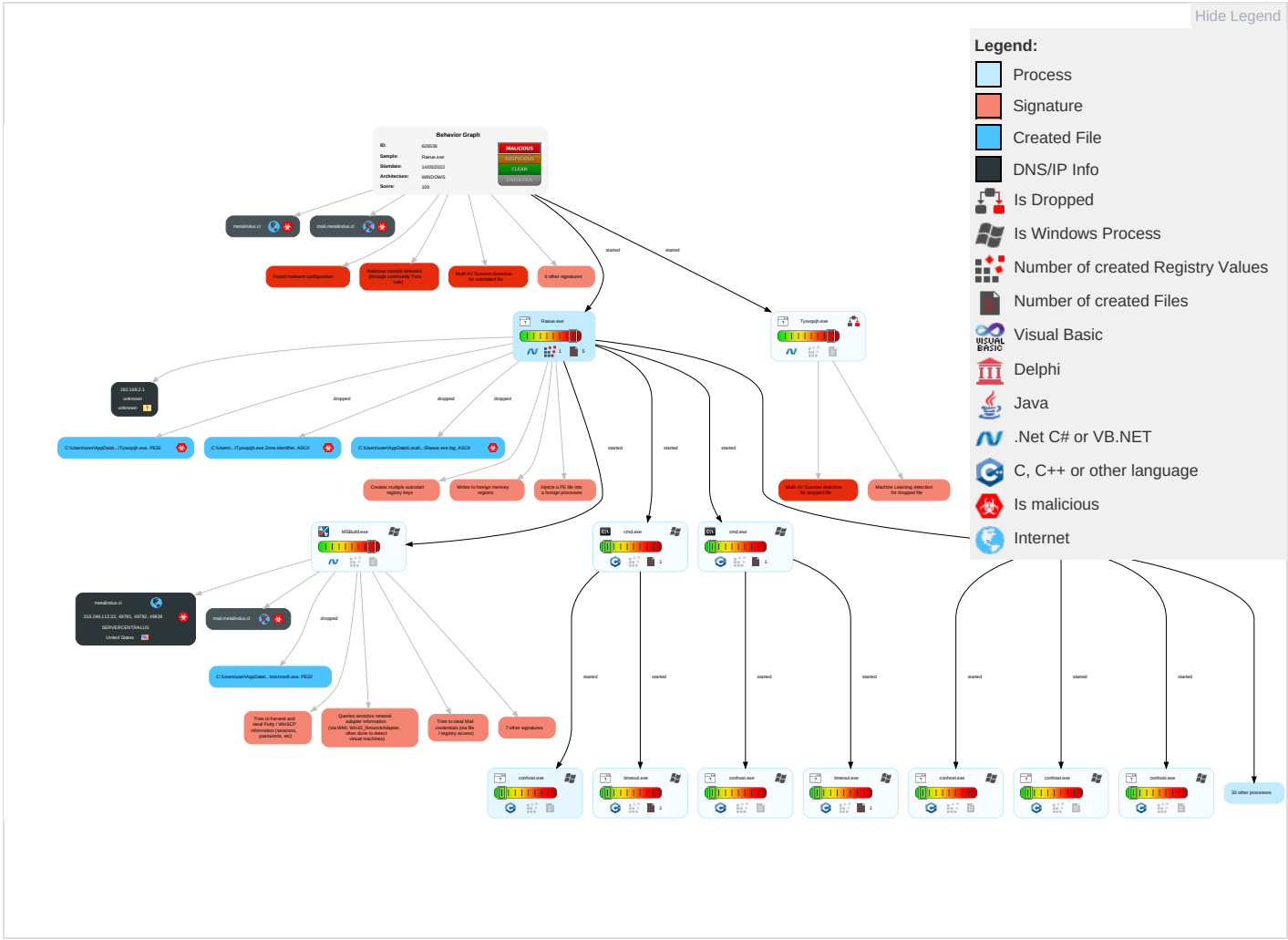
Yara detected AgentTesla

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	1 Scheduled Task/Job	2 1 2 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-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 3 Software Packing	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	2 Process Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	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 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	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 1 2 Process Injection	Proc Filesystem	1 Remote System Discovery	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 Hidden Files and Directories	/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

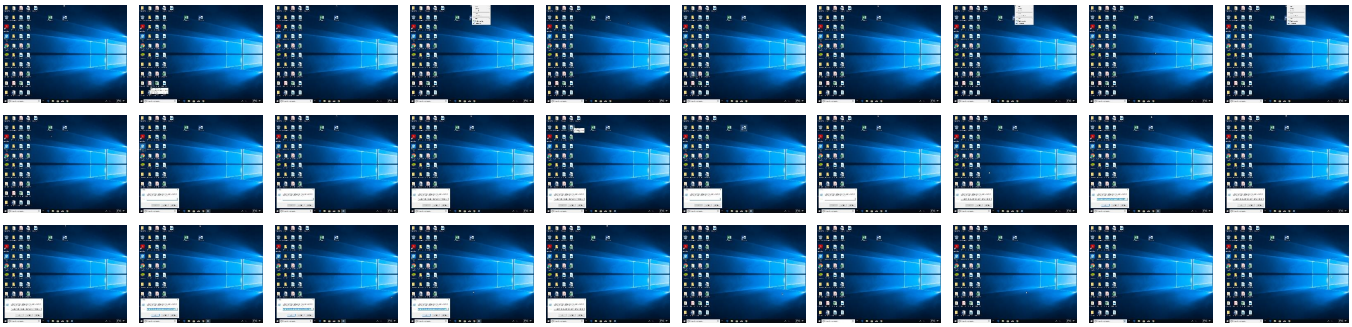
Behavior Graph



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
Raeue.exe	31%	Virustotal		Browse
Raeue.exe	34%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
Raeue.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe	34%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\Microsoft\microsoft.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\microsoft.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
76.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
79.2.Tyovqojh.exe.5b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
76.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.Raeue.exe.910000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
79.0.Tyovqojh.exe.5b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
76.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
76.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
76.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.Raeue.exe.910000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
76.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
metalindus.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://mail.metalindus.cl	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://pz3rRFNMLjA.org	0%	Avira URL Cloud	safe	
http://rfQUKE.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://crt.comodoca	0%	Avira URL Cloud	safe	
http://metalindus.cl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
metalindus.cl	216.246.112.22	true	true	• 0%, Virustotal, Browse	unknown
mail.metalindus.cl	unknown	unknown	true		unknown

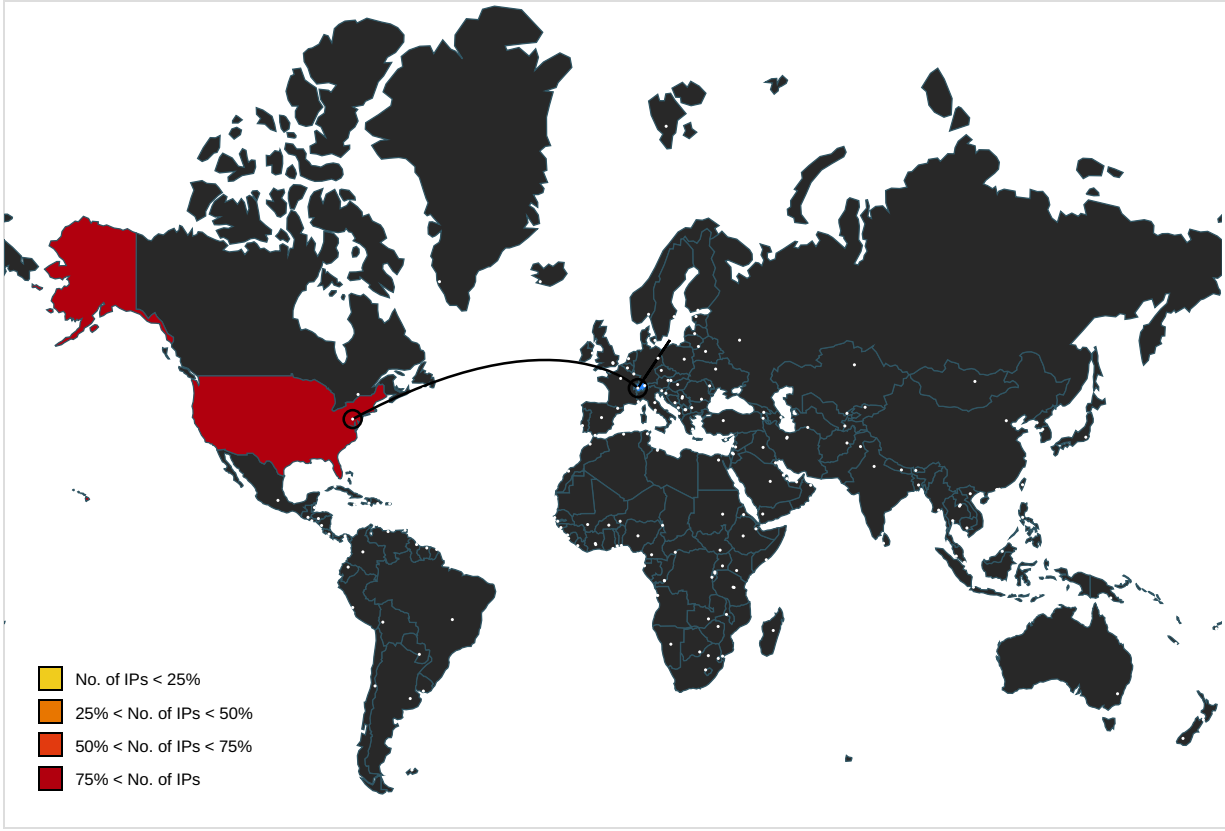
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://sectigo.com/CPS0	MSBuild.exe, 0000004C.00000002.468702711.0000000003281000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468588154.0000000003227000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000003.406287361.0000000006324000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.469905610.0000000006368000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.469702419.00000000062F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-neti	Raeue.exe, 00000000.00000002.383484734.0000000005D30000.00000004.08000000.00040000.00000000.sdmp, Raeue.exe, 00000000.00000003.364931995.0000000004047000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000003.364871019.0000000003FB3000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000002.396837651.0000000007E0C000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459692423.0000000003C53000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459793124.0000000003CE7000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.482201276.0000000007C5D000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/14436606/23354	Tyovqojh.exe, 0000004F.00000002.482201276.0000000007C5D000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481446949.00000000076C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-netJ	Raeue.exe, 00000000.00000002.383484734.0000000005D30000.00000004.08000000.00040000.00000000.sdmp, Raeue.exe, 00000000.00000003.364931995.0000000004047000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000003.364871019.0000000003FB3000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000002.396837651.0000000007E0C000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459692423.0000000003C53000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459793124.0000000003CE7000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.482201276.0000000007C5D000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp	false		high
http://mail.metalindus.cl	MSBuild.exe, 0000004C.00000002.468588154.0000000003227000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468687746.000000000326D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%appdata	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://stackoverflow.com/q/11564914/23354;	Raeue.exe, 00000000.00000002.383484734.0000000005D30000.00000004.08000000.00040000.00000000.sdmp, Raeue.exe, 00000000.00000003.364931995.0000000004047000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000003.364871019.0000000003FB3000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000002.396837651.0000000007E0C000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459692423.0000000003C53000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459793124.0000000003CE7000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.482201276.0000000007C5D000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/2152978/23354	Raeue.exe, 00000000.00000002.383484734.0000000005D30000.00000004.08000000.00040000.00000000.sdmp, Raeue.exe, 00000000.00000003.364931995.0000000004047000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000003.364871019.0000000003FB3000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459692423.0000000003C53000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459793124.0000000003CE7000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/mgravell/protobuf-net	Raeue.exe, 00000000.00000002.383484734.0000000005D30000.00000004.08000000.00040000.00000000.sdmp, Raeue.exe, 00000000.00000003.364931995.0000000004047000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000003.364871019.0000000003FB3000.00000004.00000800.00020000.00000000.sdmp, Raeue.exe, 00000000.00000002.396837651.0000000007E0C000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459692423.0000000003C53000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000003.459793124.0000000003CE7000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.482201276.000000007C5D000.00000004.00000800.00020000.00000000.sdmp, Tyovqojh.exe, 0000004F.00000002.481284902.0000000005B90000.00000004.08000000.00040000.00000000.sdmp	false		high
http://pz3rRFNMLjA.org	MSBuild.exe, 0000004C.00000002.468636703.0000000003253000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468627879.000000000324B000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468568665.0000000003221000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468409660.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://rfQUKE.com	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%	MSBuild.exe, 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crt.comodoca	MSBuild.exe, 0000004C.00000002.469702419.00000000062F0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://metalindus.cl	MSBuild.exe, 0000004C.00000002.468588154.0000000003227000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000004C.00000002.468687746.000000000326D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.246.112.22	metalindus.cl	United States		23352	SERVERCENTRALUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626539
Start date and time: 14/05/202211:39:31	2022-05-14 11:39:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Raeue.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:	80
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.spre.troj.spyw.evad.winEXE@124/6@8/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.2%) • Quality average: 45.4% • Quality standard deviation: 43.2%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.82.210.154, 23.211.6.115, 40.126.31.68, 20.190.159.70, 20.190.159.22, 40.126.31.64, 20.190.159.3, 20.190.159.74, 20.190.159.72, 40.126.31.70, 20.49.150.241, 23.211.4.86, 20.190.159.5, 20.190.159.1, 40.126.31.72, 20.199.120.182, 173.222.108.226, 173.222.108.210, 20.199.120.85, 20.199.120.151, 80.67.82.235, 80.67.82.211, 20.54.89.106, 40.125.122.176, 20.223.24.244, 40.112.88.60
- Excluded domains from analysis (whitelisted): www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, atm-settingsfe-prod-geo.trafficmanager.net, prod.fs.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ris-prod.trafficmanager.net, asf-ris-prod-neu.northeurope.cloudapp.azure.com, setti
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:41:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Tyovqojh "C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe"
11:41:33	API Interceptor	270x Sleep call for process: MSBuild.exe modified
11:41:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run microsoft C:\Users\user\AppData\Roaming\microsoft\microsoft.exe
11:41:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Tyovqojh "C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe"
11:41:58	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run microsoft C:\Users\user\AppData\Roaming\microsoft\microsoft.exe

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\Raeue.exe.log

Process:	C:\Users\user\Desktop\Raeue.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1213
Entropy (8bit):	5.346387745306316
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7QJE4jE4Kx1qE4FsXE4j:MxHKXwYHKhQnoPtHoxHhAHKzvQJHjHKh
MD5:	F4C7B39CFF5A2F242F694D97216F9E9C
SHA1:	3905274915EFA33D4BAC01AE14829AAA5C5C044C
SHA-256:	E300E29CDE7B77AADAD24A0157E5252EF754E842D21291AAE34D891E4DB15456
SHA-512:	D7BD11A51D5EB2FC93D252780559E010610AF4F2898D14565141CBBF12FBD52B76C9C61A255C2CC211AF0E216F6251BC0515FADB0A7DDB6329449625D80C1B B
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","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\8d67d92724ba49 4b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Security, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, Publ

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

Process:	C:\Users\user\AppData\Roaming\Iqbhgo\Tyovqojh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1121
Entropy (8bit):	5.353852130793033
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7QJE4jE4Kx1qE4j:MxHKXwYHKhQnoPtHoxHhAHKzvQJHjHKg
MD5:	91F948D29B57F0086ED4AB9F8447B315
SHA1:	632D82F2FC4181137657F593BB7850A9F01A3EF3
SHA-256:	8D5276512C4BC5AA67979A8CC3CB3441DD9B837CA821037D49ECBF03CAE1B983
SHA-512:	56D1FD69A3572E124DFB28E0C01A90920F7EE7993A975AE3716EEE9A800FE6A52F060770372078ADA64F810F2AC9B4FCF4F17663B8F67A9C601EC1FBB9AD616 A
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","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\8d67d92724ba49 4b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Security, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, Publ

C:\Users\user\AppData\Roaming\Iqbhgo\Tyovqojh.exe

Process:	C:\Users\user\Desktop\Raeue.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	778752
Entropy (8bit):	6.2529606578734045
Encrypted:	false
SSDEEP:	12288:Ro7VntzJOQX040txZp8sNx2HExIWtWrnngnnnKnanxNY:u104SgWtWrnngnnnKnanxN
MD5:	47D09683FC102A85A7DEA2516CA81FA3
SHA1:	F64CC824ABD8804458C3F31F06C16D0BEC9338DD
SHA-256:	848CE511DAF9046AB1AB3BED080D5C20BDEB3FD0BEBC016FC3AF70B892EBB5C9

SHA-512:	ECCFF33ADE27412BE147D7F792EC150F79F0FBA322CBF4A2BEFB46F615A71C578BD15C324C579FDBB9C377F221679CF4A04575C9F8F4814841346A244E80A2A6
Malicious:	**true**
Yara Hits:	• Rule: Typical_Malware_String_Transforms, Description: Detects typical strings in a reversed or otherwise modified form, Source: C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 34%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?.7.....0..r...n.....Z.... .....@.. .....@ .....@.....O.....\j..... ....H.....text...`q... ...r..... ..`.rsrc...\j.....l...t.....@..@.relo c..... .....@..B.....<.....H.....$..\.....5...Z.....6.s....(.....*".(.....*..0..6.....s.....i.+.....o.....%.Y.....-..o....(...+.+..*...0..u.....s... ....o.....s..... .....'....+.....o.....io....%.....-..o.....!.,..o.....,..o.....,..o.....*....(.....<Q.....M\.....`g.....0.....(....(.....+..*".(.....*...0..4.....(.....s....(....(.....o!...o". .....,...+...+..*.0..k.....s#.....(.....,R..($...o%..

C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Raeue.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Microsoft\microsoft.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z....."...0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z... ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z.....&..}.....*.*..... ...0..5.....(....-..*.-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(....*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....,*..(....-..}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

C:\Users\user\AppData\Roaming\gxhyyeyp.j44\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false

Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.2529606578734045
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Raeue.exe
File size:	778752
MD5:	47d09683fc102a85a7dea2516ca81fa3
SHA1:	f64cc824abd8804458c3f31f06c16d0bec9338dd
SHA256:	848ce511daf9046ab1ab3bed080d5c20bdeb3fd0bebc016fc3af70b892ebb5c9
SHA512:	eccff33ade27412be147d7f792ec150f79f0fba322cbf4a2befb46f615a71c578bd15c324c579fdbb9c377f221679cf4a04575c9f8f4814841346a244e80a2a6
SSDEEP:	12288:Ro7VntzJOQX040txZp8sNx2HExlWtWrnngnnnKnanxNY:u104SgWtWrnngnnnKnanxN
TLSH:	AFF46CA1E9534828C9245739BAB352B02DB9EC70C517E37267607EEBF037B20AD75172
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?.7.....0..r...n.....Z.... .....@.. .....@.....@.....

File Icon

Icon Hash:	71f094cef0f03082

Static PE Info

General

Entrypoint:	0x46915a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x9C37093F [Sat Jan 18 22:35:43 2053 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0x69108	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6a000	0x56a5c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x690ec	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x67160	0x67200	False	0.784997632576	data	7.52419685998	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	0x6a000	0x56a5c	0x56c00	False	0.0990662148775	data	4.07481812029	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6a180	0x42028	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xac1b8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xbc9f0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbefa8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc0060	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc04d8	0x4c	data		
RT_VERSION	0xc0534	0x328	data		
RT_MANIFEST	0xc086c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

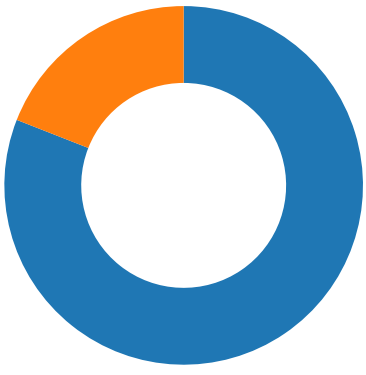
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.1
InternalName	Raeue.exe
FileVersion	0.0.0.1
CompanyName	
LegalTrademarks	
Comments	NeonDS public version
ProductName	NeonDS
ProductVersion	0.0.0.1
FileDescription	NeonDS public version
OriginalFilename	Raeue.exe

Network Behavior

Network Port Distribution



Total Packets: 42

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:40:27.247693062 CEST	49695	443	192.168.2.3	40.126.31.143
May 14, 2022 11:40:27.794401884 CEST	49698	443	192.168.2.3	40.126.31.143
May 14, 2022 11:40:27.967834949 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.967905045 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.967957020 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.967995882 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968034029 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968060017 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968075037 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968097925 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968111038 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.968125105 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.984200001 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984245062 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984272003 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984301090 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984329939 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984359026 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984390974 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984417915 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984447002 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984472990 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984534979 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984570980 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984596014 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984646082 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984677076 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984705925 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984734058 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984823942 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984852076 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984931946 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984941006 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.984965086 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.984993935 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985022068 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985050917 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985079050 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985157013 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985184908 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985253096 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985282898 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985307932 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985388041 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985418081 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985445976 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985471964 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985547066 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985598087 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985625982 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985676050 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985707045 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985754967 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985780001 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:27.985829115 CEST	443	49691	204.79.197.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:40:27.985856056 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985918045 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985946894 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.985977888 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986005068 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986085892 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986115932 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986145020 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986172915 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986202002 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986229897 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986275911 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:27.986355066 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:28.029622078 CEST	443	49691	204.79.197.200	192.168.2.3
May 14, 2022 11:40:28.029700994 CEST	49691	443	192.168.2.3	204.79.197.200
May 14, 2022 11:40:28.107018948 CEST	49706	443	192.168.2.3	40.126.31.143
May 14, 2022 11:40:38.360152960 CEST	49747	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.360208035 CEST	443	49747	40.126.31.4	192.168.2.3
May 14, 2022 11:40:38.360301018 CEST	49747	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.363143921 CEST	49747	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.363169909 CEST	443	49747	40.126.31.4	192.168.2.3
May 14, 2022 11:40:38.655924082 CEST	49748	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.655994892 CEST	443	49748	40.126.31.4	192.168.2.3
May 14, 2022 11:40:38.656083107 CEST	49748	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.656239986 CEST	49749	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.656315088 CEST	443	49749	40.126.31.4	192.168.2.3
May 14, 2022 11:40:38.656392097 CEST	49749	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.657080889 CEST	49748	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.657104969 CEST	443	49748	40.126.31.4	192.168.2.3
May 14, 2022 11:40:38.657260895 CEST	49749	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:38.657285929 CEST	443	49749	40.126.31.4	192.168.2.3
May 14, 2022 11:40:39.436511993 CEST	49750	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.436563015 CEST	443	49750	40.126.31.4	192.168.2.3
May 14, 2022 11:40:39.436676025 CEST	49750	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.436950922 CEST	49750	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.436970949 CEST	443	49750	40.126.31.4	192.168.2.3
May 14, 2022 11:40:39.938683033 CEST	49751	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.938752890 CEST	443	49751	40.126.31.4	192.168.2.3
May 14, 2022 11:40:39.938852072 CEST	49751	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.939223051 CEST	49751	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:39.939249992 CEST	443	49751	40.126.31.4	192.168.2.3
May 14, 2022 11:40:40.250390053 CEST	49752	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:40.250452995 CEST	443	49752	40.126.31.4	192.168.2.3
May 14, 2022 11:40:40.250607014 CEST	49752	443	192.168.2.3	40.126.31.4
May 14, 2022 11:40:40.250804901 CEST	49752	443	192.168.2.3	40.126.31.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:41:42.227566004 CEST	58625	53	192.168.2.3	8.8.8.8
May 14, 2022 11:41:42.456279039 CEST	53	58625	8.8.8.8	192.168.2.3
May 14, 2022 11:41:42.517323971 CEST	50778	53	192.168.2.3	8.8.8.8
May 14, 2022 11:41:42.762320995 CEST	53	50778	8.8.8.8	192.168.2.3
May 14, 2022 11:41:49.320611954 CEST	60640	53	192.168.2.3	8.8.8.8
May 14, 2022 11:41:49.557310104 CEST	53	60640	8.8.8.8	192.168.2.3
May 14, 2022 11:41:49.982928991 CEST	63861	53	192.168.2.3	8.8.8.8
May 14, 2022 11:41:50.223973036 CEST	53	63861	8.8.8.8	192.168.2.3
May 14, 2022 11:42:17.052181005 CEST	53524	53	192.168.2.3	8.8.8.8
May 14, 2022 11:42:17.299803019 CEST	53	53524	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:42:17.302987099 CEST	58561	53	192.168.2.3	8.8.8.8
May 14, 2022 11:42:17.530401945 CEST	53	58561	8.8.8.8	192.168.2.3
May 14, 2022 11:42:22.961636066 CEST	62547	53	192.168.2.3	8.8.8.8
May 14, 2022 11:42:22.980106115 CEST	53	62547	8.8.8.8	192.168.2.3
May 14, 2022 11:42:22.983575106 CEST	54096	53	192.168.2.3	8.8.8.8
May 14, 2022 11:42:23.002037048 CEST	53	54096	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 11:41:42.227566004 CEST	192.168.2.3	8.8.8.8	0xd123	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:41:42.517323971 CEST	192.168.2.3	8.8.8.8	0xfd5c	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:41:49.320611954 CEST	192.168.2.3	8.8.8.8	0x171e	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:41:49.982928991 CEST	192.168.2.3	8.8.8.8	0x662b	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:42:17.052181005 CEST	192.168.2.3	8.8.8.8	0x13a8	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:42:17.302987099 CEST	192.168.2.3	8.8.8.8	0xf696	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:42:22.961636066 CEST	192.168.2.3	8.8.8.8	0x5910	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)
May 14, 2022 11:42:22.983575106 CEST	192.168.2.3	8.8.8.8	0x884b	Standard query (0)	mail.metalindus.cl	A (IP address)	IN (0x0001)

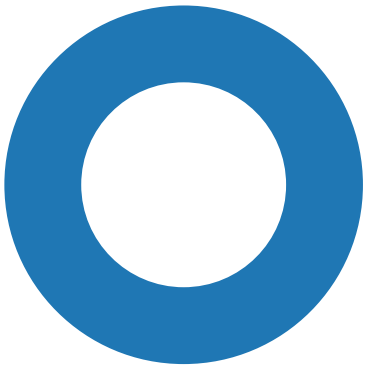
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:41:02.547914028 CEST	8.8.8.8	192.168.2.3	0xef27	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:14.825031042 CEST	8.8.8.8	192.168.2.3	0x1b33	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:42.456279039 CEST	8.8.8.8	192.168.2.3	0xd123	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:42.456279039 CEST	8.8.8.8	192.168.2.3	0xd123	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:41:42.762320995 CEST	8.8.8.8	192.168.2.3	0xfd5c	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:42.762320995 CEST	8.8.8.8	192.168.2.3	0xfd5c	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:41:49.557310104 CEST	8.8.8.8	192.168.2.3	0x171e	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:49.557310104 CEST	8.8.8.8	192.168.2.3	0x171e	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:41:50.223973036 CEST	8.8.8.8	192.168.2.3	0x662b	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:41:50.223973036 CEST	8.8.8.8	192.168.2.3	0x662b	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:42:17.299803019 CEST	8.8.8.8	192.168.2.3	0x13a8	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:42:17.299803019 CEST	8.8.8.8	192.168.2.3	0x13a8	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:42:17.530401945 CEST	8.8.8.8	192.168.2.3	0xf696	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:42:17.530401945 CEST	8.8.8.8	192.168.2.3	0xf696	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)
May 14, 2022 11:42:22.980106115 CEST	8.8.8.8	192.168.2.3	0x5910	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:42:22.980106115 CEST	8.8.8.8	192.168.2.3	0x5910	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:42:23.002037048 CEST	8.8.8.8	192.168.2.3	0x884b	No error (0)	mail.metalindus.cl	metalindus.cl		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:42:23.002037048 CEST	8.8.8.8	192.168.2.3	0x884b	No error (0)	metalindus.cl		216.246.112.22	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:41:43.189877987 CEST	587	49781	216.246.112.22	192.168.2.3	220-priva95.privatednsorg.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:41:42 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:41:43.217617989 CEST	49781	587	192.168.2.3	216.246.112.22	EHLO 124406
May 14, 2022 11:41:43.333342075 CEST	587	49781	216.246.112.22	192.168.2.3	250-priva95.privatednsorg.com Hello 124406 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 11:41:43.408979893 CEST	49781	587	192.168.2.3	216.246.112.22	STARTTLS
May 14, 2022 11:41:43.526446104 CEST	587	49781	216.246.112.22	192.168.2.3	220 TLS go ahead
May 14, 2022 11:41:50.566000938 CEST	587	49792	216.246.112.22	192.168.2.3	220-priva95.privatednsorg.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:41:49 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:41:50.566306114 CEST	49792	587	192.168.2.3	216.246.112.22	EHLO 124406
May 14, 2022 11:41:50.683195114 CEST	587	49792	216.246.112.22	192.168.2.3	250-priva95.privatednsorg.com Hello 124406 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 11:41:50.683720112 CEST	49792	587	192.168.2.3	216.246.112.22	STARTTLS
May 14, 2022 11:41:50.803344011 CEST	587	49792	216.246.112.22	192.168.2.3	220 TLS go ahead
May 14, 2022 11:42:17.888864040 CEST	587	49839	216.246.112.22	192.168.2.3	220-priva95.privatednsorg.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:42:17 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:42:17.889961958 CEST	49839	587	192.168.2.3	216.246.112.22	EHLO 124406
May 14, 2022 11:42:18.006761074 CEST	587	49839	216.246.112.22	192.168.2.3	250-priva95.privatednsorg.com Hello 124406 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 11:42:18.007395029 CEST	49839	587	192.168.2.3	216.246.112.22	STARTTLS
May 14, 2022 11:42:18.126185894 CEST	587	49839	216.246.112.22	192.168.2.3	220 TLS go ahead
May 14, 2022 11:42:23.251547098 CEST	587	49841	216.246.112.22	192.168.2.3	220-priva95.privatednsorg.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:42:22 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:42:23.251890898 CEST	49841	587	192.168.2.3	216.246.112.22	EHLO 124406
May 14, 2022 11:42:23.368700027 CEST	587	49841	216.246.112.22	192.168.2.3	250-priva95.privatednsorg.com Hello 124406 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 11:42:23.368897915 CEST	49841	587	192.168.2.3	216.246.112.22	STARTTLS
May 14, 2022 11:42:23.487533092 CEST	587	49841	216.246.112.22	192.168.2.3	220 TLS go ahead
May 14, 2022 11:42:27.053615093 CEST	587	49856	216.246.112.22	192.168.2.3	220-priva95.privatednsorg.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:42:26 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:42:27.054924011 CEST	49856	587	192.168.2.3	216.246.112.22	EHLO 124406



Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:42:27.212974072 CEST	587	49856	216.246.112.22	192.168.2.3	250-priva95.privatednsorg.com Hello 124406 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 11:42:27.213399887 CEST	49856	587	192.168.2.3	216.246.112.22	STARTTLS
May 14, 2022 11:42:27.373087883 CEST	587	49856	216.246.112.22	192.168.2.3	220 TLS go ahead

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Raeue.exe PID: 6964, Parent PID: 472

General

Target ID:	0
Start time:	11:40:33
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Raeue.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Raeue.exe"
Imagebase:	0x910000
File size:	778752 bytes
MD5 hash:	47D09683FC102A85A7DEA2516CA81FA3
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: 00000000.00000002.382727411.0000000003F92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.382727411.0000000003F92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.380956103.0000000003DD1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.380956103.0000000003DD1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Tyovqojh	unicode	"C:\Users\user\AppData\Roaming\Iqbhgo\Tyovqojh.exe"	success or wait	1	6CBD646A	RegSetValueExW

Analysis Process: cmd.exe PID: 7028, Parent PID: 6964

General

Target ID:	1
Start time:	11:40:34
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: **7044**, Parent PID: **7028**

General

Target ID:	2
Start time:	11:40:35
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: timeout.exe PID: **7076**, Parent PID: **7028**

General

Target ID:	3
Start time:	11:40:35
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: cmd.exe PID: **7120**, Parent PID: **6964**

General

Target ID:	4
Start time:	11:40:36
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 7128, Parent PID: 7120

General

Target ID:	5
Start time:	11:40:37
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: timeout.exe PID: 7164, Parent PID: 7120

General

Target ID:	6
Start time:	11:40:37
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: cmd.exe PID: 5812, Parent PID: 6964

General

Target ID:	7
Start time:	11:40:38
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1

Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 3896, Parent PID: 5812

General

Target ID:	9
Start time:	11:40:39
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: timeout.exe PID: 5260, Parent PID: 5812

General

Target ID:	10
Start time:	11:40:39
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: cmd.exe PID: 5228, Parent PID: 6964

General

Target ID:	12

Start time:	11:40:40
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: **6100**, Parent PID: **5228**

General

Target ID:	13
Start time:	11:40:40
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: timeout.exe PID: **6384**, Parent PID: **5228**

General

Target ID:	14
Start time:	11:40:41
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: cmd.exe PID: **6436**, Parent PID: **6964**

General	
Target ID:	16
Start time:	11:40:42
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **6448**, Parent PID: **6436**

General	
Target ID:	17
Start time:	11:40:42
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6476**, Parent PID: **6436**

General	
Target ID:	18
Start time:	11:40:43
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **2972**, Parent PID: **6964**

General

Target ID:	19
Start time:	11:40:44
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **3956**, Parent PID: **2972**

General

Target ID:	20
Start time:	11:40:44
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **2948**, Parent PID: **2972**

General

Target ID:	21
Start time:	11:40:45
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **4756**, Parent PID: **6964**

General

Target ID:	22
Start time:	11:40:46
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **6028**, Parent PID: **4756**

General

Target ID:	23
Start time:	11:40:46
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **4592**, Parent PID: **4756**

General

Target ID:	24
Start time:	11:40:47
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

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: cmd.exe PID: **4180**, Parent PID: **6964**

General	
Target ID:	25
Start time:	11:40:49
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **744**, Parent PID: **4180**

General	
Target ID:	26
Start time:	11:40:49
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6292**, Parent PID: **4180**

General	
Target ID:	27
Start time:	11:40:51
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **6944**, Parent PID: **6964**

General	
Target ID:	29
Start time:	11:40:52
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **6660**, Parent PID: **6944**

General	
Target ID:	30
Start time:	11:40:52
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6632**, Parent PID: **6944**

General	
Target ID:	31
Start time:	11:40:53
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0x7ff73c930000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **6000**, Parent PID: **6964**

General	
Target ID:	32
Start time:	11:40:54
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6556**, Parent PID: **6000**

General	
Target ID:	34
Start time:	11:40:54
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **7064**, Parent PID: **6000**

General	
Target ID:	36
Start time:	11:40:55
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **6796**, Parent PID: **6964**

General

Target ID:	38
Start time:	11:40:56
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6712**, Parent PID: **6796**

General

Target ID:	40
Start time:	11:40:56
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6296**, Parent PID: **6796**

General

Target ID:	41
Start time:	11:40:57
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **4052**, Parent PID: **6964**

General

Target ID:	44
Start time:	11:40:58
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **6372**, Parent PID: **4052**

General

Target ID:	45
Start time:	11:40:58
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6464**, Parent PID: **4052**

General

Target ID:	46
Start time:	11:40:59
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: cmd.exe PID: **6484**, Parent PID: **6964**

General

Target ID:	47
Start time:	11:41:00
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **6448**, Parent PID: **6484**

General

Target ID:	49
Start time:	11:41:00
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **5704**, Parent PID: **6484**

General

Target ID:	50
Start time:	11:41:01
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

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: cmd.exe PID: **1532**, Parent PID: **6964**

General	
Target ID:	51
Start time:	11:41:02
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3920**, Parent PID: **1532**

General	
Target ID:	52
Start time:	11:41:02
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **4856**, Parent PID: **1532**

General	
Target ID:	54
Start time:	11:41:03
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6584**, Parent PID: **6964**

General	
Target ID:	55
Start time:	11:41:04
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6248**, Parent PID: **6584**

General	
Target ID:	56
Start time:	11:41:04
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6516**, Parent PID: **6584**

General	
Target ID:	57
Start time:	11:41:05
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5756**, Parent PID: **6964**

General	
Target ID:	58
Start time:	11:41:06
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6128**, Parent PID: **5756**

General	
Target ID:	59
Start time:	11:41:07
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6396**, Parent PID: **5756**

General	
Target ID:	60
Start time:	11:41:08
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3036**, Parent PID: **6964**

General	
Target ID:	62
Start time:	11:41:10
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7000**, Parent PID: **3036**

General	
Target ID:	63
Start time:	11:41:10
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6488**, Parent PID: **3036**

General	
Target ID:	64
Start time:	11:41:11
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6576**, Parent PID: **6964**

General	
Target ID:	65
Start time:	11:41:12
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1028**, Parent PID: **6576**

General	
Target ID:	66
Start time:	11:41:12

Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **7056**, Parent PID: **6576**

General

Target ID:	67
Start time:	11:41:13
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6472**, Parent PID: **6964**

General

Target ID:	68
Start time:	11:41:14
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6604**, Parent PID: **6472**

General

Target ID:	69
Start time:	11:41:14
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6328**, Parent PID: **6472**

General

Target ID:	70
Start time:	11:41:15
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6052**, Parent PID: **6964**

General

Target ID:	71
Start time:	11:41:16
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6948**, Parent PID: **6052**

General

Target ID:	72
Start time:	11:41:16
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **6356**, Parent PID: **6052**

General

Target ID:	73

Start time:	11:41:17
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xbe0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MSBuild.exe PID: **4788**, Parent PID: **6964**

General

Target ID:	76
Start time:	11:41:29
Start date:	14/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0xb30000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 0000004C.00000000.368773514.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004C.00000000.368773514.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004C.00000000.368417395.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004C.00000000.368417395.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004C.00000000.367740613.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004C.00000000.367740613.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004C.00000000.368074941.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004C.00000000.368074941.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004C.00000002.464873991.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004C.00000002.464873991.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000004C.00000002.466512329.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: Tyovqojh.exe PID: **412**, Parent PID: **3968**

General

Target ID:	79
Start time:	11:41:40
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\Iqbhgo\Tyovqojh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Iqbhgo\Tyovqojh.exe"
Imagebase:	0x5b0000
File size:	778752 bytes
MD5 hash:	47D09683FC102A85A7DEA2516CA81FA3
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004F.00000002.479898674.0000000003A71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004F.00000002.479898674.0000000003A71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004F.00000002.480513797.0000000003C32000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004F.00000002.480513797.0000000003C32000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000004F.00000002.481850600.0000000007A0C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000004F.00000002.481850600.0000000007A0C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Typical_Malware_String_Transforms, Description: Detects typical strings in a reversed or otherwise modified form, Source: C:\Users\user\AppData\Roaming\lqbhgo\Tyovqojh.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 34%, ReversingLabs

Disassembly

No disassembly