ID: 828936
Sample Name: aOHLlvfakv.dll
Cookbook: default.jbs
Time: 17:36:40
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report aOHLlvfakv.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Threatname: Emotet 5
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
E-Banking Fraud 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 12
Public IPs 13
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 15
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 16
Static File Info 16
General 16
File Icon 16
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 18
Sections 18
Resources 19
Imports 19
Exports 19
Possible Origin 19
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 20
ICMP Packets 22
HTTP Request Dependency Graph 22
Statistics 22
Behavior 22

System Behavior 23
Analysis Process: loaddll64.exePID: 9132, Parent PID: 4808 23
General 23
File Activities 23
Analysis Process: conhost.exePID: 9020, Parent PID: 9132 23
General 23
File Activities 24
Analysis Process: cmd.exePID: 2940, Parent PID: 9132 24
General 24
File Activities 24
Analysis Process: regsvr32.exePID: 3112, Parent PID: 9132 24
General 24
File Activities 24
Analysis Process: rundll32.exePID: 4616, Parent PID: 2940 25
General 25
File Activities 25
File Deleted 25
Analysis Process: rundll32.exePID: 4588, Parent PID: 9132 25
General 25
File Activities 25
Analysis Process: regsvr32.exePID: 7556, Parent PID: 4616 26
General 26
File Activities 26
Analysis Process: regsvr32.exePID: 9004, Parent PID: 4588 26
General 26
File Activities 26
Analysis Process: regsvr32.exePID: 8668, Parent PID: 3112 26
General 26
File Activities 27
Analysis Process: rundll32.exePID: 3296, Parent PID: 9132 27
General 27
File Activities 27
Disassembly 27

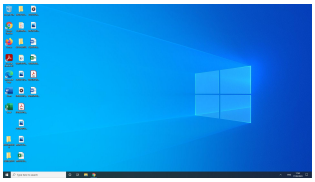
Windows Analysis Report

aOHLlvfakv.dll

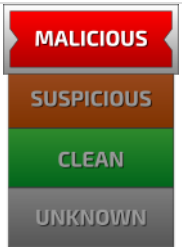
Overview

General Information

Sample Name:	aOHLlvfakv.dll
Analysis ID:	828936
MD5:	362f48619364e..
SHA1:	ae1423153935...
SHA256:	a873911592c3...
Infos:	



Detection



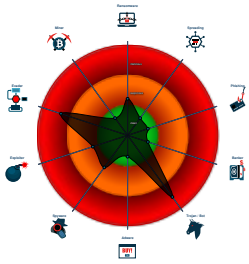
Emotet

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64native**
- loaddll64.exe (PID: 9132 cmdline: loaddll64.exe "C:\Users\user\Desktop\aOHLlvfakv.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 9020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - cmd.exe (PID: 2940 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\aOHLlvfakv.dll",#1 MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - rundll32.exe (PID: 4616 cmdline: rundll32.exe "C:\Users\user\Desktop\aOHLlvfakv.dll",#1 MD5: EF3179D498793BF4234F708D3BE28633)
      - regsvr32.exe (PID: 7556 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HRYKmulti\sEzrCiJYDniwfP.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
  - regsvr32.exe (PID: 3112 cmdline: regsvr32.exe /s C:\Users\user\Desktop\aOHLlvfakv.dll MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
    - regsvr32.exe (PID: 8668 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YDgQnzosNBGOURNE\pquwSRMRvDBcLA.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
  - rundll32.exe (PID: 4588 cmdline: rundll32.exe C:\Users\user\Desktop\aOHLlvfakv.dll,DllRegisterServer MD5: EF3179D498793BF4234F708D3BE28633)
    - regsvr32.exe (PID: 9004 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LwITFj\lcEQL.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
  - rundll32.exe (PID: 3296 cmdline: rundll32.exe C:\Users\user\Desktop\aOHLlvfakv.dll,__CPPdebugHook MD5: EF3179D498793BF4234F708D3BE28633)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Emotet	While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.	• GOLD CABIN • MUMMY SPIDER • Mealybug	http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.htmlhttps://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "91.121.146.47:8080",
    "66.228.32.31:7080",
    "182.162.143.56:443",
    "187.63.160.88:80",
    "167.172.199.165:8080",
    "164.90.222.65:443",
    "104.168.155.143:8080",
    "91.207.28.33:8080",
    "72.15.201.15:8080",
    "183.111.227.137:8080",
    "103.132.242.26:8080",
    "159.65.88.10:8080",
    "173.212.193.249:8080",
    "82.223.21.224:8080",
    "172.105.226.75:8080",
    "103.43.75.120:443",
    "167.172.253.162:8080",
    "1.234.2.232:8080",
    "159.89.202.34:443",
    "186.194.240.217:443",
    "185.4.135.165:8080",
    "139.59.126.41:443",
    "164.68.99.3:8080",
    "95.217.221.146:8080",
    "129.232.188.93:443",
    "45.176.232.124:443",
    "163.44.196.120:8080",
    "79.137.35.198:8080",
    "153.92.5.27:8080",
    "160.16.142.56:8080",
    "202.129.205.3:8080",
    "201.94.166.162:443",
    "119.59.103.152:8080",
    "153.126.146.25:7080",
    "188.44.20.25:443",
    "115.68.227.76:8080",
    "147.139.166.154:8080",
    "149.56.131.28:8080",
    "107.170.39.149:8080",
    "213.239.212.5:443",
    "197.242.150.244:8080",
    "206.189.28.199:8080",
    "5.135.159.50:443",
    "169.57.156.166:8080",
    "103.75.201.2:443",
    "110.232.117.186:8080",
    "94.23.45.86:4143",
    "45.235.8.30:8080",
    "101.50.0.91:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5LpP78wADAJA=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2VJJV8wAlAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.861337089.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.3286848282.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.860427801.0000000001370000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.858909413.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.860809198.0000025255CD0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.2410000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.25255cd0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1b91a160000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.1370000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.25255cd0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.11.20 - Destination IP: 91.121.146.47

Timestamp:	192.168.11.2091.121.146.474979380802404344 03/17/23-17:41:58.374772
SID:	2404344
Source Port:	49793
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.11.20 - Destination IP: 182.162.143.56

Timestamp:	192.168.11.20182.162.143.56497994432404312 03/17/23-17:42:13.021219
SID:	2404312
Source Port:	49799
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.11.20 - Destination IP: 167.172.199.165

Timestamp:	192.168.11.20167.172.199.1654980880802404308 03/17/23-17:42:27.268480
SID:	2404308
Source Port:	49808
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.11.20 - Destination IP: 164.90.222.65

Timestamp:	192.168.11.20164.90.222.65498104432404308 03/17/23-17:42:33.407520
SID:	2404308
Source Port:	49810
Destination Port:	443
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.11.20 - Destination IP: 104.168.155.143	
Timestamp:	192.168.11.20104.168.155.1434981180802404302 03/17/23-17:42:37.517558
SID:	2404302
Source Port:	49811
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.11.20 - Destination IP: 66.228.32.31	
Timestamp:	192.168.11.2066.228.32.314979570802404330 03/17/23-17:42:05.273202
SID:	2404330
Source Port:	49795
Destination Port:	7080
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

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

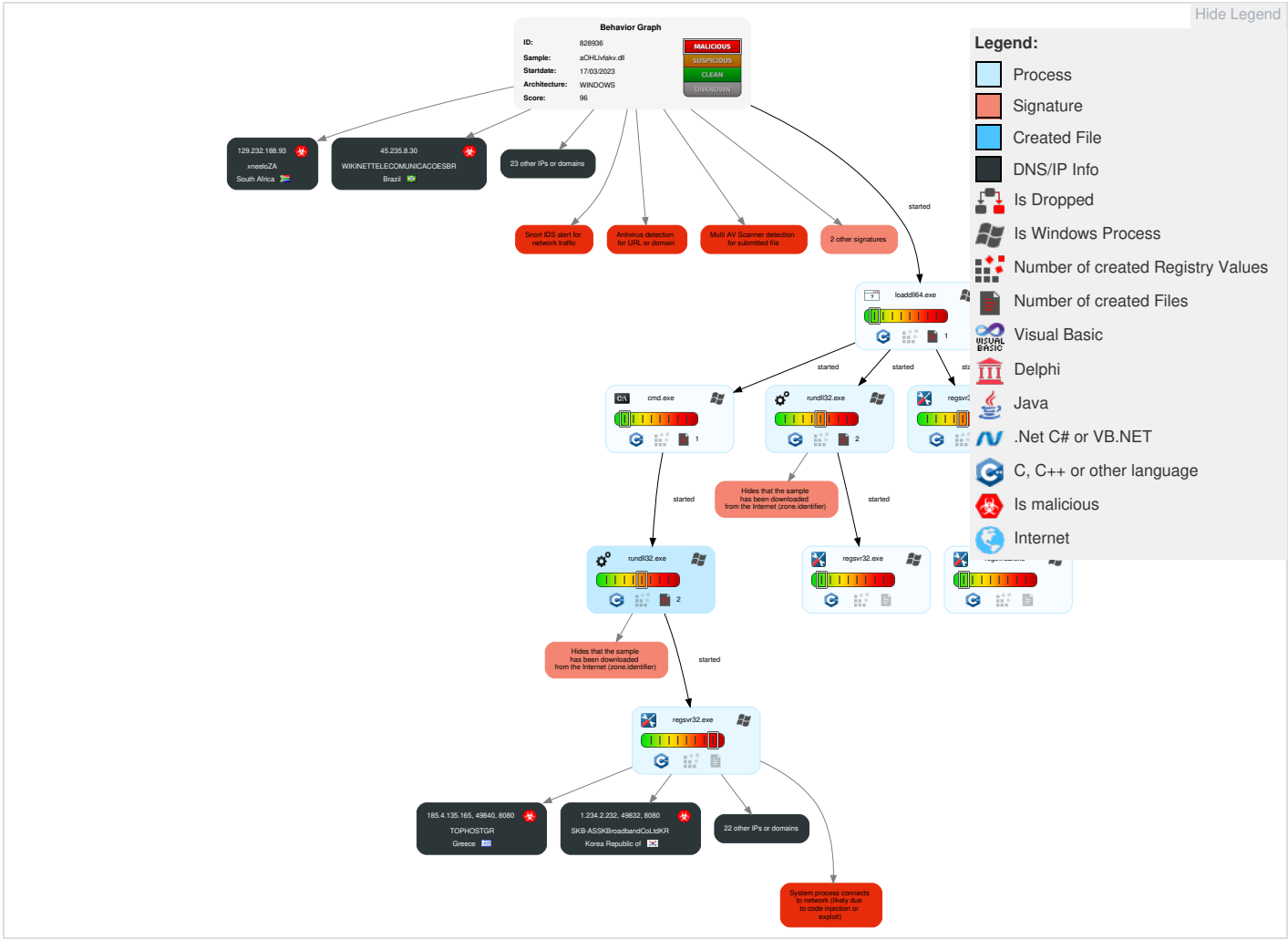
Yara detected Emotet

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 Virtualization/Sandbox Evasion	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	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	1 Rundll32	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 DLL Side-Loading	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

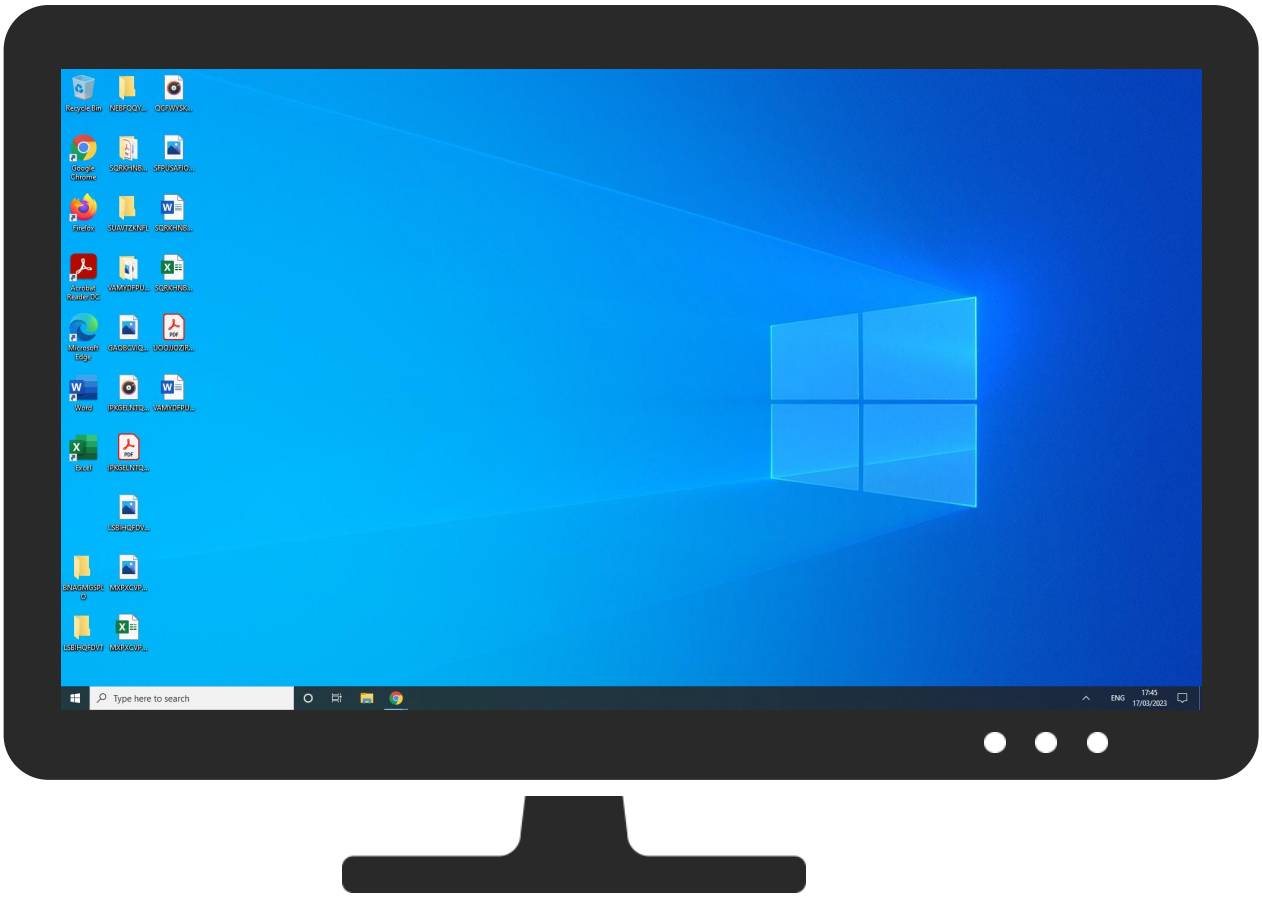
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
aOHLlvfakv.dll	54%	Virustotal		Browse
aOHLlvfakv.dll	28%	ReversingLabs	Win64.Trojan.Emotetcrypt	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://186.194.240.217:443/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/0	100%	Avira URL Cloud	malware	
http://https://139.59.126.41/0/	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/p	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/wW	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/	100%	Avira URL Cloud	malware	
http://https://95.217.221.146:8080/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://139.59.126.41/	100%	Avira URL Cloud	malware	
http://https://139.59.126.41/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/D	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/pescnrsqtrnp/icjmpjlu/d	100%	Avira URL Cloud	malware	
http://https://95.217.221.146:8080/pescnrsqtrnp/icjmpjlu//CW	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://139.59.126.41/jlu/_E	100%	Avira URL Cloud	malware	
http://https://95.217.221.146:8080/	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/L	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/#Ws	100%	Avira URL Cloud	malware	
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/	100%	Avira URL Cloud	malware	
http://https://186.194.240.217/3WC	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

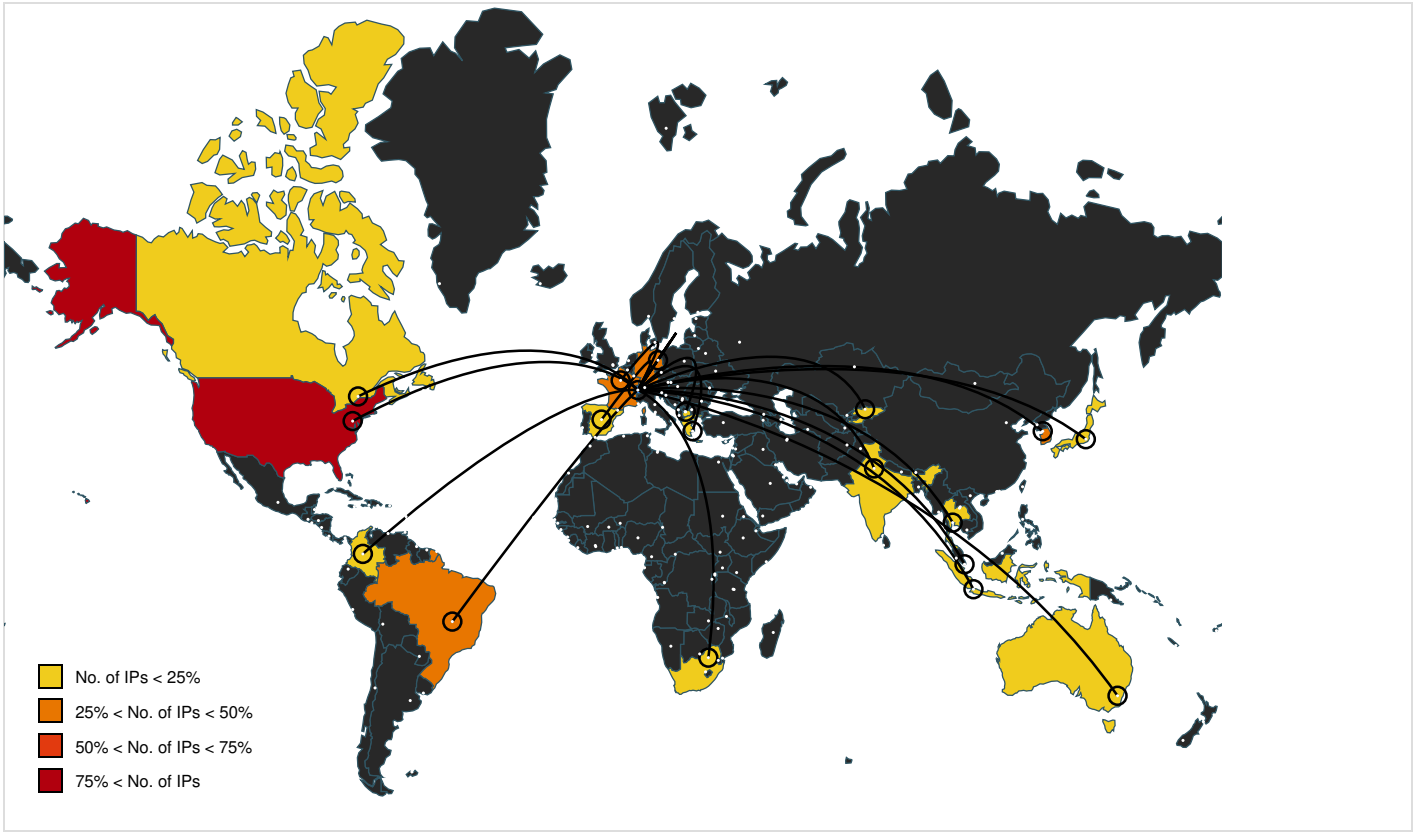
Name	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/pescnrsqtrnp/icjmpjlu/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/0	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A28000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/p	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://186.194.240.217:443/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000002.32829588 11.000000000098B000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://139.59.126.41/0/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://164.68.99.3:8080/wW	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://95.217.221.146:8080/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A28000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.3284094347.0000000000A6300 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/	regsvr32.exe, 00000007.00000003.15150801 00.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000003.15020201 56.0000000000A65000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.1515080100.0000000000A6300 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://139.59.126.41/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://139.59.126.41/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A19000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.68.99.3:8080/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/D	regsvr32.exe, 00000007.00000003.15019810 02.0000000002CF5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.3285581454.0000000002CF500 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://91.121.146.47:8080/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000003.12381127 14.0000000000A05000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.1514297126.0000000000A0500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1502020156.000 0000000A05000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000007.0 0000002.3282958811.000000000098B000.0000 0004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://91.121.146.47:8080/pescnrsqtrnp/icjmpjlu/d	regsvr32.exe, 00000007.00000002.32829588 11.000000000098B000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://95.217.221.146:8080/pescnrsqtrnp/icjmpjlu//CW	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://167.172.199.165:8080/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000003.15020201 56.0000000000A1A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://139.59.126.41/jlu/_E	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://95.217.221.146:8080/	regsvr32.exe, 00000007.00000002.32855814 54.0000000002C90000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/L	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A19000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/#Ws	regsvr32.exe, 00000007.00000003.15020201 56.0000000000A65000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.1515080100.0000000000A6300 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://164.68.99.3:8080/pescnrsqtrnp/icjmpjlu/	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://186.194.240.217/3WC	regsvr32.exe, 00000007.00000002.32840943 47.0000000000A63000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/	regsvr32.exe, 00000007.00000003.15142971 26.00000000009EC000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.1236480763.00000000009EC00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1502020156.000 00000009EC000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000007.0 0000002.3282958811.00000000009DB000.0000 0004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true
79.137.35.198	unknown	France		16276	OVHFR	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
66.228.32.31	unknown	United States		63949	LINODE-APLinodeLLCUS	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
101.50.0.91	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
91.121.146.47	unknown	France		16276	OVHFR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
187.63.160.88	unknown	Brazil		28169	BITCOMPROVEDORDESERVICOSDEINTERNETLTDABR	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
94.23.45.86	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828936
Start date and time:	2023-03-17 17:36:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	aOHLlvfakv.dll

Detection:	MAL
Classification:	mal96.troj.evad.winDLL@18/2@0/49
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.2% (good quality ratio 31%) • Quality average: 76.9% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.248.139.254, 8.248.135.254, 8.248.117.254, 8.253.204.249, 67.26.137.254
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:42:00	API Interceptor	24x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe

File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62582 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	**7.996063107774368**
Encrypted:	**true**
SSDEEP:	1536:Jk3XPi43VgGp0gB2itudTSRAn/TWTdWftu:CHa43V5p022iZ4CgA
MD5:	E71C8443AE0BC2E282C73FAEAD0A6DD3
SHA1:	0C110C1B01E68EDFACAEAE64781A37B1995FA94B
SHA-256:	95B0A5ACC5BF70D3ABDFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Preview:	MSCF....v.....,.....I.....BVrl .authroot.stl....oJ5..CK..8U....a..3.1.P. J.".t..2F2e.dHH.....$E.KB.2D..-SJE....^..'..y.}..,{m.....\...]4.G.....h....148...e.gr.....48:.L. ..g.....Xef.x:..t...J...6-....kW6Z>....&.....ye.U.Q&z:.vZ..._....a...]..T.E.....B.h.,...[....V.O.3..EW.x.?.Q..$.@.W..=.B.f..8a.Y.JK..g./%p..C.4CD.s..Jd.u..@.g=...a.. .h%..'.xjy7.E ..\.....A..':.4TdW?Ko3$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ.;....I&?.....F...p?... .p.....{S.L4..v.+...7.T?.....p..`..&..9.....f...0+.L.....1.2b)..vX5L'.~....2vz.,E.Ni.{#...o..w.?.#.3 ..h.v<.S%.].tD@!Le.w.q.7.8....QW.FT.....hE.....Y...../.%Q...k...*.Y.n..v.A..../...>B..5\..-Ko.....O<.b.K.{.O.b...._.7...4.;%9N..K.X>.....kg-9..r.c.g.G|.*[.-...HT...",?.q...ad. ...7RE.....!f..#../....?.-.^.K.c^...+{.g.....]<..$.=.O....ii7.wJ+S..Z..d.....>..J*...T..Q7..`.r,<$....\d:K`..T.n....N.....C..j.;.1SX..j....1...R....+....Yg....]....3..9..S..D..`.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1335351732898324
Encrypted:	false
SSDEEP:	6:kKNLry/7UN+SkQlPlEGYRMY9z+4KIDA3RUecZUt:9CvkPlE99SNxAhUext
MD5:	141ADD778B4D9D765C44061B65895A5C
SHA1:	B04B46DFF42488E393A9DC339242CFAEC02D4B4D
SHA-256:	F6E040EEB2079A3E39E26EA4B0C633250A3E0A756F2FC31F47FFF07852014F61
SHA-512:	74A62B27AA08D8A394883C1FE03CDC002D0FC00C8C09146E9C721EF9CE955B8F7ECF0ED108144B3AA2CDB31F0C85D6004FBC5959ACD43F73D4FBA025675056 57
Malicious:	false
Preview:	p..... .....#...X..(..... .....).K.....&.....v...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.2.f.9.2.9.a.7.4.b.d.9.1.:.0."...

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	0.018845395989010114
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 58.55% • InstallShield setup (43055/19) 24.71% • Windows Screen Saver (13104/52) 7.52% • Win64 Executable (generic) (12005/4) 6.89% • Generic Win/DOS Executable (2004/3) 1.15%
File name:	aOHLlvfakv.dll
File size:	571122142
MD5:	362f48619364efe57ecd00f83d1bca62
SHA1:	ae142315393512fe3f3e03dc07aed88428b6e29b
SHA256:	a873911592c3ce95d36e009f40bb376f587ad0ba6971a150a2ac10c87a2465f5
SHA512:	1ed6695b6bfdce048697963812deafcde28f7c4397af824fc6ffeda03c5ad282b52728620bb2b81a2caa782a8e91f1e888687aaf1727323d2c8365edf8c9a33a
SSDEEP:	
TLSH:	
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401300
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, DLL
DLL Characteristics:	
Time Stamp:	0x64078C02 [Tue Mar 7 19:09:54 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	c73bbc818ceb2fafea2b25df17dec187

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
dec eax
mov eax, ecx
mov dword ptr [00050D8Bh], edx
dec esp
mov dword ptr [00050D88h], eax
dec eax
mov dword ptr [00050D75h], eax
dec eax
cmp edx, 01h
jne 00007F6B510E3691h
call 00007F6B511191CFh
call 00007F6B51114D8Ah
call 00007F6B511191D5h
dec eax
lea eax, dword ptr [00050CC9h]
dec eax
lea ecx, dword ptr [00047372h]
dec eax
mov dword ptr [eax+30h], ecx
dec eax
lea ecx, dword ptr [FFFFFCB7h]
dec eax
mov dword ptr [eax], ecx
dec eax
lea ecx, dword ptr [FFFFFF59h]
dec eax
mov dword ptr [eax+08h], ecx
dec eax
lea ecx, dword ptr [FFFFFF4Eh]
dec eax
mov dword ptr [eax+10h], ecx
dec eax
lea ecx, dword ptr [FFFFFF8Bh]
dec eax
mov dword ptr [eax+18h], ecx

Instruction
dec eax
lea ecx, dword ptr [0004617Ch]
dec eax
mov dword ptr [eax+68h], ecx
dec eax
lea ecx, dword ptr [00046571h]
dec eax
mov dword ptr [eax+70h], ecx
dec eax
lea ecx, dword ptr [00046596h]
dec eax
mov dword ptr [eax+78h], ecx
dec eax
lea ecx, dword ptr [00046B3Bh]
dec eax
mov dword ptr [eax+00000080h], ecx
dec eax
lea ecx, dword ptr [0005D2EDh]
dec eax
mov dword ptr [eax+50h], ecx
mov dword ptr [eax+20h], 00000001h
dec eax
mov ecx, eax
dec eax
mov edx, dword ptr [00050CD8h]
inc esp
mov eax, dword ptr [00050CD9h]
dec esp
mov ecx, dword ptr [00050CD6h]
call 00007F6B510E373Ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x81000	0x69	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80000	0xb38	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x2be00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x76000	0x3a38	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0x11b4	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4c4c8	0x4c600	False	0.4390311732815057	data	6.348222298404593	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rodata	0x4e000	0x3600	0x3600	False	0.3231336805555556	data	5.09617814286108	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x52000	0x22de0	0xe400	False	0.17931058114035087	data	2.348309483365582	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x75000	0x5d0	0x600	False	0.013020833333333334	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x76000	0x3a38	0x3c00	False	0.4626953125	data	5.526910649754969	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xdata	0x7a000	0x5fd0	0x6000	False	0.14701334635416666	shared library	4.906149317469979	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x80000	0xb38	0xc00	False	0.2919921875	data	3.959226833867136	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.edata	0x81000	0x69	0x200	False	0.181640625	data	1.2134297058839834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x2be00	0x2be00	False	0.8775151353276354	data	7.859341694371929	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0x11b4	0x1200	False	0.6178385416666666	data	5.813939662419332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
VNRKGF	0x82184	0xa2c	data	English	United States
VNRKGF	0x82bb0	0x2b000	data	English	United States
RT_RCDATA	0xadbb0	0x10	data		
RT_RCDATA	0xadbc0	0x2	data	English	United States
RT_VERSION	0xadbc4	0x1f4	data	English	United States

Imports

DLL	Import
KERNEL32	AddVectoredExceptionHandler, CloseHandle, CreateDirectoryA, CreateFileA, CreateFileW, DeleteCriticalSection, DeleteFileA, EnterCriticalSection, ExitProcess, FreeEnvironmentStringsA, GetACP, GetCPInfo, GetCurrentProcessId, GetCurrentThreadId, GetDateFormatA, GetEnvironmentStrings, GetFileAttributesA, GetFileAttributesW, GetFileSize, GetFileType, GetLastError, GetLocalTime, GetLocaleInfoA, GetModuleFileNameA, GetModuleHandleA, GetOEMCP, GetProcAddress, GetProcessHeap, GetStartupInfoA, GetStdHandle, GetStringTypeA, GetStringTypeW, GetSystemDefaultLangID, GetSystemInfo, GetTickCount, GetTimeZoneInformation, GetUserDefaultLCID, GetVersion, GetVersionExA, HeapAlloc, HeapFree, InitializeCriticalSection, InitializeCriticalSectionAndSpinCount, IsDBCSLeadByteEx, IsDebuggerPresent, IsValidLocale, LCMapStringA, LeaveCriticalSection, LoadLibraryA, LoadLibraryW, LocalFileTimeToFileTime, MultiByteToWideChar, RaiseException, ReadFile, RemoveDirectoryA, RemoveVectoredExceptionHandler, RtlCaptureContext, SetConsoleCtrlHandler, SetEndOfFile, SetFilePointer, SetFileTime, SetHandleCount, SetLastError, SetThreadLocale, Sleep, SleepEx, SystemTimeToFileTime, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, VirtualAlloc, VirtualFree, VirtualQuery, WideCharToMultiByte, WriteFile, RtlRestoreContext, RtlUnwindEx
USER32	EnumThreadWindows, MessageBoxA, wsprintfA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x401da0
__CPPdebugHook	2	0x474aa0

Possible Origin

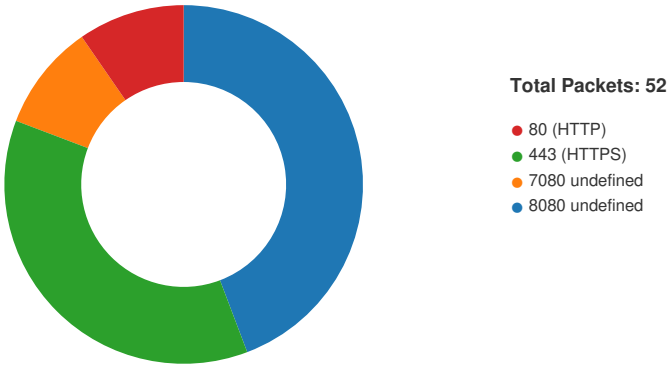
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2091.121.146.47497938080240434403/17/23-17:41:58.374772	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49793	8080	192.168.11.20	91.121.146.47
192.168.11.20182.162.143.56497994432404312 03/17/23-17:42:13.021219	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49799	443	192.168.11.20	182.162.143.56
192.168.11.20167.172.199.165498080880802404308 03/17/23-17:42:27.268480	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49808	8080	192.168.11.20	167.172.199.165
192.168.11.20164.90.222.65498104432404308 03/17/23-17:42:33.407520	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49810	443	192.168.11.20	164.90.222.65
192.168.11.20104.168.155.143498118080240430203/17/23-17:42:37.517558	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49811	8080	192.168.11.20	104.168.155.143
192.168.11.2066.228.32.314979570802404330 03/17/23-17:42:05.273202	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49795	7080	192.168.11.20	66.228.32.31

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:41:58.374772072 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:58.394654989 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:41:58.394908905 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:58.396826982 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:58.416774988 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:41:58.438533068 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:41:58.438611031 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:41:58.438812971 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:58.441060066 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:58.461968899 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:41:58.506763935 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:59.256028891 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:59.256028891 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:41:59.276854038 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:42:01.236709118 CET	8080	49793	91.121.146.47	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:42:01.287337065 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:42:04.236349106 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:42:04.236385107 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:42:04.236536980 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:42:04.236789942 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:42:04.236789942 CET	49793	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:42:04.256392956 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:42:04.256506920 CET	8080	49793	91.121.146.47	192.168.11.20
Mar 17, 2023 17:42:05.273201942 CET	49795	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:42:05.365420103 CET	7080	49795	66.228.32.31	192.168.11.20
Mar 17, 2023 17:42:05.880079031 CET	49795	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:42:05.972516060 CET	7080	49795	66.228.32.31	192.168.11.20
Mar 17, 2023 17:42:06.473604918 CET	49795	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:42:06.565701962 CET	7080	49795	66.228.32.31	192.168.11.20
Mar 17, 2023 17:42:07.067228079 CET	49795	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:42:07.159077883 CET	7080	49795	66.228.32.31	192.168.11.20
Mar 17, 2023 17:42:07.660923004 CET	49795	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:42:07.753176928 CET	7080	49795	66.228.32.31	192.168.11.20
Mar 17, 2023 17:42:13.021219015 CET	49799	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.021243095 CET	443	49799	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.021507025 CET	49799	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.021766901 CET	49799	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.021780014 CET	443	49799	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.262397051 CET	443	49799	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.263051987 CET	49800	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.263098955 CET	443	49800	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.263350010 CET	49800	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.263613939 CET	49800	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.263655901 CET	443	49800	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.506201982 CET	443	49800	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.506864071 CET	49801	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.506884098 CET	443	49801	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.507070065 CET	49801	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.507759094 CET	49801	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:13.507816076 CET	443	49801	182.162.143.56	192.168.11.20
Mar 17, 2023 17:42:13.508106947 CET	49801	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:42:18.770060062 CET	49802	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:42:18.991063118 CET	80	49802	187.63.160.88	192.168.11.20
Mar 17, 2023 17:42:19.501975060 CET	49802	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:42:19.722867966 CET	80	49802	187.63.160.88	192.168.11.20
Mar 17, 2023 17:42:20.236145973 CET	49802	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:42:20.457137108 CET	80	49802	187.63.160.88	192.168.11.20
Mar 17, 2023 17:42:20.970432043 CET	49802	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:42:21.191561937 CET	80	49802	187.63.160.88	192.168.11.20
Mar 17, 2023 17:42:21.704818010 CET	49802	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:42:21.925785065 CET	80	49802	187.63.160.88	192.168.11.20
Mar 17, 2023 17:42:27.268480062 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:27.428508043 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:27.428760052 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:27.429096937 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:27.588521957 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:27.598985910 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:27.599060059 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:27.599360943 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:27.602097034 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:27.762232065 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:27.812634945 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:28.055224895 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:28.255151033 CET	8080	49808	167.172.199.165	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:42:28.880906105 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:28.921806097 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:31.878376961 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:31.878443956 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:31.878724098 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:31.878724098 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:31.878724098 CET	49808	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:42:32.038175106 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:32.038233042 CET	8080	49808	167.172.199.165	192.168.11.20
Mar 17, 2023 17:42:33.266638041 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.266664028 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.266859055 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.267117977 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.267132044 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.404678106 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.404896021 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.406138897 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.406156063 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.406534910 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.407407999 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.448353052 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.604700089 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.604796886 CET	443	49810	164.90.222.65	192.168.11.20
Mar 17, 2023 17:42:33.605035067 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.606838942 CET	49810	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:42:33.606838942 CET	49810	443	192.168.11.20	164.90.222.65

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 17, 2023 17:43:28.805680990 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable
Mar 17, 2023 17:43:29.806631088 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable
Mar 17, 2023 17:43:31.821768999 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable
Mar 17, 2023 17:43:35.836711884 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable

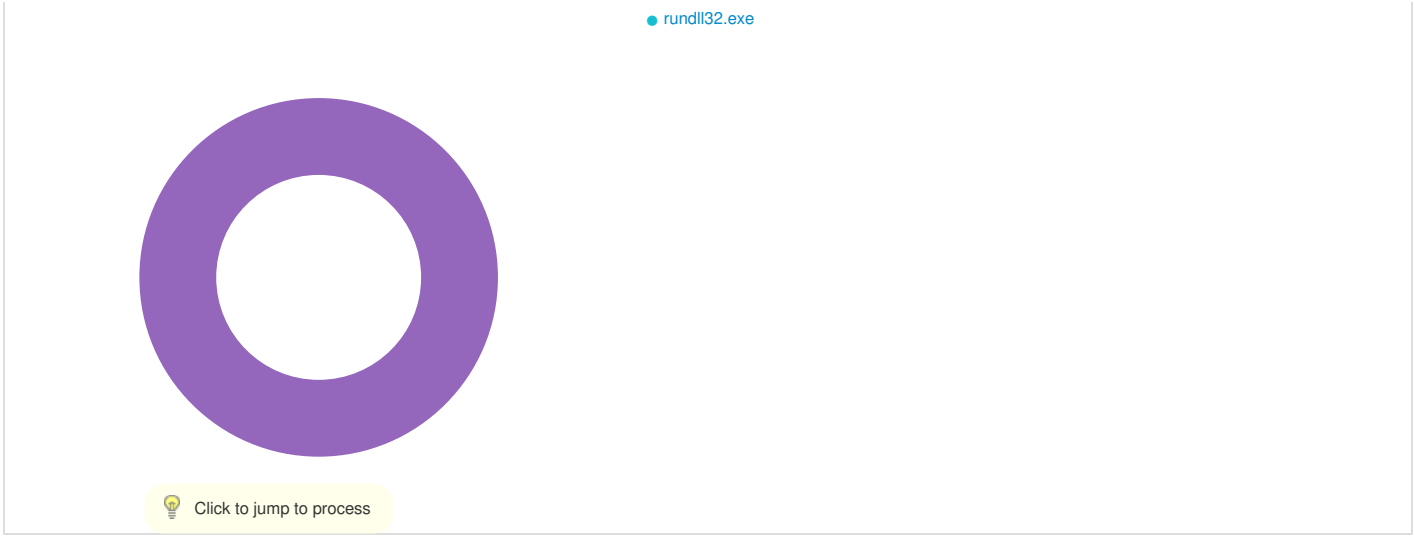
HTTP Request Dependency Graph

- 164.90.222.65

Statistics

Behavior

- loaddll64.exe
- conhost.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe



System Behavior

Analysis Process: loaddll64.exe PID: 9132, Parent PID: 4808

General

Target ID:	0
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\aOHLIvfakv.dll"
Imagebase:	0x7ff7a5a40000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: 9020, Parent PID: 9132

General

Target ID:	1
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76e060000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2940**, Parent PID: **9132**

General

Target ID:	2
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\aOHLlvfakv.dll",#1
Imagebase:	0x7ff785600000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: regsvr32.exe PID: **3112**, Parent PID: **9132**

General

Target ID:	3
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\aOHLlvfakv.dll
Imagebase:	0x7ff62d2c0000
File size:	25088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.861337089.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.860427801.0000000001370000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4616**, Parent PID: **2940**

General

Target ID:	4
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\aOHLlvfakv.dll",#1
Imagebase:	0x7ff6a2320000
File size:	71680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.858695133.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.860577207.000001B91A160000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\HRYKmuIti\sEzrCiJYDniwfP.dll:Zone.Identifier	success or wait	1	18000289D	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4588**, Parent PID: **9132**

General

Target ID:	5
Start time:	17:41:20
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\aOHLlvfakv.dll,DllRegisterServer
Imagebase:	0x7ff6a2320000
File size:	71680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.858909413.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.860809198.0000025255CD0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **7556**, Parent PID: **4616**

General

Target ID:	7
Start time:	17:41:22
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HRYKmuIti\sEzrCiJYDniwfP.dll"
Imagebase:	0x7ff62d2c0000
File size:	25088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.3286848282.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000007.00000002.3282958811.000000000098B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.3285052145.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **9004**, Parent PID: **4588**

General

Target ID:	8
Start time:	17:41:22
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LwITFj\lcEQL.dll"
Imagebase:	0x7ff62d2c0000
File size:	25088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **8668**, Parent PID: **3112**

General

Target ID:	9
Start time:	17:41:22
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YDgQnzosNBGOURNE\pquwSRMRvDBcLA.dll"
Imagebase:	0x7ff62d2c0000
File size:	25088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3296**, Parent PID: **9132**

General

Target ID:	10
Start time:	17:41:23
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\aOHLlvfakv.dll,__CPPdebugHook
Imagebase:	0x7ff6a2320000
File size:	71680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly