ID: 831147
Sample Name: VM From (937) 669-5620 On Tue March 21 2023.msg
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 06:22:21
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

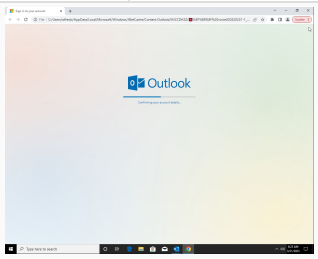
Windows Analysis Report

VM From (937) 669-5620 On Tue March 21 2023.msg

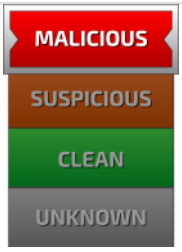
Overview

General Information

Sample Name:	VM From (937) 669-5620 On Tue March 21 2023.msg
Analysis ID:	831147
MD5:	67a7c87d2ee1…
SHA1:	97b8ce82e0ae…
SHA256:	82c95297d4b3…



Detection



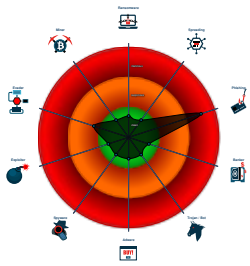
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- None HTTPS page querying sensitiv…
- No HTML title found
- HTML body contains low number of …
- Invalid T&C link found
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 5208 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
  - chrome.exe (PID: 6828 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\MJCCDA3Z\?? voice020320231-1_2.htm MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 7004 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2036 --field-trial-handle=1804,i,3897548645690479120,18138799228922854456,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- OUTLOOK.EXE (PID: 6600 cmdline: C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /f "C:\Users\alfredo\Desktop\VM From (937) 669-5620 On Tue March 21 2023.msg MD5: CA3FDE8329DE07C95897DB0D828545CD)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
88868.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

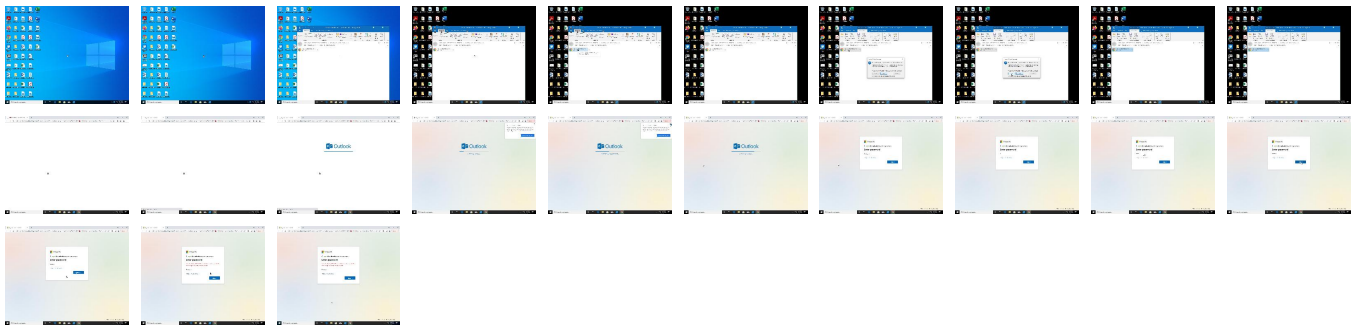
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	3 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 1 Process Injection	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
jsdelivr.map.fastly.net	0%	Virustotal		Browse
part-0017.t-0009.fdv2-t-msedge.net	0%	Virustotal		Browse
tquip.mycustomerconnect.com	1%	Virustotal		Browse
mycustomerconnect.com	2%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

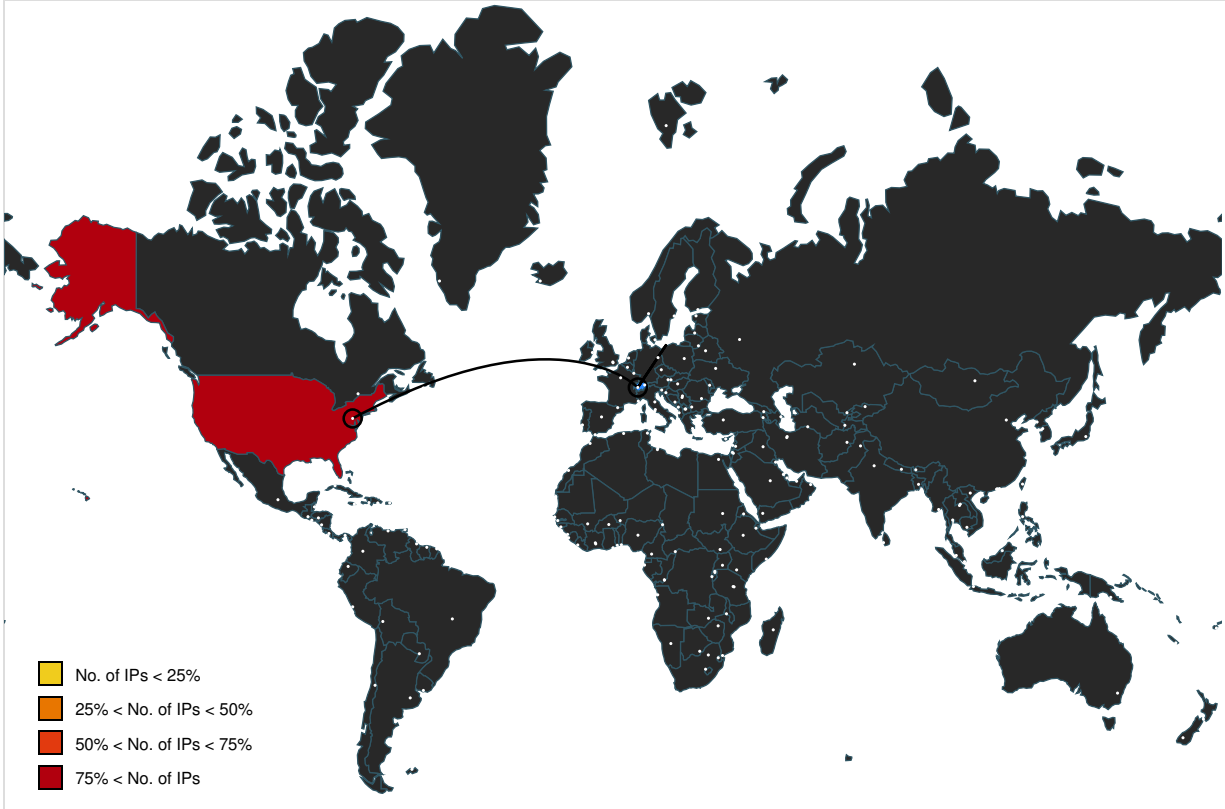
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jsdelivr.map.fastly.net	151.101.1.229	true	false	• 0%, Virustotal, Browse	unknown
tinyurl.com	172.67.1.225	true	false		high
accounts.google.com	216.58.212.141	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
mycustomerconnect.com	54.68.60.236	true	false	• 2%, Virustotal, Browse	unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
www.google.com	172.217.18.4	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.238.45	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.185.174	true	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
tquip.mycustomerconnect.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
cdn.jsdelivr.net	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/alfredo/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/MJCCDA3Z/%E2%98%8E%EF%B8%8F%20voice020320231-1_2.htm#De8I7ldDVcQPzOZv5aKslOaTD0clGWhL05o2MOLPQHbd2USsywLu9tfBJHoJ5HhlZ9R2dyU0k8tbYb9kjimP7E1imnHHNf7S8cvXFGWlJMfMtn3l3LcpsEH2efmezVAKd5bslUT5UjerHfAMDdetvA7e1Y94r9mIP9PLBludJS2pithsfdfO3DT8uQNZkgetImpTEWa8NHUmS39gaLjxZoRKhzkOOX961eOtCiSP44lXySYGW6U5CWwBdbZ7LxNlFIxlci9rKUqkchuvP87nrQx32uT4hmLlOlT1dgFFrYJe=enquiries@healthtranslationsa.org.au	true		low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.170	unknown	United States		15169	GOOGLEUS	false
52.109.88.193	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.227	unknown	United States		15169	GOOGLEUS	false
172.64.169.22	unknown	United States		13335	CLOUDFLARENETUS	false
13.107.238.45	part-0017.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
69.16.175.10	unknown	United States		20446	HIGHWINDS3US	false
142.250.186.132	unknown	United States		15169	GOOGLEUS	false
142.250.184.227	unknown	United States		15169	GOOGLEUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
151.101.1.229	jsdelivr.map.fastly.net	United States		54113	FASTLYUS	false
142.250.185.67	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
54.68.60.236	mycustomerconnect.com	United States		16509	AMAZON-02US	false
172.67.1.225	tinyurl.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.138	unknown	United States		15169	GOOGLEUS	false
142.250.185.174	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.109.8.45	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
216.58.212.141	accounts.google.com	United States		15169	GOOGLEUS	false
104.18.22.52	unknown	United States		13335	CLOUDFLARENETUS	false
52.109.76.141	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831147
Start date and time:	2023-03-21 06:22:21 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	VM From (937) 669-5620 On Tue March 21 2023.msg
Detection:	MAL
Classification:	mal60.phis.winMSG@23/62@12/175
Cookbook Comments:	• Found application associated with file extension: .msg

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, SIHClient.exe
- Excluded IPs from analysis (whitelisted): 52.109.88.193, 142.250.185.227
- Excluded domains from analysis (whitelisted): login.live.com
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

C:\Users\alfredo\AppData\Local\Microsoft\FORMS\FRMDATA64.DAT

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	239628
Entropy (8bit):	4.264170784213018
Encrypted:	false
SSDEEP:	
MD5:	0318082B1BA8FFA6D42416E2734A9EC5
SHA1:	F64406E92488A7643756C7C4A14B07594329C248
SHA-256:	0A82C6A7FE1FAB369BB565016FF597A86CFF224192F01044468BD0A720CA27F4
SHA-512:	F8D1D41B4A014C9E8B3C93DFB6666DF39545F72C250686025A7092F0218CF226491092BD81D31025EE3CC48D629C21BD309626BBD7C6948AB8FB44EED137227
Malicious:	false
Reputation:	low
Preview:	TH02..... ..x.(.[.....SM01(.....(.[.....IPM.Activity.....h.....h/.....O'/.....H..h.....q..B.....h/.....H..h.... .....B.....h....0.....h..... .....hB.....B...py..B.....h/...@.....O.....h....H.....>..w.....0B...T.....%K.....d.....2hB... .....k.....E.\.....!hB..... hB.....O.....#h. ...8.....$hB.....<.....''h.....:.B.....'h.....O'/.....1h....<.....0hiles8.....utoIt3\.../h....l.....B.c....H..h....p.....P.W.B.....-h.....O.....+hB..... ....F7.....FIPM.Activity....Form....Standard....Journal Entry...IPM.Microsoft.FolderDesign.FormsDescription.....F.k.....B...112211002 0000000....Microsoft...This form is used to create journal entries.....kf..... .....&.....(.....(...

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\MJCCDA3Z\?? voice020320231-1_2 (002).htm:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\MJCCDA3Z\?? voice020320231-1_2.htm

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	HTML document, ASCII text, with very long lines (65491), with CRLF line terminators
Category:	dropped
Size (bytes):	298067
Entropy (8bit):	5.278308592195371
Encrypted:	false
SSDEEP:	
MD5:	92DDE27C0253C7588B9350B725BA66ED
SHA1:	1F78B37B169FAEDE5053A08DC181467CE6902911
SHA-256:	3F3036330867FFC0038507C7B2C027943D1199CBC739D390292650E55D14F462
SHA-512:	1A0B004DD97160C58CA2C35AA0EA63019DC45CA4B889FDA007AB6F9F6672C32B89BFDFBFEF61E572B249B4BAB9C18D91222FE8355A44C43B482295A8B17EEE FE

Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en">..<script>..(function(_0x58f06d,_0x566222){function _0x84bde8(_0x144409,_0x504e1d,_0x31c7b1,_0x16b672){return _0x3143(_0x144409- -0x26,_0x504e1d);}function _0x6f39bc(_0x40067a,_0x275db6,_0x4d5a1b,_0x1f8abc){return _0x3143(_0x40067a- -0x82,_0x275db6);}const _0x134c56=_0x58f06d();while(!![]){try{const _0x321ae5=-parseInt(_0x84bde8(0x104b,0xba9,0xf4f,0xb40))/(-0x7*-0x454+-0x1362+-0xae9)+parseInt(_0x84bde8(0x452,0xc56,-0x444,0xa21))/(-0x309*0x1+-0xd46*-0x2+-0x1781)*(-parseInt(_0x84bde8(0x8c6,0x10df,0x2a8,0x61b))/(-0xb34+-0x2479+-0x17d8*-0x2))+-parseInt(_0x84bde8(0x8d0,0xd5b,0x6b2,0x649))/(-0x1*-0x1fb9+-0xb35*0x3+0x2*0xf5)*(parseInt(_0x6f39bc(0x902,0x85b,0x328,0x85))/(0x2fc*-0x2+-0x83*0x19+0x12c8))+parseInt(_0x6f39bc(0xf5e,0xed5,0x1119,0x1230))/(0x1398+-0x1*0x1993+-0x35*-0x1d)+parseInt(_0x84bde8(0x111c,0x12ca,0x1854,0x148e))/(-0x20fa+-0x14c*-0x2+-0x361*-0x9)+parseInt(_0x84bde8(0x28a,0xb01,0xb94,0x825))/(0x297*-0x9+-0x5*0x2c5+0x11*0x230)*(parseInt(_0x84bde8(0

C:\Users\alfredo\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230321T0622590045-6600.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.6438275929252164
Encrypted:	false
SSDEEP:	
MD5:	AAB97592F2F452C55B05E891D4F6C397
SHA1:	D7121B8DCC48A923F2FA767EEE3205923BFD854E
SHA-256:	9D83B8C0AE8B4A5456145141457A11BDD92B113E5E0206632CC87E1929C338C5
SHA-512:	9863175A40EF28E705FCB9A5AF4053DA506010D1598EA6CC31CEAB089ABE858616231597E1309DDB063306A651447062ACE6CFD5D5185704F0EDD20B4B29922
Malicious:	false
Reputation:	low
Preview:	.....n.....q.43.[.....G.....C3.[..Zb..2.....@.t.z.r.e.s...d.l.l.,.-.3.2.2.....@.t.z.r.e.s...d.l.l.,.-.3.2.1.....Fv.....q.43.[.....v.2._.O.U.T.L.O.O.K.:.1.9.c.8.:.4.6.d.1.a.2.8.f.9.0.7.d.4.2.4.c.9.e.7.6.b.b.0.4.1.0.5.0.f.2.f.2...C.:.\.U.s.e.r.s.\.a.l.f.r.e.d.o.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.O.u.t.l.o.o.k. .L.o.g.g.i.n.g.\.O.U.T.L.O.O.K._.1.6._.0._.1.3.9.2.9._.2.0.3.8.6.-.2.0.2.3.0.3.2.1.T.0.6.2.2.5.9.0.0.4.5.-.6.6.0.0...e.t.l.....P.P.....q.43.[.....

C:\Users\alfredo\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	
MD5:	F265DE41A3438656937BE5C5D5533FD0
SHA1:	821DB3674A94901FB5EC364B219CD1988114E406
SHA-256:	18EB4D03AEAF29E2919C8D5382C2184B16ACFE5E4F3A2CEA39E43D8A02C284F1
SHA-512:	7B3485397CFD4F88E2C7A36FB4642A3F9C996127BA36E8C306CB7560B03EE8AE839EE0564FB47A06BCE6DC01CD82BEC5D1479B70054F2186C255C4CE33C5EC F1
Malicious:	false
Reputation:	low
Preview:	..a.l.f.r.e.d.o.....

C:\Users\alfredo\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	43494
Entropy (8bit):	4.546457165631174
Encrypted:	false
SSDEEP:	
MD5:	8E30E83288F6888A24008D4D41CD3653
SHA1:	E40B58B1F0C87992FB9D7897CE5FC8746B3CA742
SHA-256:	7AE971F47890A72BE8597EC8313C4FFA6268AAB3B7BFDAC58CB84381F4E94513
SHA-512:	3FDAED39DCCDF378079122E7283854876A60897E5A1E9A5D832F8C9C1C1F0BC3BAE0234BE4257169D50CF3100CADD0D682E6FA98E5A38AE3D0DDCAF21B40D FCC
Malicious:	false
Reputation:	low

Preview:	.A..LAAAAAAA..nA.AAA6#.A&AAA.#.AAAAA..bAAAAAb.bAAAAA...AAAAA*.A.AAAe..6.AAA.A.AYApA:A.A.A.A.A.AxA.A.A.A.A,A.A.A.AYApA:A.A.A.A6.AAA6!AAA.AtA.ABA[A.A.....h.h.....A...AAAAAAA...AAAAA.5&A&AJA.ALAAAAAAAAAAA.AGA.A.b.A%A.A...6.AqA.^bA...A..bA5..A...A6#tA.!bA.SAA.AbA.S.A.6.AA..A...Ab.&A6.b.!.#A.d.A..A..bAb~.A.n.6.~.A...6!~LA..An~.A..bA.~HA...S.cA.t.A..A.].A,.EA...6..A...6Y.A.*bA..A...AAA.AtA.A.....p.....A...AAAAAAA...AAAAA.5.A.A.A.ALAAAAAAAAAA.6#.tA.ntA...A...6..LA..bA...A...A6#.A...A.#.A...6L#.A.dbA...A.bbAb..A...A...A6!.A*.HA...6e.`A.]bA.w.A..bA.w#A...6~w.A..bA9S.A..tA#ScA.tbA;S.A.*.A8SqA..A.S&A.^bA.SAA.AbA.S.A.6bA...A...AAA.AtA.A.....d..#.R.....+A..LAAAAAAA..nA.AAA6#.A&AAA..bAAAAAb.bAAAAA...AAAAA.A.AJA.A.A.ALA.A.A.A.AbAAA.AtA.A+A.....V.(.m.9*.....AAAAAAA...A&AAA...A.A.A.ALAAAA6AAAAAA.AGA.A.b.A.AMA..A~A(A.?bA...A..bA5..A...A6#tA.!.A.#.A.]bA...A..bA6&.A.1bA.SAA.AbA.S.A.6.AA..A...Ab..A6.b.!.#A.d.A..A..bAf..A

Chrome Cache Entry: 119	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1993)
Category:	downloaded
Size (bytes):	2333
Entropy (8bit):	5.3037723566289285
Encrypted:	false
SSDEEP:	
MD5:	C0AC9C9487D60DE96DC68DBB25BD8DD6
SHA1:	99419B0BE4B85422FF84870E54DBD8A52DC6DAB1
SHA-256:	76AD6584AC5BDD459939DC7532FAE7C2BDD8E22D773FF16D2306F42A1FFC569C
SHA-512:	C62F8DF47104F7B878772DCCA4AEA04D11AB1144E73492BF5E49B9FC92582EB23C7F7ED8A580214F7772506A47602815311D2F3EE3AC3C9B8AA4AADE319BA1D7
Malicious:	false
Reputation:	low
URL:	https://cdn.jsdelivr.net/npm/jquery.session@1.0.0/jquery.session.min.js
Preview:	/**. * Minified by jsDelivr using UglifyJS v3.0.24.. * Original file: /npm/jquery.session@1.0.0/jquery.session.js. * . * Do NOT use SRI with dynamically generated files! More information: https://www.jsdelivr.com/using-sri-with-dynamic-files. */.!function(e){e.session={_id:null,_cookieCache:void 0,_init:function(){window.name||(window.name=Math.random()),this._id=window.name,this._initCache();var e=new RegExp(this._generatePrefix()+"=([^;]+);").exec(document.cookie);if(e&&document.location.protocol!==e[1]){this._clearSession();for(var t in this._cookieCache)try{window.sessionStorage.setItem(t,this._cookieCache[t])}catch(e){}}document.cookie=this._generatePrefix()+"="+document.location.protocol+";path=/;expires="+new Date((new Date).getTime()+12e4).toUTCString()},_generatePrefix:function(){return"__session:"+this._id+":"},_initCache:function(){var e=document.cookie.split(";");this._cookieCache={};for(var t in e){var i=e[t].split("=");new RegExp(this._generatePrefix()+".+").test(i[0])&&i

Chrome Cache Entry: 120	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 78168, version 331.-31196
Category:	downloaded
Size (bytes):	78168
Entropy (8bit):	**7.996980715595138**
Encrypted:	**true**
SSDEEP:	
MD5:	A9FD1225FB2CD32320E2B931DCA01089
SHA1:	44EC5C6A868B4CE62350D9F040ED8E18F7A1D128
SHA-256:	C5DD43F53F3AF822CBF17B1FB75F46192CDBD51724F277ACF6CF0DACB3FD57E7
SHA-512:	58F45066D5738B1EF1F431EB9FC911FC9E6F61F60538F1577CD2EBE651BD8E7B87124DAE36C4E66FB303FD249EBA333BF41D316774201948CAD056BB0E4B4F2E
Malicious:	false
Reputation:	low
URL:	https://ka-f.fontawesome.com/releases/v5.15.4/webfonts/free-fa-solid-900.woff2
Preview:	wOF2.....1X.....0..K.$.....?FFTM...`..N.....h..B.6.$..0..4.. ..+...[.u...m.....6.....f%...N\!7.....w!.....K..~.....DP)..V.u].5a..dQT1..#.bIIL&L=.....z....}4E.8..`..-..8..?....Xk.C..mV..`&...D."...V.c'.).....".../ .AD.4...i..S)e.72..@D ".....~.Jj...~...so7r.....TK...P6..m5.>....1...=x...~.....mD...&.....4/.#[...v.U.,.3.O[aoy.....f|.gKL..d.....e...P.....c.j.....H..../+d..Z....@..._....8.yk.0p.._~..g.C.:{..u.....h..n...l..%..#aD..$@..... .....'..G.89.*n...*._q.~....+]..uvX.r..!~n...7r.7*.9..6..7...`....=..j..~.:.....y..P.[.Q.7.../..../....J..j..B[`KliY.-m,.i..6.eW..^u]W7..qu.r..K.N..O..i9`H..0.!0.6.....d..f.....e.!,..oK....N:..-..X}..."....]..........j2....8.f5/b..n5..V.....d.C.....a.d!.,.../00).{y9V.W!..o.S.<..B>...mhH..%...X.....m~&....&.i.)`rS...."l..d.....l.....B....;2Cb.SD.....F..s.Z.S.Acb-.C.@..vj....=..Si..... .....i}._m..v.L..x..K.j_.v.....]y...WV.B-{}1..E.9.{...9\.. .H..:svr..E_..q....._w...

Chrome Cache Entry: 121	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 1864
Category:	downloaded
Size (bytes):	673
Entropy (8bit):	7.6596900876595075
Encrypted:	false
SSDEEP:	
MD5:	0E176276362B94279A4492511BFCBD98
SHA1:	389FE6B51F62254BB98939896B8C89EBEFFE2A02

SHA-256:	9A2C174AE45CAC057822844211156A5ED293E65C5F69E1D211A7206472C5C80C
SHA-512:	8D61C9E464C8F3C77BF1729E32F92BBB1B426A19907E418862EFE117DBD1F0A26FCC3A6FE1D1B22B836853D43C964F6B6D25E414649767FBEA7FE10D2048D7A1
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	.....U.n.0....}i..P..C..7l/..d.....n...G....yl. .E.....Tu.F.....?$.i.s..s...C..wi$.....r....CT.U.FuS..r.e.~...G.q...*..~M..mu}.0.=..&.~.e.WLX.....X..%p..i.....7+.....?.....WN..%>...$..c..}N....Y4?..x.1.....*.#v...Gal9.!.9.A.u..b..>..".#A2"+...<qc.v....)3...x.p&..K.&..T.r.'....J.T....Q..=..H).X...<.r...KkX.....)5i4.+.h.....5.<..5.^O.eC%V^....Nx.E..;..52..h....C"l./.`..O...f..r..n.h.r]}.G^..D.7..i.].}.G.].....{....oW.....h.4...}~=6u..k...=.X..+z}.4.].....YS5..J.....).....m....w.....~}.C.b_..[.u..9_7.u.u.....y.ss....:_yQ<{..K.V_Z....c.G.N.a...?/..%. .-..K.td....4...5.(.e.`G7..]t?.3..\..... ....G.H...

Chrome Cache Entry: 122	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (48664)
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F22
Malicious:	false
Reputation:	low
URL:	https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

Chrome Cache Entry: 123	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32012)
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
URL:	https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector	(c) JS Foundation and other contributors	jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

Chrome Cache Entry: 124	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false

SSDEEP:	
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD01
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(...................................."P.."""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""

Chrome Cache Entry: 125

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (60130)
Category:	downloaded
Size (bytes):	60312
Entropy (8bit):	4.72859504417617
Encrypted:	false
SSDEEP:	
MD5:	A12EC7EBE75A4D59A5DD6B79E2BA2E16
SHA1:	28F5DCC595EE6D4163481EF64170180502C8629B
SHA-256:	FC5128DFDCDFA0C3A9967A6D2F19399D7BF1AAAE6AD7571B96B03915A1F30DDA
SHA-512:	28B9EA5F3F95807259C2745162424ACEECAC2556BC1AB9A3B33E4E15B54C6970A4DF4A5892FE83C1155C82CA8D93AEBB173BE32F1A7F8B9D3CE038B2DD1E6F FE
Malicious:	false
Reputation:	low
URL:	https://ka-f.fontawesome.com/releases/v5.15.4/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.4 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

Chrome Cache Entry: 127

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1185
Entropy (8bit):	5.488237858804326
Encrypted:	false
SSDEEP:	
MD5:	5BFD7881F8A5D01AE358B73450D830B3
SHA1:	0427DA32A536ACE96DDF03439A14DA012D95E192
SHA-256:	E1D007077DBE23399DA0D65F37C9A14CEA2FA2E1BABB405ACE619EB6B58A2321
SHA-512:	B43C6C8BA46D8ADB72052D8509ADE7BDC129632E51286A3AFC69BF229A8DE759876E3BA6BA2A2163258FF9C9C29537F4903ECC5A3D1C5DEE766FCE7BB0965 67
Malicious:	false
Reputation:	low
URL:	https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap
Preview:	/* vietnamese */.@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v28/tss5ApVBdCYD5Q7hcxTE1ArZ0Zz8oY2KRmwvKhhvLFG6rHmsJCQ.woff2) format('woff2');. unicode-range: U+0102-0103, U+0110-0111, U+0128-0129, U+0168-0169, U+01A0-01A1, U+01AF-01B0, U+1EA0-1EF9, U+20AB;.}./* latin-ext */.@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v28/tss5ApVBdCYD5Q7hcxTE1ArZ0Zz8oY2KRmwvKhhvLFG6rXmsJCQ.woff2) format('woff2');. unicode-range: U+0100-024F, U+0259, U+1E00-1EFF, U+2020, U+20A0-20AB, U+20AD-20CF, U+2113, U+2C60-2C7F, U+A720-A7FF;.}./* latin */.@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v28/tss5ApVBdCYD5Q7hcxTE1ArZ0Zz8oY2KRmwvKhhvLFG6o3ms.woff2) format(

Chrome Cache Entry: 128

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with very long lines (32061)
Category:	downloaded
Size (bytes):	84245
Entropy (8bit):	5.369495907619158
Encrypted:	false
SSDEEP:	
MD5:	E40EC2161FE7993196F23C8A07346306
SHA1:	AFB90752E0A90C24B7F724FACA86C5F3D15D1178
SHA-256:	874706B2B1311A0719B5267F7D1CF803057E367E94AE1FF7BF78C5450D30F5D4
SHA-512:	5F57CC757FFF0E9990A72E78F6373F0A24BCE2EDF3C4559F0B6FEF3CF65EDF932C0F3ECA5A35511EA11EABC0A412F1C7563282EC76F6FA005CC595044171595B
Malicious:	false
Reputation:	low
URL:	https://code.jquery.com/jquery-2.1.1.min.js
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?modul e.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window? window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructo r:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(th is.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,functi

Chrome Cache Entry: 129

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (26500)
Category:	downloaded
Size (bytes):	26682
Entropy (8bit):	4.82962335901065
Encrypted:	false
SSDEEP:	
MD5:	76F34B71FC9FB641507FF6A822CC07F5
SHA1:	73ED2F8F21CD40FB496E61306ACBB5849D4DBFF4
SHA-256:	6DEA47458A4CD7CD7312CC780A53C62E0C8B3CCC8D0B13C1AC0EA6E3DFCECEA8
SHA-512:	6C4002CE78247B50BFA835A098980AF340E4E9F05F7097C1E83301289051CE1282E647ABAB87DB28A32FBFE0263C7318D2444B7D57875873908D6D5ED2AF882F
Malicious:	false
Reputation:	low
URL:	https://ka-f.fontawesome.com/releases/v5.15.4/css/free-v4-shims.min.css?token=585b051251
Preview:	/*! * Font Awesome Free 5.15.4 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 F ree";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{co ntent:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

Chrome Cache Entry: 130

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (19015)
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
URL:	https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof ex ports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&' [object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName? e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.b ody;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BOD Y'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentEleme nt}functio

Chrome Cache Entry: 131	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65447)
Category:	downloaded
Size (bytes):	89501
Entropy (8bit):	5.289893677458563
Encrypted:	false
SSDEEP:	
MD5:	8FB8FEE4FCC3CC86FF6C724154C49C42
SHA1:	B82D238D4E31FDF618BAE8AC11A6C812C03DD0D4
SHA-256:	FF1523FB7389539C84C65ABA19260648793BB4F5E29329D2EE8804BC37A3FE6E
SHA-512:	F3DE1813A4160F9239F4781938645E1589B876759CD50B7936DBD849A35C38FFAED53F6A61DBDD8A1CF43CF4A28AA9FFFBFDDEEC9A3811A1BB4EE6DF58652E31
Malicious:	false
Reputation:	low
URL:	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js
Preview:	/*! jQuery v3.6.0 | (c) OpenJS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType&&"function"!=typeof e.item},x=function(e){return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}funct

Chrome Cache Entry: 132	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (10594)
Category:	downloaded
Size (bytes):	11026
Entropy (8bit):	5.189973145931987
Encrypted:	false
SSDEEP:	
MD5:	B5A82299925AC96A1454732AB97F2BB5
SHA1:	ADD67DDD5F4EDE50DCEA8D89EA55F253F8C42990
SHA-256:	CDDAEF1A49287960674430F7B2F137494671F37CD426B97A718F7957FB3926F4
SHA-512:	2033BBB4B864CE5ADFA8454E2C17A6AF14D625E64702ACD234ED2A24E01DDF50B360B4903F893CB7C8874FAB0BD00A8632EAE5EEC6C48C104969AB2830709EB3
Malicious:	false
Reputation:	low
URL:	https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"v5FontFaceShim":{"enabled":false},"version":"5.15.4"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.

Chrome Cache Entry: 134	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32065)
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C

SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
URL:	https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

Static File Info

General

File type:	CDFV2 Microsoft Outlook Message
Entropy (8bit):	5.415631843565651
TrID:	• Outlook Message (71009/1) 58.92% • Outlook Form Template (41509/1) 34.44% • Generic OLE2 / Multistream Compound File (8008/1) 6.64%
File name:	VM From (937) 669-5620 On Tue March 21 2023.msg
File size:	358400
MD5:	67a7c87d2ee1477eef1fe5fac5f529da
SHA1:	97b8ce82e0ae1bdcb701791831109f6690c6f71d
SHA256:	82c95297d4b36023d21baafda0d3fff1197a60233ffc31348db5d80985f30ef4
SHA512:	92aac18086e5207ab0e01edf635466c9c3487ca6bc57043adf057aa110fbf8deb578ed91a4f58d931323dd52b12e5a535977b17f048a3662dbba0508a5bee8b9
SSDEEP:	6144:OJOJdzjJD2o4A6iL3oD0oW7L7tvJ3vSQ5qmFq/fqhZjV4vhPRnU3U/uli:OJez1D2RA3oWf7tvBqbmFQf+ZjV4vhPd
TLSH:	F074F0887ED67913D01263337A1091F0BFA5FC09D54CC4BAA68EBDD4E06AE62D9C5273
File Content Preview:	.....>.....k...l...m...n...o.....

File Icon

Icon Hash:	00ecb28ec8d28200