ID: 441424
Cookbook: browseurl.jbs
Time: 22:26:34
Date: 28/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

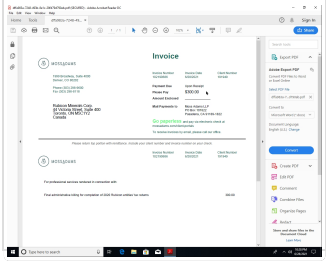
Windows Analysis Report https://bms.kaseya.com/Com…

Overview

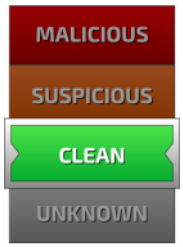
General Information

Sample URL:	https://bms.kaseya.com/Common/GetFile.ashx?enc=iAIF3krAhFnrzr2%2fdZEndh%2fo...HtbR9vpsvc9XqhjBxH0y6QoOe1BdU1OcYCSw%2fCxijoaHl0%2faUv%2fJAurw9NEQN2A5zE%3d
Analysis ID:	441424
Infos:	

Most interesting Screenshot:



Detection

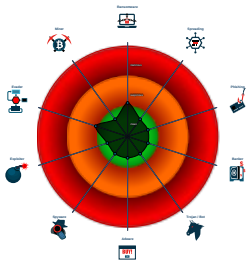


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6776 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6828 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6776 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - AcroRd32.exe (PID: 5148 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - AcroRd32.exe (PID: 4244 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - RdrCEF.exe (PID: 6472 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6584 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5642234162136683367 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=5642234162136683367 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6416 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=6949978120898280864 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6960 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=348665043263964070 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=348665043263964070 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 7092 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12973235889727847520 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=12973235889727847520 --renderer-client-id=5 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

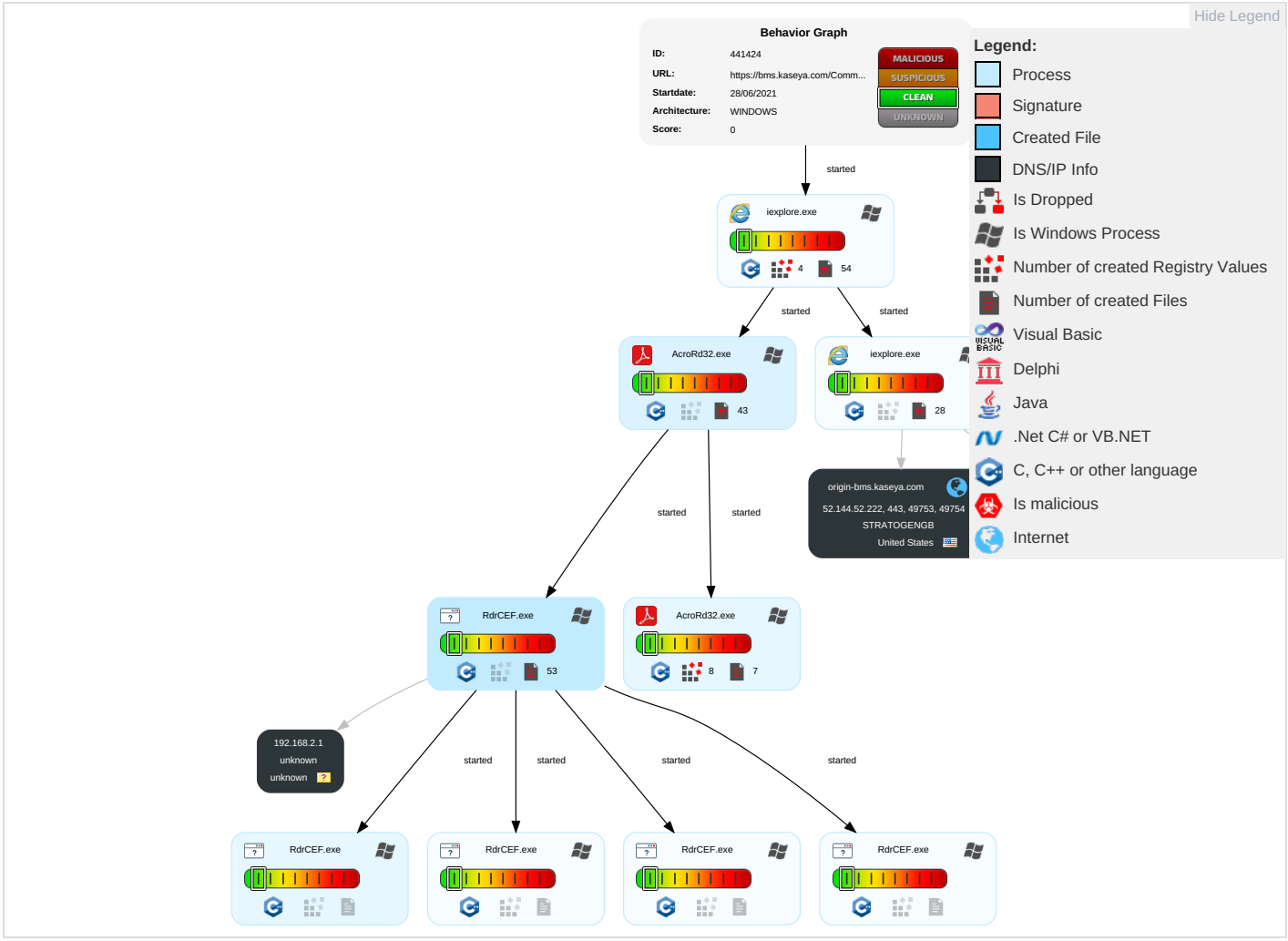
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

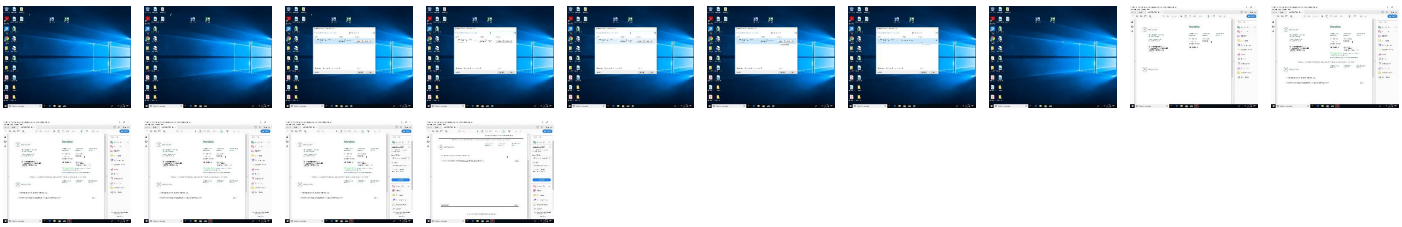
Behavior Graph

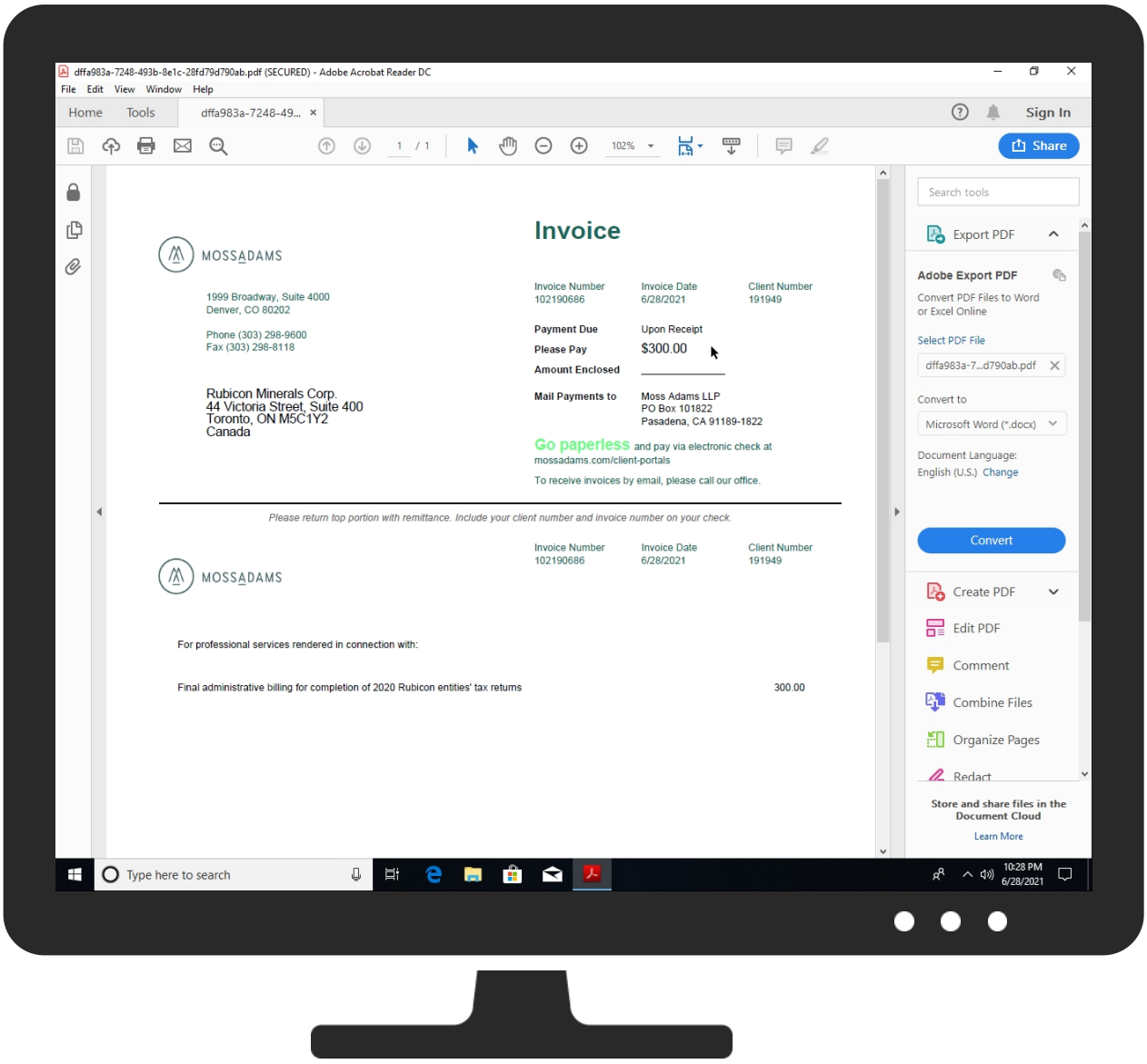


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://bms.kaseya.com/Common/GetFile.ashx?enc=iAIF3krAhFnrzr2%2fdZEndh%2foMj7qNe0PshuhX7KBbHtbR9vpsvc9XqhjBxH0y6QoOe1BdU1OcYCSw%2fCxijoaHl0%2faUv%2fJAurw9NEQN2A5zE%3d	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
0	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
origin-bms.kaseya.com	52.144.52.222	true	false		high
bms.kaseya.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0	false	• 1%, Virustotal, Browse	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.144.52.222	origin-bms.kaseya.com	United States		50292	STRATOGENGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441424
Start date:	28.06.2021
Start time:	22:26:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bms.kaseya.com/Common/GetFile.ashx?enc=iAIF3krAhFnrzr2%2fdZEndh%2foMj7qNe0PshuhX7KBbHtbR9vpsvc9XqhjBxH0y6QoOe1BdU1OcYCSw%2fCxijoaHl0%2faUv%2fJAurw9NEQN2A5zE%3d
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@17/61@1/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found PDF document • Find and activate links • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:27:52	API Interceptor	6x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.683336056838172
Encrypted:	false
SSDEEP:	12:vDRM9bTZiEVODRM9BNVZiEsHDRM9OUGZiE:7OMEVEvEA6TE
MD5:	A290CCFD836DF13697F726CA3E0C6191
SHA1:	7E69BB315157C2CFE0BFEF5999F6AEB1137FED91
SHA-256:	E33536D46BB01976BF864C907B4968D06CABCE5CF06F55A3D4DB694522867294
SHA-512:	A815BCEB831A1F36CC9E2C83DE43D6A6D71FEEF39CF28DCEA8453CFD5A17430A33507F19E2B8AB8D2D011EEDFADE3A991F0EAF0959B8CA608DFB9719F2942757
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..;..o$/....."#.D...3.6.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....u..E.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .1Q..o$/....."#.D.O.4.6.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo....._Z.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..J .o$/....."#.Du.95.6.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	522

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Entropy (8bit):	5.628153370407874
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEknWZ8Be7Ywcr1TK6tZ2i9NqEYOFLvEkqSh8Be7Ywcr1TK6tii9NK:V9zHg9PQjl9zJh9PQT9zCT9PQg
MD5:	510671D92800292E52F41811532D6CAA
SHA1:	6159D6232B16D29A7083C876F48DCB697D9E1226
SHA-256:	2CBD365C2A6135AF675A7B8C495CD7B814BF8CB7EE9E5B86A112B67A8DA05D60
SHA-512:	FB0A139A0CC44F46817EEBCD131E570A148DD95E9F12B7D1E91827B4188CB650AEC59F39C25C574C3CDE0187E4E285AF5027B9C9CDCF29B777E3581E7BC705 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js .c<..o$/....."#.D..93.6.A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,...._keyh ttps://rna-resource.acrobat.com/init.js ....o$/....."#.D.7:4.6.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....2.....0\r..m.....,...._keyhttps://rna-resource.acrobat.co m/init.js .i...o$/....."#.D6..4.6.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....s.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	738
Entropy (8bit):	5.615348625039501
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAF3lUo6jTyeRVFAFjVFAFgQ4lUo6jHyeRVFAFjVFAFIohlUo6j:tB4v43SBdB4v4V4SBpB4v4DSB
MD5:	C81E8CB59F45D18E7D428A50D6F2FD9A
SHA1:	D0F9CC56E490BBE427870F6AF2E2E9A33D2740BC
SHA-256:	7FC404D23BF6CB0C069795E14B01FBEC383569652743C0A5F285B16DFAD1A9B9
SHA-512:	DFC1C5B12B23179D89EADE6FFC88F76ABC428F97BF3601EBBC847519B2ECE4EEF1D91C580B8F09384DCC0A284A887A0E9F38E9A0B387EFB3FEAA9A2B48D9F 7D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .>9..o$/....."#.D$.3.6.A..hvD O.N.t@.....n.*..... ....A..Eo.....A..Eo.....?Bm.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js /home-view/selector.js .....o$/....."#.D..~4.6.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....e.:.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/stat ic/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..`..o$/....."#.D#K15.6.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....8.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	464
Entropy (8bit):	5.633348187679963
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rs4jLij2iWulHyA1TK6t6NtVYOFLvEWdFCi5RsNd2iWulHym:IbRkiDTCLWuss2bRkiDQLWussD
MD5:	33FD974542857726A68D15980C33159E
SHA1:	DD8A9CEDE266ED85681F77557BDA0920CE7667DB
SHA-256:	8DDAF39870EA80C049BA4E9F5ACCADD5D436248783D53AFEA13D5F5F3C061BEE
SHA-512:	3CB3E53F5DF6137751DCD15DF62D5DEDCD9580A71CCDE894CEA6C4821DDABE5FEB8C62643F4D197BA73601E3DFACFC037F4A67D0E6A9829A359690AC25E7 875
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .Ls..o$/....."#.DR..3.6.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....rn.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .g...o$/..... #.D2..4.6.A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....y.A.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.581265567074103
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu+5BuX83Vyh9PT41TK6tq:pyixRu1XQV41TE8
MD5:	E179A603644A30D959FDB0CA41933DF0
SHA1:	6EC683634BCA836A7AB517CAFB013A276DA761B1
SHA-256:	913AFAF101EFF8EE64E2A38F34F21E0B59BDA20AEAB4395C97256F335C4494DF

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
SHA-512:	5E37ACBCBDEF5448AB1350E6B6BB70CF75DEE3E5F8A66F256C799FD7AB6631D2A4043B8C7428DE2D1CE946E9B979F7EDB845964465922265376F0C4B7D9B3AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....o$/....."#.D..25.6.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. ....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.607086575850694
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQJ+hfUhLZIl6P41TK6t:0Rhk6yALZC
MD5:	7AD6D9CBA079B8658A24153584E93A51
SHA1:	0DBB4C2AC9812651302E836D7EF347262A1CA42D
SHA-256:	6F84FD5A769103C66D2FE927D0A000FE517B7F651B2704A3D044BFF33E6DDCB2
SHA-512:	A984B3A6A2491890938E371B0600C3E6D72E4426CBF785C7312B5B1985F0ED820F179AB1DB4D26D6EF20B0EAEF7C755563600A4F6206539CA0E27DCCB7158BA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .....o$/....."#.D...5.6.A.].>....uUf..N...k.....c..I.A..Eo.....A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.469833795125909
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVXktAfkEGFcyxMtv9EWm1TK5q:mJYOFLvEWdGQRQOdQFkfkEGF6g1TK6t
MD5:	F82C2EB61356B583C4BA6B72C438D7D0
SHA1:	FA35399CA3611DD224D0FDFFEBC409CCAA6D0B2C
SHA-256:	B57257C8D4C33FE9342082403F3FFC45A61C1F756C36A0EC194563D2F087D9D9
SHA-512:	6A9DD85B62ED80924A12A586BCD29E9D4359DF5899E467FE104B6A5586CD7102BE3DF712CC439BBB7BDF6BDDC130A2EA25F97941075EC93C41CC70B54F4699 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ... .o$/....."#.D.H25.6.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....o\.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.599600513769249
Encrypted:	false
SSDEEP:	12:Z5MXXMuR/Ej5MLRo8MuR/EDJ5MGlFrIMuR/EJFl:ZSsuR/EjS1ouR/EFSGJuR/Erl
MD5:	E07300244E488D1F1D525867EB8FF635
SHA1:	82F360BB7C6FB9DA3C7808C244605E3AB28018E4
SHA-256:	A9CE3909A44D6BB7E2922B31FCA7432FC65838DC6B5EA1891A2ACEAE52CA0F2B
SHA-512:	D00414610E716C64EA9894060BCB025888800C33A117EB4C0540D68E32D5A5174DE9223AF54249C519077BC033BD2F86375B59375E7C0A744E838BA27DFFCECC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..B..o$/....."#.D..93.6.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....x.q.....0\r..m..... .3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .M..o$/....."#.D.M:4.6.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb.... _keyhttps://rna-resource.acrobat.com/base_uris.js .'...o$/....."#.D...4.6.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo...../T.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Size (bytes):	214
Entropy (8bit):	5.5166147778424435
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtupWipcby0zBUKSAA1TK6tXll:pRJKcbexll
MD5:	15B525F619A84499021453FCF0240C3E
SHA1:	7086AAE283AB76436B60D927B0D5D8EB49612CD2
SHA-256:	0B1B9926E28624A1062E33C3DFC9A8FB6A5800AC2603AF5493E50E9FFEB6F15D
SHA-512:	81C8134C730A3705C01C9F6911F0409A32228E0F62A9EA39600C16A5724E22533114E2B28CF64ADC2D935ECD89F798DB4A85681A01B6A140EBEB8675DF52CDF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ... .o$/....."#.D..25.6.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.5449090515340655
Encrypted:	false
SSDEEP:	12:KkXxKMSCvAWtUlMCkXxKMSCv/otUlakXxKMSCvV3tUl:KkXxiCYWWMCkXxiC4WakXxiCN3W
MD5:	079F67B62965A4E9B04C0D4CF797E3B9
SHA1:	060E832B366426FCF84DAC9E02F5C641A14B1847
SHA-256:	92543001184908C5EC6EA245E8B0AF2FC717128E0626754146015D94053C228F
SHA-512:	08E5501082D1D6D3A6834E99EA0313E2662E5B1DAAE984FDF4958215F94EDF4D4E1718F284DFDF14817A75F6511BFF40BEB77D68B97F598DACC002A758EA057
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..>..o$/....."#.DV.93.6.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....#.....0\r..m.....1. .....5...._keyhttps://rna-resource.acrobat.com/plugins.js .D..o$/....."#.D_F:4.6.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....&.....0\r..m.....1.....5...._key https://rna-resource.acrobat.com/plugins.js .k...o$/....."#.D#..4.6.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....a.f.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	561
Entropy (8bit):	5.583674396476667
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLMP8T9qyM+VY1TK6tBSkl9YOFLvEWsfOLkz8RyM+VY1TK6tZ+g:5h6OLMP8hk5h6OLk4ck1h6OLhk
MD5:	A1A1C84E253B0A28808AAB45F7E656BE
SHA1:	4002120FC3BF08790A9EE566E9E7C3E637DE89BF
SHA-256:	636FF4EA829FDFA68A1687C0B9BC3648C9D575F9FA4167C11D0FD3854E84498D
SHA-512:	9FAA623211613DBD6CD19418B7004C43E0AF8D4ADA4200A4B571DF3243A3206661CF433FC97B4B90DDF374A1CEE2108A81108283DD45C374D9AFAB9FE9A7DC C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....o$/....."#.Ddxu3.6.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....N.....0\r..m.....;... I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....o$/....."#.D..m4.6.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....7.....0\r..m.....;...I..... .._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....o$/....."#.D...5.6.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	732
Entropy (8bit):	5.649709060603581
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFRWwSeKaTLnWkRVFAFjVFAFrLvwSeKaTLnvNeRVFAFjVFAFGGSwSez:UB4v4MwzXLnWkB4v4rTwzXLnvNeB4v4j
MD5:	0C58C758F97961292D56411AB46AE3C2
SHA1:	8E8E7C8DA6DD8B1F1B4C5BB53145BF1598245E22
SHA-256:	726762A8AB3003997452553CA13EF4BB04D0BF07CDA6FEAF739BD7F0B08C4AF0
SHA-512:	7BFF972C0CB943856EC0233212D296DEAC8BB858A2C69FB5A28F9A376D589BA9063C734A3809EB412C37774AD6F5B14C10B8A3B17D75D28731A6A983588AD81
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Preview:	0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .8...o$/....."#.D.2.3.6.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....5Y.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .!...o$/....."#.D*.4.6.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....eO?.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .....o$/....."#.Dg`45.6.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....s=.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.521816048040188
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuCKlJn511TK6t9dN:BsR2EseP6JXrdN
MD5:	4889E3F8858D1FD305ABC1AD3ED2B002
SHA1:	55CBDECE0822801C9E8029ACE57788A9F4654C97
SHA-256:	01685239C76F8BEC4AB8E55F7B947C2C24CC7C7E1444EF8D31B8618954A40E1D
SHA-512:	C542C7481739AFFE08D0D332608DF455A95E364EF0D9A19FD87B4EB2F035F2C179C5A0F345CCC8D6306E7D3CF9B658825FC4F6F91CEBD4589304B5AD2A3D52
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .H...o$/....."#.Dm.15.6.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.591490820931043
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQS8kIFB7OhKlvA1TK6tjl:RbR16L7IFBJk
MD5:	5189BDDB4AF244D007552B9883B84B8A
SHA1:	AC07CBF838F4BFD1EE970DD72E27FF865F3B26A6
SHA-256:	ED0677F5ACD00893BE00BD144CC509EC75F44DF1915B4C01DEB14D7E42CDCF25
SHA-512:	2AC795500EA07CE06414CEE8DC557F965E7F3DF92EE577FD55B4C16C13EB7AC144A92E478EBBE0236F9F78925C3582ADC1BED2FD74B2078A1311EB46B5CEAE 21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .....o$/....."#.D.m.5.6.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.539902690176604
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVumX9RQdFt1TK6tv:B2geRHRQP70F
MD5:	FD5D8860611F93BED3353A692BD0A7D5
SHA1:	0C55A2CEE9F1200B2353BA072727ABDD9B6EEC81
SHA-256:	CC73EDCE6F10D66A392C5042CA4B8613893A487D8BCD1DECD4EF71B1CBAE6317
SHA-512:	419604CDB21EE942002C63BD06A41BE9130AE6814CD0604A583A9033778745771D2CADE7EDEE83540119BAB75799EFEEED44CB7D69AE7298D547240F8314F9E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .{...o$/....."#.D.15.6.A@..{o]...9o|..qY....T....{..u.b..A..Eo..... .....A..Eo.....^zD.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.628178594662831
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
SSDEEP:	12:WyeRlgunEt1wlyeRlDt1wX+yeRliDKt1wh:WJllfwlJbfwX+JaWfwh
MD5:	4950592581BE2383DEC139C117C4496E
SHA1:	2234DAD6B55ACEE48D2AE13F2A1E5FF214E56DF3
SHA-256:	1396B125237750C2FD1644D5AEF43842F0DFACC64C22FF8CCB0FD209FDA7DCCE
SHA-512:	B247B43D1227511288E50293364170CDF45D0660E3774A46ECFA66EED57B7C4E5E972EEB35C304F0D5A1C73EC369665AE8ED9E662493D48E136FAF07734CF083
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...o$/....."#.D..}3.6.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... .....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..l.o$/....."#.D.0u4.6.A.t\a.....x5.'OuE.C..@.....x..A..Eo..... ..A..Eo.....<2.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .....o$/....."#.D.N.5.6.A.t\a.....x5.'OuE.C..@.....x..A..Eo... .....A..Eo.....#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.512378896332743
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFve/IQ9ONqww6U+5m1TK5kteut:mnYOFLvEWdhwyu7COqwK+41TK6tpt
MD5:	E12C6403B5B3DBE385478E34453EEC12
SHA1:	CB7C3A7B3F0D2E5D64B1B222E2FD508D4C848A68
SHA-256:	28FA8742224E3A22DC06FED30746882538F6D0024A5BE0F3A7CEF5461D09A7F4
SHA-512:	148A3E0F9598C6A5BF36A559FBAF0082CF790DA4627CD3303C534D70DC1AC5DC9249CEC9F3E888FDF0CA1B748E7EDD7C01026D12890B672EFAC921357A853F C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .y;..o$/....."#.D0I.5.6.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....6S.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	690
Entropy (8bit):	5.642891527413466
Encrypted:	false
SSDEEP:	12:/RrROk/LisfLEt9HXRrROk/J/sfLEeRrROk/MgcWsfLEY:/PJ/+s4fXPJ/J/s4ePJ/MgcWs4Y
MD5:	5036D5D957557E886A93EA2350E88EFE
SHA1:	4E055DE7ADB8B36B23BF0D37D4EDE0D08B2E4EDB
SHA-256:	8B46B1DBEA36F612C2C9BF18D4A9A68C6456E2C82EAB00729A32B255344546B9
SHA-512:	E86F97A85F89EEEDA24449080D8099C6501A2B4A29ACAF4B2847B5EC3285103FF38F78726404DD0249F62AF3400C58766BBC40062F1117CF87070978A47AEC0B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....o$/....."#.D~.|3.6.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....u.X.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....o$/....."#.D..u4.6.A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..s ..o$/....."#.D.9.5.6.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.6075274034418925
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXI8a1QPLr1TK6t4emDEYOFLvEWXIe921QPLr1TK6tU/2mDEYOFLvj:xqTnaCPLnm5qTCCPLny/BqTr2CPLnr
MD5:	0553DA8FD4F7DE2E3F9BAA9829F7782E
SHA1:	8127F9552690250E7DC4EA9C8875AE832329341F
SHA-256:	C22344F0627A301F18496B91458E5B38EE7D94BFF2DD775D581F8A39C0496AAF
SHA-512:	F3F6C6FE2B10FE337B079F98F440348649092005D0EF843D647CB75893B51B7ECDB424DF6B0FE09984A64F9A9304E6A42B16FA57F87A9DC6C3CCEF28A02306B5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .w...o$/....."#.DIgu3.6.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....i.o.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...o$/....."#.D^.m4.6.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....%j.....0\r..m.....:....f....._keyht tps://rna-resource.acrobat.com/static/js/config.js .....o$/....."#.D,..5.6.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.600585035304388
Encrypted:	false
SSDEEP:	12:zRMgQfLsDwtjRMUCROfLsD+RMKuBfLsD:zxXDQj0HD+M+D
MD5:	923BFD208C809D0B9A54B7D5C08A8E36
SHA1:	D036D97919567A67942057E87DCACE15D0DDE1DB
SHA-256:	50541B1F07946A881A7122FAF5F4CC94511A90AABC10AD4BC44CA7FD51CA569C
SHA-512:	5B936EE11CCA8E9F4C3C172DC33741B4532BB923A7C8054B4AA383489F030AC77A4974911335AB2D91FC709BE7DECC86073D42F289A93A627A06B87A5F092EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....o$/....."#.D...3.6.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ....Z.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .J...o$/....."#.D..{4.6.A..z._a...'.v.....4p3..1.']...A..Eo.....A.. Eo.....i.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....o$/....."#.D..15.6.A..z._a...'.v.....4p3..1.']...A..Eo..... A..Eo....._.W.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.622604084742001
Encrypted:	false
SSDEEP:	12:6lJRt+TFoMKclJRojacFoMPlJRQcCFoM:Y+FoMdqRFoMbWcCFoM
MD5:	B63CB56DA539B376FC5A6ABEBDAFC8A3
SHA1:	B93B6A4740808A948B0CDE3A0A4B2919026825FD
SHA-256:	20411B13B0FC52BCDFEB2A4FB30CB90EA413DC3320D50CD52EDC6F75DC31067F
SHA-512:	3D17489B0DD457A7E82EA8D19AE4DFA445886B8520A410601D3FD23A3C374D2CBAB2F6640494F44E2EEB67B4E57A18A3BEE2FF23DB2EFA8B25B131F6F5793F5 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .....o$/....."#.D..3.6.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo ......W.wa.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .$...o$/....."#.D.P{4.6.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..... .....A..Eo.....M.....0\r..m.....R....\|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .>...o$/....."#.D..15.6.Ac}.H7M=M..-.....Ix..R.l. ..}Rl.$q.A..Eo.....A..Eo.....HX.C.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.64016667948459
Encrypted:	false
SSDEEP:	12:F8hRrROk/SpQUzce2Z8hRrROk/3xQLe238hRrROk/FAt91e2E:UPJ/SL2gPJ/3xv2iPJ/6vw2E
MD5:	B13631B00D44B3A978BA4E6BCEA9103F
SHA1:	0DD625E59983A1207D2CB77EC87616DC1D8CB2AC
SHA-256:	713B6F07587739E3C75D37A69C4C00237DD96603972BC3F814171232FA377595
SHA-512:	D7826561004FD009F18E39FE4336AD49F0093BABF6A9D784929B5A59E0EB134A68E44F7724484CF9FC1A67513A7CDC1E205DAC85937578F93F0FF75AF703DAE2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..(..o$/....."#.D..\|3.6.A..%.k.SZ..~W.....:)'B..ad.....A..Eo..... .....A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....o$/....."#.D..u4.6.A..%.k.SZ..~W.....:)' B..ad.....A..Eo.....A..Eo.....?.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..q..o$/....."#. D.%.5.6.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....ZtC.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Category:	dropped
Size (bytes):	639
Entropy (8bit):	5.698159931282341
Encrypted:	false
SSDEEP:	12:ehRceBXqrNJICghRcNcYrNJICDGhRcXCrNJIC:ehROJICghOJICDGhZJIC
MD5:	DC4FFDE3C1884A8745515784B56CC011
SHA1:	F728E26E245C631F470BC5CB403EC81BE6062E6B
SHA-256:	399ECACECD10D68419096A2B2973A23E384BA37276E299A66657CFA061096044
SHA-512:	EDCADD624839B8257C33324B8F19F980478142B4CC952A8449B110DB56DE395F3A3F00D9063D95C5178E8FC66FB661817114EE2B51DB4733425055E5BEF5DCD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .....o$/....."#.D.<}3.6.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....H.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..n.o$/....."#.D.Tu4.6.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.. .....A..Eo.....{d.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .....o$/....."#.D.t.5.6.A.;"./N_.,.:C..2....9L.H...3 :...A..Eo.....A..Eo.....6.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.57557187223121
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuib8/04TLzgm2d/1TK6tdOEYOFLvEWdrIhu8Wg8Lzgm2d/1TK8:0RG8/043ReZRVRegRpAiRe
MD5:	5927163763A45A94379336026A11086D
SHA1:	43E30417CD62E3C1CA9E814CD13D96C1ADCC9BFC
SHA-256:	C303BE46A05E03B8D79FB6A2A1B6266F16CF4CE237F676A2B94C55BF4D38FBED
SHA-512:	FFC391EA0FC7DAD962072ADC0E24770A95A3FCF79EB5C084ED8BDD7FAB233D5B05EC47F266B869D7FED1FCAA23DE822ABD556E8D01F1A32CFD91064C8A2E EA96
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..%..o$/....."#.D..\|3.6.AZ.Z}Q..4.o....0+..[\|.n:*..U.W.A..Eo.....A..Eo.. .....y.e.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .#..o$/....."#.D.(t4.6.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....(.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..o..o$/....."#.D...5.6.AZ.Z}Q..4.o....0+..[|..n:*..U.W. A..Eo.....A..Eo.....*r.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.6253667932712235
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KJ4q8kx56uvp1TK6t9MAElVYOFLvEW1KRgvchkx56uvp1TK6thZ:6JJKN7MJJKRgUKHgJJKZK
MD5:	633A6A7007C48416BB07687AA0538E39
SHA1:	9FEAE4A1F27260EE3305A5AA791607543188C8AC
SHA-256:	3A88361A2FABD3D63FE3D1B706B68969D68333336491FA4900400227BE3AC6DD
SHA-512:	0EAF71C8280B86CAF1DF9D6CD758F59460923756EB37A9D16D7A299710FD6FD0397C50B0A081471A489E815E67924F6B4B673FACBF9928BAB8D98CB6EDD8506
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....o$/....."#.D..O3.6.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....;..+.....0\r ..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....o$/....."#.D.zO4.6.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....k.....0\r..m..... <...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....o$/....."#.DxF.4.6.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....m.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.621068277146069
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvumc2ihUDLYtmOZn1TK6t+:xRBJ02XDcFZLE
MD5:	60A71E0BF54C3A8958294D2619772F2D
SHA1:	F930F9372B288A8646C02DB0B556DD6C4F2F72B5
SHA-256:	9CA83D40B8074FD6B502C5874E407DFAF4F6883E8FCFD7885E46DA102F5D6813

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
SHA-512:	9CFB5FE58119E27B260BB7C9D1D77632433934A66BE8464E7894D645CFD4B57FE534639DC9763A52C17218481DC592217CFA981FA617FC9FDF18587CC327C3A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .x...o$/....."#.DL.15.6.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....iv.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.6085092802866825
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7k+iMkkVPu1TK6tj1sRPYOFLvEWIa7zp7VL+hu7VPu1TK6t1:BPHyqkkc5+PHGu7cwPHnI7c5u
MD5:	15D6A962603048F5A0E9E7D78F94C9B5
SHA1:	0DE5FEC404F2BB89659E14021BF6FBA222BCDFD5
SHA-256:	77D9977B0CB3499EBCC90F5A9437B07D42C25E450CD3475C90A35DE45C10A1A5
SHA-512:	7C983611A32C6EF9F1DB218C10FC5D68A27ABF6E5203CF200E63B1D2EC6A8DEC7DABB38DCCD7EEBCE9EC4D3D8A3A79CA29749E9055B84D4A00BDC7BCC04627C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...{.j...._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..`..o$/....."#.D0.:3.6.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....c.....0\r..m.....S...{.j...._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....o$/....."#.Dh.:4.6.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....n..-.....0\r..m.....S...{.j...._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....o$/....."#.D...4.6.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....S.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.568070241144575
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVLG/G8xk144XVAZ+8cV3vRm1TK+:mKPYOFLvEWdENU9QyxPiM3Y1TK6t
MD5:	DE28044E53608C441BC2BAFE1E637E88
SHA1:	9AC8484A8E9F359ED8F2EDE4675B572AC3980EE9
SHA-256:	5AA8BB12D5B9B17E989000968E1D6C1CCA860A95DCB44FAE0B6C0FB2FB5708E2
SHA-512:	9E573857500EEED1E1BBB0B2BE20BFD64D47E94B3A28BCAEE2DB01D34BE5EFC6E869CB1655C96792FFCE87A297428D0743E6A2D91A0E3DCE115EAF31393C0225
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .$...o$/....."#.DV..5.6.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.614270435733212
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQXSTOwgjBRCh/41TK6th:XRc9ZOwgDi/E3
MD5:	3C2FE741EAC123075B6F0D522B08797F
SHA1:	3CB625F39F327919B1E545E059EDC046FFE6FB21
SHA-256:	608CD1FDF11DC6BCF864DA17E1C8809B4615B8CB6C7DC65B13101B600DEFCDF3
SHA-512:	D667DDE3DE22BF57FA196C63FFC2D3570845BEE2CB922C0DA8772444C22AC27E45683ED050E7A1FA91A9187B6BA5C95AAC85141F185844890BC6063020C473A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .H...o$/....."#.D..<5.6.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.6190384763231
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhumEULlF4r1TK6tC3qs6XYOFLvEWdFCi5mhurO5ULlF4r5:bs6xRkiSLlF4nPs6xRkigKLlF4n
MD5:	0BFE781FBE4464047A6C77A422580FD7
SHA1:	A2C5263CFA9F81CB205CE9665DCB3B5FCC87A88C
SHA-256:	381419A533AF19B2A4193F413DEC74A255038BA13FF73560B25616FC152F1669
SHA-512:	0814E63A2F3A862B14EB0A808527331568A4C6F1FDF555D3F464AE6E95FAF6A2BF0B405342DB9DBCA931D76FF67B2A13D4DFF95893D88772ABEB631744F7CB9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...o$/....."#.D#K.3.6.A.P...#4..l....5...5..).w.. .h.~ ..A..Eo.....A..Eo.....CF.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .d..o$/....."#. D..u4.6.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....X.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.46164816744069
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvRmdXHC9V4cu1isLK5m1TK5ktdl/:mhYOFLvEWd/aFu7mxC9VT941TK6t
MD5:	5EB4832D242E7CAAE57DA0A7C2930314
SHA1:	2F9E9ADAD0E6E250AB1968A3EC45A17E7D89BB8A
SHA-256:	553F20CE61C87DCCCEFE077DA221FD6312F0289C70870EAC73A121461E64A872
SHA-512:	879A4E5B5C8FF5B57E44CCC6C7DB32FED47F7E903DF124203A5C15423EBE4E935DDE88A2517AADC5434BD910CB961D5FB1243921B39BD6D1E52A54BE26AFE D8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .4. .o$/....."#.D..25.6.A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A ..Eo.....n.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.468433284876771
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQRTGUBoBMqVd3G4K41TK6tgP:2DRuRLbB9Vd2k
MD5:	3053C9937930DF389238ACBB5F82081B
SHA1:	F3A21983CEF0829F2D248E9E44E531C2D9D136BF
SHA-256:	48FA9025565E540132E711D6B459E7284BEDAFCF5A5ED2353AD44D8797643B58
SHA-512:	FD6035D428D4EEE9EED33259949D6275F84A66299C2F6E56858ADA571C4C684F2C0DF91B5F742689B7B218C198094858457C3BB1D74153CB940F304789FF3BF6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .*. .o$/....."#.Dan25.6.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. .....(.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.6190075548395395
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QRz7uA424r1TK6tzlEkqYOFLvEWd8CAd9QJ1cyxmuA424r13:+RQ+ernkRQQ1dnrnjURQjrn9
MD5:	F58B6B0906DC7EC7B64794F9F048D28B
SHA1:	22EC9220867D32F811ADD5799E82F56F3DAEEA20
SHA-256:	9AF4D39AB7C32A8055D5AAC939C8AC6A9D9B56D27539174D7A4C34270DF0C06D
SHA-512:	21599AB0CB3F0E5F4598734A33677DCFA2BEF6BA2B689236BDEA41529893EA60513ACC58D5789C1C7F1AAE036B70F469F34769C0D239ED8D1A42DB54FCD0B9 1
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..@..o$/....."#.D.c.3.6.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....S.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....o$/....."#.DL..4.6.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo..... WH.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .i. .o$/....."#.DR.<5.6.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo...../r.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.553697708132705
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuzbyC8n1TK6tnOilt:xhRThb7Q9OGt
MD5:	701C6D852A8FBDB3710775F3ABEDBADF
SHA1:	3F1089DC4CD64CC1CF83E53215F37C902A67D7A7
SHA-256:	D33D1D5BE548F4CDFB4AC76BC6CBC6DB4FA9EA954D812C5E6476FBC551BAA704
SHA-512:	BE4C5EFB4150E3097E1E5E4F558C815D2890D8692648F3F24D26B2EBDB268606695BBC5714129FAA7F3B70A3E9EF232D726FF4B3EE504BE7737129CB4130093D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..9..o$/....."#.D{3.5.6.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....*z.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.614385179951818
Encrypted:	false
SSDEEP:	12:nRrROk/Vq5Yc+mBRrROk/VzpMmeXlRrROk/VSY2Mom:nPJ/kYKBPJ/RbiPJ/R2M
MD5:	CC8E4E58E38A5FE9C6CD0729A5D43946
SHA1:	FC97B4509B833D3AC34B8306F208C38DAEF7D22F
SHA-256:	087D892B2422F630B66017C91C125DDD232F9F725E6B1D6A497F24780BACA276
SHA-512:	CFA94DB9DC8A7F5B4FBE698A6B29BDFFF9BCBD0DABD3FE31776EE9A4279BFD70362E84F921990A677481482643408212772660D51C7D47C66DC1DBA2C98599BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .C...o$/....."#.D.K}3.6.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....*.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..s.o$/....."#.DEeu4.6.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....D.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .o...o$/....." #.DQ..5.6.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....b#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.583412995165492
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuzeskGAdm9741TK6tzd:qxRcx/kGAdu7Ez
MD5:	36E475D858F910E8E190298451D5EAA1
SHA1:	48BBB9DB50C8CA55C1C1A47C02F80D6D953D5A5D
SHA-256:	E08055827733EC427E75575F1EF9927B45175DCE1B4C77AC903495B50ACB2760
SHA-512:	531C7EF868FA87AEEBA0D0F7E33CD761C86A8D523B35FA09A4C95B9BF91D7385962F963C6EE7A801EB80C30B4F39C48A930E56F3E54C92CCADCF1FB5DE15D300
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .<d..o$/....."#.D.x15.6.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.532812051454632
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvodc/hB6shoq+Nem1TK5ktz0/:mMOYOFLvEWdwAPVuKbJn1TK6tz
MD5:	CD78523D761E019C47D9D0ABC1A1A7EF
SHA1:	EDBB8BBCBF3D47BA3CF4BF7A8CA665D65057D3E0
SHA-256:	29ABDF48D4BADDC86574C0115A159421DA82B95138E9C8CC3B5E2C8213687EA3
SHA-512:	084EFA80B2D0DC9DA91925D0074D559F6468AEC196727DEB95F012EF6F311A88563C6CADA3FC6BC99330A98B9BCB65B8EA89BA169895D41CBF69DBBF995EFB 2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .`7..o$/....."#.De..5.6.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... .KY.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.62505801304337
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQzTdzhcsBXIh1TK6t+:mxRBJQwdDB0
MD5:	5EC19779C6E4BB06112392C021E54AD3
SHA1:	A91E6E4760E30DA4495374E366EA997F5D447B14
SHA-256:	79BF4EAF1A24649E24BB735E327613B860A0CBC15D413ED5F62C0D62F647D863
SHA-512:	5CC429CF169B194F6E50E8442B1FC2B509224A2E1F15217BAB7F59E6AF814F18AA6FD44A74886ED33E163762659190F6D6B3EBF6EEA7887A37B373523FD55575
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .eH .o$/....."#.D..25.6.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	684
Entropy (8bit):	5.626925480924286
Encrypted:	false
SSDEEP:	12:3RrROk/sWbBaScyRrROk/sZp6chdRrROk/sjoc:3PJ/EyPJ/8rDPJ/K
MD5:	E640F6D0A129D81E477DEC6DEF751925
SHA1:	DD5BF4DE76C6CDD3982127517870D9024C22090E
SHA-256:	FC17213A1721D072CB604AE3C1F7AA4502F2DE77D1E4C26D3DBB787E38B35FD7
SHA-512:	F260F35D7935B27851744009ABC97F03F1F2D1EA29E2304B625F7C483F533B58D447161909571C257C789164D62493869A27034592283A612C6389DA71285A1F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .$...o$/....."#.D.C~3.6.A.....9Q].8O.z....=..:.N.{....N{. A..Eo.....A..Eo.....;).....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..t.o$/....."#.D..u4 .6.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....g.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-sele ct/js/plugin.js .@...o$/....."#.DL..5.6.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....@.....

C:\Users\user\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:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	4.933170394205689
Encrypted:	false
SSDEEP:	12:klyUvgupGigSzwWTUTiEdMzlQgsSvLcdvcMfEcU5E5tPTAzQ/uVFqyEuX:qPZpgSzVTUTiEdMWgwSMtSgu7BEuX
MD5:	C59DD3B8872482BAF6E2AAD197EDA13F
SHA1:	DCD67AB0B1A7C794F08B41BCAB20F9FC88063E6D
SHA-256:	EF6E1AB3F63CB8750E8EE4C5870AD7A0E79F856CE68CCBE73832B3F19C162734
SHA-512:	51D4D9321EDAA5CFD605F27512F337B3CB608DB054DA42170A97DE77663FEC72A5697806436B7B119A853D8580D5D84E5AED468E57F0B59BAE41EB40A660189
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Reputation:	low
Preview:	....@...oy retne....)........T.....3.....o$/.....v...q.....o$/.....C..M.....k.....#...(...k.....]...I.@V.o$/.....o$/.....6<|.....o$/.....<...W..J....o$/..... .oB*....o$/.....a.....o$/.....;.y~A.....o$/.....P....V....o$/.....F..=z;.....o$/.....o.....o$/.....*.....o$/.....2q.....o$/.....Gy.'.h.....o$/.....k7A.....o$/. .....:..N.A.....o$/.....;/.....o$/.....o$/.....P[. q....o$/.....,+..._.#....o$/.....J..j.....o$/.....A?.2:.....o$/.....q.....o$/.....u\]..q....o$/.....!...0.o....o $/.....*.....o$/.....o..k.....o$/.....^.~..z.....o$/.....[.i..%.....o$/.....+.{..'....o$/.....@..x.....o$/.....*)....J:....o$/.....&.S.....o$/.....MV3.....o$/..... .+.U.!..V....o$/.....D.4.....o$/.....~.,.4>.....o$/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.259218660969952
Encrypted:	false
SSDEEP:	6:m4Pin+q2Pwkn2nKuAl9OmbnIFUtptPitZmwPtPiiFPVkwOwkn2nKuAl9OmbjLJ:dvYfHAahFUtpW/Pvr5JfHAaSJ
MD5:	E1DB42FCF89CE83A498517A602CDD489
SHA1:	8304A89BB901BF44BE5B36E690B7A100511C20F9
SHA-256:	2FC3C9386755DF8354CD13FBE0635F51316D9E9693F0FDBCF3C9D93F63416A04
SHA-512:	31E3017D398BF705D78A4313DC344BA98A7FDA2DAAEF816DF1E02F0B65D00AEB1B7712E3D03808783ABD7CB0357EDCF6C3C2ACEDFE5DE1DF29D4B60FB21E 9D1
Malicious:	false
Reputation:	low
Preview:	2021/06/28-22:27:57.992 1b78 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/06/28-22:27:57.994 1b 78 Recovering log #3.2021/06/28-22:27:57.995 1b78 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.008399703044392193
Encrypted:	false
SSDEEP:	24:TmbsmbPXytHwytHwytHwytHwytHwytHwy:TmwmEHRHRHRHRHRHRH
MD5:	05C31564F5D129E37A363E150A042D4D
SHA1:	FA62CA0C75E503D2C5E83FE48A9846CD48FFF480
SHA-256:	64044EF0EAA6C2CCA1F6D5E32B8C1AD305D642A8AF7F91C89CACC2BF8642C5D1
SHA-512:	895CB367D69A3A2D619868DBDA6DA0EB5FFDC20D6B9B2740E7CAE3F9ED91F29BFB9DBA5FA68E72998E92AE68B66BAB551A53B48575B3CD1C27ABE3C923E1F DAA
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....).0k.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210628213639Z-225.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	0.8472086746898779
Encrypted:	false
SSDEEP:	96:Yu70k3kGM6KjLMNMMMEMMMeMMiMf9Q3KYGt9XakGng673koE8W:Yu7hkH6KjAO3KT9Xak6g679E8W
MD5:	1055D11813EFE9205962259949194741
SHA1:	B07665F4649A0131B066CE12B88E878FEFA50596
SHA-256:	52A51394AF040A43F3FE0C82C5677F32EF289F93543C31D221686E7C7264B5DA
SHA-512:	E2FF1E353A5A26461037C2257258E2285EC4744D247EC425F7F6D33850C3CE4DBCDC7C57ED6E5221338ECC74A52CA77DE7340C0F8A5E4380892F406A40B3E95
Malicious:	false
Reputation:	low
Preview:	BM.....6...(...u...h.... .....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4512866868935514
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CKB49IVXEBodRBkWCgrOh1CKx49IVXEBodRBkWCgrOh+:HedRBMedRBledRB2edRBb
MD5:	442A3392FA25BFF1EC9087C57F006979
SHA1:	F8B6A8F188ED0DB74215A56179A25C626F8D7937
SHA-256:	0F439BD4C67B194EB562DB972BB0F0132E9181846BFF8700CDBFE93C13BF0E7B
SHA-512:	8E71F4ED9F10B9029CEFD0FAE470C2F61132455E239B43183F5C17F58FB77E164B3DB033505DA97EDC397AF4A14E0E46DFDDA62FB54EE47F14E8D262D45D8F(4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.316438261067227
Encrypted:	false
SSDEEP:	96:RCgOOhZCPl949IVXEBodRBkeCgOOh1CKxt49IVXEBodRBk8ACgrOh1CKOd49IVXs:CiedRBzSedRBOCedRBeyedRBh
MD5:	C31FD5AB5CFADF1EDA275408FCA9F2B1
SHA1:	4602D9F5CEA0D32FDF46FC04D73039BD92B2921E
SHA-256:	ABF41A25F961556D3CB5378E1D187BB9451EC272A6BB2F77B688CB814C23DB88
SHA-512:	C30F24B886EDF6C1D5BE034E74F500927D52BE02D66DA6592DA95B3333F5BF33A02C4A1A6BC0FC059DA7744ABDBBC13DE4808690662346E06D3550C3898072
Malicious:	false
Reputation:	low
Preview:	.....Lp_..... .....W....X.W .L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4244	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6E B8
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.Na meArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleN ame:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.N ameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-Bold MT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.4244	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.4244	
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMIzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\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):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0Z6PGfAf99clajFCyKBNsIMk1wO/Yyu:J0GpiyVFih6ufAf9GDBNPMkbK
MD5:	AED51F94F257BDA3834B6861C33A1C9E
SHA1:	90A26B1890E98554F317E3781D24ACEAC3896CFA
SHA-256:	657F858BE441E2D2605B359C3F1B95051EEC188FDD3E5B6D4137C103ACD891EC
SHA-512:	CE425536C46F89CC4CFA29958F2DD9E17226381D33CAAABF52DF89EA304E9B54572190D5E352E5F0783EBF47DF6275702FBBD159567B15C04495B4F3397E9762
Malicious:	false
Reputation:	low
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.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-B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3B83DA5F-D84F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7938256080494313
Encrypted:	false
SSDEEP:	192:roZLTZ12OWZt3Pif6/PBPzMAPJPBUPbP1PkXPEPAaP9Pp2:roL1slLYHMrR
MD5:	6BC1D6985D3D907EFA14297EED6ED007
SHA1:	D8660D72CB52D087DB9ACFD96F89325A78621072
SHA-256:	28FD89A25DE8009E0E24A206ED710FC571A1210FE4583DFEC9632F1D70D229CE
SHA-512:	C86E490F11F147A4EA5D0533D753522E1598A312E57FA1040885242B1BB22E65B6B93C14DC859C9F6E4F379310B7EEEC1149C322C23B2A0040A85A5C0EA1B7E8
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3B83DA61-D84F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5935900811948658
Encrypted:	false
SSDEEP:	48:IwuGcpr1ZGwpaXG4pQXGrapbSTGQpB6GHHpcbTGUpQrnOGcpm:ryZ1TQZ6rBStjB2167yg

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3B83DA61-D84F-11EB-90EB-ECF4BBEA1588}.dat	
MD5:	6C36C806B9F4601FE1D5F7C98F26F521
SHA1:	BAC6461A8054229EB489064FC9E69B18E21CD680
SHA-256:	6B4B5D40E88A79FF93D971CAB30A3921270DCEC04819AD0EBC72861811EA98E3
SHA-512:	00FCE230763BFD810585AAB4B46E2670D29ADC5A8AD295D050D1565D9B4A469515117BB1AC0017FDB2633741799F6EED1CF8A3D0D07480011E3FABFE7A1C140
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GetFile[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.618436513098483
Encrypted:	false
SSDEEP:	6:AYSl0MXLxu2CAluh7FU19jtwktLMIgaA0fumnUaZbRB:zSabxiAlkBU1Lwk19UaB
MD5:	993DBD09D125CD5C7FA6AA21A16386BD
SHA1:	6078DA6DE6C544C35BD32FFFCB0558AC88B44068
SHA-256:	589A1603A7DBB984C34E7BDB167F0262AEC72BB2E0B05328EA75410F997F98A5
SHA-512:	372262E180F97B17C4371DCBD33816B53C4E9E7757BF094DBC55583B0DF5EBCF2279F1923BCEEB0807AFFE170CA9AA03953A75C35162DACAF34E6D64981003E3
Malicious:	false
Reputation:	low
Preview:	<head><title>Document Moved</title></head>.<body> Object Moved This document may be found <a HREF="https://bms.kaseya.com/media/GetFile.ashx?enc=iAIF3krAhFnrzr2%2fdZEndh%2foMj7qNe0PshuhX7KBbHtbR9vpsvc9XqhjBxH0y6QoOe1BdU1OcYCSw%2fCxijoaHl0%2faUv%2fJAurw9NEQN2A5zE%3d">here </body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf.mqkffie.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.4
Category:	dropped
Size (bytes):	17845
Entropy (8bit):	7.6453586217218605
Encrypted:	false
SSDEEP:	384:llGfuuLdu5jhxZ4owypHjjF/9gQwaC4GCA4DcKXcJoNlu38:osLdu5jhxxwKF/pwD4GL4c+3us
MD5:	BB9E07B1314958DB05E28E57CDAFB3EA
SHA1:	94B4051C8B557D875A5DDA4C6865B3C043F884CA
SHA-256:	5F544F5E6A1F6855DC058DBF566442A7538F71CC6DAF422F53B2C69FC533D586
SHA-512:	16F17FA29AED1FCFF96A58D1D3BDD4081A9BDE8488A972845BA932E5384232EBDDB3A571A7647F7BEAAC6B9C29351EC4F8B498DBB7C0FB0B7DE70ACBBD954CCD
Malicious:	false
Reputation:	low
Preview:	%PDF-1.4.%.....1 0 obj.<<./Type /Catalog./Pages 2 0 R.>>.endobj.3 0 obj.<<./ModDate <3B7D6EB216FE1A30BFDE85A88D8EFA7EEA3EADD0B234E6>./Creator <3B2230F641A40A4BEC85DBF5D2D1B66A8A5ED6D7B6>./CreationDate <3B7D6EB216FE1A30BFDE85A88D8EFA7EEA3EADD0B234E6>./Producer <161339FA50EF1828BCC887BB95DEB66AAB61ED96E56DA4E30D0A839A>./Author <0B2E28EE41F20842E892D5F2D1D9AB6A8F61EF85F124A0A30A45BCD254748471BDD336808EC5E785A5A2F4E0A7859AFE15D9D7D1F0738F9E0A4F26E32689431E5E5D7E3892EB9F09BA0768035D52479EB0CA4D049CB06EC8EA98>. >>.endobj.2 0 obj.<<./Kids [4 0 R].Type /Pages./Count 1.>>.endobj.4 0 obj.<<./Contents 5 0 R./Type /Page./Resources <<./ProcSet [/PDF /Text /ImageB /ImageC /ImageI]./Font <<./F1 6 0 R./F2 7 0 R./F3 8 0 R.>>./XObject <<./img1 9 0 R./img0 10 0 R.>>.>>./Parent 2 0 R./MediaBox [0 0 612 792].>>.endobj.5 0 obj.<<./Length 1165./Filter /FlateDecode.>>.stream...P..*j..DMsVLR...P.=.6.k.`s..K..3...9D.B.I...a.J..z....w.[..2.f.|...40t.....A.....M.....?i....0.....9!..''..O....e.....b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf.mqkffie.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf.mqkffie.partial:Zone.Identifier	
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D1279902724145098065199450142 3A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dffa983a-7248-493b-8e1c-28fd79d790ab[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.4
Category:	dropped
Size (bytes):	17845
Entropy (8bit):	7.6453586217218605
Encrypted:	false
SSDEEP:	384:llGfuuLdu5jhxZ4owypHjjF/9gQwaC4GCA4DcKXcJoNlu38:osLdu5jhxxwKF/pwD4GL4c+3us
MD5:	BB9E07B1314958DB05E28E57CDAFB3EA
SHA1:	94B4051C8B557D875A5DDA4C6865B3C043F884CA
SHA-256:	5F544F5E6A1F6855DC058DBF566442A7538F71CC6DAF422F53B2C69FC533D586
SHA-512:	16F17FA29AED1FCFF96A58D1D3BDD4081A9BDE8488A972845BA932E5384232EBDDB3A571A7647F7BEAAC6B9C29351EC4F8B498DBB7C0FB0B7DE70ACBBD954 CCD
Malicious:	false
Reputation:	low
Preview:	%PDF-1.4.%.....1 0 obj.<<./Type /Catalog./Pages 2 0 R.>>.endobj.3 0 obj.<<./ModDate <3B7D6EB216FE1A30BFDE85A88D8EFA7EEA3EADD0B234E6>./Creator <3B2230F641A40A4BEC85DBF5D2D1B66A8A5ED6D7B6>./CreationDate <3B7D6EB216FE1A30BFDE85A88D8EFA7EEA3EADD0B234E6>./Producer <161339FA5 0EF1828BCC887BB95DEB66AAB61ED96E56DA4E30D0A839A>./Author <0B2E28EE41F20842E892D5F2D1D9AB6A8F61EF85F124A0A30A45BCD2547484 71BDD336808EC5E785A5A2F4E0A7859AFE15D9D7D1F0738F9E0A4F26E32689431E5E5D7E3892EB9F09BA0768035D52479EB0CA4D049CB06EC8EA98>. >>.endobj.2 0 obj.<<./Kids [4 0 R].Type /Pages./Count 1.>>.endobj.4 0 obj.<<./Contents 5 0 R./Type /Page./Resources <<./ProcSet [/PDF /Text /ImageB /ImageC /Im ageI]./Font <<./F1 6 0 R./F2 7 0 R./F3 8 0 R.>>./XObject <<./img1 9 0 R./img0 10 0 R.>>.>>./Parent 2 0 R./MediaBox [0 0 612 792].>>.endobj.5 0 obj.<<./Length 11 65./Filter /FlateDecode.>>.stream...P..*j..DMsVLR...P.=.6.k.`s..K..3...9D.B.I...a.J..z....w.[..2.f.|...40t.....A.....M.....?i....0.....9!..''..O....e.....b

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.366670544419046
Encrypted:	false
SSDEEP:	3:oVXUbXH/cx008JOGXnEbXH/cx0vun:o9UD0xlqED0xEu
MD5:	3A54D7E87934C2AC399DEF4E1F7F5A34
SHA1:	4154E3ADC7E5BCF8FA8E9E3A44D916D97359D769
SHA-256:	66F2D8D151D90806337437CD5781A2CDADEA43A0D2B12C7443718479266F5B35
SHA-512:	72CAFA77CE259CF82E8D3A0A5D6E2B32D03D8C83587E873B0717F17CAA79DE2D4817AE5FA38E510F42413882EBC7978B3F476A4F2CFA086496D4800666505DF
Malicious:	false
Reputation:	low
Preview:	[2021/06/28 22:27:19.806] Latest deploy version: ..[2021/06/28 22:27:19.806] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF50DFDE34EA9244B9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989

C:\Users\user\AppData\Local\Temp\~DF50DFDE34EA9244B9.TMP	
Entropy (8bit):	0.3291978434531541
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwx9lw6k9l23/9l2P9l5:kBqoxKAuvScS+iE3+Cry
MD5:	9BE3E1922A9765523BDB110097BCEAA0
SHA1:	95C4500327265479ECFB4A4486BFF065C343D3B0
SHA-256:	38A833C9318E09823401CE0124CE9AD3333E5B8055F7E1263BB6234927893E73
SHA-512:	8E49EE3E6F536FE8743AF288A6F90058D7A318C720B6FF7DC7272A6580EC73767276576817920857 6A19CBC67DE2BF1294DBBF3795B070A4ED9E307461C4EF51
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF87D44F45FD4D4F92.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.44315310457304546
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lovS9lovC9lWvbh2OhKlKF3:kBqolvdvbvbh2OhKlKF3
MD5:	0289F667939CBC2F55B26007E6949AD6
SHA1:	A88BB77C96C9657035C8FD45ECAB8E0CC4B8BF7F
SHA-256:	96A084C3EC86E17C34CFBEA0BAA46A821E61CDC1348415AAC2E88127209558DC
SHA-512:	EE097A7A433A4001EC995C1120BCD4904A3E992FA9E7BEF4750977FCFE17F4743E18E6872DA8999020CA79A2D0D2D23AA411834C2F12E777983908FCB77E27C5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\JSCache\GlobSettings	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text
Category:	modified
Size (bytes):	24
Entropy (8bit):	3.66829583405449
Encrypted:	false
SSDEEP:	3:So6FwHn:So6FwHn
MD5:	DD4A3BD8B9FF61628346391EA9987E1D
SHA1:	474076C122CACAAF112469FC62976BB69187AA2B
SHA-256:	7C22C759CA704106556BBC4FC10B7F53404CA1F8B40F01038D3F7C4B8183F486
SHA-512:	FDAF3D9F8072ED7DE9B2528376C10E3C3FDBEA74347710A4795BECF23C6577B3582B2E89D3C04EF0523C98FE0A46F2AF3629490701A20B848C63BA7B26579491
Malicious:	false
Reputation:	low
Preview:	<</Settings [/c <<>>].>>

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	6.934613832614919
Encrypted:	false
SSDEEP:	3:Nlm3TnZ1PWNmIkP/wkIQOpVou3ms8xKGL8sP8PJJYwfZEmaNAkIidQPeuWr2DW:wdKinJ+VFWVxvRPAYwfZEmapQHu7W
MD5:	5899D998731A4A9337869D49C04FD8DB
SHA1:	15859C86F73A4F8DFEF2C64F4A9833F02242D893
SHA-256:	A0127D63E20482835F839E787AC3B684BD65EF1FDD1D381810240E3F94876AB6
SHA-512:	2C4010EF24D15FEF70055980FCC4927CF629ADB9A5820D3A0670FF4542F6A39633D3198F2684A2B0A8F319BB315F80E062307419662723D020FD2F6D49BE89F1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store	
Preview:	...S.v...:@..hC-.H.QE..|....l.s......0...!.k..'T.U.......epaCp\fw.f+.......U.h3..s..+1.M`-..`.....Y.d.{....C.....I*.....lM..=B.]QV..F...)'....^.2........._CR...Y.....m.C..|......q.?.u.{....X.J..J

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	MS Windows COFF PA-RISC object file
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	7.8586600085802205
Encrypted:	false
SSDEEP:	24:FDVDuHh0UDvNs90LbglAUnYn/fVtBUG6/HOKZP2ZWedbpUQK:FDVQh0IseHGRc/TBW/uKUEY2t
MD5:	F4DA58794E43BC05D7FBFB49300A3D25
SHA1:	A089EB6F634C19B95A804EBBDDB8854316DD87AF
SHA-256:	B81A2359D689BF6611E529F93A285E3E1827D07E8953DFA92CDE0F85646136C0
SHA-512:	8374395D425C550F42DDE0FB614B0918BD61FA763B2A94A32FCB8EA913CDC97A8FD6202FE6D5EA01A4204DE5213A1140C91D9639585408C198AF9D8591198C6
Malicious:	false
Reputation:	low
Preview:	.....J0....^RS.BXQ$i.....e._.=#T.e.Z.<.t"5.y..X..X...Wa.....2...0em-...N.&wK.....L.^.X...s.k.fP...W..<yM..S.....<].tT....v..3h...g...:[W...Z-:.q..D.:e..z..>.8w..z..?....F{.n.. ....rP....T8.f ..1..v..v..:O(.....$....J.E.7.!..I...>.,...3.D...{....k%..g.....ye.....5..NY2.5.4...b.....~.VEjx..U.....S....6q.:.RDVJ..0.:LDq..c...]^.....-.U..$-....E.....M.....).i$...'=F_....T^..&.V.U.MX.; .....R..h..o.....6.R...SX.....ER.Q1....<^s.zf.eb...M;..1....TX.....j.Y.{u.....i..4z\[.q.....#.ZZs.uT..(.h9...r....}.....=.RA....ZF.rc....u..t...0).`n.t).W.C...[$.},aC.6....i...?w&rB{..NH9...5.. D.'.....'..!.pB.pw..Ks.O.B.....v..>.....%..G."4)....v0..O....,(~..Ti.B;.e.....4...A;...rB..O.....2..]...W.S..Bu.....b.}...9...].dVER.o....:..j.&...:&.)..''<....8....:...$.6yI....4:W.`..... ..VIc....|.c;...:..xR+K.d....4:~..*MVs.%.rO...b.....J..F....H.Rk.o.0..Pi.....<_..C.....*kB".y.L..o....J....^.....H.7..4n..Z..&...o.....pV....r..f.}....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 28, 2021 22:27:20.672254086 CEST	192.168.2.4	8.8.8.8	0x747f	Standard query (0)	bms.kaseya.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 22:27:20.733299971 CEST	8.8.8.8	192.168.2.4	0x747f	No error (0)	bms.kaseya.com	origin-bms.kaseya.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 22:27:20.733299971 CEST	8.8.8.8	192.168.2.4	0x747f	No error (0)	origin-bms.kaseya.com		52.144.52.222	A (IP address)	IN (0x0001)
Jun 28, 2021 22:27:20.733299971 CEST	8.8.8.8	192.168.2.4	0x747f	No error (0)	origin-bms.kaseya.com		52.144.52.223	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6776 Parent PID: 800

General

Start time:	22:27:18
Start date:	28/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff712e00000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6828 Parent PID: 6776

General

Start time:	22:27:19
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6776 CREDAT:17410 /prefetch:2
Imagebase:	0x1380000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: AcroRd32.exe PID: 5148 Parent PID: 6776

General

Start time:	22:27:43
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf'
Imagebase:	0x1200000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Moved

Registry Activities

Show Windows behavior

Key Created

Analysis Process: AcroRd32.exe PID: 4244 Parent PID: 5148

General

Start time:	22:27:44
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dffa983a-7248-493b-8e1c-28fd79d790ab.pdf'
Imagebase:	0x1200000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6472 Parent PID: 5148

General

Start time:	22:27:51
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043

Imagebase:	0xf00000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: RdrCEF.exe PID: 6584 Parent PID: 6472

General

Start time:	22:27:54
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5642234162136683367 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=5642234162136683367 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf00000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6416 Parent PID: 6472

General

Start time:	22:27:56
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1676,13757733991334525867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=6949978120898280864 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xf00000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6960 Parent PID: 6472

General

Start time:	22:27:58
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,137577339913345 25867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=348665043263964070 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=348665043263964070 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf00000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 7092 Parent PID: 6472

General

Start time:	22:28:01
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1676,137577339913345 25867,7786359997496625938,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12973235889727847520 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=12973235889727847520 --renderer-client-id=5 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf00000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Disassembly