ID: 339405
Sample Name: MALWARE ACH WIRE PAYMENT ADVICE..xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:50:02
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

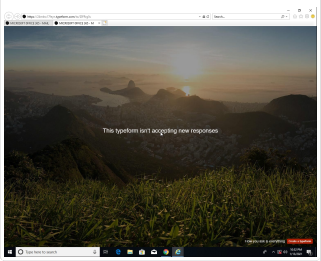
Analysis Report MALWARE ACH WIRE PAYMENT ADVIC…

Overview

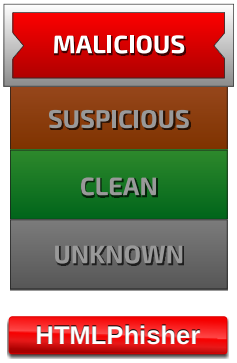
General Information

Sample Name:	MALWARE ACH WIRE PAYMENT ADVICE..xlsx
Analysis ID:	339405
MD5:	a66a202e970df08.
SHA1:	c8986173e16bb9..
SHA256:	e29c6206512f1f7..

Most interesting Screenshot:



Detection

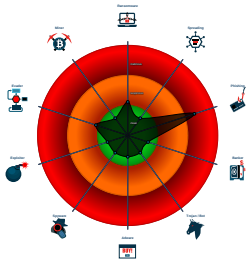


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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: 5656 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- iexplore.exe (PID: 6796 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4780 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5248 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:82946 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

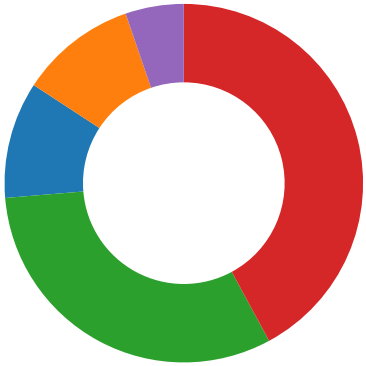
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ZlFRrg5s[2].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ZlFRrg5s[1].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Phishing
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

Phishing:

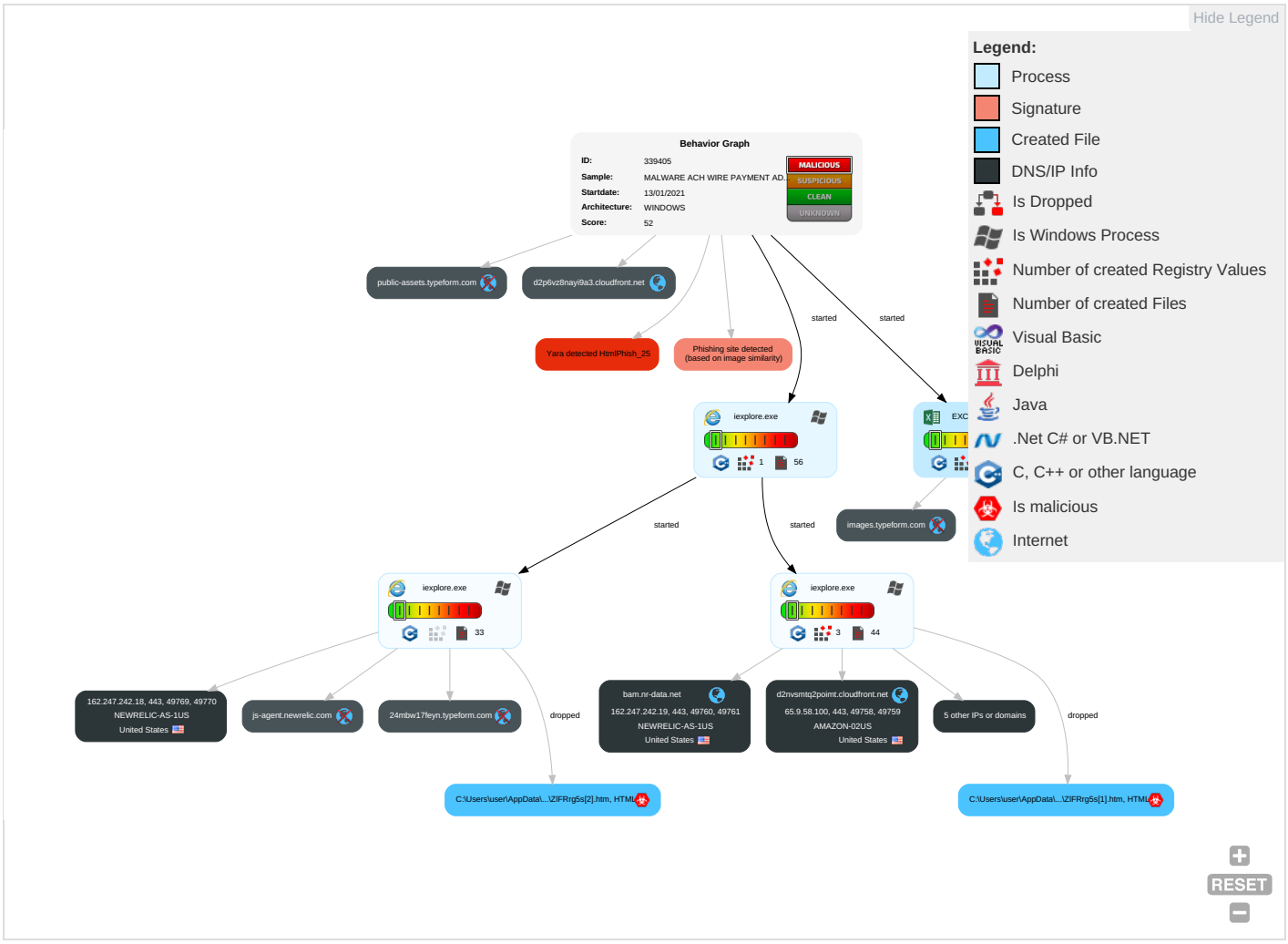
Yara detected HtmlPhish_25

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

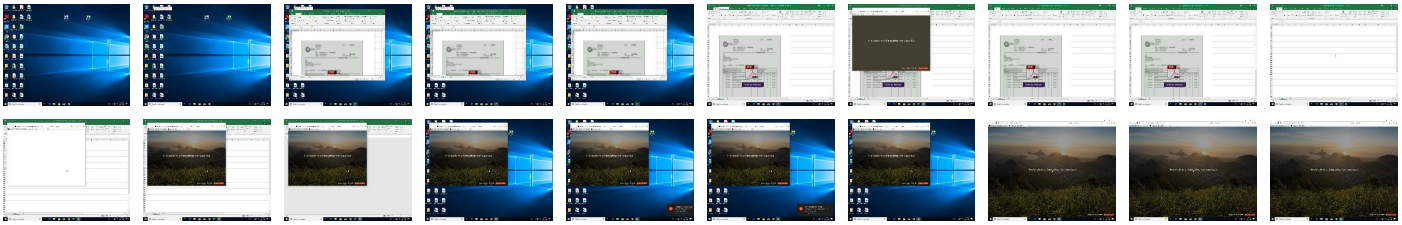
Behavior Graph

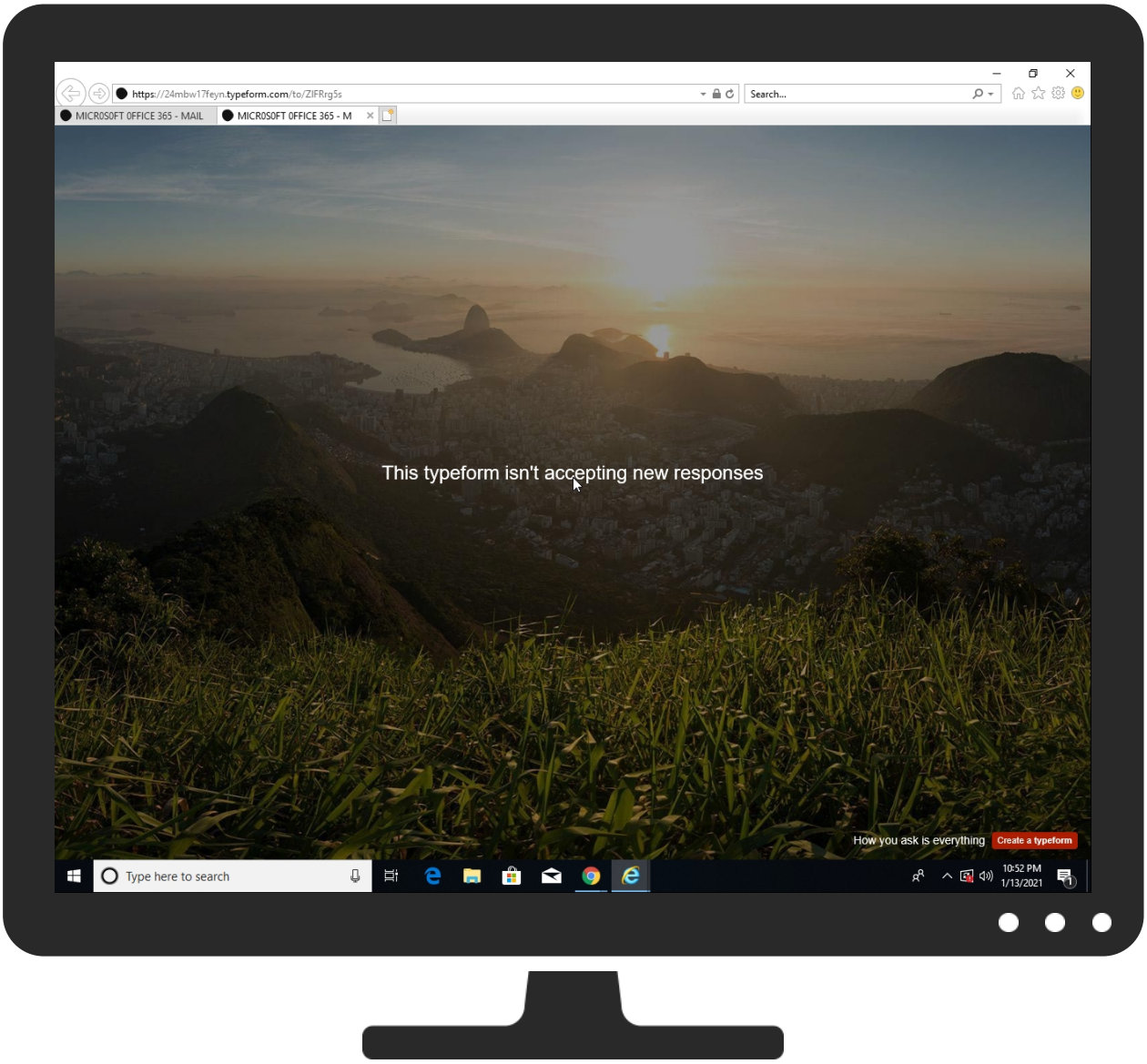


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MALWARE ACH WIRE PAYMENT ADVICE..xlsx	0%	Virustotal		Browse

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

Source	Detection	Scanner	Label	Link
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	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	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://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://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d2nvsmtq2poimt.cloudfront.net	65.9.58.100	true	false		high
bam.nr-data.net	162.247.242.19	true	false	• 0%, Virustotal, Browse	unknown
d2p6vz8nayi9a3.cloudfront.net	65.9.58.120	true	false		high
public-assets.typeform.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
images.typeform.com	unknown	unknown	false		high
24mbw17feyn.typeform.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_medium=typeform&utm_content=typeform-closescreen&utm_term=EN	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s	false		high

URLs from Memory and Binaries

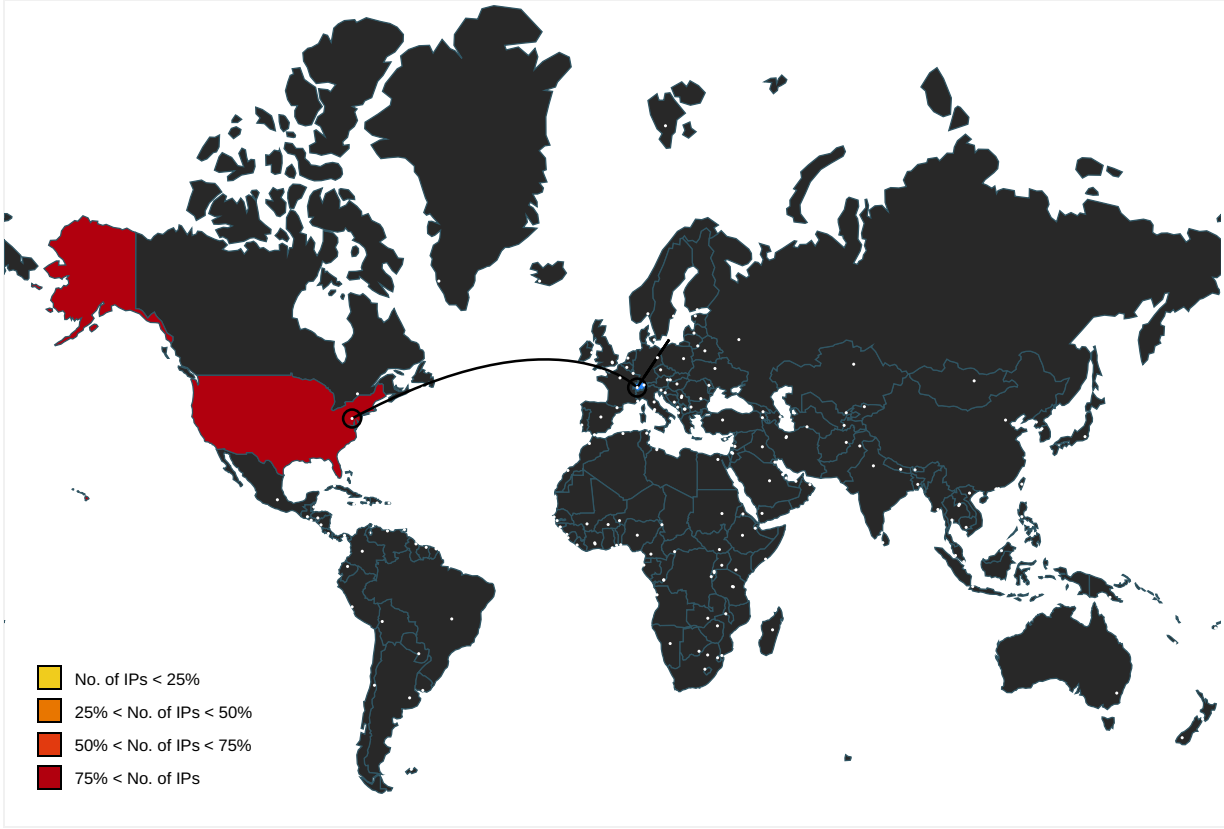
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://login.microsoftonline.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://shell.suite.office.com:1443	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://autodiscover-s.outlook.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-16x16.png	ZlFRrg5s[1].htm.16.dr	false		high
http://https://cdn.entity.	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://wus2-000.contentsync.	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.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	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://cortana.ai	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://public-assets.typeform.com/public/favicon/browserconfig.xml	ZlFRrg5s[1].htm.16.dr	false		high
http://https://public-assets.typeform.com/public/favicon/site.webmanifest	ZlFRrg5s[1].htm.16.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://api.aadrm.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://public-assets.typeform.com/public/favicon/apple-touch-icon.png	ZlFRrg5s[1].htm.16.dr	false		high
http://https://www.typeform.c	{FC4D58F0-5634-11EB-90E5-ECF4BB2D2496}.dat.15.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://api.microsoftstream.com/api/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5sRoot	{FC4D58F0-5634-11EB-90E5-ECF4BB2D2496}.dat.15.dr	false		high
http://https://cr.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_medium=ty	~DF51C6581021C56EF5.TMP.15.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://graph.ppe.windows.net	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://24mbw17feyn.typeform.com/oembed?url=https%3A%2F%2F24mbw17feyn.typeform.com%2Fto%2FZlFRrg5s	ZlFRrg5s[1].htm.16.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://store.officeppe.com/addinstemplate	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://images.typeform.com/images/nXkRcNPp6wtg/background/large);background-position:top	ZlFRrg5s[1].htm.16.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://web.microsoftstream.com/video/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://graph.windows.net	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://dataservice.o365filtering.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png-	imagestore.dat.16.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://weather.service.msn.com/data.aspx	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://apis.live.net/v5.0/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.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	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_m	ZlFRrg5s[1].htm.16.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://management.azure.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png	ZlFRrg5s[1].htm.16.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s6MlCR0S0FT	{FC4D58F0-5634-11EB-90E5-ECF4BB2D2496}.dat.15.dr	false		high
http://https://incidents.diagnostics.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://api.office.net	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://entitlement.diagnostics.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://outlook.office.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://templatelogging.office.com/client/log	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://outlook.office365.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://webshell.suite.office.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://management.azure.com/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://ncus-000.contentsync.	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high
http://https://devnull.onenote.com	E9D02DAF-639A-4CA7-B004-139D7F3D657E.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.9.58.100	unknown	United States		16509	AMAZON-02US	false
65.9.58.120	unknown	United States		16509	AMAZON-02US	false
162.247.242.19	unknown	United States		23467	NEWRELIC-AS-1US	false
162.247.242.18	unknown	United States		23467	NEWRELIC-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339405
Start date:	13.01.2021
Start time:	22:50:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MALWARE ACH WIRE PAYMENT 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:	24
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:	mal52.phis.winXLSX@6/26@12/4
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://24mbw17fe yn.typeform.com/to/ZlFRrg5s • Scroll down • Close Viewer • Browsing link: https://www.typeform.com/? utm_campaign=undefi ned&utm_source=typeform.com-17520522-Free&utm_medium =typeform&utm_content=typeform-closescreen&utm_term=EN
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.109.76.68, 52.109.8.24, 52.109.12.24, 13.88.21.125, 52.255.188.83, 51.11.168.160, 92.122.213.247, 92.122.213.194, 13.64.90.137, 52.155.217.156, 2.20.142.209, 2.20.142.210, 51.103.5.159, 20.54.26.129, 88.221.62.148, 104.18.26.71, 104.18.27.71, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 51.104.139.180, 23.210.248.85, 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, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, random.typeform.com.cdn.cloudflare.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.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, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, f4.shared.global.fastly.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.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
65.9.58.100	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
65.9.58.120	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	
162.247.242.19	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	
	ACH WIRE PAYMENT.xlsx	Get hash	malicious	Browse	
	http://https://mmemicrosoftwebsss.typeform.com/to/sIZVMxGk	Get hash	malicious	Browse	
	http://https://forums.iboats.com/forum/general-boating-outdoors-activities/boat-topics-and-questions-not-user-topics/558373-need-help-from-all-my-tahoe-q4-guys-regaring-smart-tabs-sx	Get hash	malicious	Browse	
	http://https://app.box.com/s/4qh80d5v0isn028co16h3leg3k11ku28	Get hash	malicious	Browse	
	http://https://app.box.com/s/5gniwwclsyw9ejzutmi7mtewylcjhxai	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.247.242.18	http://owoxchweb.emyspot.com/	Get hash	malicious	Browse	• bam.nr-data.net/1/1eb02dae32?a=16828251&v=918.2e0ff1d&to=J1oIRBZeWVQHSxwNBApRD14DHkZQDU4%3D&rst=5148&ap=12&be=3893&fe=1108&dc=825&f=%5B%22err%22,%22xhr%22,%22stn%22,%22ins%22%5D&perf=%7B%22timing%22:%7B%22of%22:1531118387055,%22n%22:0,%22dl%22:0,%22di%22:4547,%22ds%22:4547,%22de%22:4718,%22dc%22:4998,%22l%22:4999,%22le%22:5005,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:42%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan-0289287.pdf	Get hash	malicious	Browse	• bam.nr-data.net/1/be34c3f7ff?a=1795030&pl=1509054230154&v=632.2b17625&to=blwEZERTDEJXUhBZDVcWM0JfHQFeWEILXAcWThFHGV4NVl9fS1kMXVweHkZaEg%3D%3D&be=22892&fe=153&dc=152&f=%5B%5D&perf=%7B%22timing%22:%7B%22of%22:150905423015 4,%22n%22:0,%22dl%22:22600,%22di%22:23065,%22ds%22:23065,%22de%22:23066,%22dc%22:23067,%22l%22:23067,%22le%22:23081,%22f%22:0,%22dn%22:22598,%22dne%22:22598,%22c%22:22598,%22ce%22:22598,%22rq%22:22598,%22rp%22:22600,%22rpe%22:22625%7D,%22navigation%22:%7B%7D%7D&at=QhsHEgxJH0w%3D&jsonp=NREUM.setToken

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d2p6vz8nayi9a3.cloudfront.net	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.120
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 13.224.194.7
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 13.224.194.82
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.117
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.117
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.24
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.31
	http://https://kevindenkmann.typeform.com/to/rZWKMQjQ	Get hash	malicious	Browse	• 65.9.20.8
	http://https://mmemicrosoftwebsss.typeform.com/to/sIZVMxGk	Get hash	malicious	Browse	• 13.224.102.23
	http://https://onedriveonlinemicrosoft.typeform.com/to/EM15DyjP	Get hash	malicious	Browse	• 13.224.102.23
	http://https://avecassurance.typeform.com/to/Mfo29tYj	Get hash	malicious	Browse	• 13.225.25.26
	Welcome to your new OneDrive!.pdf	Get hash	malicious	Browse	• 54.192.216.121
bam.nr-data.net	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.19
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.19
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 162.247.242.21

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 162.247.242.21
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 162.247.242.21
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 162.247.242.20
	http://https://bit.do/fLVUm	Get hash	malicious	Browse	• 162.247.242.21
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Fbit.do%2FfLVUm%3Ffbclid%3DIwAR3_y5be7qgzc9rWXbeIQlHePNYF96mJvcjTtfijse-VyaDOGbdXhiymogA&h=AT2La9RfuL-CBpF75ix5HdI9lLnyapdVZIzXgRQt4G1Y7x5nZpCr9RLeZPnCT8_3vYaiFFnwir6t35RvMH3lJhYuYrzugBPtxdx4PUirtTUjKnczau25WjD4XcXiFnckifU	Get hash	malicious	Browse	• 162.247.242.21
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 162.247.242.20
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706574475616c2e636f6d2e6175	Get hash	malicious	Browse	• 162.247.242.18
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 162.247.242.21
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 162.247.242.19
	http://view.e.business.officedepot.com/?qs=3fe5dee3fd6dc334e57f4fe8c13caa1dc833d1845b46e0df5e76d8dcd189c65840b833e5f8853ee5eca50625943bfd8b71f0d693bc12eda6d7c035c0df2243dc5fe3f7c370b5320b8fd654c8b827b865	Get hash	malicious	Browse	• 162.247.242.18
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.21
d2nvsmtq2poimt.cloudfront.net	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.16
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 143.204.93.16
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.87
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.109
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.88
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.98
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 13.224.94.83
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 143.204.90.37
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 13.224.93.102
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.20
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.90.8
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.87
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.226.169.98
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 65.9.68.116
	ACH WIRE PAYMENT REMITTANCE ._ (002).xlsx	Get hash	malicious	Browse	• 13.224.93.75
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 13.224.93.75
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 13.224.93.75
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 143.204.208.61
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 143.204.208.119

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 34.213.143.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 3.13.31.214
AMAZON-02US	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
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 34.213.143.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 3.13.31.214
NEWRELIC-AS-1US	MALWARE ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 162.247.242.21
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.18
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 162.247.242.19
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 162.247.242.20
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 162.247.242.20
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 162.247.242.20
	http://https://bit.do/fLVUm	Get hash	malicious	Browse	• 162.247.242.21
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Fbit.do%2FfLVUm%3Ffbclid%3DIwAR3_y5be7qgzc9rWXbeIQlHePNYF96mJvcjTtfijse-VyaDOGbdXhiymogA&h=AT2La9RfuL-CBpF75ix5HdI9ILnyapdVZIzXgRQt4G1Y7x5nZpCr9RLeZPnCT8_3vYaiFFnwir6t35RvMH3lJhYuYrzugBPtxdx4PUirtTUjKnczau25WjD4XcXiFnckifU	Get hash	malicious	Browse	• 162.247.242.21
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 162.247.242.20
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706574756 16c2e636f6d2e6175	Get hash	malicious	Browse	• 162.247.242.18
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 162.247.242.18
	http://https://documentaxxxxxxxxckcnq009sos.typeform.com/to/jLMhWTCn	Get hash	malicious	Browse	• 162.247.242.19
	http://view.e.business.officedepot.com/?qs=3fe5dee3fd6dc334e57f4fe8c13caa1dc833d1845b46e0df5e76d8dcd189c65840b833e5f8853ee5eca50625943bfd8b71f0d693bc12eda6d7c035c0df2243dc5fe3f7c370b5320b8fd654c8b827b865	Get hash	malicious	Browse	• 162.247.242.18
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	ACH_WIRE_REMITTANCE_PAYMENT_ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.20
	http://https://www.freightwaves.com/news/canadian-fuel-distributor-parkland-targeted-in-cyberattack	Get hash	malicious	Browse	• 162.247.242.19

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	AS006-20211201.pdf.exe	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	DataServer.dll	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	nsaCDED.dll	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202114170492f#U0433#U03bfm+19796076561 19796076561.HTM	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	PolicyUpdate.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	l0sjk3o.dll	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	COMFAM INVOICE.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	P396143.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	sfk_setup.exe	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
	P166824.htm	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	e-card.htm .exe	Get hash	malicious	Browse	• 65.9.58.100 • 162.247.242.18 • 65.9.58.120 • 162.247.242.19
37f463bf4616ecd445d4a1937da06e19	Notification_71823.xls	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202114170492f#U0433#U03bfm+19796076561 19796076561.HTM	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	J04gSlH5wR.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	rufus-2.9.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Invoice-ID43739424297.vbs	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Customer_Receivables_Aging_20210112_2663535345242424242.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Listings.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Transferencia,pdf.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Dhl Client Invoice.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	64D5aP6jQz.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	P396143.htm	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	Code.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	UbisoftInstaller.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	New inquiry CON 20-10630.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	RLFGB8pdA6.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120
	MPnIQlfxon.exe	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\24mbw17feyn.typeform[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FC4D58EE-5634-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42072
Entropy (8bit):	1.9418441075907897
Encrypted:	false
SSDEEP:	192:rVZiZn2s9Wvt4fm1MnK9ykfVJMr2+SfzcW:rb+2sU1GLnK9yKVU2+QR
MD5:	F1EB8013875B0503170473D84856EE27
SHA1:	A5E686B18B7D24F7E48F1D4F1AD50B6654CD9186
SHA-256:	AEA970E81922C3CC17C662EC662A13F0C0615433E59CB5C491C048EF6303E49B
SHA-512:	A17689DDC0B0DC2DA08225C82C83B6F6F8E7F0BB16E212767F5FF37480F85E5992BCF62602EF629860E90F4AC2B3C8EF5DFEB7D4C91C2F4C753E8F31D869BEB
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\{06866D36-5635-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566503333055085
Encrypted:	false
SSDEEP:	48:IwyGcpr7GwpaqG4pQWGrapbSFrGQpKQG7HpRQsTGIpG:rGZVQK6YBSFFArTQ4A
MD5:	ACBCE55087B43222397873A624D04A44
SHA1:	00FD6040779F106C072F8853493CA37A5B443044
SHA-256:	51991AB5D34C019FFD133528F42339883773BB9D8AB1A97941249B65573A6815
SHA-512:	9D6AC38A6C1F76A60FBCB34F18BB1AA5D9962A62D30D186CC2CEAAD8AFC0F44A244A02B65F5773FD8F26B21242682B10BA863A3FEEF12BA40D1B601E8F1448AC
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\{FC4D58F0-5634-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	44148
Entropy (8bit):	2.0287823179173476
Encrypted:	false
SSDEEP:	384:rsoeiJhESzVWJ1Rqwd1m9/13PwT9+421V9UV1GPwT9E:TcwHiuJiq
MD5:	250F510BB5CE71E99E3878F9DCA8ABC1
SHA1:	801733BC9CD77F5A979C837415473E7088322033
SHA-256:	F16FA65645C2B65FFC2C9D19F3D127A282CE6F8C72F2C6E9B6D8CC76FCAC10FD
SHA-512:	2D5F156B8C2F1F7226909F8C4B449500F421103F4106DEB5D9AD706B195411746D0B67FF00DE806ABE80B9367C7B4FCF4598A3A944D74166EDDA8738E8748953
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\{FC4D58F1-5634-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26428
Entropy (8bit):	1.668257695265872
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC4D58F1-5634-11EB-90E5-ECF4BB2D2496}.dat	
SSDEEP:	96:rSrZ8mQH6BBSTFhS5K7SQ2C0Kx5izc2pahB:rSrZ8mQH6BkTFE5K7SQ2C0K3izc2pahB
MD5:	4B356EBE4FC6412723DA25C7CA46B9F9
SHA1:	C58BE6D0F7081A09B46E6EC7B43CFE83995268A0
SHA-256:	B40FC39E6D6D41363CF033861950DF942DE4128C57383E089643F8228445D2B2
SHA-512:	7B42AC6FC9ECE1BA2A5D65B9359B06BD83631AEAB6DFA27725DDA42E3691936FB17A40415BFDBFEDF655F3386766B2342D50FC232416FB620FEB54F72365785C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1241
Entropy (8bit):	7.239044094211204
Encrypted:	false
SSDEEP:	24:Yt4/pSym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02EfIH6l:YUx0v9PoQ5VqKwspEeV6l
MD5:	E334507E2BCC05FD24EEEE96F9288311
SHA1:	108C46F9A1C2167DE8D90A5DA5E9251061E27ECB
SHA-256:	052A97D706B4828FD9A36EA94BAC92F82BB50278163D86CD915D70B64AEA7B7B
SHA-512:	5288851FFBDE7C5FAF9E765462EFAF00D42A4B168B7305F801B77FE71E51B9D9D4BFAF50D2EEC99E9A0B695CE611168BD4B4B6E62E4365658336BAB821EA1CD7
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\E9D02DAF-639A-4CA7-B004-139D7F3D657E	
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):	5.37291559797381
Encrypted:	false
SSDEEP:	1536:TcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:XrQ9DQW+zBX8P
MD5:	DF163976C93D0D201C34C2012ACFBCDA
SHA1:	B05A8A9BAE729D4F8BCADBE331971BD6B4FB634E
SHA-256:	5CA742085EB32C6DE8A8300B22C924CD7CD52D7D59B2D89A2120F11792E0F81A
SHA-512:	F49610B7CF86D56AA37FCF6113933931D78F2086F4A5585DD1D60C411B5380492E4341642276F9271787A201C0E8AD13A39E5B5CBAC4BB1FE88C33DA788C0717
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="2021-01-13T21:50:59">.. Build: 16.0.13710.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>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\79E5A9C2.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\79E5A9C2.jpeg	
SHA-512:	68C2826235479DC52C10A6EAF078BA3FA0D77120517D608A69349258F5C3646382431CCDA4AEEBCA1026EE877AE180F06E44E6FDD6888681C660D053EA3427B/
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\3Y2ADQKS\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
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #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: #000000;.. 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\3Y2ADQKS\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\3Y2ADQKS\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..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`.

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\httpErrorPagesScripts[1]</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode (with BOM) text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>12105</td></tr>
<tr><td>Entropy (8bit):</td><td>5.451485481468043</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f</td></tr>
<tr><td>MD5:</td><td>9234071287E637F85D721463C488704C</td></tr>
<tr><td>SHA1:</td><td>CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152</td></tr>
<tr><td>SHA-256:</td><td>65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649</td></tr>
<tr><td>SHA-512:</td><td>87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>res://ieframe.dll/httpErrorPagesScripts.js</td></tr>
<tr><td>Preview:</td><td>...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file):///", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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/nXkRcNPp6wtg/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*..

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\nr-1123.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines, with no line terminators</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>24380</td></tr>
<tr><td>Entropy (8bit):</td><td>5.3039076589847856</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:yNeRyajOhmUdGa4PFaOy0hGF1Ux9EmiwbikgkYPMvFzoUMC0GPwi5MteM7gN+u:yNP0HgGa4P7x+XM9zoJmlGtGN+u</td></tr>
<tr><td>MD5:</td><td>7FFB242072196E9DB5F4F1BFBFA2ED7D</td></tr>
<tr><td>SHA1:</td><td>6CFD443F06C2D4E96E14765E045277B67DA0EEC5</td></tr>
<tr><td>SHA-256:</td><td>94CDF5B7F868883DE0E1248CD80B42DD84E3F38685F2B234747550C02190DC82</td></tr>
<tr><td>SHA-512:</td><td>371BCC019D60EDBC2DD331F379AC46951B6D8E50FCA25FC79062C02F4E78A6B41DC884C590FD2E8F47EDE8BC392F3A84B0CFE102386282504538BFD157848B</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://js-agent.newrelic.com/nr-1123.min.js</td></tr>
<tr><td>Preview:</td><td>!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</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\LnkQ4hGmxTTD[1].png	
Size (bytes):	11245
Entropy (8bit):	7.975358433194237
Encrypted:	false
SSDEEP:	192:mbz+31SP85NJJDasl02Sj6cPXana59Wh50KH83Yh7Ewnp4Un5To75yhoEbN:ONIlSB/aabCeHSEwnp4UnpoFhEbN
MD5:	9936A0F33BBE88F448A1E166B8CCD4A9
SHA1:	EBBE8544383B73EB0C8BA6733B3588F7781B5B23
SHA-256:	B0CF2B3D20750F69559365B1926CA243502BE1E58EFBCB45E8315C943BE1BCDF
SHA-512:	58BD2ECF7E1DADBC96DF63B01595C5B8E5E9301B5AC55645B6F36C4B831F39E89375476076CCCC20204B53960C153FBF1103710A74DC41EEBC23C5ABAD58140
Malicious:	false
IE Cache URL:	http://https://images.typeform.com/images/LnkQ4hGmxTTD
Preview:	.PNG.....IHDR.....m.....+.IDATx..].x.U.^.H.d..f..l(b.....`.....)...g..SJ...M.....bGQ." *.;**...M#$.....L.....s.Mvgvg.{.{.s.....V.....'.YR.s..?-e..V..t.....SE0..%...V..e.....-.....r.[..=_..W.....(.g..KC.....[...8.X..;`S .U..=.('.....S,..Z..Gq.....,..W...p._...o.?.>....c....?.....A....Q..].s....+..^*..NOj..Y....%..3.&.n.....b..0...B.....!$G..rN....+.r..tL...M.(.{XY..*.F6....]RY....Y..XS=9$..k...k....$.....S0.'c.~.....|.z.....*.A..)...._.#..QN....&.....P.U8..%.vM+....B..1.?..UP.....3..f.....J.@.h....xc$..5...a>~....1..&.v^... ....*f....5.C3.g.).c.#..._J.....Z.jWO.f...9w.q...o(...&i%L....#V.\,.,..4M@.W..ZQ`.P..T.....5K...w..}.Jsj.ZR.W`x.f.3.\....C.J.*.*R...g..S2.qx...&N.yr.B...0..'.....,....`:0A..%.\.A^%fa.....y}.+..6i..fx..d..8..).e@..Uk.}...S..M8..}.:.Qk..K.S...[...H.T.Bh..i..\'..%..$Q..W....el.....ru.._....ySy..t..ZR..b.V.:.M.....`:.9.L[.V...Mu...U.7X.....3.G..9.....Z....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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\OTUW0Q90\ZlFRrg5s[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):	47327
Entropy (8bit):	5.405580504251236
Encrypted:	false
SSDEEP:	768:Z4/WZQ7GyOGtbkTKZp05mKXyyos3XnhyVOZQYI:ZsWLCJ05x93XYYI
MD5:	DDF03CF31DDB2D4BDBF4F0F041E58FFE
SHA1:	CE18D64A5FE8AAF91C2C583483A74944877988E5
SHA-256:	2CBBB66DF6458F334886A95EA557AA8A78FE0E9134A1F5A8D68E71E5EFC58C75
SHA-512:	850B93073547A6857A645E901292B851F27EE539866D057185A22A89A9777630F1EC9C45B84551D8A715DEC4CD90F21F457A973EE70DAFA7FDC4111B8CE490AF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_25, Description: Yara detected HtmlPhish_25, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ZlFRrg5s[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\OTUW0Q90\ZlFRrg5s[2].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):	47327

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ZlFRrg5s[2].htm	
Entropy (8bit):	5.405580504251236
Encrypted:	false
SSDEEP:	768:Z4/WZQ7GyOGtbkTKZp05mKXyyos3XnhyVOZQYI:ZsWLCJ05x93XYYI
MD5:	DDF03CF31DDB2D4BDBF4F0F041E58FFE
SHA1:	CE18D64A5FE8AAF91C2C583483A74944877988E5
SHA-256:	2CBBB66DF6458F334886A95EA557AA8A78FE0E9134A1F5A8D68E71E5EFC58C75
SHA-512:	850B93073547A6857A645E901292B851F27EE539866D057185A22A89A9777630F1EC9C45B84551D8A715DEC4CD90F21F457A973EE70DAFA7FDC4111B8CE490AF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_25, Description: Yara detected HtmlPhish_25, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ZlFRrg5s[2].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\OTUW0Q90\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\OTUW0Q90\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
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\OTUW0Q90\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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon-32x32[1].png</th></tr>
<tr><td>SHA-512:</td><td>5DB18A7D2A60BD729F6F12E8A9B05F7A15E90C68CF3415993E8A5B1DB2B5BBA0D4B34B3F2A989E47C7495B9CF202703F0E50694E8865B0784A88EC1A40AF878</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png</td></tr>
<tr><td>Preview:</td><td>.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 i ptc..x.....qV((.</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF51C6581021C56EF5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	48473
Entropy (8bit):	0.5794886893099513
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+kCo5i5x3CmV/La8lHfwUnCmM/La8lHvdCmn/La8lH:kBqoxKAuqR+kCo5i5x31XBwu1Gxd1V
MD5:	E368631D5C0DEB2D0E92255CBA5D5664
SHA1:	AE83B54E60136766FDF3936685E474D550811CBA
SHA-256:	E60B329A0A0010E5C5A1C6411BBAC05EBEBEB8809E9CDEDF705B9A88CFC143ED
SHA-512:	43F15B6E7A304778E2ED3AA1C82DF9FDC10DCB424CC70AAC9558E899141A0617C2D6BDFF99CA952DEA3E6D6E1FB55D685A28767E87B40383B4E65BB74A09AE 40
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDFF887D055A021F6.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\~DFEEEF4F44F2D8283B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38485
Entropy (8bit):	0.35860375685684465
Encrypted:	false
SSDEEP:	48:kBqoxKAuvS8SkH2zHzXz9DzGyDqn0z+hCjUK:kBqoxKAuvS8SkH2zHzXz1ze0z+hs
MD5:	94650DE722D3C7B9FA039637D52F565B
SHA1:	5A0AA4C20AE25614707856ED41D4DF96262A2852
SHA-256:	FD27EE717FDB7F609886B2B00E3E8B31579E1A371982637B2012E471D37777D6
SHA-512:	F55472C622C92981DE1A42C23DEAD3521BB27EBDFAB35230A75ADB5126C86B8333D9542F9CB3578E92B9F44FBF0AF71758D3F10CC2DBDCD9F4EE9CE90BF37 5C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF6F9769A935F1716.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13221
Entropy (8bit):	0.6075213731302237
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo79lo79lWQxv/MskAw0:kBqoI8Cw
MD5:	23627A3180D1ADCB0C9908297CE2B5A3
SHA1:	366C7D91A8C864554FD5611C863F24773A62F171
SHA-256:	4C3301B918B942371D1640A5342E72291D5C720AB2BBF8BF584A2815A7C3F9C5
SHA-512:	B6D45A771FBEEDF681ED8D399E4FF86517FB551F952CA10A4CF882463B33D8EE1B74CBD1234FC16C8E647095EE7B4848B7089BEAE417F78BC311D853431D8C8 9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT ADVICE..xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C 7
Malicious:	false
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.657144801353107
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	MALWARE ACH WIRE PAYMENT ADVICE..xlsx
File size:	76184
MD5:	a66a202e970df086cc265cb646127bfb
SHA1:	c8986173e16bb9b0703490afba594ec5eef08a4a
SHA256:	e29c6206512f1f778f1af9a1ff2af2bb82107271e00c873930398b703294d75e
SHA512:	c4abfe1cb7af45bcde87899efc3d07ce1f54395140ce2709b95608113af6c65ea4aa7d4b763b1fdf67599f42502684dfb33db161be6f0a13b81be3cc861f0e52
SSDEEP:	1536:ExGP/kQbgQywBGmkla+bsaCaWyVvXmkXwhHFo:Ec3FgQxFklapal0o
File Content Preview:	PK.....!..0. .....[Content_Types].xml ...(..... ....

File Icon

	
Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

Network Port Distribution

Total Packets: 105

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:51:57.618689060 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.618897915 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.658435106 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.658482075 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.661434889 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.661493063 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.662581921 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.665467024 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.692908049 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.693479061 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.703743935 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.704205036 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.704231977 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.704257011 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.706265926 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.706581116 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.706599951 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.706614971 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.707178116 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.707976103 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.708368063 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.708388090 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.708884001 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.712383986 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.719280005 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.719757080 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.720046997 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.720709085 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.721163988 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.732677937 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.733072996 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.734102964 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.734113932 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.735588074 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.735611916 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.759210110 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.760041952 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.761929989 CET	443	49755	65.9.58.120	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:51:57.761955976 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.761974096 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.761990070 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.762006044 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.762028933 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.762046099 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.762481928 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.762500048 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.763370037 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.763411045 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.768451929 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.768846989 CET	49754	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.769937038 CET	49755	443	192.168.2.6	65.9.58.120
Jan 13, 2021 22:51:57.775409937 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.775439978 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.775804043 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.775877953 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.775898933 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.775957108 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.776031971 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.776051044 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.778045893 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.779850960 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.780035973 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.782078981 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.795938969 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.808159113 CET	443	49755	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.808402061 CET	443	49754	65.9.58.120	192.168.2.6
Jan 13, 2021 22:51:57.814040899 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.855956078 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.857656002 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.859400034 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.859950066 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.860327005 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.895958900 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.896339893 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.896501064 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.897922039 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.898207903 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.899656057 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.899787903 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.899801970 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.899960995 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.899974108 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.900104046 CET	443	49759	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.900585890 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.900696993 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.901078939 CET	49758	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.901245117 CET	49759	443	192.168.2.6	65.9.58.100
Jan 13, 2021 22:51:57.904980898 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905013084 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905030966 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905047894 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905067921 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905088902 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.905868053 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.906017065 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.907166958 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.907192945 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.908166885 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.908191919 CET	443	49758	65.9.58.100	192.168.2.6
Jan 13, 2021 22:51:57.909317970 CET	443	49758	65.9.58.100	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:50:59.371241093 CET	58384	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:50:59.429884911 CET	53	58384	8.8.8.8	192.168.2.6
Jan 13, 2021 22:50:59.863677025 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:50:59.932600021 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:00.874387980 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:00.930651903 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:01.889663935 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:01.949326038 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:03.905915022 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:03.962312937 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:07.921549082 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:07.977792025 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:08.871186972 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:08.919209003 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:11.682442904 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:11.741838932 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:12.824217081 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:12.872309923 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:13.646181107 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:13.705759048 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:14.466227055 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:14.525917053 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:15.268739939 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:15.325067997 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:16.414292097 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:16.465138912 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:17.265610933 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:17.313638926 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:18.386339903 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:18.390455961 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:18.437463999 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:18.448796034 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:19.548613071 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:19.605252028 CET	53	63307	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:23.337635040 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:23.398334980 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:27.387453079 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:27.435447931 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:28.196722984 CET	50010	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:28.244683981 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:29.453263998 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:29.504985094 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:36.822719097 CET	62116	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:36.870976925 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:37.623783112 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:37.674571991 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:38.053783894 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:38.114690065 CET	53	55014	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:38.213444948 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:38.237400055 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:38.277772903 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:38.293848038 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:38.446774006 CET	51818	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:38.505980968 CET	53	51818	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:38.729199886 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:38.787534952 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:39.213207960 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:39.276784897 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:39.562308073 CET	53799	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:39.621589899 CET	53	53799	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:39.816159964 CET	54683	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:39.864032030 CET	53	54683	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:40.447916031 CET	59329	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:40.497940063 CET	53	59329	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:51:41.297344923 CET	64021	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:41.345345020 CET	53	64021	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:42.363348961 CET	56129	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:42.419841051 CET	53	56129	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:43.192054987 CET	58177	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:43.248392105 CET	53	58177	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:45.850908041 CET	50700	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:45.908791065 CET	53	50700	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:54.915931940 CET	54069	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:54.978532076 CET	53	54069	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:56.326149940 CET	61178	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:56.391632080 CET	53	61178	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:57.542036057 CET	57017	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:57.605716944 CET	53	57017	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:57.612813950 CET	56327	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:57.622381926 CET	50243	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:57.670505047 CET	53	56327	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:57.681005001 CET	53	50243	8.8.8.8	192.168.2.6
Jan 13, 2021 22:51:58.228162050 CET	62055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:51:58.276146889 CET	53	62055	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:02.826802015 CET	61249	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:02.886157036 CET	53	61249	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:03.602689981 CET	65252	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:03.659049988 CET	53	65252	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:04.352720022 CET	64367	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:04.411977053 CET	53	64367	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:05.525481939 CET	55066	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:05.595688105 CET	53	55066	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:06.478426933 CET	60211	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:06.535959959 CET	53	60211	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:06.753577948 CET	56570	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:06.801414967 CET	53	56570	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:23.012975931 CET	58454	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:23.060898066 CET	53	58454	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:23.778888941 CET	55180	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:23.837110996 CET	53	55180	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:24.910330057 CET	58721	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:24.961242914 CET	53	58721	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:25.694274902 CET	57691	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:25.750886917 CET	53	57691	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:25.923122883 CET	58721	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:25.974016905 CET	53	58721	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:26.689341068 CET	57691	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:26.737471104 CET	53	57691	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:26.925797939 CET	58721	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:26.976628065 CET	53	58721	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:27.704539061 CET	57691	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:27.752531052 CET	53	57691	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:28.923640013 CET	58721	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:28.983098984 CET	53	58721	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:29.705168962 CET	57691	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:29.761420012 CET	53	57691	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:32.939722061 CET	58721	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:32.990437984 CET	53	58721	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:33.721203089 CET	57691	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:33.769216061 CET	53	57691	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:35.001910925 CET	52943	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:35.058449984 CET	53	52943	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:36.017735958 CET	52943	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:36.073874950 CET	53	52943	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:37.017766953 CET	52943	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:37.074093103 CET	53	52943	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:39.036242962 CET	52943	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:39.084233999 CET	53	52943	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:52:43.042478085 CET	52943	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:43.090298891 CET	53	52943	8.8.8.8	192.168.2.6
Jan 13, 2021 22:52:52.678906918 CET	59489	53	192.168.2.6	8.8.8.8
Jan 13, 2021 22:52:52.738214016 CET	53	59489	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 22:51:56.326149940 CET	192.168.2.6	8.8.8.8	0x2a54	Standard query (0)	24mbw17feyn.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.542036057 CET	192.168.2.6	8.8.8.8	0x2252	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.612813950 CET	192.168.2.6	8.8.8.8	0xb06c	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.622381926 CET	192.168.2.6	8.8.8.8	0xdd60	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:58.228162050 CET	192.168.2.6	8.8.8.8	0x5ff6	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:02.826802015 CET	192.168.2.6	8.8.8.8	0xb095	Standard query (0)	24mbw17feyn.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:03.602689981 CET	192.168.2.6	8.8.8.8	0xc271	Standard query (0)	24mbw17feyn.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:04.352720022 CET	192.168.2.6	8.8.8.8	0x5681	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:05.525481939 CET	192.168.2.6	8.8.8.8	0x4e41	Standard query (0)	24mbw17feyn.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:06.478426933 CET	192.168.2.6	8.8.8.8	0x8321	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:06.753577948 CET	192.168.2.6	8.8.8.8	0x1b96	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:52.678906918 CET	192.168.2.6	8.8.8.8	0xdcae	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 22:51:56.391632080 CET	8.8.8.8	192.168.2.6	0x2a54	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:51:57.605716944 CET	8.8.8.8	192.168.2.6	0x2252	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:51:57.605716944 CET	8.8.8.8	192.168.2.6	0x2252	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.120	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.605716944 CET	8.8.8.8	192.168.2.6	0x2252	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.128	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.605716944 CET	8.8.8.8	192.168.2.6	0x2252	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.605716944 CET	8.8.8.8	192.168.2.6	0x2252	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.37	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.670505047 CET	8.8.8.8	192.168.2.6	0xb06c	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:51:57.681005001 CET	8.8.8.8	192.168.2.6	0xdd60	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:51:57.681005001 CET	8.8.8.8	192.168.2.6	0xdd60	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.681005001 CET	8.8.8.8	192.168.2.6	0xdd60	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.681005001 CET	8.8.8.8	192.168.2.6	0xdd60	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:57.681005001 CET	8.8.8.8	192.168.2.6	0xdd60	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:58.276146889 CET	8.8.8.8	192.168.2.6	0x5ff6	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 22:51:58.276146889 CET	8.8.8.8	192.168.2.6	0x5ff6	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:58.276146889 CET	8.8.8.8	192.168.2.6	0x5ff6	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 13, 2021 22:51:58.276146889 CET	8.8.8.8	192.168.2.6	0x5ff6	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:02.886157036 CET	8.8.8.8	192.168.2.6	0xb095	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:03.659049988 CET	8.8.8.8	192.168.2.6	0xc271	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:04.411977053 CET	8.8.8.8	192.168.2.6	0x5681	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:04.411977053 CET	8.8.8.8	192.168.2.6	0x5681	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:04.411977053 CET	8.8.8.8	192.168.2.6	0x5681	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:04.411977053 CET	8.8.8.8	192.168.2.6	0x5681	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:04.411977053 CET	8.8.8.8	192.168.2.6	0x5681	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:05.595688105 CET	8.8.8.8	192.168.2.6	0x4e41	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:06.535959959 CET	8.8.8.8	192.168.2.6	0x8321	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:06.801414967 CET	8.8.8.8	192.168.2.6	0x1b96	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:06.801414967 CET	8.8.8.8	192.168.2.6	0x1b96	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:06.801414967 CET	8.8.8.8	192.168.2.6	0x1b96	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:06.801414967 CET	8.8.8.8	192.168.2.6	0x1b96	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:52.738214016 CET	8.8.8.8	192.168.2.6	0xdcae	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:52:52.738214016 CET	8.8.8.8	192.168.2.6	0xdcae	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.120	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:52.738214016 CET	8.8.8.8	192.168.2.6	0xdcae	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.128	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:52.738214016 CET	8.8.8.8	192.168.2.6	0xdcae	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 13, 2021 22:52:52.738214016 CET	8.8.8.8	192.168.2.6	0xdcae	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.37	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 22:51:57.707178116 CET	65.9.58.120	443	192.168.2.6	49755	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 13, 2021 22:51:57.708884001 CET	65.9.58.120	443	192.168.2.6	49754	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 13, 2021 22:51:57.778045893 CET	65.9.58.100	443	192.168.2.6	49758	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 13, 2021 22:51:57.779850960 CET	65.9.58.100	443	192.168.2.6	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		

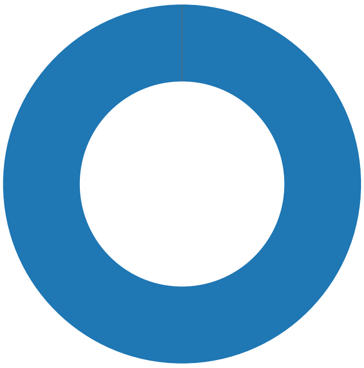
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 22:51:58.604672909 CET	162.247.242.19	443	192.168.2.6	49760	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 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 13, 2021 22:51:58.616316080 CET	162.247.242.19	443	192.168.2.6	49761	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 13, 2021 22:52:04.497446060 CET	65.9.58.100	443	192.168.2.6	49764	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 13, 2021 22:52:07.106585979 CET	162.247.242.18	443	192.168.2.6	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 22:52:07.106663942 CET	162.247.242.18	443	192.168.2.6	49769	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 13, 2021 22:52:52.829714060 CET	65.9.58.120	443	192.168.2.6	49775	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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5656 Parent PID: 792

General

Start time:	22:50:57
Start date:	13/01/2021
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:	0xa80000
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\463EEADB.tmp	success or wait	1	BF495B	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\~$MALWARE ACH WIRE PAYMENT 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	BE51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT 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	BE5241	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	AF20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	AF211C	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	AF213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	AF213B	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 6796 Parent PID: 792

General

Start time:	22:51:54
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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	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: 4780 Parent PID: 6796

General

Start time:	22:51:54
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
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

Analysis Process: iexplore.exe PID: 5248 Parent PID: 6796

General

Start time:	22:52:04
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:82946 /prefetch:2
Imagebase:	0x20000
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

Disassembly