ID: 831024
Sample Name:
skm_03029876554.htm
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 01:03:39
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

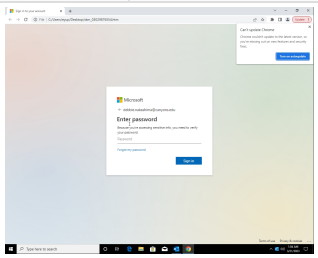
Windows Analysis Report

skm_03029876554.htm

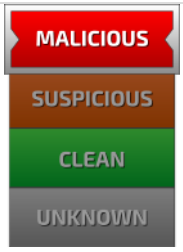
Overview

General Information

Sample Name:	skm_03029876554.htm
Analysis ID:	831024
MD5:	b5d7fc94a3f36…
SHA1:	88a5a06a5e4a…
SHA256:	62aea8fb264b0..
Infos:	



Detection



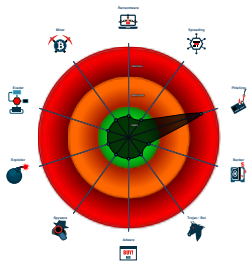
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Multi AV Scanner detection for subm…
- HTML document with suspicious title
- Phishing site detected (based on im…
- Drops files with a non-matching file …
- Invalid 'forgot password' link found
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 5272 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 2712 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\eyup\Desktop\skm_03029876554.htm MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 5920 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=2040 --field-trial-handle=1776,i,8774751515711196105,4137559805763673810,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - AcroRd32.exe (PID: 936 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\eyup\Downloads\sa100-2021.pdf MD5: 0EAC436587F5A1BEF8AEB2E2381D2405)
    - RdrCEF.exe (PID: 6408 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 4AC861CBCAFA331A72C04BF35AE792E3)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
skm_03029876554.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
58594.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

Copyright Joe Security LLC 2023

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

System Summary

HTML document with suspicious title

Mitre Att&ck Matrix

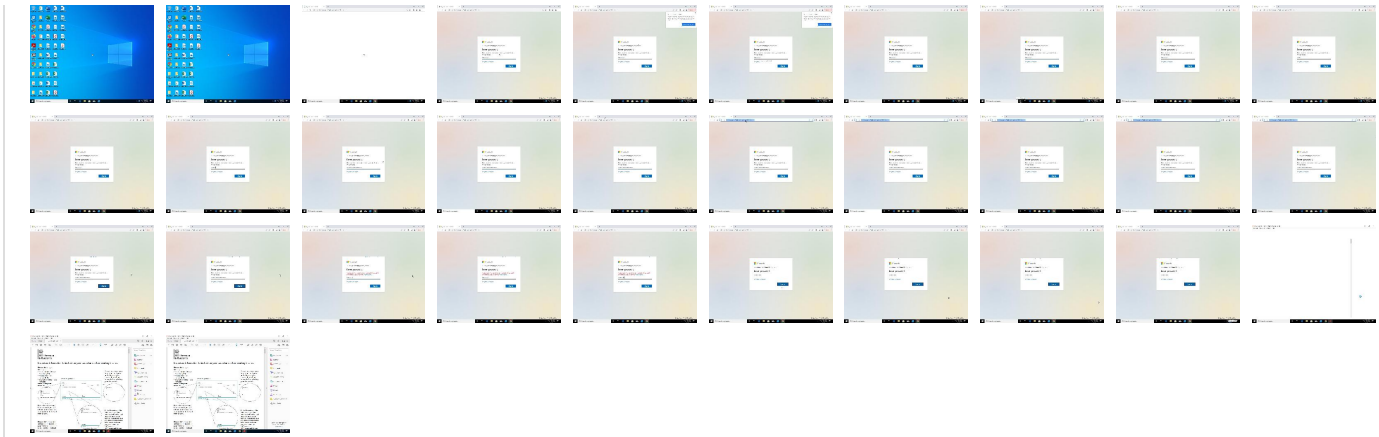
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 3 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	3 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	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 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	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

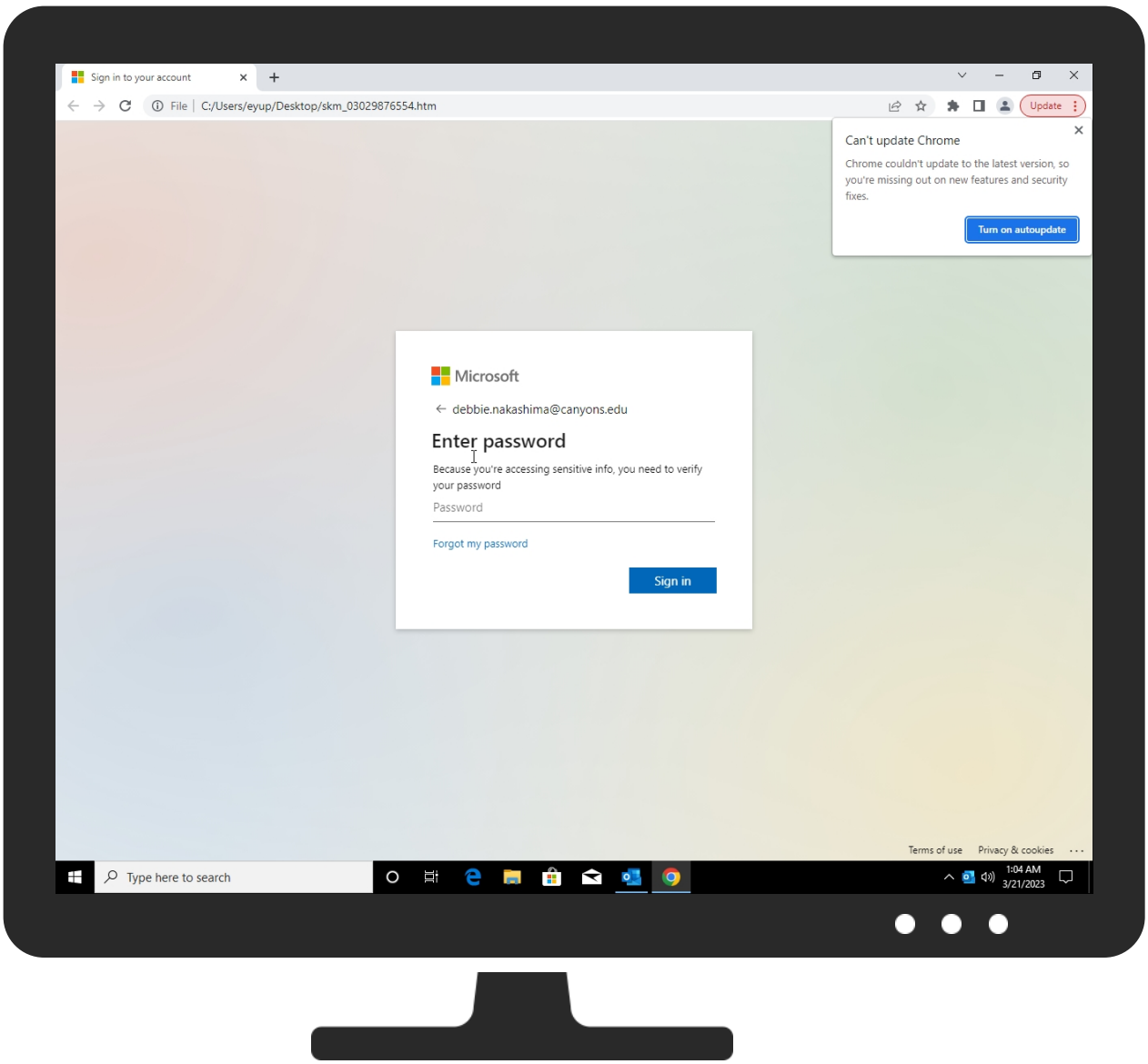
Screenshots

Thumbnails

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

Copyright Joe Security LLC 2023





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
skm_03029876554.htm	25%	Virustotal		Browse

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2023

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
amidaworld.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://amidaworld.com/set/style.css	0%	Avira URL Cloud	safe	

Domains and IPs

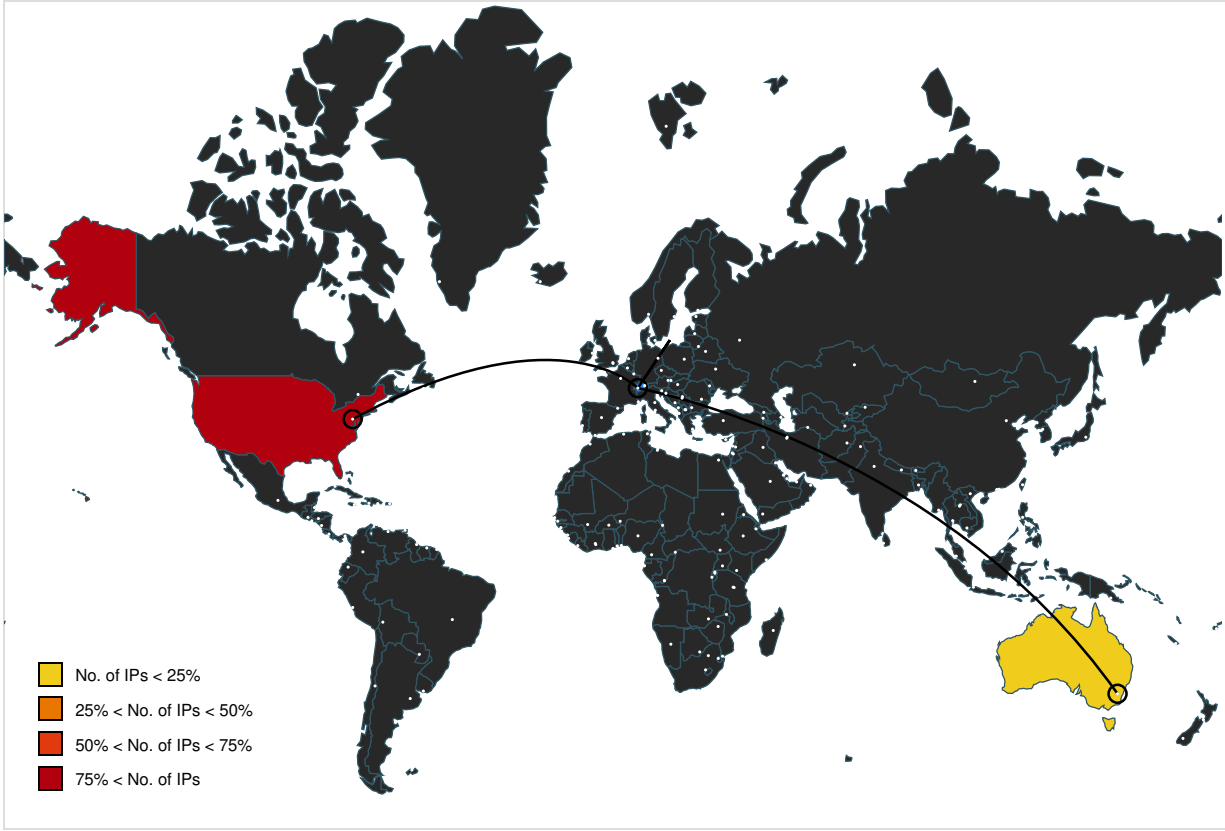
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.185.205	true	false		high
www.google.com	142.250.186.100	true	false		high
clients.l.google.com	172.217.16.206	true	false		high
amidaworld.com	192.3.140.99	true	false	• 2%, Virustotal, Browse	unknown
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
file:///C:/Users/eyup/Desktop/skm_03029876554.htm	true		low
http://amidaworld.com/set/style.css	false	• Avira URL Cloud: safe	unknown

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
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
216.58.212.164	unknown	United States		15169	GOOGLEUS	false
172.217.16.206	clients.l.google.com	United States		15169	GOOGLEUS	false
151.101.0.144	unknown	United States		54113	FASTLYUS	false
52.109.13.64	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.205	accounts.google.com	United States		15169	GOOGLEUS	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
20.189.173.15	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.3.243.146	unknown	United States		36352	AS-COLOCROSSINGUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
192.3.140.99	amidaworld.com	United States		36352	AS-COLOCROSSINGUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
52.109.76.141	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831024
Start date and time:	2023-03-21 01:03:39 +01:00

Copyright Joe Security LLC 2023

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:	6
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:	skm_03029876554.htm
Detection:	MAL
Classification:	mal72.phis.winHTM@38/27@7/174
Cookbook Comments:	• Found application associated with file extension: .htm

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- Excluded IPs from analysis (whitelisted): 69.16.175.42, 69.16.175.10, 142.250.184.195, 34.104.35.123
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, edgedl.me.gvt1.com, login.live.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: file:///C:/Users/eyup/Desktop/skm_03029876554.htm
- VT rate limit hit for: http://amidaworld.com/set/style.css

Created / dropped Files

C:\Users\eyup\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.046705279358675
Encrypted:	false
SSDEEP:	
MD5:	85F192DA73838B74673431BC56B4ACFC
SHA1:	EF8AE1B58CEC1A00F27C85BC03BBE3F65B44B6DC
SHA-256:	BA48E6DF6DCA51CFF662ED01CE07D5C11EACBF8F62AE036D54EFD2AD48C7EC23
SHA-512:	E968CC67BD76E22A1AFFE0BC840AE6340EB8883FAE104A7C17F73DCC6857E0F50B6DB63AB4D3EB491912779F91C107B1EBD8AA9673C83D298E2DAAAE5BABB6FB
Malicious:	false
Reputation:	low
Preview:	....ol..oy retne....&.....&.....:.y~A.....!/.....*.....!/.....9.cmvd@....!/.....oB*.....!/.....#...(.,i..!/.....k7A.....!/.....D.4..C...!/.....[.i..%..C...!/....., +..._.#.....!/.....<...W..J.....!/.....6<|.....!/.....A?.2:...C...!/.....+.{..'.C...!/.....?..7X.L.C...!/.....2q.....!/.....P....V.....!/.....+.U.!..V.C...!/.....P[. q.....!/... .....!...0.o.C...!/.....u\]..q.C...!/.....~.,.4>..C...!/.....&..r.....!/.....=..(Q.x.....!/.....!/.....*.....C...!/.....o..k...C...!/.....^.~..z..C...!/.....o.....!/.....Gy. '.h.....!/.....F..=z;.....!/.....3.....!/.....v...q.....!/.....C..M...,i..!/.....a.....!/.....$..+I..@....!/.....=....m...C...!/.....q..C...!/.....:..N.A.....!/.....u...!/.

C:\Users\eyup\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.046705279358675
Encrypted:	false
SSDEEP:	
MD5:	85F192DA73838B74673431BC56B4ACFC

SHA1:	EF8AE1B58CEC1A00F27C85BC03BBE3F65B44B6DC
SHA-256:	BA48E6DF6DCA51CFF662ED01CE07D5C11EACBF8F62AE036D54EFD2AD48C7EC23
SHA-512:	E968CC67BD76E22A1AFFE0BC840AE6340EB8883FAE104A7C17F73DCC6857E0F50B6DB63AB4D3EB491912779F91C107B1EBD8AA9673C83D298E2DAAAE5BABB6FB
Malicious:	false
Reputation:	low
Preview:	....ol..oy retne....&.....&.....;.y~A.....!/.....*.....!/.....9.cmvd@....!/.....oB*.....!/.....#...(.,i..!/.....k7A.....!/.....D.4..C...!/.....[.i..%..C...!/....., +...._.#.....!/.....<...W..J.....!/.....6<|.....!/.....A?.2:...C...!/.....+.{..'.C...!/.....?..7X.L.C...!/.....2q.....!/.....P....V.....!/.....+.U.!..V.C...!/.....P[. q.....!/... .....!...0.o.C...!/.....u\]..q.C...!/.....~.,.4>..C...!/.....&..r.....!/.....=..(Q.x.....!/.....!/.....*.....C...!/.....o..k...C...!/.....^.~..z..C...!/.....o.....!/.....Gy. '.h.....!/.....F..=z;.....!/.....3.....!/.....v...q.....!/.....C..M...,i..!/.....a.....!/.....$..+I..@....!/.....=....m...C...!/.....q..C...!/.....:..N.A.....!/.....u...!/.

C:\Users\eyup\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230321000632Z-238.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32, cbSize 65110, bits offset 54
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.7457613733254205
Encrypted:	false
SSDEEP:	
MD5:	38327A90092CAC6C4FC9638C31153D31
SHA1:	A776D8DE3C60296038D8FCC3AD6C850E1DFEDE07
SHA-256:	16C3DA8CD1D17DEF93284EC5F121912E6FD4A4E4997CE14B04B584DD06142372
SHA-512:	1E864E3C9E19DAC87ED87E9CFBD0CC127B1C96C037174B0E93B85359F7EF4E8283AE20639FADE275218E16A83567D22832F09D681922F46696F062FC4CFEF2DC
Malicious:	false
Reputation:	low
Preview:	BMV.....6...(...k...h..... ....

C:\Users\eyup\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	
MD5:	DC84B0D741E5BEAE8070013ADDCC8C28
SHA1:	802F4A6A20CBF157AAF6C4E07E4301578D5936A2
SHA-256:	81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06
SHA-512:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB1
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\eyup\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.041320905832144
Encrypted:	false
SSDEEP:	
MD5:	9C021B642B15DC8101446194BA02B5C1
SHA1:	CDA3794446008F3E73288B270EF20A66EFEF0ECC
SHA-256:	D2B14AD1218BA9107E4AA69F93108E0CF67940EF421DBC8BA34ACA9FBDED7E0D
SHA-512:	C3472A168B345D0684C3D49F277C3B43C1DABDA817562A6E6A51B478EE118065B7BC482EADD2F1E624E42914EBA6C1BE4ED80A0A1518BF3BEC2953197C361A37
Malicious:	false

Reputation:	low
Preview:	{"all":[{"id":"TESTING","info":{"dg":"DG","sid":"TESTING"},"mimeType":"file","size":4,"ts":1679357189000},{"id":"Edit_InApp_Aug2020","info":{"dg":"161d51769e661 f1fdd4d398c6abbbefd","sid":"Edit_InApp_Aug2020"},"mimeType":"file","size":782,"ts":1622133335000},{"id":"DC_Reader_RHP_Banner","info":{"dg":"0454e964c da3563bc5709c3bb96ca22b","sid":"DC_Reader_RHP_Banner"},"mimeType":"file","size":1393,"ts":1622133335000},{"id":"DC_Reader_RHP_Retention","info":{"dg": "5ad4c6bdddc427069eaf1f4b15aa994a","sid":"DC_Reader_RHP_Retention"},"mimeType":"file","size":287,"ts":1622133335000}],"g_info":{"Version":"0.0.0.1"}}

C:\Users\eyup\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	40393
Entropy (8bit):	5.5182337348115755
Encrypted:	false
SSDEEP:	
MD5:	D61BAC3B8217D3AD798E5074710D725A
SHA1:	B6D19A7783A90B7B27BCB5F15D3EBE826489E1BE
SHA-256:	8C5E5610296C1A6C2883B1282786C8C74283D92407086064AD60D31A524CFE30
SHA-512:	A70C78F7840D09F99FE0C297D351DB01F63A52C70BD61D15433351B66478CD2E84D1E12DF64A08F9E9B5E2D621F732B3B2CC8172C5CBBF32958D791A8519038
Malicious:	false
Reputation:	low
Preview:	4.241.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$..... ....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic. L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-BoldItalicMT.P:Arial Bold Italic.L:$..... ....."F:Arial.#.91.FID.2:o:.....:F:Arial-Black.P:Arial Black.L:-....."F:Arial Black.#.103.FID.2:o:.....:F:Bahnschrift.P:Bahnschrift Light.L:&.....,... ....."F:Bahnschrift Light.#.

C:\Users\eyup\AppData\Local\Temp\acrord32_sbx\A9pi4hwn_1u6bam5_1dg.tmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PDF document, version 1.6, 0 pages
Category:	dropped
Size (bytes):	358
Entropy (8bit):	4.956606839690132
Encrypted:	false
SSDEEP:	
MD5:	415A3E1EC16C8BBF1C59F10905C6B5C2
SHA1:	A557237DB395902676ECF4121C8E4D53F11A5821
SHA-256:	39ED393C1C2D9E2AE0FE6B5BDA63371BC7CDBB8CD37226A874DB1E1B37574CC8
SHA-512:	FC9EDD1DF795B9F06AFC762FBEB15CDFD9AC6F52694F14AE646FED671E4ABEEC53165897D2A3C60C9D81ED937CE58D678E44E20F558C2674BE3958567ECAF 88A
Malicious:	false
Reputation:	low
Preview:	%PDF-1.6.%.....1 0 obj.<</Pages 2 0 R/Type/Catalog>>.endobj.2 0 obj.<</Count 0/Kids[]/Type/Pages>>.endobj.3 0 obj.<<>>.endobj.xref..0 4..0000000000 65535 f..00 00000016 00000 n..0000000061 00000 n..0000000107 00000 n..trailer..<</Size 4/Root 1 0 R/Info 3 0 R/ID[<1F0E77321FF04D47851F040FF11DEFA9><1F0 E77321FF04D47851F040FF11DEFA9>]>>..startxref..127..%%EOF..

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):	9830
Entropy (8bit):	2.262474443886637
Encrypted:	false
SSDEEP:	
MD5:	13C11A5715992237A09B81E73A061528
SHA1:	330B58D8BCF3E9183A4D6C605E651346DE96949B
SHA-256:	75C5758E43AD5DC9E5FED5AFE0E1FAB4BAB99EA412D2C4512A0BB2D2BF867F7F
SHA-512:	E621EF9D70E4EF9EB9CB8FE2E4C31B3446F605D68130E25DCBF7D42A752F0AB72D22D39DAC6B4F1D9B5395D4F4D0AE3BA950CCA1F8A27F1489DEE9A2696EC 8C4
Malicious:	false
Reputation:	low

Preview:	.6...AAAAAAA...AAAAA...A.A.A/ALAAAAAAAAAAAbA5AtA.!.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.A...A.L.AL..A. ..A}.A...A..(A.}.A?..A.1.A...A..A...A...A1..A..A..yA._.AH.MA...A_.A...A...A...6...A...6...A.?.69..A.H.A..A.9bAF.XA...A`..A...AN.DA..A...A.%bA..A.;b...A.#b...7A...Aw..A68 .AAA.AtA.6.....@..ve.....,.....c.....L..... .....

C:\Users\eyup\Downloads\0743ed68-e186-4fdd-be66-e56798cabd74.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.6 (zip deflate encoded)
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	7.83129527186236
Encrypted:	false
SSDEEP:	
MD5:	1CB582FAE8CAA96E56AEF44F41EB7F31
SHA1:	1F77ED6BF5F55DDFE08D0001604EC699452388B0
SHA-256:	65C913B0D1A088AAEED06CC308EE68AF6E6716BBC0FAA8F295F5D32034B66983
SHA-512:	D801DA93C8BFE10C3C0D4A35A6ED9CC60963716799D22479B84D5B1B4C03F3AFE80E59C160448552570B010B7228F2F3393889A629ED54880BA905D7FC77D27
Malicious:	false
Reputation:	low
Preview:	%PDF-1.6.%.....823 0 obj.<</Linearized 1/L 1459845/O 825/E 264898/N 10/T 1459310/H [627 443]>>.endobj. .862 0 obj.<</DecodeParms<</Columns 5/Predict or 12>>/Filter/FlateDecode/ID[<E77D3F16EE59464DA97F4E343FB6F67B><58C879C0AF2342069FF2766B75F51FCF>]/Index[823 85]/Info 822 0 R/Length 157/Prev 1459311/Root 824 0 R/Size 908/Type/XRef/W[1 3 1]>>stream..h.bbd`.``b``.....R...".^.H.G Ru.X$.L^..Y."..$...XM&....."..@$..B...,....."..,...`...^.-.. ...l...../.I..I{An..@..$.[=.t....> bd`>.v...&.3.....`..=.!.endstream.endobj.startxref.0.%%EOF. .907 0 obj.<</C 390/Filter/FlateDecode/I 413/Length 349/S 2 36/V 367>>stream..h.b```b``Vd`c``td.f@.a.V.(..G....@....a../...a..pn..&.}..S$D^8....1d..U.....n.....v.....f.....>.....>.;..Z}Z..}..u..7e..j:(.&{;.....e..60ttt4....P0....P.`.....\. ..Tb`u...@I...?.....,..*.j.m.QJ.e/.Jqq102.3<f`...x.k6.....N1.1.1F1.c4l.>.....f.f.dG4...5<...t...|&~F....7X/!

C:\Users\eyup\Downloads\sa100-2021.pdf (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.6 (zip deflate encoded)
Category:	dropped
Size (bytes):	1459845
Entropy (8bit):	7.380920052115249
Encrypted:	false
SSDEEP:	
MD5:	8B6D1B4C2E818F61AC264C1106C3190B
SHA1:	A1BE39455B10CA90D13DBACF066DAE85148F1765
SHA-256:	BD8C253F36B54B82DC61AFFFD76FD041AFCC72ABAA34D27A5C2F46F4E08F3A66
SHA-512:	7A810E88A7B6AF90554871BCFFEBBE3758019EA5827F495AC5A0800EB16CA607E75C8C16EC61173D8B684BF3F1CCBB668715B7E035EFB1B612401449BD454DE E
Malicious:	false
Reputation:	low
Preview:	%PDF-1.6.%.....823 0 obj.<</Linearized 1/L 1459845/O 825/E 264898/N 10/T 1459310/H [627 443]>>.endobj. .862 0 obj.<</DecodeParms<</Columns 5/Predict or 12>>/Filter/FlateDecode/ID[<E77D3F16EE59464DA97F4E343FB6F67B><58C879C0AF2342069FF2766B75F51FCF>]/Index[823 85]/Info 822 0 R/Length 157/Prev 1459311/Root 824 0 R/Size 908/Type/XRef/W[1 3 1]>>stream..h.bbd`.``b``.....R...".^.H.G Ru.X$.L^..Y."..$...XM&....."..@$..B...,....."..,...`...^.-.. ...l...../.I..I{An..@..$.[=.t....> bd`>.v...&.3.....`..=.!.endstream.endobj.startxref.0.%%EOF. .907 0 obj.<</C 390/Filter/FlateDecode/I 413/Length 349/S 2 36/V 367>>stream..h.b```b``Vd`c``td.f@.a.V.(..G....@....a../...a..pn..&.}..S$D^8....1d..U.....n.....v.....f.....>.....>.;..Z}Z..}..u..7e..j:(.&{;.....e..60ttt4....P0....P.`.....\. ..Tb`u...@I...?.....,..*.j.m.QJ.e/.Jqq102.3<f`...x.k6.....N1.1.1F1.c4l.>.....f.f.dG4...5<...t...|&~F....7X/!

C:\Users\eyup\Downloads\sa100-2021.pdf.crdownload	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.6 (zip deflate encoded)
Category:	dropped
Size (bytes):	1459845
Entropy (8bit):	7.380920052115249
Encrypted:	false
SSDEEP:	
MD5:	8B6D1B4C2E818F61AC264C1106C3190B
SHA1:	A1BE39455B10CA90D13DBACF066DAE85148F1765
SHA-256:	BD8C253F36B54B82DC61AFFFD76FD041AFCC72ABAA34D27A5C2F46F4E08F3A66
SHA-512:	7A810E88A7B6AF90554871BCFFEBBE3758019EA5827F495AC5A0800EB16CA607E75C8C16EC61173D8B684BF3F1CCBB668715B7E035EFB1B612401449BD454DE E
Malicious:	false
Reputation:	low

Preview:	%PDF-1.6.%.....823 0 obj.<</Linearized 1/L 1459845/O 825/E 264898/N 10/T 1459310/H [627 443]>>.endobj. .862 0 obj.<</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<E77D3F16EE59464DA97F4E343FB6F67B><58C879C0AF2342069FF2766B75F51FCF>]/Index[823 85]/Info 822 0 R/Length 157/Prev 1459311/Root 824 0 R/Size 908/Type/XRef/W[1 3 1]>>stream..h.bbd`.``b``.....R...".^.H.G Ru.X$.L^..Y."..$...XM&....."..@$..B...,....."..,...`...^.-.. ...!..../.I..I{An..@..$.[=.t....>bd`>.v...&.3.....`..=.!.endstream.endobj.startxref.0.%%EOF. .907 0 obj.<</C 390/Filter/FlateDecode/I 413/Length 349/S 236/V 367>>stream..h.b```b``Vd`c``td.f@.a.V.(..G....@....a../...a..pn..&.}..S$D^8....1d..U.....n.....v.....f.....>.....>.;..Z}Z..}..u..7e..j:(.&{;.....e..60ttt4....P0....P.`.....\...Tb`u...@I...?.....,..*.j.m.QJ.e/.Jqq102.3<f`...x.k6.....N1.1.1F1.c4I.>.....f.f.dG4...5<...t...|&~F....7X/!

Chrome Cache Entry: 123

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-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.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,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.</path>

Chrome Cache Entry: 124

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
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: 126

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	assembler source, ASCII text
Category:	downloaded
Size (bytes):	139982
Entropy (8bit):	4.917184725631878
Encrypted:	false
SSDEEP:	
MD5:	F0F452924F2FF22B5C73A3D99BDA9349
SHA1:	27AD12AAE7B126C0B55AD418C7F0F55491F0DB49
SHA-256:	B1B322FEC0D1640F1C1FE868AF8F9CB0965912A7E45E56943DE55710165027D3

SHA-512:	0B30CCEE498F0816EE32C31A9E099CE20003B08D037364A3231ACB656CC658B39BBB3015630845D8657B4EE97ED682BD7B10FE5623DC8C5F04EAEA27AC946AF2
Malicious:	false
Reputation:	low
URL:	http://amidaworld.com/set/style.css
Preview:	html {. font-family: sans-serif;. -ms-text-size-adjust: 100%;. -webkit-text-size-adjust: 100%;.}..body {. margin: 0;.}..article,.aside,.details,.figcaption,.figure,.footer,.header,.hgroup,.main,.menu,.nav,.section,.summary {. display: block;.}..audio,.canvas,.progress,.video {. display: inline-block;. vertical-align: baseline;.}..audio:not([controls]) {. display: none;. height: 0;.}..[hidden],.template {. display: none;.}..a {. background-color: transparent;.}..a:active,.a:hover {. outline: 0;.}..abbr[title] {. border-bottom: 1px dotted;.}..b,.strong {. font-weight: 700;.}..dfn {. font-style: italic;.}..h1 {. font-size: 2em;. margin: 0.67em 0;.}..mark {. background: #ff0;. color: #000;.}..small {. font-size: 80%;.}..sub,.sup {. font-size: 75%;. line-height: 0;. position: relative;. vertical-align: baseline;.}..sup {. top: -0.5em;.}..sub {. bottom: -0.25em;.}..img {. border: 0;.}..svg:not(:root) {. overf

Chrome Cache Entry: 127

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD97F
Malicious:	false
Reputation:	low
URL:	https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

Chrome Cache Entry: 128

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.."""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""

Chrome Cache Entry: 130

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.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="3.1.1",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

Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	2.986914097449634
TrID:	• HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11001/1) 18.97%
File name:	skm_03029876554.htm
File size:	18434
MD5:	b5d7fc94a3f36ff6ef2d544577e2ba77
SHA1:	88a5a06a5e4aa9c9a83c2ffd44cc9aeb44a8ba87
SHA256:	62aea8fb264b0ad6e5076e98c5c67f99cf484680ee0df854c7917a13418a5e6a
SHA512:	e8ff89b3fb16c85a65edfe42f966b3ffe15c34149b3c3dce34a32888dc68d46c5abe84a09a7f831791a2e1bc30074ebf4701d8566bd103d8bd583ca4c74c9176
SSDEEP:	96:CWzcE1uPshrWH06Rpd7Y7clZ6lzuYYujEKr2w+5f7X6y+EnYEnKczNn:AxRJlE1HQ7KYNn
TLSH:	6D822F6564D1102603B3C1956AB6AB09FF25C20BC706CA143AEC6FC71FF3E16CD67698
File Content Preview:	<html dir="ltr" class="" lang="en">....<head>.. <title>Sign in to your account</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.. <meta http-equiv="X-UA-Compatible" content="IE=edge" />.. <meta name="viewport" co

File Icon

Icon Hash:	78d0a8cccc88c460