ID: 339432
Sample Name: ACH REMITTANCE ADVICE..xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:35:11
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

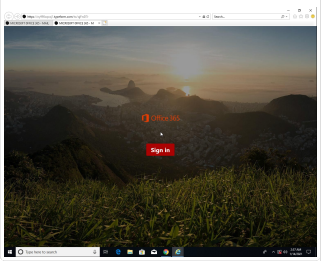
Analysis Report ACH REMITTANCE ADVICE..xlsx

Overview

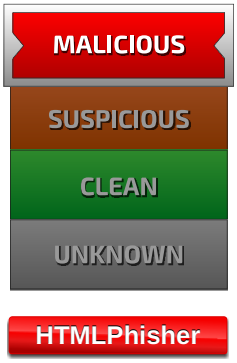
General Information

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

Most interesting Screenshot:



Detection

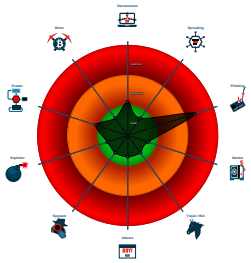


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6616 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- iexplore.exe (PID: 7152 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5676 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7152 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6340 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7152 CREDAT:17434 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\qjFrxD7r[1].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

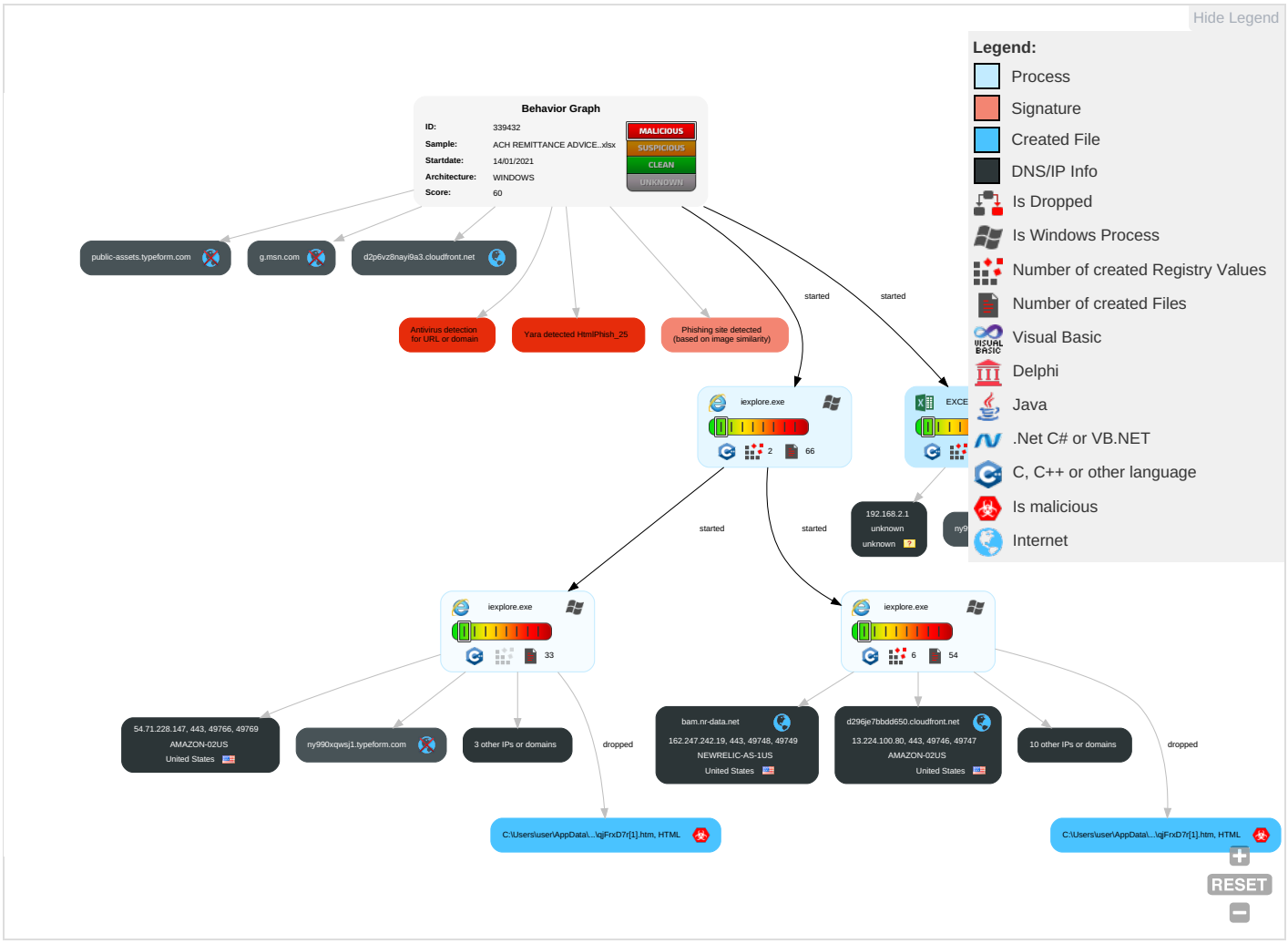
Yara detected HtmlPhish_25

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	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	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 Lockc
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

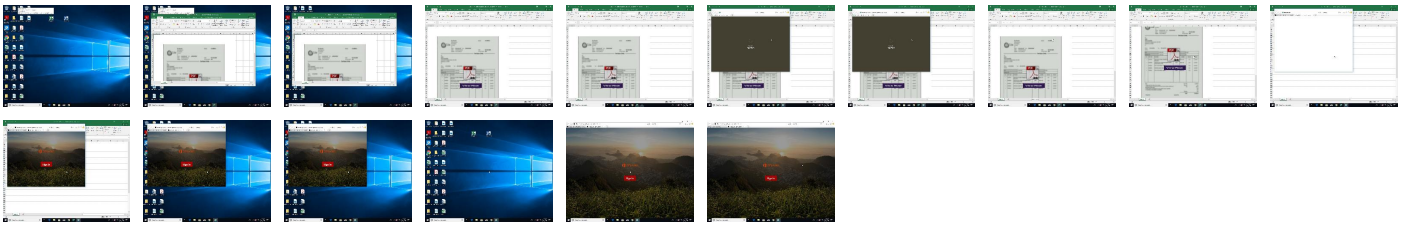
Behavior Graph

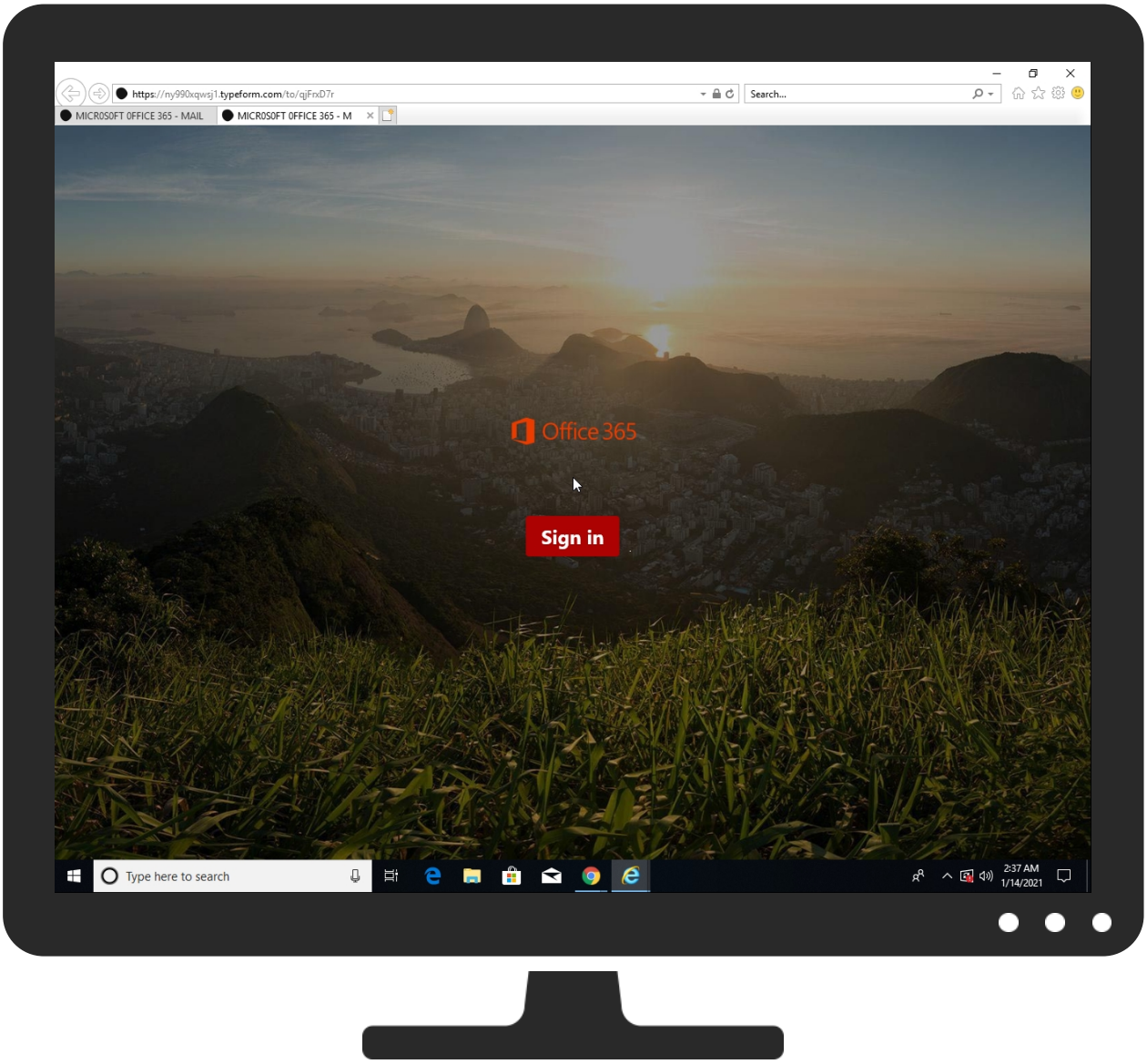


Screenshots

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://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://www.typeform.c	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://ny990xqwsj1.typefRoot	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ny990xqwsj1.ty	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d296je7bbdd650.cloudfront.net	13.224.100.80	true	false		high
api.segment.io	52.34.69.24	true	false		high
d2citsn5wf4j9j.cloudfront.net	13.224.94.129	true	false		high
d2nvsmtq2poimt.cloudfront.net	13.224.94.83	true	false		high
bam.nr-data.net	162.247.242.19	true	false	• 0%, Virustotal, Browse	unknown
d2p6vz8nayi9a3.cloudfront.net	13.224.94.20	true	false		high
cdn.segment.com	unknown	unknown	false		high
g.msn.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

URLs from Memory and Binaries

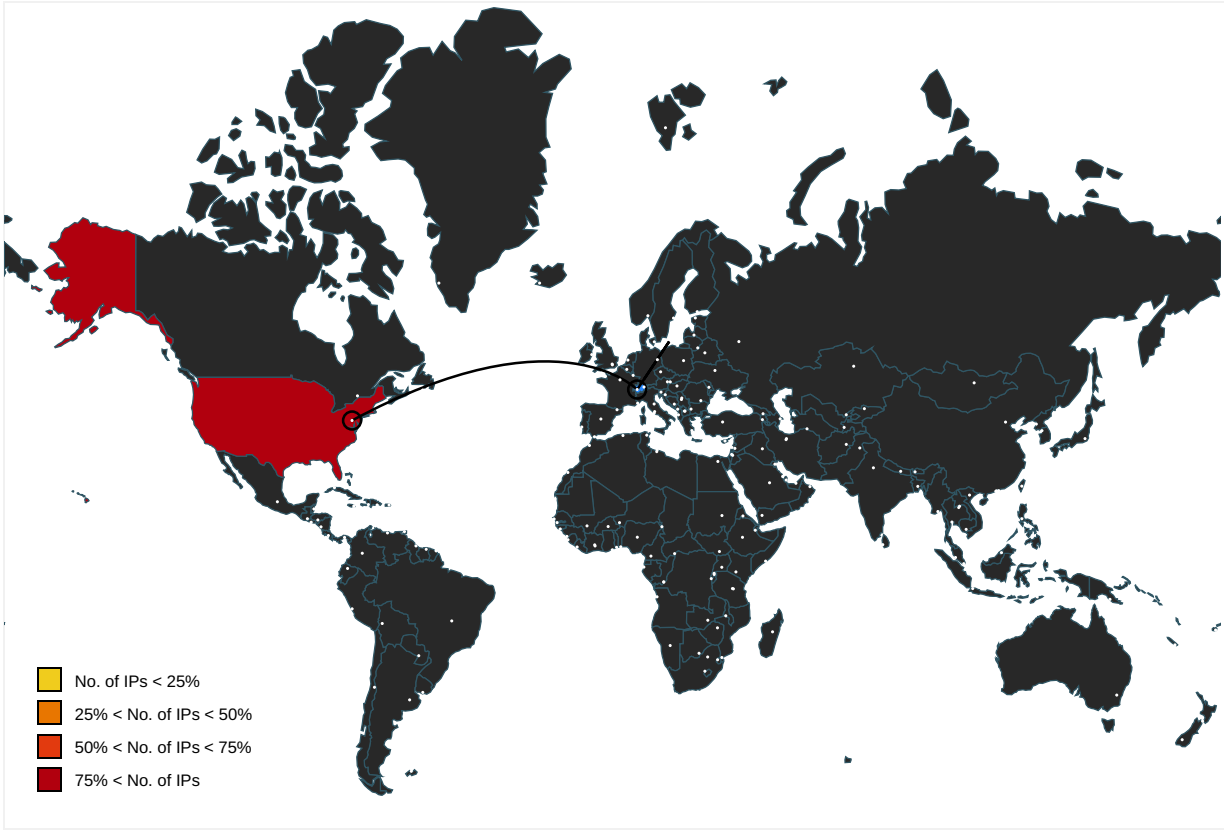
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://login.microsoftonline.com/	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://shell.suite.office.com:1443	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://autodiscover-s.outlook.com/	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://renderer-assets.typeform.com/vendors~phonenumber.32d788474b661d4d3074.js	qjFrxD7r[1].htm.18.dr	false		high
http://https://renderer-assets.typeform.com/blocks-matrix.0544beec0e1a4e11a24a.js	qjFrxD7r[1].htm.18.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-16x16.png	qjFrxD7r[1].htm.18.dr	false		high
http://https://cdn.entity.	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://renderer-assets.typeform.com/phonenumber.6ea5ec50b9fa21e816ff.js	qjFrxD7r[1].htm.18.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://wus2-000.contentsync.	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://powerlift.acompli.net	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://cortana.ai	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6peform.com/to/qjFrxD7rRoot	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false		high
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://public-assets.typeform.com/public/favicon/browserconfig.xml	qjFrxD7r[1].htm.18.dr	false		high
http://https://public-assets.typeform.com/public/favicon/site.webmanifest	qjFrxD7r[1].htm.18.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://api.aadrm.com/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://images.typeform.com/images/HzxaK5qZrKPU/image/default	qjFrxD7r[1].htm.18.dr	false		high
http://https://ofcrecsvcapi-int.azurewebsites.net/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://public-assets.typeform.com/public/favicon/apple-touch-icon.png	qjFrxD7r[1].htm.18.dr	false		high
http://https://www.typeform.c	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false	• Avira URL Cloud: safe	unknown
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6orm.com/to/qjFrxD7r	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://api.microsoftstream.com/api/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://cr.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://graph.ppe.windows.net	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://res.getmicrosoftkey.com/api/redemptionevents	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://sr.outlook.office.net/ws/speech/recognize/assistant/work	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://ny990xqwsj1.typeform.com/oembed?url=https%3A%2F%2Fny990xqwsj1.typeform.com%2Fto%2FqjFrxD7r	qjFrxD7r[1].htm.18.dr	false		high
http://https://store.office.cn/addinstemplate	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://images.typeform.com/images/m9zWqYibLnGK/background/large);background-position:top	qjFrxD7r[1].htm.18.dr	false		high
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http:// https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://web.microsoftstream.com/video/	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://graph.windows.net	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://dataservice.o365filtering.com/	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r	qjFrxD7r[1].htm.18.dr	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http:// https://outlook.office365.com/autodiscover/autodiscover.json	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high
http:// https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2243009E-8CA2-444D-8CD7-D96533 3DA10B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://www.typeform.com/?utm_campaign=qjFrxD7r&utm_source=typeform.com-17523577-Free&utm_medium=typ	~DF634E439E9B8080F4.TMP.17.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png-	imagestore.dat.18.dr	false		high
http://https://github.com/js-cookie/js-cookie	renderer.0f5a683b381b67dbbf89[1].js.18.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://weather.service.msn.com/data.aspx	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://apis.live.net/v5.0/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://renderer-assets.typeform.com/vendors~attachment.6e37d3fcdf703c1517e1.js	qjFrxD7r[1].htm.18.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7rRoot	{75F60466-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false		high
http://https://ny990xqwsj1.typefRoot	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false	• Avira URL Cloud: safe	unknown
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://management.azure.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png	~DF634E439E9B8080F4.TMP.17.dr, qjFrxD7r[1].htm.18.dr	false		high
http://https://ny990xqwsj1.typeform.com/to/qjFrxD7r6om/?utm_campaign=qjFrxD7r&utm_so	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false		high
http://https://incidents.diagnostics.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://renderer-assets.typeform.com/vendors~blocks-ranking.f8aee16223a106724ea1.js	qjFrxD7r[1].htm.18.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://api.office.net	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://github.com/kof/animationFrame	vendors~form.965f5dedbb854e83c6c8[1].js.18.dr	false		high
http://https://entitlement.diagnostics.office.com	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://outlook.office.com/	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high
http://https://ny990xqwsj1.ty	{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat.17.dr	false	• Avira URL Cloud: safe	unknown
http://https://storage.live.com/clientlogs/uploadlocation	2243009E-8CA2-444D-8CD7-D965333DA10B.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.71.228.147	unknown	United States		16509	AMAZON-02US	false
13.224.94.83	unknown	United States		16509	AMAZON-02US	false
13.224.100.80	unknown	United States		16509	AMAZON-02US	false
13.224.94.20	unknown	United States		16509	AMAZON-02US	false
13.224.94.129	unknown	United States		16509	AMAZON-02US	false
162.247.242.19	unknown	United States		23467	NEWRELIC-AS-1US	false
52.34.69.24	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339432
Start date:	14.01.2021
Start time:	02:35:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ACH REMITTANCE ADVICE..xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.winXLSX@6/34@19/8
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://ny990xqwsj1.typeform.com/to/qjFrxD7r • Scroll down • Close Viewer • Browsing link: https://www.typeform.com/?utm_campaign=qjFrxD7r&utm_source=typeform.com-17523577-Free&utm_medium=typeform&utm_content=typeform-footer&utm_term=EN
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.109.88.177, 52.109.8.22, 52.109.8.24, 168.61.161.212, 51.104.139.180, 2.20.84.85, 92.122.213.194, 92.122.213.247, 20.54.26.129, 2.20.142.209, 2.20.142.210, 88.221.62.148, 52.142.114.176, 104.18.27.71, 104.18.26.71, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 152.199.19.161 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, random.typeform.com.cdn.cloudflare.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, f4.shared.global.fastly.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.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
13.224.94.83	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	
13.224.100.80	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	
	http://https://target-care.webflow.io/	Get hash	malicious	Browse	
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	
	http://secure-file-transfer-link-on.webflow.io	Get hash	malicious	Browse	
	http://https://secure-file-transfer-link-on.webflow.io	Get hash	malicious	Browse	
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	
	http://https://mshad4064.typeform.com/to/TEglyNGg	Get hash	malicious	Browse	
	http://https://newrfpsubmissioncall.typeform.com/to/Mfm0qNbE	Get hash	malicious	Browse	
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	
	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACH - WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACH - WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
	ACHWIRE REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	
	ACHWIRE REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	
	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	
	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	
	ACH WIRE PAYMENT.xlsx	Get hash	malicious	Browse	
13.224.94.129	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	
162.247.242.19	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	
	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	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ACH WIRE PAYMENT.xlsx	Get hash	malicious	Browse	
52.34.69.24	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d2nvsmtq2poimt.cloudfront.net	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.87
	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
api.segment.io	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 44.225.192.231
	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
d2citsn5wf4j9j.cloudfront.net	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.106
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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	• 143.204.208.110
	ACH & WIRE PAYMENT.xlsx	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/673616c6c792e64756e6e6540706572706574756c2e636f6d2e6175	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	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
AMAZON-02US	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
AMAZON-02US	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	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
	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
AMAZON-02US	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	AS006-20211201.pdf.exe	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	DataServer.dll	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	nsaCDED.dll	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202114170492f#U0433#U03bfm+19796076561 19796076561.HTM	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	PolicyUpdate.htm	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	l0sjk3o.dll	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	COMFAM INVOICE.htm	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	P396143.htm	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
	sfk_setup.exe	Get hash	malicious	Browse	• 54.71.228.147 • 13.224.94.83 • 13.224.100.80 • 13.224.94.20 • 13.224.94.129 • 162.247.242.19 • 52.34.69.24
37f463bf4616ecd445d4a1937da06e19	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 13.224.94.83
	ACH REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 13.224.94.83
	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 13.224.94.83
	Notification_71823.xls	Get hash	malicious	Browse	• 13.224.94.83
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 13.224.94.83
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202114170492f#U0433#U03bfm+19796076561 19796076561.HTM	Get hash	malicious	Browse	• 13.224.94.83
	J04gSlH5wR.exe	Get hash	malicious	Browse	• 13.224.94.83
	rufus-2.9.exe	Get hash	malicious	Browse	• 13.224.94.83
	Invoice-ID43739424297.vbs	Get hash	malicious	Browse	• 13.224.94.83
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 13.224.94.83
	Customer_Receivables_Aging_20210112_2663535345242424242.exe	Get hash	malicious	Browse	• 13.224.94.83
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.224.94.83
	Listings.exe	Get hash	malicious	Browse	• 13.224.94.83
	Transferencia,pdf.exe	Get hash	malicious	Browse	• 13.224.94.83
	Dhl Client Invoice.exe	Get hash	malicious	Browse	• 13.224.94.83
	64D5aP6jQz.exe	Get hash	malicious	Browse	• 13.224.94.83
	P396143.htm	Get hash	malicious	Browse	• 13.224.94.83
	Code.exe	Get hash	malicious	Browse	• 13.224.94.83
	UbisoftInstaller.exe	Get hash	malicious	Browse	• 13.224.94.83

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New inquiry CON 20-10630.exe	Get hash	malicious	Browse	• 13.224.94.83

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\0WZGNI7O\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):	308716
Entropy (8bit):	5.23118253767301
Encrypted:	false
SSDEEP:	1536:s5eS5ofbBvofbNvofbcvofbYvofbPvofbiH+mfbRHDHHfbxHDHHfb1HDHHfb9HDb:vhD9DBD5DvDoDoD7y+D0IYY
MD5:	76A99D2CD14233CCD0D1E091F985E4C2
SHA1:	602B4B9DD8B4C71E3FB10E669E6CB5A67CB91C53
SHA-256:	E38AE2208CEEA566F882B78F18BD649087436E4227832301AEB6022F30A2179A
SHA-512:	0644BCFE7A77B8C0F374D51C8FF85ECC04752F831E301647E4CC00C6A8C1C66BAA758A585C29D8EA73FAD0D5D1A878BEB6BDBCEFBA0438B1AA16005BD4FC3166
Malicious:	false
Reputation:	low
Preview:	<root><item name="qjFrxD7r-visitorId" value="qjFrxD7r-1610620625963-33" ltime="872924384" htime="30861921" /><item name="debug" value="undefined" ltime="978654384" htime="30861921" /><item name="segmentio.c39bd0ea-6c0b-404f-b7d8-c294ecbcb033.inProgress" value="{}" ltime="914494384" htime="30861921" /><item name="segmentio.c39bd0ea-6c0b-404f-b7d8-c294ecbcb033.queue" value="[]" ltime="911664384" htime="30861921" /><item name="segmentio.c39bd0ea-6c0b-404f-b7d8-c294ecbcb033.ack" value="1610620635812" ltime="971414384" htime="30861921" /><item name="segmentio.c39bd0ea-6c0b-404f-b7d8-c294ecbcb033.reclaimStart" value="null" ltime="971414384" htime="30861921" /><item name="segmentio.c39bd0ea-6c0b-404f-b7d8-c294ecbcb033.reclaimEnd" value="null" ltime="971414384" htime="30861921" /><item name="ajs_anonymous_id" value=""d943661c-fba0-49bd-ae89-abc1d19ab5f4"" ltime="915294384" htime="30861921" /></root><root><item name="qjFrxD7r-visitorId" value="qjFrxD7r-1610620625963-33" ltime="8729243

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6EA7867C-5654-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42072
Entropy (8bit):	1.9333560134658265
Encrypted:	false
SSDEEP:	96:r4ZbZk2k9WgLtg9fgaRMgQgqgLfgQsrgagTgx+fg8F8W:r4ZbZk2k9WetMfhRMzVafjsrhg5fH8W
MD5:	CA84203ED557FEFEB761EEE6C50EB315
SHA1:	36409E2F40A048F70F26493D5E9397AB67ED06B5
SHA-256:	77B366020AF771C0CF7B141DB8A7F8D4F2EFD1F86EC0FFFAFA50318998BA124C
SHA-512:	BC295F74BFCAB3896109A00416D16CF6B51E8B13046EA65D42E95E5D06371798C486B7FB98D5348B28A7AD69B7892D443057BFC1C205F578D15A48FCC9FB8DF
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\{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	47916
Entropy (8bit):	2.073390658583188
Encrypted:	false
SSDEEP:	192:rtZ2QK6bk5FjxP2xikWxdMxSYTbuYbBUxNbqg0YbTNb/sUYubf7E1baTbqoSg:rDD1g5hMccsWn9UH2gh9gU7r7kOTuol
MD5:	EF469BA6EE4B8C0EC2AD1508CE93FECC
SHA1:	C07CA3ABB07EA134595E1F994C16925BE149A98B
SHA-256:	5BB5EFF6676021A757625D24532D7D2C618465EDC140D006243B8D73F2A34662
SHA-512:	50207879C115B32929D3F6FB5917E0A42E4B224D17A3872AEC618F7F73F077C36FF3CAAF8651E473B87BC137FA942F6CDCBB5DCB59BD2BC61C62EEF4437EE43

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6EA7867E-5654-11EB-90E4-ECF4BB862DED}.dat	
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\{75F60466-5654-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29618
Entropy (8bit):	1.800259633462054
Encrypted:	false
SSDEEP:	96:rxZSQr6lBSHFj12rkWNMIYstzuVNuI4MZiuJ/g:rxZSQr6lkHFj12rkWNMIYstz4NOMjhg
MD5:	A139228AB7C848CC9A53921C7A4CAD88
SHA1:	93181AE201A80DE48BD8D7359A5BC1BD178AACD6
SHA-256:	F19B6DE044F024CD28BAF55A269EFBF6CF14B0F527E3A4AE166CF2A7700BCACA
SHA-512:	FC534AB773E12D21588079ABA1C116285E489E24712A93C8EB2A1C91AC822056DCD9F182176F8F99DFE2E45C0437BDF92CDFC3EF42397BB4EB7B03394489CD3
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\{75F60467-5654-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5625040666113363
Encrypted:	false
SSDEEP:	48:IwahGcprg6GwpaChG4pQUTGrapbSgrGQpKeG7HpRosTGIpG:raXZgiQCz6U3BSgFAZTo4A
MD5:	2ECBABF5D8CB685870BF561E48D7C8B2
SHA1:	444F8F5A043C420867355400DAB2787E576F01FD
SHA-256:	1D6ED1CC30860EF53DDF520C7FB16BB6BEA666CB48A96DEAB14FD6943FF933F5
SHA-512:	388CF0321AB708C7F144875B4B8CC2F4698CF52EBF78118A881193352FBBF807C7A1BBF7D676034C3D38F11B5506C35155D2313BA576178D4DFFAF02B0E0F1B0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1241
Entropy (8bit):	7.2332899980558745
Encrypted:	false
SSDEEP:	24:Yt4/pSym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02EflyL:YUx0v9PoQ5VqKwspEegL
MD5:	032A6EEACC1A8DEC225EE22B74E24C25
SHA1:	8213981EF8AC7E3E948CD74CE63AE88E585413FD
SHA-256:	33C48C03D929A55E2FFD1CE747432C0CC758F84F969690D6C4AC1FF53B2FC428
SHA-512:	BBEA9FF11E7660E8E89DEC4A740ED88E46B3EA6885711B620AD4CFEC07902C94F3601B85BB8E00A4EA74251222424B62B886D5FB8F693B4D93F7ED16F3D2FA8A
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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2243009E-8CA2-444D-8CD7-D965333DA10B	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132942
Entropy (8bit):	5.372898838782893
Encrypted:	false
SSDEEP:	1536:XcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:rrQ9DQW+zBX8P
MD5:	98E4607FE430B02605DF78083FFE57F3
SHA1:	4B9B88733FC7F16A9E6BBA2D55DEBBABFD6223FF
SHA-256:	8DE37332155F4AE645232D164AB5F9678BAB80DD317A344597DC63CE07A2AB54
SHA-512:	9E7FA98999083326FEC1CEBA99A90B64B1360034E07CF26583B1DFC8D2DD318D2D5E67592C4B3E83E2D5F67BBED3C7B891E5122FB8CCE19DC6002FDA7EF404
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-14T01:36:06">.. Build: 16.0.13712.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\62720AA2.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	68C2826235479DC52C10A6EAF078BA3FA0D77120517D608A69349258F5C3646382431CCDA4AEEBCA1026EE877AE180F06E44E6FDD6888681C660D053EA3427BA
Malicious:	false
Reputation:	moderate, very likely benign file
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\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\analytics.min[1].js	
MD5:	C972CB2152B4CA69E1AD84AD369E5D49
SHA1:	2D408DC4AA2394089E145D4619793835A5745AB4
SHA-256:	18FBDEDB7C4B401C5FFA1A76F429FEECEC9928679D485A0CE3F2EA90F709B61E
SHA-512:	3F3294A19D98A64C76929F3F098982B210D83E2FD55487B0B05010D5E073633770C697773682FE053A015CBAD3F316DE2211948F8D5DB2A0974E95BCD09D4FF6
Malicious:	false
Reputation:	low
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\INetCache\IE\0W10PBUV\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):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	high, very likely benign file
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 connection.";..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 = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website\u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	6EA26FF4BACBF426B403E1FCB19D5B17913B0560EF81AB937AECC9D55F6941DEF849C7506AD40A46F0E3DC77ABB53FEE5ABC6C5EC18FC084000829A6A1BD97D6
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\INetCache\IE\0W10PBUV\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/7D5GccKppVCJ05n1aqhbEIGhnLd71UDWfef:ZYzVl1CIKp7eDFnQyV8kAhvzwqy
MD5:	5F8E3CF84B81846FED1820FFAFE7F8A4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\qjFrxD7r[1].htm	
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\INetCache\IE\0W10PBUV\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\INetCache\IE\MEEXW4H4\LnkQ4hGmxTTD[1].png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:ONIISB/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..I(b.....`.....)...g..SJ...M.....bGQ." *.;**...M#$.....L.....s.Mvgvg.{.{.s.....V.....'.YR.s..?-e..V..t.....SE0..%...V..e.....-.....r.[..=_..W.....(.g..KC.....[...8.X..;`S .U..=.('.....S,..Z..Gq.....,..W...p._...o.?.>....c....?.....A....Q..].s....+..^*..NOj..Y....%..3.&.n.....b..0...B.....!$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\INetCache\IE\MEEXW4H4\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):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
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>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\form.9cd5d6381506e5950fe0[1].js	
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\INetCache\IE\MEEXW4H4\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
Encrypted:	false
SSDEEP:	3072:hO203o4PRjCe7bmD2NF1q2ZG8njVKG85sLGU115ZZQjOurJgR8rrjoP7Gwc4/:hUCkbm6r1q23nkGEsLGgt0a5PKwB
MD5:	6F33B62669DF8B6E094E941BB2F1BB39
SHA1:	D2A46B58E82E30176BDAF55CD018FC89AB9F0C23
SHA-256:	645A6486495927D9FC72EDF35C46B50C990F3DCED2101C79F753F6FA8EC11E16
SHA-512:	D0BDB5C7E927C49908667D60B967D75A0D3D7E05FE09A1F24ED13C2F7E411B6D9B57E140CDD7FE742F3ED7A6364EE6AEB8FC1DB1116364F3B6309A4DE30FC4 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 l})),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\INetCache\IE\PSUEOSZZ\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):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
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: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. 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: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\aa6e0ec721[1].gif	
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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..$..r.....Z....-.[.....,SWK[.T..U..Q;L....F^..IHB.....$ ...#$.....o....%..W.....K...K...K....)..L...]..q .e.3s(..5.3.u..M.....W.....I....A.?...iG..VebB~:.!.{.y.e...t..^.Y..".o4ec.A.J.....t}wS.Kj.....]i.R.t..8. ..5d.W.al!....[..a.a.....?..u).*-.....J;R.\....).....<..M.\..o....[.b..r<...%....D ...go....m.b...?..lY....z:.t.H....w...Ui].U* ~...h..2.O.{q{.._.....S].O...s..>....T...W`.U.4J.b..C.EY.EO.....1.....F/.z..... .z.f...d.?p!>'..c.....*&..4...>.....i.O.....t-...0.....c...e{.....^.\. ?..+...s...xZDY.....~.. .q.j......./.....#..Dc....[..g....V...>.X._.a.....9.z.....L..F.n.j..g...'...J><.`E....Vn..'..$.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\INetCache\IE\PSUEOSZZ\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):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...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 getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\INetCache\IE\WJ8I2OL4\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\INetCache\IE\WJ8I2OL4\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):	4.340020120659463
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\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG........IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon-32x32[1].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\INetCache\IE\WJ8I2OL4\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\INetCache\IE\WJ8I2OL4\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\INetCache\IE\WJ8I2OL4\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
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\Temp\~DF228D0BBFA2956A34.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39427
Entropy (8bit):	0.5030967751369914
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+1bWAWhWNIWN/54WNvwNr9KzCpu9KzC4Mkhu9KzCOn9KzL9Kzo9L:kBqoxKAuvScS+1bZILq+0uI4MZiuJ
MD5:	D23C6A6542E34659AB0B2BF9EB1C2604
SHA1:	4774B10352C8C9306A3A91F41A50091BBB614BEE
SHA-256:	0FFBE37963D6A47502461B1701CDE8B9E19370BE685B6B9B6B3082F0E329DFB8
SHA-512:	C23EF41A42F9754B0C012AFE62AA9B48D7F05E1938CB29FCFA95F7932A1C296A25C8FCE0A92E7C429EACCBB9AFAEDB58F8EB27FA40EEEE6748E05273665F68F1
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF228D0BBFA2956A34.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF36CFA6982EF8C0BF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF634E439E9B8080F4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	49471
Entropy (8bit):	0.6757969284190302
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+xexYxSxbxIxvbBUzgxbRp+bSbLpbg:kBqoxKAuqR+w2st299Uzgx9p+WvpE
MD5:	2C9D4CB093178FFA10E652C22405EE40
SHA1:	EDD1D547D190F9F98FD640294C2E4C405857F207
SHA-256:	68F60DC9BB920789DE2350EF92B479F8A1FF78CC5EE1711079A18CDDD36A5BB8
SHA-512:	E8D524A3673DBCBC4665E0D2BB1E68B3F48BFAACFEF86E1F80DB66A02A8AB0289B1C63086CB90284A1FD8B09A615BADB067E31213EA88A0710D62A1E35D74E 4D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8B9F9D209989C9B3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13221
Entropy (8bit):	0.6084892749718764
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo73F9lo7V9lW7gOabHXOaMyGaMMV7XVCaOtaOasiVy7XF:kBqoIakAFFhh1OEOqyhye
MD5:	914424542E0B3F62D4F6E3BF84928CCA
SHA1:	00ECF012877A6443D3ECCD4EF44CC53AAA0F258B
SHA-256:	DD87CDC83ADC14307CED2380345D431132E6BBA764CE072566DC2B53D12EB295
SHA-512:	1AEEA3C3314D4E8685A32A9C92F299D6B3422CD283580300CFCD6911D2E3C637E9C975DE4E7A4CD95F3905571AB4140672F6420C32F7CD22B32DBDB1DA8E86
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165

C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..xlsx	
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53620 7
Malicious:	false
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

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 REMITTANCE ADVICE..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:	74ecd0d2d6d6d0dc

Network Behavior

Network Port Distribution

Total Packets: 118

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:37:03.997338057 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:03.997392893 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.042592049 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.042638063 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.043989897 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.044033051 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.299216032 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.308510065 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.344396114 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.344593048 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.344635010 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.344661951 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.344679117 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.344727993 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.344778061 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.346510887 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.346596956 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.353619099 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.353873968 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.353913069 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.353945017 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.353956938 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.353987932 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.354033947 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.355720997 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.355784893 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.356957912 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.357346058 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.357537031 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.361546993 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.361896992 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.402041912 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.402085066 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.402111053 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.402170897 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.402192116 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.402302980 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.402329922 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.402410984 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.402458906 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.403465033 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.403502941 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.403552055 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.403563023 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.403575897 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.403595924 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.403644085 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.403712034 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.404036045 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.404772043 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.404814959 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.404844046 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.404859066 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.406068087 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406114101 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406148911 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.406166077 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.406496048 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406724930 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406752110 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406788111 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.406821012 CET	443	49739	13.224.94.129	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:37:04.406845093 CET	443	49739	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.406867981 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.406888962 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.407351971 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.407397985 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.407433033 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.407457113 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.407819033 CET	49739	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.408657074 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.408713102 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.408725023 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.408755064 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.409965992 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.410007954 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.410034895 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.410062075 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.411288977 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.411331892 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.411379099 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.411393881 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.412610054 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.412656069 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.412703991 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.412719965 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.413904905 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.413944006 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.413974047 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.413991928 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.415209055 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.415252924 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.415282965 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.415297985 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.416558027 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.416599035 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.416651011 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.416671038 CET	49738	443	192.168.2.3	13.224.94.129
Jan 14, 2021 02:37:04.417815924 CET	443	49738	13.224.94.129	192.168.2.3
Jan 14, 2021 02:37:04.417850971 CET	443	49738	13.224.94.129	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:35:55.436562061 CET	55984	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:35:55.495922089 CET	53	55984	8.8.8.8	192.168.2.3
Jan 14, 2021 02:35:56.701812029 CET	64185	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:35:56.749871016 CET	53	64185	8.8.8.8	192.168.2.3
Jan 14, 2021 02:35:57.822118044 CET	65110	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:35:57.878601074 CET	53	65110	8.8.8.8	192.168.2.3
Jan 14, 2021 02:35:59.125400066 CET	58361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:35:59.173496962 CET	53	58361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:02.930073977 CET	63492	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:02.989536047 CET	53	63492	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:05.396471024 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:05.447432041 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:06.392335892 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:06.453135967 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:06.871258020 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:06.929698944 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:07.593800068 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:07.652745962 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:07.883615017 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:07.972846031 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:08.882635117 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:08.938937902 CET	53	53195	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:36:09.526330948 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:09.574270010 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:10.692225933 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:10.748270035 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:10.882776976 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:10.938955069 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:11.952227116 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:12.000082016 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:13.153018951 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:13.200994968 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:14.308006048 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:14.372155905 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:14.883403063 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:14.939608097 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:15.534929037 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:15.583039999 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:20.917921066 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:20.965754986 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:22.030843019 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:22.081583977 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:23.044450998 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:23.092502117 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:23.505810022 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:23.553608894 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:28.518965006 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:28.576637983 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:31.465507984 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:31.532107115 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:40.727293015 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:40.794517040 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:45.346565962 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:45.416306973 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 02:36:59.784451008 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:36:59.832318068 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:01.366476059 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:01.424135923 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:01.914854050 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:01.979423046 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:02.676433086 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:02.734812021 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:03.929677963 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:03.991137981 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:04.488121986 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:04.547466040 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:06.305413008 CET	61946	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:06.317107916 CET	64910	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:06.365509987 CET	53	61946	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:06.377032995 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:06.378170013 CET	53	64910	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:06.438112020 CET	53	52123	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:06.906306028 CET	56130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:06.956945896 CET	53	56130	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:07.175900936 CET	56338	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:07.223720074 CET	53	56338	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:08.857270956 CET	59420	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:08.924032927 CET	53	59420	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:11.950086117 CET	58784	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:12.006634951 CET	53	58784	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:12.674956083 CET	63978	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:12.744143009 CET	53	63978	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:13.388638020 CET	62938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:13.464698076 CET	53	62938	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:14.644049883 CET	55708	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:14.700777054 CET	53	55708	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:37:16.097661972 CET	56803	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:16.154225111 CET	53	56803	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:16.531657934 CET	57145	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:16.587994099 CET	53	57145	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:17.032516003 CET	55359	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:17.091814995 CET	53	55359	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:17.096211910 CET	58306	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:17.152664900 CET	53	58306	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:17.373924971 CET	64124	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:17.430097103 CET	53	64124	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:31.375605106 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:31.432080030 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:32.131283998 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:32.187804937 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:32.384583950 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:32.432738066 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:33.133754969 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:33.181591034 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:33.398958921 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:33.446866035 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:34.153610945 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:34.209974051 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:34.470834017 CET	53279	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:34.521541119 CET	53	53279	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:35.414985895 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:35.471204042 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:36.164983988 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:36.220995903 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:39.416403055 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:39.472651005 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:40.166496038 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:40.214222908 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:44.339025021 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:44.387109995 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:45.337593079 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:45.385670900 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:46.337825060 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:46.394361019 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:48.353187084 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:48.409502029 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 02:37:52.353713989 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:37:52.410011053 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 02:38:00.672314882 CET	53642	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:38:00.735732079 CET	53	53642	8.8.8.8	192.168.2.3
Jan 14, 2021 02:38:09.067884922 CET	55667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:38:09.118848085 CET	53	55667	8.8.8.8	192.168.2.3
Jan 14, 2021 02:38:09.727406979 CET	54833	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:38:09.799846888 CET	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:37:01.914854050 CET	192.168.2.3	8.8.8.8	0x3e3f	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:02.676433086 CET	192.168.2.3	8.8.8.8	0xf40a	Standard query (0)	ny990xqwsj1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:03.929677963 CET	192.168.2.3	8.8.8.8	0x532e	Standard query (0)	renderer-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:04.488121986 CET	192.168.2.3	8.8.8.8	0x8d0e	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.305413008 CET	192.168.2.3	8.8.8.8	0x7929	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.317107916 CET	192.168.2.3	8.8.8.8	0x7753	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:37:06.377032995 CET	192.168.2.3	8.8.8.8	0xce78	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.906306028 CET	192.168.2.3	8.8.8.8	0xff81	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.175900936 CET	192.168.2.3	8.8.8.8	0x4b9e	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:11.950086117 CET	192.168.2.3	8.8.8.8	0xe7da	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:12.674956083 CET	192.168.2.3	8.8.8.8	0x61af	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:13.388638020 CET	192.168.2.3	8.8.8.8	0xef47	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:14.644049883 CET	192.168.2.3	8.8.8.8	0x3082	Standard query (0)	ny990xqwsj 1.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.097661972 CET	192.168.2.3	8.8.8.8	0x42a6	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.531657934 CET	192.168.2.3	8.8.8.8	0xc5d0	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.032516003 CET	192.168.2.3	8.8.8.8	0x2577	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.096211910 CET	192.168.2.3	8.8.8.8	0xdc2f	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.373924971 CET	192.168.2.3	8.8.8.8	0xde3a	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:38:00.672314882 CET	192.168.2.3	8.8.8.8	0xbcee	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 02:37:01.979423046 CET	8.8.8.8	192.168.2.3	0x3e3f	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:02.734812021 CET	8.8.8.8	192.168.2.3	0xf40a	No error (0)	ny990xqwsj 1.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:03.991137981 CET	8.8.8.8	192.168.2.3	0x532e	No error (0)	renderer-a ssets.type form.com	d2citsn5wf4j9j.cloudfront. net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:03.991137981 CET	8.8.8.8	192.168.2.3	0x532e	No error (0)	d2citsn5wf 4j9j.cloud front.net		13.224.94.129	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:03.991137981 CET	8.8.8.8	192.168.2.3	0x532e	No error (0)	d2citsn5wf 4j9j.cloud front.net		13.224.94.58	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:03.991137981 CET	8.8.8.8	192.168.2.3	0x532e	No error (0)	d2citsn5wf 4j9j.cloud front.net		13.224.94.118	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:03.991137981 CET	8.8.8.8	192.168.2.3	0x532e	No error (0)	d2citsn5wf 4j9j.cloud front.net		13.224.94.31	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:04.547466040 CET	8.8.8.8	192.168.2.3	0x8d0e	No error (0)	images.typ eform.com	d2nvsmtq2poimt.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:04.547466040 CET	8.8.8.8	192.168.2.3	0x8d0e	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.83	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:04.547466040 CET	8.8.8.8	192.168.2.3	0x8d0e	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.25	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:04.547466040 CET	8.8.8.8	192.168.2.3	0x8d0e	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.88	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:04.547466040 CET	8.8.8.8	192.168.2.3	0x8d0e	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.92	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.365509987 CET	8.8.8.8	192.168.2.3	0x7929	No error (0)	js-agent.n ewrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:06.378170013 CET	8.8.8.8	192.168.2.3	0x7753	No error (0)	public-ass ets.typefo rm.com	d2p6vz8nayi9a3.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:06.378170013 CET	8.8.8.8	192.168.2.3	0x7753	No error (0)	d2p6vz8nay i9a3.cloud front.net		13.224.94.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:37:06.378170013 CET	8.8.8.8	192.168.2.3	0x7753	No error (0)	d2p6vz8nay i9a3.cloud front.net		13.224.94.107	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.378170013 CET	8.8.8.8	192.168.2.3	0x7753	No error (0)	d2p6vz8nay i9a3.cloud front.net		13.224.94.86	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.378170013 CET	8.8.8.8	192.168.2.3	0x7753	No error (0)	d2p6vz8nay i9a3.cloud front.net		13.224.94.17	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.438112020 CET	8.8.8.8	192.168.2.3	0xce78	No error (0)	cdn.segmen t.com	d296je7bbdd650.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:06.438112020 CET	8.8.8.8	192.168.2.3	0xce78	No error (0)	d296je7bbd d650.cloud front.net		13.224.100.80	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.956945896 CET	8.8.8.8	192.168.2.3	0xff81	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.956945896 CET	8.8.8.8	192.168.2.3	0xff81	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.956945896 CET	8.8.8.8	192.168.2.3	0xff81	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:06.956945896 CET	8.8.8.8	192.168.2.3	0xff81	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		52.34.69.24	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		54.200.56.207	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		54.69.174.156	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		35.161.28.39	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		52.38.215.191	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		54.213.130.70	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		54.201.197.201	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:07.223720074 CET	8.8.8.8	192.168.2.3	0x4b9e	No error (0)	api.segment.io		35.162.116.128	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:12.006634951 CET	8.8.8.8	192.168.2.3	0xe7da	No error (0)	ny990xqwsj 1.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:12.744143009 CET	8.8.8.8	192.168.2.3	0x61af	No error (0)	ny990xqwsj 1.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:13.464698076 CET	8.8.8.8	192.168.2.3	0xef47	No error (0)	images.typ eform.com	d2nvsmtq2poimt.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:13.464698076 CET	8.8.8.8	192.168.2.3	0xef47	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.83	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:13.464698076 CET	8.8.8.8	192.168.2.3	0xef47	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.92	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:13.464698076 CET	8.8.8.8	192.168.2.3	0xef47	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.88	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:13.464698076 CET	8.8.8.8	192.168.2.3	0xef47	No error (0)	d2nvsmtq2p oimt.cloud front.net		13.224.94.25	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:14.700777054 CET	8.8.8.8	192.168.2.3	0x3082	No error (0)	ny990xqwsj 1.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:16.154225111 CET	8.8.8.8	192.168.2.3	0x42a6	No error (0)	images.typ eform.com	d2nvsmtq2poimt.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:37:16.154225111 CET	8.8.8.8	192.168.2.3	0x42a6	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.83	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.154225111 CET	8.8.8.8	192.168.2.3	0x42a6	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.25	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.154225111 CET	8.8.8.8	192.168.2.3	0x42a6	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.88	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.154225111 CET	8.8.8.8	192.168.2.3	0x42a6	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.92	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:16.587994099 CET	8.8.8.8	192.168.2.3	0xc5d0	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:16.587994099 CET	8.8.8.8	192.168.2.3	0xc5d0	No error (0)	d296je7bbdd650.cloudfront.net		13.224.100.80	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		54.71.228.147	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		52.39.24.11	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		52.43.15.143	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		54.200.228.33	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		54.69.66.94	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		52.11.35.251	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		52.35.195.250	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.091814995 CET	8.8.8.8	192.168.2.3	0x2577	No error (0)	api.segment.io		52.38.120.169	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.152664900 CET	8.8.8.8	192.168.2.3	0xdc2f	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:37:17.430097103 CET	8.8.8.8	192.168.2.3	0xde3a	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.430097103 CET	8.8.8.8	192.168.2.3	0xde3a	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.430097103 CET	8.8.8.8	192.168.2.3	0xde3a	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:37:17.430097103 CET	8.8.8.8	192.168.2.3	0xde3a	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 14, 2021 02:38:00.735732079 CET	8.8.8.8	192.168.2.3	0xbcee	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:38:00.735732079 CET	8.8.8.8	192.168.2.3	0xbcee	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.107	A (IP address)	IN (0x0001)
Jan 14, 2021 02:38:00.735732079 CET	8.8.8.8	192.168.2.3	0xbcee	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:38:00.735732079 CET	8.8.8.8	192.168.2.3	0xbcee	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.17	A (IP address)	IN (0x0001)
Jan 14, 2021 02:38:00.735732079 CET	8.8.8.8	192.168.2.3	0xbcee	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.86	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 02:37:04.346510887 CET	13.224.94.129	443	192.168.2.3	49738	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:04.355720997 CET	13.224.94.129	443	192.168.2.3	49739	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:05.104773045 CET	13.224.94.83	443	192.168.2.3	49741	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:05.105020046 CET	13.224.94.83	443	192.168.2.3	49740	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:06.505294085 CET	13.224.94.20	443	192.168.2.3	49744	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:06.505999088 CET	13.224.94.20	443	192.168.2.3	49745	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:06.549537897 CET	13.224.100.80	443	192.168.2.3	49746	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:06.566716909 CET	13.224.100.80	443	192.168.2.3	49747	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:07.254024029 CET	162.247.242.19	443	192.168.2.3	49748	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:07.257832050 CET	162.247.242.19	443	192.168.2.3	49749	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:07.647115946 CET	52.34.69.24	443	192.168.2.3	49750	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:07.943125963 CET	52.34.69.24	443	192.168.2.3	49751	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:13.560971975 CET	13.224.94.83	443	192.168.2.3	49759	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=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 02:37:16.265929937 CET	13.224.94.83	443	192.168.2.3	49762	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		

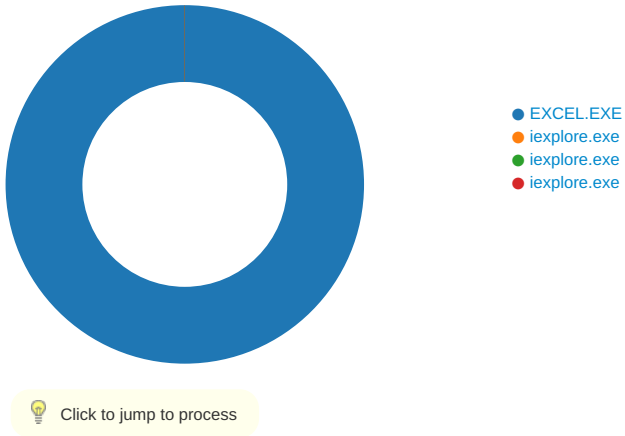
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, 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 02:37:16.266278982 CET	13.224.94.83	443	192.168.2.3	49763	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:16.703676939 CET	13.224.100.80	443	192.168.2.3	49764	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:16.739160061 CET	13.224.100.80	443	192.168.2.3	49765	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:17.509977102 CET	54.71.228.147	443	192.168.2.3	49766	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 02:37:17.736193895 CET	162.247.242.19	443	192.168.2.3	49770	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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 02:37:17.736464024 CET	162.247.242.19	443	192.168.2.3	49771	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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: 6616 Parent PID: 792

General

Start time:	02:36:04
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x9e0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\79D9163B.tmp	success or wait	1	B5495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..xlsx	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	B451E4	WriteFile
C:\Users\user\Desktop\~$ACH REMITTANCE ADVICE..xlsx	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	B45241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	A520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	A5211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	A5213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	A5213B	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 7152 Parent PID: 792

General

Start time:	02:37:00
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:	0x7ff6dd110000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key 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: 5676 Parent PID: 7152

General

Start time:	02:37:01
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:7152 CREDAT:17410 /prefetch:2
Imagebase:	0x120000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key 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: 6340 Parent PID: 7152

General

Start time:	02:37:13
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:7152 CREDAT:17434 /prefetch:2
Imagebase:	0x120000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly