ID: 438537
Cookbook: browseurl.jbs
Time: 18:15:05
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Windows Analysis Report http://3c4e7b.zgmwgzfzdwxnr…

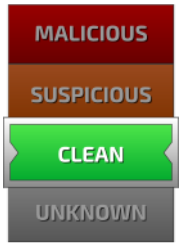
Overview

General Information

Sample URL:	http://3c4e7b.zgmwgzfzdwxnrfq.com
Analysis ID:	438537
Infos:	

Most interesting Screenshot:

Detection

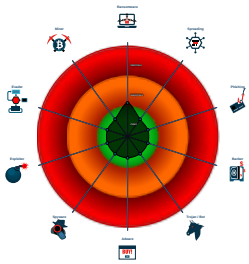


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 4580 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5436 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

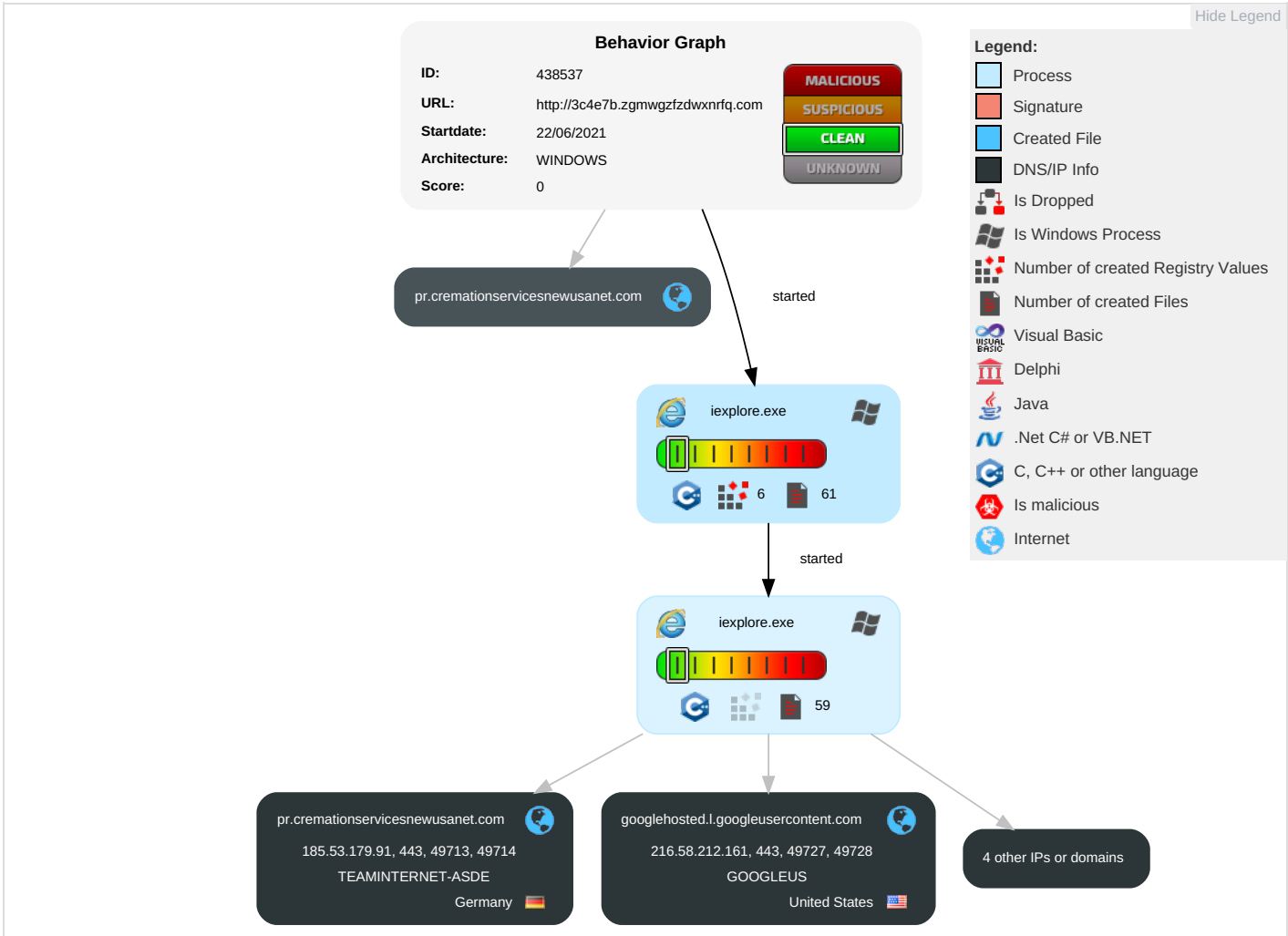
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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 Billin Fraud

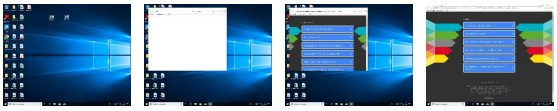
Behavior Graph

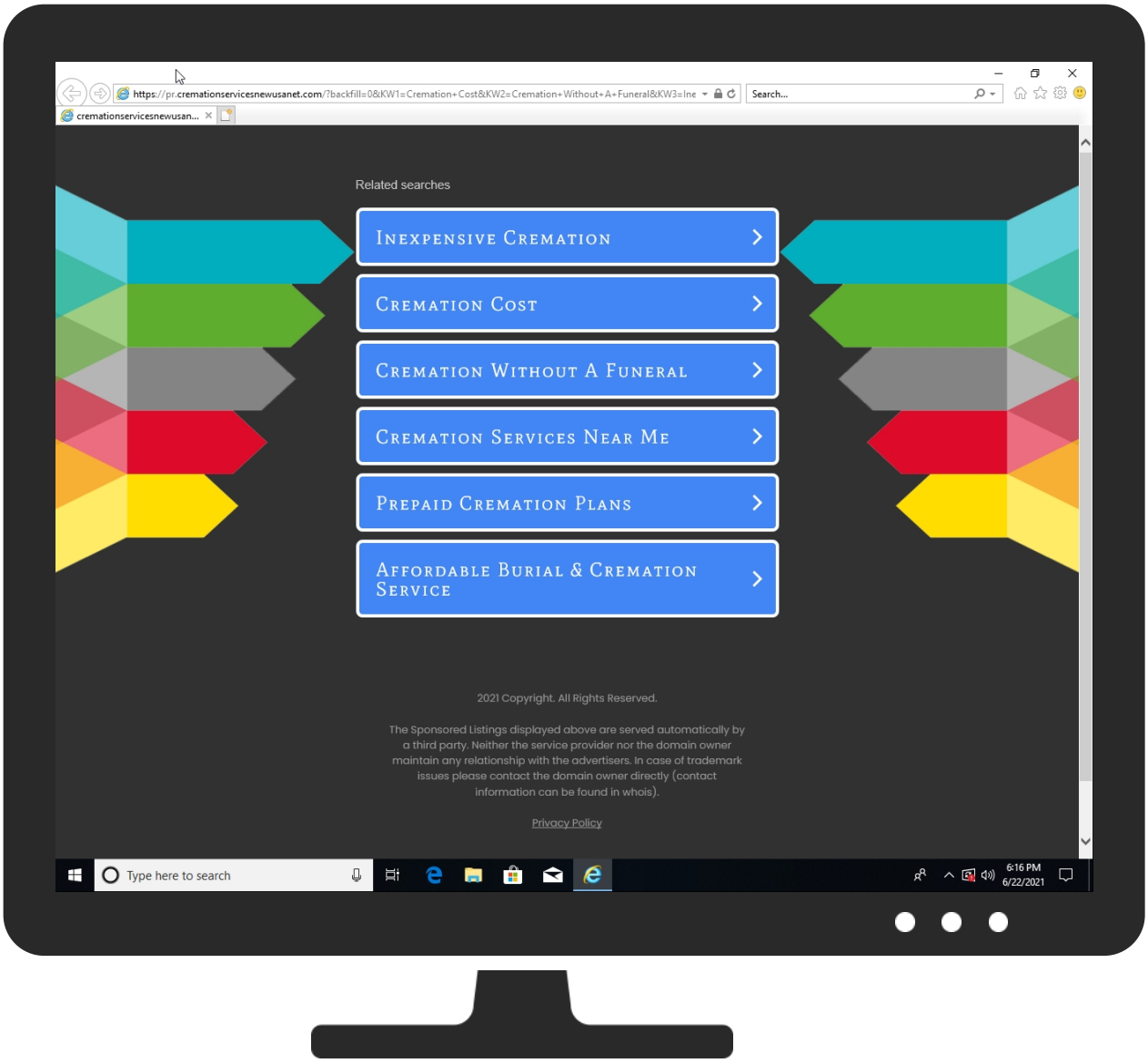


Screenshots

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://3c4e7b.zgmwgzfzdwxnrfq.com	0%	Virustotal		Browse
http://3c4e7b.zgmwgzfzdwxnrfq.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
pr.cremationservicesnewusanet.com	0%	Virustotal		Browse
3c4e7b.zgmwgzfzdwxnrfq.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://pr.cremationservicesnewusanet.com/%253Fbackfill%253D0%2526KW1%253DCremation%252BCost%2526KW2	0%	Avira URL Cloud	safe	
http://https://pr.cremationservicesnewusanet.com/?backfill=0&KW1=Cremation	0%	Avira URL Cloud	safe	
http://https://parking-crew.com/track.	0%	Avira URL Cloud	safe	
http://3c4e7b.zgmwgzfzdwxnrfq.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dk8g5exin21my.cloudfront.net	13.224.193.70	true	false		high
pr.cremationservicesnewusanet.com	185.53.179.91	true	false	• 0%, Virustotal, Browse	unknown
d1lxhc4jvstzrp.cloudfront.net	13.224.194.160	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.161	true	false		high
afs.googleusercontent.com	unknown	unknown	false		high
3c4e7b.zgmwgzfzdwxnrfq.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://3c4e7b.zgmwgzfzdwxnrfq.com/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.194.160	d1lxhc4jvstzrp.cloudfront.net	United States		16509	AMAZON-02US	false
185.53.179.91	pr.cremationservicesnewusanet.com	Germany		61969	TEAMINTERNET-ASDE	false
13.224.193.70	dk8g5exin21my.cloudfront.net	United States		16509	AMAZON-02US	false
216.58.212.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438537
Start date:	22.06.2021
Start time:	18:15:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://3c4e7b.zgmwgzfzdwxnrfq.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:	5
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:	CLEAN
Classification:	clean0.win@3/24@5/4
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

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\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8A846DAC-D3C0-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8576329461807604
Encrypted:	false
SSDEEP:	96:rgZbZn2sWN2tN3fNG5PJMNuvNEi9NdfNcR8ZX:rgZbZn2sW4t5fk5PJMkv2i9rf+R8ZX
MD5:	7C7EA8F34EBF4FC6DFD4CCB00AFE16CD

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8A846DAC-D3C0-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	6DFCA7F449AA4FB2370A190B7AF39B0E910702C4
SHA-256:	F63346C29FFC48F4726D6E187497511738F1971F9155732A1AA4AA59C8872796
SHA-512:	F02413E0ADCAB471A16B3B07F21A563328D3E7B7477CC6C388C28C0D70CC844BFBFE97B62A10D4254AD64A7CB84B6AF23045885533F4E2563DC8634D0EFFC3 5
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\{8A846DAE-D3C0-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27536
Entropy (8bit):	1.7756010713189636
Encrypted:	false
SSDEEP:	96:r9ZOQ+6sBSSjV25WCMq4CF5wcuDqTqVUPMUrBr:r9ZOQ+6skSjV25WCMq4O5wccnUPMUrBr
MD5:	E40522EF391BBEBE0751BE97352836CC
SHA1:	3ED13598ABF88E328952207DE5C0AAF8EE50BA42
SHA-256:	FBAF1082D55F6432A436A83A71AD6EA88AFF963628833B17F51CE90285BBED79
SHA-512:	CE3547BE05E2F3076FEF0326F0D924CBEB8FC1FA6330A385D46359AEA8A49CC31E53AE1E570CA2C53B9343E4130D972BD2C4D4072D53882DC433A517306C238
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\{8A846DAF-D3C0-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5638113470855957
Encrypted:	false
SSDEEP:	48:IwKGcprjGwpaSG4pQuGrapbShcGQpKDUG7HpRYTGIpG:ruZ9Qi6gBSh0ADfT8A
MD5:	347838AB8CA480746ED1037415401A0A
SHA1:	4743E6A049725A00430A8C14A1BAD9DCF60BF976
SHA-256:	0F46B7E8C34AC5FEA2A9C3206023673E220BED789B8E2356681162CD279ED867
SHA-512:	EB9296C93DBC08E2185569E4ACF7FD0924C7B18FF48820D2080F2222222A64FB8077969AABEFAC86E584912C3CAAA60249E4B6BA845FA4D0725B0E1FEF4B281 B
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\XjWJv9LQfx407iOuFqfg52ImSSTEQJORsxDRpBL3wWM[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):	21220
Entropy (8bit):	5.603190267916989
Encrypted:	false
SSDEEP:	384:lJ9/gLU3gFbszPJnRuR7mx4jMfvdTYOuqEUEJJQ3SZeh5:l7/gw3gts04nF8C/z
MD5:	1D2D321139D5C039E4B25BFE1B265D86
SHA1:	6CBAE7EE462629679C4A477462A52A0C94231735
SHA-256:	5E3589BFD2D07F1E34EE23AE16A7E0E762264924C4409391B310D1A412F7C163
SHA-512:	85EE19A9BAF51313B2F4FFCE15729C49BB33928EFED77FDDA26BD9C2BF2875A02E0BB51D6F38598388AE922275CC0DE151137C1F01BAB0B684B6E30A7D875A3 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\XjWJv9LQfx407iOuFqfg52ImSSTEQJORsxDRpBL3wWM[1].js	
IE Cache URL:	http://https://www.google.com/js/bg/XjWJv9LQfx407iOuFqfg52ImSSTEQJORsxDRpBL3wWM.js
Preview:	(function(){var N=function(x,a){if((a=(x=K.trustedTypes,null),!x)||!x.createPolicy)return a;try{a=x.createPolicy("bg",{createHTML:J,createScript:J,createScriptURL:J})}cat ch(w){K.console&&K.console.error(w.message)}return a},J=function(x){return x},K=this||self;(0,eval)(function(x,a){return(a=N())&&1===x.eval(a.createScript("1"))?function(w){return a.createScript(w)}:function(w){return""+w}}(K)(Array(7824*Math.random()|0).join("\n")+'(function(){var xW=function(x){return x},a_=function(x,a){function K(){}x .Dz=(x.prototype=(x.F=(K.prototype=a.prototype,a.prototype),new K),x.prototype.constructor=x,function(J,b,w){for(var N=Array(arguments.length-2),E=2;E<arguments .length;E++)N[E-2]=arguments[E];return a.prototype[b].apply(J,N)})},KR=function(x,a,K,J,b){return J=wW(x,function(w){b&&(a&&P(a),K=w,b(),b=void 0)},(b=(K=void 0 ,function(){}),!!a))[0],{invoke:function(w,N,E,V,X){if(!N)return N=J(E),w&&w(N),N;(V=function(){K(function(m){P(function(){w(m)})},E)},K)?V():(X=b,b=function(){X(),P(V)})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	16502
Entropy (8bit):	6.084222295357422
Encrypted:	false
SSDEEP:	384:AE6ldIFY7Pn36ohBPEOTcxh2SdnwXUkU7nqce/xXfjV/lTKnqcIzar5Cq:V6laFY7Pnrp6iUkU7Te/xXf5/lTKTuaL
MD5:	E89234F3C1BD383D808AC6FBA52BDBB1
SHA1:	238324DA7F2E2279B3717BD256CA45FC70109147
SHA-256:	53F529B5C165F6747A74870F2951C0A7528822FEA9E8498EC0D88F7F3FBF9420
SHA-512:	B4FA89A6C67906CB0D5AF9E5F2F59BBBAC93026EECD69CB0D9E227934DD0DF597F1D71AEF5484C8506B1E144C3A52B48A3A79398232DCE62CBBC69E02854D 89
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/dp/ads?adtest=off&channel=000001%2C000003%2C000489%2Cbucket052%2Cbucket077&cpp=0&hl=en&pcsa=false&client=dp-teaminternet08_3ph&r=m&psid=1349223201&type=3&max_radlink_len=40&swp=as-drid-2208190545638630&terms=Cremation%20Cost%2CCremation%20Without%20A%20Funeral%2CInexpensive%20Cremation%2CPrepaid%20Cremation%20Plans%2CCre mation%20Services%20Near%20Me%2CAffordable%20Burial%20%26%20Cremation%20Service&uiopt=true&oe=UTF-8&ie=UTF-8&fexp=21404%2C17300494%2C17300496%2C17300709%2C17300712%2C17300713&format=r6%7Cs&num=0&output=afd_ads&domain_name=pr.cremationservicesn ewusanet.com&v=3&adext=as1%2Csr1&bsl=8&u_his=1&u_tz=-420&dt=1624410951816&u_w=1280&u_h=1024&biw=767&bih=554&psw=767&psh=842&frm=0&uio=ff2sa16fa2sl1sr1-sa14st24lt34-&cont=tc&csize=w522h0&inames=master-1&jsv=17704&rurl=https%3A%2F%2Fpr.cremationservicesnewusanet.com%2F%3Fbackfill%3D0%26KW1%3DCremation%2BCost%26KW2%3DCremation%2BWithout%2BA%2BFuneral%26KW3%3DInexpensive%2BCremation%26KW4%3DPrepaid%2BCremation%2BPlans%26KW5%3DCremation%2BServices%2BNear%2BMe%26KW6%3DAffordable%2BBurial%2B%2526%2BCremation%2BService%26domainname%3D0%26searchbox%3D0%26subid1%3D7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045%26track_id%3D7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045%26kcoptimize%3D1%26theme%3DDo Plus
Preview:	<!doctype html><html lang="en-ES"> <head> <meta content="NOINDEX, NOFOLLOW" name="ROBOTS"> <meta content="telephone=no" name="format-detection"> <meta content="origin" name="referrer"> </head> <body> <script nonce="67K4xd4k1QFWLKlN2U4kSQ==">window.IS_GOOGLE_AF S_IFRAME_ = true;function populate(el) { var adBlock = document.getElementById("adBlock"); adBlock.innerHTML += el;}.var IS_GOOGLE_AFS_IFRAME_ = true;.var ad_json = {"caps":[{"n":"queryId","v":"twzSYLPwJ9XtxwLb4Lv4Dw"},{"n":"isLtr","v":"t"},{"n":"popstripeRs","v":"#1F8A70,#BEDB39,#FFE11A,#FD7400,#004358"}],"at":[{"v":" 52cc6eba","at":4,"r":[{"k":"ri133","v":"Related searches"},{"k":"ri143","v":"https://afs.googleusercontent.com/ad_icons/standard/publisher_icon_image/chevron.svg"},{"k":" ri102","v":"https://afs.googleusercontent.com/ad_icons/standard/publisher_icon_image/search.svg"}],"l":{"nt":0,"lr":{"o":0},"ch":[{"nt":0,"dbk":"t","lr":{"o":0,"a":6},"ch":[{"nt":0 ,"lr":{"o":0,"a":7},"ch":[{"nt":2,"dbk":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	183
Entropy (8bit):	5.149011623222219
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCNFSRI5XwDKLRIHDfFWYhfqzrZqcd+58d1gqdJtDQUYARNin:0IFFNFS+56Zzhizlpd+Gdeqd7JNin
MD5:	C8EF962B45D389627349DCA20FF07173
SHA1:	F5C9F3102E8258DB46005D9518E37F41339A1D0B
SHA-256:	7CF8B1AFE7BD63D68B7693798541404FC4DD9E962005D24A32F3B33E1EC72288
SHA-512:	131A8B9D6E32A63F42FC12FBC2BAC0C9CDE15E166C5DDBFC793EA5992D1ED67BBAEDFAE3B643FC0874A9289EB04CF69AEFC09B64DF99D6A043B2F3AF45B5 C85D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Poppins:300
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLDz8Z1xlEw.woff) forma t('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pxiByp8kv8JHgFVrLDz8Z1xlEw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10504, version 1.1
Category:	downloaded
Size (bytes):	10504
Entropy (8bit):	7.94478537149278

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pxiByp8kv8JHgFVrLDz8Z1xlEw[1].woff	
Encrypted:	false
SSDEEP:	192:QfEodsD0GBYNXGNpEg/cKhMTcWRCD0Y6MSPUakMo8Hpia8f8D3C3IBH0ZRvz9/y:QfEom7BYNWP7hicWwoYmPUakMKae3I5h
MD5:	081C758544B2BD948EB5D9CC419A597E
SHA1:	E81D58D009D6B57A3ABC3A8FE9C26845C1F9D54B
SHA-256:	8E14553C0CA1D74DCD39B12E0DE5815C599710BEB7E2EAE43BA4FE6B6628D66D
SHA-512:	94F245D9B06D7235A91F23A063B15DBA416833C9A3AB482EF09C242C2CA6527B94BBDCE6D273C40BAAA126F5E468B118FB417464C550A94B3AED0A8E3A09D25 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLDz8Z1xlEw.woff
Preview:	wOFF.....).....? .....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...l...N...`Y...cmap.....glyf...P.. 5..3bAd.head.."....6...6..$Yhhea.."....$....hmtx.."....h.( mloca..$.....e.xmaxp..&.... ... .\.1name..&.....&e?bpost..'....g....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r,,@..?.....<....x.c`a.a.a`e``.b.```...q.F...@.....H.3..... (..E.),.L.....ArLJL{.....m..x.c```.bf ....`.....aP..x.,^:.....L{..1.b.. . . ....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G.."....5..x.Z.`....]....B...X.m...S.,[V. ...16.tL/)tx.?.'.'.....IOH...4.K..5.....;I.....t7.:;;;....t...Kr..P.....eI..X*...8K(....4|.{..'N.C'..8A.;.....X.%....A..i2....H .d..zF.#..!;3.2I...#.....q.....@...>..A_!.....S.S....*.{.....!.....y ....2 .w...`.pP.L.N..nU8....._._.o=i.....'adk.A...T.*.....X.+-.399.,....t..nd@.* b...q.^...A.....@...h0..V6.O.gT3.&#{.....e..b..7L..T.&aqvq.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\caf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	177611
Entropy (8bit):	5.600340944097303
Encrypted:	false
SSDEEP:	3072:CMqhjo69iispe8huUC4bea4a9akUlq93Me+7K/gB3:Fw8dispe8ZbP98kUlqlN+7vx
MD5:	DCE0DBEF8CD7BB1EA335E303966DD282
SHA1:	96DEAB9410C0BAAECA8300F2400D453B681ACFE5
SHA-256:	1C93CF7C729BCCE819DF72E770B8C87980C02EB6B7A28AE298B2A131E7792203
SHA-512:	A0EE7899D32481ED71A38C6C722650F8724ED84F32B01F8015BC74BFD1D2D78952C79772D87AB12B3BA046BD4BEC763E3BA4A61E62AA83165021AB6476682BF
Malicious:	false
Reputation:	low
Preview:	if(!window['googleNDT_']){window['googleNDT_']=(new Date()).getTime();}window._googCsaExpIds='17300494,17300496,17300709,17300712,17300713';window._go ogCsaAlwaysHttps=1;window._googEnableCcpaForCanoeV2=1;window._googEnableQup=1;window._googErrorTurnOffPersonalization=1;window._googTimeoutT urnOffPersonalization=1;window._googLazyLoadingDenyList='bS5zZWFycy5jb20saXppdG8semFwbWV0YSxhbWVyaWNhbmxpc3RlZC5jb20sYmVzdHJldmlld 3MuZ3VpZGUsY2FyZWVyamV0LmpwLGN5YmVybW9uZGFsZGVhbHMuY2VudGVyLGVsY2xhc2lmaWNhZG8uY29tLGpvcmEuY29tLHd3dy5ub3ctc2FsZS5jby51a yxjbC5iZWJlZS5jb20sc3VjaGUud2ViLmRlLHd3dy5hbGxzZWFyY2hzaXRlLmNvbSx3d3cueWVsbG93cGFnZXMuY29tLGRlLmpvYnJhcGlkby5jb20sZnIuY29uc3VtZXJ zZWFyY2guY29tLGhhc2dlbmVyYWwuaW5mbyxpbnQuc2VhcmNoLm15d2F5LmNvbSxpbnQuc2VhcmNoLnRiLmFzay5jb20sam9vYmxlLm9yZyxtLmFwa3B1cmU uY29tLG0uaW5kaWFtYXJ0LmNvbSxtLmluLmxvY2FuLnRvLG0ucXVva2EuZGUsbXlicm93c2VyLXNlYXJjaC5jb20sbm9ydG9uc2FmZS5zZWFyY2guYXNrLmNvbSxydS5na WdhcHJvbW8uY29tLHNkLmNhYy5hdHRvcm5leSxzZWFyY2gubXl3YXkuY29tLHNlYXJjaC5zbXQuZG9jb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	200
Entropy (8bit):	5.071788021786005
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCrv/MRI5XwDKLRIHDfFRWdFWLRI9j9v7fqzrZqcdZAWHTLj/+xEBxg:0IFFrs+56ZRWHMqh7izlpdZAS+xqNin
MD5:	29E08504335319B088079B0C9D9F60D4
SHA1:	7F7419D267FB821F50E27FDF14346758770F8F77
SHA-256:	76E06BF782F5DC3057859F0DCC0C09744294DE99BE3E09743BFB72117482D4CA
SHA-512:	CB0C302B3438FF16964FADEE54802394FA7E9638D5AE9670BD9213133C345C5273829A17A88EE7BFE0834C72882177EEBFC2FF1952EA1A51AC400A96DBFCC72
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Mate%20SC&display=swap
Preview:	@font-face {. font-family: 'Mate SC';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/matesc/v11/-nF8OGQ1-uoVr2wK- iLT8A.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js3caf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7000
Entropy (8bit):	4.809324911486411
Encrypted:	false
SSDEEP:	192:wnS/jBKcACl3gC2z12a+hh9I3Dr+3SQ4sX5sU827yiQT+ddQ1:wS/jBKoBC2aQhKDy3SJs59ON1
MD5:	CCE7F943EC8E7B4BA13BE4ABA6B463D9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js3caf[1].js	
SHA1:	220F3E8CA723DAA91FD040CF518991A65F2BF110
SHA-256:	BA5B7354353B0EEC1637564DAE072FEE662A5B9862F6BF7ED5E60A5A76F2EF44
SHA-512:	5534D4EE216A7CBACE73E66D9BA9D36C78EEE2FEE0EFDD84A84042BD0DFCCFE0EC6BCF9CB6A6EC8968EE5EB252C865995BA9B730AE7E53F64167C0577A5181A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1lxhc4jvstzrp.cloudfront.net/scripts/js3caf.js
Preview:	var pageLoadedCallbackTriggered = false;.var fallbackTriggered = false;.var formerCalledArguments = false;..var pageOptions = {. 'pubId': 'dp-teaminternet01',. 'resultsPageBaseUrl': '//parkingcrew.net/?ts=',. 'fontFamily': 'arial',. 'optimizeTerms': true,. 'maxTermLength': 40,. 'adtest': true,. 'clicktrackUrl': '//track.parkingcrew.net/track.php?',. 'attributionText': 'Ads',. 'colorAttribution': '#b7b7b7',. 'fontSizeAttribution': 16,. 'attributionBold': false,. 'rolloverLinkBold': false,. 'fontFamilyAttribution': 'arial',. 'adLoadedCallback': function(containerName, adsLoaded, isExperimentVariant, callbackOptions) {. if (!adsLoaded) {. try {. var ele = document.getElementById(container).getElementsByTagName('iframe')[0];. var vars = JSON.parse(ele.name.substr(ele.id.length + 1));. if (typeof vars[ele.id].type == "string" && vars[ele.id].type == "relatedsearch") {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\search[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	4.739217439523181
Encrypted:	false
SSDEEP:	6:t6D14mc4slzTPl2O4UYaeLIT4W+KS4S1UpMTQpi6jUs8sh6B+BSmK0C:t6+FPUPkHSt1UiT6i6jUs8b0l0C
MD5:	10216A4FE40133F3238AB3422FD7E706
SHA1:	958B620EE5D32C871395749B2145514368EB8920
SHA-256:	1FD2E4AD62FA13E30DCE09194A2D054B4537BBD2ED6F25E7202B3B7BA537155F
SHA-512:	4285A3DDD1487A69209BE4A2C25BD6313BA42D43319A7B7EF221030061F441B9E219409278597DC824004548C1622A2200B24CCF2AA4C3CC1ED2FCA25ADF3D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://afs.googleusercontent.com/ad_icons/standard/publisher_icon_image/search.svg?c=%2376ff03
Preview:	<svg fill='#76ff03' xmlns="http://www.w3.org/2000/svg" width="200" height="200" viewBox="0 0 24 24"><path d="M15.5 14h-.79l-.28-.27C15.41 12.59 16 11.11 16 9.5 16 5.91 13.09 3 9.5 3S3 5.91 3 9.5 5.91 16 9.5 16c1.61 0 3.09-.59 4.23-1.57l.27.28v.79l5 4.99L20.49 19l-4.99-5zm-6 0C7.01 14 5 11.99 5 9.5S7.01 5 9.5 5 14 7.01 14 9.5 11.99 14 9.5 14z"/><path d="M0 0h24v24H0z" fill="none"/></svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	829
Entropy (8bit):	5.058569541320297
Encrypted:	false
SSDEEP:	24:wB02AmB02AmB02ApaGJ/CxJLZHuK7e5CZduSZ+:kHHca3TZGJ
MD5:	96F84D0985AF87B4D4F6AE8816F9C5C5
SHA1:	9CF62A3E426361587207124EB6CAF0AEEB3CB030
SHA-256:	93A1109ADA0CD55DEDEAF7E9C4251A7F91AC3C3E1AB85E25E37B6CD4E47D504B
SHA-512:	0423C77082E7CEDE3ED0C10219D8DCE268D2F137C2B5BD46D1A9FC1A15EEFD316D190BACD3AC22C60FDE155DC044ED3886646A2C1453EA3B82393ABDCF7D2B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1lxhc4jvstzrp.cloudfront.net/themes/assets/style.css
Preview:	.asset_star0 {..background: url('star0.gif') no-repeat center;..width: 13px;..height: 12px;..display: inline-block;.}...asset_star1 {..background: url('star1.gif') no-repeat center;..width: 13px;..height: 12px;..display: inline-block;.}...asset_starH {..background: url('starH.gif') no-repeat center;..width: 13px;..height: 12px;..display: inline-block;.}...sitelink {..padding-right: 16px;.}...sellerRatings a:link,..sellerRatings a:visited,..sellerRatings a:hover,..sellerRatings a:active {..text-decoration: none;..cursor: text;.}...sellerRatings {..margin:0 0 3px 20px;.}...sitelinkHolder {..margin:-15px 0 15px 35px;.}..#ajaxloaderHolder {..display: block;..width: 24px;..height: 24px;..background: #fff;..padding: 8px 0 0 8px;..margin:10px auto;..-webkit-border-radius: 4px;..-moz-border-radius: 4px;..border-radius: 4px;.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1417
Entropy (8bit):	4.785311295820333
Encrypted:	false
SSDEEP:	24:dvSFF9vW7UcfU5HKLUtFuac0PNTZpYj1qRbUJ9blQxkFzUzojULIbWNEc4DMk5Em:dvKHHK7ac0PNNJR49CkFW1w
MD5:	29952CF23B2A110A8085FBE5C29C14C0
SHA1:	CC0A7F1AD0A5B132821DBED19D593C98361C0CD0
SHA-256:	2E3C8229D7851FA3345FA481BA64B70590D92E466CBC4BCC3E9905AC27C80B2F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[2].css	
SHA-512:	2314407FD20B43DE1FAFDF10BAE22AAE7DFA28E50979EE708FDEF8FBDC9F247DE3445B64DA07C4D179061CF7FC5B21A694C4F4F328710FD59B891D9B3706FD9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/style.css
Preview:	* {margin:0;padding:0}..body {. background:#313131;. font-family: 'Poppins',sans-serif;. text-align: center;. font-size:1rem;.}...header {. padding:1rem 1rem 0;. overflow:hidden;.}..h1 {. color:#848484;. font-size:1.5rem;.}...wrapper1 {. margin:1rem;.}...wrapper2 {. background:url('img/bottom.png') no-repeat center bottom;. padding-bottom:140px;.}...wrapper3 {. background:#fff;. max-width:300px;. margin:0 auto 1rem;. padding-top:1px;. padding-bottom:1px;.}...onDesktop {. display:none;.}...tcHolder {. margin:1rem 4px 2rem;.}...adsHolder {. margin:1rem;. overflow:hidden;.}...searchHolder {. padding:1px 0 1px 1px;. margin:1rem auto;. background:#848484;.}...footer {. color:#949494;. padding:2rem 1rem;. font-size:.8rem;. margin:0 auto;. max-width:440px;.}...footer a:link,..footer a:visited {. color:#949494;.}...wrapper1 .sale_link_bold a,..wrapper1 .sale_link a {. color:#ccc;.}...wrapper1 .sale_link_b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\chevron[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	200
Entropy (8bit):	5.025855206845441
Encrypted:	false
SSDEEP:	6:t6wfDpmc4slhohC/vmI4SmK0xhFELE47zF:t6qnoU/vmRI0xQTF
MD5:	11B3089D616633CA6B73B57AA877EEB4
SHA1:	07632F63E06B30D9B63C97177D3A8122629BDA9B
SHA-256:	809FB4619D2A2F1A85DBDA8CC69A7F1659215212D708A098D62150EEE57070C1
SHA-512:	079B0E35B479DFDBE64A987661000F4A034B10688E26F2A5FE6AAA807E81CCC5593D40609B731AB3340E687D83DD08DE4B8B1E01CDAC9D4523A9F6BB3ACFCEA0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://afs.googleusercontent.com/ad_icons/standard/publisher_icon_image/chevron.svg?c=%23ffffff
Preview:	<svg fill='#ffffff' xmlns="http://www.w3.org/2000/svg" height="24" viewBox="0 0 24 24" width="24"><path d="M0 0h24v24H0z" fill="none"/><path d="M5.88 4.12L13.76 12l-7.88 7.88L8 22l10-10L8 2z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	179
Entropy (8bit):	5.067165111291868
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCNFSRI5XwDKLRIHDfFRWdFTfqzrZqcd+M+jgXNYARNin:0IFFNFS+56ZRWHTizlpd+M+cXFNin
MD5:	46FFF5C1AE13CAC68764A9BBF1B78C6B
SHA1:	3257E52A6E325355B6F596930457200988412 6FD
SHA-256:	2CA8E111AAE98F36D0F4671DBB9C6898627637AABA90A7626BDA425C28A4C35A
SHA-512:	6D8F5485A7C32E9F4AC2948CDAD2D077A693AAFDD258591E9F57927C59A6FF9206AA6615C3145A1ACFB01732C46A22BA1EE0306D671C4FCB63D5CE32EA47152
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Poppins
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfedA.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\webfont[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13188
Entropy (8bit):	5.4223896155104025
Encrypted:	false
SSDEEP:	384:i11kqRm4UjryX2DfatZrT80NCGz5r2zItrX:iEqRm4cy338m7d
MD5:	7C96A5F11D9741541D5E3C42FF6380D7
SHA1:	D3FA2564C021CF730E58FFDDB138CF6B57ED126E
SHA-256:	81016AC6BE850B72DF5D4FAA0C3CEC8E2C1B0BA0045712144A6766ADFAD40BEE
SHA-512:	23C162A2E268951729B580E5035AD6CA9969CFCC5CE58A220817B912E76B38BE6C29C3CA7680CB4E8198863D95A72EA65BD06FF7189B5C8475E4C1CE501AEAE1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\webfont[1].js	
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/webfont/1/webfont.js
Preview:	/*. * Copyright 2016 Small Batch, Inc.. *. * Licensed under the Apache License, Version 2.0 (the "License"); you may not. * use this file except in compliance with the Li cense. You may obtain a copy of. * the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, softwa re. * distributed under the License is distributed on an "AS IS" BASIS, WITHOUT. * WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the. * License for the specific language governing permissions and limitations under. * the License.. */./* Web Font Loader v1.6.26 - (c) Adobe Systems, Google. License: Apache 2.0 */(function(){function aa(a,b,c){return a.call.apply(a.bind,arguments)}function ba(a,b,c){if(!a)throw Error();if(2<arguments.length){var d=Array.prototype.sl ice.call(arguments,2);return function(){var c=Array.prototype.slice.call(arguments);Array.prototype.unshift.apply(c,d);return a.apply(b,c)}}return function(){return a.app

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\-nF8OGQ1-uoVr2wK-iLT8A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 12396, version 1.1
Category:	downloaded
Size (bytes):	12396
Entropy (8bit):	7.9490517609360225
Encrypted:	false
SSDEEP:	384:cEbZyCKxgHARlRZbNFH5X0667NU0ajlSUM:cEbZyCLelRZb/H5E1V
MD5:	54E2D4A178793E6F674A0E356E7BF277
SHA1:	6E09B9B2BA35EB38985F80719D7847BDCE7710BD
SHA-256:	95D4C520ED7CCE462884A77119FF377A5700FADD36C0D1632FA7C2E9E0D31B26
SHA-512:	B799008400BD55EC484253C67EA2786C8EDE5CCE80474BBB07958C61D27CF91AE8B5EB2925CDDAD97C57C7AF7597B41A31376AB90F08D562D63F796BACFF97 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/matesc/v11/-nF8OGQ1-uoVr2wK-iLT8A.woff
Preview:	wOFF.....0l.....].....GDEF...X.....GPOS...p...6.....G-1GSUB.....l.t.OS/2.....N...`dB".cmap.....{..gasp.....glyf.....%...M..1qhead..*,...2...6.. .hhea..*`.....$...khmtx..*.....T...<loca..,X.....maxp..... ... .$..name... .....-wF.post../(...9..../..prep..0d.....h.....x.u...\Q.F.u1,.....m..ZQm....m.n.....|.s.=... ...*..!.'...0.....r2.cQ...KG.]u.V.lY.S..4..3..l.0.y...!J..F.s..^....q./.Y.i^Z.U../.hB.:.^...N47[iiN.V.Jw.i.1Sk.d...2OB....D%&q..m.]v.N.%{..N....].d.l...Sv..9&>.k...%"Q.I\.j....D$*1.. V.sB...D%&q..KH.....$.6.q..i.$..0[.~.G./2...h.e..<OX....I....i.....&...Nd.h.....u...,..DujP.....hLS...>..?....%,e..Y.JV.....^.....0g8.y.`S....*.....P]...\j. ..C..r.DX4U...N*.U.4#.....U.. (..*.2V.F9lT.!.....<...V.4-..yU..*....r~O.a>.-....KW...[.....|LW~f2.....0..,.e...Gy.w....a..r8.....4.....latn.....x.c`b<.8.....i.S...C..f..`...(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\C4004G0V.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13150
Entropy (8bit):	5.956395844202734
Encrypted:	false
SSDEEP:	192:TiqHHpziim56yMyTvitjb050CG99iP2tvW1612ecDmKJ1r8ipzxcgYVq7D:Ti8C56yMPtjb05xewAGJ1r8ipzxcgUqX
MD5:	20D91D3EC7EE3715F50DE972CF26FC9A
SHA1:	65E96FA53D54C01FE587F9B1940DE1307F2E17DD
SHA-256:	C826B99B4354A8B527A61982FF798EF0D6B81D9578FF9F8D941DDAFCE6914952
SHA-512:	C85108C2127DA51D545C4B5DFD290E19BE84B86CEE4EFE528C3EFBA50714BDB378F5A04309DA4D9FB95B7C923BF66BD0614F7FA44CEF112BC5CF9334A5159C 7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pr.cremationservicesnewusanet.com/?backfill=0&KW1=Cremation+Cost&KW2=Cremation+Without+A+Funeral&KW3=Inexpensive+Cremation&KW4=Prepaid+Cremation+Plans&KW5=Cremation+Services+Near+Me&KW6=Affordable+Burial+%26+Cremation+Service&domainname=0&searchbox=0&subid1=7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5a eb045&track_id=7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045&kcoptimize=1&theme=DoriPlus
Preview:	<!DOCTYPE html>.<html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALquDFETXRn0Hr05fUP7EJT77xYnPmRbpMy4vk8KYiHnkNpednjOANJcaXD XcKQJN0nXKZJL7TciJD8AoHXK158CAwEAAQ==_Aj8QvmOk8YDTnWYYFzUxuEg6EazTV676m44gnb8IRF22EgbDP+B7I52r5IiAH5+CccolyPeraUEyNWR0NMKlwA==" xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>. <meta name="viewpo rt" content="width=device-width, initial-scale=1, shrink-to-fit=no" />. <title>cremationservicesnewusanet.com</title>..<script src="//www.google.com/adsense/domains/ca f.js" type="text/javascript" ></script>..<link href="//d1lxhc4jvstzrp.cloudfront.net/themes/assets/style.css" rel="stylesheet" type="text/css" media="screen" />..<link hr ef="//d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/style.css" rel="stylesheet" type="text/css" media="screen" />..<link href="https://fonts.googleapis.com/css?family=Poppins:300" rel="stylesheet">..<meta name="description"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\arrows[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1500 x 600, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	15544
Entropy (8bit):	7.830892060370354
Encrypted:	false
SSDEEP:	384:gH9eTHok3FZUG6SZhaQtDvcaiCjVpNLeQtf1cg:Cebokfn6SZhP8CxpNz1z
MD5:	72A92898F1DD7EA307CE6F2890D165F4
SHA1:	CF167FF00875385B08356A9E3B82C8930F019107
SHA-256:	8FCEB564C059D6FFAD5C8F3A5E5617A57D501C1E10DE1874357505831E2FDB4C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\arrows[1].png	
SHA-512:	14BFEDD1A64F62EF28D0A985FC525A0964BCCB8809878C9950813314C3831E6F4239C3AEDAB2912C2E7F18992CC593CC72BD3C963C76584821D9625389D364D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/img/arrows.png
Preview:	.PNG.....IHDR.....X.....Om.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns :xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:D3C817C4AD4111E981BCF119B51C018E" xmpMM:InstanceID="xmp.iid:D3C817C3AD4111E981 BCF119B51C018E" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:AF76D76FB59311E68C42BF3A 862DE99B" stRef:documentID="xmp.did:AF76D770B59311E68C42BF3A862DE99B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>`.H.....PLTE111. ..ZZZ_./f....fj.U.....3@....)4.....Ual.\.X_.&4...Pa..e..C666.m.....+7..[mnY.8..{.hvwt\888.&3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\caf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	177611
Entropy (8bit):	5.600343596240036
Encrypted:	false
SSDEEP:	3072:NMqhjo69iispe8huUC4bea4a9akUlq93Me+7K/gB3:+w8dispe8ZbP98kUlqlN+7vx
MD5:	FA50ECE2AE647B0E59B3ECD6A9DD714F
SHA1:	76EFD35869E183E4E03F0716C9BA983C1CDA404E
SHA-256:	CA83A4A1C9B9CA48743A7CFA2D9C07FD21B7C79F5EEF27BD5CC1E1DA2CA676AB
SHA-512:	4AC993466609B49274FC714050BBC463BC3EBD4CEBE6606E23739E5D00A2C91103B7C7EDB280AA041F3C502C72D651DA15B52696C527DA6422E70C37AAF9453
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/adsense/domains/caf.js
Preview:	if(!window['googleNDT_']){window['googleNDT_']=(new Date()).getTime();}window._googCsaExpIds='17300494,17300496,17300709,17300712,17300714';window._go ogCsaAlwaysHttps=1;window._googEnableCcpaForCanoeV2=1;window._googEnableQup=1;window._googErrorTurnOffPersonalization=1;window._googTimeoutT urnOffPersonalization=1;window._googLazyLoadingDenyList='bS5zZWFycy5jb20saXppdG8semFwbWV0YSxhbWVyaWNhbmxpc3RlZC5jb20sYmVzdHJldmlld 3MuZ3VpZGUsY2FyZWVyamV0LmpwLGN5YmVybW9uZGFsZGVhbHMuY2VudGVyLGVsY2xhc2lmaWNhZG8uY29tLGpvcmEuY29tLHd3dy5ub3ctc2FsZS5jby51a yxjbC5iZWJlZS5jb20sc3VjaGUud2ViLmRlLHd3dy5hbGxzZWFyY2hzaXRlLmNvbSx3d3cueWVsbG93cGFnZXMuY29tLGRlLmpvYnJhcGlkby5jb20sZnluY29uc3VtZXJ zZWFyY2guY29tLGhhc2dlbmVyYWwuaW5mbyxpbnQuc2VhcmNoLm15d2F5LmNvbSxpbnQuc2VhcmNoLnRiLmFzay5jb20sam9vYmxlLm9yZyxtLmFwa3B1cmU uY29tLG0uaW5kaWFtYXJ0LmNvbSxtLmluLmxvY2FuLnRvLG0ucXVva2EuZGUsbXlicm93c2VyLXNlYXJjaC5jb20sbm9ydG9uc2FmZS5zZWFyY2guYXNrLmNvbSxydS5na WdhcHJvbW8uY29tLHNkLmNhYy5hdHRvcm5leSxzZWFyY2gubXl3YXkuY29tLHNlYXJjaC5zbXQuZG9jb
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\pxiEyp8kv8JHgFVrJJfedA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10536, version 1.1
Category:	downloaded
Size (bytes):	10536
Entropy (8bit):	7.942419499918068
Encrypted:	false
SSDEEP:	192:YLS34U1mA6N/1JO/mA4WIxpqVkHm8zXxykTBBq1SEOAY/y:YLSoU1mA6N/1A/2XqVkHfznN8Hv
MD5:	4FC29212BD42883C45EDD0BFBD91AD72
SHA1:	6FF25B6FAE5D1C35B9255A483283AA7F698A10E8
SHA-256:	12BCAA5F5203A347C58533BE7E0051BB7EA4432D27A472CC36E32C398A585B00
SHA-512:	A29A37030600435E64B19C1ACCA2E47C7533DCEAA2FE01BB3D3577DFFA4E29DA9FFC912D00FEC1C1DCC3FE50DADA9153B72090AF1FB290D14BFF8B92AE1D(249
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfedA.woff
Preview:	wOFF.....)(.....?.....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...I...M...`Y..cmap.....glyf...P.. Y..32.w..head..''....6...6..$ahhea..''.....$.u..hmtx..#.....h.( .loca..%.....E.fmaxp..&.... ... .\.,name..&.....(.C.post..'....g.....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r.,.@..?.....<....x.c`a.f.....=.\....3 ...7.....J.,R ..1...3.+00L..1.0..R.,.....x.c```.bf ....`.....aP..x.,^.:.....L{..1.b.. . . .....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G..''.....5..x.:.`SG..+c.md..''K.\%[.Y.U.b ..]r/.....:...HHo...\...+\.|.{.!.J..'G:..?..$.....N...f!.....9h>J@(Q.(.''!O+..d).....w3...|. ...U.....v.3...1.3..''.=t..K.#.....*.R.''X./~a.w^.D..&.....`.$=]B/.+&-...X>..J.....)\.%/....!.K$_....t. .1_.e/....|z.\.W.5.;o/n+~..=...~(....w...?..2.5D.0.).[..[.$..).....bu~.T..''T..,F.V.....,''@....$i.*.....*..%..*IM..nM..}.T.V...i..U.....g....g.I.x-...>..

C:\Users\user\AppData\Local\Temp\~DF0EAA380694CF522F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35235
Entropy (8bit):	0.48036794253751314
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+UeZbS5FCF5wcuDqTqVU:kBqoxKAuqR+UeZbS5FO5wccnU
MD5:	7E338190BE8013CD7A16F5F15AFF98A7

C:\Users\user\AppData\Local\Temp\~DF0EAA380694CF522F.TMP	
SHA1:	D9B79F386B783C4CFE0413E9FF9B5FC4AE140FD4
SHA-256:	D12DCBDB7CB675103230D0C2EFDE8D1D9634E9A2324D3E3BD1D70600C5E08137
SHA-512:	3EDBDA7A7C9D8D6785F64262EDCC52FB98F348F6DB26800E67937771196B19C300DF1C78D97854A84D6BE58458D67289E9C2CDECD823903AD703F220F405F4C
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF69E7BBDB605ADC19.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.34049148406226865
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA2OlqHLgg:kBqoxxJhHWSVSEab
MD5:	EACD1DC197B9E63735BD101D8C05001B
SHA1:	C2A64A41A8E81814DE78E9BC6B98D0A890C110AD
SHA-256:	FD52F1C72386F843D0C1A249190D45F33FAF1091766CDC2C4EC8AEBFC331020F
SHA-512:	EE3DBCE33D80E36CEC6CF16884F66E0A7E1CAC38F8CE1746120B0B1B4C8B9FFC13FC19F969728403770B615DF560C82154E0888A320B952A9A485712FB164AA
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF72E20344339451D6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48135009926254485
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9losF9loM9lWt+PNvtOxF:kBqoIHhtANvtyF
MD5:	927E04837A14EF65ECB6CA0B1F0B51CE
SHA1:	B67F57782663DE67F5E6C93FAC4DC5F68C519BA6
SHA-256:	05A5C2AE13AB2AD9E9A2677A0D743D612DA6E125388208C5258AB79BA08550D5
SHA-512:	FBE52AF4DAEBD8134ADF17624819FC38CF6731C8CDBE808F7BF58FC6978CB69D0C71BBE587462DE28179ED97F1AFD17C3C4B1DBD39913D000BBF1712B300B B0
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

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:15:49.634982109 CEST	192.168.2.3	8.8.8.8	0xc3d8	Standard query (0)	3c4e7b.zgmwgzfzdwxnrfq.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.152076006 CEST	192.168.2.3	8.8.8.8	0x42a3	Standard query (0)	pr.cremationservicesnewusanet.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.824862003 CEST	192.168.2.3	8.8.8.8	0xfa6f	Standard query (0)	d1lxhc4jvstzrp.cloudfront.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:52.330718040 CEST	192.168.2.3	8.8.8.8	0x5bc8	Standard query (0)	afs.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:16:06.418153048 CEST	192.168.2.3	8.8.8.8	0x29b6	Standard query (0)	pr.cremationservicesnewusanet.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:15:49.717869997 CEST	8.8.8.8	192.168.2.3	0xc3d8	No error (0)	3c4e7b.zgmwgzfzdwxnrfq.com	dk8g5exin21my.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:15:49.717869997 CEST	8.8.8.8	192.168.2.3	0xc3d8	No error (0)	dk8g5exin21my.cloudfront.net		13.224.193.70	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:49.717869997 CEST	8.8.8.8	192.168.2.3	0xc3d8	No error (0)	dk8g5exin21my.cloudfront.net		13.224.193.62	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:49.717869997 CEST	8.8.8.8	192.168.2.3	0xc3d8	No error (0)	dk8g5exin21my.cloudfront.net		13.224.193.10	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:49.717869997 CEST	8.8.8.8	192.168.2.3	0xc3d8	No error (0)	dk8g5exin21my.cloudfront.net		13.224.193.117	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.225207090 CEST	8.8.8.8	192.168.2.3	0x42a3	No error (0)	pr.cremationservicesnewusanet.com		185.53.179.91	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.895144939 CEST	8.8.8.8	192.168.2.3	0xfa6f	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.194.160	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.895144939 CEST	8.8.8.8	192.168.2.3	0xfa6f	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.194.39	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.895144939 CEST	8.8.8.8	192.168.2.3	0xfa6f	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.194.227	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:50.895144939 CEST	8.8.8.8	192.168.2.3	0xfa6f	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.194.139	A (IP address)	IN (0x0001)
Jun 22, 2021 18:15:52.397872925 CEST	8.8.8.8	192.168.2.3	0x5bc8	No error (0)	afs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:15:52.397872925 CEST	8.8.8.8	192.168.2.3	0x5bc8	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.161	A (IP address)	IN (0x0001)
Jun 22, 2021 18:16:06.481455088 CEST	8.8.8.8	192.168.2.3	0x29b6	No error (0)	pr.cremationservicesnewusanet.com		185.53.179.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 3c4e7b.zgmwgzfzdwxnrfq.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	13.224.193.70	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:15:49.777601004 CEST	1196	OUT	GET / 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: 3c4e7b.zgmwgzfzdwxnrfq.com Connection: Keep-Alive
Jun 22, 2021 18:15:50.139503002 CEST	1205	IN	HTTP/1.1 307 Temporary Redirect Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Date: Tue, 22 Jun 2021 16:15:50 GMT Server: nginx X-Status: OK X-UID: d69f5f37 Location: https://pr.cremationservicesnewusanet.com?backfill=0&KW1=Cremation+Cost&KW2=Cremation+Without+A+Funeral&KW3=Inexpensive+Cremation&KW4=Prepaid+Cremation+Plans&KW5=Cremation+Services+Near+Me&KW6=Affordable+Burial+%26+Cremation+Service&domainname=0&searchbox=0&subid1=7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045&track_id=7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045&kcoptimize=1&theme=DoriPlus Referrer-Policy: unsafe-url X-Cache: Miss from cloudfront Via: 1.1 f7bf326347bdd7f275a38a22b5b83724.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA2-C1 X-Amz-Cf-Id: 8tCb0Mm1neJIQs0gBID-V4Q7ZhDPJxLIrw7S-kdqe2TuxGSI-RtB0Q== Data Raw: 31 64 62 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 31 3b 75 72 6c 3d 68 74 74 70 73 3a 2f 2f 70 72 2e 63 72 65 6d 61 74 69 6f 6e 73 65 72 76 69 63 65 73 6e 65 77 75 73 61 6e 65 74 2e 63 6f 6d 3f 62 61 63 6b 66 69 6c 6c 3d 30 26 4b 57 31 3d 43 72 65 6d 61 74 69 6f 6e 2b 43 6f 73 74 26 4b 57 32 3d 43 72 65 6d 61 74 69 6f 6e 2b 57 69 74 68 6f 75 74 2b 41 2b 46 75 6e 65 72 61 6c 26 4b 57 33 3d 49 6e 65 78 70 65 6e 73 69 76 65 2b 43 72 65 6d 61 74 69 6f 6e 26 4b 57 34 3d 50 72 65 70 61 69 64 2b 43 72 65 6d 61 74 69 6f 6e 2b 50 6c 61 6e 73 26 4b 57 35 3d 43 72 65 6d 61 74 69 6f 6e 2b 53 65 72 76 69 63 65 73 2b 4e 65 61 72 2b 4d 65 26 4b 57 36 3d 41 66 66 6f 72 64 61 62 6c 65 2b 42 75 72 69 61 6c 2b 25 32 36 2b 43 72 65 6d 61 74 69 6f 6e 2b 53 65 72 76 69 63 65 26 64 6f 6d 61 69 6e 6e 61 6d 65 3d 30 26 73 65 61 72 63 68 62 6f 78 3d 30 26 73 75 62 69 64 31 3d 37 65 30 36 64 30 66 37 30 62 35 64 62 33 36 34 62 36 34 33 64 32 31 33 34 35 64 31 32 36 30 61 39 38 36 65 36 38 36 30 63 65 37 33 30 34 35 36 39 62 63 30 34 31 62 30 61 35 61 65 62 30 34 35 26 74 72 61 63 6b 5f 69 64 3d 37 65 30 36 64 30 66 37 30 62 35 64 62 33 36 34 62 36 34 33 64 32 31 33 34 35 64 31 32 36 30 61 39 38 36 65 36 38 36 Data Ascii: 1db7<!DOCTYPE html><html><head> <meta http-equiv="refresh" content="1;url=https://pr.cremationservicesnewusanet.com?backfill=0&KW1=Cremation+Cost&KW2=Cremation+Without+A+Funeral&KW3=Inexpensive+Cremation&KW4=Prepaid+Cremation+Plans&KW5=Cremation+Services+Near+Me&KW6=Affordable+Burial+%26+Cremation+Service&domainname=0&searchbox=0&subid1=7e06d0f70b5db364b643d21345d1260a986e6860ce7304569bc041b0a5aeb045&track_id=7e06d0f70b5db364b643d21345d1260a986e686

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
Jun 22, 2021 18:15:50.358321905 CEST	185.53.179.91	443	192.168.2.3	49713	CN=pr.cremationservicesnewusanet.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 30 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Aug 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jun 22, 2021 18:15:50.360755920 CEST	185.53.179.91	443	192.168.2.3	49714	CN=pr.cremationservicesnewusanet.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 30 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Aug 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jun 22, 2021 18:15:51.009607077 CEST	13.224.194.160	443	192.168.2.3	49719	CN=*.cloudfront.net 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	Fri Mar 19 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Mar 18 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:15:51.011410952 CEST	13.224.194.160	443	192.168.2.3	49718	CN=*.cloudfront.net 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	Fri Mar 19 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Mar 18 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 22, 2021 18:15:51.014213085 CEST	13.224.194.160	443	192.168.2.3	49717	CN=*.cloudfront.net 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	Fri Mar 19 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Mar 18 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:15:52.493772984 CEST	216.58.212.161	443	192.168.2.3	49727	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 24 04:59:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 16 04:59:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 22, 2021 18:15:52.494096994 CEST	216.58.212.161	443	192.168.2.3	49728	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 24 04:59:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 16 04:59:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 22, 2021 18:16:06.614042044 CEST	185.53.179.91	443	192.168.2.3	49737	CN=pr.cremationservicesnewusanet.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 30 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Aug 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4580 Parent PID: 792

General

Start time:	18:15:48
Start date:	22/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff628c90000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5436 Parent PID: 4580

General

Start time:	18:15:49
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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

Show Windows behavior

Disassembly