ID: 339405
Sample Name: MALWARE ACH WIRE PAYMENT ADVICE..xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:43:44
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

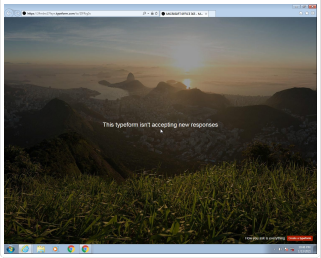
Analysis Report MALWARE ACH WIRE PAYMENT ADVIC…

Overview

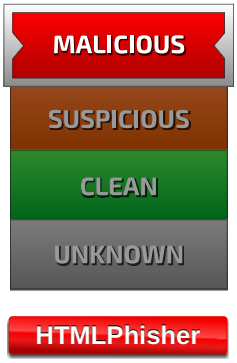
General Information

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

Most interesting Screenshot:



Detection

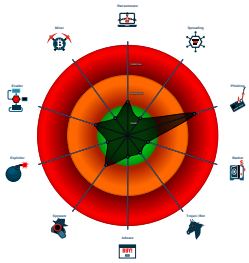


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Steals Internet Explorer cookies

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2440 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - iexplore.exe (PID: 1836 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://24mbw17feyn.typeform.com/to/ZlFRrg5s MD5: 4EB098135821348270F27157F7A84E65)
    - iexplore.exe (PID: 1900 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1836 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 2528 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2696 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2528 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

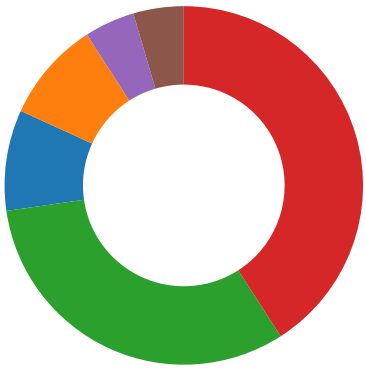
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ZlFRrg5s[1].htm	JoeSecurity_HtmlPhish_25	Yara detected HtmlPhish_25	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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
- Stealing of Sensitive Information

Click to jump to signature section

Phishing:

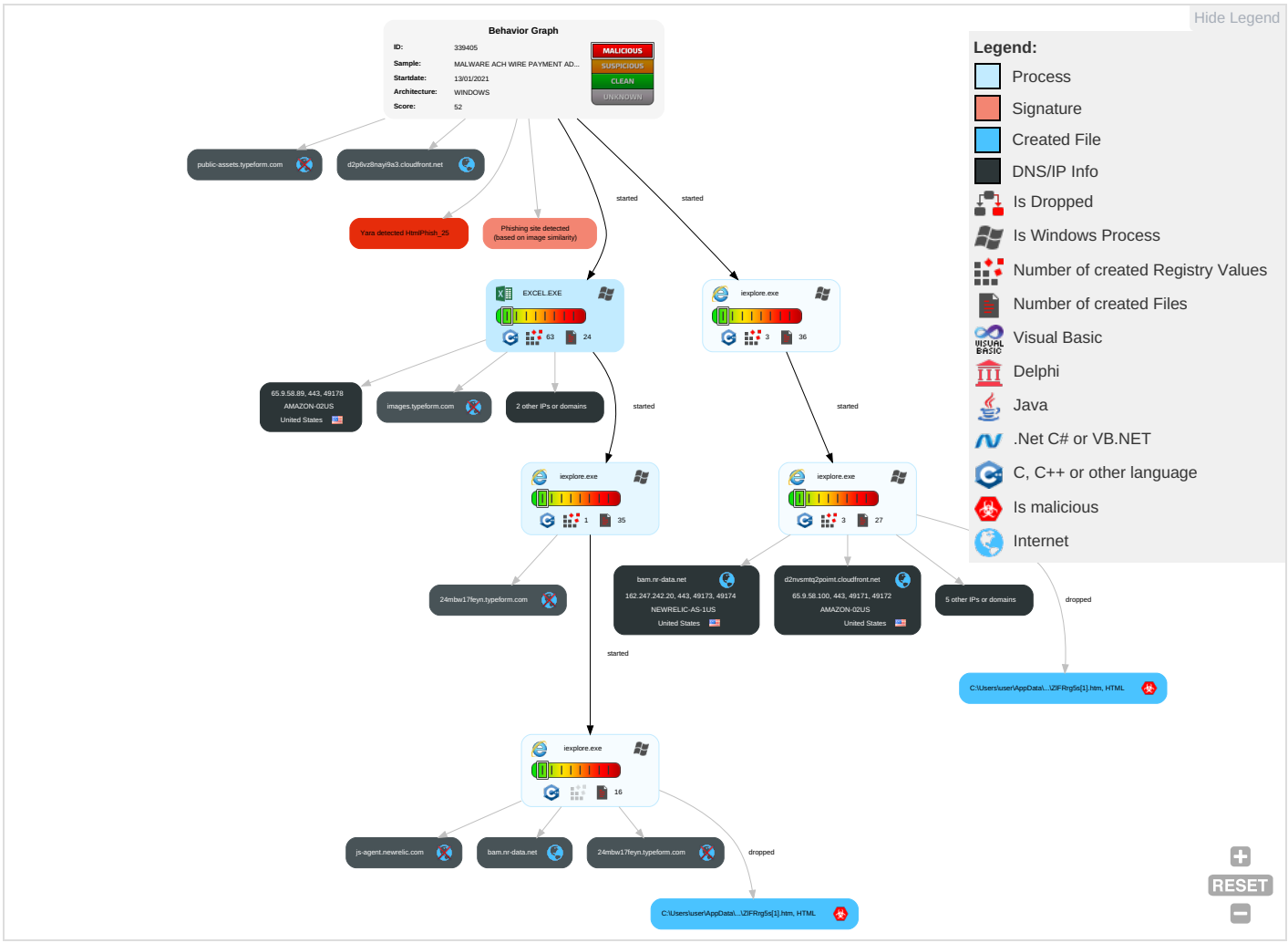
Yara detected HtmlPhish_25

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

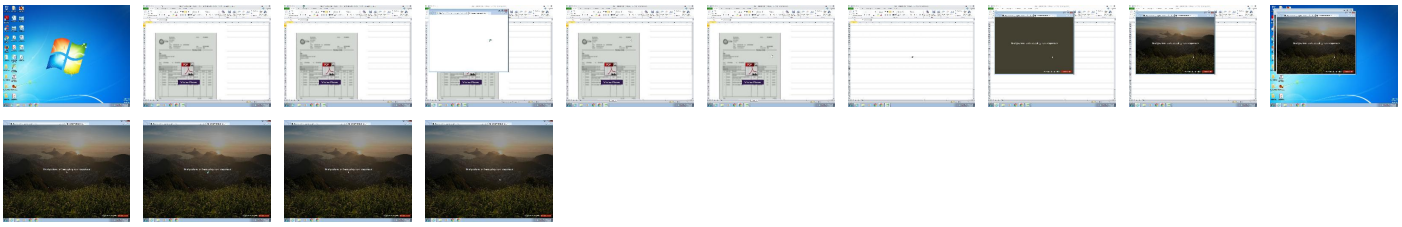
Behavior Graph

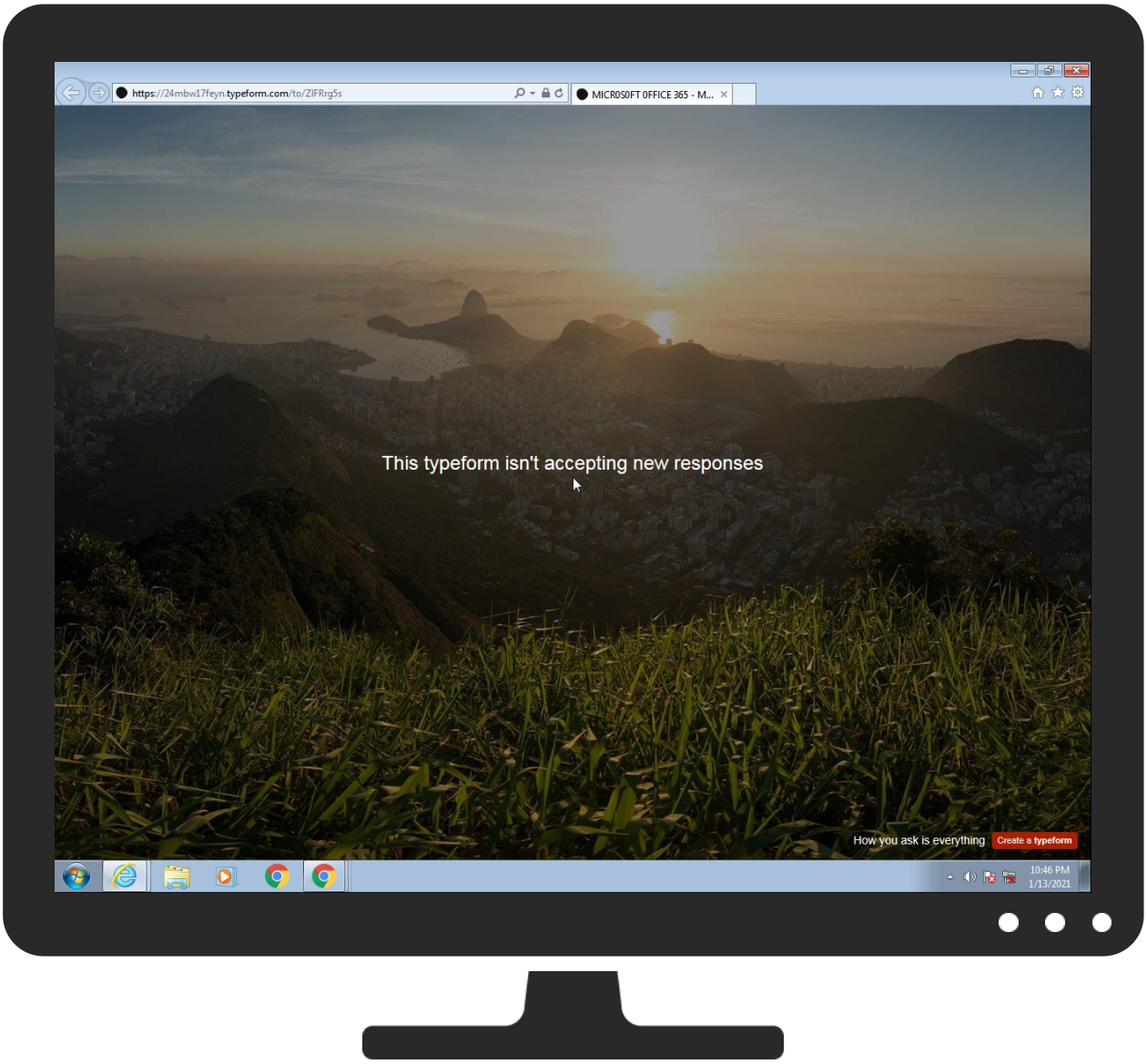


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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://24mbw17feyn.ty	0%	Avira URL Cloud	safe	
http://https://www.typeform.c	0%	Avira URL Cloud	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	162.247.242.20	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

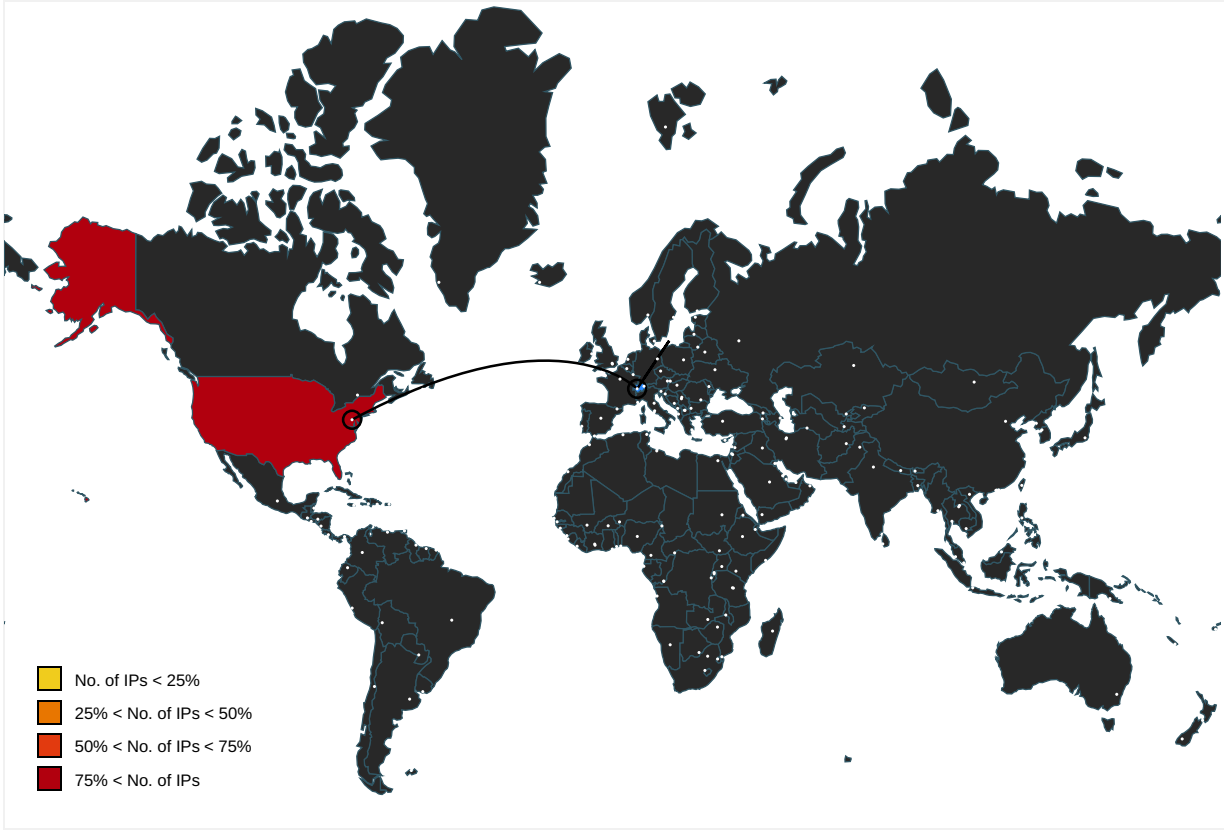
Name	Malicious	Antivirus Detection	Reputation
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_medium=typeform&utm_content=typeform-closescreen&utm_term=EN	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images.typeform.com/images/CJr828dpN5yQ/image/default	ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png	ZlFRrg5s[1].htm.3.dr	false		high
http://https://images.typeform.com/images/nXkRcNPp6wtg/background/large	ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/safari-pinned-tab.svg	ZlFRrg5s[1].htm.3.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s6MlCR0S0FT	~DF603759FFBDDCD7CD.TMP.2.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s	ZlFRrg5s[1].htm.3.dr, {0B7414B6-5634-11EB-ADCF-ECF4BBB5915B}.dat.6.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s6om/?utm_campaign=undefined&utm_sorm.com/to/ZlFRrg5s	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://24mbw17feyn.ty	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://24mbw17feyn.typeform.com/oembed?url=https%3A%2F%2F24mbw17feyn.typeform.com%2Fto%2FZlFRrg5s	ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-16x16.png	ZlFRrg5s[1].htm.3.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s6peform.com/to/ZlFRrg5sRoot	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://images.typeform.com/images/nXkRcNPp6wtg/background/large);background-position:top	ZlFRrg5s[1].htm.3.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s6Root	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://images.typeform.com/images/FYUps4mFKPYK/image/default	ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/browserconfig.xml	~DF603759FFBDDCD7CD.TMP.2.dr, ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/site.webmanifest	ZlFRrg5s[1].htm.3.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon.ico	ZlFRrg5s[1].htm.3.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5sz	~DF603759FFBDDCD7CD.TMP.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/apple-touch-icon.png	ZlFRrg5s[1].htm.3.dr	false		high
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5s/favicon-32x32.png	~DF603759FFBDDCD7CD.TMP.2.dr	false		high
http://https://www.typeform.c	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://24mbw17feyn.typeform.com/to/ZlFRrg5sRoot	{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png-	imagestore.dat.3.dr	false		high
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_medium=ty	~DF603759FFBDDCD7CD.TMP.2.dr	false		high
http://https://www.typeform.com/?utm_campaign=undefined&utm_source=typeform.com-17520522-Free&utm_m	ZlFRrg5s[1].htm.3.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
162.247.242.20	unknown	United States		23467	NEWRELIC-AS-1US	false
65.9.58.89	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339405
Start date:	13.01.2021
Start time:	22:43:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
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 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.winXLSX@8/31@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): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 104.18.27.71, 104.18.26.71, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 204.79.197.200, 13.107.21.200, 13.107.5.80, 152.199.19.161 • Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, api.bing.com, f4.shared.global.fastly.net, r20swj13mr.microsoft.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e-0001.e-msedge.net, go.microsoft.com, random.typeform.com.cdn.cloudflare.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, api-bing-com.e-0001.e-msedge.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.247.242.20	http://sitesumo.com/Outlook/main.html	Get hash	malicious	Browse	• bam.nr-data.net/1/1eb02dae32?a=16828251&v=918.2e0ff1d&to=J1oIRBZeWVQHSxwNBApRD14DHkZQDU4%3D&rst=2825&ap=12&be=1733&fe=956&dc=61&f=%5B%22err%22,%22xhr%22,%22stn%22,%22ins%22%5D&perf=%7B%22timing%22:%7B%22of%22:1582239691683,%22n%22:0,%22dl%22:0,%22di%22:1789,%22ds%22:1789,%22de%22:1792,%22dc%22:2683,%22l%22:2683,%22le%22:2705,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:442%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d2p6vz8nayi9a3.cloudfront.net	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	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/673616c6c792e64756e6e6540706572706757475616c2e636f6d2e6175	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
	http://https://www.freightwaves.com/news/canadian-fuel-distributor-parkland-targeted-in-cyberattack	Get hash	malicious	Browse	• 162.247.242.19
d2nvsmtq2poimt.cloudfront.net	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
	http://https://mainprops.typeform.com/to/gHgyBoFX	Get hash	malicious	Browse	• 143.204.208.81

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	JAAkR51fQY.exe	Get hash	malicious	Browse	• 99.83.185.45
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 54.69.177.146
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 34.218.160.124
	13-01-21.xlsx	Get hash	malicious	Browse	• 18.195.87.136
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 54.254.26.94
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	rB26M8hflh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 34.213.143.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 3.13.31.214
	Consignment Details.exe	Get hash	malicious	Browse	• 52.58.78.16
AMAZON-02US	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
	Consignment Details.exe	Get hash	malicious	Browse	• 52.58.78.16
NEWRELIC-AS-1US	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/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	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
	ACH & WIRE REMITTANCE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 162.247.242.19

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Notification_71823.xls	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	Notification_71823.xls	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	Monex_USD.doc	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.27970.rtf	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.31662.rtf	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18733.rtf	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	n#U00b0 761.doc	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	swift 0182021.xls	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 65.9.58.100 • 65.9.58.120 • 162.247.242.20 • 65.9.58.89

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MP98E46N\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.{06357C73-5634-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24664
Entropy (8bit):	1.7922972563783217
Encrypted:	false
SSDEEP:	96:MdoKzb9KqvpqxsY9Jqxs0laqxs0Ox0qxs0O7Vh3qxs0fuR7Aqxs0fk7I:MdoKzb9KWpE9JXaz0rh3WQ
MD5:	E96C71E2243EF054FCB5638BA846DA5C
SHA1:	05C0853EBB0BEE7AB9D7AD0EEE068138ABFE2783
SHA-256:	88BC41D25CDA269C4A97AAA56143C703CDD1CAD2E0CDAE3C3B92458E1FBDE7E3
SHA-512:	9AF3E34AC402240FC8C6565E3A9FD8EC4868BECA3FA60CB6C475E8F1FE0CC21C67043B0C57ED339D2CCEAE72852B95428673A494443C0C8987B68E92E93FABB
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0B7414B4-5634-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29784
Entropy (8bit):	1.8209225417926482
Encrypted:	false
SSDEEP:	48:IvdGcpUkjGwp0gxG/apngjurGIpHgjBtIGvnZpEgjBtVGvHZpqgjBtCiGoP1qpEU:MDKk9KcpV9JcaL0taZ7JaU0cMX
MD5:	E18D152C1FBAC8C1128E42522374B8FA
SHA1:	BC3B346C48E1CDCC15BD9E971146D2B7CA69A3BF
SHA-256:	6B724F40738EBE70429E7A7DCA76C0043DB5263BED8022BBD22BB4D1985919CB
SHA-512:	C44C3120B42D3C30333B8C5FCC8BF204B698D6F0B3E5482DA0DD21F4BE492494BD859112C3444E514EBAA7F539A352F1EC14BAC24957DC656D3424F31255E3F
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\{06357C75-5634-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	35278
Entropy (8bit):	1.9223900511599943
Encrypted:	false
SSDEEP:	192:MJKG9b6J47KFcppIkJZz/Ys8vhwWO7vDiJ1372:MQEOGKirX5/1ihwlzK13y
MD5:	D51AD6A63DE1424A1D2DC9BBE94A5697
SHA1:	BFDF9135D613906F7FCCEC830EE94F7B70E034C8
SHA-256:	5073E119EBD5282772304C5C8B5DAD7F757202AF6440EB02A1D53172616F4174
SHA-512:	E57954154B229EDEE80CE2857A8DB0A4C99C09DDEA9D8D9EB2963888752052004 03ADD38FBC84EC36A0E1D0C9E7885F0E9100471A0D7EFE0C270DCB2A28BF3B6
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\{0B7414B6-5634-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23640
Entropy (8bit):	1.7321549669006275
Encrypted:	false
SSDEEP:	96:MLK49bAt2aGSUAZK5ZSRZZ+2oZ90SIZJh:MLK49bAt27SUAZK5ZSRZZRoZySIZJh
MD5:	33CEA0C4EE524476D6C1520E06241D6A
SHA1:	11EEF6FF4065A7470D5BDBD995EE359ADA28A89C
SHA-256:	21F9E36165382C1F17C84D468EBFF5DC4F45C1907999AA41201DED94A45E33CB
SHA-512:	276A78E37553104D1891064578C0611DEE77E29BCFC9B48E52525CAED70A8006D6B64D87738E551BA7923B35BBE2182969CCC349E194C50FB87532958B073523
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\{0B7414B7-5634-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5637281477894307
Encrypted:	false
SSDEEP:	48:IvsGcpUZjGwpNUG4pPAGrapgSUrGQpZOG7HpCWXsTGIpG:MwKZ9bkJeeSUF/J0WX4A

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B7414B7-5634-11EB-ADCF-ECF4BBB5915B}.dat	
MD5:	F9E24451076045A2D20B7FB32A99CB7E
SHA1:	93D96CB1FDD4EEE72147C29D44386A900D6D77BB
SHA-256:	60A8296E765E122C52680F5EC01BA7FBC89FAF6EF66949BA1FCD7CDB7BD0269A
SHA-512:	F6538563B84E72D349E9458A832BE65A8E4F0DF55110F688DCB1F431F1D7E029D69CC1EF6AB700D27DE70DA1ED1A70659087742BDCDEA33A77B6029D3397AE2
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1241
Entropy (8bit):	7.238498951271338
Encrypted:	false
SSDEEP:	24:Yt4/pSym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02Efl2:YUx0v9PoQ5VqKwspEes
MD5:	0CE026DF55FAD767F2CB2996E96C9300
SHA1:	2FDF74FDB6400E416722CA7FF73C8BBB911BEF2B
SHA-256:	B6540A80A16E4FC60A609F3B0D92DD3C1ECB9B050A82E3D0BE2207102E7EC0B6
SHA-512:	9609A3591CF7A3CA0D253F4E962A039EE037F32033C36F6E9CE95187118037712E0FFAE664DC1353FB13BC70405D06B6BC83695F0F64A78105939FC4221C1C96
Malicious:	false
Reputation:	low
Preview:	C.h.t.t.p.s.:././.p.u.b.l.i.c.-.a.s.s.e.t.s...t.y.p.e.f.o.r.m...c.o.m./.p.u.b.l.i.c./.f.a.v.i.c.o.n./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.-....PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z &.....u0...`.:....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\ .W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ..._.X...T.Z.f..S.{.#..{...Op.Y.87..X.9...[.,.$..Z|oV{..c.|#_c.. ....!.0..t.gs...X{c..6G.X.9.. ..".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q...../L.2..2.x.Qj.....9 .$-.e88... ..G.YF.G....b.C.[%.u..c...q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>..GE..8.....[r.9C/...d;.PH....3.m....[._ .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	4.6050684780693905
Encrypted:	false
SSDEEP:	24:rCUcWh0sEimVM4mVMyIjyAV28EFySd8/k+C2E93vjqF4IAr4:uUjEiV4VtLV2lFjq29vjNRr4
MD5:	73C70B34B5F8F158D38A94B9D7766515
SHA1:	E9EAA065BD6585A1B176E13615FD7E6EF96230A9
SHA-256:	3EBD34328A4386B4EBA1F3D5F1252E7BD13744A6918720735020B4689C13FCF4
SHA-512:	927DCD4A8CFDEB0F970CB4EE3F059168B37E1E4E04733ED3356F77CA0448D2145E1ABDD4F7CE1C6CA23C1E3676056894625B17987CC56C84C78E73F60E08FCD
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/dnserror.htm
Preview:	.<!DOCTYPE HTML>..<html>.... <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>This page can’t be displayed</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:getInfo();">.. .. This page can’t be displayed .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct. .. <li id="task1-2">Look for the page with your search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon[1].ico	
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23(B
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.I...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	8714
Entropy (8bit):	5.312819714818054
Encrypted:	false
SSDEEP:	192:xmjriGCiOciwd1BtvjrG8tAGGGHmjOWnvyJVUXiki3ayimi5ezxiV:xmjriGCi/i+1Btvjy815HmjqVUXiki3g
MD5:	3F57B781CB3EF114DD0B665151571B7B
SHA1:	CE6A63F996DF3A1CCCB81720E21204B825E0238C
SHA-256:	46E019FA34465F4ED096A9665D1827B54553931AD82E98BE01EDB1DDBC94D3AD
SHA-512:	8CBF4EF582332AE7EA605F910AD6F8A4BC28513482409FA84F08943A72CAC2CF0FA32B6AF4C20C697E1FAC2C5BA16B5A64A23AF0C11EEFBF69625B8F9F90C8 A
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function expandCollapse(elem,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\LnkQ4hGmxTTD[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 131 x 109, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11245
Entropy (8bit):	7.975358433194237
Encrypted:	false
SSDEEP:	192:mbz+31SP85NJJDasl02Sj6cPXana59Wh50KH83Yh7Ewnp4Un5To75yhoEbN:ONIlSB/aabCeHSEwnp4UnpoFhEbN
MD5:	9936A0F33BBE88F448A1E166B8CCD4A9
SHA1:	EBBE8544383B73EB0C8BA6733B3588F7781B5B23
SHA-256:	B0CF2B3D20750F69559365B1926CA243502BE1E58EFBCB45E8315C943BE1BCDF
SHA-512:	58BD2ECF7E1DADBC96DF63B01595C5B8E5E9301B5AC55645B6F36C4B831F39E89375476076CCCC20204B53960C153FBF1103710A74DC41EEBC23C5ABAD5814 0
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..*.F 6....]RY....Y..XS=9$..k...k....$.....S0.'c.~.....|.z.....*.A..)..._.#..QN....&.....P.U8..%.vM+....B..1.?..UP.....3..f.....J.@.h....xc$..5...a>~....1..&.v^... ....*f....5.C3.g.).c.#...\|_J..... ..Z.jWO.f...9w.q...o(...&i%L....#V.\|.,..4M@.W..ZQ`.P..T.....5K...w..}.Jsj.ZR.W`x.f.3.\....C.J.*.*R...g..S2.qx...&N.yr.B...0..'.....,....`:0A..%.\.A^%fa.....y}.+..6i..fx..d..8..).e@.. Uk.}...S..M8..}.:.Qk..K.S...[...H.T.Bh..i..\'..%..$Q..W....el.....ru._....ySy..t..ZR..b.V.:.M.....`:.9.L[.V...Mu...U.7X.....3.G..9.....Z....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\ZlFRrg5s[1].htm, Author: Joe Security

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ZlFRrg5s[1].htm	
Preview:	<!DOCTYPE html><html lang="en"><head><title>MICR0S0FT 0FFICE 365 - MAIL</title><meta charSet="utf-8"/><meta content="#434032" name="theme-color"/><meta content="width=device-width, initial-scale=1.0, viewport-fit=cover" name="viewport"/><meta content="Turn data collection into an experience with Typeform. Create beautiful online forms, surveys, quizzes, and so much more. Try it for FREE." name="description"/><meta content="ie=edge" http-equiv="x-ua-compatible"/><meta content="yes" name="apple-mobile-web-app-capable"/><meta content="noindex,nofollow" name="robots"/><meta content="no-referrer-when-downgrade" name="referrer"/><meta content="#000000" name="msapplication-TileColor"/><meta content="https://public-assets.typeform.com/public/favicon/browserconfig.xml" name="msapplication-config"/><link href="https://public-assets.typeform.com/public/favicon/apple-touch-icon.png" rel="apple-touch-icon" sizes="180x180"/><link href="https://public-assets.typeform.com/public/favicon/favicon-32x32.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	1069
Entropy (8bit):	7.54915864947209
Encrypted:	false
SSDEEP:	24:pym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02Efl9:E0v9PoQ5VqKwspEeT
MD5:	4A35A27936C43081F0865E2E603DF15D
SHA1:	A6D584D829C87EFF74C08F770CD2EF78EE75742E
SHA-256:	DCAE3697C63FCB6AE03D2FD99FB96AF8B14848B71A259ED2E05DBCF5CEDEA5B2
SHA-512:	5DB18A7D2A60BD729F6F12E8A9B05F7A15E90C68CF3415993E8A5B1DB2B5BBA0D4B34B3F2A989E47C7495B9CF202703F0E50694E8865B0784A88EC1A40AF878
Malicious:	false
IE Cache URL:	http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\.W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ..._.X...T.Z.f..S.{.#..{...Op.Y.87 ..X.9...[.,.$..Z\|oV{..c.\|#_c.. ....!.0..t.gs...X{c..6G.X.9....".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q......./L.2..2.x.Qj.....9 .$~.e88... ..G.YF.G....b.C.[%.u..c... q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>. .GE..8.....[r.9C/...d;.PH....3.m....[._ .....%tEXtdate:create.2021-01-04T13:10:14+01:00yu.}...%tEXtdate:modify.2021-01-04T13:10:14+01:00.(g....WzTXtRaw profile type iptc..x.....qV((.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\ZlFRrg5s[1].htm, Author: Joe Security

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\ZlFRrg5s[1].htm	
Preview:	<!DOCTYPE html><html lang="en"><head><title>MICR0S0FT 0FFICE 365 - MAIL</title><meta charSet="utf-8"/><meta content="#434032" name="theme-color"/><meta content="width=device-width, initial-scale=1.0, viewport-fit=cover" name="viewport"/><meta content="Turn data collection into an experience with Typeform. Create beautiful online forms, surveys, quizzes, and so much more. Try it for FREE." name="description"/><meta content="ie=edge" http-equiv="x-ua-compatible"/><meta content="yes" name="apple-mobile-web-app-capable"/><meta content="noindex,nofollow" name="robots"/><meta content="no-referrer-when-downgrade" name="referrer"/><meta content="#000000" name="msapplication-TileColor"/><meta content="https://public-assets.typeform.com/public/favicon/browserconfig.xml" name="msapplication-config"/><link href="https://public-assets.typeform.com/public/favicon/apple-touch-icon.png" rel="apple-touch-icon" sizes="180x180"/><link href="https://public-assets.typeform.com/public/favicon/favicon-32x32.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\aa6e0ec721[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3470
Entropy (8bit):	5.076790888059907
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRHERyRyntQRXaR8RS6C87a/5/+mhPcF+5g+mOC53B5Fqs1qP:JsUOHaQyYX4yJQOWCbz1Qb5
MD5:	6B26ECFA58E37D4B5EC861FCDD3F04FA
SHA1:	B69CD71F68FE35A9CE0D7EA17B5F1B2BAD9EA8FA
SHA-256:	7F7D1069CA8A852C1C8EB36E1D988FE6A9C17ECB8EFF1F66FC5EBFEB5418723A
SHA-512:	1676D43B977C07A3F6A5473F12FD16E56487803A1CB9771D0F189B1201642EE79480C33A010F08DC521E57332EC4C4D888D693C6A2323C97750E97640918C3F4
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet 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 = "The security certificate presented by this website was not issued by a trusted certificate authority.";..var L_CertExpired_TEXT = "The security certificate presented by this website has expired or is not yet valid.";..var L_CertCNMismatch_TEXT = "The security certificate presented by this website was issued for a di

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1310

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
Entropy (8bit):	4.810709096040597
Encrypted:	false
SSDEEP:	24:5Y0bn73pHIUZtJD0lFBohpZlJiHqw87xTeB0yVFaFG:5b73HJq0TJiHp89TOwU
MD5:	CDF81E591D9CBFB47A7F97A2BCDB70B9
SHA1:	8F12010DFAACDECAD77B70A3E781C707CF328496
SHA-256:	204D95C6FB161368C795BB63E538FE0B11F9E406494BB5758B3B0D60C5F651BD
SHA-512:	977DCC2C6488ACAF0E5970CEF1A7A72C9F9DC6BB82DA54F057E0853C8E939E4AB01B163EB7A5058E093A8BC44ECAD9D06880FDC883E67E28AC67FEE4D070A4CC
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #575757;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #2778ec;.. font-size: 38pt;.. font-weight: 300;.. vertical-align:bottom;.. margin-bottom: 20px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 40px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.. padding-top: 5px;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsBu

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.MSO\B24727B2.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 816x1056, frames 3
Category:	dropped
Size (bytes):	65057
Entropy (8bit):	7.714453186203319
Encrypted:	false
SSDEEP:	768:WbZakMgV6yb0BGmdBGAUx3BZP3tUL4dbsaPaVOZIBeSGrS0GUysJEWznmkXHGdhc:WQbgQywBGmkla+bsaCaWyVvXmkXwhH8

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B24727B2.jpeg	
MD5:	89776C76604B8117DFD73CA3604286AB
SHA1:	097D88821166432D9C8EF52CF807353BCC34952F
SHA-256:	5F43444269E5E9E7D1B94660AD93B9CCFED6622A1D415BDE414D478526A3F5D2
SHA-512:	68C2826235479DC52C10A6EAF078BA3FA0D77120517D608A69349258F5C3646382431CCDA4AEEBCA1026EE877AE180F06E44E6FDD6888681C660D053EA3427B
Malicious:	false
Preview:	......JFIF.....`.`.....C.....C..... .0.."...../1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..S..(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Temp\~DF0E06319D83AC7A0C.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.9544673276521939
Encrypted:	false
SSDEEP:	96:LyMegIpCvngIpz46xgIpRwhgIpISaS+gIpRlugIp:LyMbQCvgQz46iQRwyQFv7QRlLQ
MD5:	9A57BFE0FB53D6B906E4C9DE6040FA67
SHA1:	4A2BF255AA0A88C1D8246D7D34C2F55F608F7BE5
SHA-256:	8AA23D7F9AD1AAF90E8036E9E7B6D98FE1B5B6EFFD07F36EAF37184DDAC60BCC
SHA-512:	4BBC732AC5007D5A481F9871AAAF0270931C9825F71C7EB03E171ED6F917D437273EC8847902A7D756E309BB6EF17B5A650FBB61C836E8E6823C1EDF657904B7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....t.....s.....t.....t.....t.....N..... .....N.....y.....K.....I..... .....#.....S..... .....q.....`q.....0t.....Pt.....s.....xt.....s.....

C:\Users\user\AppData\Local\Temp\~DF37DFCB5A035E701F.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.9368970741646527
Encrypted:	false
SSDEEP:	48:LypvljG3q2qIq26GVq2Es2H2h2w2H282j4R282T:LypvlEq1IqiqxsUO7UfuifM
MD5:	C8F03D079424519698A2AB9C42042BCA
SHA1:	98783529A3F774407F7E9BEEB9260CE6448E7763
SHA-256:	EEEA04DC8AA54AB11E39318E691771431C0B132D1132777300D468730FB121AC
SHA-512:	3504D9254E5EBB09D12E20CBEFD38778BAFAE0C099F778E3A93FAC32DC2EE7F158AE06BBF8EC0C18854AF3C31AB202C09A2F0C2C9E6A15E546E0EF12D4DC8 99A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF603759FFBDDCD7CD.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	43963
Entropy (8bit):	2.2992582524525402
Encrypted:	false
SSDEEP:	384:Lyhv89eVoq1zxTQ7JdDZVd8hw3ahan1yT:GToxOT
MD5:	772D8A64A7F9E9C67C9BBBF36DF5BF6C
SHA1:	6498A8048329D9E1984318BAEC0BE698F90C319E
SHA-256:	9B5B5E1AD3DEC7E1E57A1C5F3347465A3FFAF33F1CD154BA651C75557EE7730F
SHA-512:	30F362FBFD2745349CFCFEE117491D1674DDF505216EBCF060D3853B62E94AD560858200A2B8A5F089E69CD6F16504DA1C6DD2BE106C4DDF1423360AD4F61F0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....@.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFE817CF54CF726A92.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34429
Entropy (8bit):	2.098653134200038
Encrypted:	false
SSDEEP:	192:Ly/vx9MV/ONdTudZEZc1snZoZU1sRZtZ:Ly/vx9MVwTudSrn+PRH
MD5:	D7F2E59027C3B44E63ED5A8CDE784794
SHA1:	35F21E41C361EF2DA8B9C3A6C053BF386B0C4FC0
SHA-256:	BDE63EA46781BA8AD628A0397FCA27E3C0A34636B6CDCA37715C43C65A816181
SHA-512:	2B3B2F171CD02A395267422ADCF791C4F1AB2C311D849FF879A541B578539D2855527CFE59D9FABA8B6B30DDAA3C0BCB84F139D2EC1ECEE2E92632A82F3661 6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....2.@.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFF6708434B88E8000.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	1.4036744517476905
Encrypted:	false
SSDEEP:	24:3NlLONlL1G8/NIlkNIlljG8BNlogqXNlog6G8lNlWgjBtDtCWBdv/W/o:Ly1GnvljG9gqIg6GPgjBtDtCWBdv/W/o
MD5:	413DF1A180B150C5BAE6687A97231EF8
SHA1:	8370905BD0884485FBCC1D9FB79B31BF5920C748
SHA-256:	43B0CE40EE31113D90F67CD4BBD8DBA9D700ADA024DF7AB4487C0BBA8BAA943B
SHA-512:	847411B3F4AED1552307904B8E011611BB8987220D57C7B891F35D91C21AD11A73AFF3621CF5625B6749C9E1F552E7C743DC626FCC3183E3E0B6B514664B2D74
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....!.@.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\BPMGT7B2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114
Entropy (8bit):	4.391231629479217
Encrypted:	false
SSDEEP:	3:GmM/N0WP5TA4WEXKR9v/JGGESMMj7eV07dQWWuTUlPv:XM/N5SwS93JGRV6ZDWcUVv
MD5:	06667F8C010611ACA4501AC1BDEBFCFA
SHA1:	01FA600DCA017440074758206D9AE62033776A67
SHA-256:	0BCC2E82CD6DB92E64E595F06300ECD25FE656BCE3172C0891B52269C95F2062
SHA-512:	E1DA74136615FBDFBCD6C222C81DBA198085839F7E3635D189F57DA50EF88951A9B730493267990010009 4D59C4F3715D90FEA5A6B5B54D289AC103A55F30E5C
Malicious:	false
IE Cache URL:	typeform.com/
Preview:	__cfduid.d1108a5fb5331ed69f71916e5ce173c621610574300.typeform.com/.9729.1342100992.30867848.3385641980.30861888.*.

C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT ADVICE..xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58

C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT ADVICE..xlsx	
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

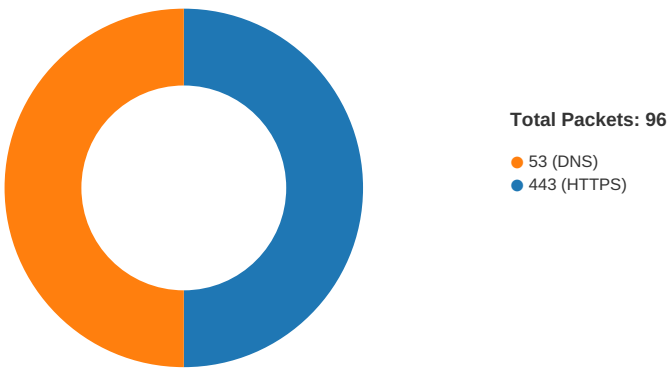
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.657144801353107
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	MALWARE ACH WIRE PAYMENT ADVICE..xlsx
File size:	76184
MD5:	a66a202e970df086cc265cb646127bfb
SHA1:	c8986173e16bb9b0703490afba594ec5eef08a4a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

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:45:01.132178068 CET	49167	443	192.168.2.22	65.9.58.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:45:01.133759975 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.171926022 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.172127008 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.172811031 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.173497915 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.173665047 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.173697948 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.173875093 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.174350977 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.212465048 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.212575912 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.213037968 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.213337898 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.213352919 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.213548899 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.213699102 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.213735104 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.213751078 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.213815928 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.213903904 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.213912010 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.213917017 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.214392900 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.214411020 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.214426994 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.214967012 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.215915918 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.215980053 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.216511011 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.216672897 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.222848892 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.224275112 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.252621889 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.253060102 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.253102064 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.253148079 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.253523111 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.254363060 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.254400969 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.254440069 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.255353928 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.256091118 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.257520914 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.257685900 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.260423899 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.260705948 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.262518883 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.263003111 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.263911009 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.264580965 CET	443	49168	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.267199039 CET	49168	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.267205000 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.274723053 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.282058001 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.282732964 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.314407110 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.316826105 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.316859007 CET	443	49167	65.9.58.120	192.168.2.22
Jan 13, 2021 22:45:01.316921949 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.316953897 CET	49167	443	192.168.2.22	65.9.58.120
Jan 13, 2021 22:45:01.322181940 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.322803974 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.323348045 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.323429108 CET	49172	443	192.168.2.22	65.9.58.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:45:01.323537111 CET	443	49171	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.323673010 CET	49171	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.329344034 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.369087934 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.377995014 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378052950 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378103018 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378113985 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.378150940 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.378155947 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378175974 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.378213882 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378233910 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.378252983 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.378295898 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.378321886 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.379035950 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.379076004 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.379134893 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.379173040 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.380218029 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.380264044 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.380345106 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.380424976 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.381315947 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.381372929 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.381449938 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.381481886 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.382369041 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.382411003 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.382463932 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.382483959 CET	49172	443	192.168.2.22	65.9.58.100
Jan 13, 2021 22:45:01.383557081 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.383598089 CET	443	49172	65.9.58.100	192.168.2.22
Jan 13, 2021 22:45:01.383661985 CET	49172	443	192.168.2.22	65.9.58.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:44:58.646605015 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:44:58.708503962 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 22:44:59.535016060 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:44:59.614025116 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:01.061003923 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:01.103913069 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:01.108506918 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:01.130477905 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:01.161554098 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:01.169493914 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:01.420845985 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:01.468712091 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.196921110 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.199506998 CET	61865	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.206126928 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.208365917 CET	52496	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.220397949 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.224283934 CET	63009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:03.253714085 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.256123066 CET	53	61865	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.256264925 CET	53	52496	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.256814003 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.273168087 CET	53	63009	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:03.277730942 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:04.775885105 CET	59319	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:45:04.827557087 CET	53	59319	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:05.863800049 CET	53070	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:05.919761896 CET	53	53070	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:06.904443026 CET	59770	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:06.970279932 CET	53	59770	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:07.485677004 CET	61523	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:07.530018091 CET	62791	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:07.543410063 CET	53	61523	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:07.586607933 CET	53	62791	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:08.238852024 CET	50667	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:08.311408043 CET	53	50667	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:09.588413000 CET	54129	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:09.647537947 CET	53	54129	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:09.889767885 CET	65329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:09.937613964 CET	53	65329	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:11.962959051 CET	60718	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:11.964278936 CET	49157	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:11.964951992 CET	57391	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:11.973038912 CET	61858	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:11.974108934 CET	62500	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:11.974556923 CET	51652	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:12.010992050 CET	53	60718	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:12.012120008 CET	53	49157	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:12.012649059 CET	53	57391	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:12.021020889 CET	53	61858	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:12.022120953 CET	53	62500	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:12.025217056 CET	53	51652	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:29.296828032 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:29.344930887 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:30.303073883 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:30.351015091 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:31.053142071 CET	56905	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:31.101066113 CET	53	56905	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:31.316874027 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:31.364913940 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:33.329627037 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:33.389683962 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:37.339955091 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:37.396106005 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:38.072352886 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:38.123188972 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:39.086579084 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:39.138878107 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:40.541578054 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:40.593525887 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:42.550210953 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:42.602185965 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:46.559760094 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:46.618947029 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 22:45:59.113362074 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:45:59.172688961 CET	53	58101	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:00.117126942 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:00.167889118 CET	53	58101	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:01.132438898 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:01.183310032 CET	53	58101	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:03.143750906 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:03.195957899 CET	53	58101	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:07.153458118 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:07.204332113 CET	53	58101	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:07.987795115 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:08.038759947 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:08.994398117 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:09.045101881 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:10.008434057 CET	64329	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:46:10.059293032 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:11.174501896 CET	64881	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:11.240571022 CET	53	64881	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:12.020884991 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:12.071672916 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 22:46:16.030729055 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 22:46:16.081491947 CET	53	64329	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 22:44:59.535016060 CET	192.168.2.22	8.8.8.8	0xc117	Standard query (0)	24mbw17fey n.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.061003923 CET	192.168.2.22	8.8.8.8	0x6f0c	Standard query (0)	public-ass ets.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.103913069 CET	192.168.2.22	8.8.8.8	0x2ae1	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.108506918 CET	192.168.2.22	8.8.8.8	0xdaae	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.420845985 CET	192.168.2.22	8.8.8.8	0x368b	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:05.863800049 CET	192.168.2.22	8.8.8.8	0x315e	Standard query (0)	24mbw17fey n.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:06.904443026 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	images.typ eform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:07.530018091 CET	192.168.2.22	8.8.8.8	0xda32	Standard query (0)	24mbw17fey n.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:08.238852024 CET	192.168.2.22	8.8.8.8	0xc8de	Standard query (0)	24mbw17fey n.typeform.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:09.588413000 CET	192.168.2.22	8.8.8.8	0x19a4	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:09.889767885 CET	192.168.2.22	8.8.8.8	0x55aa	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 13, 2021 22:46:11.174501896 CET	192.168.2.22	8.8.8.8	0x1a93	Standard query (0)	public-ass ets.typeform.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 22:44:59.614025116 CET	8.8.8.8	192.168.2.22	0xc117	No error (0)	24mbw17fey n.typeform.com	random.typeform.com.cd n.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:01.130477905 CET	8.8.8.8	192.168.2.22	0x6f0c	No error (0)	public-ass ets.typefo rm.com	d2p6vz8nayi9a3.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:01.130477905 CET	8.8.8.8	192.168.2.22	0x6f0c	No error (0)	d2p6vz8nay i9a3.cloud front.net		65.9.58.120	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.130477905 CET	8.8.8.8	192.168.2.22	0x6f0c	No error (0)	d2p6vz8nay i9a3.cloud front.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.130477905 CET	8.8.8.8	192.168.2.22	0x6f0c	No error (0)	d2p6vz8nay i9a3.cloud front.net		65.9.58.128	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.130477905 CET	8.8.8.8	192.168.2.22	0x6f0c	No error (0)	d2p6vz8nay i9a3.cloud front.net		65.9.58.37	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.161554098 CET	8.8.8.8	192.168.2.22	0x2ae1	No error (0)	js-agent.n ewrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:01.169493914 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	images.typ eform.com	d2nvsmtq2poimt.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:01.169493914 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.169493914 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.169493914 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	d2nvsmtq2p oimt.cloud front.net		65.9.58.57	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 22:45:01.169493914 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.468712091 CET	8.8.8.8	192.168.2.22	0x368b	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.468712091 CET	8.8.8.8	192.168.2.22	0x368b	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.468712091 CET	8.8.8.8	192.168.2.22	0x368b	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:01.468712091 CET	8.8.8.8	192.168.2.22	0x368b	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:05.919761896 CET	8.8.8.8	192.168.2.22	0x315e	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:06.970279932 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:06.970279932 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.89	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:06.970279932 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.57	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:06.970279932 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.100	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:06.970279932 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	d2nvsmtq2poimt.cloudfront.net		65.9.58.87	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:07.586607933 CET	8.8.8.8	192.168.2.22	0xda32	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:08.311408043 CET	8.8.8.8	192.168.2.22	0xc8de	No error (0)	24mbw17feyn.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:09.647537947 CET	8.8.8.8	192.168.2.22	0x19a4	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:45:09.937613964 CET	8.8.8.8	192.168.2.22	0x55aa	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:09.937613964 CET	8.8.8.8	192.168.2.22	0x55aa	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:09.937613964 CET	8.8.8.8	192.168.2.22	0x55aa	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 13, 2021 22:45:09.937613964 CET	8.8.8.8	192.168.2.22	0x55aa	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 13, 2021 22:46:11.240571022 CET	8.8.8.8	192.168.2.22	0x1a93	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:46:11.240571022 CET	8.8.8.8	192.168.2.22	0x1a93	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.37	A (IP address)	IN (0x0001)
Jan 13, 2021 22:46:11.240571022 CET	8.8.8.8	192.168.2.22	0x1a93	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.116	A (IP address)	IN (0x0001)
Jan 13, 2021 22:46:11.240571022 CET	8.8.8.8	192.168.2.22	0x1a93	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.128	A (IP address)	IN (0x0001)
Jan 13, 2021 22:46:11.240571022 CET	8.8.8.8	192.168.2.22	0x1a93	No error (0)	d2p6vz8nayi9a3.cloudfront.net		65.9.58.120	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 22:45:01.215915918 CET	65.9.58.120	443	192.168.2.22	49167	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 13, 2021 22:45:01.216511011 CET	65.9.58.120	443	192.168.2.22	49168	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 22:45:01.255353928 CET	65.9.58.100	443	192.168.2.22	49171	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 13, 2021 22:45:01.256091118 CET	65.9.58.100	443	192.168.2.22	49172	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 Dec 30 00:59:59 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

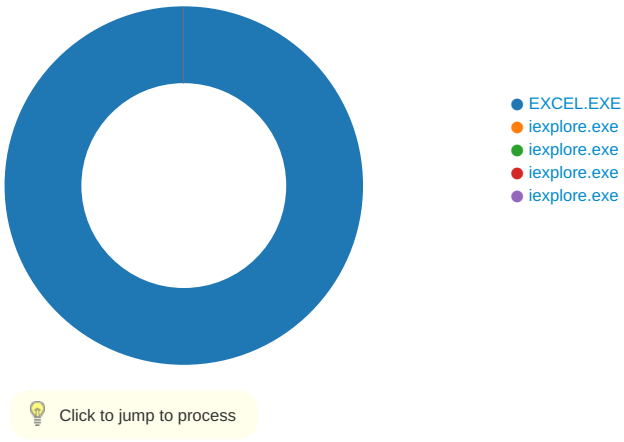
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 22:45:01.767494917 CET	162.247.242.20	443	192.168.2.22	49174	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 13, 2021 22:45:01.767631054 CET	162.247.242.20	443	192.168.2.22	49173	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 13, 2021 22:45:07.058155060 CET	65.9.58.89	443	192.168.2.22	49178	CN=*.typeform.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Nov 30 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Dec 30 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 13, 2021 22:45:10.236735106 CET	162.247.242.20	443	192.168.2.22	49184	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

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 22:45:10.237107992 CET	162.247.242.20	443	192.168.2.22	49183	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2440 Parent PID: 584

General

Start time:	22:44:37
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f800000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\313E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB4EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\313E.tmp	success or wait	1	13FDBB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT ADVICE..xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FA4F526	WriteFile
C:\Users\user\Desktop\~$MALWARE ACH WIRE PAYMENT ADVICE..xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FA4F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\LnkQ4hGmxTTD[1].png	unknown	329	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 83 00 00 00 6d 08 06 00 00 00 82 d3 d2 94 00 00 2b b4 49 44 41 54 78 da ed 5d 07 78 14 55 d7 5e a4 48 d9 64 93 ec 66 cb cc 6c 28 62 03 c5 02 fa d9 10 ec 60 c1 f2 89 05 15 e9 f8 29 d6 df ca 67 89 e5 53 4a b2 9b dd 4d 02 88 88 bd a0 62 47 51 8a 22 20 2a d8 3b 2a 2a 88 f4 94 4d 23 24 b9 ff fb de 99 d5 10 b6 4c 84 00 81 bd cf 73 9f 4d 76 67 76 67 e6 9e 7b ce 7b de 73 ee b9 96 dd b5 89 ec ec 56 9b c6 8d b3 15 fb 27 1c 59 52 90 73 94 18 3f 2d 65 83 cf a7 56 e6 e7 74 dc 14 f4 f5 ae 98 e4 53 45 30 b8 af 25 d9 f6 9c 56 e2 f3 65 84 0b fc 07 97 e6 e7 de 16 0e f9 9e 2d 09 f8 af 09 87 72 ff 5b 12 f4 3d 5f 1a cc 9d 57 12 ca fd 1d 7f af 28 e1 67 c1 dc b7 4b 43 be ef ca f3 fd 5b f0 f7 c7 38 2e 58 94 97 3b 60 53 20	.PNG.....IHDR.....m.....+.IDATx..].x.U.^.H.d..f..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	success or wait	3	7FEE9D13B4B	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B24727B2.jpeg	0	4096	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B24727B2.jpeg	0	65057	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B24727B2.jpeg	0	4096	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B24727B2.jpeg	0	65057	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3312	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F34F5	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	=&2	binary	3D 26 32 00 88 09 00 00 02 00 00 00 00 00 00 00 9A 00 00 00 01 00 00 00 4C 00 00 00 42 00 00 00 6D 00 61 00 6C 00 77 00 61 00 72 00 65 00 20 00 61 00 63 00 68 00 20 00 77 00 69 00 72 00 65 00 20 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 20 00 61 00 64 00 76 00 69 00 63 00 65 00 2E 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6D 00 61 00 6C 00 77 00 61 00 72 00 65 00 20 00 61 00 63 00 68 00 20 00 77 00 69 00 72 00 65 00 20 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 20 00 61 00 64 00 76 00 69 00 63 00 65 00 2E 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3312	F3312	binary	04 00 00 00 88 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 99 B3 A9 C9 40 EA D6 01 12 33 0F 00 12 33 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F34F5	F34F5	binary	04 00 00 00 88 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 99 B3 A9 C9 40 EA D6 01 F5 34 0F 00 F5 34 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: iexplore.exe PID: 2528 Parent PID: 584

General

Start time:	22:45:01
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:	0x13f780000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2696 Parent PID: 2528

General

Start time:	22:45:02
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:2528 CREDAT:275457 /prefetch:2
Imagebase:	0x1380000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1836 Parent PID: 2440

General

Start time:	22:45:10
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' https://24mbw17feyn.typeform.com/to/ZlFRrg5s
Imagebase:	0x13f780000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1900 Parent PID: 1836

General

Start time:	22:45:10
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:1836 CREDAT:275457 /prefetch:2
Imagebase:	0x1380000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly