ID: 830996
Sample Name: AkimaPAYROLL 2023-03-20.htm
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 23:08:36
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

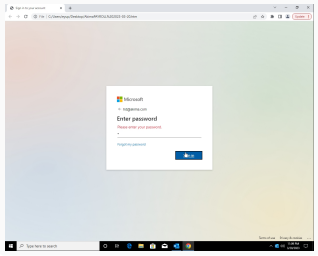
Windows Analysis Report

AkimaPAYROLL 2023-03-20.htm

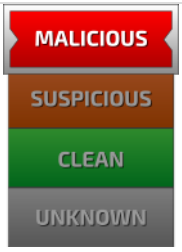
Overview

General Information

Sample Name:	AkimaPAYROLL 2023-03-20.htm
Analysis ID:	830996
MD5:	09ee47c5b227…
SHA1:	e450aa71a310…
SHA256:	99a2d35ba109…



Detection



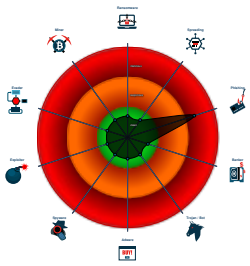
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- Snort IDS alert for network traffic
- HTML document with suspicious title
- HTML document with suspicious na…
- Phishing site detected (based on im…
- Yara signature match
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…
- No HTML title found
- Submit button contains javascript call

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 2892 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 244 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\eyup\Desktop\AkimaPAYROLL 2023-03-20.htm MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6220 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=2056 --field-trial-handle=1804,i,3339978135350707528,1139100625420908023 9,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
76063.0.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x21c:$c8: while(!![]) • 0xc62ba:$c8: while(!![]) • 0xd46b1:$c8: while(!![]) • 0xd4aab:$c8: while(!![]) • 0xd46cf:$d1: parseInt(_0x2fbcfd(0x138))/0x1+-parseInt(_0x2fbcfd(0x135))/0x2+-parseInt(_0x2fbcfd(0x139))/0x3+parseInt(_0x2fbcfd(0x13e))/0x4+-parseInt(_0x2fbcfd(0x13b))/0x5+-parseInt(_0x2fbcfd(0x134))/0x6*(• 0xd46ef:$d1: parseInt(_0x2fbcfd(0x135))/0x2+-parseInt(_0x2fbcfd(0x139))/0x3+parseInt(_0x2fbcfd(0x13e))/0x4+-parseInt(_0x2fbcfd(0x13b))/0x5+-parseInt(_0x2fbcfd(0x134))/0x6*(parseInt(_0x2fbcfd(0x137))/0x7)+ • 0xd4aca:$d1: parseInt(_0x41cb61(0x1be))/0x1*(parseInt(_0x41cb61(0x1d3))/0x2)+parseInt(_0x41cb61(0x1c3))/0x3+parseInt(_0x41cb61(0x1c5))/0x4+parseInt(_0x41cb61(0x1d0))/0x5+parseInt(_0x41cb61(0x1c4))/0x6*(- • 0xd4aea:$d1: parseInt(_0x41cb61(0x1d3))/0x2)+parseInt(_0x41cb61(0x1c3))/0x3+parseInt(_0x41cb61(0x1c5))/0x4+parseInt(_0x41cb61(0x1d0))/0x5+parseInt(_0x41cb61(0x1c4))/0x6*(-parseInt(_0x41cb61(0x1c7))/0x7)+ • 0xd4b0a:$d1: parseInt(_0x41cb61(0x1c3))/0x3+parseInt(_0x41cb61(0x1c5))/0x4+parseInt(_0x41cb61(0x1d0))/0x5+parseInt(_0x41cb61(0x1c4))/0x6*(-parseInt(_0x41cb61(0x1c7))/0x7)+parseInt(_0x41cb61(0x1c1))/0x8*(• 0xd4b29:$d1: parseInt(_0x41cb61(0x1c5))/0x4+parseInt(_0x41cb61(0x1d0))/0x5+parseInt(_0x41cb61(0x1c4))/0x6*(-parseInt(_0x41cb61(0x1c7))/0x7)+parseInt(_0x41cb61(0x1c1))/0x8*(parseInt(_0x41cb61(0x1da))/0x9)+-
76063.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.2.2 - Destination IP: 1.1.1.1

Timestamp:	192.168.2.21.1.1.150628532012811 03/20/23-23:09:46.006535
SID:	2012811
Source Port:	50628
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Networking

Snort IDS alert for network traffic

System Summary

HTML document with suspicious title

HTML document with suspicious name

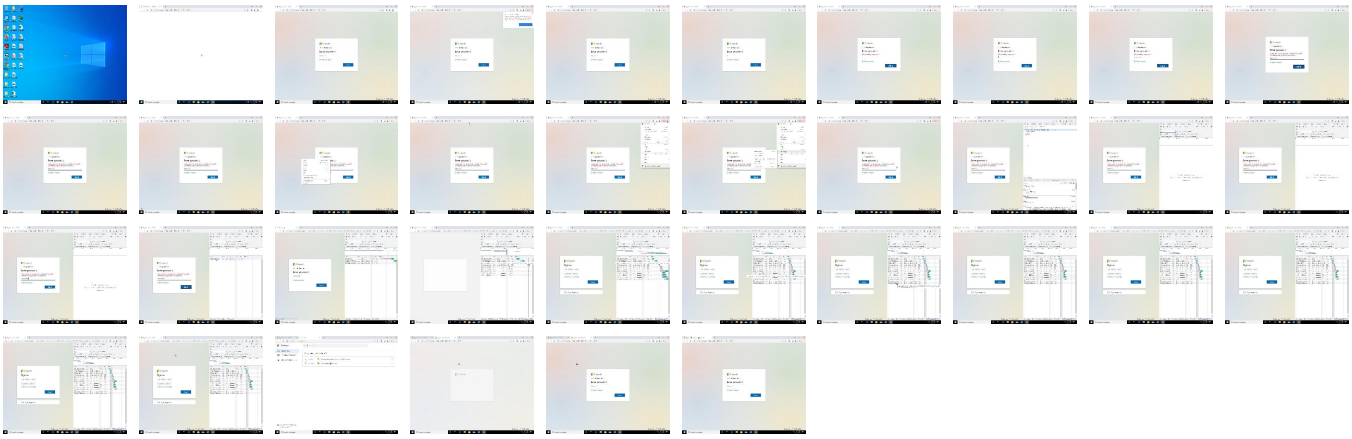
Mitre Att&ck Matrix

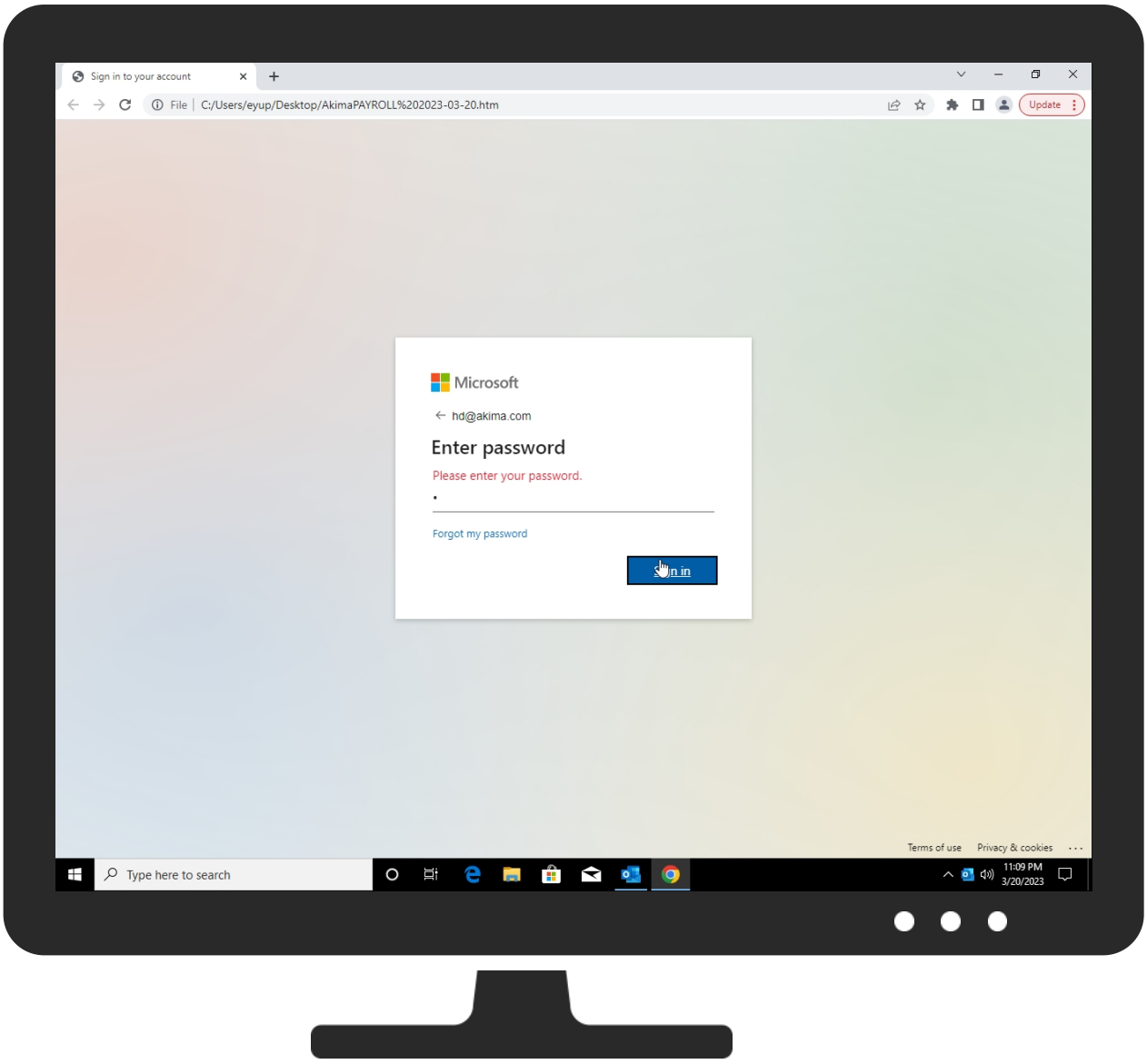
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Information 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 Process Injection	LSASS Memory	Application Window 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 Scripting	Security Account Manager	Query Registry	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)	1 Extra Window Memory Injection	NTDS	System Network Configuration 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
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

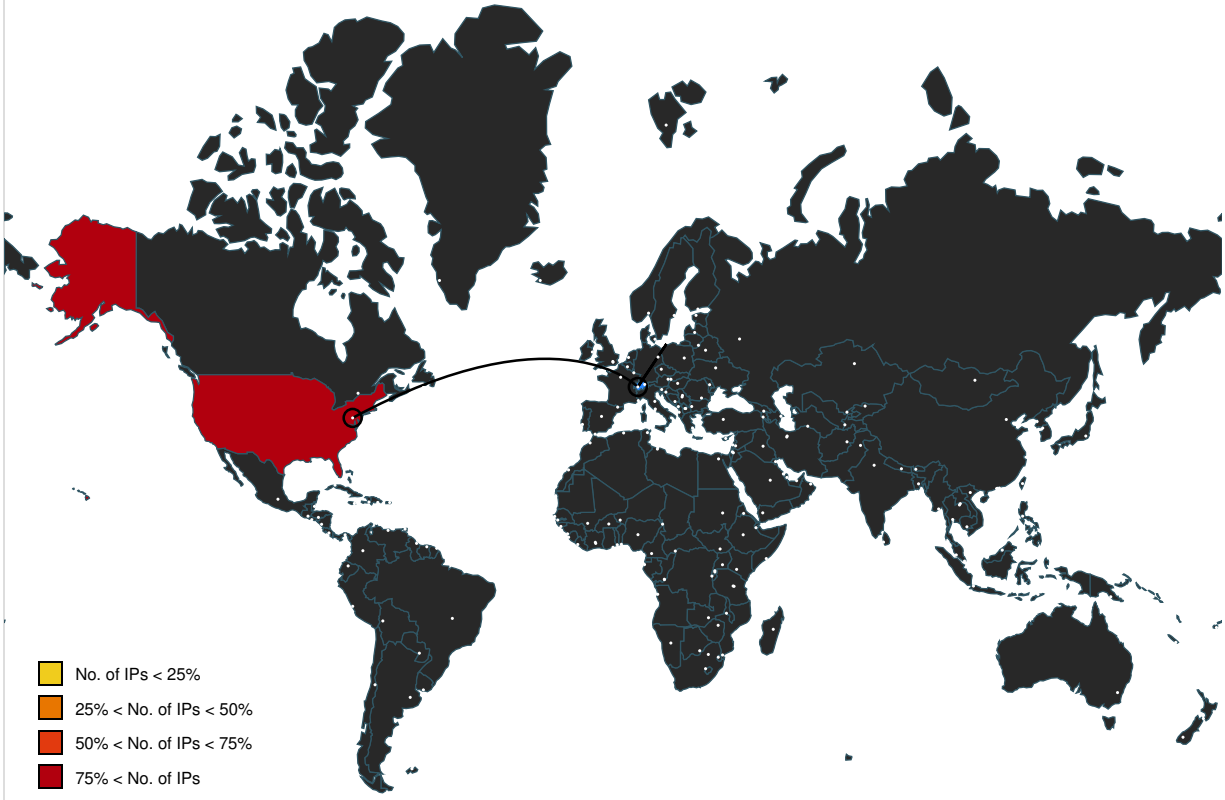
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l0u4.tk	8.39.235.63	true	false		unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.185.141	true	false		high
www.google.com	172.217.18.100	true	false		high
clients.l.google.com	142.250.185.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DyTv8auMLORdlcWeO11-2rveQJRH_dYo9RISyrj0a1sCP5C-YZOFmewUrp_ro-Kr7aBo_hYN_nbj6VXY8rQWMD9NGkN7i4QkVe6mHpNHef8Uvad_iTMMkpEY4xjmLQ8-RA0VMG1rw3ZXloOzjsCfEww&response_mode=form_post&nonce=638149470490347218.YTQ1NWI5MzQtNGYyMy00MmFhLWI5ODMtZTQ2MTkyMjI0NzAyYmRiNzFmZTgtODdlZi00NmFiLWI1OTItNWFlYzg1YTM0MDBk&redirect_uri=https%3A%2F%2Fportal.office.com%2Flanding&ui_locales=en-US&mkt=en-US&client-request-id=a8e8bdec-70fe-4013-911c-97f82fdc6d64&x-client-SKU=ID_NET472&x-client-ver=6.16.0.0	false		high
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DyTv8auMLORdlcWeO11-2rveQJRH_dYo9RISyrj0a1sCP5C-YZOFmewUrp_ro-Kr7aBo_hYN_nbj6VXY8rQWMD9NGkN7i4QkVe6mHpNHef8Uvad_iTMMkpEY4xjmLQ8-RA0VMG1rw3ZXloOzjsCfEww&response_mode=form_post&nonce=638149470490347218.YTQ1NWI5MzQtNGYyMy00MmFhLWI5ODMtZTQ2MTkyMjI0NzAyYmRiNzFmZTgtODdlZi00NmFiLWI1OTItNWFlYzg1YTM0MDBk&redirect_uri=https%3A%2F%2Fportal.office.com%2Flanding&ui_locales=en-US&mkt=en-US&client-request-id=a8e8bdec-70fe-4013-911c-97f82fdc6d64&x-client-SKU=ID_NET472&x-client-ver=6.16.0.0&sso_reload=true	false		high
file:///C:/Users/eyup/Desktop/AkimaPAYROLL%202023-03-20.htm	true		low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.195	unknown	United States		15169	GOOGLEUS	false
13.107.6.156	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.67	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
20.224.254.73	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.190.159.73	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.110	clients.l.google.com	United States		15169	GOOGLEUS	false
52.109.88.191	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.202	unknown	United States		15169	GOOGLEUS	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
20.190.160.14	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.19.126.200	unknown	European Union		16625	AKAMAI-ASUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.141	accounts.google.com	United States		15169	GOOGLEUS	false
13.107.237.45	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
142.250.184.228	unknown	United States		15169	GOOGLEUS	false
8.39.235.63	l0u4.tk	United States		397423	TIER-NETUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830996
Start date and time:	2023-03-20 23:08:36 +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:	9
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:	AkimaPAYROLL 2023-03-20.htm
Detection:	MAL
Classification:	mal68.phis.winHTM@31/44@7/176
Cookbook Comments:	• Found application associated with file extension: .htm

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.184.195, 69.16.175.42, 69.16.175.10, 34.104.35.123
- Excluded domains from analysis (whitelisted): login.live.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: l0u4.tk

Created / dropped Files

C:\Users\eyup\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):	576
Entropy (8bit):	5.051544237902749
Encrypted:	false
SSDEEP:	
MD5:	6BD63A3846959F3C0CB44819E57D0DCA
SHA1:	AF7B8AFDA9946DA28E1095E70D72479FDE9E467B
SHA-256:	2CF08F8D294FEEE880AD49AE3CFC391FB6B3437F49E6221C17F85C8B9CE2199B
SHA-512:	16EA17B9FF89F50270C758F6B5756FBA7BE467FE12E1F5BB6C9B5207937EE37C8D1103C4578FD43FCA32D9889F8CCCA3F550FD2D58D9EDFC8F9101B4877EEBD
Malicious:	false
Reputation:	low
Preview:	.6...AAAAAAA...AAAAA...A.A.A/ALAAAAAAAAAAAAbA5AtA.!.AGA.A.bbA.A`A.].A%A.A...A AHA...AVA.A.n.AKA.A6d.A.A.A6.A~AEA...6.A.A..Ab.A...A...A...An.LA..bA...A. .bA..#A..bA5..A...6#.qA.^tA..&A.5.6..A..bA..A...6`.~A.G.6N..A..bA2..A...A6#.A.-.A.#.A...A.#cA...6*#.A.*bA..A...An..A...A..A..bA..A. bA..A.tbA.SAA.AbA.S.A.6.AF..A.L.A`..A. ..AN.A...A..(A.}.A...A.1.A...A..A...A...AV..A..AQ.yA._.AE.MA...A|.A...AU..A...6...A...6...A.?.6...A.H.A..A.9bAK.XA...A...A...A..DA..A...A.%bAZ.A.;b.q..A.#b...7A...Aw..A68 .AAA.AtA.6.....

Chrome Cache Entry: 136

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	40
Entropy (8bit):	4.384183719779188
Encrypted:	false
SSDEEP:	
MD5:	FB5091BD594CF7D209A7FAC6528A0344
SHA1:	8C4F8863DA36CA8E3F0467D6C4E167987741E812
SHA-256:	0AD7D750945C04134391827A3777A2DC6B0CAEAF906D3B46FFD3E85C54F24ED0
SHA-512:	C5A5FCD38E68B1DD7C68070BAAA07EB9FEA896D404CF05C26EF5FEE769584F45908354BAFE0E779E57C8298BE858B1018BEF618B16A6C6355F9585A7921A4055
Malicious:	false
Reputation:	low
URL:	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTA0LjAuNTExMi4xMDISFwmCAmly1gHbXRIFDdFbUVISBQ1Xevf9?alt=proto
Preview:	ChwKDQ3RW1FSGgQIVhgCIAEKCw1Xevf9GgQISxgC

Chrome Cache Entry: 137

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (2345), with CRLF line terminators
Category:	downloaded
Size (bytes):	2347
Entropy (8bit):	5.290031538794594
Encrypted:	false
SSDEEP:	
MD5:	E86EF8B6111E5FB1D1665BCDC90888C9
SHA1:	994BF7651CB967CD9053056AF2D69ACB74DB7F29
SHA-256:	3410242720DE50B090D07A23AEE2DAD879B31D36F2615732962EC4CFA8A9D458

SHA-512:	2486B491681EE91A9CD1ECC9AA011A3FB34B48358C5D7A4D503A5357BC5CE4CA22999F918D40AC60A3063940D5F326FC7E4E5713D89D5C102DE68824E371B3B
Malicious:	false
Reputation:	low
URL:	https://login.live.com/Me.htm?v=3
Preview:	<script type="text/javascript">!function(n,t){for(var e in t)n[e]=t[e]}(this,function(n){function t(i){if(e[i])return e[i].exports;var s=e[i]={exports:{},id:i,loaded:!1};return n[i].call(s.exports,s,s.exports,t),s.loaded=!0,s.exports}var e={};return t.m=n,t.c=e,t.p="",t(0)}([function(n,t){function e(n){for(var t=g[c],e=0,i=t.length;e<i;++e)if(t[e]===n)return!0;return!1}function i(n){if(!n)return null;for(var t=n+"=",e=document.cookie.split(";"),i=0,s=e.length;i<s;i++){var o=e[i].replace(/^\s*(\w+)\s*=\s*/,"$1=").replace(/(\s+$)/,"");if(0===o.indexOf(t))return o.substring(t.length)}return null}function s(n,t,e){if(n)for(var i=n.split(":"),s=null,o=0,a=i.length;o<a;++o){var l=null,c=i[o].split("$");if(0===o&&(s=parseInt(c.shift()),!s))return;var p=c.length;if(p>=1){var f=r(s,c[0]);if(!f||e[f])continue;l={signInName:f,idp:"msa",isSignedIn:!0}}if(p>=3&&(l.firstName=r(s,c[1]),l.lastName=r(s,c[2])),p>=4){var g=c[3],m=g.split("|");l.otherHashedAliases=m}if(p>=5){var h=parseInt(c[4],16);h&&(l.

Chrome Cache Entry: 139

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 3651
Category:	downloaded
Size (bytes):	1435
Entropy (8bit):	7.8613342322590265
Encrypted:	false
SSDEEP:	
MD5:	9F368BC4580FED907775F31C6B26D6CF
SHA1:	E393A40B3E337F43057EEE3DE189F197AB056451
SHA-256:	7ECBBA946C099539C3D9C03F4B6804958900E5B90D48336EEA7E5A2ED050FA36
SHA-512:	0023B04D1EEC26719363AED57C95C1A91244C5AFF0BB53091938798FB16E230680E1F972D166B633C1D2B314B34FE0B9D7C18442410DB7DD6024E279AAFD61B
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	.....WMo.7..+..uV.HJ...{.....&..v...(Q.F.....aW.Q.|..~.|{~...b{8...zv.....8|...b.gxb.y{.x<\lS...p...p..l7...o.}.v.....t.....r..r.|9?.....HP...r.4.aGA.j....7.!....K.n.B.Z.C.]....kj..A..p...xl...b..l!K..><.B..O....#...$.]h.bU.;.Y...).r.u....g*.-w.2..vPh....q....4_..N\..@y).t{.2pj.f..4h.....NC.....x.R..P..9.....".4.`%N..&...a.@.....fS)A4.F..8e9KHE....8d.CR.K..g..Q.....a....f.....dg*N.N.k..#w.....,,".%..I.q.Y.R]..7.!.:.Ux...T.ql..{..,b..2..B...Bh...[o..[4....dZ.z.!.l....E.9$..Y.'...M.,p..$..8Ns3.B.....{.....H..Se3....%.Ly...VP{.Bh.D.+....p..(..`....t....U.e....2.....j...%..0.f<...q...B.k..N....03...8....l.....bS...vh..8..Q..LWXW..C.....3..Pr.V.l...^=VX\,d9f.Y;1!w.d,.qvs....f*;.....Zhrr.,.U....6.Y....+Zd.*R...but...".....4.L...z.....L.Q.....).....,].Y.&....*ZsIVG.^...#...e..r....Z..F..c..... .QDCmV..1.~...J9..b_Oov\..X.R..._.TqH.q.5G.0{ZphQ..k...s..\.../.Dp..d`#.....8.#Y...Mb.j.Q.....=n4.c....p.[.SI.....0.N.

Chrome Cache Entry: 141

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 113577
Category:	downloaded
Size (bytes):	35823
Entropy (8bit):	**7.993294075345085**
Encrypted:	**true**
SSDEEP:	
MD5:	957CCAAEC3BBDC8FD4129E2412EDE20C
SHA1:	2528E3E157B4C37E4F4979878822B523AAD7ABD9
SHA-256:	BE496ADE64AD854B0B379A96D5FB7CD96BF7167230021128CB97CCF150197B35
SHA-512:	CBE73F576CBA4D2C55D90A15E53C2F00A8CE21035E54CD05547F0EBAFA5EA88CAB354C90ED6731552A75A1FD36D9CD3A0DC818906FDD91A403E475DA38ED5A31
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pstringcustomizationhelper_c0f2645501c8b52bd96c.js
Preview:	.....{..8.(.....f...,.-.....N6.....$.)R&)?.{?..*.I.l.=....L.D.P(..B.P....._[?l.}.....O...z{.....g[. ..._.~|sz..t.R...".fQ...$..t+M..l+J.4[.YP.|k..,..Y.....Ze...,..8..(4aqz.U.r.t.]...[o.9...Z4..(...{x_.[IZD!...)Q.!..lk.LY.u.....Q..y:+.2....*.....p...m...Y..|4.> ...S5.....h..g.PxB...Y\...X&M....."...<l...}.....D.|.....kr..t.....9.n..8.J.=."a.....[.B..o. A....y..%...cTtr..-W.....by..V,.%.Q..r.lm...I..{.Uo5..^.....(.U~..?...z.....4].. ...+h.t.o.....{....eu..n=.....e.%..w...X..'..../.....q....wv...._..(..h.e.U.^..$..7...Fc..Z..h.n.....`.NBlV....9_o.l+.z.qs?Y..a..~s....e|..q.\E.{|.d,.....nq.J..W.g.|t...d..8.H5...y^..Y.fn.....7.4M....l.c?....!.,....5...p.o!..q.Rc..(.7./iq...:.M..{v..26}u_.. c.:Kj....C.....<...D...=[..;c70j/@{|..B...b.4...&....l.Hn.|.(..d.S6).4/..[D.....(.+.O..U...oi.h.Oc|.........65.Z"...)*1Px6.3.B .[P....^.bV.....gHs.J..4.'.|.....-*..Z.Z.W.....|....7.U.....O+1....c.>.$.'..+.Z'.....f....%Tc.o...M.P.+....r.~..g+..

Chrome Cache Entry: 142

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	

MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 7F
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12 l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141- .071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594- .595-.071-.07Z" fill="#404040"/></svg>

Chrome Cache Entry: 143

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 347498
Category:	downloaded
Size (bytes):	95939
Entropy (8bit):	**7.9969515592420315**
Encrypted:	**true**
SSDEEP:	
MD5:	81B1118B15E614E071B2C34D06920874
SHA1:	FBE82CFE4F9BDEA8DDBC5B31110DF7A8963F6F5A
SHA-256:	86CD5F262B23015F9C849E725F408ACF89D4606FC1F52C48AD61D71C8CBD5BFA
SHA-512:	B224CF9ECC8E33A729586D24326DC90F64516394B899BC0F20891D191195305179CC484FD9C779BDDF20DF7B173B23E97F02F3D2BD7B2035C5200E8D3D2B237
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/c0f2645501c8b52bd96c.map
Preview:	.....iW....._.S..{..~.....m....2..<.....x"..m..]u.9ow.6%K9FF.....u{..M.?.....b..7.....h.M....e2..../2j2og*.yo.Q..r2.m.K].=.....q..#?2..Gf<i._G..j.^dF...5.....23.e...h2.....w.Y5.. .O2....{.])3ow.?..\..../'../..=^..zR..Tk5.fz.... ..t>.I.f.....i....V .]..... b..7.....Bo.A{.OV.._k.=.v.....oc..h~....._.~.V...{..G....6....F.....m.....e...6.1L^5..^...../..j/..1..&..?..m....Q~....9....Z ..4n.{....p.....@..Rc.....=.6..f...|.4.....d.....1.....f2....n&...&....y._k.....D=....q.o...5a...c.....d|.FK.).m-.r{z.6:.../H.h....D(..".".....W..^4.....L...-...z.F..M..ZN.....e.c../H... .....N....[d."Z.....SH~...U.}x.$..4H..d..<].?IX...*.o...g.V.....#.7o/...>.....*..=...v.!..?l....n.....7F...X..u..T.Nn..._....=._hG..dU.....P...t.<...m..[,..|>.7_...7=..p....z..1t...bQ.....(u.6=+=5 ..L..^..-.`Q.,..~;...-..C{....-.s.]].%.....C{...\{.k.....O...S.! 0....W.Q.Y-.D.0.|.....O...Y.&z.~.Q.+j.tGq)]FMF.DzI...c...].

Chrome Cache Entry: 144

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:	dropped
Size (bytes):	673
Entropy (8bit):	7.6596900876595075
Encrypted:	false
SSDEEP:	
MD5:	0E176276362B94279A4492511BFCBD98
SHA1:	389FE6B51F62254BB98939896B8C89EBEFFE2A02
SHA-256:	9A2C174AE45CAC057822844211156A5ED293E65C5F69E1D211A7206472C5C80C
SHA-512:	8D61C9E464C8F3C77BF1729E32F92BBB1B426A19907E418862EFE117DBD1F0A26FCC3A6FE1D1B22B836853D43C964F6B6D25E414649767FBEA7FE10D2048D7A 1
Malicious:	false
Reputation:	low
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"I./ .`..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: 145

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 47818
Category:	downloaded
Size (bytes):	13919
Entropy (8bit):	7.98572491076564
Encrypted:	false
SSDEEP:	
MD5:	1631C39AF69D99BFD1AEA7ACB8FBC4FA

SHA1:	7613A14FD31A598E3E2365BC8E529DAAC6FD7A4C
SHA-256:	E7DCAF045B59E7C04E1DF2459273E735FAF28E4F6F6FF7741691CE1ACB857DD5
SHA-512:	EC50A403214158576588C5A3EA395F3D80F41797D59517BE27B05FE680417E5109FCFE04A0983DB0E8D2D4E5114753DCB8CF7C43C429B1CDC35A25E6E7A4C15
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_cfi3giy70wfemn6mr5vbma2.js
Preview:	.....}.r#G..._Q.qL7..!<.D.j....m...`S.IF...Y.@.\Uh6..cv^x...+/...r#.....@J..{=1.".q....'.~7_{.....Q.m....Gw..... ..:.,..(... ..~v.+.cQ.Q....lwV.....[.U`..X....;.....+..O8.[.....l.8.. ..^(.....i....+...Ww_..>.....?...S...(p.....ufv.....Lx...".oV.W...F"...`*^..((..D.Q.....}.4.|....X|..f .HX.u.N.?...L.....'.w.....BsL.....}&I@.BW8@..@.[.....-.i...;..8].X..%..z. M.n..u..v.;.K.^.;...u=1..@.....XL.....W.V.z..p@.....0.^(.....*WK.j.....~S.....j..o...2..C..8.\....(.9K.wf/.8?.b~:..$.4.w...>0.....Xz.d.....J.[.&*..`.D...n.L...7..~.$B.%.i.....`u}. ..P.{....a{_.+.Y...N..X..%,;.....g..{.m=...u+,.C.up1..W...^p...oa}.....@.9V@.X3.....+...Y.Fb..[.....UdE..p..B.S.3.wC.....P .s\..G...|~.....rf.@.a....\....`.$4c7d..H..a..,i .K..&..O.g.[.....).....8.....I*t..... .Tlk...e..+.....-.....e..v.)...zz/..H.!4.-..lc.;.suF..qM.....@.uhO..L....'.lj.v.....y..

Chrome Cache Entry: 146	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 148	
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 854156
Category:	downloaded
Size (bytes):	246985
Entropy (8bit):	**7.992684851782322**
Encrypted:	**true**
SSDEEP:	
MD5:	ECC18A7CA743FF778D8DD9C83ABD20B0
SHA1:	AD1FC250E4DDD0EFCADC6D1A30B8A0CDB61B3F1C
SHA-256:	7978A2A6F9372E8373723DC281A2684B463F09278F22D6D561A4D9F9D83C67C1
SHA-512:	2358C8A8DE05AEDF113D5843CC5E60D103DEBF5B0961F2D8D12341F0726CCA2C30BBC104E079410D9B7B82DA3A5708B2D4395725163D1D0DC9546F01CD154C F
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/aeb718e8cbcfba8bf6ed.map
Preview:	.....kS"K.-._:.7{.TTt.OUE.% " .../y.K.z...9....^.....UY..9s.3..|.....l..?..-g.E.....m.=ou^.#.J...h..f.^*X/W...2%..V.....%5.mS.Y..<.u...2.....Z....)>.-W...e....@?.....e...p.. ...V.....b.]...hj8..v..yk....wf.lo....._....OW....p...5.\..|7....[,f.....?..|13.m..}..>..Z....oMe{...[.>.9.7y...?y...3..Z..(..k.....6..Plk.h.....\v1.}Uv.....S.=.....1..m...z.....\bB...'...*0..^... ...%c..r=.G..=.....Eg...y[.:;...B./..2.hJ..b.....5.v....>.>l..?...x..ko:.....|..m....wy.[.7.....k...{..|:.?..>.....R.I.?.m=.b....o..Z.....Z;.'0.j.....Q..=I.gb.](.uo<7..}5.....q.....nn...3 .kM..y5.._..l.kT.lk.2o{/.s[_..<6.b.R.....l|^.V..`....O..y....r\..;..z.....F..2 ..=^....J.7....k...A..,..&...{K.x....l;..7[..r.....].a.....zi...E.....nM.c...1m...G..`..k7..-....c@.1.9..C..Y[...2{0..... ...[cC.....a;a..t+&8%...2..7.....s.n1...6+.q33..dk....Oi..r H.2u..^0...2.1../SM.f/.. ..Y.lW..[..n.W.,z.v(.d.u'..8Nnq..N.S...<..

Chrome Cache Entry: 149	
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 110674
Category:	downloaded
Size (bytes):	19995
Entropy (8bit):	7.9805569589072585
Encrypted:	false

SSDEEP:	
MD5:	E7CA24DC3A47160C9AF0D45E48F1F911
SHA1:	C689E79B895A18C9F1334D6EFF56744AE22739B6
SHA-256:	ABB85C399C274734C689156024267ECE39C2B96D82C752065C9A649A8ABB4C42
SHA-512:	1B6C6E386B8AE1202E7699B2A56C7573EF44661C7C4977B0A9E261C576066EC3C536EA94C7A4CBB5D70EBEF2405AD71AA1E3A10C2A9340C69831DB53E2FCCA BD
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_dxlgfz8kx1amwm8vpguk7w2.css
Preview:	...........}ks.6.....\.R;.J.H=-WR;..&>g^53.G.R[.DY<C..$e.WG.....)...{+'g...l.....bw_f7.:x..<x.-.*V5)/wE..Y...gy.0.*(.*-o.e.|...._..l.....?<{.!x...W..._..^..p..E..'..Y...<.....*]..6(. ..D..*...Y.....:.ve.?..!..|t...].+.....a.....|.P...u.H.d.d.r.c[..~.L..n.-.}e.H3...r..^..iP.u.*.z.....)..Z.jx..C'.....u..{.C...N.o.m~..F(b..f.....h..O.....6....kr.....n2m M$.R..R..i{.~...*..n. dKY..#.Kn.4..G...O..I.#.a=..iU..].S.2.wY..O.|...Z.A....].uU.._%U.<...pp..u=.....C.R..S.....0...A<.....&...W..'o.T..".jO..^+.....DiW.b..7i..7.....IKe.0.~B0.....zQu#...YB.,.{* .&.6..G.6..._...J.i.?.LS$(.^.{..u.-.0....K....M&j..s.yB..+....^.)...7e.....]..eFI_.kRX.B.....D[.4.....+.u=>....R.`QEK...R..d...*S.. ,c5RKBK(.....][..eF{T.....6..."....Uk:..S.0Ro.}B.dwJZ }U..S.F.....&.&.~\|.....{..Ep.>x..._....}p..=.}...v...7?}...g..1&.....}...^...o.x.>x...../.^...._.....w.v./.....BA...{J..w..$?.}w....?zO.r..5...7.gl..z...g.?.{....R.....yGj

Chrome Cache Entry: 151	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

Chrome Cache Entry: 152	
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 1266361
Category:	downloaded
Size (bytes):	294170
Entropy (8bit):	**7.9985945743163205**
Encrypted:	**true**
SSDEEP:	
MD5:	39588FAC6FCE9FFFEB7900439B502D7A
SHA1:	5145EFD9526ED189262ED1CF0A486CAA267BAD0F
SHA-256:	4FBD69CC175D26C02CB774BEF0EED18C377F9ECEC11398FB5FDC47EDFE82FEDE
SHA-512:	819936DE3104C498AADDD53E08F4D6D9BFD80A59116B158F9EABF7EAA933D64E19172BBBCD9AEC58DBF584A7105E8F93BA9EDFF41B273F7B4E5652EF603A2 CE5
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/4b54de7a650872dc9ebb.map
Preview:	.....v.. .+gq.C.T..m...O HJ.D.&)...X....H..@]..... E.g.i..).=322222"..t..L...g.t.lW.....?_.z%...*.".;....|..|.gE.?iYEiU..[./O.....U.m.d.L..}..n ....j.N..._...r ..m.,.....s ..l.....Le r...m..e4...q.-.=..Vl:...u...M.]...<lW.....4~|.B_.m..m.....7....9..<...wq...$.,...U\twU.....).....C0.F.|.9=..q3E.F.\z.2...Ev....._.....|..P...D.....S...b_..x.o.x.D.*+..t.<.Fi<K.....=]..7. U../...F.mf.....U.thI2..0{8#..L..|.M.EVf.*.d.,|\'U..<]...|8.....v.^\E..Hd6d.a.3.K..`*Z....t.wbMK.....~^.....o.y..6Pj.xt.=.$8../R...<...E.....m.....&.+....h.,.*.....#l_.6.]t.:. .:...% /.5+x.c..Ws..3..K.....U._2/W.K....?J...L..4Rx.i.F.5.....>l.....h[...p.b..Xh...Q.x...m.bV. ....J....R.Q7J...m iu....d*..4.V..|j9..E67...Jl...9...u.R2.....t..'.=.oZ..... .Wl...E..... ..'10u.~~.vP.p|i...,%X..n*..fi..wp.{.....?.m..F.}...>2..j}}d.7'....|....?.d...p..8>....8!....}J.O..)}?;.....=...'.}wr..N.....8!.'....y.:.....2...8!

Chrome Cache Entry: 155	
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 1592
Category:	dropped
Size (bytes):	621

Entropy (8bit):	7.673946009263606
Encrypted:	false
SSDEEP:	
MD5:	4761405717E938D7E7400BB15715DB1E
SHA1:	76FED7C229D353A27DB3257F5927C1EAF0AB8DE9
SHA-256:	F7ED91A1DAB5BB2802A7A3B3890DF4777588CCBE04903260FBA83E6E64C90DDF
SHA-512:	E8DAC6F81EB4EBA2722E9F34DAF9B99548E5C40CCA93791FBEDA3DEBD8D6E401975FC1A75986C0E7262AFA1B9D1475E1008A89B92C8A7BEC84D8A917F221B4A2
Malicious:	false
Reputation:	low
Preview:	..........}UMo"1..+.....G; .8l...M..$.U.AW......UaX..`'.=......\|..z3...Ms>..Y...QB..W..y..6.......?..........L.W=m....=..w.)...nw...a.z......#.y.j...m...P...#...6....6.u.u...OF.V..07b..\...s .f..U..N..B...>.d.-z..x.2..Lr.Rr)....JF.z.;Lh.....q.2.A....[.&".S..:......]........#k.U#57V..k5.tdM.j.9.FMQ2..H:.~op..H.......hQ.#...r[.T.$.@........j.xc.x0..I.B:#{iP1.e'..S4.:...mN.4)<W.A.) .g.+..PZ&.$.#.6v.+.!...x*...}.._...d...#.Cb..(..^k..h!..7.dx.WHB......(.6g.7.Wwt.I<.......o.;.....Oi$}f.6.....:P..!<5.(.p.e.%et.)w8LA.l9r..n.....?.F.DrK...H....0F...{.,........{E.."....*...x.@..? u......../....8...

Chrome Cache Entry: 157

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 412391
Category:	downloaded
Size (bytes):	114301
Entropy (8bit):	**7.99779365786384**
Encrypted:	**true**
SSDEEP:	
MD5:	BB47875EB7ACF3BCA0526431119B35B2
SHA1:	8412901F917EAA99887A439E2AFE3B0FAD4F4BC8
SHA-256:	0C452C04F71F1AC96C5BACEB10E9E6A60FBFD5B97E18C5CCFB40D7F6661A9BC7
SHA-512:	1D97554D694B261CB2F01AFADB81556373B9BF0510E3450DF6BE513B250D8F52BA4220F079821DBAB3F78B06D51A824C351554A7FA449A4E429CD299690E9D84
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/ConvergedLogin_PCore_EH-q9hPYkBqq2xSfT_DcJw2.js
Preview:	...........{W.H.8....F3......,Z...U..Lc..Y...R...W.y.....L)%.T...{.....WdddDdd.o._..Wv.......u]..V.....+.......z88..z.Q..../.L=.U...3....0.x..F.0...W..o..~e..O..U.Q.'s...{q..&.._*U..r+.v..U. .z..gP.7..(..7...T.0..V...j..#.Ye..,..<x.C..s.0..I%b...x...&....J..4....Ze......-......\.pJ...0@/....0h,...[M.DZ..7.J.V...}6./.U.oO1...Yu..w.$..0c.=c.}...xT!d....{..@.Uf.. .es0q.,b.....cTt.V ......Qaq......._...$.T*..a...W..z..[....:.zH.yl~.4...O..p1.....<...O.9.].....g.Wf.r1..T..'..d[.*..9._J..................ik....X..K...T.......7<#.......?.;#..c....?.5..... ...=+.....WM.f?...9.=...%.....S.....o o.....S./.*~@+..?...v ..D.wU...TYe......jp..]..#{.;....&U.........e.i.W.).BD.7.z.....d....].:....Pi....g..on5..i.W..Q.a!.c"......u..z..:..P.=......X.(.........N1.F....@...<D....R...(..i........I.F< .. T...`1.W3...L..Q.....f.\............Z.a..%R?.>e..3....=..o..H..*....w/...G.*........t.0%+.$.Ta.3u#R..y...t....G....z.O?g,9..Go....~bU..4..2.(..%'<B....

Chrome Cache Entry: 158

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:	dropped
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD01
Malicious:	false
Reputation:	low
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(..................................."P..."""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""" """"""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""" """""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""

Chrome Cache Entry: 159

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32030)
Category:	downloaded
Size (bytes):	86709

Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067 65
Malicious:	false
Reputation:	low
URL:	https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?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.toSt ring,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="3.1.1",r=function(a,b) {return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r, length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

Chrome Cache Entry: 160

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 109863
Category:	downloaded
Size (bytes):	32195
Entropy (8bit):	**7.993880801346853**
Encrypted:	**true**
SSDEEP:	
MD5:	039CD406CB780BD9DAE8410D38CE69CB
SHA1:	5DEFD37654F47F6DF5E104D3A34BCB3C1E307A1D
SHA-256:	16C6585A09A7E87B4CB30718E8BDA247C78FFBE590A8043FFE8ECC486270D2D4
SHA-512:	DC2A2B2FE9B02E35537902F65869D35D051F0F720B9BB4D4726D5EDE15B6611D4F12389242350515023C032CA98FD1ED406A694FFD894DFAB7B059F06BFCA84
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pcustomizationloader_aeb718e8cbcfba8bf6ed.js
Preview:	.....z.H.(.....V....H.b.$.]...l...s..,....P..6..."..7"..$)......"...DFFFD....._...o.^..z.....z.O.m.|....g.o.;...].Ek.'.../..-ZY...V..|..Q..5...Q.Z..u..b.U....e.J...X.}ny.\.h....._.)|=.V7.. .I.Y..Y+J..Z..i.ZU.`y..U<.j.....e+gs...N.....V..V...2..+>.^.-.....0.O...\.D._.`...W.L.....g.B5....*..MV.....e..v]P?X...I,..y..Y....1IZ.T.[.....b_VP.HnZ.y.".ew.p.e..5K.....V|.....+.I.b..- 5.9.XO.A..{.....E....'..q.?.....\.....z...`.U.IT....ar...|..e.....j.z]]..Z?e.Q..^...nA....+.....{....?.....q..I...V.....V..I.>...UU\y...g.....J.8+..e...."X.0..~.....9.....<|....8.{..<...a.{[.JO+ X.....%{.....}...xWe....!..V.?Ee.$....ZK.$ge...F+....+._./oX....q..../>)z9CJ..cQ.....T[iP....KV..'#..3@.|w.b...T?...A..V.....F?.....YV..Cv..Y..]<.}s.kb..M.....(N..9....$.ze'..8....@/.. {...K..k..G.T.I..m|...z..R....W`..as~...Xz..v...Y.....S.eoNh.....0.e....E.[h.....+.]so.).vU.....H.....,4.7.|.@h@..|.{.|&...`..Q...X..o..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines (65386), with CRLF line terminators
Entropy (8bit):	4.3280715807044485
TrID:	
File name:	AkimaPAYROLL 2023-03-20.htm
File size:	758479
MD5:	09ee47c5b227fcbf4b803a69ac0547c0
SHA1:	e450aa71a3101821d24f8d9a419e78c6e2356bf4
SHA256:	99a2d35ba109bd4317ae26c4c9557007b7186cc6bc94b926d340f4bf745026a3
SHA512:	46d0de373d5a668c956e5dc5105225de13d522aa83a51d258b7f80e92827e1ac3010aa1ee2ff3f1f1084f8d735f8e351d99265f0b54efb0e8721808048cc47e4
SSDEEP:	3072:95pE0U2pEGQqJXtzV0/b+kv46ey7ozB5hKGyiWQ:6l22CJXtzV06kv46ey7ozjhKGyiWQ
TLSH:	D8F46E383B4CD27F60D551F6AE14BBCE95E07C05EA8D4C5A51183B94B1B23B9EAE3072
File Content Preview:	<html dir="ltr" class="" lang="en">..<script language="javascript">.. ..// == Code Obfuscation Protection from https://blackhackertools.com == //..function _0x50d9(_0xd984f1,_0x2cb0af){var _0x457459=_0x39eb();return _0x50d9=function(_0x34ff68,_0x2fc8e0

File Icon

Icon Hash:	78d0a8cccc88c460