ID: 339432
Sample Name: ACH REMITTANCE ADVICE..xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:28:38
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report ACH REMlTTANCE ADVlCE..xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 13
JA3 Fingerprints 15
Dropped Files 17
Created / dropped Files 17
Static File Info 40
General 40
File Icon 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 41
UDP Packets 42
DNS Queries 44
DNS Answers 45
HTTPS Packets 47
Code Manipulations 56
Statistics 56
Behavior 56
System Behavior 56

Analysis Process: EXCEL.EXE PID: 2100 Parent PID: 584 56
General 56
File Activities 57
File Created 57
File Deleted 57
File Moved 57
File Written 57
File Read 58
Registry Activities 58
Key Created 58
Key Value Created 58
Analysis Process: iexplore.exe PID: 1976 Parent PID: 584 62
General 62
File Activities 63
Registry Activities 63
Analysis Process: iexplore.exe PID: 2364 Parent PID: 1976 63
General 63
File Activities 63
Registry Activities 63
Analysis Process: iexplore.exe PID: 2864 Parent PID: 2100 64
General 64
File Activities 64
Registry Activities 64
Analysis Process: iexplore.exe PID: 3056 Parent PID: 2864 64
General 64
File Activities 64
Registry Activities 65
Disassembly 65

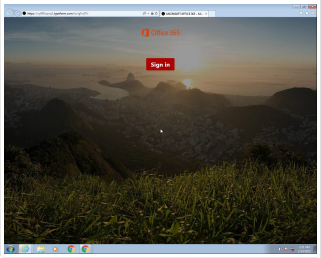
Analysis Report ACH REMITTANCE ADVICE..xlsx

Overview

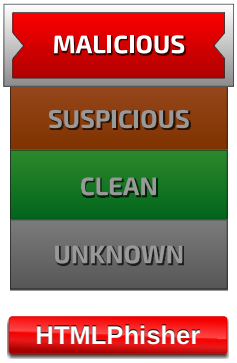
General Information

Sample Name:	ACH REMITTANCE ADVICE..xlsx
Analysis ID:	339432
MD5:	1726734045f0135.
SHA1:	b6c9fb364f0bb87..
SHA256:	46f4cb7548dfcb3..

Most interesting Screenshot:



Detection

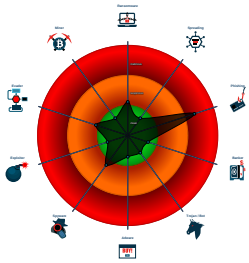


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_25
- Phishing site detected (based on im…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Steals Internet Explorer cookies

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2100 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - iexplore.exe (PID: 2864 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://ny990xqwsj1.typeform.com/to/qjFrxD7r MD5: 4EB098135821348270F27157F7A84E65)
    - iexplore.exe (PID: 3056 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2864 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 1976 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2364 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1976 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

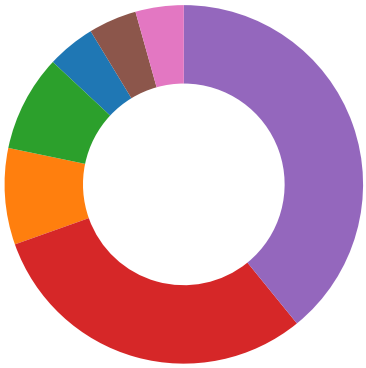
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\qjFrxD7r[1].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\qjFrxD7r[1].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

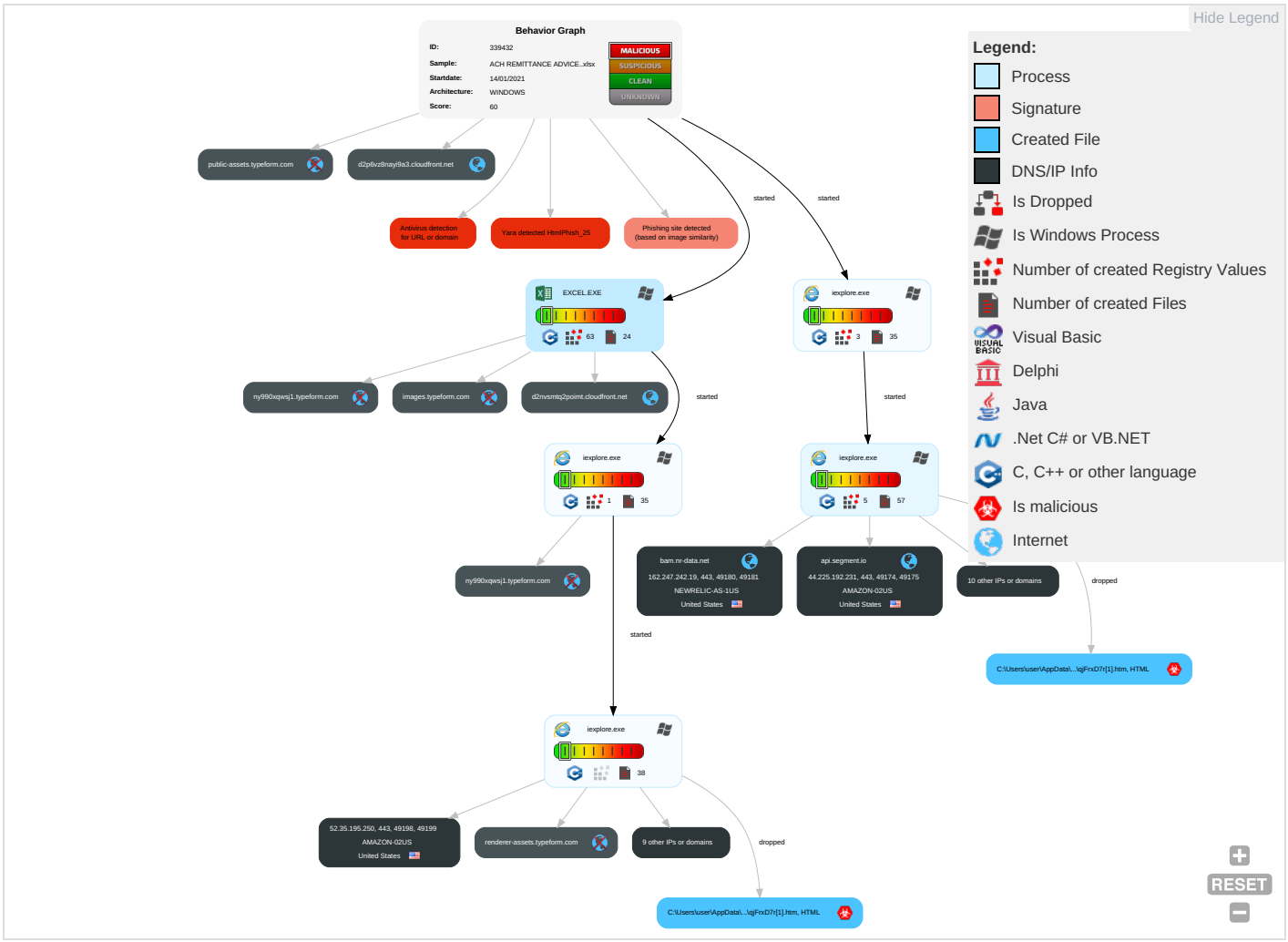
Yara detected HtmlPhish_25

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	Credentials In Files 1	File and Directory Discovery 1	Remote Services	Data from Local System 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Frau

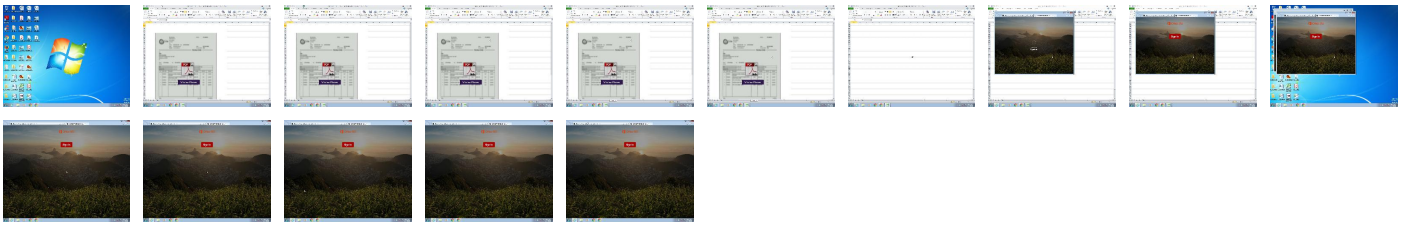
Behavior Graph

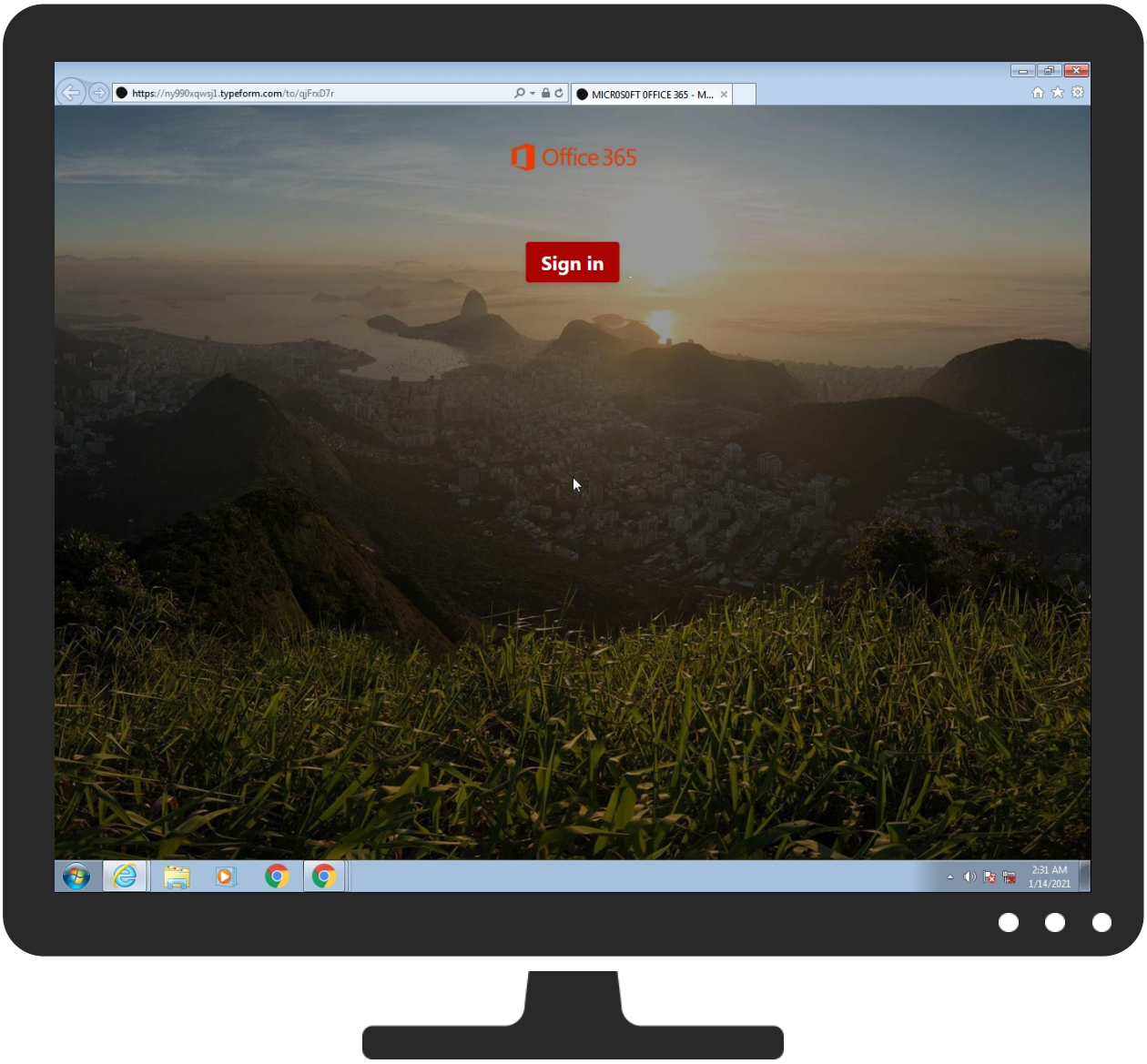


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bam.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://www.typeform.c	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.typeform.cpeform.com/to/qjFrxD7rz	0%	Avira URL Cloud	safe	
http://https://ny990xqwsj1.typefRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d296je7bbdd650.cloudfront.net	65.9.70.129	true	false		high
api.segment.io	44.225.192.231	true	false		high
d2citsn5wf4j9j.cloudfront.net	65.9.58.106	true	false		high
d2nvsmtq2poimt.cloudfront.net	65.9.58.87	true	false		high
bam.nr-data.net	162.247.242.19	true	false	• 0%, Virustotal, Browse	unknown
d2p6vz8nayi9a3.cloudfront.net	65.9.58.120	true	false		high
cdn.segment.com	unknown	unknown	false		high
renderer-assets.typeform.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
public-assets.typeform.com	unknown	unknown	false		high
images.typeform.com	unknown	unknown	false		high
ny990xqwsj1.typeform.com	unknown	unknown	false		high

Contacted URLs

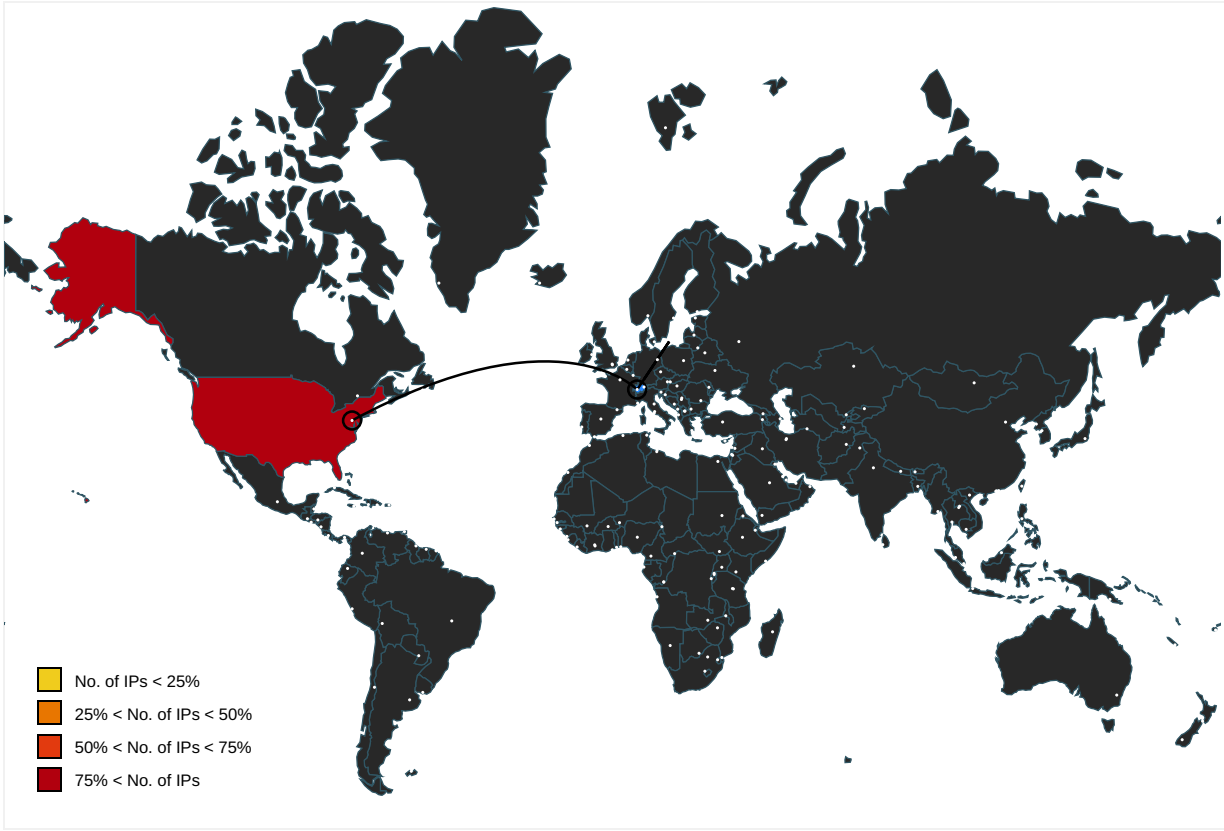
Name	Malicious	Antivirus Detection	Reputation
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://www.typeform.com/?utm_campaign=qjFrxD7r&utm_source=typeform.com-17523577-Free&utm_medium=typeform&utm_content=typeform-footer&utm_term=EN	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png	qjFrxD7r[1].htm.3.dr, ~DF72A7006BFF98A571.TMP.6.dr	false		high
http://https://renderer-assets.typeform.com/	qjFrxD7r[1].htm.3.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	vendors~form.965f5dedbb854e83c6c8[1].js.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/safari-pinned-tab.svg	qjFrxD7r[1].htm.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/oembed?url=https%3A%2F%2Fny990xqwsj1.typeform.com%2Fto%2FqjFrxD7r	qjFrxD7r[1].htm.3.dr	false		high
http://https://renderer-assets.typeform.com/vendors~blocks-ranking.f8aee16223a106724ea1.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://renderer-assets.typeform.com/vendors~phonenumber.32d788474b661d4d3074.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://images.typeform.com/images/m9zWqYibLnGK/background/large);background-position:top	qjFrxD7r[1].htm.3.dr	false		high
http://https://renderer-assets.typeform.com/blocks-matrix.0544beec0e1a4e11a24a.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6Root	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-16x16.png	qjFrxD7r[1].htm.3.dr	false		high
http://https://renderer-assets.typeform.com/phonenumber.6ea5ec50b9fa21e816ff.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://github.com/kof/animationFrame	vendors~form.965f5dedbb854e83c6c8[1].js.3.dr	false		high
http://https://renderer-assets.typeform.com/renderer.0f5a683b381b67dbbf89.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://renderer-assets.typeform.com/vendors~form.965f5dedbb854e83c6c8.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://images.typeform.com/images/FYUps4mFKPYK/image/default	qjFrxD7r[1].htm.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://public-assets.typeform.com/public/favicon/browserconfig.xml	~DFC448DC16F91BBCE4.TMP.6.dr, qjFrxD7r[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/site.webmanifest	qjFrxD7r[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon.ico	qjFrxD7r[1].htm.3.dr	false		high
http://https://images.typeform.com/images/HzxaK5qZrKPU/image/default	qjFrxD7r[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/apple-touch-icon.png	qjFrxD7r[1].htm.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r	qjFrxD7r[1].htm.3.dr	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://www.typeform.c	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.typeform.cpeform.com/to/qjFrxD7rz	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6orm.com/to/qjFrxD7r	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://renderer-assets.typeform.com/form.9cd5d6381506e5950fe0.js	qjFrxD7r[1].htm.3.dr	false		high
http://www.jacklmoore.com/autosize	vendors~form.965f5dedbb854e83c6c8[1].js.3.dr	false		high
http://https://www.typeform.com/?utm_campaign=qjFrxD7r&utm_source=typeform.com-17523577-Free&utm_medium=typ	~DFBC05D677CD36F01B.TMP.2.dr	false		high
http://https://renderer-assets.typeform.com/modern-renderer.36eec26e0148023415c0.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png-	imagestore.dat.3.dr	false		high
http://https://github.com/js-cookie/js-cookie	renderer.0f5a683b381b67dbbf89[1].js.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6om/?utm_campaign=qjFrxD7r&utm_soorm.com/to/qjFrxD7r	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://renderer-assets.typeform.com/vendors~attachment.6e37d3fcdf703c1517e1.js	qjFrxD7r[1].htm.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6MlCR0S0FT	~DFBC05D677CD36F01B.TMP.2.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7rRoot	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://ny990xqwsj1.typefRoot	{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://images.typeform.com/images/m9zWqYibLnGK/background/large	qjFrxD7r[1].htm.3.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7rz	~DFBC05D677CD36F01B.TMP.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.9.58.87	unknown	United States		16509	AMAZON-02US	false
44.225.192.231	unknown	United States		16509	AMAZON-02US	false
162.247.242.19	unknown	United States		23467	NEWRELIC-AS-1US	false
65.9.58.106	unknown	United States		16509	AMAZON-02US	false
52.35.195.250	unknown	United States		16509	AMAZON-02US	false
65.9.70.129	unknown	United States		16509	AMAZON-02US	false
65.9.58.120	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339432
Start date:	14.01.2021
Start time:	02:28:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ACH REMITTANCE ADVICE..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:	9
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.winXLSX@8/83@19/7
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 • Browse link: https://ny990xqws j1.typeform.com/to/qjFrxD7r • Scroll down • Close Viewer • Browsing link: https://www.typeform.com/? utm_campaign=qjFrxD 7r&utm_source=typeform.com-17523577-Free&utm_medium= typeform&utm_content=typeform-footer&utm_term=EN
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 104.18.26.71, 104.18.27.71, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 204.79.197.200, 13.107.21.200, 13.107.5.80, 152.199.19.161 • Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, api.bing.com, f4.shared.global.fastly.net, r20swj13mr.microsoft.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e-0001.e-msedge.net, go.microsoft.com, random.typeform.com.cdn.cloudflare.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, api-bing-com.e-0001.e-msedge.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
44.225.192.231	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
52.35.195.250	http://https://owaonlineportalsfseyyq.yolasite.com/	Get hash	malicious	Browse	
65.9.70.129	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	
65.9.58.120	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
162.247.242.19	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	
	http://https://www.freightwaves.com/news/canadian-fuel-distributor-parkland-targeted-in-cyberattack	Get hash	malicious	Browse	
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	
	ACH WIRE REMITTANCE COPY.xlsx	Get hash	malicious	Browse	
	ACH WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT.xlsx	Get hash	malicious	Browse	
	http://https://mmemicrosoftwebsss.typeform.com/to/sIZVMxGk	Get hash	malicious	Browse	
65.9.58.106	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.segment.io	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.187.246.64
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.148.169.229
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.69.177.146
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 34.218.160.124
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.218.98.189
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.71.252.35
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 44.229.187.242
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.149.194.4
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 52.43.118.59
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 52.35.191.167
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 52.11.35.251
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 52.37.21.144
	http://https://aud-amplified.unicornplatform.com/	Get hash	malicious	Browse	• 35.162.116.128
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 54.70.113.89
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 54.69.52.31
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 54.190.208.247
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 34.210.41.193
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 54.186.56.40
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 54.148.169.229
	http://https://secure-teams-storage.webflow.io/	Get hash	malicious	Browse	• 54.149.50.128
d2citsn5wf4j9j.cloudfront.net	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.93.122
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 65.9.58.106
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.100
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.27
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.27
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.111
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 13.224.94.129
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 143.204.90.86
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 13.224.93.43
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.110
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.4
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.111

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.27
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 65.9.68.126
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 13.224.93.43
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 143.204.20 8.110
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 143.204.208.47
	http://https://mainprops.typeform.com/to/gHgyBoFX	Get hash	malicious	Browse	• 143.204.208.47
d296je7bbdd650.cloudfront.net	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.99.83
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 65.9.70.129
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.99.83
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.99.83
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 143.204.5.83
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 143.204.5.83
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 143.204.5.83
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 143.204.5.83
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 143.204.5.83
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 13.224.100.80
	http://https://target-care.webflow.io/	Get hash	malicious	Browse	• 13.224.100.80
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706 57475616c2e636f6d2e6175	Get hash	malicious	Browse	• 65.9.58.129
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 143.204.99.83
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 13.224.100.80
	http://https://stevenscapitaladvisors.webflow.io/	Get hash	malicious	Browse	• 65.9.58.129
	http://https://stevenscapitaladvisors.webflow.io/	Get hash	malicious	Browse	• 65.9.58.129
	http://https://aud-amplified.unicornplatform.com/	Get hash	malicious	Browse	• 143.204.99.83
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.99.83
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.99.83
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.5.83
d2nvsmtq2poimt.cloudfront.net	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.93.30
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.100
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 65.9.58.100
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.100
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.16
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.16
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.87
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.109
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.88
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.98
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 13.224.94.83
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 143.204.90.37
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 13.224.93.102
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.20
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.8
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.87
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.98
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 65.9.68.116
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 13.224.93.75
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 13.224.93.75

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 15.237.76.117
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.93.122
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.148.169.229
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 99.83.185.45
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.69.177.146
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 34.218.160.124
	13-01-21.xlsx	Get hash	malicious	Browse	• 18.195.87.136
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 54.254.26.94
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
NEWRELIC-AS-1US	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.19
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.18
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.18
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.19
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 162.247.242.20
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 162.247.242.20
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 162.247.242.20
	http://https://bit.do/fLVUm	Get hash	malicious	Browse	• 162.247.242.21
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Fbit.do%2FfLVUm%3Ffbclid%3DIwAR3_y5be7qgzc9rWXbeIQlHePNYF96mJvcjTtfijse-VyaDOGbdXhiymogA&h=AT2La9RfuL-CBpF75ix5HdI9ILnyapdVZIzXgRQt4G1Y7x5nZpCr9RLeZPnCT8_3vYaiFFnwir6t35RvMH3lJhYuYrzugBPtxdx4PUirtTUjKnczau25WjD4XcXiFnckifU	Get hash	malicious	Browse	• 162.247.242.21
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 162.247.242.20
	http://perpetual.veteran.az/673616c6c792e64756e6e654070657270657475616c2e636f6d2e6175	Get hash	malicious	Browse	• 162.247.242.18
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 162.247.242.18
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 162.247.242.19
	http://view.e.business.officedepot.com/?qs=3fe5dee3fd6dc334e57f4fe8c13caa1dc833d1845b46e0df5e76d8dcd189c65840b833e5f8853ee5eca50625943bfd8b71f0d693bc12eda6d7c035c0df2243dc5fe3f7c370b5320b8fd654c8b827b865	Get hash	malicious	Browse	• 162.247.242.18
AMAZON-02US	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 15.237.76.117
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.93.122
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.148.169.229
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.89
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 99.83.185.45
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.69.177.146
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 34.218.160.124
	13-01-21.xlsx	Get hash	malicious	Browse	• 18.195.87.136
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 54.254.26.94
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
AMAZON-02US	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 15.237.76.117
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.93.122
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.148.169.229
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.89
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 99.83.185.45
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.69.177.146
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 34.218.160.124
	13-01-21.xlsx	Get hash	malicious	Browse	• 18.195.87.136
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 54.254.26.94
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	rB26M8hflh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	Notification_71823.xls	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	Notification_71823.xls	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	Monex_USD.doc	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.27970.rtf	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.31662.rtf	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18733.rtf	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106
	n#U00b0 761.doc	Get hash	malicious	Browse	• 65.9.58.87 • 44.225.192.231 • 52.35.195.250 • 65.9.70.129 • 65.9.58.120 • 162.247.242.19 • 65.9.58.106

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23 B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.I...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MP98E46N\ny990xqwsj1.typeform[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	528940
Entropy (8bit):	5.20171008801215
Encrypted:	false
SSDEEP:	3072:jy6662hIn1n6nGnynvnXnOnKn0n3bOAVc4:p
MD5:	E0B17CD8E6B15C5246DE77B578F616C2
SHA1:	3937AF81CF5CAC3C80C638FDE94683242D1C82C8
SHA-256:	2E06EC78B18095F36737DF0C74921B7B55898222E3CDB15EB8BCBEDBF7FEAE74
SHA-512:	7627A2B053A00614AF88BC1307B1D28985793848445D30B678DCED17174175CAACF72FF4569D524004467D66BED54F88915379048E8AB017526D79323D04D73C
Malicious:	false
Reputation:	low
Preview:	<root><item name="qjFrxD7r-visitorId" value="qjFrxD7r-1610620203169-47" ltime="939931680" htime="30861920" /><item name="debug" value="undefined" ltim e="1027511680" htime="30861920" /><item name="segmentio.96a0917f-50c7-4a31-a5a2-947c083fcae7.inProgress" value="{}" ltime="980321680" htime="30861920" /> <item name="segmentio.96a0917f-50c7-4a31-a5a2-947c083fcae7.queue" value="[]" ltime="977981680" htime="30861920" /><item name="segmentio.96a0917f-50c7- 4a31-a5a2-947c083fcae7.ack" value="1610620211642" ltime="1024621680" htime="30861920" /><item name="segmentio.96a0917f-50c7-4a31-a5a2-947c083fcae7. reclaimStart" value="null" ltime="1024621680" htime="30861920" /><item name="segmentio.96a0917f-50c7-4a31-a5a2-947c083fcae7.reclaimEnd" value="null" l time="1024621680" htime="30861920" /><item name="ajs_anonymous_id" value=""0bf607f4-babe-45e7-8a96-59d6e6d55eb7"" ltime="981571680" htime="3 0861920" /></root><root><item name="qjFrxD7r-visitorId" value="qjFrxD7r-1610620203169-47" ltime="939

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{739E3DFD-5653-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24664
Entropy (8bit):	1.7881473705030495
Encrypted:	false
SSDEEP:	48:IvcGcpUxGwp0jwG/apnjG2rGIpHjG0nGvnZpEjG0c8Go6VqpqjG0cRaGo4WO5pZS:MAKrK+pT9JKad0SF3Xi
MD5:	591F72436BC98027DD171072E9269001
SHA1:	20FA5FD282D9A31114E6457BF956B0C704167368
SHA-256:	638BE889A61D407EDE23529141EB2734E4A170B8566B0EE432FDB6725F428D96
SHA-512:	77C5EA6AE1301C7799450DB7B4C1DAF75782FB861D897C64CCEA41029EE15ACA31A84899CBEDA0E4D3C6AB1F15C24D93D21CB63132331E33F4B6E87343CCF 45
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{78AC5478-5653-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29784
Entropy (8bit):	1.8234946456000842
Encrypted:	false
SSDEEP:	96:M3KEK+ph9JlaJ0+Za3hYsJzQZt1D0tqehRcX:M3KEK+ph9JlaJ0aa3XJqtJ0tqeMX
MD5:	D8B72E95BBFA43C57C6EC38F82DD38F6
SHA1:	D982613B0F9445629C5DDF490FC2347177690B64
SHA-256:	A1077BEF8153230236D9AB21C83BF865DD0B76FCFB7B77D7660373AD6B1305D9
SHA-512:	81888917C1D37B9EC6D1826A69954CCA40E26CF233C2914254D76A48EB5F3FFD90E1524AE2CD08561140D6CA8C5B4FF25211935C39226316F821B25E92CC7758
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{739E3DFF-5653-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39466
Entropy (8bit):	2.0451544258467638
Encrypted:	false
SSDEEP:	192:MLKkb5Jz7OFcJpYkJHzRYsGvQUfOdgLHgfm1HcbrA:M2i73OiLnTR1cQU2dg7gedc4
MD5:	BFFB43C42C114FA649AD28060F6224C8
SHA1:	239391FA45582A773A8E6B2656F055EC20632601
SHA-256:	E6E4D0053C8798EBB59C30243911040A599A179FD109EA77722D425FFAC22AEB
SHA-512:	45CF6CCB5B33AF96489EAC4EFE907E5C8CD0220D3E3E40B6F92AED1453A720C12378E51A3043E081BA583C545CA4F8580D4534A93765F4A7E8EC9B6488DABD 2
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{78AC547A-5653-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27002
Entropy (8bit):	1.877239133243687
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{78AC547A-5653-11EB-ADCF-ECF4BBB5915B}.dat	
SSDEEP:	192:MRK5bZtJ7o3UAoL5owRZotoouSIoNoomUXr:M4JPRoBotowToSoaoyomU7
MD5:	0F37D42AAE8E1259B86ADE4D87F56931
SHA1:	6225FFB058A1C038FB267ED551294113C6B3A46A
SHA-256:	E5FC991CFEC88B27843B55066CB2D65B8627A9D38120A130DD063D0226FDB020
SHA-512:	17B4737B7F3F1A73EDD6426093AC637DC903FED21A11BD69E4D02C8ACE10CEF64FFEBC176AD728060F99DDE48D995213A88572C4DCDDEA809BF38E925ED05AC
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{78AC547B-5653-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669180708460706
Encrypted:	false
SSDEEP:	48:IvRGcpUwGwpN2G4pPeGrapgSDrGQpZdG7HpCssTGIpG:MnKYbGJQeSDF/80s4A
MD5:	4DD8669F581EC52065E2E026EFED4E04
SHA1:	0FE740CFE15B6EFEA12FCCFAFB98AE7F975D0E1A
SHA-256:	0F4ED79AD6F839A33FB4FDBF9A152833913D7F79F466762E0CC7989A074D2864
SHA-512:	8AE537AA483EEB2ECDB0C98E8246DD181F6091DD72E7D7D2181E5439C1E1CA8ABBDAD6B2889F0DD4A76956750BC068CE79A01EC363D1D18A1E18C63269A55C6
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1241
Entropy (8bit):	7.232601236595541
Encrypted:	false
SSDEEP:	24:Yt4/pSym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02Efl58l:YUx0v9PoQ5VqKwspEej8l
MD5:	099D4E6AADF10881B160C8C13F88941C
SHA1:	28ECDECD0727DD57CAD9595AF9812872B2E9E20E
SHA-256:	9828D9E958E5339756991830B45FDB234AEBC584679CACEE656075E5A39076C2
SHA-512:	35E4FA811BD2DB47B4CC82C31B7A55A3A63E409B76F03A6BF97D978CCE38E71AB7BCA33314AD57BD6E3C2CC8F65739ACF275B5F714B9A3345AAD8B0524978FEA
Malicious:	false
Reputation:	low
Preview:	C.h.t.t.p.s.:././.p.u.b.l.i.c.-.a.s.s.e.t.s...t.y.p.e.f.o.r.m...c.o.m./.p.u.b.l.i.c./.f.a.v.i.c.o.n./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.-....PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z &.....u0...`.:.....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\ .W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ..._.X...T.Z.f..S.{.#..{...Op.Y.87..X.9...[.,.$..Z]oV{..c.|#_c.. ....!.0..t.gs...X{c..6G.X.9.. ..".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q......./L.2..2.x.Qj.....9 .$-.e88... ..G.YF.G....b.C.[%.u..c...q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>..GE..8.....[r.9C/...d;.PH....3.m....[._ .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1310
Entropy (8bit):	4.810709096040597
Encrypted:	false
SSDEEP:	24:5Y0bn73pHIUZtJD0lFBohpZlJiHqw87xTeB0yVFaFG:5b73HJq0TJiHp89TOwU
MD5:	CDF81E591D9CBFB47A7F97A2BCDB70B9
SHA1:	8F12010DFAACDECAD77B70A3E781C707CF328496
SHA-256:	204D95C6FB161368C795BB63E538FE0B11F9E406494BB5758B3B0D60C5F651BD

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\NewErrorPageTemplate[1]	
SHA-512:	977DCC2C6488ACAF0E5970CEF1A7A72C9F9DC6BB82DA54F057E0853C8E939E4AB01B163EB7A5058E093A8BC44ECAD9D06880FDC883E67E28AC67FEE4D070A4CC
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #575757;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #2778ec;.. font-size: 38pt;.. font-weight: 300;.. vertical-align:bottom;.. margin-bottom: 20px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 40px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.. padding-top: 5px;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsBu

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\aa6e0ec721[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.31817604175005
Encrypted:	false
SSDEEP:	3:U3KTDWuvMiqVkMWVrfUh:HnNukMWVr8h
MD5:	79F2D634CE67570918939DF10A075576
SHA1:	BA47B7DACB11250F9B1B3974B34954B188E3ECAD
SHA-256:	D10C94B6CDB747904BAEE9070F003BB45849DA46F8100B1320F286C21CBCAAA1
SHA-512:	155FAB1EC68F300DDCB948D024995539C721A2AB0FD89C220F0EFFA68C3863507CBEF806F087F5C84EAB38D4C53DA94BC893894E8FC9DED388DACFE3244E18E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NREUM.setToken({'stn':1,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\aa6e0ec721[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\default[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 158 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4301
Entropy (8bit):	7.933099795148911
Encrypted:	false
SSDEEP:	96:DJsJ9I1DId7LovB7A/LIVh3wJSRhRAnGn6pfQDEk/3o:W77L2t6InwmgiyfQto
MD5:	7EDA9EC93D911B48A77B18FFAD77F7DC
SHA1:	1678B6CC7973C764289783D63A7797E1AE85DA99
SHA-256:	00BAB0371C61890A7EEEF86A0C1F0E4F037861C02E78EB1BE127CA00288F91E4
SHA-512:	7A6DF695ECFFE124E066672548AEBA8CD5E88140B5C2DA80153825544A6F44350A966A8006716076FDC972B778533268EA28033ADDC5446C3338668A047E71B7
Malicious:	false
IE Cache URL:	http://https://images.typeform.com/images/HzxaK5qZrKPU/image/default
Preview:	.PNG.....IHDR.....0.....pHYs.....~.....IDATx..\.tU..b-3N.. :...A..$..r.....Z....-.[.....,SWK[.T..U..Q;L....F^..IHB.....$ ...#$.....o....%..W.....K...K...K....)..L...]..q .e.3s(..5.3.u..M.....W.....l....A.?...iG..VebB~:.!.{.y.e...t..^.Y..".o4ec.A.J.....t}wS.Kj.....]i.R.t..8. ..5d.W.al!....[..a.a.....?..u).*-.....J;R.\....).....<..M.\..o....[.b..r<...%....D ...go....m.b...?..lY....z:.t.H....w...Ui].U* ~...h..2.O.{q{.._.....S].O...s..>....T...W`.U.4J.b..C.EY.EO.....1....F/.z..... .z.f...d.?p!>'..c.....*&..4...>.....i.O.....t-...0.....c...e{.....^.\.. ?..+...s...xZDY.....~.. .q.j...../.....#..Dc....[..g....V...>.X._.a.....9.z.....L..F.n.j..g...'...J><.`E....Vn..'..$.g^....`...#..e\o.x.16..a. .:.....E...t ....xjI:FuzYA&n4..c..K.....A<X..q+3p.... ..NOw.o.p....ka...v#.5.....s_.~&.v.hn..(.yW....0`Y:..H.`..._....pw-.o.....:U.....{.g.#..0f.A.....).O$D.(.w[.c.Y.>#..lx>...t.N.....7...7.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\qjFrxD7r[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	124165
Entropy (8bit):	5.3813477847900675
Encrypted:	false
SSDEEP:	1536:ZYzPhzpZaX8ynI1Z4tG81pMH/+eA/7D5GccKppVCJ05n1aqhbElGhnLd71UDWfef:ZYzVl1CIKp7eDFnQyV8kAhvzwqy
MD5:	5F8E3CF84B81846FED1820FFAFE7F8A4
SHA1:	D5E2F76505D5F3625E46EF2DADECDB8E81AEE387
SHA-256:	2D5A929E571DDDE99947D402D2B823BEE42CA062A4C32735475B9A0848FF6F32
SHA-512:	0D635EFDFB564F64EA5085BF1D58AD09816E8509080B186804CD57982B2D7A9A6A310FB32E43AFC895337405089067164EA4ECA1F3710F3CA555844E6797A07E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_25, Description: Yara detected HtmlPhish_25, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\qjFrxD7r[1].htm, Author: Joe Security
Preview:	<!DOCTYPE html><html lang="en"><head><title>MICR0S0FT 0FFICE 365 - MAIL</title><meta charSet="utf-8"/><meta content="#434032" name="theme-color"/><meta content="width=device-width, initial-scale=1.0, viewport-fit=cover" name="viewport"/><meta content="Turn data collection into an experience with Typeform. Create beautiful online forms, surveys, quizzes, and so much more. Try it for FREE." name="description"/><meta content="ie=edge" http-equiv="x-ua-compatible"/><meta content="yes" name="apple-mobile-web-app-capable"/><meta content="noindex,nofollow" name="robots"/><meta content="no-referrer-when-downgrade" name="referrer"/><meta content="#000000" name="msapplication-TileColor"/><meta content="https://public-assets.typeform.com/public/favicon/browserconfig.xml" name="msapplication-config"/><link href="https://public-assets.typeform.com/public/favicon/apple-touch-icon.png" rel="apple-touch-icon" sizes="180x180"/><link href="https://public-assets.typeform.com/public/favicon/favicon-32x32.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\aa6e0ec721[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	4.6050684780693905
Encrypted:	false
SSDEEP:	24:rCUcWh0sEimVM4mVMyljyAV28EFySd8/k+C2E93vjqF4IAr4:uUjEiV4VtLV2lFjq29vjNRr4
MD5:	73C70B34B5F8F158D38A94B9D7766515
SHA1:	E9EAA065BD6585A1B176E13615FD7E6EF96230A9
SHA-256:	3EBD34328A4386B4EBA1F3D5F1252E7BD13744A6918720735020B4689C13FCF4
SHA-512:	927DCD4A8CFDEB0F970CB4EE3F059168B37E1E4E04733ED3356F77CA0448D2145E1ABDD4F7CE1C6CA23C1E3676056894625B17987CC56C84C78E73F60E08FCD
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm
Preview:	.<!DOCTYPE HTML>..<html>.... <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>This page can’t be displayed</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:getInfo();">.. .. This page can’t be displayed .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct. .. <li id="task1-2">Look for the page with your search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	1069
Entropy (8bit):	7.54915864947209

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon-32x32[1].png	
Encrypted:	false
SSDEEP:	24:pym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02Efl9:E0v9PoQ5VqKwspEeT
MD5:	4A35A27936C43081F0865E2E603DF15D
SHA1:	A6D584D829C87EFF74C08F770CD2EF78EE75742E
SHA-256:	DCAE3697C63FCB6AE03D2FD99FB96AF8B14848B71A259ED2E05DBCF5CEDEA5B2
SHA-512:	5DB18A7D2A60BD729F6F12E8A9B05F7A15E90C68CF3415993E8A5B1DB2B5BBA0D4B34B3F2A989E47C7495B9CF202703F0E50694E8865B0784A88EC1A40AF878
Malicious:	false
IE Cache URL:	http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\.W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ...._.X...T.Z.f..S.{.#..{...Op.Y.87 ..X.9...[.,.$..Z\|oV{..c.\|#_c.. ....!.0..t.gs...X{c..6G.X.9....".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q......./L.2..2.x.Qj.....9 .$-.e88... ..G.YF.G....b.C.[%.u..c... q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>. .GE..8.....[r.9C/...d;.PH....3.m....[._ .....%tEXtdate:create.2021-01-04T13:10:14+01:00yu.}...%tEXtdate:modify.2021-01-04T13:10:14+01:00.(g....WzTXtRaw profile type iptc..x.....qV((.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\nr-1123.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	24380
Entropy (8bit):	5.3039076589847856
Encrypted:	false
SSDEEP:	384:yNeRyajOhmUdGa4PFaOy0hGF1Ux9EmiwbikgkYPMvFzoUMC0GPwi5MteM7gN+u:yNP0HgGa4P7x+XM9zoJmlGtGN+u
MD5:	7FFB242072196E9DB5F4F1BFBFA2ED7D
SHA1:	6CFD443F06C2D4E96E14765E045277B67DA0EEC5
SHA-256:	94CDF5B7F868883DE0E1248CD80B42DD84E3F38685F2B234747550C02190DC82
SHA-512:	371BCC019D60EDBC2DD331F379AC46951B6D8E50FCA25FC79062C02F4E78A6B41DC884C590FD2E8F47EDE8BC392F3A84B0CFE102386282504538BFD157848B
Malicious:	false
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1123.min.js
Preview:	!function(n,e,t){function r(t,i){if(!e[t]){if(!n[t]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(t,!0);if(o)return o(t,!0);throw new Error("Cannot find module '"+t+"'")}var s=e[t]={exports:{}};n[t][0].call(s.exports,function(e){var o=n[t][1][e];return r(o||e)},s,s.exports)}return e[t].exports}for(var o="function"==typeof __nr_require&&__nr_require,i=0;i<t.length;i++)r(t[i]);return r}({1:[function(n,e,t){e.exports=function(n,e){return"addEventListener"in window?window.addEventListener(n,e,!1):"attachEvent"in window?window.attachEvent("on"+n,e):void 0}},{}],2:[function(n,e,t){function r(n,e,t,r,i){d[n]||(d[n]={});var a=d[n][e];return a||(a=d[n][e]={params:t||{}},i&&(a.custom=i)),a.metrics=o(r,a.metrics),a}function o(n,e){return e||(e={count:0}),e.count+=1,f(n,function(n,t){e[n]=i(t,e[n])}),e}function i(n,e){return e?(e&&!e.c&&(e={t:e.t,min:e.t,max:e.t,sos:e.t*e.t,c:1}),e.c+=1,e.t+=n,e.sos+=n*n,n>e.max&&(e.max=n),n<e.min&&(e.min=n),e):{t:n}}function a(n,e){return

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\qjFrxD7r[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	124165
Entropy (8bit):	5.3813477847900675
Encrypted:	false
SSDEEP:	1536:ZYzPhzpZaX8ynI1Z4tG81pMH/+eA/7D5GccKppVCJ05n1aqhbElGhnLd71UDWfef:ZYzVl1CIKp7eDFnQyV8kAhvzwqy
MD5:	5F8E3CF84B81846FED1820FFAFE7F8A4
SHA1:	D5E2F76505D5F3625E46EF2DADECDB8E81AEE387
SHA-256:	2D5A929E571DDDE99947D402D2B823BEE42CA062A4C32735475B9A0848FF6F32
SHA-512:	0D635EFDFB564F64EA5085BF1D58AD09816E8509080B186804CD57982B2D7A9A6A310FB32E43AFC8953374050890671 64EA4ECA1F3710F3CA555844E6797A07E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_25, Description: Yara detected HtmlPhish_25, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\qjFrxD7r[1].htm, Author: Joe Security
Preview:	<!DOCTYPE html><html lang="en"><head><title>MICR0S0FT 0FFICE 365 - MAIL</title><meta charSet="utf-8"/><meta content="#434032" name="theme-color"/><meta content="width=device-width, initial-scale=1.0, viewport-fit=cover" name="viewport"/><meta content="Turn data collection into an experience with Typeform. Create beautiful online forms, surveys, quizzes, and so much more. Try it for FREE." name="description"/><meta content="ie=edge" http-equiv="x-ua-compatible"/><meta content="yes" name="apple-mobile-web-app-capable"/><meta content="noindex,nofollow" name="robots"/><meta content="no-referrer-when-downgrade" name="referrer"/><meta content="#000000" name="msapplication-TileColor"/><meta content="https://public-assets.typeform.com/public/favicon/browserconfig.xml" name="msapplication-config"/><link href="https://public-assets.typeform.com/public/favicon/apple-touch-icon.png" rel="apple-touch-icon" sizes="180x180"/><link href="https://public-assets.typeform.com/public/favicon/favicon-32x32.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\renderer.0f5a683b381b67dbbf89[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	547595
Entropy (8bit):	5.364917573850198
Encrypted:	false
SSDEEP:	6144:6dGbloGH/Oj9iAv4FulWwPfqz+5Z/jaZ6ZTDOY3hiuXrlx:4JpjfPZJeY31x

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\renderer.0f5a683b381b67dbbf89[1].js	
MD5:	0D4FA25B79D12FA4DFF120ACB7069AF8
SHA1:	A28C700592908992B0489B6CE9B269DDEC2860CC
SHA-256:	BC722206827BE6DA76A00C5B6362D0663B14264B9AFD0AFA672FED1E7E20DA85
SHA-512:	4EC4D441A31F69817F9A88C9B6B6CDF678D05AF8C21D79980543D9E10770972C24187234754DDC577EF634A1D189EC1FD74074827DA15CCAEF9ECC553B6ABF
Malicious:	false
IE Cache URL:	http://https://renderer-assets.typeform.com/renderer.0f5a683b381b67dbbf89.js
Preview:	window.renderer=function(e){function t(t){for(var n,o,i=t[0],a=t[1],u=0,l=[];u<i.length;u++)o=i[u],Object.prototype.hasOwnProperty.call(r,o)&&r[o]&&l.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(c&&c(t);l.length;)l.shift()()}var n={},r={3:0};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var i=new Promise((function(t,o){n=r[e]=[t,o]}));t.push(n[2]=i);var a,u=document.createElement("script");u.charset="utf-8",u.timeout=120,o.nc&&u.setAttribute("nonce",o.nc),u.src=function(e){return o.p+""+({0:"blocks-matrix",1:"form",2:"phonenumber",4:"vendors~attachment",5:"vendors~blocks-ranking",6:"vendors~form",7:"vendors~phonenumber"}[e]||e)+"."+{0:"0544beec0e1a4e11a24a",1:"9cd5d6381506e5950fe0",2:"6ea5ec50b9fa21e816ff",4:"6e37d3fcdf703c1517e1",5:"f8aee16223a106724ea1",6:"965f5dedbb854e83c6c8",7:"32d78847

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\LnkQ4hGmxTTD[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 131 x 109, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11245
Entropy (8bit):	7.975358433194237
Encrypted:	false
SSDEEP:	192:mbz+31SP85NJJDasl02Sj6cPXana59Wh50KH83Yh7Ewnp4Un5To75yhoEbN:ONIlSB/aabCeHSEwnp4UnpoFhEbN
MD5:	9936A0F33BBE88F448A1E166B8CCD4A9
SHA1:	EBBE8544383B73EB0C8BA6733B3588F7781B5B23
SHA-256:	B0CF2B3D20750F69559365B1926CA243502BE1E58EFBCB45E8315C943BE1BCDF
SHA-512:	58BD2ECF7E1DADBC96DF63B01595C5B8E5E9301B5AC55645B6F36C4B831F39E89375476076CCCC20204B53960C153FBF1103710A74DC41EEBC23C5ABAD58140
Malicious:	false
IE Cache URL:	http://https://images.typeform.com/images/LnkQ4hGmxTTD
Preview:	.PNG.....IHDR.....m.....+.IDATx..].x.U.^.H.d..f..l(b.....`.....)...g..SJ...M.....bGQ." *.;**...M#$.....L.....s.Mvgvg.{.{.s.....V.....'.YR.s..?-e..V..t.....SE0..%...V..e.....-.....r.[..=_..W.....(.g..KC.....[...8.X..;`S .U..=.('.....S,..Z..Gq.....,..W...p._...o.?.>....c....?.....A....Q..].s....+..^*..NOj..Y....%..3.&.n.....b..0...B.....!$G..rN....+.r..tL...M.(.{XY..*.F6....]RY....Y..XS=9$..k...k....$.....S0.'c.~.....|.z.....*.A..)..._.#..QN....&.....P.U8..%.vM+....B..1.?..UP.....3..f.....J.@.h....xc$..5...a>~....1..&.v^... ....*f....5.C3.g.).c.#...|_J.....Z.jWO.f...9w.q...o(...&i%L....#V.|.,..4M@.W..ZQ`.P..T.....5K...w..}.Jsj.ZR.W`x.f.3.\....C.J.*.*R...g..S2.qx...&N.yr.B...0..'.....,....`:0A..%.\.A^%fa.....y}.+..6i..fx..d..8..).e@..Uk.}...S..M8..}.:.Qk..K.S...[...H.T.Bh..i..\'..%..$Q..W....el.....ru..._....ySy..t..ZR..b.V.:.M.....`:.9.L[.V...Mu...U.7X.....3.G..9.....Z....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\analytics.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	356061
Entropy (8bit):	5.3421494353818195
Encrypted:	false
SSDEEP:	3072:X0GSREKFgJ8O0W8U2CtdZsE0nlZSfFp1Jv36yMtkcJsh+qykB:kGcEcfCtdZsE6lk7IuuC
MD5:	C972CB2152B4CA69E1AD84AD369E5D49
SHA1:	2D408DC4AA2394089E145D4619793835A5745AB4
SHA-256:	18FBDEDB7C4B401C5FFA1A76F429FEECEC9928679D485A0CE3F2EA90F709B61E
SHA-512:	3F3294A19D98A64C76929F3F098982B210D83E2FD55487B0B05010D5E073633770C697773682FE053A015CBAD3F316DE2211948F8D5DB2A0974E95BCD09D4FF6
Malicious:	false
IE Cache URL:	http://https://cdn.segment.com/analytics.js/v1/9at6spGDYXelHDdz4r0cP73b3wV1f0ri/analytics.min.js
Preview:	!function(define){"function"==typeof define&&define.amd&&(define=undefined);!function(){function e(t,n,o){function i(r,s){if(!n[r]){if(!t[r]){var u="function"==typeof require&&require;if(!s&&u)return u(r,!0);if(a)return a(r,!0);var l=new Error("Cannot find module '"+r+"'");throw l.code="MODULE_NOT_FOUND",l}var d=n[r]={exports:{}};t[r][0].call(d.exports,function(e){return i(t[r][1][e]||e)},d,d.exports,e,t,n,o)}return n[r].exports}for(var a="function"==typeof require&&require,r=0;r<o.length;r++)i(o[r]);return i}return e}()({1:[function(e,t,n){"use strict";var o=e("@segment/analytics.js-core"),i=e("@ndhoule/each");t.exports=function(e){i(function(e){o.use(e)},e);return o}},{"@ndhoule/each":32,"@segment/analytics.js-core":76}],2:[function(e,t,n){(function(n){"use strict";var o=e("@segment/send-json");t.exports=function(){for(var e=!1,t=!1,i=/.*\/analytics\.js\/v1\/([^/]*)(\/platform)?\/analytics.*/,a=n.document.getElementsByTagName("script"),r=0;r<a.length;r++){var s=a[r].src,u=i.exec(s);i

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	8714
Entropy (8bit):	5.312819714818054
Encrypted:	false
SSDEEP:	192:xmjriGCiOciwd1BtvjrG8tAGGGHmjOWnvyJVUXiki3ayimi5ezxiV:xmjriGCi/i+1Btvjy815HmjqVUXiki3g
MD5:	3F57B781CB3EF114DD0B665151571B7B
SHA1:	CE6A63F996DF3A1CCCB81720E21204B825E0238C
SHA-256:	46E019FA34465F4ED096A9665D1827B54553931AD82E98BE01EDB1DDBC94D3AD

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\httpErrorPagesScripts[1]

<table>
<tr><td>SHA-512:</td><td>8CBF4EF582332AE7EA605F910AD6F8A4BC28513482409FA84F08943A72CAC2CF0FA32B6AF4C20C697E1FAC2C5BA16B5A64A23AF0C11EEFBF69625B8F9F90C8I
A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>res://ieframe.dll/httpErrorPagesScripts.js</td></tr>
<tr><td>Preview:</td><td>...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function expandCollapse(elem,</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\large[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	283919
Entropy (8bit):	7.970997679074108
Encrypted:	false
SSDEEP:	6144:DNmdUglMt7+XF0CDk8tZcIlpatPG27ZGAOl93b/myKU:DwrlMt7+XFXD9Z/paRGSZGnOXU
MD5:	0554F0D0A177ACFFDF74BD226B654D77
SHA1:	DB298AA8FA59397323F8ABC0D91E12F64E298988
SHA-256:	FF6D65827CC40A27DCAE15A090D56D3FB38536A3B76A3ED62732C86EC6F05AB0
SHA-512:	6EA26FF4BACBF426B403E1FCB19D5B17913B0560EF81AB937AECC9D55F6941DEF849C7506AD40A46F0E3DC77ABB53FEE5ABC6C5EC18FC084000829A6A1BD9 7D6
Malicious:	false
IE Cache URL:	http://https://images.typeform.com/images/m9zWqYibLnGK/background/large
Preview:	.....C..................................%...#... , #&')*)..-0-(0%()(...C...........(...((......8...."......................................G........................!.1AQ."aq2.... #BR..b.....$3r.CS.%4c..D...&Es.............................1.....................!..1AQ"a..2q.....B....R#.3............?..U]J..<..R.....T.1.,1@:0.rF..H.6..g;.DFLQT.T...W6.. ...*.P..1WQh.6.w ...f....a.....J...R..*T.@J.*P..J.A1S.u1P..J.(....J.T...A*T.^*..U.&*.W.,P....X.T2...j.Z.@V*.TU.Z-......QO....c..4R.>.b<..1R.JP(.}j.;b....S.....b.q.Ed...j..sQ.9..dr.).S...T.c?.G.02.... {5[e.....j....F.....:...M....5<:......j.(..zV.....K-...V.7.........J...0=.b...U....^*......Ai...K.,.0.k..W........S.G.V.....R...9..<<uZ.=V...z..*i=........z-M.J...).....M...S..*.C%`T.^(...J<U...*.S. .b..zh....,U....D.X.x...J=5x...@U..Uy....I..&.....F.S.A*.P.:..WR..UJ.x.R..W...&*Qb.(h.*.T..1P..Q.@LT.]J.&*T.@J.*P..J...R....UGC@UJ:..%J.(.R.J.*.]J..XQT...L).8..t..@)..).)l*..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\urlblockindex[1].bin

Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2...........

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\aa6e0ec721[1].gif

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075E 4E
Malicious:	false
Preview:	GIF89a.......,..........

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3470
Entropy (8bit):	5.076790888059907
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRHERyRyntQRXaR8RS6C87a/5/+mhPcF+5g+mOC53B5Fqs1qP:JsUOHaQyYX4yJQOWCbz1Qb5
MD5:	6B26ECFA58E37D4B5EC861FCDD3F04FA
SHA1:	B69CD71F68FE35A9CE0D7EA17B5F1B2BAD9EA8FA
SHA-256:	7F7D1069CA8A852C1C8EB36E1D988FE6A9C17ECB8EFF1F66FC5EBFEB5418723A
SHA-512:	1676D43B977C07A3F6A5473F12FD16E56487803A1CB9771D0F189B1201642EE79480C33A010F08DC521E57332EC4C4D888D693C6A2323C97750E97640918C3F4
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "The security certificate presented by this website was not issued by a trusted certificate authority.";..var L_CertExpi red_TEXT = "The security certificate presented by this website has expired or is not yet valid.";..var L_CertCNMismatch_TEXT = "The security certificate presented by this website was issued for a di

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23(B
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.I...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\form.9cd5d6381506e5950fe0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	227059
Entropy (8bit):	5.280936780615679
Encrypted:	false
SSDEEP:	3072:5hjrDWVbCG3oaMZ7wLNM5NTM20ZPL4BrWN0QzFI+VDvoDa9f:6Vb0aMsQlMBPLUr58dDvsm
MD5:	DD7F1393ACBF039DA8D9970914488D42
SHA1:	6471C4824923D895CCE1D956F1D93CC6C57AB9EF
SHA-256:	3DF9AAE60EBE3300471A343673C3771D554934DDA473CE495CD0539AEF8872A0
SHA-512:	C3E97929DABD62E75D54C47E5D6E59630407FF1FEA5BE94D4B2C8BC131541FAD1008D99294FE39887C468A951B951C0A4C2BF32DEA33901BEF1296CB336061F
Malicious:	false
IE Cache URL:	http://https://renderer-assets.typeform.com/form.9cd5d6381506e5950fe0.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[1],{236:function(e,t,n){"use strict";n.d(t,"a",(function(){return o})),n.d(t,"b",(function(){return a})); var r=n(10),o=function(){return{type:r.t,payload:{}}},a=function(){return{type:r.F,payload:{}}}},237:function(e,t,n){"use strict";n.d(t,"b",(function(){return o})),n.d(t,"a",(function() {return a}));var r=n(10);function o(e){return{type:r.A,payload:e}}function a(e){return{type:r.z,payload:e}}},238:function(e,t,n){"use strict";n.d(t,"b",(function(){return je})),n.d(t,"a",(function(){return Ee}));var r=n(80),o=n.n(r),a=(n(158),n(117)),c=n.n(a),i=n(3),u=n(26),s=n(75),l=n(6),p=n(505);n(442);var d=n(150),f=(n(24),n(506),n(507),n(6 08),n(20),n(13)),b=n.n(f),m=n(615),h=n.n(m),v=n(609),g=n.n(v),y=n(2),O=n.n(y),j=n(225),w=(n(22),n(29),n(472),n(84),n(208)),k=n.n(w),x=function(e){var t=e.split("-"),n=b() (t,3),r=n[0],o=n[1],a=n[2];if(!r||!o||!a)return!1;r=r.padStart(4,"0"),o=o.padStart(2,"0"),a=a.padStart(2,"0");var c=new Date("".co

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vendors~form.965f5dedbb854e83c6c8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	418096
Entropy (8bit):	5.702124589125958

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vendors~form.965f5dedbb854e83c6c8[1].js	
Encrypted:	false
SSDEEP:	3072:hO203o4PRjCe7bmD2NF1q2ZG8njVKG85sLGU115ZZQjOurJgR8rrjoP7Gwc4/:hUCkbm6r1q23nkGEsLGgt0a5PKwB
MD5:	6F33B62669DF8B6E094E941BB2F1BB39
SHA1:	D2A46B58E82E30176BDAF55CD018FC89AB9F0C23
SHA-256:	645A6486495927D9FC72EDF35C46B50C990F3DCED2101C79F753F6FA8EC11E16
SHA-512:	D0BDB5C7E927C49908667D60B967D75A0D3D7E05FE09A1F24ED13C2F7E411B6D9B57E140CDD7FE742F3ED7A6364EE6AEB8FC1DB1116364F3B6309A4DE30FC 82
Malicious:	false
IE Cache URL:	http://https://renderer-assets.typeform.com/vendors~form.965f5dedbb854e83c6c8.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[6],Array(429).concat([function(e,t,n){"use strict";n.d(t,"a",(function(){return R})),n.d(t,"b", (function(){return v})),n.d(t,"c",(function(){return A})),n.d(t,"d",(function(){return q})),n.d(t,"e",(function(){return I})),n.d(t,"f",(function(){return H})),n.d(t,"g",(function(){return K })),n.d(t,"h",(function(){return P})),n.d(t,"i",(function(){return D})),n.d(t,"j",(function(){return X})),n.d(t,"k",(function(){return re})),n.d(t,"l",(function(){return ae})),n.d(t,"m",(fun ction(){return ne})),n.d(t,"n",(function(){return ce})),n.d(t,"o",(function(){return M})),n.d(t,"p",(function(){return j})),n.d(t,"q",(function(){return L})),n.d(t,"r",(function(){return F})),n.d(t,"s",(function(){return N})),n.d(t,"t",(function(){return le})),n.d(t,"u",(function(){return ee})),n.d(t,"v",(function(){return Z})),n.d(t,"w",(function(){return J})),n.d(t,"x",(funct ion(){return z})),n.d(t,"y",(function(){return oe})),n.d(t,"z",(function(){retur

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90BCE4B8.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 816x1056, frames 3
Category:	dropped
Size (bytes):	65057
Entropy (8bit):	7.714453186203319
Encrypted:	false
SSDEEP:	768:WbZakMgV6yb0BGmdBGAUx3BZP3tUL4dbsaPaVOZIBeSGrS0GUysJEWznmkXHGdhc:WQbgQywBGmkla+bsaCaWyVvXmkXwhH8
MD5:	89776C76604B8117DFD73CA3604286AB
SHA1:	097D88821166432D9C8EF52CF807353BCC34952F
SHA-256:	5F43444269E5E9E7D1B94660AD93B9CCFED6622A1D415BDE414D478526A3F5D2
SHA-512:	68C2826235479DC52C10A6EAF078BA3FA0D77120517D608A69349258F5C3646382431CCDA4AEEBCA1026EE877AE180F06E44E6FDD6888681C660D053EA3427B
Malicious:	false
Preview:	......JFIF.....`.`.....C...C.. .0.."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..S..(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Temp\~DF5AD0E20F440D8F8C.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	1.3765045529971895
Encrypted:	false
SSDEEP:	48:LykGwYQv5fGPBYwjqIj6GyYOjG0cxv0ldlQ:LyUv5KOI2S
MD5:	DCA6B45C7185E6152666C461C9E5333E
SHA1:	C803CDFBB15EA0C2E94B8AE760A8C1BD2BEA1FD3
SHA-256:	A48DBE386C1EF345F94299D6D7E990A4E956515EC82A6EE41E6BBF25292C9899
SHA-512:	C7268FCAAA65DD31BE8BF4213EF3CE303B8A7C140BF0F37BA97C89F37B21120A566A67CD80D5CB49AD65A9EA7BB423B515476719E830E900376F7D4C7F589C 5
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....@6`................K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e...........8...X... ....

C:\Users\user\AppData\Local\Temp\~DF72A7006BFF98A571.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.9013103102456824
Encrypted:	false
SSDEEP:	48:LysBoFU03P11zv7FU03P11CxmLFU03P11IwfqU03P115SaSGqU03P11IasNU03P/:LyG4PrvfP64PPQwOPRSaSfPQlLP
MD5:	908775B0538E4C929A9E8A8D4DE99563
SHA1:	944B3EC24C23A59DB836D7C47FBFFF3004572B80
SHA-256:	80C326A69D6DE95AF047018A759638CB8618DF209BF760CD006A80450CBFD8FB
SHA-512:	894C06F633D1C262273F9D1621788D98CF000823C080478AB9948E702B3D2BF9CE90E346FC932F1AAD3FA5F7AE20C27A4E75F8A8F1EAD20334E1F5F4FF3DB5C

C:\Users\user\AppData\Local\Temp\~DF72A7006BFF98A571.TMP	
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....M.I.C.R.0.S.0.F.T. .0.F.F.I.C.E. .3.6.5. .-. .M.A.I.L.....@...`1.....D...h.t.t.p.s.:././.p.u.b.l.i.c.-.a.s.s.e.t.s...t.y.p.e.f.o.r.m...c.o.m./.p.u.b.l.i.c./.f.a.v.i.c.o.n./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.....%... .....D...h.t.t.p.s.:././.p.u.b.l.i.c.-.a.s.s.e.t.s...t.y.p.e.f.o.r.m...c.o.m./.p.u.b.l.i.c./.f.a.v.i.c.o.n./.b.r.o.w.s.e.r.c.o.n.f.i.g...x.m.l.....&.....1SPS.....F....'.....! .....@.....8`.....=.....B.....p.r.o.p.4.2.9.4.9.6.7.2.9.5.....(....@...`1..... ....

C:\Users\user\AppData\Local\Temp\~DFAB08615A49F50372.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	1.4017618013955384
Encrypted:	false
SSDEEP:	48:LyJGQyv5fGAlSiqIi6GUlsiVrt4t5Nwrn0ND1wD1o:Lyiv5K5lcVq2
MD5:	6A48DE1CE1B04447581C81C3C045DA66
SHA1:	A53E1B15729871DC8FF0522576BA76DD4E265031
SHA-256:	3DBD9FD45978C943376C35EDE626B08715BA29624518A806ACB9E7280566B575
SHA-512:	68011EA3B9E45E81EBBBC1D194E6A5B4A22A97C90453F8D4AC96D79E82365F74AC63EF0213B66DF3BF1DB40926C3FF1B0C862DA66E5A468665008AF7B1F37C17
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... cU;`.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFBC05D677CD36F01B.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44961
Entropy (8bit):	3.157336566829594
Encrypted:	false
SSDEEP:	384:LyhvA9o7VVPd3mKW94VjdMq1o9I7U4igUvQUBgluLm2s3LZAgGdzm2s3:Dvzc1rGy
MD5:	C661F58B750B81690852B2782DCEB56A
SHA1:	91504FB6E6CCF25CDF87E56071857D6335C0735B
SHA-256:	2701AA67281CFA4F3F6457CE2C7BCCF72F2E63E102569A861DBC305B8DF27A49
SHA-512:	46DFC0CE6B641472B05B02B0CD7C718F969514DB526A2F34ED67423DB9EF63CBB706A0BAA303B3A0F2D687A18C388BB7EFBB71FD88DBD83D0E2F417C0B7EC19
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....L6`.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFC448DC16F91BBCE4.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35359
Entropy (8bit):	1.1854320418886954
Encrypted:	false
SSDEEP:	96:Ly0v49hhZhwGhueGhuEhughuSP2hu0huFPshuRhuRPS4UZi:Ly0v49hTTovoEogoS+o0oF0oRoR5U
MD5:	B2A96A94A41020A71A601AA87BA593C5
SHA1:	4A4A86D74CF35724D9E5BC4C335FE5BDE6FA7AFA
SHA-256:	A18FB56D5BE642CFDABE1813D43A7E4ECB382DA436DF615873FDDE0888F0860D
SHA-512:	07E4F47DFF8D03C094EA07C4EEF97D7828E23B9A22C8391C660242F470BE21CC6662D096D5FCB07BFCE323443DA3231D5746DF10DA917E58EC37925343C5074
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....f;`.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\3QCZ05YH.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\3QCZ05YH.txt	
Category:	dropped
Size (bytes):	427
Entropy (8bit):	4.731775598417146
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjw2aTVbpeA:hr/JqLDGSPIZJwx1gw2ceA
MD5:	AA8A30722B18ECC2031DE8E47FBE6E83
SHA1:	FE0E69433573669822850618 9EDD8B02669B4081
SHA-256:	3521BDF58E8163C91D86E48DA9EF9CF387DCD886941633E523C2CBED785482DA
SHA-512:	AFAB2541C34355BF4B86C8CD7BE4D78B13E7960BA50F346A4A1CAC8A4F95E48913E62B54C3BAC4256100A07068556E17157A39EDEFD21C542411BDFB335D57E9
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs%3Atest.true.typeform.com/.1600.3044522880.30935345.1027795901.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\440HZ239.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.725907942101141
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVtf:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTP
MD5:	C57D8D504C7BF71DBAABD442FCB00D1D
SHA1:	EEFE62257A38B0FA3C1A46C3B822FF7D3E514F5C
SHA-256:	08F121EB1AA1F6C17EB6C7FA4B00B4C203BEE712031F97E1C8431F1B039FF053
SHA-512:	3F4CEE911D605512DB8DF892EC4DEADAEE10EC264680A46BEED1157F8060C0CF323FE06B34B7CFE6AB3105406CDE058F31F09432E9E8E21B0D5BE59CD0886225
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2974522880.30935345.952089748.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\4AQZ4AVS.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\4PKDOOYM.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	4.723507985939382
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVD0:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTa
MD5:	70DDA74A63DBDBDEF67BB79D81B50E15
SHA1:	ADB475C8AA7B6D17A7BC041DAE40C45C1567C6F1
SHA-256:	71B68D89524261CFBAD1919843B26D2B8809E14963857A242984A329B65A54F7
SHA-512:	41F6BB94403E4C3E13CAAEF8103C4EC4A6BB5BBD7AF2ED2C618BE059A2B85F819EFE4DF1C1108FFE97E35663F2D50BF4FCB32CF5A8EA125050BC394EC22F34F
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\4PKDOOYM.txt	
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3054522880.30935345.1035297927.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6VKINCBQ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	4.723225438230034
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTV9t:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTF
MD5:	D384057D3BF13C341768EA9877AFCA58
SHA1:	6D6C1B63881EB5A340E0038C70FCC8A41F25CB25
SHA-256:	6E8DE92360EB6A34545E2D8E81E1D8FEC1D6DE09F92A84939EC2C35A47B8980B
SHA-512:	FC28C597138757E213C91018A8263BA25F5EDEEAD2246239AFC5A4E809DDB1F57FF1B4554A33ECFC01986A17087593B43DE979043373EB3E2E4D1D1161C8C5C
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3084522880.30935345.1062441975.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\84PIV8PN.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\8WEWASYB.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	433
Entropy (8bit):	4.703698026330058
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVWdddIUaTVbzd:hr/JqLDGSPIZJwx1hddRa
MD5:	769CBF5A34CD8CA012A218FFA99BCF5B
SHA1:	94D624D3A06206B5E17C97DCC5703B8852D5D393
SHA-256:	C0C4B19B6D1D3279568EAE1BDFC443348D558FD6D4BE05B4CA8C333584D87FB9
SHA-512:	5284F0FF67AAF01C2EB31ACBF98C3605345C9C0AC56D9D0155935C50D4AF65BEAC192B6922916A33B8FB85C42E34BCDDAC797BE1198EC22D80A5725D62EBB395
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3054522880.30935345.1028420910.30861920.*.ajs_user_id.17522027.typeform.com/.1600.3044522880.30935345.1028345909.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\9EAYE1UQ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\9EAYE1UQ.txt	
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32(
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\A3Q1GN13.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.722851007646604
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnG:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aT0
MD5:	B7BC45ED470524F6416046096CA17661
SHA1:	C13C19C8CEFD44296D21AE43B14638695A1AA7BB
SHA-256:	155F5612F569977E1163D7D3BF617FFD8A2122C0F848F08166816F655AD2D834
SHA-512:	55D82796C3842D8C88EFBD3E8491625FCB02342D905E30488A678C0A8ECEEDACD093959F69AF85032490F8E9C7FAB433A4FC4B2FA12A3A48C1AF8FD5F4044F4
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981261799.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\B61YPJUS.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	309
Entropy (8bit):	4.712603648415208
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXESNR3GZTVtcNCRYivX:KN4zX/JSCaLyQGSCzyIaTViNNaTVtcoJ
MD5:	683CEC41BF6A55D49CBD119806BDB0E2
SHA1:	03259E3ADF0A72F303FC64B78B3CB04FB4688BA9
SHA-256:	45A46E74B2B468DB360D4E559848FC021DA1A6751CF9054BC4566871680BFC7D
SHA-512:	63022D6614C47E425A3397CAEC0541E9531A3C7515E921DB0F16746415B4F07C1E2D31D04D5BD61F32B00AA64AF4273DE69CF7D4ECE99C09A2449D8B7E4FAD4B
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs%3Acookies.true.typeform.com/.1600.2964522880.30935345.943746732.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\CQZDUWDX.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	433
Entropy (8bit):	4.708016801554199
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVAKolcIUaTVAKolA:hr/JqLDGSPIZJwx1+R+
MD5:	76DEE649B8279AA2979032089DB0F952
SHA1:	3A46B3F304CD42BA37B6C9174FE0B5A9F8B3480D
SHA-256:	9E05DBC5B36ABCFD8ED21EF3C2EA9D5F51F2C657591538DE908DD113D2AD3055
SHA-512:	E6BF31ED63EC8CDF900F02EFD6B8B887B91B48D41A5DA9CDAABBA34C46EC01033D8508762E8AECD5CAF7A5DC724D155CF98EEF78A12016655747D4099ACB8B9
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3074522880.30935345.1055733963.30861920.*.ajs_user_id.17522027.typeform.com/.1600.3074522880.30935345.1055733963.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\DGJVF474.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\DGJVF474.txt	
File Type:	ASCII text
Category:	dropped
Size (bytes):	311
Entropy (8bit):	4.654196076810098
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXECqBUGZTVtcNCylivX:KN4zX/JSCaLyQGSCzyIaTViNxIUaTVt3
MD5:	F70C25D057B9A7F45708EEEEB6B83F9D
SHA1:	44D32CDB8CFFF9FE4BE65144EB6749FD6BB29A81
SHA-256:	43634EF6187003A3BF6D1296B60105841EDD1026BD3FD02F39FD61FCF19E6200
SHA-512:	1E18D6796C9E23A0AED27622F2E7991383AD140D511935B38E26D21B8C9E3ABCE7163E5A4FFAA5790BFFF523358017A2CF6E921ACDD922520753274282A66EC5
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2964522880.30935345.944058733.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EZEPC3VR.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FI67OFMM.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\G6MNA809.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.685553042877065
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXE6Wr3GZTVtcNCmyivX:KN4zX/JSCaLyQGSCzyIaTViNX2aTVtct
MD5:	50775FD5988DF6199A8971A6DBAF3A49
SHA1:	1340C1988D4F25586E93B5FAE3867BBFA514A661
SHA-256:	AA582E94AB2C1930A453483A296BBB99D760CBAC556B8CD30210D0E19082FEAD
SHA-512:	93B8DF7BB7A313AB305246827BB1E606703C036F9B998F076B3A89B5030FC0FFC85EFAC22D0B47C8A5873733E8ACD04C04EA7F0CDDF45DB01463B79B9254A4C6
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\G6MNA809.txt	
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs%3Atest.true.typeform.com/.1600.2964522880.30935345.943902733.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\GBP7WF6A.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	433
Entropy (8bit):	4.709733594494096
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVWZlUaTVAz:hr/JqLDGSPIZJwx1FRV
MD5:	A4785BF20A3DBD5749FEB5D5D9698DD7
SHA1:	A0741E90AEC6C5E7B1B20D3AEAB6DDFA45078E31
SHA-256:	78D8604F9D583C2A6CE289B7842A1E00205E89D5F44E9F9BD2E9B50F134D3E9D
SHA-512:	7A1A7A7C343D6AA7199AB259BC2D37E5B24F3B5FDB50F6303A1042A6483978BD36F3C15CDC779E60EE0C242D67B8C9F61FFB51B8D95A6069414ABF3715C6E55D
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3054522880.30935345.1035297927.30861920.*.ajs_user_id.17522027.typeform.com/.1600.3074522880.30935345.1055577962.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\GIVQW2Q2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	4.730881075160914
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjw2aTVbjQV:hr/JqLDGSPIZJwx1gw2FV
MD5:	855929C19B0D4E3A297692B133BAB983
SHA1:	E1FFE3309A2152E82B32284EA3DE1DE6FEAAC171
SHA-256:	BFC36136725B8FF9C4A5D0716C10551F252850C3E7977155DDDF66282F6CB43E
SHA-512:	48BD04DC3FE8909D16A6573D5E358760D2E880C68433796A6BD6387AB8D709083854219D98C8EDA24654A75B3CCA7C444E4D16FAA18A936F6B252A4876C20E4
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs%3Atest.true.typeform.com/.1600.3044522880.30935345.1027995904.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\GS98OH3Z.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\GXDP9IRM.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\GXDP9IRM.txt	
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\H5W6R21B.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	4.746562753246648
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjeaTVb+/:hr/JqLDGSPIZJwx1gej
MD5:	1CAEA744D6C339EF8430504D7322F7C8
SHA1:	B2F34EEDF6B68943A4CB124E99060F548EF9E17B
SHA-256:	4BD0CABBFCE76B33B6F5906F6A835542757F7FAAFEB7F7A080AE1BF5E7E588C7
SHA-512:	E0EA46989404ADA0E78289117EAE980783BEB4AEE72932EB55902CD67D211646C587F3B461E9D564DC5BDCFB2D4D0FA9450388843EBCF972BC8DBF0D1D9DC6 94
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs%3Acookies.true.typeform.com/.1600.3044522880.30935345.1027870902.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\KF47PMGD.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	4.715387424444603
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNxIUaTVtcow6Z+x1aTVtcF9:hr/JqLDGSPIZxRUc+wx1UcX
MD5:	B10F47F28610CD1CAE9B77676C74C05B
SHA1:	D9191FAA316E3ECE143D5B58F9E7587A701F4D3E
SHA-256:	564D15F7815E964817BDDD69CC825B24BC4DE77C7E551DC3553DDA48C179A197
SHA-512:	3FF8B18073822260CB2113EB3D112DD7FB01EF1BA2E5A302B35A6D563E3B23FA01F498D0D47111DA1E6E93DBE6A6BDB95D6B43DCF13190100F8E6F9ECFFC2D 7B
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2964522880.30935345.944214733.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2974522880.30935345.951309747.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\L42YGXX7.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	4.7157040319970225
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVtc3Vs2lUaTVtc3VsG:hr/JqLDGSPIZJwx1Uc/RUcN
MD5:	F2BAFAEE7A36F593B120B0A8914DF229
SHA1:	2D1D14DCE700FA7A5ADF64047D40EC0BFF6C9C79
SHA-256:	0CFEBCF6264642A7A1C8FB4929362832B1046EBA39E2C591D7D49601B1FEB217
SHA-512:	6C7D3A6C3141EC8AA1E8D00AEE8042C68CE27BDE3923C43650B81C411011C69206F927F1333CAC7699D2A3C21E6DA258F0CFB9509436020B90932917DC0462A
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2994522880.30935345.974397787.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2994522880.30935345.974397787.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\L67IQF1E.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\L67IQF1E.txt	
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32(
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LJ7CSFR1.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32(
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\N6BBHH3T.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32(
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\O75T4BO6.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	351
Entropy (8bit):	4.7239528788670535
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTV9t:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aT1
MD5:	E540B5BC1790B191D9C52EE0FFDB52C0
SHA1:	B522C2152F161FD8B9B1F552CE0765DA5F419B43
SHA-256:	375A2C99224F5B3E25E441729E707229619E4C244940DC1F0BC76A7739389084
SHA-512:	3EE048940FB6EBBDE2FBE87241E817E4C4631883874D5722069F11905997FAADF32956F6D8CA618E7C927405794B0051114A56C235DDA2485658DF6D507CE50D
Malicious:	false
IE Cache URL:	typeform.com/
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3084522880.30935345.1062597975.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\OJSMKIWJ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	4.747264835428299
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjeaTVbdA:hr/JqLDGSPIZJwx1ge5
MD5:	4D00FDE8104542DC5EF5872DF9A90210
SHA1:	FA11B0FBB251AA3404D32E7FC96CD3A95E7C274E
SHA-256:	5430C18460F4CF085080427C36B30D0E0C1097D3F2A85B305FBBE8FB1D34DA7B
SHA-512:	8F3B37F8F6D26CCDA172390B6A812123E150F878A04B91D8C1EC8B28452721B37FD4D8BAFCA9124EEF7B17498F30E910CF5342213FFBC4694F601F18175A0B3F
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs%3Acookies.true.typeform.com/.1600.3044522880.30935345.1027945903.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\OOTH8647.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\P10TD78T.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.689644730790302
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXE6Wr3GZTVtcNCRYivX:KN4zX/JSCaLyQGSCzyIaTViNX2aTVtcK
MD5:	C3019A42FC4B3B13375CC3E95463CC48
SHA1:	7DDAB1B7D7166F44D39AA51CC2BD0997036F35BB
SHA-256:	40BC29BA8EB4A5B2F5A41C9BDFFECCCBEF95B49120A5162944B3C5B95758C5D9
SHA-512:	CC2EB51B5F69351666D849D7B964FAFC3ADAC440C5EF2080C7FC706832366ED30FBED33CB0273B92EB06D74D72985D02A99B68EB2B373D72664EFB058212985
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs%3Atest.true.typeform.com/.1600.2964522880.30935345.943746732.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\PZZYJFRJ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	433
Entropy (8bit):	4.706105325555157
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTV9ROIUaTVAKolA:hr/JqLDGSPIZJwx1/R+
MD5:	D7ECBF342A17B781875F4CB11CEC0189
SHA1:	31E3069A71508F8973C4FE078AF1B6F65AA4BA08
SHA-256:	C86F8F329315F5E92C2812D79B61B04893DE5918CF9A0166FDA97C7074F939D6
SHA-512:	D95BB858476F2870C829E8AA06DF59AD34B1908B24D2DC4C9C3BF3D3A71B14B3761FABCBF51ABC47B42DBAE4386EBA60C9FD247A1E1EF264030282BBE9CD1D7E
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\PZZYJFRJ.txt	
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3084522880.30935345.1059009969.30861920.*.ajs_user_id.17522027.typeform.com/.1600.3074522880.30935345.1055733963.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QGL92SEJ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.688110766421138
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXE6Wr3GZTVtcNCUYivX:KN4zX/JSCaLyQGSCzyIaTViNX2aTVtcb
MD5:	3C2B45D7F7A1CC9B57E991C15DAE0826
SHA1:	13BD074007855ABC6337C9C26D8B9B87EC171AA7
SHA-256:	403625A2D1B921948E3DFBC8B67119561CDDDBC69EBDB8568041E0AB1C50179F
SHA-512:	EA45C82C95F14BBC6457E5F484F12C994A9A4E96E44ED39F7371856EAEC8711C732E3150D123180E6350F38E65B277E449C7B5E05B8EBE2C33A9CACF67C77A2B
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs%3Atest.true.typeform.com/.1600.2964522880.30935345.943590732.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QLEJV3Z7.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	4.728529430443941
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjw2aTVbV:hr/JqLDGSPIZJwx1gw2S
MD5:	45DF527FEC774DEA28C0D9F0986A7A86
SHA1:	D8E888E6C33A1671551C2645EF922056C6D7664E
SHA-256:	47626505F28734E4BD77383D162B23BFE2BF8F1DCDF503BAE572B54759A14071
SHA-512:	CDA19F037E33BA3CA1E6977B468806F9483EC24C83E84882E0AB403261C1503B67F4D10394A2ABAE0C5FE6ED4DE350D0E2102BAE17CAA84945787D2D5701576
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs%3Atest.true.typeform.com/.1600.3044522880.30935345.1028095905.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QYK7T31P.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\RWRDSMGU.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.644420058103625
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXn:KN4zX/JSCaLyQGSCzyIaTViNT
MD5:	11F3C7B8DF12CF145FB1555C0F3ECBC6

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\RWRDSMGU.txt	
SHA1:	608CE34AC191D41B17684DB588D6B6A719874249
SHA-256:	DA92AAF2354C1C5906338D4925777DDDAD308DDE52C6010793BC001DD7EC7E1D
SHA-512:	CD73125125358DFC3780C7F09BC8464163F64CF1F39FB801CAE606813A39F41A46D0370B368EE38D53D0C4117B7CFA5A91DD449A54A65956D2F2ABD07014D32
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TLQ0O6XV.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	4.714106302555666
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnWxIUaTVtc3VsG:hr/JqLDGSPIZJwx1nxRUcN
MD5:	4187AB60D3BBB55D950AF742E86B74D9
SHA1:	80520753ED1A0861B12552C8F40694CAEB565905
SHA-256:	D1F764054692237D03DEFF6E6178480C18F4A6E16FAECD14D0A12CE121E88912
SHA-512:	73803BCF910058703A08F79E74F7B6A43018E2716910B2FEF4F4728C2A9674C3847E2155A4CE1E28653FF858DE4535B0DD9422291F4A3D6C83B4770F02CD32F9
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981261799.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2994522880.30935345.974397787.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\U2PP9MVW.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	309
Entropy (8bit):	4.712603648415208
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXESNR3GZTVtcNCRYivX:KN4zX/JSCaLyQGSCzyIaTViNNaTVtcoJ
MD5:	683CEC41BF6A55D49CBD119806BDB0E2
SHA1:	03259E3ADF0A72F303FC64B78B3CB04FB4688BA9
SHA-256:	45A46E74B2B468DB360D4E559848FC021DA1A6751CF9054BC4566871680BFC7D
SHA-512:	63022D6614C47E425A3397CAEC0541E9531A3C7515E921DB0F16746415B4F07C1E2D31D04D5BD61F32B00AA64AF4273DE69CF7D4ECE99C09A2449D8B7E4FAD4B
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs%3Acookies.true.typeform.com/.1600.2964522880.30935345.943746732.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\V6L4R22H.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	4.722235813978645
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVDm:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTE
MD5:	DE0286A64ED315A2397E2C217406F4F8
SHA1:	AE8EF160597279968C80A0E0D04AB525E25C5780
SHA-256:	5BBF456591DC588CB8A917CA832E58411D300D96384FF55BC3B3741382F1014C
SHA-512:	21B1E26BC0DFB5D1256794EFC03B56E8752DFB2A6C780D055CF8637CDB097E49C8A131011081FD862B2795B863ED72168F5FE37F735892C4BD6C28DD9315E36
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3054522880.30935345.1034985926.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WBLPQVYT.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	113

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WBLPQVYT.txt	
Entropy (8bit):	4.426545301008578
Encrypted:	false
SSDEEP:	3:GmM/NRGn9RMMKmv/JGGESMONdDd0cevQuOoivXn:XM/N4zPv/JGRVIacevQMivXn
MD5:	31E51082B114573A7392EC47753DE059
SHA1:	83BDD4CB26DE945701300864E8BA8B573A8C31C0
SHA-256:	01D71141E9E8539647333D3151D667DC352F6E9DBEB0276524394401B0DEF6D7
SHA-512:	5429F8B067A5DC6A7546CB058AF54BA3370A4FC6881914EC65310C0377879E74CAE892235A4DA6E1087DE6D9161C3AA6848E8F46FF7025FB5DE1D013AA60E713
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WJUVDUR5.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WWM5HRIM.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.726356737134679
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVtm:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTW
MD5:	0D438040483AD4045EC565D4735E9E7B
SHA1:	DC8AEA97AC858679F8FBC7CD0312DB9EDA20BEC2
SHA-256:	390B563DB6474933E50867C7EAE81F020F5E26A1C2002C9EA4A6F9A444E1FE8A
SHA-512:	26A6F9104FF9B51D529C86AAD8195DE57D69031BC5F8CED8449866BBF75DD92CB611EA715586A8269917BC01395CADB8F1ED18754A1ACF28BA4F217CCC05B5D
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2974522880.30935345.951309747.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\XEHEBG1L.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	4.706255696990537
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVnnjIIUaTVbO:hr/JqLDGSPIZJwx1gIR9
MD5:	341B497ECE139D2D27844A783016FB7C
SHA1:	474E34A412650786161CBA6B03433276DF22966D
SHA-256:	3AC88811F6B1612ECC1498D2290C3239DFD8A24B09661D1A1C580A8387C014AC
SHA-512:	5DF96E6F47D885E44A9E138779A3307B36C7900FB4919D9F4A656BD10805F8EEB404B2493FDC9411B9EE4E6CECC87C322B0ABDA58ECB77A00DF2D08F99F6155
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.ajs_user_id.17522027.typeform.com/.1600.3044522880.30935345.1028295908.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\XIKWRY8N.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	4.713480508059008
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNxIUaTVtcow6Z+x1aTVtcowA:hr/JqLDGSPlZxRUc+wx1Uc8
MD5:	F51517CC7E2CDF81D9760873659B1574
SHA1:	0362EA9F207ACCC54C82EA34967BB2596B87CF6A
SHA-256:	1C18058174BEE2DBDD3050AA9DEF59216ACD64DF88204FF9273BDF71A7C1D31D
SHA-512:	4696A9351E0A2486AB321D6AAA12933ACFB8CC1FCF8CFE5378136462331BD1C2D698799CBB5C4B79B91BF60AD1A93C4F90866DF6E5CAF8DEC30F537EFFD4D2AC
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2964522880.30935345.944214733.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2964522880.30935345.944214733.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y4CMWY8S.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\YW1T938Y.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	4.715400034469946
Encrypted:	false
SSDEEP:	12:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTVtcFJ/uIUaTVtc3Vf:hr/JqLDGSPlZJwx1Uc/uRUcF
MD5:	86E44791529AC5888220B2C5D3E1031F
SHA1:	EF2AB0F5FCBA322B848734C23CDB6A04793A6ADC
SHA-256:	ED7AD01DBE0C284F6726BDDB8E37DEBB404ADD8BB3477290D42474765D1A3B65
SHA-512:	0EC7FA0F2A253A665416039A5F127404D0EC1C7E1A431BE6A31C9D8E87CF14428A56970B9B3224DF6FCB3958B6CEDF9CD38B7BB5634CFD865C7CB501C8A072F
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.2974522880.30935345.952089748.30861920.*.ajs_user_id.17522027.typeform.com/.1600.2994522880.30935345.974241787.30861920.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZX0PPYVU.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.7222821211513635
Encrypted:	false
SSDEEP:	6:XM/N4zPv/JGRVIacevQMivXEt6QGSC8hKOhIGZTVHCNDvXEkQw8Vm+xRnzGZTVnw:KN4zX/JSCaLyQGSCzyIaTViNJZ+x1aTO
MD5:	14E62DEA5FAA7F6244A57EC8494CECE0
SHA1:	7A0753511E55AF5FC55412309FF84D3FE9B75486
SHA-256:	5D601E79655A756048B1D95B33DCA7A6717A1E548D7FEF60922E338B85F0988B

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZX0PPYVU.txt	
SHA-512:	2C4E404186F6D0548EBE32EAF57204172338754449B9EAE5F07B19DB594D97D3EF355E0B0DF9FA66285B1D4BD3BB7AC396EB3289380499BD4D4A048E7A5A12AD
Malicious:	false
Preview:	__cfduid.dfe3114d464311bbd077826b3c4a7ab071610587792.typeform.com/.9729.3118114816.30867879.926408551.30861920.*.attribution_user_id.5d08959a-2522-4e74-9c1f-ec3364b3446a.typeform.com/.1601.2964522880.30935345.939960687.30861920.*.ajs_anonymous_id.%220bf607f4-babe-45e7-8a96-59d6e6d55eb7%22.typeform.com/.1600.3004522880.30935345.981417800.30861920.*.

C:\Users\user\Desktop\~$ACH REMlTTANCE ADVlCE..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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

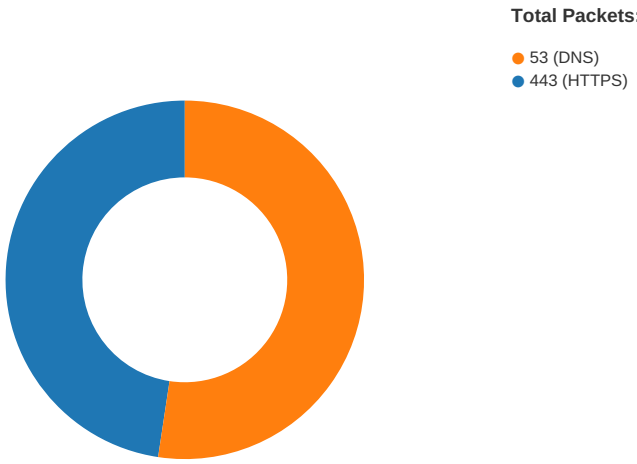
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.655219374040481
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	ACH REMlTTANCE ADVlCE..xlsx
File size:	75584
MD5:	1726734045f013554979c6c7c1932b7c
SHA1:	b6c9fb364f0bb8726be22bdacc6dc4f3acb31f7d
SHA256:	46f4cb7548dfcb39a289f186fbd4f9ed8169e1917a29de1c3492773568e5ee45
SHA512:	7b3dc863f53f0709b448b12cc4d5866847c8a6582b2fbc90c6fb9024f905c748c82eeb761285dd826a6c59dc9d166043a1c9fbfdb6a7d5b1887301b3a6be3b38
SSDEEP:	1536:SuxGP/W6QbgQywBGmkla+bsaCaWyVvXmkXwhHkl:Suc3kgQxFklapalP
File Content Preview:	PK..........!..z..z...<.......[Content_Types].xml ...(..

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:29:53.543081045 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.543346882 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.582880974 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.582952023 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.582962990 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.584079981 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.584737062 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.585199118 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.624406099 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.624811888 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.624867916 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.624907017 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.624948978 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.625091076 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.625128031 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.625165939 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.627341986 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.627975941 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.635596037 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.635667086 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.641025066 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.641051054 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.642769098 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.643313885 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.651999950 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.652348042 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.682531118 CET	443	49169	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.682609081 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.682929039 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.683011055 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.683410883 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.683414936 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.692506075 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.692549944 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.692900896 CET	443	49168	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.692992926 CET	49168	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.693051100 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.693171978 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.705224991 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.723118067 CET	443	49169	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723170996 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723342896 CET	443	49169	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723387003 CET	443	49169	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723423958 CET	443	49169	65.9.58.87	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:29:53.723429918 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.723454952 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.723472118 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723503113 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.723516941 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723551989 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.723572016 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.723588943 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.723613024 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.725197077 CET	443	49169	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.725272894 CET	443	49170	65.9.58.87	192.168.2.22
Jan 14, 2021 02:29:53.725313902 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.725352049 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.739490032 CET	49170	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.739842892 CET	49169	443	192.168.2.22	65.9.58.87
Jan 14, 2021 02:29:53.744978905 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.747950077 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748004913 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748044968 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748099089 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748100042 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.748146057 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.748157024 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.748164892 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748210907 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.748219967 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.748267889 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.748955965 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.749000072 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.749016047 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.749047995 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.750037909 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.750082016 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.750096083 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.750128984 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.751147985 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.751216888 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.751229048 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.751285076 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.752310038 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.752353907 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.752376080 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.752393961 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.753431082 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.753480911 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.753525019 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.753546000 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.754584074 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.754622936 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.754662991 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.755530119 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.755695105 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.755734921 CET	443	49167	65.9.58.106	192.168.2.22
Jan 14, 2021 02:29:53.755749941 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.755781889 CET	49167	443	192.168.2.22	65.9.58.106
Jan 14, 2021 02:29:53.756922960 CET	443	49167	65.9.58.106	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:29:51.182050943 CET	52197	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:51.239650965 CET	53	52197	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:52.053100109 CET	53099	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:52.125509024 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:29:53.473893881 CET	52838	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:53.540930033 CET	53	52838	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:53.564682961 CET	61200	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:53.623610973 CET	53	61200	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:54.558667898 CET	49548	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:54.617681980 CET	53	49548	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:54.999401093 CET	55627	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.055706978 CET	53	55627	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.435576916 CET	56009	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.438646078 CET	61865	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.493249893 CET	53	56009	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.506669998 CET	53	61865	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.671377897 CET	55171	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.673849106 CET	52496	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.676264048 CET	57564	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.685020924 CET	63009	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.724133015 CET	53	57564	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.730143070 CET	53	52496	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.730463028 CET	53	55171	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.741986990 CET	53	63009	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.747963905 CET	59319	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.760092020 CET	53070	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.807200909 CET	53	59319	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.816327095 CET	53	53070	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:55.895736933 CET	59770	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:55.943603992 CET	53	59770	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:57.028104067 CET	61523	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:57.084543943 CET	53	61523	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:58.225255013 CET	62791	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:58.296145916 CET	53	62791	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:59.178215981 CET	50667	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:59.237360954 CET	53	50667	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:59.683063030 CET	54129	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:59.735567093 CET	65329	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:29:59.739413977 CET	53	54129	8.8.8.8	192.168.2.22
Jan 14, 2021 02:29:59.794075966 CET	53	65329	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:00.472238064 CET	60718	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:00.528801918 CET	53	60718	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:01.727206945 CET	49157	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:01.794816017 CET	53	49157	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:02.473959923 CET	57391	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:02.531307936 CET	53	57391	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:02.579865932 CET	61858	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:02.635931015 CET	53	61858	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:02.907228947 CET	62500	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:02.918025017 CET	51652	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:02.955111027 CET	53	62500	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:02.981494904 CET	53	51652	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:03.410605907 CET	62762	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:03.458503008 CET	53	62762	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.186808109 CET	56905	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.187629938 CET	54609	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.188152075 CET	58101	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.195388079 CET	64329	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.195658922 CET	64881	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.195831060 CET	55327	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:04.238277912 CET	53	54609	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.242985010 CET	53	56905	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.247195005 CET	53	58101	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.252206087 CET	53	64881	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.252233982 CET	53	55327	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:04.254466057 CET	53	64329	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:21.845623970 CET	59150	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:21.896464109 CET	53	59150	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:30:22.858372927 CET	59150	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:22.917593002 CET	53	59150	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:23.872721910 CET	59150	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:23.923677921 CET	53	59150	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:24.998470068 CET	63439	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:25.049276114 CET	53	63439	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:25.448621035 CET	65040	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:25.511019945 CET	53	65040	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:25.885045052 CET	59150	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:25.944200039 CET	53	59150	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:26.009996891 CET	63439	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:26.069371939 CET	53	63439	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:27.023936033 CET	63439	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:27.083574057 CET	53	63439	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:29.036446095 CET	63439	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:29.087392092 CET	53	63439	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:29.894790888 CET	59150	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:29.954273939 CET	53	59150	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:30.302447081 CET	61369	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:30.358839035 CET	53	61369	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:31.534101009 CET	61369	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:31.582144976 CET	53	61369	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:32.691620111 CET	61369	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:32.739562988 CET	53	61369	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:33.046180964 CET	63439	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:33.105501890 CET	53	63439	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:33.410373926 CET	65515	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:33.469474077 CET	53	65515	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:34.419254065 CET	65515	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:34.478539944 CET	53	65515	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:34.700151920 CET	61369	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:34.756635904 CET	53	61369	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:35.433377981 CET	65515	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:35.492521048 CET	53	65515	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:37.445890903 CET	65515	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:37.496680021 CET	53	65515	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:38.709301949 CET	61369	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:38.757405043 CET	53	61369	8.8.8.8	192.168.2.22
Jan 14, 2021 02:30:41.455387115 CET	65515	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:30:41.514520884 CET	53	65515	8.8.8.8	192.168.2.22
Jan 14, 2021 02:31:03.760581970 CET	60236	53	192.168.2.22	8.8.8.8
Jan 14, 2021 02:31:03.823954105 CET	53	60236	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:29:52.053100109 CET	192.168.2.22	8.8.8.8	0xd6ca	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.473893881 CET	192.168.2.22	8.8.8.8	0x75c8	Standard query (0)	renderer-a ssets.type form.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.564682961 CET	192.168.2.22	8.8.8.8	0x6401	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:54.558667898 CET	192.168.2.22	8.8.8.8	0x8482	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:54.999401093 CET	192.168.2.22	8.8.8.8	0xac8c	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.435576916 CET	192.168.2.22	8.8.8.8	0x9faf	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.438646078 CET	192.168.2.22	8.8.8.8	0xab5f	Standard query (0)	public-ass ets.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.895736933 CET	192.168.2.22	8.8.8.8	0x6428	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:58.225255013 CET	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:59.178215981 CET	192.168.2.22	8.8.8.8	0xbf29	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:29:59.735567093 CET	192.168.2.22	8.8.8.8	0xba59	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:00.472238064 CET	192.168.2.22	8.8.8.8	0xfe02	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:01.727206945 CET	192.168.2.22	8.8.8.8	0x4ac9	Standard query (0)	renderer-a ssets.type form.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.473959923 CET	192.168.2.22	8.8.8.8	0xc48a	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.579865932 CET	192.168.2.22	8.8.8.8	0x1b2a	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.907228947 CET	192.168.2.22	8.8.8.8	0xf27f	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.918025017 CET	192.168.2.22	8.8.8.8	0x3bdc	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.410605907 CET	192.168.2.22	8.8.8.8	0x7adc	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 14, 2021 02:31:03.760581970 CET	192.168.2.22	8.8.8.8	0xd927	Standard query (0)	public-ass ets.typeform.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:29:52.125509024 CET	8.8.8.8	192.168.2.22	0xd6ca	No error (0)	ny990xqwsj 1.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:53.540930033 CET	8.8.8.8	192.168.2.22	0x75c8	No error (0)	renderer-a ssets.type form.com	d2citsn5wf4j9j.cloudfront. net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:53.540930033 CET	8.8.8.8	192.168.2.22	0x75c8	No error (0)	d2citsn5wf 4j9j.cloud front.net		65.9.58.106	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.540930033 CET	8.8.8.8	192.168.2.22	0x75c8	No error (0)	d2citsn5wf 4j9j.cloud front.net		65.9.58.119	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.540930033 CET	8.8.8.8	192.168.2.22	0x75c8	No error (0)	d2citsn5wf 4j9j.cloud front.net		65.9.58.77	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.540930033 CET	8.8.8.8	192.168.2.22	0x75c8	No error (0)	d2citsn5wf 4j9j.cloud front.net		65.9.58.68	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.623610973 CET	8.8.8.8	192.168.2.22	0x6401	No error (0)	images.typ eform.com	d2nvsmtq2poimt.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:53.623610973 CET	8.8.8.8	192.168.2.22	0x6401	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.623610973 CET	8.8.8.8	192.168.2.22	0x6401	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.623610973 CET	8.8.8.8	192.168.2.22	0x6401	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:53.623610973 CET	8.8.8.8	192.168.2.22	0x6401	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:54.617681980 CET	8.8.8.8	192.168.2.22	0x8482	No error (0)	cdn.segmen t.com	d296je7bbdd650.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:54.617681980 CET	8.8.8.8	192.168.2.22	0x8482	No error (0)	d296je7bbd d650.cloud front.net		65.9.70.129	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		44.225.192.231	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		52.42.46.86	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		54.68.229.68	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		52.10.17.224	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		52.11.35.251	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		52.39.143.152	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		54.69.177.146	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.055706978 CET	8.8.8.8	192.168.2.22	0xac8c	No error (0)	api.segment.io		54.70.9.247	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.493249893 CET	8.8.8.8	192.168.2.22	0x9faf	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:55.506669998 CET	8.8.8.8	192.168.2.22	0xab5f	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:55.506669998 CET	8.8.8.8	192.168.2.22	0xab5f	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.120	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.506669998 CET	8.8.8.8	192.168.2.22	0xab5f	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.128	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.506669998 CET	8.8.8.8	192.168.2.22	0xab5f	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.506669998 CET	8.8.8.8	192.168.2.22	0xab5f	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.37	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.943603992 CET	8.8.8.8	192.168.2.22	0x6428	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.943603992 CET	8.8.8.8	192.168.2.22	0x6428	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.943603992 CET	8.8.8.8	192.168.2.22	0x6428	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:55.943603992 CET	8.8.8.8	192.168.2.22	0x6428	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:58.296145916 CET	8.8.8.8	192.168.2.22	0xed69	No error (0)	ny990xqwsj1.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:59.237360954 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:29:59.237360954 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:59.237360954 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:59.237360954 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:59.237360954 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 14, 2021 02:29:59.794075966 CET	8.8.8.8	192.168.2.22	0xba59	No error (0)	ny990xqwsj1.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:00.528801918 CET	8.8.8.8	192.168.2.22	0xfe02	No error (0)	ny990xqwsj1.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:01.794816017 CET	8.8.8.8	192.168.2.22	0x4ac9	No error (0)	renderer-assets.typeform.com	d2citsn5wf4j9j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:01.794816017 CET	8.8.8.8	192.168.2.22	0x4ac9	No error (0)	d2citsn5wf4j9j.cloudfront.net		65.9.58.106	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:01.794816017 CET	8.8.8.8	192.168.2.22	0x4ac9	No error (0)	d2citsn5wf4j9j.cloudfront.net		65.9.58.119	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:01.794816017 CET	8.8.8.8	192.168.2.22	0x4ac9	No error (0)	d2citsn5wf4j9j.cloudfront.net		65.9.58.77	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:01.794816017 CET	8.8.8.8	192.168.2.22	0x4ac9	No error (0)	d2citsn5wf4j9j.cloudfront.net		65.9.58.68	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:30:02.531307936 CET	8.8.8.8	192.168.2.22	0xc48a	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:02.635931015 CET	8.8.8.8	192.168.2.22	0x1b2a	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:02.635931015 CET	8.8.8.8	192.168.2.22	0x1b2a	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.635931015 CET	8.8.8.8	192.168.2.22	0x1b2a	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.635931015 CET	8.8.8.8	192.168.2.22	0x1b2a	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.635931015 CET	8.8.8.8	192.168.2.22	0x1b2a	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.955111027 CET	8.8.8.8	192.168.2.22	0xf27f	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.955111027 CET	8.8.8.8	192.168.2.22	0xf27f	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.955111027 CET	8.8.8.8	192.168.2.22	0xf27f	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.955111027 CET	8.8.8.8	192.168.2.22	0xf27f	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:02.981494904 CET	8.8.8.8	192.168.2.22	0x3bdc	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:30:02.981494904 CET	8.8.8.8	192.168.2.22	0x3bdc	No error (0)	d296je7bbdd650.cloudfront.net		65.9.70.129	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		52.35.195.250	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		35.164.219.175	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		52.43.10.86	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		52.43.15.143	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		54.201.197.201	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		54.71.192.93	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		54.200.228.33	A (IP address)	IN (0x0001)
Jan 14, 2021 02:30:03.458503008 CET	8.8.8.8	192.168.2.22	0x7adc	No error (0)	api.segment.io		52.88.208.102	A (IP address)	IN (0x0001)
Jan 14, 2021 02:31:03.823954105 CET	8.8.8.8	192.168.2.22	0xd927	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:31:03.823954105 CET	8.8.8.8	192.168.2.22	0xd927	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.37	A (IP address)	IN (0x0001)
Jan 14, 2021 02:31:03.823954105 CET	8.8.8.8	192.168.2.22	0xd927	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.120	A (IP address)	IN (0x0001)
Jan 14, 2021 02:31:03.823954105 CET	8.8.8.8	192.168.2.22	0xd927	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 14, 2021 02:31:03.823954105 CET	8.8.8.8	192.168.2.22	0xd927	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.128	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:29:53.627341986 CET	65.9.58.106	443	192.168.2.22	49167	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:29:53.627975941 CET	65.9.58.106	443	192.168.2.22	49168	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:29:53.725197077 CET	65.9.58.87	443	192.168.2.22	49169	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:29:53.725272894 CET	65.9.58.87	443	192.168.2.22	49170	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:29:54.532316923 CET	65.9.58.87	443	192.168.2.22	49171	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:29:54.701976061 CET	65.9.70.129	443	192.168.2.22	49172	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:29:54.703998089 CET	65.9.70.129	443	192.168.2.22	49173	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:29:55.552287102 CET	44.225.192.231	443	192.168.2.22	49174	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:29:55.596678019 CET	65.9.58.120	443	192.168.2.22	49179	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:29:55.596718073 CET	65.9.58.120	443	192.168.2.22	49178	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:29:55.775126934 CET	44.225.192.231	443	192.168.2.22	49175	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:29:56.239269972 CET	162.247.242.19	443	192.168.2.22	49180	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:29:56.256606102 CET	162.247.242.19	443	192.168.2.22	49181	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:29:59.324135065 CET	65.9.58.87	443	192.168.2.22	49185	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:30:01.878551960 CET	65.9.58.106	443	192.168.2.22	49188	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:30:01.880961895 CET	65.9.58.106	443	192.168.2.22	49189	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:30:02.721120119 CET	65.9.58.87	443	192.168.2.22	49192	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 02:30:02.722842932 CET	65.9.58.87	443	192.168.2.22	49193	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

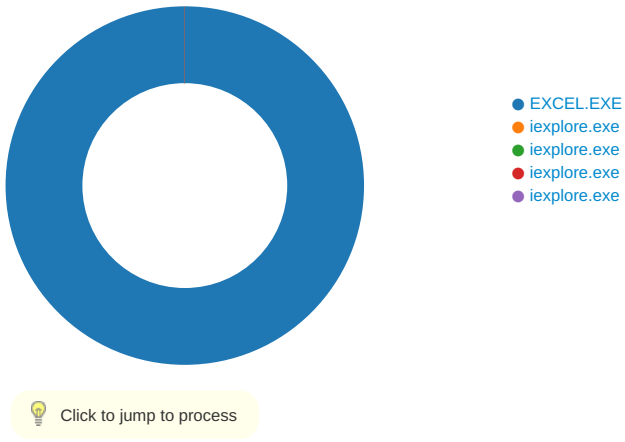
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:30:03.084264994 CET	65.9.70.129	443	192.168.2.22	49196	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:30:03.095767021 CET	65.9.70.129	443	192.168.2.22	49197	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:30:03.283369064 CET	162.247.242.19	443	192.168.2.22	49194	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:30:03.303157091 CET	162.247.242.19	443	192.168.2.22	49195	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:30:03.878695011 CET	52.35.195.250	443	192.168.2.22	49198	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:30:04.154705048 CET	52.35.195.250	443	192.168.2.22	49199	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2100 Parent PID: 584

General

Start time:	02:29:35
Start date:	14/01/2021
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:	0x13f910000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\28B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FC5EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\28B6.tmp	success or wait	1	13FECB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA9E9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FB5F526	WriteFile
C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..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	13FB5F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\LnkQ4hGmxTTD[1].png	unknown	329	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 83 00 00 00 6d 08 06 00 00 00 82 d3 d2 94 00 00 2b b4 49 44 41 54 78 da ed 5d 07 78 14 55 d7 5e a4 48 d9 64 93 ec 66 cb cc 6c 28 62 03 c5 02 fa d9 10 ec 60 c1 f2 89 05 15 e9 f8 29 d6 df ca 67 89 e5 53 4a b2 9b dd 4d 02 88 88 bd a0 62 47 51 8a 22 20 2a d8 3b 2a 2a 88 f4 94 4d 23 24 b9 ff fb de 99 d5 10 b6 4c 84 00 81 bd cf 73 9f 4d 76 67 76 67 e6 9e 7b ce 7b de 73 ee b9 96 dd b5 89 ec ec 56 9b c6 8d b3 15 fb 27 1c 59 52 90 73 94 18 3f 2d 65 83 cf a7 56 e6 e7 74 dc 14 f4 f5 ae 98 e4 53 45 30 b8 af 25 d9 f6 9c 56 e2 f3 65 84 0b fc 07 97 e6 e7 de 16 0e f9 9e 2d 09 f8 af 09 87 72 ff 5b 12 f4 3d 5f 1a cc 9d 57 12 ca fd 1d 7f af 28 e1 67 c1 dc b7 4b 43 be ef ca f3 fd 5b f0 f7 c7 38 2e 58 94 97 3b 60 53 20	.PNG.....IHDR.....m..... .....+.IDATx..].x.U.^.H.d..f.. I(b.....`.....)...g..SJ... M.....bGQ." *.;**...M#$..... .L.....s.Mvgvg..{.{.s.....V .....'.YR.s..?-e...V..t..... .SE0..%...V..e.....-.....r. [..=_...W.....(.g...KC..... [...8.X..;`S	success or wait	3	7FEE9AA3B4B	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90BCE4B8.jpeg	0	4096	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90BCE4B8.jpeg	0	65057	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90BCE4B8.jpeg	0	4096	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90BCE4B8.jpeg	0	65057	success or wait	1	7FEEA9E9AC0	unknown

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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2A99	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2C3E	success or wait	1	7FEEA9E9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	p&3	binary	70 26 33 00 34 08 00 00 02 00 00 00 00 00 00 00 72 00 00 00 01 00 00 00 38 00 00 00 2E 00 00 00 61 00 63 00 68 00 20 00 72 00 65 00 6D 00 6C 00 74 00 74 00 61 00 6E 00 63 00 65 00 20 00 61 00 64 00 76 00 6C 00 63 00 65 00 2E 00 2E 00 78 00 6C 00 73 00 78 00 00 00 61 00 63 00 68 00 20 00 72 00 65 00 6D 00 6C 00 74 00 74 00 61 00 6E 00 63 00 65 00 20 00 61 00 64 00 76 00 6C 00 63 00 65 00 2E 00 00 00	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7454812183.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3209467860.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2A99	F2A99	binary	04 00 00 00 34 08 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 00 00 00 00 22 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 01 00 00 00 01 00 00 00 05 1C FF 36 60 EA D6 01 99 2A 0F 00 99 2A 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7454812183.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3209467860.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2C3E	F2C3E	binary	04 00 00 00 34 08 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 00 00 00 00 22 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 01 00 00 00 01 00 00 00 05 1C FF 36 60 EA D6 01 3E 2C 0F 00 3E 2C 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA9E9AC0	unknown

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

Analysis Process: iexplore.exe PID: 1976 Parent PID: 584

General

Start time:	02:29:59
Start date:	14/01/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe

Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f340000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2364 Parent PID: 1976

General

Start time:	02:29:59
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1976 CREDAT:275457 /prefetch:2
Imagebase:	0x1160000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2864 Parent PID: 2100

General

Start time:	02:30:07
Start date:	14/01/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://ny990xqwsj1.typeform.com/to/qjFrxD7r
Imagebase:	0x13f340000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 3056 Parent PID: 2864

General

Start time:	02:30:08
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2864 CREDAT:275457 /prefetch:2
Imagebase:	0x1160000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly