

JoeSandbox Cloud BASIC



ID: 828936

Sample Name: aOHLlvfakv.dll

Cookbook: default.jbs

Time: 17:52:24

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	13
Public IPs	14
General Information	15
Warnings	16
Simulations	16
Behavior and APIs	16
Joe Sandbox View / Context	16
IPs	16
Domains	16
ASNs	16
JA3 Fingerprints	16
Dropped Files	16
Created / dropped Files	16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	17
Static File Info	17
General	17
File Icon	17
Static PE Info	17
General	18
Entrypoint Preview	18
Data Directories	19
Sections	19
Resources	20
Imports	20
Exports	20
Possible Origin	20
Network Behavior	21
Snort IDS Alerts	21
Network Port Distribution	21
TCP Packets	21
ICMP Packets	23
HTTP Request Dependency Graph	23
Statistics	23
Behavior	23

System Behavior	24
Analysis Process: loadll64.exePID: 8532, Parent PID: 4660	24
General	24
File Activities	24
Analysis Process: conhost.exePID: 8560, Parent PID: 8532	24
General	24
File Activities	25
Analysis Process: cmd.exePID: 8704, Parent PID: 8532	25
General	25
File Activities	25
Analysis Process: regsvr32.exePID: 8688, Parent PID: 8532	25
General	25
File Activities	25
Analysis Process: rundll32.exePID: 7436, Parent PID: 8704	26
General	26
File Activities	26
File Deleted	26
Analysis Process: rundll32.exePID: 7448, Parent PID: 8532	26
General	26
File Activities	26
Analysis Process: regsvr32.exePID: 8788, Parent PID: 7436	27
General	27
File Activities	27
Analysis Process: regsvr32.exePID: 7460, Parent PID: 7448	27
General	27
File Activities	27
Analysis Process: regsvr32.exePID: 7592, Parent PID: 8688	27
General	27
File Activities	28
Analysis Process: rundll32.exePID: 372, Parent PID: 8532	28
General	28
File Activities	28
Disassembly	28

Windows Analysis Report

aOHLlvfakv.dll

Overview

General Information

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

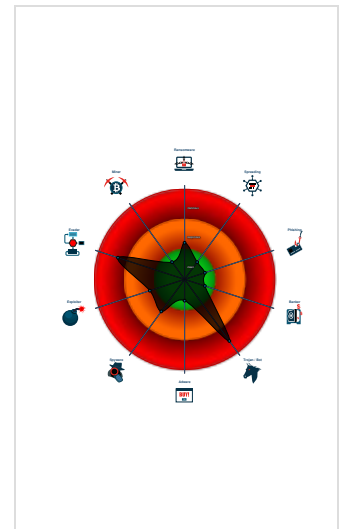
Detection

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

Signatures

Multi AV Scanner detection for subm...
Yara detected Emotet
System process connects to network...
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
loadll64.exe (PID: 8532 cmdline: loadll64.exe "C:\Users\user\Desktop\laOHLlvfakv.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
conhost.exe (PID: 8560 cmdline: C:\Windows\system32\conhost.exe 0xfffffff -ForceV1 MD5: 81CA40085FC75B8BD2C91D18AA9FFA68)
cmd.exe (PID: 8704 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\laOHLlvfakv.dll",#1 MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
rundll32.exe (PID: 7436 cmdline: rundll32.exe "C:\Users\user\Desktop\laOHLlvfakv.dll",#1 MD5: EF3179D498793BF4234F708D3BE28633)
regsvr32.exe (PID: 8788 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JanzBeoSOFKqX\hUQcK.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
regsvr32.exe (PID: 8688 cmdline: regsvr32.exe /s C:\Users\user\Desktop\laOHLlvfakv.dll MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
regsvr32.exe (PID: 7592 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SAo\KOHOGzImreJ\DHZYcsMibMOGCXWD.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
rundll32.exe (PID: 7448 cmdline: rundll32.exe C:\Users\user\Desktop\laOHLlvfakv.dll,DllRegisterServer MD5: EF3179D498793BF4234F708D3BE28633)
regsvr32.exe (PID: 7460 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FAAMB\YSmuMEqbrgG.dll" MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
rundll32.exe (PID: 372 cmdline: rundll32.exe C:\Users\user\Desktop\laOHLlvfakv.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-1 http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.html http://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	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+motfPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNI0PFj5n2amIQAjAIA=",
    "RUNLMSAAAADzoZW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx22WZ4IQAVAJA="
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2442517269.0000029592A20000.0000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.2442904998.0000000180001000.0000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2440735305.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.2440693096.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.2442401873.0000000002D30000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.29592a20000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.25313ba0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.25313ba0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.29592a20000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.2d30000.1.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 16 - Source IP: 192.168.11.20 - Destination IP: 66.228.32.31		—
Timestamp:	192.168.11.2066.228.32.314982970802404330 03/17/23-17:55:08.721674	
SID:	2404330	
Source Port:	49829	
Destination Port:	7080	
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:	192.168.11.20104.168.155.1434983880802404302 03/17/23-17:55:40.214505	
SID:	2404302	
Source Port:	49838	
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: 167.172.199.165		—
Timestamp:	192.168.11.20167.172.199.1654983580802404308 03/17/23-17:55:30.717404	
SID:	2404308	
Source Port:	49835	
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:	192.168.11.20164.90.222.65498374432404308 03/17/23-17:55:36.091806	
SID:	2404308	
Source Port:	49837	

Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.11.20 - Destination IP: 91.121.146.47	
Timestamp:	192.168.11.2091.121.146.474982780802404344 03/17/23-17:55:03.822964
SID:	2404344
Source Port:	49827
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:	192.168.11.20182.162.143.56498314432404312 03/17/23-17:55:16.470008
SID:	2404312
Source Port:	49831
Destination Port:	443
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

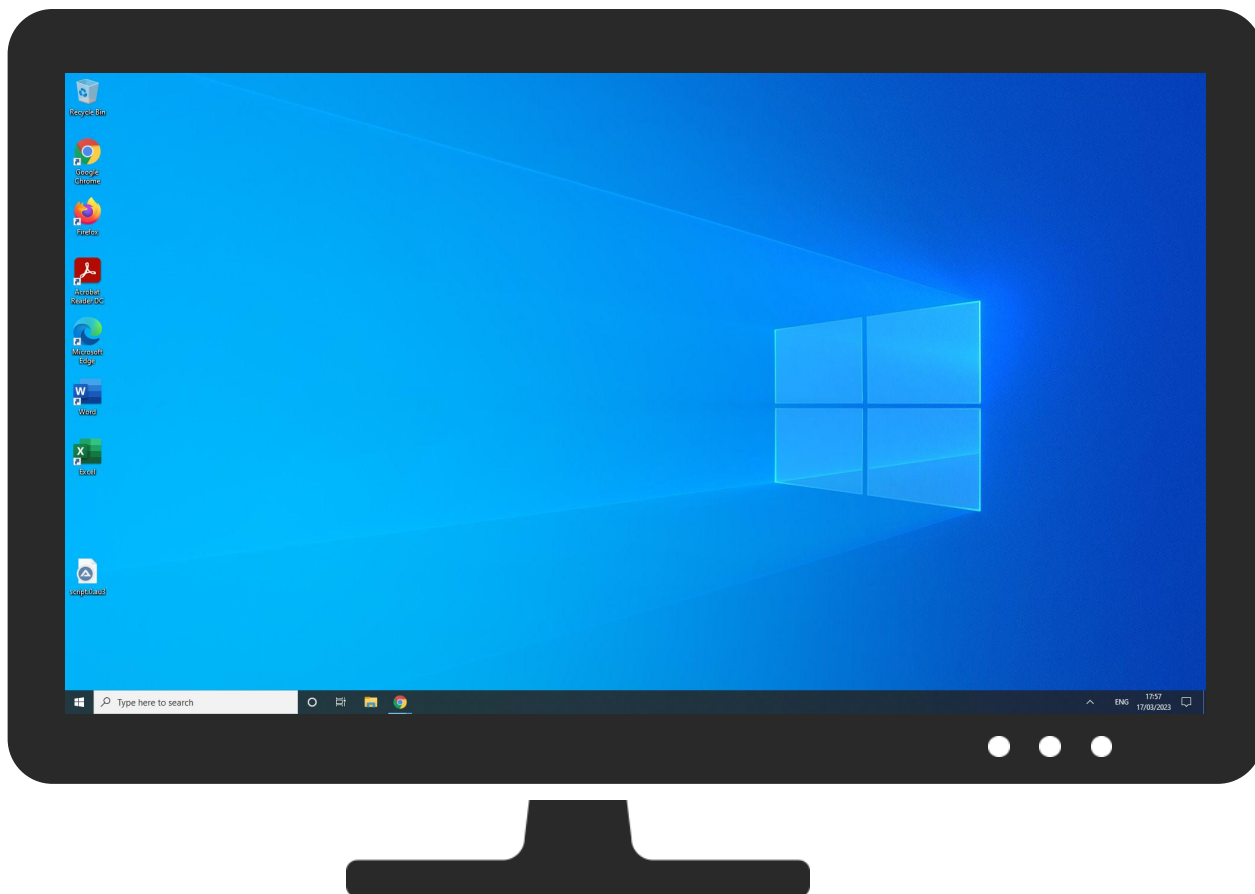


Yara detected Emotet

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
Valid Accounts	1 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time 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 1 Security Software Discovery	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 Virtualization/Sandbox Evasion	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	2 Process 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	1 File and Directory 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	2 5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
aOHLVfakv.dll	28%	ReversingLabs	Win64.Trojan.Emot etcrypt	
aOHLVfakv.dll	54%	Virustotal		Browse

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://103.43.75.120:443/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/a/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/\$	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/z	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/zxqya/	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://159.65.88.10:8080/	100%	Avira URL Cloud	malware	
http://https://82.223.21.224:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/K	100%	Avira URL Cloud	malware	
http://https://82.223.21.224:8080/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://167.172.199.165:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/j	100%	Avira URL Cloud	malware	
http://https://187.63.160.88:80/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/STEM327	100%	Avira URL Cloud	malware	
http://https://183.111.227.137:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/327	100%	Avira URL Cloud	malware	
http://https://187.63.160.88:80/	100%	Avira URL Cloud	malware	
http://https://72.15.201.15:8080/	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://103.132.242.26:8080/	0%	Avira URL Cloud	safe	
http://https://103.43.75.120/0/	100%	Avira URL Cloud	malware	
http://https://159.65.88.10:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/u	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/080/d	100%	Avira URL Cloud	malware	
http://https://173.212.193.249:8080/ert	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/S	100%	Avira URL Cloud	malware	
http://https://173.212.193.249:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/j	100%	Avira URL Cloud	malware	
http://https://183.111.227.137:8080/	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/xqya/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/	100%	Avira URL Cloud	malware	
http://https://173.212.193.249:8080/	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/F	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/d	100%	Avira URL Cloud	malware	
http://https://173.212.193.249:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/icy)	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/k	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/l	100%	Avira URL Cloud	malware	

Domains and IPs
Contacted Domains
 No contacted domains info

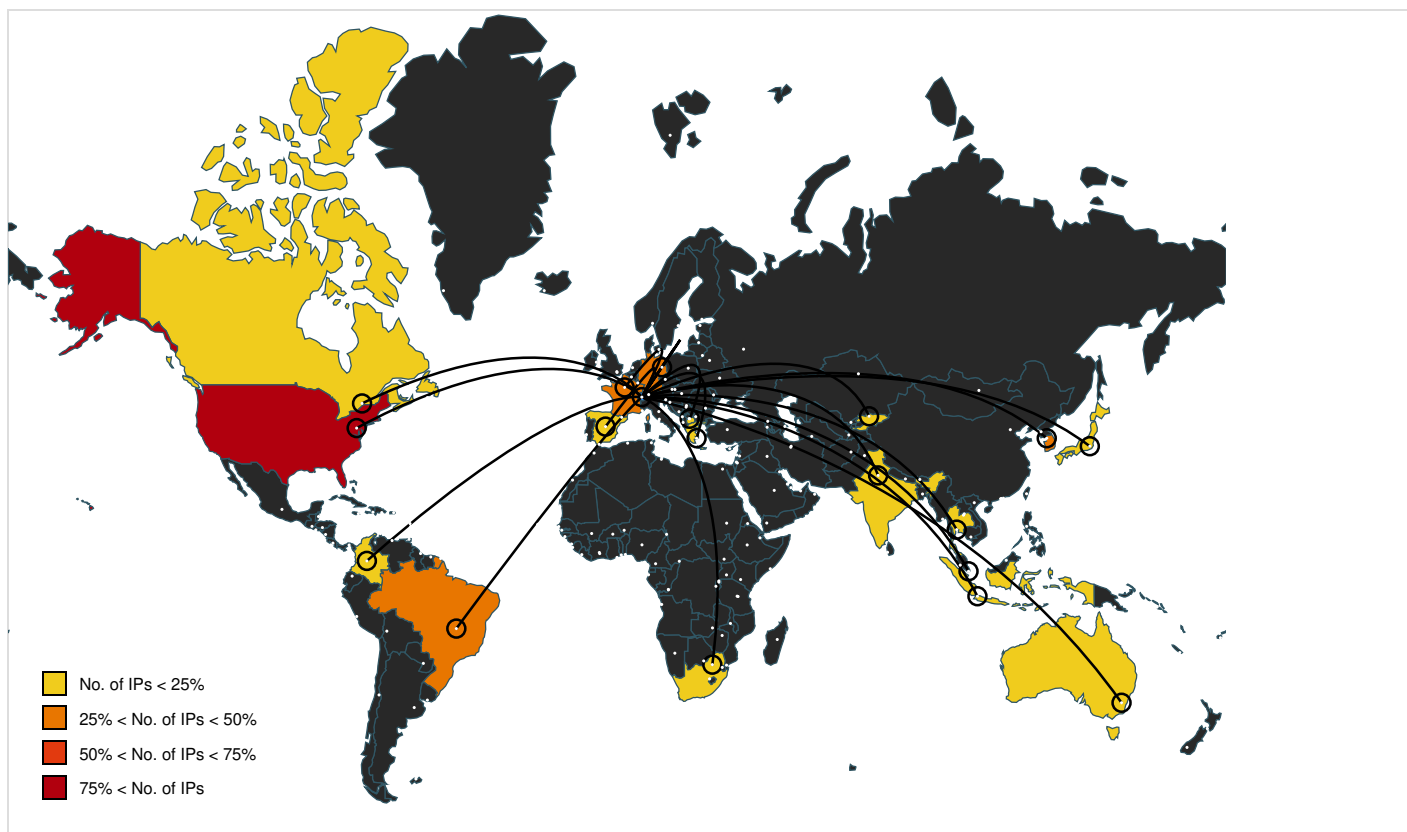
Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	true	Avira URL Cloud: malware	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/zxqya/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B1D000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/\$	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/z	regsvr32.exe, 00000007.00000003.31027094 80.00000000007C6000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.4270670203.0000000007C600 0.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://103.43.75.120:443/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/a/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B1D000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://103.43.75.120/nwgvnyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://159.65.88.10:8080/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://82.223.21.224:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/K	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://82.223.21.224:8080/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/j	regsvr32.exe, 00000007.00000003.31015238 36.000000000077A000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.3104301699.000000000077A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.4273374444.000 0000002B00000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://187.63.160.88:80/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/STEM327	regsvr32.exe, 00000007.00000003.31015238 36.000000000077A000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.3104301699.000000000077A00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://183.111.227.137:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/327	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://187.63.160.88:80/	regsvr32.exe, 00000007.00000003.31015238 36.000000000077A000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.3104301699.000000000077A00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://72.15.201.15:8080/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/	regsvr32.exe, 00000007.00000003.31036015 21.0000000000763000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.2798696588.000000000076300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.3102709480.000 0000000763000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000007.0 0000002.4270670203.0000000000763000.0000 0004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/	regsvr32.exe, 00000007.00000003.31015238 36.000000000077A000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.3104301699.000000000077A00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://103.132.242.26:8080/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://103.43.75.120/0/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://159.65.88.10:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/u	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://103.43.75.120/080/d	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://173.212.193.249:8080/ert	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://103.43.75.120/	regsvr32.exe, 00000007.00000002.42738372 70.0000000002CC7000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/S	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://173.212.193.249:8080/nwgvynyayplzdkad/hjvnruywtgrpudcxhduglli/orzxqya/j	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://183.111.227.137:8080/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://66.228.32.31:7080/	regsvr32.exe, 00000007.00000003.31036015 21.0000000000763000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000003.3102709480.00000000007C600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.4270670203.000 00000007C6000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000007.0 0000003.3102709480.0000000000763000.0000 0004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://103.43.75.120/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/xqya/	regsvr32.exe, 00000007.00000002.42706702 03.00000000007C6000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	regsvr32.exe, 00000007.00000003.31036015 21.0000000000763000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.4270670203.00000000006EB00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.3102709480.000 0000000763000.00000004.00000020.00020000 .00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/	regsvr32.exe, 00000007.00000003.31014183 74.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://173.212.193.249:8080/	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/F	regsvr32.exe, 00000007.00000003.31027094 80.00000000007C6000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.4270670203.00000000007C600 0.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/d	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://173.212.193.249:8080/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://172.105.226.75:8080/icy	regsvr32.exe, 00000007.00000002.42733744 44.0000000002B74000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://103.43.75.120/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/k	regsvr32.exe, 00000007.00000002.42706702 03.000000000078A000.00000004.00000020.00 020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/nwgvynyayplzdkad/hjvnrupyw/tgrpudcxhduglli/orzxqya/l	regsvr32.exe, 00000007.00000003.27986965 88.0000000000763000.00000004.00000020.00 020000.00000000.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-BSAKURAIInternetIncJP	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	WIKINETTELECOMUNICA COESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAIInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
187.63.160.88	unknown	Brazil		28169	BITCOMPROVEDORDESE RVICOSDEINTERNETLTD ABR	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 17:52:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
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:	15
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:	aOHLivfakv.dll

Detection:	MAL
Classification:	mal96.troj.evad.winDLL@18/2@0/49
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 31.8% (good quality ratio 29.6%) - Quality average: 77.1% - Quality standard deviation: 27.3%
HCA Information:	- Successful, ratio: 69% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Found application associated with file extension: .dll - Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.16.241.12, 2.16.241.4, 209.197.3.8
- Excluded domains from analysis (whitelisted): wdcpl.t.microsoft.com, login.live.com, ctdl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wdcpl.microsoft.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Not all processes were analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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

No simulations

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:	95B0A5ACC5BF70D3ABDFFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Preview:	MSCF...v.....l.....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;...l&?...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.Gl."[-...HT..."?..q...ad.. ...7RE.....lf.#./....?-^..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):	3.1213400513386125
Encrypted:	false
SSDEEP:	6:kKdjry/7UN+SkQlPIEGYRMYY9z+4KiDA3RUecZUt:CvkPIE99SNxAhUext
MD5:	C9D0D1DB22CC93F91EA057685D74E8FA
SHA1:	35513EECACAF029FCDFCEC79FA528B80B6F9C64
SHA-256:	66E217986722B5CC1E3EA7051722144A610F33534D1AD7F9923AF0C149C8DF04
SHA-512:	086A420A12949D721D1F798D4DE4CF4BE29652A282B4658FB256F6CC53D0686D15BBE2BA303F4A17266D713816DB8AB4BB14A7BCE1E3CB1D60F3F5564211B054
Malicious:	false
Preview:	p.....7...X..(.....).K.....&.....v...http://.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:	1ed6695b6bfdce048697963812deafcdce28f7c4397af824fc6ffeda03c5ad282b52728620bb2b81a2caa782a8e91f1e888687aaf1727323d2c8365edf8c9a33a
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 00007FA2F0934601h
call 00007FA2F096A13Fh
call 00007FA2F0965CFAh
call 00007FA2F096A145h
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 [FFFFFFCB7h]
dec eax
mov dword ptr [eax], ecx
dec eax
lea ecx, dword ptr [FFFFFFF59h]
dec eax
mov dword ptr [eax+08h], ecx
dec eax
lea ecx, dword ptr [FFFFFFF4Eh]
dec eax
mov dword ptr [eax+10h], ecx
dec eax
lea ecx, dword ptr [FFFFFFF8Bh]
dec eax
mov dword ptr [eax+18h], ecx
dec eax

Instruction
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 00007FA2F09346AAh

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_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x75000	0x5d0	0x600	False	0.01302083333333334	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x76000	0x3a38	0x3c00	False	0.4626953125	data	5.526910649754969	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.xdata	0x7a000	0x5fd0	0x6000	False	0.14701334635416666	shared library	4.906149317469979	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.idata	0x80000	0xb38	0xc00	False	0.2919921875	data	3.959226833867136	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.edata	0x81000	0x69	0x200	False	0.181640625	data	1.2134297058839834	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x2be00	0x2be00	False	0.8775151353276354	data	7.859341694371929	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0x11b4	0x1200	False	0.6178385416666666	data	5.813939662419332	IMAGE_SCN_CNT_INITIALIZE D_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

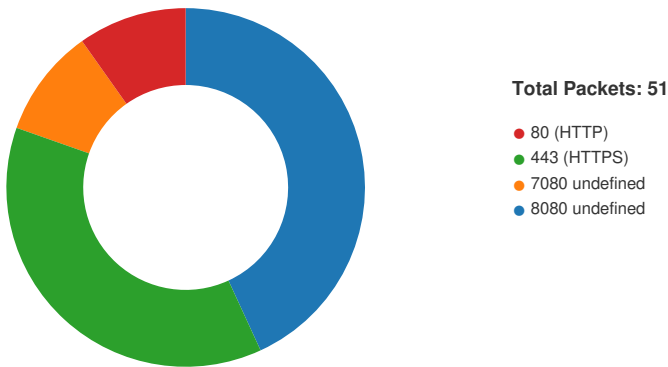
Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2066.228.32.3 14982970802404330 03/17/23- 17:55:08.721674	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49829	7080	192.168.11.20	66.228.32.31
192.168.11.20104.168.15 5.1434983880802404302 03/17/23- 17:55:40.214505	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49838	8080	192.168.11.20	104.168.155.143
192.168.11.20167.172.19 9.1654983580802404308 03/17/23- 17:55:30.717404	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49835	8080	192.168.11.20	167.172.199.165
192.168.11.20164.90.222. 65498374432404308 03/17/23- 17:55:36.091806	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49837	443	192.168.11.20	164.90.222.65
192.168.11.2091.121.146. 474982780802404344 03/17/23- 17:55:03.822964	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49827	8080	192.168.11.20	91.121.146.47
192.168.11.20182.162.14 3.56498314432404312 03/17/23- 17:55:16.470008	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49831	443	192.168.11.20	182.162.143.56

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:55:03.822963953 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:03.842253923 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:03.842469931 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:03.844355106 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:03.863508940 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:03.884574890 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:03.884633064 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:03.884812117 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:03.887244940 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:03.907407045 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:03.954986095 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:04.660682917 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:04.660682917 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:04.680037022 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:04.751033068 CET	8080	49827	91.121.146.47	192.168.11.20

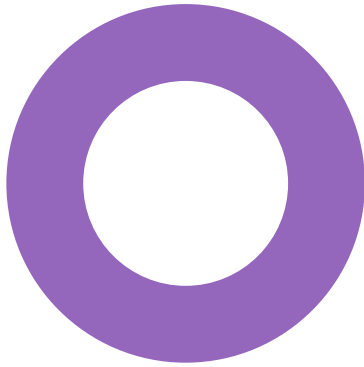
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:55:04.798549891 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:07.748513937 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:07.748599052 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:07.748816967 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:07.748817921 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:07.748817921 CET	49827	8080	192.168.11.20	91.121.146.47
Mar 17, 2023 17:55:07.768208981 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:07.768244028 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:07.768269062 CET	8080	49827	91.121.146.47	192.168.11.20
Mar 17, 2023 17:55:08.721673965 CET	49829	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:55:08.813566923 CET	7080	49829	66.228.32.31	192.168.11.20
Mar 17, 2023 17:55:09.313343048 CET	49829	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:55:09.405122995 CET	7080	49829	66.228.32.31	192.168.11.20
Mar 17, 2023 17:55:09.906966925 CET	49829	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:55:09.998740911 CET	7080	49829	66.228.32.31	192.168.11.20
Mar 17, 2023 17:55:10.500451088 CET	49829	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:55:10.591742039 CET	7080	49829	66.228.32.31	192.168.11.20
Mar 17, 2023 17:55:11.094125986 CET	49829	7080	192.168.11.20	66.228.32.31
Mar 17, 2023 17:55:11.185641050 CET	7080	49829	66.228.32.31	192.168.11.20
Mar 17, 2023 17:55:16.470007896 CET	49831	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.470108032 CET	443	49831	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.470316887 CET	49831	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.470504045 CET	49831	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.470545053 CET	443	49831	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.705921888 CET	443	49831	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.706535101 CET	49832	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.706639051 CET	443	49832	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.706866980 CET	49832	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.707146883 CET	49832	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.707223892 CET	443	49832	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.945801020 CET	443	49832	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.946307898 CET	49833	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.946396112 CET	443	49833	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.946610928 CET	49833	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.946799040 CET	49833	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:16.947004080 CET	443	49833	182.162.143.56	192.168.11.20
Mar 17, 2023 17:55:16.947177887 CET	49833	443	192.168.11.20	182.162.143.56
Mar 17, 2023 17:55:22.222096920 CET	49834	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:55:22.442723036 CET	80	49834	187.63.160.88	192.168.11.20
Mar 17, 2023 17:55:22.950834990 CET	49834	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:55:23.171304941 CET	80	49834	187.63.160.88	192.168.11.20
Mar 17, 2023 17:55:23.685240030 CET	49834	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:55:23.905503988 CET	80	49834	187.63.160.88	192.168.11.20
Mar 17, 2023 17:55:24.419260979 CET	49834	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:55:24.639291048 CET	80	49834	187.63.160.88	192.168.11.20
Mar 17, 2023 17:55:25.153383970 CET	49834	80	192.168.11.20	187.63.160.88
Mar 17, 2023 17:55:25.373801947 CET	80	49834	187.63.160.88	192.168.11.20
Mar 17, 2023 17:55:30.717403889 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:30.877808094 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:30.878029108 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:30.878396034 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:31.038242102 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:31.048325062 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:31.048401117 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:31.048665047 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:31.051322937 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:31.212112904 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:31.213166952 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:31.415318966 CET	8080	49835	167.172.199.165	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 17:55:32.039026022 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:32.089509964 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:35.039800882 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:35.039868116 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:35.040082932 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:35.040082932 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:35.040082932 CET	49835	8080	192.168.11.20	167.172.199.165
Mar 17, 2023 17:55:35.199883938 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:35.199937105 CET	8080	49835	167.172.199.165	192.168.11.20
Mar 17, 2023 17:55:35.966129065 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:35.966291904 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:35.966497898 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:35.966687918 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:35.966737032 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.087966919 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.088268042 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:36.089459896 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:36.089535952 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.090668917 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.091527939 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:36.132508039 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.291066885 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.291352987 CET	443	49837	164.90.222.65	192.168.11.20
Mar 17, 2023 17:55:36.291520119 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:36.292974949 CET	49837	443	192.168.11.20	164.90.222.65
Mar 17, 2023 17:55:36.292974949 CET	49837	443	192.168.11.20	164.90.222.65

ICMP Packets						
Timestamp	Source IP	Dest IP	Checksum	Code	Type	
Mar 17, 2023 17:56:37.473143101 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable	
Mar 17, 2023 17:56:38.486097097 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable	
Mar 17, 2023 17:56:40.502083063 CET	103.132.242.26	192.168.11.20	2278	(Unknown)	Destination Unreachable	
Mar 17, 2023 17:56:44.516495943 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



Click to jump to process

System Behavior

Analysis Process: loadll64.exe PID: 8532, Parent PID: 4660

General

Target ID:	0
Start time:	17:54:25
Start date:	17/03/2023
Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe "C:\Users\user\Desktop\laOHLivfakv.dll"
Imagebase:	0x7ff64c450000
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: 8560, Parent PID: 8532

General

Target ID:	1
Start time:	17:54:25
Start date:	17/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ca940000
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: 8704, Parent PID: 8532	
General	
Target ID:	2
Start time:	17:54:26
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\OHLlvfakv.dll",#1
Imagebase:	0x7ff7a07d0000
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: 8688, Parent PID: 8532	
General	
Target ID:	3
Start time:	17:54:26
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\OHLlvfakv.dll
Imagebase:	0x7ff642830000
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: 00000003.00000002.2442904998.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.2442401873.0000000002D30000.00000040.00001000.00020000.00000000.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: 7436, Parent PID: 8704

General

Target ID:	4
Start time:	17:54:26
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\laOHLlvfakv.dll",#1
Imagebase:	0x7ff660480000
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: 00000004.00000002.2442517269.0000029592A20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.2440693096.0000000180001000.00000020.00001000.00020000.00000000.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\AnzBeoSOFkqX\hUQcK.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: 7448, Parent PID: 8532

General

Target ID:	5
Start time:	17:54:26
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\laOHLlvfakv.dll,DllRegisterServer
Imagebase:	0x7ff660480000
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: 00000005.00000002.2440735305.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.2442528537.0000025313BA0000.00000040.00001000.00020000.00000000.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: 8788, Parent PID: 7436

General

Target ID:	7
Start time:	17:54:27
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JanzBeoSOFkqX\hUQcK.dll"
Imagebase:	0x7ff642830000
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_3, Description: Yara detected Emotet, Source: 00000007.00000002.4270670203.00000000006EB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.4274390875.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.4271871616.0000000000A10000.00000040.00001000.00020000.00000000.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: 7460, Parent PID: 7448

General

Target ID:	8
Start time:	17:54:27
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FAAMB\YSmuMEqbrG.dll"
Imagebase:	0x7ff642830000
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: 7592, Parent PID: 8688

General

Target ID:	9
Start time:	17:54:27
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SAolKOHOGzImreJ\NDHZYcsMibMOGCXWD.dll"
Imagebase:	0x7ff642830000
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: 372, Parent PID: 8532	
General	
Target ID:	10
Start time:	17:54:29
Start date:	17/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\OHLivfakv.dll,__CPPdebugHook
Imagebase:	0x7ff660480000
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