ID: 412578
Cookbook: browseurl.jbs
Time: 19:38:34
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

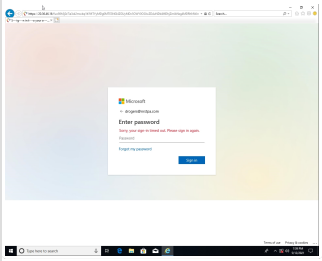
Analysis Report https://hangouts.google.com/linkredire…

Overview

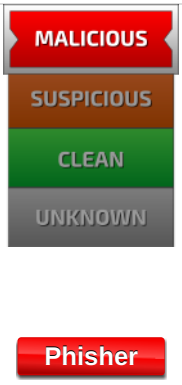
General Information

Sample URL:	http://https://hangouts.google.com/linkredirect?dest=Nrstpa.lwfiacades.com/drogers@nrstpa.com
Analysis ID:	412578
Infos:	

Most interesting Screenshot:



Detection

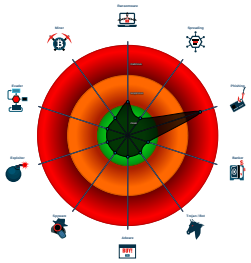


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected Phisher
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5696 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5552 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

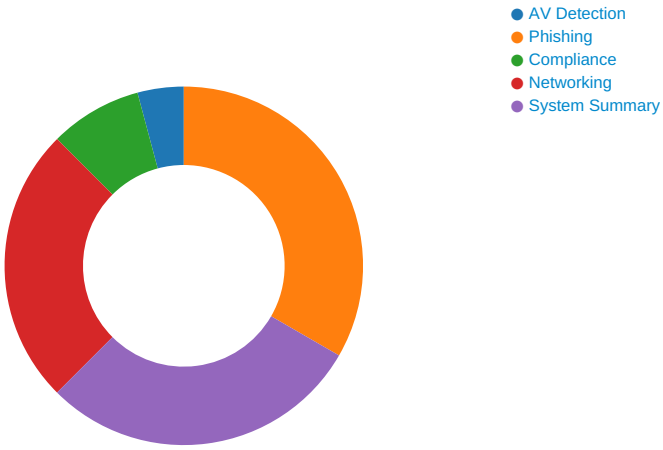
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\drogers@nrstpa[1].htm	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

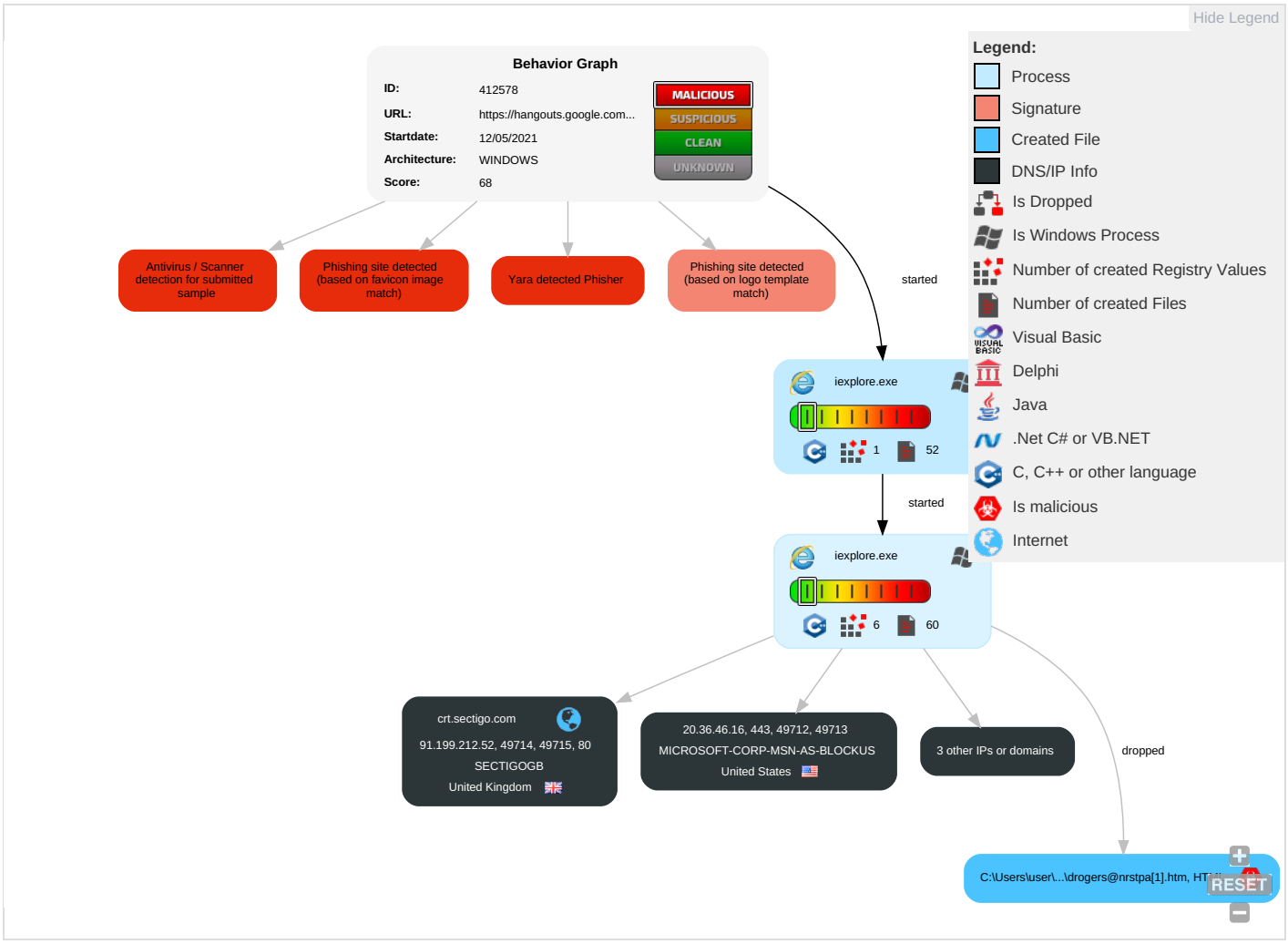
Yara detected Phisher

Phishing site detected (based on logo template match)

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	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	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 3	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 Billing Fraud

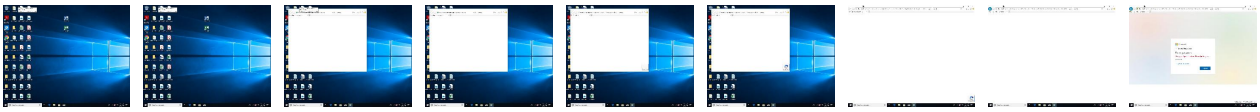
Behavior Graph

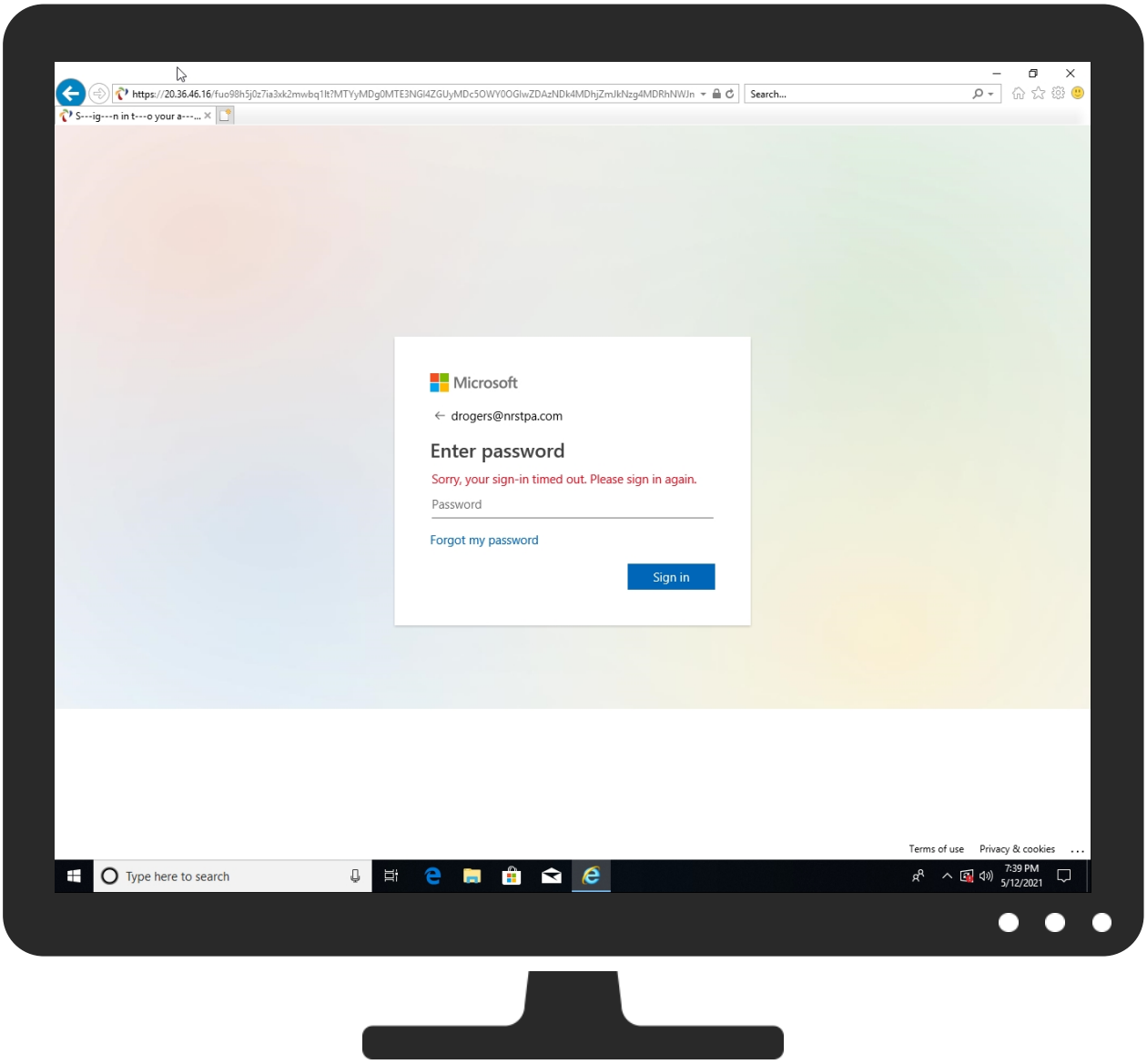


Screenshots

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
http://https://hangouts.google.com/linkredirect?dest=Nrstpa.lwfiacades.com/drogers@nrstpa.com	0%	Virustotal		Browse
http://https://hangouts.google.com/linkredirect?dest=Nrstpa.lwfiacades.com/drogers@nrstpa.com	0%	Avira URL Cloud	safe	
http://https://hangouts.google.com/linkredirect?dest=Nrstpa.lwfiacades.com/drogers@nrstpa.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://nrstpa.lwfiacad/url?hl=en-US&q=http://Nrstpa.lwfiacades.com/drogers	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/eu	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/css/favicon.ico~	0%	Avira URL Cloud	safe	
http://nrstpa.lwfiacades.com/drogers@nrstpa.com	0%	Avira URL Cloud	safe	
http://Nrstpa.lwfiacades.com/drogers	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/?drogers	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/css/favicon.ico~(	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/eu?MTYyMDg0MTE3M2I4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJlMDE1ZTUwY	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/fu	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/fuo98h5j0z7ia3xk2mwbq1lt?MTYyMDg0MTE3NGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDR	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/eu?MTYyMDg0MTE2OGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJmOGEyMTQ5Y	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/css/favicon.ico	0%	Avira URL Cloud	safe	
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/enes.com/drogers	0%	Avira URL Cloud	safe	
http://https://20.36.46.16/en?MTYyMDg0MTE2OGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJmOGEyMTQ5Y	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
crt.sectigo.com	91.199.212.52	true	false		unknown
nrstpa.lwfiacades.com	51.103.149.73	true	false		unknown
zerossl.crt.sectigo.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nrstpa.lwfiacades.com/drogers@nrstpa.com	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/fuo98h5j0z7ia3xk2mwbq1lt?MTYyMDg0MTE3NGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJkYTM1YmYyZjZhZDNkOGVjZTA2NTcyNmUzODk5NmY1Yw==&id=38342e31372e35322e3738&email=drogers@nrstpa.com&logo=b2ZmaWNlL2Jhbm5lci5wbmc/YW55aG9wZQ==&background=b2ZmaWNlL2JhY2tncm91bmQuanBnP2FueWhvcGU=	true		unknown
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nrstpa.lwfiacad/url?hl=en-US&q=http://Nrstpa.lwfiacades.com/drogers	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/eu	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	KFOmCnqEu92Fr1Mu4mxP[1].ttf.3.dr, KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf.3.dr, KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf.3.dr	false		high
http://https://20.36.46.16/css/favicon.ico~	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://Nrstpa.lwfiacades.com/drogers	url[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/?drogers	drogers@nrstpa[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/css/favicon.ico~(	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://nrstpa.lwfiacades.com/drogers	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr, ~DF4FBE3EEF91A8D364.TMP.2.dr	false		unknown
http://https://20.36.46.16/eu?MTYyMDg0MTE3M2I4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJlMDE1ZTUwY	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr, ~DF4FBE3EEF91A8D364.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/fu	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/favicon.ico~	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://20.36.46.16/fuo98h5j0z7ia3xk2mwbq1lt?MTYyMDg0MTE3NGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDR	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr, ~DF4FBE3EEF91A8D364.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/eu?MTYyMDg0MTE2OGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJmOGEyMTQ5Y	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/css/favicon.ico	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/enes.com/drogers	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://20.36.46.16/en?MTYyMDg0MTE2OGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJmOGEyMTQ5Y	{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat.2.dr, ~DF4FBE3EEF91A8D364.TMP.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.199.212.52	crt.sectigo.com	United Kingdom		48447	SECTIGOGB	false
20.36.46.16	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
51.103.149.73	nrstpa.lwfiacades.com	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412578
Start date:	12.05.2021

Start time:	19:38:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://hangouts.google.com/linkredirect?dest=Nrstpa.lwfiacades.com/drogers@nrstpa.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@3/32@2/4
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 52.147.198.201, 40.88.32.150, 88.221.62.148, 142.250.185.78, 142.250.184.196, 142.250.186.67, 104.42.151.234, 142.250.185.131, 184.30.24.56, 152.199.19.161, 20.82.209.183 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, www.gstatic.com, prod.fs.microsoft.com.akadns.net, hangouts.google.com, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, www3.l.google.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3506
Entropy (8bit):	7.54155945514523
Encrypted:	false
SSDEEP:	48:m4qXYiteL8B0wtUJgVXpxi4sVQmjPOZphFRl1P4qXYiteL8B0wtUJgVXpxi4sVQO:StO+0mrZn/T5RptO+0mrZn/T5R+
MD5:	5C8E451E4A7E09535AB02C6301187E84
SHA1:	CE337AB88CDAD351169A54668C6651E37D2C3A58
SHA-256:	3BEE4411F74C082D025884DA0688FE633DF567E220D9D17FD2733AF378123E5C
SHA-512:	2B7948258DB6C51A266E356B89B7659866220FE916CC051E0C26563E9D729500A73163DA21686FBAB15F9AED9CB240F3658F6F69DF8863FDDE6E8CA81940DA14
Malicious:	false
Reputation:	low
Preview:	0...0.....lU.....0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...2001300000000Z..3001292359595Z0K1.0...U....AT1.0...U....ZeroSSL1*0(..U...!ZeroSSL RSA Domain Secure Site CA0.."0...*.H.....0.....is~..1.#.m...T.....!.~].R|?1..l.Y8^g~KV.u..7.5Zd..L.,$..m....Mf.....!t..C..q...L8}.*.....8...N..h..kw..@...._.....=$._.d...Y..B.oPR..Z.'<.....^...T.c.....q.+{@.5.....A...F..|2E...E.e..Pt.....Vu..J..j.u...5../.]..\..;..w..%5-.V..^x$.....(g..0...mZ'...;.`.r3..}.*c...C.u.;.L..7t...>.D....B.f...tJ..."Y..bf:!...'.{...r2n..]tU.....F.....Ex;6E.....-5E*....X.....B.y9.$....g.....|..OxR..WOaU.'.8y..B...-....jG.iV'4%:KI.J.v.i.-o....."m.z.Wc..%9J.~h.i.H.@...#....Ui.(KBU.....u0..q0...U.#..0...Sy.Z.+J.T.....f.0...U.....xh...h.=r._.>....0...U.....0...U.....0.....0...U.%..0...+.....+.....0"..U. ..0.0...+.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	548
Entropy (8bit):	3.082145184273114
Encrypted:	false
SSDEEP:	6:kKp/fY4qMUjKFgJE5Y7EyUWOJ9jnsKp/fY4qMUjKFgJE5Y7EyUWOJ9jn/:FY4qMUE0WYtBoxndY4qMUE0WYtBoxn/
MD5:	57737E1689CA31A69579323C46D3345F
SHA1:	6227D8E6518D92AB68810DDEDE532DDCE87C4FE2
SHA-256:	BBBC6C1417D519BFA6F90D4EBDCC19678562D0E519F5A1E36D9F492D431745AE
SHA-512:	34383918CD8B7CB396DB3E1A147D31AAD1A3E4011D4CD1BE25D0BAB27D3501E130300F0EDA68656250F6F629983CDA74F4B014A193FC928CD6F043C043561F2
Malicious:	false
Reputation:	low
Preview:	p..... .....j1.G..(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...p..... .....j1.G..(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\HI3R5GFT\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	926
Entropy (8bit):	5.65038015415166
Encrypted:	false
SSDEEP:	24:ybCeHaDiHUbCeHaDifARiHUbCeHaDifARiZpELqZvqo21s4jiHUbCeHaDit:ybNau0bNauf0bNaufXELCvqoIa0bNaut
MD5:	21E6B036B80D38D437C14480676328D1
SHA1:	68A3CEE5336C6DFFAE167F7A07F6FEA1C22D2393
SHA-256:	89E32AEAC89CC24F9795D8D08C4908676A0D8EAD57672E6DDCF167D2F173CF85
SHA-512:	2FA5E1CB641BCD2C81D110B2E1A25127A61B43432B367D387F5B31ADA13836FEAACB054EEA26BB0A9C412C75BFB6FF34F77A15FEFD1E22EF1A45952BFEF19470
Malicious:	false
Reputation:	low
Preview:	<root><item name="rc::a" value="MTk5aHc3enNnMXpoNg==" ltime="880574272" htime="30885793" /></root><root><item name="rc::a" value="MTk5aHc3enNnMXpoNg==" ltime="880574272" htime="30885793" /><item name="rc::d-1620873572911" value="MWt6ODhwaTZkN2gycw==" ltime="883054272" htime="30885793" /></root><root><item name="rc::a" value="MTk5aHc3enNnMXpoNg==" ltime="880574272" htime="30885793" /><item name="rc::d-1620873572911" value="MWt6ODhwaTZkN2gycw==" ltime="883054272" htime="30885793" /><item name="rc::d-1620873572911-4ab476f1" value="ChNyYzo6ZC0xNjIwODczNTcyOTExEAAaCGZiZTg1NmVkIpIBCokBYnhFV192UGswUHdJMHFqNDUzeWMwTkhrNmJkOTlXRml5UEs1ck5VZzgtcmZ0UmFvX0xFUkdlMFVKVTBvNEZYb3g1V3ZyYjBxdTJGYzRDaWR4cFQtbGRMV01kMTVfU2pveWVFcnF4eTFyT0FwR2EwU0JmV2hsSUVKWFZDMWdORWMtUmlFd0dsMXUQlrbAogYqAjFy" ltime="885084272" htime="30885793" /></root><root><item name="rc::a" value="MTk5aHc3enNnMXpoNg==" ltime="880574272" htime="30885793" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\20.36.46[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.6006902885994965
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFws5YgWHqJQAqVcF1UP899wENY3DCRVr9g3Ao/prQUUoSDjLO66UVm:JFK1rUFqgDeAqVcF1378CRVWwcrBU7jS
MD5:	BCFEB714C58D1D958F2DF59E1ADFA7DD
SHA1:	6109CC0A55195C0DF7E436807A5C60FFED697CEB
SHA-256:	E8295F0FB83D232ACAE77945ED8BB36A9AC6FF07EC05829FA31402979AE92C86
SHA-512:	8FBC04E10C1F1DEE794D982DBA70E633B6B5DFC9213B59B8F6F08F52EA5036A81CF688F54519B602F102E2D4491EB96634DA5FDA18FF182FD27D3A9B6F6890DE
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="_grecaptcha" value="09ANblmngQP5dvfKViC_HjkuGkMGxRYZXjfQaJpVZ5GBinYofgCsbpN2TZvE24H64CiiQtGgZtjCy511Mwf80YgCY" ltime="887624272" htime="30885793" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6C8C9A57-B394-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8558411484637318
Encrypted:	false
SSDEEP:	192:reZRZY2YWXtkifbJXzM3vBaVDtsfvJ2jX:rq3Pv95WJ2g4
MD5:	26D6AF0E5BABCE356963E6A2DCF26B5D
SHA1:	21BCBB772BAD878A1723AB6557FE7F76E24DB7F1
SHA-256:	8BE8B72B36E96F6F8A53806889B96396F180450718947AF86A85E467678AAA7A
SHA-512:	3FDD4599F5FC6C6A4FE464753D7FB621D09B0436C124445916CF3E38496E84ED68E735EA5672476B17DC3528C32243A69171C4EC9AC8AD0667C81225B724237F
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\{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	72496
Entropy (8bit):	3.1418706819570374
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6C8C9A59-B394-11EB-90E6-ECF4BB82F7E0}.dat	
SSDEEP:	384:roEptiw40HxkEVj3ZU7swdrq3lVj3ZU7swdrq3gmfpmbamgRdnw6D6g8646e6HYu:6Yf8p4azRF3X
MD5:	E3D15986536FDCE968CE8514D3140343
SHA1:	5006F64F7D1C19B085F98B1BEDA45112959E9E9C
SHA-256:	3D95B8EAA36B574C03AD9701E6F620BCD1000E55C5CC9F0FEAC822FD1105FA73
SHA-512:	17ED0AE07F31E855BF94F42099861A0207F1A948B95CB9351DF70C269AAE248AEDBAF6EC5C548AD47E0A41687B4B6A4EE411737EAD33CD52E13C11B57993CB 7
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\{765A0962-B394-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564443447490526
Encrypted:	false
SSDEEP:	48:Iw7GcpruGwpa2G4pQUGrapbStGQpKzG7HpR6DTGIpG:rhZGQG6iBSXACT6pA
MD5:	9321BC40398EE4D65587DF1952C9DF20
SHA1:	21455E739E863DE964FAAC6036A5C53460341A3A
SHA-256:	B497F332694B91358F6E39ABA6CD346B12322276E54A7F03BCC7CAC9AF3BD8B1
SHA-512:	F7084E47096BE34F2D849B841B5F6CFE2A217551DE3F61F775BD2029AF0BBF92B72DF6D0131315E822F391A848779DE60D97C24D3CE4C4F4B877DFE7C249BAF
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	24750
Entropy (8bit):	3.9299786147597056
Encrypted:	false
SSDEEP:	96:YvIJct+oP47v+rcqlBPG9leA19/QQQQQN:YvI6tBPqWceBPGDfe
MD5:	FD66FD5A2EE3E3853D474DA11C0EDA43
SHA1:	80D3E7435205D9DE27DCEDB6E0F31ECB769D6A65
SHA-256:	30E698B994CB8D0845A9704EF7DC304E4BE58508016A83BAAFEFE403D1AEDAA5
SHA-512:	76531DAB7709B753F85EF38E5C73DFB15581C85569F89D9D6409F330AFF8015BF66311C5863621B89692EEDBB6E22F1674631D6FE16147E79317C66019CDE8E7
Malicious:	false
Reputation:	low
Preview:	".h.t.t.p.s.:./.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... .....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V. 8.....F..B.....B.....B..B..B..B...u.....B..B..B..B..B...{.....5.....k..... .....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv..... .....]i..<J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	..... GDEF.....{....dGPOS.....|<....GSUB7b.....8....OS/2t.#...r....`cmap.....st...Lcvt 1..K..y....\fpgm..$...v.....gasp.....{.....glyf.'.....,..j.hdmx.....r\|....head...r..n....6hhea.....q. ...$hmtx..MO..n@....loca\v@z..l(....maxp.....l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(.....o.....9.....EX../... >Y..EX../....>Y.....9.....9.....9..... ...9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....<.....9.....EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~.....J.JH.H.....9KK97JJ....e...@..... %...EX../..."> Y..../..../...../01..#.3..#.3..#...-#...w.}..../.....`.....EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,..*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y.....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__._.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C.,..E.D.E.E...,...C.@.,....f.....`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...I...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.. ....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#...../.....9 ../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.# .3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..".>Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	41842
Entropy (8bit):	5.894230053494729
Encrypted:	false
SSDEEP:	768:v/SNIihoKqnkgFoBMkZ/83m0Qif69vrWwnnDfHIjWSU6L2zYM:qIiqK/Zhcm0Ry9SWnbI9UWEX
MD5:	78738D182FF6BD5F50FB4F17AEF1131E
SHA1:	44D9667F4580232E5E15F93FC9DA7BE10F574297
SHA-256:	8F80D647CF7B1D4243EC9A005892D542B0529C8A62C18F3BA33DAFDDEA65F182
SHA-512:	4A7A9B4955A3FD28A40265F18B501D3912B867EC9D7FC39AE68B8E976BDD3919D98AF1D6C6C8E6E639F9EAB020631076C8478F02E5D19CA47D90DADD10D7FFA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\anchor[1].htm	
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/styles__ltr.css">.<script nonce="XrshL7giYtz3bWh+nYkMsQ" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wIJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wIJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B370 563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/favicon.ico
Preview:	.... .h...&... ....(....... ....0...v.].X.:.X.:.r.Y............... ....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X...................0........q.W.S.4.X.:................J...A...g.......................K.H.V.8........................F..B..................,....................... .............B...B..B..B..B..B...u..B..B..B..B..B...{................5.......k..7R..8F........... ....2........Vb..5C..;l.................R^....................0...............Xc..5C..5C..5C..5C..5C..5C..lv...]i..<J..:G..Zf....................................... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\styles__ltr[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	52732
Entropy (8bit):	5.959269303940443
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwd/Dl+x2dtYyPoiDH1fkQJVEwY:4UcW6v+2rKwFDlXP7dnY
MD5:	182B64B9E3032D6BA48A0A6C854032B0
SHA1:	879537EC1D2CE611AE82B784A25A3E2CDC1EC6FC
SHA-256:	94B328F86382CDA7D83CEBB40EE8DD8F567582A60BA91A90A37F490B0F0EDEFA
SHA-512:	2CEDB007DB16B0F25287F85D8E945172CE01C26E514FB6A2F8F2278A716B89ED327EDA9897A704E08F1715B94177B69178BC499DF56683C9CE2BFB8DE364A53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\arrow_left[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\arrow_left[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/css/arrow_left.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\banner[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2164
Entropy (8bit):	7.818339717863416
Encrypted:	false
SSDEEP:	48:QRC4G2NX3tTgg9XnFzNgz1HB6wQsMxTp05W3rN:Q1dNX3tP9XFzNMmTxTegrN
MD5:	0FE091116AC9646D59E1ED2CA60A9826
SHA1:	FD00FCAEA832259B68B03389A5D69D47D8FDC8AA
SHA-256:	D7B50AE5C86E819103451897C80511EFAEC3F05A604CD38718BE14FA7D1390A0
SHA-512:	172B76AD2BBF4631EB6EF080748F1F2F1229D0B78D779976E3D567511F3E22F0721B1BDDCB55BEC7BCF2F3ACBFF90A8C068984BC2514A381C602BF6FE03CCA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/css/banner.png
Preview:	.PNG.....IHDR...l.....pHYs.....o.d....tEXtSoftware.www.inkscape.org..<.....IDATh..}.\U.....O.j*.Z?@K.....pE.b.XLt.....@.D.v..,T..(.@...H. !.....5.H..Hi..[.3..S..e....L.9.}.s.{.s.}..X..Ds...b...j...6.p.9X.}..I....0.....?.....H&..b..t.}.].V...mi....2.Lk.X.S.&.....O&..s..$..r.e.A...N..g.....E:..t...3#.H...j.....9w.0.....%...@od...b..?.L&...0`...5.....ld>..+.$K...?....n.....Oml.=z...;v<&.T3[..D.....d.?.0.. . .V...?....v.m---...F...D."0...d....$...I...KDbE8..{0..+`..+.....pI....=$.z. .:..{.:..=W..\...Z.l#.....t:=.8]R..T.....9.....-Z..y.Z....q.-i<.....{...;....p.....X....=.V_....af..O.....dJ..,....$..`f...tw._..QqV':....o?..y..r...>....0...lf6W.!f..{..l.}..]'....<..N....u.{I...$}...X.H$..|F.....z.R....E>5|u..Agg..... .90.....(.).bq%p\C.s.....?...X_..Y..2..q.#....@..n._.....I.SM...d2.W,....t.p.P}uwwO,.....f3.....$.h.O....L..... i..M.t.pl,.[...>.c..L$...T*...b'I:. .L...0p..m.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\default[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	102257
Entropy (8bit):	5.304788392262849
Encrypted:	false
SSDEEP:	1536:QpHDglHuhw+E3mazA/PWrF7qvEAFiQcpm0tpHzyJRr:lBpbyJZ
MD5:	48ACCE3492C87668FE2FB1F531CA08A5
SHA1:	9382ABCBE4C89108F5ED6E5B9DD8860CC7EF6A07
SHA-256:	851422AB92F34CD3F6C983301748A797B51F5E9BC0A6FE6CEC5C955BFD132D21
SHA-512:	9034217E85B2634F9F48C8C00E7B6D8A249A857BBD241A4095E82A183D0B5EFAC7F8222F944A649457F7109D4C171AC67DA5C5515F0F017A307CEF7994AADCF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/css/default.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\drogers@nrstpa[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	105
Entropy (8bit):	4.84659490032807
Encrypted:	false
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDJHBJCAGRXWRVlKI+YLn:7AqJm7+mmHLMAYG8bYL
MD5:	65F40437AFA7927AC0350629B49427A9
SHA1:	C6072CE0E589E2104FAB2A3953EB3762AC832DE1
SHA-256:	E954C62ABAE826989BFDBF02DFB26DCF18B6F6AADAD261D69C06C9F658C1E068
SHA-512:	05756E078F3071CBFB93F10D90EF0DAE4EB7CD9993FCEE223E6D2B4FD8A8BE630C19A6E71A544FE47C306051AD394924FE9A5FB8DBEF70F4E5BB821C8E74FE70
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\drogers@nrstpa[1].htm	
Yara Hits:	• Rule: JoeSecurity_Phisher_2, Description: Yara detected Phisher, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\drogers@nrstpa[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://nrstpa.lwfiacades.com/drogers@nrstpa.com
Preview:	<script type="text/javascript">window.location.href = "https://20.36.46.16/?drogers@nrstpa.com"</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\eu[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.7971486122305755
Encrypted:	false
SSDEEP:	6:mAqJm7+mmDNQgMSMWsgshDhuzmBONOVrphuJqEbXKcG8vinr01bEJAE8Nc66BKBI:3qJm7+xDFGpHh9gm9pOqEmyvOgJEJmNm
MD5:	DF8B636B8D324564B300BCE8570701AA
SHA1:	0786E241D0E783D40F08698EEAA15C2A67FF0533
SHA-256:	2C9E05D06BDC04E88E2BFA56DE581FD16D0473C67A5069FCB22F9E80F33D0A70
SHA-512:	1386C1C2E5B042C3DF940F9F19F5CF7AA9F470A1553F94A58EB3CC8DC9F99B0BD284F4FDD48085E0FFE5C832C55705EED9D8BF28A9D94C00CE0E4477DA0F56F
Malicious:	false
Reputation:	low
Preview:	.<script type="text/javascript">window.location.href = 'fuo98h5j0z7ia3xk2mwbq1lt?MTYyMDg0MTE3NGI4ZGUyMDc5OWY0OGIwZDAzNDk4MDhjZmJkNzg4MDRhNWJmNTFkMmJkYTM1YmYyZjZhZDNkOGVjZTA2NTcyNmUzODk5NmY1Yw==&id=38342e31372e35322e3738&email=drogers@nrstpa.com&logo=b2ZmaWNlL2Jhbm5lci5wbmc/YW55aG9wZQ==&background=b2ZmaWNlL2JhY2tncm91bmQuanBnP2FueWhvcGU='</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	5.666174777772168
Encrypted:	false
SSDEEP:	12:7gjKnZCiiQ6CnNUv74H8LCgaxRDadye/Hsb6tyelmDvBE5tS4b8Bq5555555555Z:7genwZekmgKDaoXcKBE5tS4JN
MD5:	1E7D0E39C30B085C52379E9B837C4CAA
SHA1:	460E0AE68A6C545A5523A9E58012D273FB915600
SHA-256:	E7B0EBAFAEB03607B1C5342F52CCFEE82554BBD337920A6C7D009815A417D809
SHA-512:	914E645812D3E11C60CB880BAA88F5A787ACDBCC30A0B15B749ACFDC3940BAD65CD1E4B15B914E86BE21B605E63B5C6A80AC42159A1E9C711CF99481422F327
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/favicon.ico
Preview:	..... .h.....(..... ....@.....JF.5)$..,'..*%..c`.w.....96..%"..($.."...1.....}|.Y...." .. ...,+..VT.I..... .....aa...../.K....._a....._.....x...w..Eu...`o.c.....!...#.!.....!|L=%.....\...^...Y..eE..7.... 1..*G..... .....+p:).c(.Gb%.....Y...V...T...P..#.1..%A.o.....v@0.h,..n3!S.UF.Y...V...R...P..u/\.c(L.U.....t:(In0..w<(.fWCX...U...Q...M...F..W4t.....r4 -t6".w8$..YI.U..5P...K...G...C...>...+p./.gZ.....d:.+uPC{..)y:%+{=).C0..F3.N...P...[..]a..O...9}..3u.,s.;.sH..oBI'wO.A.d/.K9A.F3..K8..VE.....E.m.H.o!B.k98.a.0.Z.L.q.{... .\L{.N<..SA.ys.....o...R.y.R.x.N.v.K.s.F.o.W.|m.....i[].aQ..dU..iZ.....{...f...g...e...b...]...Q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\fuo98h5j0z7ia3xk2mwbq1lt[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	13492
Entropy (8bit):	4.834969275502073
Encrypted:	false
SSDEEP:	192:j21FBW+4SwprX3veevtdufRCwEuVxS/q+JG:q2pj/eotdufRCTuVx7+JG
MD5:	D194CBD3469F9A7F77DDF76A0CF26EAC
SHA1:	C140A36E93E308E3D4EE65FBAF73BE6F016519A5
SHA-256:	D305548D496DBF81E0417EC1F620A6A23A320ADD3E7DE1BD8A947A5828917266
SHA-512:	214C37DDDE247AE88B8ACBEEDF1B1383845632D96EE7AD8890FB8DF3D302A83FAF76A9F595AF65CBAA317B70AE202A4EFBDA5BBAAAE1EDE816752AE89BB9F220
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\fuo98h5j0z7ia3xk2mwbq1lt[1].htm

Preview:

.<!DOCTYPE html>.<html>.<head>.   <title>S...ig...n in t...o your a...cco...un...t</title>.   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">..<link rel="shortcut icon" href="css/favicon.ico">.   <meta name="robots" content="norobot">.<link href="css/default.css" rel="stylesheet">.</head>.<body style="background-image: url('css/background.jpg'); background-size: cover;background-repeat: no-repeat;"><div data-bind="if: activeDialog"></div> .<form name="f1" id="f1" method="post" action="home">.<input type="hidden" name="inilogo" value="b2ZmaWNlL2Jhbm5lci5wbmc/YW55aG9wZQ==">.<input type="hidden" name="inibackground" value= "b2ZmaWNlL2JhY2tncm91bmQuanBnP2FueWhvcGU=">.<div class="outer" data-bind="component: { name: 'page',.   params: {.   serverData: svr,. showButtons: svr.fShowButtons,.   showFooterLinks: true,.   useWizardBehavior: svr.fUseWizardBehavior,.   handleWizardButtons: false,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\favicon[1].ico

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/css/favicon.ico

Preview:

.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""" """""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 33333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""" """""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333 333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\logo_48[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png

Preview:

.PNG........IHDR...0...0.....W.......gAMA......a.... cHRM..z&.............u0...`..:....p..Q<....bKGD.......C......pHYs................IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!......3.po . o.L.i.I..1fl..4..ujL&6$..............w...........,Z..z. ~.....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._......B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.........jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o......*....x?!W...j..@..G=Ed.XF.........J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.......I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ...........k......'...!.a....*+.....(...S..\h....@...........I.$..%.2....l......a.|.....U....y.....t..8....TF.o.p.+.@<.g........-.M.....:.@..(.......@......>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x...........2.k.1....dd.V.....m..y5../4|...G.p.V.......6...}.....B........5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\recaptcha__en[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	342789
Entropy (8bit):	5.707535094474474
Encrypted:	false
SSDEEP:	6144:vOIYdlL+3OfOgc4ZeQEzCVVeP9JyM9dp+Ux2G8Cm:vsdrfj5eQ0CVMPnyuPx29t
MD5:	87FBEAD296F0B44EE37ECF914E7BBB5D
SHA1:	6A51A4F3ECDE8ABDEF98773D84F012FF9DDE5101
SHA-256:	99416B76EF60008EDC2057882BFB782E731A5A32264D60C7F2A5F69E577C618D
SHA-512:	74191D84ABC47DF402C0789B15A3472E64F5379AD2287CD81D05C60B14F8D85FA492F9CBF905E677D40D224FC1AB47D0FED5C5BCEFCC8C51A7A06DA906A267 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\recaptcha__en[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var Q=function(){return[function(a,K,X,N,k,T,e,h,W,G,O){if(2==(a>>1&(2==(a -(O=[3,15,8],2)&O[0]||(G=K instanceof X8?!!K.GF():!!K),a+2&23)&&(X=aW.j5().get(),G=B[0](20,X,K)),O[1])))B[48](O[0],N,X,K);return 2==(((a>>1)%10||(G=y[O[2]](12,k ,K,N,X,e,T).catch(function(){return y[17](45,T,e)})),a)+7&7)&&(W=NU,h=new $9,h.B=function(E,v){return l[18](15,function(J,L,U){U=[2,(L=[1,4,"number"],44),""];switch(J.B) {case L[0]:if(v=(J.V=U[0],N),h.b2()){J.B=L[1];break}return Q[28](93,J,q[14](26,W,T),K);case K:if(v=.J.U,v==N){J.B=L[1];break}return Q["string"!=typeof v||v.includes(U[2]) ||v.includes("\\")?typeof v==L[U[0]]?v=k+v:v=B[25](19,0,function(z){return z.stringify(v)}):v=U[2]+v+U[2],28](77,J,e(v,E),7);case 7:return J.return({o:J.U,uR:q[U[1]](1,0, v)});case L[1]:b[4](9,0,X,J);break;case U[0]:l[48](4,N,J),h.U=!0;case X:return J.return(q[33](40,E))}}},h.V=q[44](94,200),G=h),G},function(a,K,X,N,k,T,e,h,W){r
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\url[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	397
Entropy (8bit):	5.253183823178471
Encrypted:	false
SSDEEP:	6:wBzkrQWR0iYBtqW3kUWPq2JlKI7SqwUqjAYG8Mk7uRxiSqwUqjAYG8GY71Qriztr:4krY1trWPqf79ixx99QrB9zG
MD5:	33E2EAE05442443B9C6A533873A7C605
SHA1:	C675834C09A7F8F8B3118ACF406AE8ECEEC91261
SHA-256:	56BCC5624B18AA0691F646675EFFBBC67778E0F927D703D28413E5DD77DCB14D
SHA-512:	5140E2AD4DF273139AF2851FFE1FDB47A8959D737E076BE8AE40DEB7388F7EFCB6DD2222392A8C3F6D0AEDBE0B630869134BBCD5ACB4A177C79F0F108B36E5 01
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/url?hl=en-US&q=Nrstpa.lwfiacades.com/drogers@nrstpa.com&sa=D&source=hangouts&ust=1620927564919000&usg=AFQjCNFK-1TsryYdWSnw2PfXjPClsl4q4w
Preview:	<HTML><HEAD>.<meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>Redirecting</TITLE>.<META HTTP-EQUIV="refresh" content="1; url= http://Nrstpa.lwfiacades.com/drogers@nrstpa.com">.</HEAD>.<BODY onLoad="location.replace('http://Nrstpa.lwfiacades.com/drogers@nrstpa.com'+document.lo cation.hash)">.Redirecting you to http://Nrstpa.lwfiacades.com/drogers@nrstpa.com</BODY></HTML>..
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	884
Entropy (8bit):	5.599689899245158
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAxN+KVCetHx1nUsLqo40RWUnYN:VKEccQKoehx1nVLrwUnG
MD5:	73D5ABE263F69F6A69FA92F372E13F0B
SHA1:	E67CC7D669607D22AD76CEF614A3A1C695CC4084
SHA-256:	E5925A2755538844C7F961842E468BC6E0ED8F1522677D181DBD8CB0C2069252
SHA-512:	3254BAFCB81BE7994ACD034154E17F66F0A4485F0B7F74E02D168565DAF9A97900B350CCB3AB59C5A5A7E96677C3A7805321EAE6B7C2F268BED2415E3E86860
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=6LerpdEaAAAAAJwOd98lgB6kaXYe16lqEK7JOj_Z
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.r eady=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6Le rpdEaAAAAAJwOd98lgB6kaXYe16lqEK7JOj_Z');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true; po.src='https://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-+GZiSAqM kID7qhZO2RygGVH6c4kowHh+Mf1S3aQaZv8OM49ThCfu5VCTK7u2szGk';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.s etAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\background[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):	17453
Entropy (8bit):	3.890509953257612
Encrypted:	false
SSDEEP:	192:P7FRTHQpmA3ZkXOL25cYty7l6UWUjMJBSab/vR+yzP:P/cpmgkF5+JWUjMp40P
MD5:	7916A894EBDE7D29C2CC29B267F1299F
SHA1:	78345CA08F9E2C3C2CC9B318950791B349211296
SHA-256:	D8F5AB3E00202FD3B45BE1ACD95D677B137064001E171BC79B06826D98F1E1D3
SHA-512:	2180ABE47FBF76E2E0608AB3A4659C1B7AB027004298D81960DC575CC2E912ECCA8C131C6413EBBF46D2AAA90E392EB00E37AED7A79CDC0AC71BA78D828A8 C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.36.46.16/css/background.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\background[1].jpg	
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\en[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	5.246371885433475
Encrypted:	false
SSDEEP:	24:hPRCrJRMzz1LNd2RRBIBM6zyMaPfcjhy8p+M0GRRBZ0MDnjdMn:tYKzz1Lb2SaiyMorGTLun
MD5:	24A60766464F5B2BD6F87876B7DA3D95
SHA1:	FE055D077095DBC3482938E87B0E7B8C7CEF16BA
SHA-256:	A0E2E1867725DC41D4F429D92BA2A19A53674831D992A3F81067D3FAE9967B2E
SHA-512:	421CDE069482A80EB82C278BD8A63D46D95DE45A1F14F00D9EF3AE95C521FB70C45324D6308D669D98F8D95E0646713F7E69CFD1143CBCF6FF4B5E18FD3AEA D
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en">..<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <meta http-equiv="X-UA-Compatible" content="ie=edge">..<script src="https://www.google.com/recaptcha/api.js?render=6LerpdEaAAAAAJwOd98lgB6kaXYe16lqEK7JOj_Z"></ script>..<script>.. grecaptcha.ready(function() {.. grecaptcha.execute('6LerpdEaAAAAAJwOd98lgB6kaXYe16lqEK7JOj_Z', {action:'validate_captcha'}).. .then(function(token) {.. document.getElementById('g-recaptcha-response').value = token;.. });.. });..</script>..<style>...hideme..{.. display:none;.. visibilit y:hidden;..}..</style>..</head>.. <form action="ghome" id="myform" name="myform" method="POST">.. <input type="hidden" id="g-recaptcha-response" name="g-r ecaptcha-response">.. <input type="hidden" name="email" value="drogers@nrstpa.com">.. <input type="hidden" name="hidden" value="drogers@nrstpa.com">.. <input typ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.759361431501545
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKAi8KJhvqCWaee:PLKdXNQKH8KtL
MD5:	C4DAA7D3BCA5413BE7BE44A9B9A25E11
SHA1:	E06511C7E20394362B45E888CE1C98D02AC15084
SHA-256:	B0969F0CA46A6F19D27F76E8ED98F974395121D227C3085ED9325A63CCCE3102
SHA-512:	CDE714A8AAD77AC75F34E3AD50EE32ABDC211B3215B53C33691FDB0A6272FE824A28232D8E657F9335312494E66A2C266ED479C67968AC5EAE2ED84A4D3D43 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=npGaewopg1UaB8CNtYfx-y1j
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js');

C:\Users\user\AppData\Local\Temp\~DF4FBE3EEF91A8D364.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	82831
Entropy (8bit):	1.9627912939463192
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+iEOnUndd8dVj3ZU7swdrq3sVj3ZU7swdrq34mA2m71m7Hi6O6g86v:FM7T2Y1Y6
MD5:	D25C52546F613F8B90396A57DB845C64
SHA1:	4AA9E012FE27A877DACB444500887E0D6C77E945
SHA-256:	25816A27F1603E17D573EDB94261F4AFF7550A5A88ED74A5D5F53B1CD1F92C38
SHA-512:	179FD66A6E43AF5A39E9AD11E5AC8F2F555E67A75535844F11377AF99543659138041D45D935C7B7A3820BFD182D15F38C1B89DB0FB46E33FFD25568FCC7E852
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7E71A0877BF7B1F1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48162750095540563
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lor9lor9lWI/iJ1:kBqoIMSD
MD5:	996649C98315D82E24B33D7F2211479C
SHA1:	3E1D95A890CE705753FF107A09D0F06821A6DA79
SHA-256:	22B455D7D93CD23E2F7D8A5A788705B07470336FEA7CBFFF7F6BAB2FAEF9B57F
SHA-512:	122B7373D74CFF69E03CDBFE97A4D3C528AF1787CE1A28A33A657A409AACD0162714D24072BCA174C4FD5ED174DC07B20BF6F20C802CA333927C6F9C841011
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEA5CD8702A3FE0A4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 94

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:39:25.821135044 CEST	49710	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:25.821898937 CEST	49711	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:25.857424021 CEST	80	49710	51.103.149.73	192.168.2.7
May 12, 2021 19:39:25.857536077 CEST	49710	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:25.857673883 CEST	80	49711	51.103.149.73	192.168.2.7
May 12, 2021 19:39:25.857747078 CEST	49711	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:25.858885050 CEST	49710	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:25.954282045 CEST	80	49710	51.103.149.73	192.168.2.7
May 12, 2021 19:39:26.086826086 CEST	80	49710	51.103.149.73	192.168.2.7
May 12, 2021 19:39:26.086926937 CEST	49710	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:26.407232046 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:26.408025026 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:26.708643913 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:26.708762884 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:26.709434032 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:26.711952925 CEST	443	49713	20.36.46.16	192.168.2.7
May 12, 2021 19:39:26.712112904 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:26.712740898 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.009711981 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:27.009747982 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:27.009783983 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.009820938 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.016005993 CEST	443	49713	20.36.46.16	192.168.2.7
May 12, 2021 19:39:27.016037941 CEST	443	49713	20.36.46.16	192.168.2.7
May 12, 2021 19:39:27.016143084 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.353496075 CEST	49715	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.353547096 CEST	49714	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.415400028 CEST	80	49715	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.415452003 CEST	80	49714	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.415570974 CEST	49715	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.415632010 CEST	49714	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.416105032 CEST	49715	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.416120052 CEST	49714	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.476861954 CEST	80	49715	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.476931095 CEST	80	49715	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.477008104 CEST	80	49715	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.477022886 CEST	80	49714	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.477075100 CEST	49715	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.477145910 CEST	80	49714	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.477161884 CEST	80	49714	91.199.212.52	192.168.2.7
May 12, 2021 19:39:27.477242947 CEST	49714	80	192.168.2.7	91.199.212.52
May 12, 2021 19:39:27.488514900 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.500957012 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.789633036 CEST	443	49712	20.36.46.16	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:39:27.790117025 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.790493011 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:27.805314064 CEST	443	49713	20.36.46.16	192.168.2.7
May 12, 2021 19:39:27.805413961 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:28.142359972 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:28.829852104 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:28.830069065 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:28.831996918 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:29.182988882 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:30.153042078 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:30.153156042 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:30.155622959 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:30.502885103 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:31.489598036 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:31.489636898 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:31.489749908 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:31.592053890 CEST	80	49710	51.103.149.73	192.168.2.7
May 12, 2021 19:39:31.592171907 CEST	49710	80	192.168.2.7	51.103.149.73
May 12, 2021 19:39:32.302828074 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:32.603615999 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:32.603637934 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:32.603744030 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:34.333002090 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:34.333062887 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:34.631655931 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:35.581084967 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:35.584800005 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:35.646559000 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:35.999129057 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:39.639575958 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:39.639867067 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:41.366564035 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:41.366595984 CEST	49713	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:41.367002964 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:41.711255074 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722687006 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722729921 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722753048 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722775936 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722815990 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722837925 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.722840071 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722862959 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.722865105 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722875118 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.722884893 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.722893000 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.722920895 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.722937107 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.723028898 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.723053932 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.723076105 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.723077059 CEST	443	49712	20.36.46.16	192.168.2.7
May 12, 2021 19:39:42.723090887 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.723121881 CEST	49712	443	192.168.2.7	20.36.46.16
May 12, 2021 19:39:42.860706091 CEST	49730	443	192.168.2.7	20.36.46.16

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:39:16.164463997 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:16.218144894 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 19:39:16.315856934 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:16.377839088 CEST	53	53775	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:39:17.489499092 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:17.541320086 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 19:39:18.313457966 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:18.362298965 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 19:39:20.995083094 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:21.052280903 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 19:39:22.386635065 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:22.443690062 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 19:39:23.338326931 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:23.405193090 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 19:39:23.732173920 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:23.780915022 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 19:39:24.598997116 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:24.664052963 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 19:39:24.912388086 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:24.943629980 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:24.963852882 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 19:39:25.001151085 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 19:39:25.668816090 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:25.751667023 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 19:39:27.294188976 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:27.351560116 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 19:39:27.426970959 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:27.475924015 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 19:39:28.250370979 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:28.301121950 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 19:39:29.033418894 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:29.082246065 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 19:39:31.021876097 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:31.070725918 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 19:39:31.583127022 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:31.647044897 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 19:39:32.619743109 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:32.635596037 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:32.668404102 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 19:39:32.685910940 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 19:39:38.835365057 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:38.884139061 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 19:39:41.047919035 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:41.097466946 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 19:39:43.256829023 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:43.305746078 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 19:39:44.459830046 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:44.538374901 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 19:39:45.147589922 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:45.199682951 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 19:39:47.360126972 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:47.410197973 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 19:39:48.960207939 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:49.008913040 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 19:39:50.926007032 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:50.976214886 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 19:39:52.278038979 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:52.329952002 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 19:39:53.310379982 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:53.367275953 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:39:54.129307032 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:54.178054094 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 19:39:54.329054117 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:54.377811909 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:39:55.142065048 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:55.205812931 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 19:39:55.357500076 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:55.420150995 CEST	53	60983	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:39:56.164318085 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:56.223745108 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 19:39:57.455729961 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:57.513468027 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:39:57.828778982 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:57.906492949 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 19:39:58.173511028 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:39:58.230875015 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 19:40:01.470099926 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:40:01.527498007 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:40:02.189259052 CEST	49247	53	192.168.2.7	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:39:25.668816090 CEST	192.168.2.7	8.8.8.8	0xdaa5	Standard query (0)	nrstpa.lwf iacades.com	A (IP address)	IN (0x0001)
May 12, 2021 19:39:27.294188976 CEST	192.168.2.7	8.8.8.8	0x3f47	Standard query (0)	zerossl.cr t.sectigo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:39:25.751667023 CEST	8.8.8.8	192.168.2.7	0xdaa5	No error (0)	nrstpa.lwf iacades.com		51.103.149.73	A (IP address)	IN (0x0001)
May 12, 2021 19:39:27.351560116 CEST	8.8.8.8	192.168.2.7	0x3f47	No error (0)	zerossl.cr t.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:39:27.351560116 CEST	8.8.8.8	192.168.2.7	0x3f47	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nrstpa.lwfiacades.com
- zerossl.crt.sectigo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49710	51.103.149.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:39:25.858885050 CEST	1130	OUT	GET /drogers@nrstpa.com HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: nrstpa.lwfiacades.com Connection: Keep-Alive
May 12, 2021 19:39:26.086826086 CEST	1135	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:39:25 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.11 X-Powered-By: PHP/7.3.11 Content-Length: 105 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 32 30 2e 33 36 2e 34 36 2e 31 36 2f 3f 64 72 6f 67 65 72 73 40 6e 72 73 74 70 61 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://20.36.46.16/?drogers@nrstpa.com"</script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49715	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:39:27.416105032 CEST	1142	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com
May 12, 2021 19:39:27.476931095 CEST	1144	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 May 2021 17:39:27 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: mscrl1 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb6 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0200130000000Z300129235959Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@#Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49714	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:39:27.416120052 CEST	1142	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:39:27.477145910 CEST	1146	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 May 2021 17:39:27 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: mscrl1 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb6 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0200130000000Z3001292359590Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@#Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

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
May 12, 2021 19:39:27.009747982 CEST	20.36.46.16	443	192.168.2.7	49712	CN=20.36.46.16	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Wed May 12 02:00:00 CEST 2021	Wed Aug 11 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-16-23-24-65281,29-23-24,0	1c8f6068d3351ed3651b33bd2625bcdd
May 12, 2021 19:39:27.016037941 CEST	20.36.46.16	443	192.168.2.7	49713	CN=20.36.46.16	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Wed May 12 02:00:00 CEST 2021	Wed Aug 11 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-16-23-24-65281,29-23-24,0	1c8f6068d3351ed3651b33bd2625bcdd
May 12, 2021 19:39:47.146579981 CEST	20.36.46.16	443	192.168.2.7	49736	CN=20.36.46.16	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Wed May 12 02:00:00 CEST 2021	Wed Aug 11 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5696 Parent PID: 792

General

Start time:	19:39:22
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff676750000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: 5552 Parent PID: 5696

General

Start time:	19:39:23
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2
Imagebase:	0xe10000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Disassembly