ID: 338156
Cookbook: browseurl.jbs
Time: 18:23:54
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report http://pukacreations.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 5
Sigma Overview 5
Signature Overview 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 12
Private 12
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 46
No static file info 46
Network Behavior 46
Network Port Distribution 46
TCP Packets 47
UDP Packets 48
DNS Queries 50
DNS Answers 50
HTTP Request Dependency Graph 51
HTTP Packets 51
HTTPS Packets 54
Code Manipulations 57
Statistics 57
Behavior 57
System Behavior 58
Analysis Process: iexplore.exe PID: 4308 Parent PID: 792 58

General 58
File Activities 58
Registry Activities 58
Analysis Process: iexplore.exe PID: 1532 Parent PID: 4308 58
General 59
File Activities 59
Registry Activities 59
Analysis Process: AcroRd32.exe PID: 4912 Parent PID: 1532 59
General 59
File Activities 59
File Created 59
File Moved 61
File Read 61
Registry Activities 61
Key Created 62
Analysis Process: AcroRd32.exe PID: 4900 Parent PID: 4912 62
General 62
File Activities 62
Registry Activities 62
Analysis Process: RdrCEF.exe PID: 2156 Parent PID: 4912 62
General 62
File Activities 63
File Read 63
Analysis Process: RdrCEF.exe PID: 5064 Parent PID: 2156 67
General 67
File Activities 67
Analysis Process: RdrCEF.exe PID: 7004 Parent PID: 2156 67
General 67
File Activities 68
Analysis Process: RdrCEF.exe PID: 5004 Parent PID: 2156 68
General 68
File Activities 68
Analysis Process: RdrCEF.exe PID: 7112 Parent PID: 2156 68
General 68
Disassembly 69
Code Analysis 69

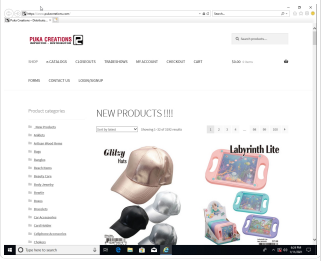
Analysis Report http://pukacreations.com

Overview

General Information

Sample URL:	http://pukacreations.com
Analysis ID:	338156

Most interesting Screenshot:



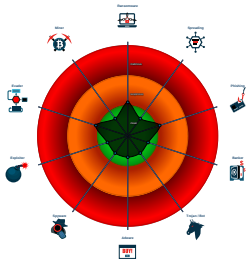
Detection

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

Signatures

Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4308 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 4912 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 1532 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 4900 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 1532 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - RdrCEF.exe (PID: 2156 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5064 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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12005084913169748714 --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=12005084913169748714 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 7004 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1716,614424777208045058,2165266707099322910,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9562498448811396969 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5004 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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13399235510371959462 --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=13399235510371959462 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 7112 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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6053178819435376673 --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=6053178819435376673 --renderer-client-id=5 --mojo-platform-channel-handle=2120 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

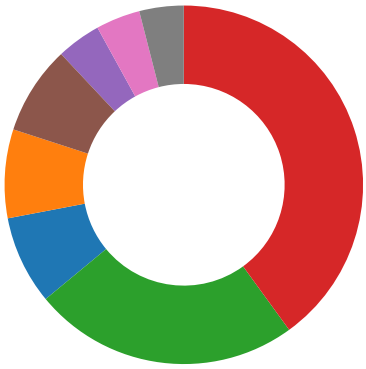
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Phishing
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

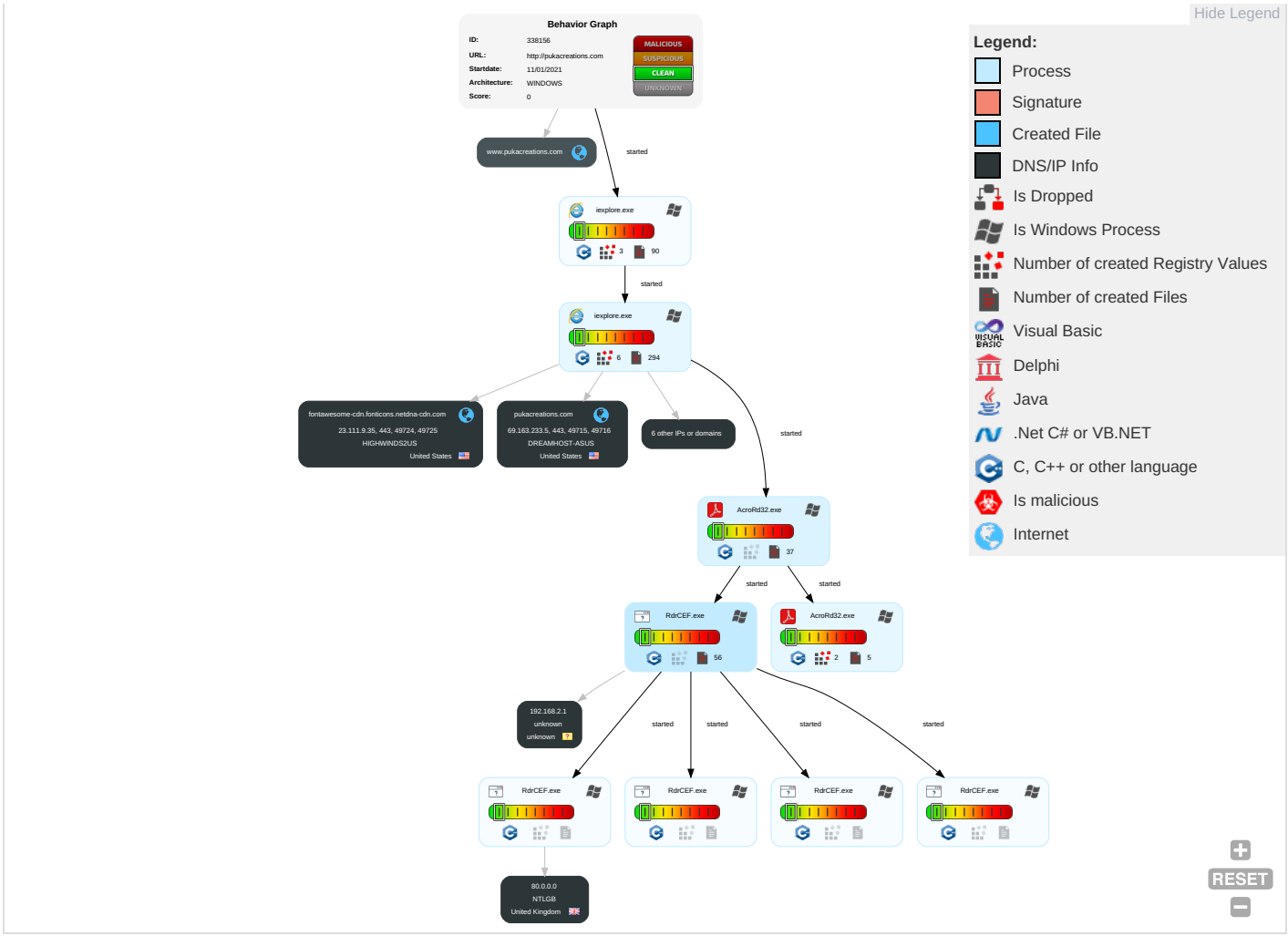
Click to jump to signature section

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

Mitre Att&ck Matrix

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

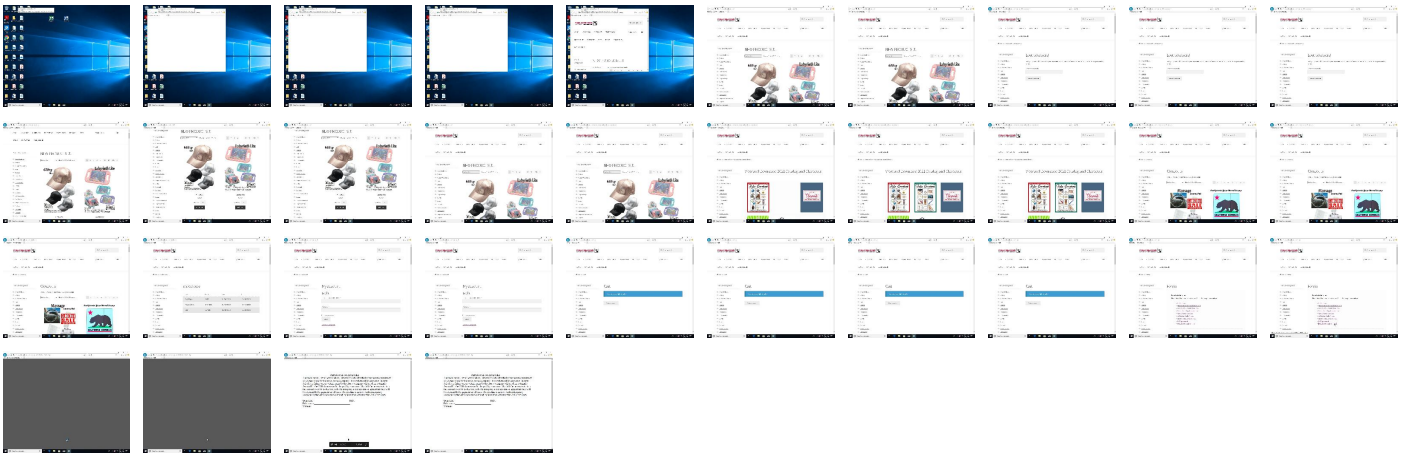
Behavior Graph

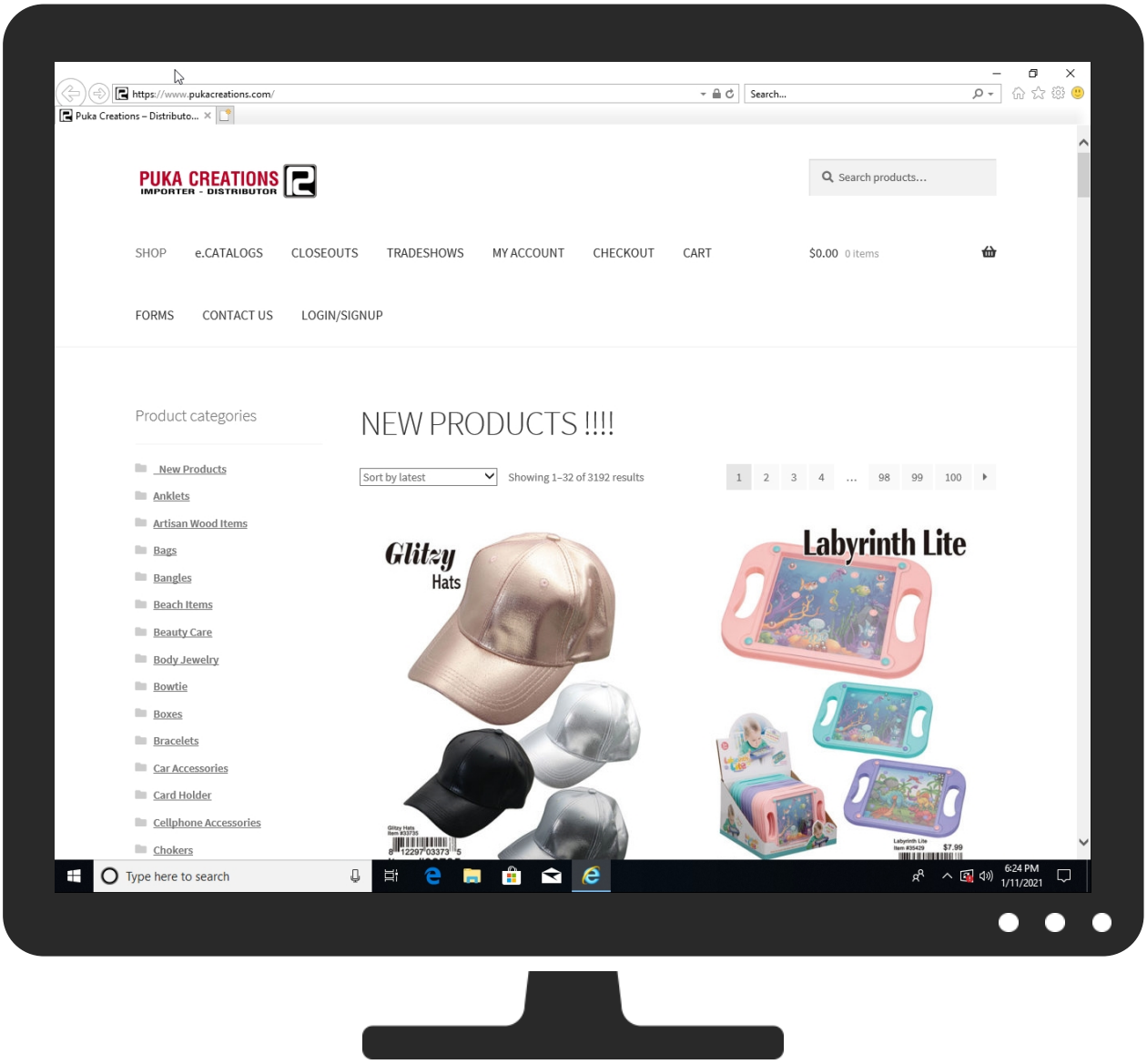


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://pukacreations.com	0%	Virustotal		Browse
http://pukacreations.com	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
http://https://www.pukacreations.com/media/Toys-32684-Walking-Pet-Dog-12-100-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Beauty-17121-Massage-Steering-Pad-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/closeouts/page/10/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.pukacreations.com/media/0000.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/emotions/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-content/plugins/jetpack/css/jetpack.css?ver=8.0	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-2-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-3-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/starfish-bling-bracelets/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Wallets-08500-Glitter-Girl-Wallets-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-5-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/contact-lens-holder/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/00000-1-Natura-1-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/vests/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-includes/js/jquery/ui/effect-slide.min.js?ver=1.11.4	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/39997-Sand-Dollar-Bracelets-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-9-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-7-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Bracelets-13376-Porcupine-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/japanese-beads-and-crystal-bracelets/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/uncategorized/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/wood-cat-figurines/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/hair-accessories/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/colorful-sea-life-earrings/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Bracelets-08173-The-Bangle-Collection-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Necklace-CL-CHCC-1-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/50770-SunMoon-Bracelets-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-13.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/cropped-header1-270x270.png	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/contact-us/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/0001-6-scaled.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/my-account/lost-password/6My	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/sarong-instruction-video/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-10-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/000001-Cover-215x300.jpg	0%	Avira URL Cloud	safe	
http://pukacreations.com/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/0001-5.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/pins/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/trump-items/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-11-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/register/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/39966-Ocean-Anklet-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/card-holder/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-12-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/00001-2-223x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/39959-Ocean-Bracelets-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-13-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-3.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/36191-Ocean-Earrings-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Cellphone-09699-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-content/themes/storefront/assets/js/footer.min.js?ver=2.5.3-b-modif	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/closeouts/d-closeouts/zz	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/tradeshows/gory/closeouts/d-closeouts/t	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/00001-Candy-Skull-Coin-Purses-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/cross-tribal-bracelet/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/50176-Crescent-Anklet-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product/florida-bottle-cap-shaped-bottle-openers/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Beads-SPRTB-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/water-essentials/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/KC-33162-Tropical-Key-Chain-72-36-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-1-416x579.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-760x1024.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?v	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/css/select2.css?ver=3.8.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.pukacreations.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/Home-Florida-Coasters-324x486.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/beauty-care/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/cropped-header1-32x32.png	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/00001-2-761x1024.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.2.2	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/view-and-download-catalog-and-closeouts/feed/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/001-scaled.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/00001-1-416x579.jpg	0%	Avira URL Cloud	safe	
http://pukacreations.com/documents/CreditTermsApplication.pdf	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/rings/	0%	Avira URL Cloud	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://www.pukacreations.com/media/0000-215x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/product-category/miscellaneous/	0%	Avira URL Cloud	safe	
http://https://www.pukacreations.com/media/0001-5-180x251.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stats.wp.com	192.0.76.3	true	false		high
secure.gravatar.com	192.0.73.2	true	false		high
www.pukacreations.com	69.163.233.5	true	false		unknown
pixel.wp.com	192.0.76.3	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
s0.wp.com	192.0.77.32	true	false		high
pukacreations.com	69.163.233.5	true	false		unknown
use.fontawesome.com	unknown	unknown	false		high

Contacted URLs

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

URLs from Memory and Binaries

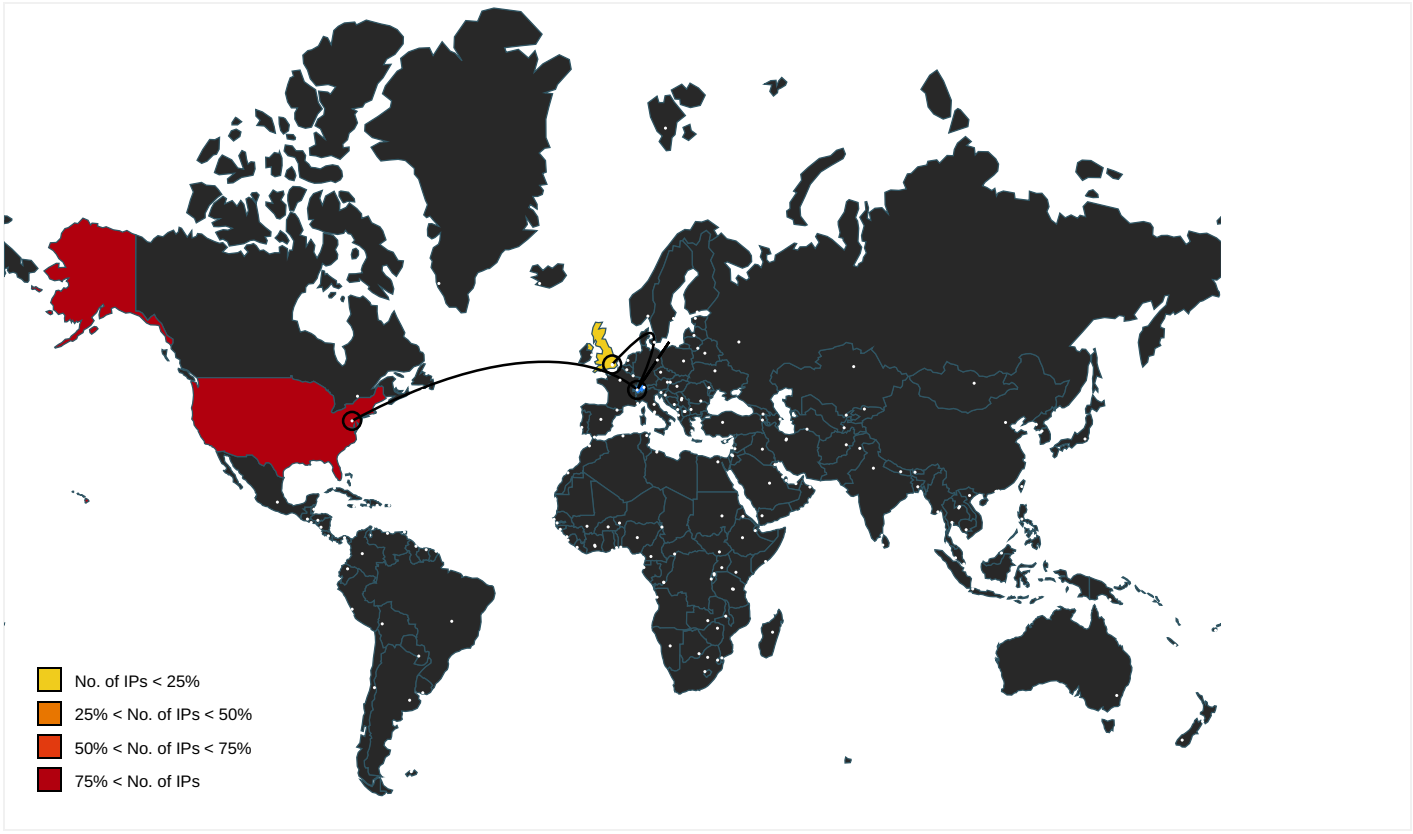
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pukacreations.com/media/Toys-32684-Walking-Pet-Dog-12-100-324x486.jpg	3DMDYVEO.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Beauty-17121-Massage-Steering-Pad-324x486.jpg	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/closeouts/page/10/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://wp.me/P9DuN9-16l	forms[1].htm.2.dr	false		high
http://https://www.pukacreations.com/media/0000.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/emotions/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-content/plugins/jetpack/css/jetpack.css?ver=8.0	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-2-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-3-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product/starfish-bling-bracelets/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Wallets-08500-Glitter-Girl-Wallets-324x486.jpg	cart[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-5-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pukacreations.com/product/contact-lens-holder/	forms[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/00000-1-Natura-1-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/vests/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-includes/js/jquery/ui/effect-slide.min.js?ver=1.11.4	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/jquery/jquery-color	effect.min[1].js.2.dr	false		high
http://https://www.pukacreations.com/media/39997-Sand-Dollar-Bracelets-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.comhttps://fontawesome.comFont	fa-solid-900[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-9-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-7-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Bracelets-13376-Porcupine-324x486.jpg	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product/japanese-beads-and-crystal-bracelets/	tradeshows[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/uncategorized/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.php	jquery.blockUI.min[1].js.2.dr	false		high
http://https://www.pukacreations.com/product/wood-cat-figurines/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://woocommerce.com/	style[2].css0.2.dr	false		high
http://https://www.pukacreations.com/product-category/hair-accessories/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.gravatar.com/images/grav-share-sprite.png);background-repeat:no-repeat;width:16px;hei	jetpack[1].css.2.dr	false		high
http://https://www.pukacreations.com/product/colorful-sea-life-earrings/	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Bracelets-08173-The-Bangle-Collection-324x486.jpg	cart[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Necklace-CL-CHCC-1-324x486.jpg	cart[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/50770-SunMoon-Bracelets-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-13.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/cropped-header1-270x270.png	closeouts[2].htm.2.dr, cart[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://www.pukacreations.com/contact-us/	closeouts[2].htm.2.dr, cart[1].htm.2.dr, 1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/0001-6-scaled.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://woocommerce.com/storefront/	style[2].css0.2.dr	false		high
http://https://www.pukacreations.com/my-account/lost-password/6My	{53A0A728-547D-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/sarong-instruction-video/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-10-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/000001-Cover-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/0001-5.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/pins/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/trump-items/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-11-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/register/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/39966-Ocean-Anklet-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/card-holder/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-12-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/00001-2-223x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/39959-Ocean-Bracelets-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://gmpg.org/xfn/11	closeouts[2].htm.2.dr	false		high
http://https://issuu.com/pukacreations/docs/2021catalog?fr=sZWU0MjEwMDIz	forms[1].htm.2.dr, view-and-download-catalog-and-closeouts[1].htm.2.dr	false		high
http://https://www.pukacreations.com/media/001-13-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-3.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/36191-Ocean-Earrings-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Cellphone-09699-324x486.jpg	cart[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-content/themes/storefront/assets/js/footer.min.js?ver=2.5.3-b-modif	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/closeouts/d-closeouts/zz	~DFBD539B381081B13B.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/tradeshows/gory/closeouts/d-closeouts/t	~DFBD539B381081B13B.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://issuu.com/pukacreations/docs/catalog-steelwear?fr=sZjU4MzEwMDIz	view-and-download-catalog-and-closeouts[1].htm.2.dr	false		high
http://https://www.pukacreations.com/media/00001-Candy-Skull-Coin-Purses-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product/cross-tribal-bracelet/	lost-password[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/50176-Crescent-Anklet-324x486.jpg	1Q8IZK6M.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://malsup.com/jquery/block/	jquery.blockUI.min[1].js.2.dr	false		high
http://https://www.pukacreations.com/product/florida-bottle-cap-shaped-bottle-openers/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Beads-SPRTB-324x486.jpg	forms[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000017.00000002.484950796.00000000099B0000.00000004.00000001.sdmp	false		high
http://https://www.pukacreations.com/product-category/water-essentials/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://issuu.com/pukacreations/docs/catalog-friendship_bracelets?fr=sY2EzZDEwMDIz	view-and-download-catalog-and-closeouts[1].htm.2.dr	false		high
http://https://wordpress.com/i/noticons/Noticons.woff)	jetpack[1].css.2.dr	false		high
http://https://www.pukacreations.com/media/KC-33162-Tropical-Key-Chain-72-36-324x486.jpg	cart[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-1-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-760x1024.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?v	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/css/select2.css?ver=3.8.1	cart[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/xmlrpc.php?rsd	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/Home-Florida-Coasters-324x486.jpg	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/jquery/PEP	pep.min[1].js.2.dr	false		high
http://https://www.pukacreations.com/product-category/beauty-care/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/cropped-header1-32x32.png	closeouts[2].htm.2.dr, imagestore.dat.2.dr, ~DFBD539B381081B13B.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/00001-2-761x1024.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.2.2	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/view-and-download-catalog-and-closeouts/feed/	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/001-scaled.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/media/00001-1-416x579.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://pukacreations.com/documents/CreditTermsApplication.pdf	forms[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/rings/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://jacklmoore.com/colorbox	jquery.colorbox[1].js.2.dr	false		high
http://jacklmoore.com/notes/click-events/	jquery.colorbox[1].js.2.dr	false		high
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000017.00000002.478721869.0000000008090000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.pukacreations.com/media/0000-215x300.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/product-category/closeouts/	{53A0A728-547D-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		unknown
http://https://www.pukacreations.com/product-category/miscellaneous/	closeouts[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.pukacreations.com/view-and-download-catalog-and-closeouts/	{53A0A728-547D-11EB-90E4-ECF4BB862DED}.dat.1.dr, ~DFBD539B381081B13B.TMP.1.dr	false		unknown
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://www.pukacreations.com/media/0001-5-180x251.jpg	view-and-download-catalog-and-closeouts[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.9.35	unknown	United States		33438	HIGHWINDS2US	false
192.0.77.32	unknown	United States		2635	AUTOMATTICUS	false
192.0.76.3	unknown	United States		2635	AUTOMATTICUS	false
69.163.233.5	unknown	United States		26347	DREAMHOST-ASUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false
192.0.73.2	unknown	United States		2635	AUTOMATTICUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338156
Start date:	11.01.2021
Start time:	18:23:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://pukacreations.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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@17/305@8/7
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.pukacreations.com/my-account/lost-password/ • Browsing link: https://www.pukacreations.com/#site-navigation • Browsing link: https://www.pukacreations.com/#content • Browsing link: https://www.pukacreations.com/ • Browsing link: https://www.pukacreations.com/view-and-download-catalog-and-closeouts/ • Browsing link: http://www.pukacreations.com/product-category/closeouts/ • Browsing link: http://www.pukacreations.com/tradeshows/ • Browsing link: https://www.pukacreations.com/my-account/ • Browsing link: https://www.pukacreations.com/checkout/ • Browsing link: https://www.pukacreations.com/cart/ • Browsing link: https://www.pukacreations.com/forms/

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 88.221.62.148, 172.217.20.234, 172.217.23.40, 172.217.23.67, 172.217.23.46, 13.107.5.88, 13.107.42.23, 93.184.220.29, 51.103.5.186, 23.210.248.85, 51.104.139.180, 152.199.19.161, 92.122.213.194, 92.122.213.247, 20.54.26.129, 23.211.4.250, 2.20.143.130, 2.20.142.203, 51.104.144.132 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, e11290.dspg.akamaiedge.net, ocsp.digicert.com, a122.dscd.akamai.net, watson.telemetry.microsoft.com, www.google-analytics.com, fonts.googleapis.com, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, e4578.dscb.akamaiedge.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, www.googletagmanager.com, emea1.notify.windows.com.akadns.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, client.wns.windows.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, armmf.adobe.com, go.microsoft.com.edgekey.net, l-0014.l-msedge.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtSetInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:26:32	API Interceptor	3x 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):	410
Entropy (8bit):	5.644665941240034
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Qyy0i7Z+P41TK6tr8en9YOFLvEWdM9Q6zx50i7Z+P41TK6tHI:vDRM96ZiEHDRM9PjZiEG
MD5:	96E9F3B6B1B4C23D017F012565628CC4
SHA1:	979E98700610C36C87538360B3CD99A5C71D96D5
SHA-256:	82BF7B57061B4A5E96EEE1708BBB86B68DE447B9D6C6B4339A7A805FD476635A
SHA-512:	3D2A3134C14F1DDC2555E10432687E10D0E08743CC8EB088ED068509C1D807F5AF0A0775C1F9CD5AD2FA79EE45897DF0EA16E2A10C5A422FE851E114DB4381
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..kL.A./....."#.D*.s8B..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....X.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....A./....."#.D.Z.9B..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....]4.....

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):	348
Entropy (8bit):	5.604779935338469
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEk3OXIeii8Be7Ywcr1TK6tui9NqEYOFLvEkbvsOb/ni8Be7Ywcr13:V9zXO19PQf9z7vbi9PQ
MD5:	1AF6C6A79D4444F1699D2C7998E442E3
SHA1:	D0917B119FDECAB4D7EE8C96CE86F72406D63743
SHA-256:	3B458E8ADAAE79B9DA84D590D8EE72F637E58D9553C5D0DA102D46FACA32F77A
SHA-512:	2A8A218D9BDC32CD70ACCFD40E5E76D75988C929543577A652AB9EEAFBE86F85F53CBB15D21BDF7D587C1AA9F6C2CCBDBAAFCCD99B33DA925A2D1769E938D144
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..+<.A./....."#.D.;,8B..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....40$@.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .T:b.A./....."#.D...8B..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....3.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.627866592394674
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFpkbNBblUo6jW7yeRVFAFjVFAFVKSBblUo6j:tB4v4KZpSBWFB4v4YSpSB
MD5:	FAE49D21346ABEBA20ED1E3A4C416182
SHA1:	B3D621A40B6FBB8A209BB715AFF45AFB788C8BF2
SHA-256:	5BC8C1E3D8815029D4032CA6C573A13A1AECBFA4BEBFA11941F3152068309CE4
SHA-512:	86A842AAE2E62EE23E0F7EECCD51F924F6CBF3AAE43AB1D27B7427B522B4B6E73414EDE68C035981BEB71FDDB5127FAD8A3E22938E01BE5B1077A668E6517520
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 ..K.A./....."#.D..q8B..A..hvD O.N.t@.....n.*..... ....A..Eo.....A..Eo....._.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js /home-view/selector.js .>...A./....."#.D..9B..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....<.....

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):	232
Entropy (8bit):	5.658640008154909
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rs5lKOBVwciWulHyA1TK6t:IbRkiDZNWuss
MD5:	81246B184E26362682FE565E57CE4923
SHA1:	E238BBA920D9DFA9AA661DFB64BB592F80A428DA
SHA-256:	46B01B76BA267DE3F19D4CF3E03B503ABA7A2F6C2593FB74F033615A29B9873D
SHA-512:	907E907F8D94F4D21C45372B879BBB873AC10D0D4A57F6FEA3742B5A58534EC84BB654A65D22A3EE019F5561A1EF3E6609909C8B06C02306E09EAF203A2CD628
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 ..ZQ.A./....."#.D.G.8B..A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....

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):	5.547439838275245
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuTD2IQUVyh9PT41TK6tt:pyixRulIl7V41TEL
MD5:	79530BED9B16FCECE8000D076BDD46D8
SHA1:	946513BE886E04C692512EA844E129FD1B6416E9
SHA-256:	116DEEB38E3AA084B16CA8CEE0AF6F802E2B947B734D07D916DAD5F69B8ECA59
SHA-512:	E15C82B8E6511A6D18DEF88A857885DCFBEF43CFB506BC56F050954F30D54446B344EDD9383B3BBA173CDA8761DC3B9E102D367EC2C6AA157E5E4081174A530
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....A./....."#.D.m.9B..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):	5.604160953416669
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQlQdyshLZIl6P41TK6t5oll:0Rhks0VhLZC
MD5:	67E913F38E2DD2C0C799C58D39C30387
SHA1:	751D4ACF2129554B200E1AF5D0C7393EA7800A11
SHA-256:	20B8CA0EEF64B3934A9448FB7BD65EABC569612740FE1DAE1B657F753BAB99DA
SHA-512:	D610255AF01ACFD9739FEE940E0C11AD3F2911E1BFAF2D664F2EDEF6350A26850509E89A04403107B38A11FF51EE4B186F6FDCE08EAA1F17269656BA39C2C42

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
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...A./....."#.D`.|9B..A.].>....uUf..N...k.....c..I.A..Eo.....A..Eo.....o.....

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):	5.5309941223691945
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVtliQ6wcyxMtv9EWm1TK5kty/:mJYOFLvEWdGQRQOdQEliQ76g1TK6ts/
MD5:	44D63CAED4CC271831E54C4CC555CBD3
SHA1:	C32959E9C23AF9677E027F1A26BE0E034FEAA132
SHA-256:	83698BAEECF1B44F5E7C39E0CCD0123FC94E374463B917E9153D51798E89CAE5
SHA-512:	AAAAC7D052E39DA04E94BAA4458A5EE452F931DFA30C8931AC43188CA920C8DAD7B835B8D7BA644EE1E9328210CC09E858E6C03E0EF48351E36FC03837C8F09F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..N..A./....."#.DN..9B..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....Z.>.....

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):	358
Entropy (8bit):	5.553194901342309
Encrypted:	false
SSDEEP:	6:mOYOFLvECML9kxbs5MuR/41TK6tHTbFEOYOFLvECMLP55MuR/41TK6ts:Z5MRky5MuR/Ezz5MN5MuR/Ei
MD5:	66647F108213B272039824C9B0EFA713
SHA1:	E11AA0B7D474E5B4025F0E34AACB94D4CE6B959E
SHA-256:	D6BCD26017149DACE09025C3714DA02D584C63F56A3AAA0B41900C6407DBDD52
SHA-512:	CB7FC02EABBC080722D191D70BEF25500BFF9D5D201E045CB25A57B5E65A0C12C7F12F5BA3A1641C98E489CA09F1F9D2FC7D3B4E18D8A397CD28D93AFBD2054
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..A<.A./....."#.D.P,8B..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....7Q6.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..>b.A./....."#.D:..8B..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....r.....

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
Size (bytes):	214
Entropy (8bit):	5.535501899244156
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu2/by0zBUKSAA1TK6tl:pRrbej
MD5:	C379DB3936868C64B830C65700CD18DB
SHA1:	0DD0EF19251089B0434AB4DADB146FDB74D191F3
SHA-256:	6F5649F9568F0BE6AFB3962AFD8ECA846E6941FAFC7B66230BF8608EFFE188F0
SHA-512:	C1D9D5976EFC87856C11CC1FA5A1A99E5598A5BD16FFC061A7D1042DE072EFD79BFD1D2DD6A13F763880AB024EE1AFF28D744E75A6D9917984D570546234E63C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..4..A./....."#.DSu.9B..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....Q.....

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):	354

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Entropy (8bit):	5.542217481620966
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFvbT9tUdyP41TK6tFtMd4HXXYOFLvEjMSWFvFYy3tUdyP41b:KkXxKMSCvVtUlJ4kXxKMSCvFY4tUljfl
MD5:	929EC81C01D9CD5FD7E29985960FC1AA
SHA1:	C0021148B597D8F9E20AC7FEB474921FFDC7EDE6
SHA-256:	CE6EA5140C295D6D3629E83DE699C3DF8DA315F16B0243D4C33103D6B96FCC46
SHA-512:	CF9A1C1EA62C48D5955EA93D11B885C2EB4807198203DB8547159929989F5D2A8469EE1B737D8429B584B4AD42B1433823D298F4D7EA1E1ECCD970CF8422926A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...<.A./....."#.D'J,8B..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....!.P.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..<b.A./....."#.DN'.8B..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....

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):	374
Entropy (8bit):	5.574450108214066
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLdig55yM+VY1TK6tJEkl9YOFLvEWsfOLBhyM+VY1TK6tcH:5h6OLdGkLh6OLWkK
MD5:	E07A09551C7CF662BB2C355250E58F25
SHA1:	774434B89079EF370FDB983F0A866EA8A600689C
SHA-256:	7224DD3161282A915EB72471B89B263E38FD8D57FA685FD386C7A29349E06F4D
SHA-512:	8E92083D8741DCAA9EF64756D027F3018F32FE27886C66F476ED04CA8EED44B9AAC23321FFA63F235FD49AA4FF44C14991FB9E87D73807169FEE59044CE5AE7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..G.A./....."#.D.w^8B..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....E.....0\r..m .....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .K...A./....."#.D..O9B..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....8.....

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):	488
Entropy (8bit):	5.642394338633895
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFmVHwSeKaTLn7CRVFAFjVFAFuXYwSeKaTLn:UB4v4awzXLnuB4v4SYwzXLn
MD5:	DEAAF18B4BFF25BC9CAE12B5437199CC
SHA1:	B426E581D807A9F7B49137C7BACF63B93D542075
SHA-256:	7FD32935EDA0A6AFDAF0E8D37D77E4A6204FD59BA55FBBC971F1CBC1403562B6
SHA-512:	E6BE7C75E7D6E461BDE7093599E9B6CFFBDA5206E6777BA6848278D19D11A2E5C9BC498F7C08D4FE5EB3AB8413B4AF5160638187012E18ED8343F50EF3ADCA F
Malicious:	false
Reputation:	low
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 ...L.A./....."#.D..x8B..A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....;.E$.....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 .....A./....."#.DY..9B..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....@[.....

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):	5.497738723578311
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvgzFNuArpYFm1TK5ktK/:ms2VYOFLvEWdvBIEGdeXuvY11TK6t
MD5:	3E14C10C90766B1A9DDF8AD17D808549
SHA1:	757A8C145D28C455CDE73015230042189C6E9DC9
SHA-256:	735B3077E6F6DBFAE1D84A1481A189F8B6A4FA19E6F614F32C54E8591A821AC9
SHA-512:	E046AE5B13910484609E134D08F3D72706075A43901B094E02254FAE4369A286270DD885A45A24747238C54939887C71B523E27CA907056A532A8D649BEC693B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .nA..A./....."#.D..9B..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):	5.649171437041949
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ3lKVB7OhKlvA1TK6ttQ:RbR16yIKTJkQ
MD5:	AC8FC5DCDE22A42AFC310508737E9768
SHA1:	0B212728CE9F653122795286DE7C9D98CCCA4958
SHA-256:	4C7437FA7CC0F0EB167FCFA39D6A65C92ECF579265BA36166CF49B26190AEC40
SHA-512:	6328993D67B5EFDF9ABC859C14C892488EB49B974F1AEF3F11E538E03EE678AB90E2E5012E23465059838A455E095FAC80C22119B0CC2641DC4B2CA406D6073
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .I...A./....."#.D.m|9B..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....L.....

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):	5.59539797901332
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVujiws0QdFt1TK6t2Y:B2geRHRQexs00
MD5:	AF29F5B4ADF825C29BEC5AFB7E7F6AFD
SHA1:	5189FB43D1A670598494CD9F25870732A35734A5
SHA-256:	F8DC9F1A176CCD4A832DCD331C079374995FADA02A53446F3E4ECFBF22E7B997
SHA-512:	83CE4C37B38C11F2F16F0FC1B575B94F353CBBCF5B7D6220C9B5E592DFB89E5C0C871A4717912FE4DE5E3682A62955B8B10C4F2733F682335143CBE4F38A50E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..5..A./....."#.D..9B..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....

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):	412
Entropy (8bit):	5.5995084362856655
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQzVPt1S/1TK6t5lMzyEYOFLvEWdrIOQP7OPt1S/1TK6tx:WyeRl4t1wzmyeRlkIt1w/
MD5:	E4BE587D57B40D777A8447F8E53349B9
SHA1:	692DB3F82F8603E66E4189B3E406C9AB0D7D727D
SHA-256:	26D4F719DFDF4F1D68AA84021417CA4125917ED603101B7E88DF3A87C844AEF8
SHA-512:	1B0C68ECB8554C6EDACBBAC87BA9C488FD30D93B9CE4057EDDB8F0393E28A7889DC25FE772DE4DB6B0E4C519FA7CBE24EA7D7C4FCDC836BC6E4D2B29F0A A4A5D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...I.A./....."#.D.9g8B..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 ..M..A./....."#.D.Ba9B..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....s./.....

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):	5.54496331398302
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvBBjqNqww6U+5m1TK5ktynll/:mnYOFLvEWdhwyuwqwK+41TK6tyl
MD5:	F0D4749B7A2F0232BCD2C9F5DD7820AC
SHA1:	42EF9C7CCD187AA04F98FFCA7BF302A527A522D7
SHA-256:	E47D4D06B4FA33E1A85FC08D3C119071FC0E16DD813225AFECE584AC7331B0AE
SHA-512:	0A8EE8A5E6A61C405C90E4CBB58F2A5B49FBBD0A6384BC53BE781F75B058824F7B0112B548AC7239DEF7872EDC14C83946C2C8830969615180F2737AE39DA97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..R..A./....."#.D9E|9B..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....

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):	460
Entropy (8bit):	5.63581385058895
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuLE66CCifO441TK6tM9/EYXYOFLvEWdrROk/RJbutzoyO:/RrROk/E4xifLE2FNRrROk/0ifLE
MD5:	317362B9995013D507F11E28FEAF5B0B
SHA1:	118E816621FAB6032C53674BD42BB941E54D55DB
SHA-256:	C54CAD05E4F59D2AC3DB56CE8C1734C68C7A48A984A5042B1EDD7EC6DD3FB0B2
SHA-512:	1BC5605C69E74125FA1709D8EB1CC9C3944C08F95C9903395A625EA184E82D255F221F4AFDD75194D499BDBB868BCB2CC0A1676E9CC6B339162EA5BC1FF3A2E
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 ...I.A./....."#.D..g8B..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....6.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ."...A./....."#.D.QW9B..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):	372
Entropy (8bit):	5.597553427139231
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIuldK1QPLr1TK6tm/2mDEYOFLvEWXIOqaJ1QPLr1TK6tll:xqTpXKCPLngBqT/qkCPLnd
MD5:	E5468592E77AFA494E0EF305456E86BA
SHA1:	28C1B9D96CD3857CD55EFF3F570E9E8E159E457A
SHA-256:	EF760B3EB4A8B7D8AC4956C6FDC15C245C80F4B07226641D9B5F69D3C7A2D592
SHA-512:	671044E879ED50DFF25F59D9476E3FD15736AF1ADC8F019AFE4900C30E19BDDE77FDEB9D687FD9A7A5D80264992851DAA462AA5EF21FA21832418E145DB5AAB3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..iG.A./....."#.D.5^8B..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo..... .'7.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .5..A./....."#.D9.O9B..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....+/l/.....

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):	414
Entropy (8bit):	5.655351124377682
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuy5/sEJ41TK6t452YOFLvEWdMAu/g8sEJ41TK6t:zRMwpsDbRMW8sD
MD5:	C5D68FD662681BA855B5AC1F4C4D0F90
SHA1:	624C2DE4EC20F64B1F37FE6B8B38DCB07118D7D7
SHA-256:	B3CCE4EC4175144BBF30AC563F17F2E6FC913F4A32F2A99A3F4FF16495D99014
SHA-512:	FF90D8705492B41E42E4DAAA7F4AB06E55DC6F6C26BA466BC174B83C56ED6132745856D965FFC2F84ADA50EA95D9BB6762AACAA108EB1566648C0B7E1C6C23E2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .1.K.A./....."#.D'.q8B..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....l.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....A./....."#.Dy!.9B..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....#.}.....

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):	420
Entropy (8bit):	5.595343025482043
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuUJBgFong1TK6tsEYilPYOFLvEWd8CAdAuKYa76PBgFonc:6lJRvPqoMqUlJRDWPBqoM
MD5:	093D67DFF5ABC4F45732ED1EF9BA3772
SHA1:	8171EF90413D28E031EB37197C8EF3ADC4C49164
SHA-256:	F771D34D882071030719435O5F54227C5697DC4B88D7678874B7B2D3EEC1D1C3
SHA-512:	3A71D612B0D4D1DDD0019A7A446ABA83E876381855408F1B81ED251B86CBEB10E43704C721D2BC59CFC52E1105C3951955D19092AE48466774F38F78380CA02D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .L.K.A./....."#.D..q8B..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....l.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .l...A./....."#.D.J.9B..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....p.....

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):	446
Entropy (8bit):	5.609982354379255
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuH+Zce16wG1TK6tjq9/EY8nYOFLvEWdrROk/Iulkbm2yca:F8hRrROk/wZn25q9v8hRrROk/ymP2I
MD5:	D8BCCA4F43D5AFA65203A5667BF9CD76
SHA1:	BBDD77B5CD714C88CC1BD7B2B428AE5B8E184EE1
SHA-256:	E6C1494EF9671356CF340AEF5483F4580B71AA1CEEF46DE7D7C813D3BD99E13A
SHA-512:	41EFFE7C39D8FAC407378CD8A1AEF93B50BD570432E30E39DF8C293E2DBAEE4E2507CA6CC51683DEBED4D72B5D951D0EC1C581984FA2C6BBAF3721F91DFFI E86
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .H.I.A./....."#.DY.g8B..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....Z.Z.....0\r..m.....__...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....A./....."#.D..W9B..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....w.....

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
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.643786617136747
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQnlYKrNJIi1TK6t1bMLrnYOFLvEWdrIoJUQ0+FYKrNJIi1f:ehRcalrNJICTIhRc0rNJICl
MD5:	97775FB1468A9972A3B859E1BDAC5F80
SHA1:	633DD1763D59DC4BDD713CEBC6DE99BAB918F5C7
SHA-256:	9542BAB92335F099BCBB5527F72FAFD6D5A6E431E6FAA577EEB15440CAF8E210
SHA-512:	3CFC486292F4B9769C1C9393D5EB9872F4DC984CF53B46E0CAFE6351E3C8E3897B5FBFA065DB058367A56805ECAEE2D76EF83F256556F26EECF644D59752823
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .N.I.A./....."#.D-^g8B..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....T[.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .fn..A./....."#.D}.a9B..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....3.....

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):	416

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Entropy (8bit):	5.602134781472781
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu0FJdaLzgm2d/1TK6tfxL9leOEYOFLvEWdrIhu2skTSaLzgm2S:0RnRe/L9SRyTZRe
MD5:	DC8A3D7C538BE4DE3088C753A85C9ADF
SHA1:	57601437E4056DE50B0A2CFD87D4CC36FA4B1444
SHA-256:	89DC7B477EB01E876304E48EFDEDBBE89F3F41D8108199EDA8D43C6F07C2B6B9
SHA-512:	3DEDE0A8DDD36EFF3B78D60D118AF95826CC94ED095A097C6AF97BDC3AEE8628562AF8A3EB861A07C665B74C85A99A56936E5533171FEFB426247C57A19308F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .i}I.A./....."#.D..f8B..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. ....o.T.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .?...A./....."#.D..V9B..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....~.....

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):	376
Entropy (8bit):	5.632280948869884
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KikRBkx56uvp1TK6tSAElVYOFLvEW1K6Bkx56uvp1TK6tl:6JJKHI8JJKqIT
MD5:	2C591D70AFED3EDF36A8971A0DE4A2EF
SHA1:	164BC80186301EC2E2777C9E92369D53BBEA9FFD
SHA-256:	93B6AE2FAC8E93CC0AEE6DFE4C57E64E198FC4CF6F1D7A91F3B790903E6DC313
SHA-512:	A56DCEFEE22D6841C951B29543D5FE4185E1459B527D2DA12F5E3645F6F256ED57B58D471283256BA3DF78FCDD17F56F2B69BC776B6E79DB6E589F22045A692
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..>.A./....."#.D..@8B..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....c}.....0\r. .m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..Bi.A./....."#.D9_.9B..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....

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):	5.623433872597828
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvumahUDLYtmOZn1TK6tl:xRBJpDcFZL
MD5:	DEDD9F8EACD9C3592BB8C4BE63E7120F
SHA1:	F226FA21BB254B84343838424D5A2EAB064974D7
SHA-256:	DD6CC7F74546050499E8DD9C3D6AF768464CF81BE501F8A504072FB5D14F5127
SHA-512:	4ED3D2F30389C90ACB7A98CE5050403C9F67567D6553D53EE465026D4AB0FB908E98C01110E729C80235E715516A7CEE032E22C8BAE55013B91197F18354CE12
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..C..A./....."#.D...9B..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....m.....

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):	422
Entropy (8bit):	5.655081050778508
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7OLVPu1TK6tcsRPYOFLvEWIa7zp7tpGLVPu1TK6t:BPHmcBPHGc
MD5:	9177EDE07B32653AFE456DF25BCA71D2
SHA1:	7E793B7E16059B3A0593D12A8E5FF894F22557E6
SHA-256:	496B073333EE4FEFE147A1D740C4E09F6944C538C8896D5ABD225DDA7D0E7D89
SHA-512:	81A06CE49E3D76FFCA324C11A071A8F69C1851BFC9DE0413204913B1C0B7E01053B4019EFB4847D622EA9B5495E635CD6E7587B017D74A5AE7DB2C0B3E3DD2 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Preview:	0\r..m......S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..C<.A./....."#.Dg},8B..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0\r..m......S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .9Qb.A./....."#.D.".8B..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

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):	5.626554842281019
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QtAweiM3Y1TK6t8vH/:bJRT96ALr0QH/
MD5:	F40D9AFC62AA62239761A6548950FE37
SHA1:	3C2D1FE9F046C88EAE1A6CDD635297A8A3E0E20B
SHA-256:	D6CE1A401BCAE30F26DABB1369362A61CDCD42551E104D892AEAE9B181A47B86
SHA-512:	4792624CFB57FDAD074DF5C4E3F282DC4B4B1233A9E9BDA3F453462B126AF480397C00DE3FBE992A5AAC1D43F60AB838FE4F78B1A270A418D8A7AFFEEE35BE23
Malicious:	false
Reputation:	low
Preview:	0\r..m......P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .....A./....."#.Dd$.9B..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....J.....

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:	modified
Size (bytes):	208
Entropy (8bit):	5.6078041955027
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQtbUKS0RjBRCh/41TK6t:XRc9gXrDi/E
MD5:	FCCD15969FBD1B501E41ECF19D77DDAC
SHA1:	AD08F02D2B867249D45CFF90E909D996B7D969DA
SHA-256:	1DA77172E142ABB760AFCC0F707A255792847E0393EFA43641AE6BF9494C7616
SHA-512:	8AC3E87B751BC7519D61DD0E522272F721510752877E85601B1B8725F82729FEF31773103085E876656E33B407840E4D2E27D6F8496159196F0C1122B3E560FC
Malicious:	false
Reputation:	low
Preview:	0\r..m......P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....A./....."#.D.9B..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....w.....

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
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.583339409313722
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuq3yVyjULlF4r1TK6tz9l:bs6xRkigC5LlF4nvl
MD5:	9FCAD6BE1663A09A9B2B611DB782D49E
SHA1:	1BAADF440204E9940D5BC3956D17A917B2FCF583
SHA-256:	99498541C3CF7FDBFE6AFFD0096F45857AAA2C66888D2AF2444ECA06169CC1B7
SHA-512:	E72FE6F32AF1F329BFDD0C1C8B44EDD66A116AD34B2875AE5B69E1118993A36D78CDA4C6321E9D58B289CC6A5B8B1978F696655F3B7B76BB470296D46AFAB5F
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 ..%J.A./....."#.D.g8B..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....y.....

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):	5.511963049149372
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvbKyjU4cu1isLK5m1TK5ktitl:mhYOFLvEWd/aFuxpjq941TK6ti
MD5:	F3039F4EEFDBC14195E7D6FCC3D656FE
SHA1:	E4B07626E73B6DE0D297C1475D4712449FD0D0FB
SHA-256:	7C17E141DBC14506176D029D2E47E9FE5698997446B7F2413C87034F6F7A3701
SHA-512:	D2DED567F03865098E21F26163589944CC0DC6DA0F0AD2ECBE82743EF554A399E4B56C1ADDEBA34B4809FEA1BE97D0BDF9266CC0E55097D8DFAE523E4F778(39
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 .>r..A./....."#.D...9B..A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A ..Eo.....

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):	5.563022573534016
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQVmcVBoBMqVd3G4K41TK6t:2DRuR5cToB9Vd2k
MD5:	56C7EC7C899F2174FB6611E0FD3E10C3
SHA1:	8CB9DBED09222404F42A5A4CF500F9FC78EAE36E
SHA-256:	0ECA65A5BB33A092B3CA678A777B853631AAC6DAAD50BA26D51D35E14073B2D7
SHA-512:	7BB65A6A4EB64CB02033B0E8A93FB18C34D8F4B4B8BE99646EC79F712D14A3C65B823C4EEA22F5DF6518B049F22A2E3D546D743C50728E8BAEB96A6D0A33C8 D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..>..A./....."#.D...9B..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):	416
Entropy (8bit):	5.621094331265112
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QlCMkuuA424r1TK6tFMkqYOFLvEWd8CAd9QCwa9uA424r1TD:+RQ24rnf8RQdvMrn
MD5:	3FFF8EE7F689B84FEABBF40A4392B6F3
SHA1:	9A6255CF06B8D8AE2D31CF9592A45964FB014D9D
SHA-256:	D9CD4DC3D4C2463D5270D022C35CADA176931D4A91A2013923EA02EEFA41E94B
SHA-512:	600000940F4239A02EBAACE35EF8C26C400A02354BFA0CA1135662C85AE2DCAE3B8B6AB5A6D20FAF29F31B1A65CAB3E351054C9830B44A4143D40292902193F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .DmL.A./....."#.D..u8B..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... ..A..Eo.....Bk$U.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .C..A./....."#.D|..9B..A#..@..k(v.8g..5.~_....]Pj.*.. 6.A..Eo.....A..Eo.....=.Gp.....

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):	5.558573059055501
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvQhkblZa3l3rg2iHio/Mm1TKj:moXXYOFLvEWdENUAu3tryC8n1TK6tG
MD5:	88752D56ED74D0DBBCBA4556DF51337F
SHA1:	183E9D9EC876A2DDBC52CB8C2309EF4684D11052
SHA-256:	2C20E89B2BA21B3B8AED5106431CB3A25D8094AC8AF23A41982531D8D10C8237
SHA-512:	C73E603BAFC8FACF624231CE09FBC2FF42B19EA33B68FDD301B601AE71C040AD2D826A47CBDEC074D5F223DC392CB5EDE7F28C1CC37CF5AE7CE7C81F1DA5 C35A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .....A./....."#.DI/|9B..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....y... .....

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):	442
Entropy (8bit):	5.613745278398665
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQCKlqe7LmB41TK6ti+QZYOFLvEWdrROk/VQrwU7LmB41TKP:nRrROk/VN+qmcRrROk/VFPmYl
MD5:	F5A22C98406510EC64A623CC6DA63426
SHA1:	A492DC8ACD6FEB22DBA1AA7500129AA3D841E453
SHA-256:	E6B5947EAFF7F003777A94B8F5BDEF0C57314C7B15B4B011D7F354D027B5C4EB
SHA-512:	B3FDD3D17778BC8713C01E17526F1F0D085207073C8D11C0FA2476DD265D2D7227572CF6292597ACED7FFF13C8D197BB4C9EE7DA3BEEEF863195AF8992F044
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .&.I.A./....."#.D..g8B..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....uBLI.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..q..A./....."#.D..t9B..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....m.G,.....

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):	5.575149483291636
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuymt4JKzAdm9741TK6t:qxRczYldu7E
MD5:	ADDB6C3F869C77B398FF4AFCA17AC422
SHA1:	692ECBB1210B96E0F399492A1447E9944FAC78C2
SHA-256:	882E2F40DDFB82E235C08BE8CCB4BE47719DD766379B5E01EE0377E624FE4EB1
SHA-512:	1C770A4F1A9F1DBAE9FB7377F9D8A2BEC1136516B384C4D1E74A67853323E4B3A03E6684486F659ACA74E41F85EFFA3439757F5A632A12DC0DC058F559E976D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .t...A./....."#.D...9B..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
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.522872733358144
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvlgPW6QfB6shoq+Nem1TK5ktXMlt:mMOYOFLvEWdwAPVuP0WnfkJn1TK6t0t
MD5:	0030B3E289AB11C9D4B9B45C704A79C5
SHA1:	3382D8E9F43FB7E133446C21E7253889AD526051
SHA-256:	834611E7838C1DA442E13236216EE962B11BB271CE6303C3806B6B283747D81E
SHA-512:	DF0F8858E59FEFBCFE1E6F10C686CB98FE07DBA896BCC835991C83A66590EBD13F6ABD3E4EF852423543F94344E4D2464D7EF987B6E42332805131D21B9A443
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .....A./....."#.D#.|9B..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....x.;9.....

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):	5.641613555516611
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQqbQ6p4zhcsBXIh1TK6t:mxRBJQXYDB0
MD5:	950E11C1CB458DE876A2575C4773E5E9
SHA1:	72E336BF35CDF26EB2D954B41179AD3B7B00924D
SHA-256:	7F19F74E1F57957104577722ED8A546288D430BF936A8B298226780CB845D843
SHA-512:	A390F50EC9DFD749153ADE6E713246411932032F06A0A44F2F41FFF8F992569C30EDBC96AEBDBDCE92E1EC4368AD7AC7551FD2AFA12A246F6C52F40D2844AC3

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .\...A./....."#.D_..9B..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....?.....

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):	456
Entropy (8bit):	5.610221471291351
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQVudG7c3Me/1TK6tl/MsPYOFLvEWdrROk/RJUQ3uW7L7M:3RrROk/smuA7crdRrROk/s+L7c17
MD5:	38E6F14B864B27CA02A5CA314A67E5BB
SHA1:	39415EBF7F4BECE97A418AF768BE3848A29AA176
SHA-256:	99A1AE1601DB8304ED00B6960EEB50F4B5B3899ED7012314FD3C703F8D40E829
SHA-512:	A037C365606A7C21E43E79D32E93FCF708A2E7C2267028A462F90D2836806872EA0403E4ADB701F2AE8543E6E5BB96FC019C9D815E5FF448FF03534ABFA88292
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 .'#J.A./....."#.D.$h8B..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....U.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....A./....."#.D'.u9B..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....Y.^.....

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:	data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/I:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
Malicious:	false
Reputation:	low
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q.....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

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):	5.185620111572282
Encrypted:	false
SSDEEP:	6:mrNQL+q2PWXp+N2nKuAl9OmbnIFUtpY9SG1ZmwPY9dQLVkwOWXp+N2nKuAl9Omb5:WvaHAahFUtp811/PEG5fHAaSJ
MD5:	8E6E804B490FA938BE204CCB636B6617
SHA1:	185F3BA8CE5A84B28047349A76B476F67780E33F
SHA-256:	E9E7176B457A2CB85671ED377E6DE8FA232A760A00E0F6ADA77FE0D225419974
SHA-512:	526DF167656F7152059A8E76FC1D0748EDD7372E52DBE6548E9B92691CA7FC5D95D214B4653677BDF225CFA22AF329BE68133AA8A9CD236F0D19F21458805BE
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:26:41.690 18c8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/01/11-18:26:41.691 18c8 Recovering log #3.2021/01/11-18:26:41.692 18c8 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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.007952317387287845
Encrypted:	false
SSDEEP:	24:TGEXiXKGEXiXJ88hMXiXN8hMXiXTg8hMXiXTg8hMXiXT:TGEiaGEiCsMi9sMiDgsMiDgsMiD
MD5:	B6D6D8092327194522BEE7EC4E9D29B0
SHA1:	248DA8ED1A94F29906C944B56FF9ECEAD7342542
SHA-256:	E2172C50F08FC62BD25EE7D9CE092A9F4BDCD3143D81E38E522A917FF7D6E86F
SHA-512:	573EBD8EE4A387576183D8232B1343E5CB51C4145068E90C144E84E10CD111A673567139E087FA7CE85FE276AD0F3CFF0A3CB2E60EB403735F2AA00520A848D3
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....Tq.>..j.....

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:	modified
Size (bytes):	24576
Entropy (8bit):	3.341317500488437
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBklOLAhFVCPL49IVXEBodRBkROL+hFVCP749IVXEBodRBkd0L7h9:iGedRBCnedRB2JedRBH
MD5:	723827EB7D29A5CCA8EF78FD18884467
SHA1:	5D60A853F5BD66FDD303F9D49BDB1A18ADE76789
SHA-256:	59D9C6401A549DB42C744E65412147F1236DA066899BD3E4DE8182B7CE1CFCCA
SHA-512:	D9DAB56BFF14BF23561498546200AA1552FD7F2B5A945F4406F2105FE3D1C7AD90AAD3D1BF0E6C024193A9551FF1503028F03825D87DCF62CAFFB31243274A7E
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):	26196
Entropy (8bit):	3.1372604831616973
Encrypted:	false
SSDEEP:	96:z7OhFVCP4949IVXEBodRBk3OLAhFVCP8LR49IVXEBodRBkMOL+hFVCPVd49IVXEF:zEiedRBsnLGedRB/oCedRBU
MD5:	A2D1F9355CF5E74B6712BA21A7C38EA2
SHA1:	8BDB19E8832D44E6D153D4952942776C83AB9A26
SHA-256:	931B16681E47836B0E93D0BBC5E371EAA9C31FB7F12C17B2F89361FA4379D9D0
SHA-512:	EA01A425AA6F86BF781E8936B6BADB9A8C8B3DC5B4BDE96DE2F662D11204770F32C8099EF52030D151F65FF642E2068DE8F9365ED08353034938E49C024FE04E
Malicious:	false
Reputation:	low
Preview:	.....6.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4900	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4900	
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
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.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.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\Microsoft\Internet Explorer\DOMStore\GBSSSDZ8\www.pukacreations[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2549
Entropy (8bit):	4.880409327636865
Encrypted:	false
SSDEEP:	48:0O+OH+O+O5+O+OZ4+O+O+O7+O+OX+O+O+O+O+O+OE+OD:R7H775776777777X777777E7D
MD5:	6535FCCD1DF44ABF39025B973ED5B7A3
SHA1:	A3504A6EB9245276F393B67ED9393ECE8E677D51
SHA-256:	C5F09EFADBFF1BC445C2AD98875B3F3D3132FA116F6D54B4F4016FE1879F8AE1
SHA-512:	2EEC80B477492C2D7BEE9580A7D6D1135EB9323D617F033B5844E52CF3B7ED3CC5F009BFCD9EDE6666DEDFC271BD8BB618C1BF234FB68F177B8DA5119F8138E4
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /><item name="wc" value="test" ltime="738870800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /><item name="wc" value="test" ltime="791460800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" value="" ltime="474510800" htime="30861450" /><item name="wc" value="test" ltime="849760800" htime="30861450" /></root><root><item name="wc_cart_hash_d19812b7dea223d345a7733f3ae94cc0" val

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{53A0A726-547D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.884181130050169
Encrypted:	false
SSDEEP:	96:rIZ0Z12Z9WmttmrwNfmliLMYMmS2Ugmgm6mIq/fmW/zLPlrmXXa:rIZ0Z12Z9Wet7fZBMKpwflcrh
MD5:	25BDD0B05F8C4D6E6F9017708C9BAD02
SHA1:	C2E3DB221A6DFF13E9CCAE52566A2AA041C09C31
SHA-256:	4E877B096215B64F4468627A7FD8ED770012F999FA371F53F005C2765B0EE8C1
SHA-512:	ECCB6D44AD1EAB3C2284FE761B042EDD4EC09DB999EAA7204A211FE4AA7DFA2CD968E8FC52654F1EF0268ECDDCB5A202D5BECEA1497D6C0DB102E1418A69E60D
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\{53A0A728-547D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	224228
Entropy (8bit):	2.770406649779604
Encrypted:	false
SSDEEP:	384:rN9LzEhMYOoBdudOW1Q1l1yhvcE7wpNd0DvW9UVxTPCNaWFW16EgIK1QYIGnrIFM:M0KjETDeLckugZS+Z9ygZFRgvgh3A
MD5:	846E8B1A2BB0BF0D8ECF2D6278A26A54
SHA1:	FA97CBBA92A3FEBE37C41E498B5B7F0F7E08D5C2
SHA-256:	B5CCC54B660523ABAEB0E3C7A379467E67709336F7FE2DFAA1FA65B98E51D453
SHA-512:	7D0E4EBA9667AD8C9D7753CA60E2C298A87968F566FF422BCEC65D51588CDCDB58465A3B04F0C8B4A2E85EDCCC1720698D22FD6EDFAEBA65DF2A7E0C81472E30

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{53A0A728-547D-11EB-90E4-ECF4BB862DED}.dat	
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\{5D412135-547D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5641804182181593
Encrypted:	false
SSDEEP:	48:IwqnGcprEcGwpaSnG4pQ41GrapbSKrGQpKAG7HpRcsTGIpG:rqNZEUQSJ64lBSKFAbTc4A
MD5:	82211E1AE366F3266141870B2A969250
SHA1:	71A8E9EC62B292713D52FA535FF71F3B356D4EE0
SHA-256:	F8D95233E1C00D0CFD2A553EE9EE29CE9E82693DD724EA17A55529BFCCEC380A
SHA-512:	8E0F215BEF08E1DBDFF88FD116E9FB070904B26F0386AE1211C920BC04529784D305CA630FC5E01D81EB705BACEDC87B1616E46741C8F683174798A326E3D505
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.099256453155121
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEfcPcrnWimI002EtM3MHdNMNxOEfcPcrnWimI00ObVbkEtMb:2d6NxOjErSZHKd6NxOjErSZ76b
MD5:	FF31616512560605ABDA93B17C67E9F6
SHA1:	96960FB37B5E844FB162C1C99120D4992E8D28F7
SHA-256:	C35407C9B21C57B31BA5807C7E52A5446F6926DB3773E10B7996470334DD31CA
SHA-512:	4260E04F9C03B80177B4267E2E60D217EFAF4747EB55BB33C49596C5896A34D93A0C14F12EDD2A3CD4DD82860796F56069ABCF2EF2C584084EFA74AD42A5B3C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.09546532712366
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kjTrnWimI002EtM3MHdNMNxe2kjTrnWimI00Obkak6EtMb:2d6Nxr0TrSZHKd6Nxr0TrSZ7Aa7b
MD5:	CCEA80D362B3EA0B95047DD47C9F9F66
SHA1:	72B61C8860968151487EE527439ED2B868A185D9
SHA-256:	3D5049B37EEF5AAA628847DCE214B44E3937F183742CED6560A1BD32A702633A
SHA-512:	E911CCBAF95E7C8F280A5FD39981399A7A5808AC4E3772BADC45DB7A790CBC6AA5DD1C70DF058906BA4B216FA1D1B1178A72DE2CEDFE8E78259E63B19584A3A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3302ad28,0x01d6e88a</date><accdate>0x3302ad28,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3302ad28,0x01d6e88a</date><accdate>0x3302ad28,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.117075069534431
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLfcPcrnWimI002EtM3MHdNMNxvLfcPcrnWimI00ObmZEtMb:2d6NxvoErSZHKd6NxvoErSZ7mb
MD5:	E45B44612B0F622606FEB576CB87E262
SHA1:	E931BABB285B1D7ACB92BB8EE22738C7E094F21A
SHA-256:	F6FA03F0DD01E034A85418FEC57445CD3148FA31FAEA821B547E0755D8B44B9A
SHA-512:	8169F5BF617D3DCB4070A0A8B2FDE8D61BFDF18BF9A1462FD7CA42D96F4191ED95C89D0C746186B2A97F7473D9E5A32D2AABD7257A44A5BEF287B4C54DE58E01
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.076439062566471
Encrypted:	false
SSDEEP:	12:TMHdNMNxi2mrnWimI002EtM3MHdNMNxi2MCd+crnWimI00Obd5EtMb:2d6NxjmrSZHKd6NxjJLrSZ7Jjb
MD5:	21DEDECA9D4172B716333383000DE57B
SHA1:	35C21A64153062CD380592520BFC414C3E8009EC
SHA-256:	9F044F9B52C87B5C0598712E30BC25655C4DE3530637B07E0488705B5049AAE6
SHA-512:	B73C7796F47D25AF0D4A57033053383EE2A61DABA76589FD055B251B16F1BC2A6A21C78D3876835B624025FBEA54A3C5020372C1EF7217AD6F4D8FFDD377994(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33050f8c,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33077 1df,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.134018939518944
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwfcPcrnWimI002EtM3MHdNMNxhGwfcPcrnWimI00Ob8K075EtMb:2d6NxQfErSZHKd6NxQfErSZ7YKajb
MD5:	9F133CEE6B45D1F243F3D88C7D36F209
SHA1:	D32392EB587A9CDAFCF92A8F14B5F39442D9EBAE
SHA-256:	768F42CC7BB2C743CECF21728D079E31E70EEE098297253D2D5F3BAA696E5921
SHA-512:	2CBAED13300EDE7C5E7B54CE6567406D8269F188760EA2301AFE22AC03024C551C68BD5BCCA6B686E43BB09769843218A3172D1EB33126013E1327882EBD8D2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3309d436,0x01d6e88a</date><accdate>0x3309d436,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.063923962279681

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n8Cd+cMCd+crnWimI002EtM3MHdNMNx0n8Cd+cMCd+crnWimI00Obxt:2d6Nx0ZLJLrSZHKd6Nx0ZLJLrSZ7nb
MD5:	DBF7995A955914A77AB3FB4DF042DFC7
SHA1:	19438CFD4AF5213A72CCB2CD3DECDDC737D253D8
SHA-256:	6BC7F2BD2D369865353160321722 1D0427DC55AB41FE54EC486523D19BC0DCE5
SHA-512:	24A5885B836481265D556D244E6572DB2E9448096DF27F391547A235CACAFAD76DB1B1EB67D809B83D9CB7044EF612DC1CF7FAAC236E24322437205A8627B20F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x330771df,0x01d6e88a</date><accdate>0x330771df,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x330771df,0x01d6e88a</date><accdate>0x330771df,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.103751555130434
Encrypted:	false
SSDEEP:	12:TMHdNMNxx8Cd+cMCd+crnWimI002EtM3MHdNMNxx8Cd+cMCd+crnWimI00Ob6Kq/:2d6NxDLJLrSZHKd6NxDLJLrSZ7ob
MD5:	88E7E10A23EBA3CD2C70F04F9D2B1728
SHA1:	02549A6DA7AE887296DC68E6F504A31A9EE2BFF6
SHA-256:	0AEB89670854EA3AE3C968B401B3B32771560BA5F0919D32B35AB8C6A2EE4615
SHA-512:	CE3DBB10DD88118265911C45C09EA6B2F3583095F52BA23DC1127CCA1A42FD37114316E51C9A1AE4B946B41B46FB16CB4AD0E9738340BC98351E162730BA167
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x330771df,0x01d6e88a</date><accdate>0x330771df,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x330771df,0x01d6e88a</date><accdate>0x330771df,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.07447376899145
Encrypted:	false
SSDEEP:	12:TMHdNMNxc2mrnWimI002EtM3MHdNMNxc2mrnWimI00ObVEtMb:2d6NxtmrSZHKd6NxtmrSZ7Db
MD5:	5C59D014BE158AC8C4A5B4ABB3DEF4EE
SHA1:	26ACD766EA1FBF638D8E047CFD2E8CD02B96EF0B
SHA-256:	D4F9DE6A09B3067D7041680D538E053232CA4EA00063439F5F64F792335BF1D3
SHA-512:	2892A6719F9CE838874F35243341B997EF91DA19FD55B70E5568A905124E75E9160DCC06BBCCEF786DA133368FEF90FA76466D9611312D5A5BAEA4298991614F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33050f8c,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33050f8c,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.056912075765338
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn2mrnWimI002EtM3MHdNMNxfn2mrnWimI00Obe5EtMb:2d6NxOmrSZHKd6NxOmrSZ7ijb
MD5:	1E4A901B31F03C13C68A62998CCC09AD
SHA1:	BF0AABEACCE6274E031AC66EA8B34405E08AB6AE
SHA-256:	E911740F872804CA384179DEB11576EAD9872F629EE5381775D175316813BDC2
SHA-512:	9FB1266FAA0FC5C2D77F65AA024FF1C7533E6502257641C5E7E413C7855454545BE843625A133A6EE68A13080F427AD7C97168673A39A453DEE3C244FA27A97A

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33050f8c,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x33050f8c,0x01d6e88a</date><accdate>0x33050f8c,0x01d6e88a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1456
Entropy (8bit):	7.282650741330681
Encrypted:	false
SSDEEP:	24:2p/EMkgTEK7XRx97IIFvnMoqSCJ257wL1xAPItQQpSeVxyjYsV7fdmezjE+EM4Ik:2xEdCEK7Xf9lJiBA7uTtjVxyJV7fbZEN
MD5:	4FC194DDADFAAAD4C337194776BE068E
SHA1:	0FCE450EF21BB2F87B7ACA0130320205EFBB3846
SHA-256:	678FB660683E8105CF1A1A6535E32F3485B43CF490EE8001CBEC23CDD9AFE978
SHA-512:	F84AF76B983E164E18AD08C340F8D0AE83390EB906614A227834D134655CC8266762A8B0CFBAE1E977B4D494E95993236DE5622A608795D49A648C51ACA202B5
Malicious:	false
Reputation:	low
Preview:	=.h.t.t.p.s.:././.w.w.w...p.u.k.a.c.r.e.a.t.i.o.n.s...c.o.m./.m.e.d.i.a./.c.r.o.p.p.e.d.-.h.e.a.d.e.r.1.-.3.2.x.3.2...p.n.g.....PNG.....IHDR... ... .D.....gAMA.....a.....sRGB.....cHRM..z&.....u0...`.:....p..Q<....PLTE ..MIFurpPLJ"..JFDSOLnkiromkhfmjhEA>...MIF...FB?da__\Z^[Y^[Zea_HDB ..olknkjurq...FFE'&&&&&...?>>AAA???>>><<<666+++...LLL.....---.....\\\...DCC//.'".....khg.....PPPjhf.....)))...../////.....777.....111.....###...EEEooo...../0/...===....**$$$...^^^hhh.....'&.....|||.....888222.....!!!.....,,.....kkk...HHH.....bbbBBB.....('kigSRR.....ttt.....KKKppp...~~~KJJTSS555322.--/..ONN...a....tRNSH...Q.....;.....B.,.....bKGD9...@....pHYs...H...H.F.k>....IDAT8...;.Q...C..%T..XBs.".?.E.n.rC..(KY.>.-..6D..&._..}0g.....9.W...B..C..(4.....d...X..q.,...E.o.:.....d.I..r+5.O.!L.oJ1.Y.Y...p..<8/..I ..].W..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\33735-Glitzy-Hats-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	30008
Entropy (8bit):	7.938489002220529
Encrypted:	false
SSDEEP:	768:rZQUlbPCxjYftWKeHyUlGnegofMg342JH71:G4CilWKeS+Q8fMc4+p
MD5:	DA334D913BBF34150C4DF32C91741EC6
SHA1:	215866934F168BFB840C56B22F96683F775FBC67
SHA-256:	8208E54912255F6A6C39801C2835812057581BC71DC17D19D1A6CEF92A19827B
SHA-512:	27302028022C7AE233940FF6855FD8C144731E5A86C9E5D257F7866DD8A03508C80249FAEB81BF468CA9CB97860C5C744D2A5CD112F1AEF1ED3E9F3114B5F4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/33735-Glitzy-Hats-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:54DAA66B433A11EBA45ADD48B4FB8971" xmpMM:InstanceID="xmp.iid:54DAA66A433A11EBA45ADD48B4FB8971" xmp:CreatorTool="Adobe Photoshop CC 2019 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:19ded9c1-dc9f-470f-ab03-cffa4e896c18" stRef:documentID="adobe:docid:photoshop:1ec333e8-e6ab-df49-83c9-473650cf6a9d"/> </rdf:Description> </rdf:RDF> </x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\35429-Labyrinth-Lite-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	43609
Entropy (8bit):	7.96165174236868
Encrypted:	false
SSDEEP:	768:Z6VPWREaCdj9B75j73gVTjKih1HktDgGV84mja8P9jqMi:0VPWRE1dj9BdjSTjJYS4mjaWhi
MD5:	50498855625BB08ED36289F9F3E95539
SHA1:	5CA38C466AA9FD5622E03146472C737C27573095
SHA-256:	075B4D8062B70B11CD3713085334923CA69FE5626CEE06C96E5E314E7B8E054A
SHA-512:	FD54676BDB70577A891F9B67B6F1E1090E3C2966CC30A1C995EE101F8F3F2F7488EA0C6F7327B9AA782705C13C11B06FD86B61F82010A6FEDC0B1EF4B29988B3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\35429-Labyrinth-Lite-324x486[1].jpg	
IE Cache URL:	http://https://www.pukacreations.com/media/35429-Labyrinth-Lite-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:A6442901433A11EBA48AC3D14C675556" xmpMM:InstanceID="xmp.iid:A6442900433A11EBA48AC3D14C675556" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:ca4e4ae8-46dd-46c1-81a0-a3eadbdcd857" stRef:documentID="adobe:docid:photoshop:fd50070f-68b1-5a47-badc-f150429e565e"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\36191-Ocean-Earrings-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	29819
Entropy (8bit):	7.945160910054961
Encrypted:	false
SSDEEP:	768:ZQzR48ulhPaIU34IRnevbIrwpZ6ZbtR523mmN3ida4uSz:2zR48ub419SIrqZ2btRmRNg
MD5:	BD65F5019E6123BBC71232A8BC740E1F
SHA1:	86CCDFD6B5B905B8B536748BB289AA39728FB49C
SHA-256:	F3B1A2EE3093CB3CB82AE127127AC1B7A332D047F7BE0B0C1482AB23BD3DA48C
SHA-512:	EC43EDF34F99A752C0CC7AD46483FFFF85E21BEAAAE4A1E7683D9F1D079EF9EBC39B75003DF669AE531003C8118A19B5A509FF1A14CE69AE6A7980A96D06E052
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/36191-Ocean-Earrings-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:9D15EAF8433B11EBB1C5FC42633BAF5D" xmpMM:InstanceID="xmp.iid:9D15EAF7433B11EBB1C5FC42633BAF5D" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:094323e1-c3a7-4b42-881e-466944c6a5ae" stRef:documentID="adobe:docid:photoshop:6fb8cd7f-14fc-014d-ab50-ffd8e8cb961e"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\37207-Ocean-Girl-Cowrie-Choker-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	28028
Entropy (8bit):	7.936937476779356
Encrypted:	false
SSDEEP:	768:ZAEJW3eDb0/jdh8JWiTyQ+zVNyUi/PuJC:uGW3MQjdhxiQzVNQuJC
MD5:	5539425146E9845A9C2A6FDF8B3E74A3
SHA1:	6E7A56E3CA324B2B67A4735008D5C0F1F699A5B9
SHA-256:	2981297DB22C5DBD9A0E347710826545A10EFA08E0345A29C3807B99273216E4
SHA-512:	2EF6EC312374C97BDA9846348E8A96B020B10DD31CDF143A0A881B9895493B4456D46D8F82795D1C95B75908A815D462234DF1475807E2D5C36F19C157E34923
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/37207-Ocean-Girl-Cowrie-Choker-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:054D4300433B11EBAFEC84CF6CFF9F18" xmpMM:InstanceID="xmp.iid:054D42FF433B11EBAFEC84CF6CFF9F18" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:7871e7bf-f926-4666-9556-541b9794676b" stRef:documentID="adobe:docid:photoshop:dba538b4-75ab-5140-94c6-9b7e21066b72"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\38235-HAND-PAINTED-SHELL-BRACELETS-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	38500
Entropy (8bit):	7.9548614534911515
Encrypted:	false
SSDEEP:	768:ZRCwU3aii0UHe18dM+Wiri7fm4HVXYBMYXqtGgCtSyXUkM3yXt:+BZUHSfimy4HVXYtKGJSy36yXt
MD5:	73BF803E8B97780F5A7533A1D85D16B7
SHA1:	FA2D3F84F3A208D2B83E9F2366E797A67004361E
SHA-256:	0F6AB66D18D1700EA87353742A4739A27DD86785CB5714CABBC5815866786488

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\38235-HAND-PAINTED-SHELL-BRACELETS-324x486[1].jpg	
SHA-512:	E76ECC2BEFBE294D8F1E7753BE0D0B22D0DFEE275B940499E6DC33C7F63F0AF93B720FB2CD9B90F9C09D7FE3B767EE0836F583DF4D2461B36B8E813B8F5456F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/38235-HAND-PAINTED-SHELL-BRACELETS-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:37F79967433B11EBB7D6DED4B141B26A" xmpMM:InstanceID="xmp.iid:37F79966433B11EBB7D6DED4B141B26A" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:bdb123c1-661a-4afc-8943-1e7813384c67" stRef:documentID="adobe:docid:photoshop:4f3ca990-c746-1745-87dc-0291e0bbe7cc"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\38241-VINTAGE-NECKLACES-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	33024
Entropy (8bit):	7.943205405197645
Encrypted:	false
SSDEEP:	768:ZG0HbsGb116XQnnDiiGXdRfrcKD7Li5MwnNuzplRjh2fmJXQS4i:Uwbn6XunYXrAKTaM5pThEATh
MD5:	041CD61E96682D9373ADA20AF7E40B05
SHA1:	1D37BD55C3EB5F88794027167C9C8721940A59E6
SHA-256:	0B2190B87BC0054F98318320908800BC491265D6555BFDC60C7D79382B254195
SHA-512:	B8451245DAA2C25985F0C525CE2DB995A3799F1654801452F385BA6B2E6951C9BF77F4C642DDC5CE2B2499E5D1A7D73553E162D0DC92DC7AB8D41F1DAA0FA59
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/38241-VINTAGE-NECKLACES-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:38F2E8C3433B11EB9987975F369A2FA0" xmpMM:InstanceID="xmp.iid:38F2E8C2433B11EB9987975F369A2FA0" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:32982e4b-677f-406f-8155-b6ed8297824c" stRef:documentID="adobe:docid:photoshop:14dc191a-fcf6-a84c-a6e2-4647a3584cfb"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39317-Tie-Dye-Silk-Scrunchies-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	50697
Entropy (8bit):	7.968113790606069
Encrypted:	false
SSDEEP:	1536:lBEVrdywt7zgZ5JMsbdwayok7hjsdqXManDVFr:lBCrzpzmX/yX1sg5z
MD5:	2B615ADEDD3F4342EE78D39AD8B0C91C
SHA1:	1D84A44567C25B9735B2DEF5DCA6780E886C0733
SHA-256:	C16263E4AAD739E4547981EA8D4D93CD2B4EBCE16CD6D68C96108BC53237D10C
SHA-512:	170A50AC3D4CD61E3BE3F69BCC9E1841BC79C6C114EBDFE7DB00630C43EB01210B9666EAA4581DF9FC80DB1AE92A856ED67E4F9FAE441D640DDF013DF0DF244D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39317-Tie-Dye-Silk-Scrunchies-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:8FC687F9CD7FE811B6DDEF9C48BB5FAC" xmpMM:DocumentID="xmp.did:3018AC804B3A11EB978B881073E0CAE6" xmpMM:InstanceID="xmp.iid:3018AC7F4B3A11EB978B881073E0CAE6" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:dd71342e-3b55-cc4f-976c-bc0ddd116c43" stRef:documentID="adobe:docid:photoshop:953a900e-b988-f948-bc3e-a9f05ad20800"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...C.....!...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39843-Sea-Horse-Love-Pearl-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	43911
Entropy (8bit):	7.957984141424705
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39843-Sea-Horse-Love-Pearl-324x486[1].jpg	
SSDEEP:	768:ZlfXf42yXBYDi3QPMUbfKS2ly8HcDGPfsgr0kVjmRhnf6x:b4xLmJr8HxsgrBlQQ
MD5:	8CC4C758D6704835DC54EF7AF920EA76
SHA1:	E012B414AA8F815B286F1A5CAC637D49A27DA3D8
SHA-256:	4DABBD42C086936C0E4F31484E663203FBEC5EFC61924D1D7F0721219C8BC607
SHA-512:	0CB77FCE74BBC1700914C284D5F6D10E96AF80D0B10E2B8C721832AE2CCF9FC83791A2290AC61C554BA3F9CEF461344FC2ACAEB6F9E65A3476BC5F657CD8B9 67
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39843-Sea-Horse-Love-Pearl-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:9857383A433B11EB802285414C34A55D" xmpMM:InstanceID="xmp.iid:98573839433B11EB802285414C34A55D" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:8bca1706-3a28-4b86-911e-3908e6d625d4" stRef:documentID="adobe :docid:photoshop:7c6b9c5b-fd12-754f-906d-d4cbc7c8deb6"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39898-Colorful-Sea-Life-Earrings-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	43945
Entropy (8bit):	7.9648092220900315
Encrypted:	false
SSDEEP:	768:ZSZMD8B+MELBGq4K+BCPQYamonrN/0nVQKk8swKzHBHyywnSVlzka:UuDU+MELBGq4K+BgWmon4DswKzRPd
MD5:	3266F3B23F45C6AA1EBEECF3FE09E334
SHA1:	183BD315E5BF20A59EAA8A5526B9F63626E33E14
SHA-256:	17C60ED249AF6B524AAD533E7C75B276C184EF44C719ADA41C2CDB297ACFE69A
SHA-512:	C799F6B93802AAEC0BCEDF8FC5D6034ADE4340DEC1C8FF6FAF95F2E3FF9D097CB17AEC197C13A5301B255414AE7567B7C1F7EA5BB6D16270C0475B128E5527 FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39898-Colorful-Sea-Life-Earrings-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:9BCCB161433B11EB953C9B5C1405AD0D" xmpMM:InstanceID="xmp.iid:9BCCB160433B11EB953C9B5C1405AD0D" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:fb36cdfa-c6c3-4307-8dba-c3f1c9a2e810" stRef:documentID="adobe :docid:photoshop:facf41a7-83e3-4b4c-8081-26cd72e06959"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39904-Sand-Dollar-Earrings-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	44417
Entropy (8bit):	7.962599470580429
Encrypted:	false
SSDEEP:	768:ZC6XB10lGaGugwIYfAo3CS8TcGwXfkCCBQvKfkdBf1s7GSDz/1OEi/708BK7rilM:sKjISYleB6ekHf1s7GS3L2xKfyKbd
MD5:	E2C3FC0A08977A2CA276587CB74060AA
SHA1:	07F49CCBB7A1F61273EE31E4A9E891319BBB9431
SHA-256:	DF1BD23449914561AE5A5AEC89398FAE9E7E02DFEC919F4EABA1A384E627D864
SHA-512:	155A2E979CD361738A6705A879A480D7E36A33877BB48A609600FEED62C9AE6478F3ED60235D42CEE5F82232E01DD57075B4A35E4E6022044A8AC01F7A1C96DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39904-Sand-Dollar-Earrings-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:9C789539433B11EB9210C1ACA8B56D87" xmpMM:InstanceID="xmp.iid:9C789538433B11EB9210C1ACA8B56D87" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:2fbe20e3-e8c6-424e-b1d0-1f61f282784e" stRef:documentID="adobe :docid:photoshop:1613e677-ba19-1040-9685-63bc488d49d0"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39959-Ocean-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39959-Ocean-Bracelets-324x486[1].jpg	
Size (bytes):	27101
Entropy (8bit):	7.9227550811533485
Encrypted:	false
SSDEEP:	768:Z4U/kUKwV9h48o7VT3hNLE5h6gGrI1dRVky7GB:SU/k0/sLNL4hiIRQB
MD5:	DC3778AE5446EDD87DA5DB4555D40781
SHA1:	9018601DF4558A8C72BF344B4B42ACB34122EB2C
SHA-256:	049D5CA7E30B2C2AA53CB63F1276FAC8E5827267BA5BE2926325644004140B13
SHA-512:	3F8C0DA23F01637E1FA35BB050AD42EE68493C3757990D88FA07CC2C8130C81AAF814BF8CBC874FA73DD83E27EF2F10613302E9E71BACBEFAF607F5E92F6B7 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39959-Ocean-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:9FB6BB14433B11EBA242E494855A9A71" xmpMM:InstanceID="xmp.iid:9FB6BB13433B11EBA242E494855A9A71" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:c8d001b3-97d6-45ab-82bd-891e13743cb6" stRef:documentID="adobe :docid:photoshop:08a8a7e2-1b8d-d44c-8feb-b9a2a7234e7d"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39966-Ocean-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	24427
Entropy (8bit):	7.91403446871713
Encrypted:	false
SSDEEP:	384:Z4n1q6qU2MtkSj73hnMVYCpOQCd5Nuzb6p9i1hFOEn2LqgADH1INSyQD9nu3+cC:ZiAd6ko73hMV5C8z27i1rFTDH1cSBnUu
MD5:	869ED568087306947BFBEF16BEB3C5F2
SHA1:	4560711AC3F122E5531DDE1CD8509D629160FCE9
SHA-256:	21AAADCB5135F3D72201BEA6456943D49737D46B84AD486DF86204F52705BC9E
SHA-512:	F0A5AE5757FB6A84A1ED12D36A6D319187616E0F45D557171DBB64034C84050B587ABCAFC0D0809FC0C9A250DDEBE063BDD4C3A62CEFDFA2EB020857F09609 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39966-Ocean-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:A0618C5C433B11EBA014CA5B4A63F31A" xmpMM:InstanceID="xmp.iid:A0618C5B433B11EBA014CA5B4A63F31A" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:a6fa6977-4b69-4f77-bdb6-6e6ce8ab0498" stRef:documentID="adobe :docid:photoshop:978ef444-54a0-934c-a69c-4bce0dcd7136"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39973-Ocean-Choker-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	22724
Entropy (8bit):	7.899719604262616
Encrypted:	false
SSDEEP:	384:ZhLP7vH/T2iQnbN2D8W+QQsUZhqmeI28Wy8168PnoXE2hIO4XO/PMB1:ZhL32pnbN2wrQQxJeIJ6P+94+/PMB1
MD5:	F79A5D21E7E4712A5A6038FD8D49B298
SHA1:	16E650F13803851FAFF1192CF492B952521EE211
SHA-256:	5FC22DC7A4065CFC35815D2FE00D83F6F797D4F277691D2166140EDF973F9695
SHA-512:	864C23C0A1A890DA8620D7FFB78F4020D5E4E03DC937C992483E2C2D6D619643E6105B328E7F488C8A5076F99D59655CCD57B42ABA1FFDD05B9E4DF0BE8B37 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39973-Ocean-Choker-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:A0FF7327433B11EBB08EEA00DDC85D43" xmpMM:InstanceID="xmp.iid:A0FF7326433B11EBB08EEA00DDC85D43" xmp:Creator Tool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:a0c4a885-c23b-4dfb-999e-dee14a46a0b0" stRef:documentID="adobe :docid:photoshop:050658a9-44cc-4940-b38f-0224799aaa47"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\39997-Sand-Dollar-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	35436
Entropy (8bit):	7.959547873880878
Encrypted:	false
SSDEEP:	768:ZvrIqK5viHxhBHucj6xpJZBT7hizLn74nYGLtgjOmOq9WEbQK3+:5r0BiHNOcWxpJZBH6uZsOAO
MD5:	CC4FDDDFB8440D396C872E56B8638606
SHA1:	04EE540BFB1E8A6E787551B2862646324BFBED78
SHA-256:	78F38A21C321F715DFF8ABDB2E5D91CA8AE9F63DE0877DB295B4BAA2448AA5A2
SHA-512:	8988921E150733297805CAF8E190794AE2FC62CD1EB6E094F9FEBC7ED0475C6B1AC4DF883A66144E11F7D98370ADC34CF2472909A1EFCBA0CE5EA6EEABA52C17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/39997-Sand-Dollar-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:A2543864433B11EB88BD9FA2A2F7AEBE" xmpMM:InstanceID="xmp.iid:A2543863433B11EB88BD9FA2A2F7AEBE" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:533c2610-a189-4368-a11a-3bb21fc39cc1" stRef:documentID="adobe:docid:photoshop:e2adf039-817f-4340-b1f0-77b9d7e4bb45"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50008-Temptation-Colorful-Sea-Life-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	42598
Entropy (8bit):	7.965751878621145
Encrypted:	false
SSDEEP:	768:Z3KyX4Q2pcD7FvuaEtuQp07k/vZqkQFjQDqVQ33GLyvzb469GbslaB:9X4zpcDpvTEtz0l/v0kQFMEiMYbpsg2
MD5:	5DDD49054CBB60CC0942B6406C3AF977
SHA1:	011B747A5C93E7BF901459E875B78BCD74F255D1
SHA-256:	0EE9F70A0C09AB511D7A6D796F1A0784B9F45B012F8ED8988C0689AE7A7A0624
SHA-512:	BF9701B9735A9D783E656F33AE625A6B1AEEC5F589C0D855D2DB0374E09901BDD639AB5CAF7CD22F189CD7334B1A3D5CA3AA818E820634FA67C7E669760B8FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50008-Temptation-Colorful-Sea-Life-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:A3129620433B11EBAAC0A400A26D4B7C" xmpMM:InstanceID="xmp.iid:A312961F433B11EBAAC0A400A26D4B7C" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:91b049eb-b3f9-4c86-812f-08dba06576d9" stRef:documentID="adobe:docid:photoshop:41bdceff-3690-264b-8ea4-e0528914980c"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50015-Temptation-Sand-Dollar-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	41478
Entropy (8bit):	7.956737513103524
Encrypted:	false
SSDEEP:	768:ZI5mQAK3a0rOgM52/nhVN+2MGucaayzetqjWa+scibPHFN2yYKmhBx3SwLLieR4j:GH3brC5SdLMG7JyzOqCfsAyAnh/A
MD5:	6B11798F67EFF6C5B3EA19C614ED8E26
SHA1:	7F1C20171EB52BC22863368B6EC203C9E2422312
SHA-256:	7723749443D87AA542056A55B2AA6B5297162D20139D0B683281DC3DC82AF8F0
SHA-512:	9C0F9CCB9722DA1E158CD192650DCAD37CF900A7D1D8AC8D3EF2112349F5916743A19C290BC2D3F9565A712FD4BB6BE78EB60BBCC94AAC0A651F4331A8330EA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50015-Temptation-Sand-Dollar-Bracelets-324x486.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50015-Temptation-Sand-Dollar-Bracelets-324x486[1].jpg	
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:A3C6AD52433B11EBBC2DD05C12150984" xmpMM:InstanceID="xmp.iid:A3C6AD51433B11EBBC2DD05C12150984" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:3fe06453-d173-4f71-bcac-ae4747b1a780" stRef:documentID="adobe:docid:photoshop:3642b193-412c-3e41-b48a-3f8d7d620a41"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50053-Ocean-Triple-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	29615
Entropy (8bit):	7.938490508661511
Encrypted:	false
SSDEEP:	768:ZjnyTqvJTG3ilF2eXsPmHtw1NRB/M2xuvhUv4:hntwvgXHK1XBZxeh24
MD5:	0BC90651FD9496B81ACB67469D45FB2E
SHA1:	EF4BDF4C2CCB251993C16641F5082E8FF2C5BA26
SHA-256:	1B555185AC60C64ECC0A9BA20A7CB6179F0221E445BD8410CF06035894579F09
SHA-512:	A5C91D7408BE9BF9614B0F34E5D95D3F285C489BA94EC93260B93636D8CC87B408ED0992E787A9E002F6C0460543EC48C7342942C33F78F617F1377DC31DA7A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50053-Ocean-Triple-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:A672A7DC433B11EB9DEE9BECC4CFBF6E" xmpMM:InstanceID="xmp.iid:A672A7DB433B11EB9DEE9BECC4CFBF6E" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:2eea35a2-a120-4bf4-a687-55f6ae808f31" stRef:documentID="adobe:docid:photoshop:a978b43c-8411-514e-a55a-56ae48834803"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50114-Nautical-Sea-Glass-Bangles-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	35070
Entropy (8bit):	7.957176047674977
Encrypted:	false
SSDEEP:	768:Z6XN1vJCdRxa8h6CzneIJvAb+8gihPiMQCLWzQXeJ0Vd8Czd6Gm4:E1R+ra8PneIJvL8tZiMQCLCMCMzdz
MD5:	774D8349F9EC7602FC4E120B984AD2C4
SHA1:	453C62B600CDF337433E23FBC6963AD8240A6D4A
SHA-256:	23A1523CC274CF13A878C6A3A72F8A4C319CF7A6E0B670A90E3A0AA0EFB32E13
SHA-512:	E23B27C8CAA0CDD237BEB7D87BA7A3684F8B1F73CBE940C023A2CB8D80ABB28DBD42CFAA652DDF814A982C06EA6C5B16476F74BDB24ECED3E20115F3D220C5A2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50114-Nautical-Sea-Glass-Bangles-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:AADC0EDA433B11EB9748D0360D91B45A" xmpMM:InstanceID="xmp.iid:AADC0ED9433B11EB9748D0360D91B45A" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:77de3aa8-04d1-4b65-924b-ce00d00c8abf" stRef:documentID="adobe:docid:photoshop:0f18f3c7-874a-f14f-8ae2-a4f3e8552b1e"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50145-Sea-Glass-Expression-pendants-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	42460
Entropy (8bit):	7.964317450539324
Encrypted:	false
SSDEEP:	768:ZT91fB+QE6aXs9NHh765ZGrtdUj5qb5qQaq3km9xEhxIct76rq:bdB+N6As31+at+jsVqQag3N+
MD5:	236C39FF3906C5FE6BBA1836C76FB846
SHA1:	6E213CA73DC0450FBF67F5937AFFD130351BA5F9
SHA-256:	DE5EDD68068411BC581F3036CF2874BAC8F7E3B495290777515B4A4700BBB9BF
SHA-512:	52FE08E4720C25BB161DB7298968D64DF9B2F6AD1EA5B2A4FFC43A2E74A123E2A27B6CE43A7BAF354EB5E53642A7965F0576BB7D347B41BBF3C09E5D7357C87

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50145-Sea-Glass-Expression-pendants-324x486[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50145-Sea-Glass-Expression-pendants-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:ACE01554433B11EBB2DAAA6767CAC571" xmpMM:InstanceID="xmp.iid:ACE01553433B11EBB2DAAA6767CAC571" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:38bf2887-6e18-4226-a563-3bb73877347c" stRef:documentID="adobe:docid:photoshop:e1d61bdb-0087-3f47-8392-f6743f8238ab"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50152-Sea-Glass-Expression-Bangles-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	38290
Entropy (8bit):	7.964083640504361
Encrypted:	false
SSDEEP:	768:Zyi7Nd38+5Gq7kEHgZKSgqsKJYdqb75pbPvwTeKfpb4vzbDRbFnxQ4ze:YYX8eG+gZK4sKJ6qP5pbXnKBibDRRxfe
MD5:	E295A7DE0C0542A4DCA2FCD589673514
SHA1:	4D9F69DE96BE71918E2761B0338B097CF82EC8CA
SHA-256:	46BCCEA54DCFBF50F6C55AAE137BD3B87D5C80168A7215230B494C8F4C1B8C3D
SHA-512:	D3EE2B6D9BA8A5A129C20EE4A9BCD5DECBB509D15683084EA899AB6D39412ECA6A77F2200E934AB07EE6FB569A203543A5A7F391E5A73D73523B04A56590DE4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50152-Sea-Glass-Expression-Bangles-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:AD7C098C433B11EB8DE48AF4CDB0A281" xmpMM:InstanceID="xmp.iid:AD7C098B433B11EB8DE48AF4CDB0A281" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:708b3913-3bb7-4d5b-8156-16c2ec5f67c5" stRef:documentID="adobe:docid:photoshop:f88d4a2a-d74d-1740-a48d-37cfc078d44e"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50176-Crescent-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	24377
Entropy (8bit):	7.917365512815731
Encrypted:	false
SSDEEP:	384:ZkLmjAagTWH61g29U5zIDROBRPSggggXLS2AYhkYcd8uvAJeVzDe:ZMRagcOU5MDROnvgxLS2ZkYcdjvkCzDe
MD5:	0A33A2166FC176557B793EDE80855F82
SHA1:	1B47C8D68CF04205F9834CC5263FF5153E14084B
SHA-256:	D8BEEB1B1152DEF827BF5B2AFF610926D5ED6182CEE579A5D8841E77CAE6FC90
SHA-512:	A054E857831EF55B7D0DEAE65CA5771A66D6B4A823859B3FE9709B9F49C98488E2C8BEF2470BC14EECD6E0B9BB044CDB87D7F1AA159C2B32C2EF13DDBBBB0C47
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50176-Crescent-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:AEB9AF3E433B11EB8B368178CE04672B" xmpMM:InstanceID="xmp.iid:AEB9AF3D433B11EB8B368178CE04672B" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:8edb1e17-b29a-4b26-a598-13758c7cfa32" stRef:documentID="adobe:docid:photoshop:acfc9502-8291-4a4b-bc78-2e5ded87dc64"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50459-Phone-Lanyard-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	34693
Entropy (8bit):	7.964816907794131
Encrypted:	false
SSDEEP:	768:UwyDZBt2APeDnlIxvknO5Z6nXonriWLzvJ29C:yzeDzOWYRLzgI
MD5:	0B16F66FFF2D11F751246529B86A4BA3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50459-Phone-Lanyard-324x486[1].jpg	
SHA1:	607C56128E34C10571F7B715B858A43CC64DE513
SHA-256:	6A1801167A2E0F39BB1A5713BB774E3CFF75916AF616E918E04CA5040C1A5670
SHA-512:	1E214126763716A295EE8512DF1CB88188F7EA88DEB8A486C36307AAA88DF5CEDABA59422F64EC528BA0F5636B2B794E44ED94D7B988F69BD0CADDBF1D392F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50459-Phone-Lanyard-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:BEB3C55A433B11EBA75589D8AF904089" xmpMM:InstanceID="xmp.iid:BEB3C559433B11EBA75589D8AF904089" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:b80cbcde-6500-4d3d-aa0c-911148621a36" stRef:documentID="adobe:docid:photoshop:05e8babd-eae5-6844-adef-c3f898417cb7"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50565-Aluminum-Zoom-Clip-Light-1-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	41447
Entropy (8bit):	7.974411733716736
Encrypted:	false
SSDEEP:	768:ZA1hg9aeVDWIxOF7ejWf81ZSjjRLsCuqoUsT++VadjP7:i1acscei6Z+jRL1sU27Vadb7
MD5:	35E47B886ACF28C24CCF5AF5C87A8B65
SHA1:	BE86A79F3FDF19ACBC38F9E7CD373646ECA25D9F
SHA-256:	896CDAD15E1387F3FC13445D84D4D4CB28D6C05B40E55E94F6801EA8A0DAD721
SHA-512:	BBC7CF8BD108922E8F29B840D95DC7988D5C3712A94FECC1826D7DC33BBDF976C23C3927ECBD46E55BEB217B2F0059F2E9CB83390AE1583C54C51C6EE4878E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50565-Aluminum-Zoom-Clip-Light-1-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:C474639E433B11EB94D88C06B21F9FAC" xmpMM:InstanceID="xmp.iid:C474639D433B11EB94D88C06B21F9FAC" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:f87f6564-3147-45fc-8dcf-4c18f6e9b86b" stRef:documentID="adobe:docid:photoshop:cda5afd8-b38e-704a-8336-69d32a568deb"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50633-Zodiac-Letter-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	35184
Entropy (8bit):	7.956101345315509
Encrypted:	false
SSDEEP:	768:Z8xagyAwtbo7lrm9aZzI45RZ7Fwq/hLQ12nsycbOuj3:6ryAwym0ccLZLQZ7KK3
MD5:	C2E1B1C86CB38A23BF6377416034C1DE
SHA1:	2C8363DAAE24636C228F01CFC6AFCB1937FD5470
SHA-256:	F5E9BB6512A14FA8C2B7C91A8939040DA1D38D8E6FAFD6C59BCA6655F67F404A
SHA-512:	4D0658ECEF6E32DEE5AAC85F69EA53A64B5E819DD426DA9DCF5893A4C3F17490A134D87DB1D8838010C7B16A5CDCE962B3DDCD2709F6331B7BE5D8EF3C551AFF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50633-Zodiac-Letter-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:C97DD69B433B11EBA1AA86238675421A" xmpMM:InstanceID="xmp.iid:C97DD69A433B11EBA1AA86238675421A" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:1dadd2a5-7b08-44c5-bcf1-bc2fbc54baf7" stRef:documentID="adobe:docid:photoshop:7dbc86eb-f8c7-904b-80bd-68bf5e225cb0"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50657-Sentiment-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	31776

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50657-Sentiment-Anklet-324x486[1].jpg	
Entropy (8bit):	7.953181668411169
Encrypted:	false
SSDEEP:	768:ZSJ2wNfqWswJhUhkaSWbEL2+uE7hlEwh8FYnvqNzNOy:GNf5swzUiv/uE12wCansly
MD5:	5184E52F5AA49D4292853D00EC0E18DE
SHA1:	63BDD552A3988257FF793D574CCC5105792D6F0A
SHA-256:	701AE2467CC9356E2E874EF167E2A274EC6A4D48B47B91D4FCA93FA2FE6B4510
SHA-512:	F8ADF100A61F0B10DB0476FB76A160509FCE3A35F105DB7209DEB93F2A1C1D916E14731D59DF968CB22392A9CEA7E3BB85BB21144EE6BC782D4447104A00591D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50657-Sentiment-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:CABCDD56433B11EBA148FFD53C315CBF" xmpMM:InstanceID="xmp.iid:CABCDD55433B11EBA148FFD53C315CBF" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:06604b10-eefa-452b-9aa9-4b08377d5fb8" stRef:documentID="adobe:docid:photoshop:b1f54fe1-bfd9-8841-a047-4e302781eb5a"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50701-Multi-Dainty-Necklaces-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	24357
Entropy (8bit):	7.896904234055267
Encrypted:	false
SSDEEP:	384:U2dKgQC9/ZbuAirCBJVNbqAP81tqRuoLeYPMeQFzBi1o77S:UVgQCtvFN2APitE5bP+F9ywS
MD5:	E1F0151429A6FE3C3DDCB964D02C03DA
SHA1:	8798D2899FBAD34F19D9E7A2B5F0FD1317BA0EEB
SHA-256:	EFD4CD756495ED38926A62C52AFA610F8EE5ED28F6F1CFD05CB84BF2639E0951
SHA-512:	C01953C6F057D14718692FFB9EF0D6748B25E2299226449F8404BF6E2CFD7339C93173994172D7745AAC64CBCA916F9514B2CBDD744D1D6AFFC8DEC36BB7A9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50701-Multi-Dainty-Necklaces-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:CDEC4566433B11EBB0CBB40C9545288D" xmpMM:InstanceID="xmp.iid:CDEC4565433B11EBB0CBB40C9545288D" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:a7a01113-11d1-440b-97ba-ebb09cc15dd2" stRef:documentID="adobe:docid:photoshop:d47f4701-6de6-f741-89ae-f2ecc340ba5d"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50718-Multi-Dainty-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	24647
Entropy (8bit):	7.90357070176987
Encrypted:	false
SSDEEP:	768:UuJWSlyoWRy/kR5SOQ4yZGZBDyQnD5bwsT:TgSMRIkR5SOQ4BBDyQn5w6
MD5:	28541DF0E98852CE4392C399FC2AB7DE
SHA1:	8D4B7A9F90DCE45B94E8BD4CB851A8D6301344AE
SHA-256:	12046BBC5A0C5DDC45FB6E72F7E7AD98254AAE7728CF4CCB8E51EFCD397CBCD0
SHA-512:	57A8BFA0346B81D8B4347045D297FC4A80D9CAF52CF96AF5EE4BB44F3FEDA7BB8450F94F6F327C06462A5FFA0F13D39F7E66A62CDB30CE9211D190E20D7D907
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50718-Multi-Dainty-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:CE8E417C433B11EB8F55F764CDF8A5B2" xmpMM:InstanceID="xmp.iid:CE8E417B433B11EB8F55F764CDF8A5B2" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:e91893b2-a8fd-4a61-a0e9-aadc0e027510" stRef:documentID="adobe:docid:photoshop:b8ec77fb-aafb-3b4c-8bec-b00433a004b5"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50725-Multi-Dainty-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50725-Multi-Dainty-Anklet-324x486[1].jpg	
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	26516
Entropy (8bit):	7.9324115582992345
Encrypted:	false
SSDEEP:	768:U72nW1LYY2tbsj2LwcoiUWh8ZBH7WEBAwgJ6:HWGej2LwcGWh+BbbBAZ6
MD5:	EB6D61A603BFF69B79D434A3CEE98653
SHA1:	BEA4D6D06A4FA670675F535F56283EBBC7DD5DD1
SHA-256:	53802248548EF9EB75466995934A711E801A4D496548887DE6F331D53FFC23AC
SHA-512:	F5026D33A7592CDB1345F450CE3B2B3B32A4C2B48D35D75EEF6D781D04CE274D641F250007893400656DDBC9212CB74BBC9DC6C56B95A519853C279F836EC7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50725-Multi-Dainty-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:CF3487C9433B11EB8B11F5396F71E0DC" xmpMM:InstanceID="xmp.iid:CF3487C8433B11EB8B11F5396F71E0DC" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:cf5b15d4-1156-4c57-8d56-31950b43b1a2" stRef:documentID="adobe:docid:photoshop:11d814fa-19d4-034c-bce4-372f75617c5f"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50749-Multi-Celestial-Anklet-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	28934
Entropy (8bit):	7.942708767733112
Encrypted:	false
SSDEEP:	768:ZKBLPABxV/TbIK91ScugpTZkg9lqhHwetanOp1Xylk:MGbPIK+cugNZkg9lsQeonU1Xylk
MD5:	2F71182472BB5EDB51F9AF1A956B6797
SHA1:	B30AEF5A9DC64BCC6DA59D89115613758DF31540
SHA-256:	33A5DF3E006BAFBCBB38FD19E1B3FB738F016DCAD1BBCAF5E87EB639B7EA6B21
SHA-512:	EC5A26F9E6D30A01083138F30BA878A5EC061642BF69A71B953E4F8250CB91AB15328503F5EAA5C9E1504FC14A859C099BE1921CDCECD9D297984422105369D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50749-Multi-Celestial-Anklet-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:D099BD9E433B11EBBFFDB422DD1D4247" xmpMM:InstanceID="xmp.iid:D099BD9D433B11EBBFFDB422DD1D4247" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:428cc7fa-206f-4815-9bf2-8eca0160d247" stRef:documentID="adobe:docid:photoshop:c0abebfd-54b2-0343-a639-ff1334c6b74e"/> </rdf:Description> </rdf:RDF> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50763-Sun-Moon-Choker-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	33303
Entropy (8bit):	7.9504413738205075
Encrypted:	false
SSDEEP:	768:UXcJ/el0BTQSndAGmMHH+qpdwnM3DM2lpR0n4sEMlcsM85xx:icJ/elgdUMn/pWn3nbEMCUxx
MD5:	DF1B90CA2A489CE279C978437AB9B2D7
SHA1:	06B5545738275279A678B124AC4AA5572FB4084F
SHA-256:	701FC422995965F8A7AB722979FA9E5950CAD07559431169946E49A31C7B2D2E
SHA-512:	55B59D81BD8D2FE7F0D9A0E0C62E784EDF589DED648657A58A9191B5ABCA34658EFC851DB1BCE705E04F653F5577808B42E51E2CE9BD36D1DF47DE4BF559C623
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50763-Sun-Moon-Choker-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:D1EEAD8B433B11EB861ECC3548702E44" xmpMM:InstanceID="xmp.iid:D1EEAD8A433B11EB861ECC3548702E44" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:bb23fcec-039f-4d4f-b70c-7009ca762cbc" stRef:documentID="adobe:docid:photoshop:81303408-00d4-a94e-826a-b871d72ef803"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50770-SunMoon-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	36802
Entropy (8bit):	7.940778146852601
Encrypted:	false
SSDEEP:	768:Udnmk16Cl9VYzxLMxMO4FJNliNTfYgFDlaMU2+7M/Npi1u5vuCN3lo1bf:XTYVIgf6tiNznXU2MyKu5u9p
MD5:	11014D782F06E8CE1875EF1C4ED5C605
SHA1:	50C7949B8831FF9B7AA40FC5100F3A2DB58EAD4A
SHA-256:	49151ABBD222739BACA71EFCAE41DCF8DF2F5BAD7BB6C6CBC98D2FEF05CED109
SHA-512:	BB0E6D74CA13B0AB6AE6B1EC073C614445B8BF9701979A077E4F4CC9EC50CAE7DD3EB34E3F05DD081A30A5119DDA38F7229D298D3761F1ADF1F4D6A3747FF4 14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/50770-SunMoon-Bracelets-324x486.jpg
Preview:	.....JFIF.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:D2A00EFA433B11EBB2FB8F81D42192EC" xmpMM:InstanceID="xmp.iid:D2A00EF9433B11EBB2FB8F81D42192EC" xmp:Creator Tool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:9df5e5c6-8d0b-45f3-96a6-014c5c5180e6" stRef:documentID="adobe:do cid:photoshop:df131fed-ddd8-0749-bde6-5e9618584c13"/> </rdf:Description> </rdf:RDF> </x:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Bracelets-Dream-Catcher-Macrame-Bracelets-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	35144
Entropy (8bit):	7.97069533165582
Encrypted:	false
SSDEEP:	768:mCHs0mEO++K8AK8QT3XDI4PCGhvzN9CPr3JQ2KSR0rhjjG:mCHNmEO++Zd8C3XBPJz+PtQ2Ohjy
MD5:	E2C9A7A875955EA0442819C9478259C0
SHA1:	10E0E021B1DB422E954163B3A28099C999069394
SHA-256:	301FDADC82B93AA595284BDB21F7F970E73EDC5B64A62B3D69F676EE1B350E5B
SHA-512:	93890CFBEA971BB0453D7624358E901BC6656401FAE7CA53E5F3AD5777CA1E181A4A2EA5B506E44DCA1B96AD9EB009152916B5B7599FCF5649DEB82140D9E07 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/Bracelets-Dream-Catcher-Macrame-Bracelets-324x486.jpg
Preview:	.....JFIF.....H.H.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:x mptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:ab out="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" x mpMM:DocumentID="xmp.did:6613846DB5C511EA9B17D88034A4976D" xmpMM:InstanceID="xmp.iid:6613846CB5C511EA9B17D88034A4976D" xmp:Creator Tool="Adobe Photoshop CS5 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:ACF504BF9C4B11E4BD359AD9CD7B13D5" stRef:documentID="xmp.d id:ACF504C09C4B11E4BD359AD9CD7B13D5"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Coconut-Tie-Knot-Bracelets-Niagara-Falls-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	37331
Entropy (8bit):	7.973389077654859
Encrypted:	false
SSDEEP:	768:hLjLyrK8xFpp7iT8qrv9jcimQmA3L1NEaIjwncpNv6:hLjLcKCFr7LqJciBd3L3Eaowncpx6
MD5:	67D53643DDB8FFF149E3D46AC3A166FA
SHA1:	6B7E2B0B39E0EC004440DA951D01928420BC9ACF
SHA-256:	8F59E70391C922F093B58CC58FC1D8061FFB4077723ADEBEC6D48A7297B7A961
SHA-512:	77FB909BE3177FA1BAF9F289FED42480BD1196ECF07F49A829FBD6946479B63648758BBE557BB911B22FD09E9A5D287E88B401E70573F462D0598571E62CFC4F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/Coconut-Tie-Knot-Bracelets-Niagara-Falls-324x486.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Coconut-Tie-Knot-Bracelets-Niagara-Falls-324x486[1].jpg	
Preview:	.....JFIF.....H.H.....Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:OriginalDocumentID="uuid:36B45AEB49F2DF11AEFDA6A493E650BA" xmpMM:DocumentID="xmp.did:320F7CFCC34211EABB3FE527DB9EA0A0" xmpMM:InstanceID="xmp.iid:320F7CFBC34211EABB3FE527DB9EA0A0" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:FCBBB275C33F11EA965FF3BE10F1E1EF" stRef:documentID="xmp.did:FCBBB276C33F11EA965FF3BE10F1E1EF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\O83YBFSH.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	113134
Entropy (8bit):	5.2689574822976395
Encrypted:	false
SSDEEP:	3072:S8PRs1CxtXzim11g8zbhkRxsQ0QS0nmXgcMimaCDnD7NGFduZC:dbC0
MD5:	8C154D42AD0CC3282FE58B7F801971BB
SHA1:	63D2FB5E562125FB0F8D23633B9175611EE199F1
SHA-256:	149D3D51451A19C92CD1C1A6892BF7B4A65E3AC56B1EAAA286ED45DCF4A57DEC
SHA-512:	360AA84F321B2313ACF2AB65E2D862CAA057C96B7C3B447E6F548D221DD3F1D0BD93D6117DF3D5F5789F5F865E2909EBB1CB5D878F21EDFFCBD8F541263417 5
Malicious:	false
Reputation:	low
Preview:	<!doctype html>.<html lang="en-US">.<head>.<meta charset="UTF-8">.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=2.0">.<link rel="profile" href="http://gmpg.org/xfn/11">.<link rel="pingback" href="https://www.pukacreations.com/xmlrpc.php">..<title>Puka Creations – Distributor and Importer</title>.<script>window._wca = window._wca || [];</script>..<link rel='dns-prefetch' href='//s0.wp.com' />.<link rel='dns-prefetch' href='//secure.gravatar.com' />.<link rel='dns-prefetch' href='//stats.wp.com' />.<link rel='dns-prefetch' href='//fonts.googleapis.com' />.<link rel='dns-prefetch' href='//use.fontawesome.com' />.<link rel='dns-prefetch' href='//s.w.org' />.<link rel="alternate" type="application/rss+xml" title="Puka Creations » Feed" href="https://www.pukacreations.com/feed/" />.<link rel="alternate" type="application/rss+xml" title="Puka Creations » Comments Feed" href="https://www.pukacreations.com/comments/feed/" />.<link rel="alter

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\PERSONAL-GUARANTEE[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	269
Entropy (8bit):	5.285209944578671
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPic4omJY7zmh+KqD:J0+ox0RJWWPwOlT
MD5:	E819A34FFE59B8DC3B9D396E4B8DE2EB
SHA1:	ACBE8DF147C264F4C014E0F7BDF7CA58889464AC
SHA-256:	A1E6A451FACE645E653C485C7771EE5DB0A29C82469011DF03EEE3F72781E8C1
SHA-512:	22418B1A05AEC59FF7076819CD1671B21C601DA8C7F40565483CC4754A17AF08251B620127E1F25CCACACF60013072BC016147FDA3B799E5858D2997A46141F7
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Rings-10498-1-324x486[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=12, height=852, bps=158, PhotometricIntepretation=RGB, orientation=upper-left, width=612], baseline, precision 8, 324x486, frames 3
Category:	downloaded
Size (bytes):	68666
Entropy (8bit):	7.901547784240792
Encrypted:	false
SSDEEP:	1536:1vet+vxnWvFHRf7T2NG7pUuU4unHYfhh3V4y7N2BcEWH:lWvFxf7CQpvU4+HshR7NXH
MD5:	FE695B95BD74D1768946829D1159CD59
SHA1:	9C74965DE9CB78097E06C6984B19DAF6282A0E10
SHA-256:	80700A22339FD1A5BDFC0FE85839E3B082E62C5488BAE26844DDB099C819A156
SHA-512:	5A9D58C28CCDE2C2FD2EA0DF3163895EFCCB153ADCDD990DF5B8E1C75168E6D9D2074FAD1160D6E1324867C183F63FE8A80C9E068C4B79F25B43CBF1FFD34 A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/Rings-10498-1-324x486.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Rings-10498-1-324x486[1].jpg	
Preview:	......JFIF.....H.H....%.Exif..II*.....d.....T.....(.....1.....2.....i.....H.....H.....Adobe Photoshop CS5 Windows.2019:02:12 20:40:08.....0221.....d.....T.....j.....r...(.....z.....7$.....H.....H.....Adobe_CM.....Adobe.d..... .....s.."....?.....3.....!.1.AQa."q.2.... .B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F..... ...Vfv.....'7GWgw.....?..T.I%4z.[.-.3:.S..5..:C.....|.r.e.<YU.Z.....7.....+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\add-to-cart.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2750
Entropy (8bit):	5.0324336359537964
Encrypted:	false
SSDEEP:	48:ZpMj3FLJ9HruTM4Qbpza2lyLXZfIYtpNa2SyGbVHf9Q4B7p3EpjiJf:bMj35JZuTW9a2HLXhIQHa2S9dBB2UJ
MD5:	51826BF206887D13AB2E82A8A7245C64
SHA1:	72F4D6B6C3F88DAA45C9CE042D9CB7E5166E9165
SHA-256:	7B082DAADD28B14604F37E9476DAB0A901DBC19F82808056E27BE8CA2AF1FD98
SHA-512:	E6B05DC7669179E9997E35AE1555CF10D7A31385D00CBC271A0A1D65D00DB38953A4F6DEC0F41DA3D43DB242D1D73A7EA27491086D678D508A15AD8FFC4643
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=3.8.1-b-modified-1577141261
Preview:	jQuery(function(o){if("undefined"==typeof wc_add_to_cart_params)return!1;function t(){this.requests=[],this.addRequest=this.addRequest.bind(this),this.run=this.run.bind(this),o(document.body).on("click",".add_to_cart_button",{addToCartHandler:this},this.onAddToCart).on("click",".remove_from_cart_button",{addToCartHandler:this},this.onRemoveFromCart).on("added_to_cart",this.updateButton).on("added_to_cart removed_from_cart",{addToCartHandler:this},this.updateFragments)}t.prototype.addRequest=function(t){this.requests.push(t),1===this.requests.length&&this.run()},t.prototype.run=function(){var t=this,a=t.requests[0].complete;t.requests[0].complete=function(){"function"==typeof a&&a(),t.requests.shift(),0<t.requests.length&&t.run()},o.ajax(this.requests[0])},t.prototype.onAddToCart=function(t){var a=o(this);if(a.is(".ajax_add_to_cart")){if(!a.attr("data-product_id"))return!0;t.preventDefault(),a.removeClass("added"),a.addClass("loading");var r={};o.each(a.data(),function(t,a){r[t]=a}),o(d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 6 x 5
Category:	downloaded
Size (bytes):	50
Entropy (8bit):	3.8488255736198
Encrypted:	false
SSDEEP:	3:CN+ltRPQEsJen2sSX:xvQEsJ42sSX
MD5:	E4D673A55C5656F19EF81563FB10884C
SHA1:	1F2D8ED221D39329251AD3A6FF1EDB20B7219443
SHA-256:	F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1
SHA-512:	E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B1B479D027016D5BEB148403EF185430DB35F5FAED362F36CE2C8ECAD0E6D8E30CEA97E 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.wp.com/c.gif?s=2&u=http%3A%2F%2Fpukacreations.com%2Fdocuments%2FPERSONAL-GUARANTEE.pdf&r=&b=142400183&p=4237&rand=0.2709828608213104
Preview:	GIF89a.....!.....,.....bx..j....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cart-fragments.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2940
Entropy (8bit):	4.991535514511927
Encrypted:	false
SSDEEP:	48:oiu6oNl0R9SxGkYK2ITm5mej11i/nOrIkX6OLbf1i/u/apqWt7g1i/qXRYyQENli:c2rBBL2nYw/U5Fe
MD5:	3518C9CF4786D55C48E6B318CDF3C8DE
SHA1:	EE13E5307A87355B9C35AA2E2907F642839A80CF
SHA-256:	BED0BD033705C33F1742D8FAB2BFED8E945567319FD00E529838392ECA49EAC0
SHA-512:	3DF98EED03673BD9DF5E8B8E0EFC490834A32D6BD80A7434D6C184F19922922CE8B8992703B331863CC030484CB97AF6D1090CBE2828EEC0EB4979982712E3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=3.8.1-b-modified-1577141261

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cart-fragments.min[1].js	
Preview:	jQuery(function(r){if("undefined"==typeof wc_cart_fragments_params)return!1;var t=!0,o=wc_cart_fragments_params.cart_hash_key;try{t="sessionStorage"in window&&null!==window.sessionStorage,window.sessionStorage.setItem("wc","test"),window.sessionStorage.removeItem("wc"),window.localStorage.setItem("wc","test"),window.localStorage.removeItem("wc")}catch(f){t=!1}function a(){t&&sessionStorage.setItem("wc_cart_created",(new Date).getTime())}function s(e){t&&(localStorage.setItem(o,e),sessionStorage.setItem(o,e))}var e={url:wc_cart_fragments_params.wc_ajax_url.toString().replace("%%endpoint%%","get_refreshed_fragments"),type:"POST",data:{time:(new Date).getTime()},timeout:wc_cart_fragments_params.request_timeout,success:function(e){e&&e.fragments&&(r.each(e.fragments,function(e,t){r(e).replaceWith(t)}),t&&(sessionStorage.setItem(wc_cart_fragments_params.fragment_name,JSON.stringify(e.fragments)),s(e.cart_hash),e.cart_hash&&a()),r(document.body).trigger("wc_fragments_refreshed"))},error:func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\colorbox[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	6111
Entropy (8bit):	5.162112064760633
Encrypted:	false
SSDEEP:	96:XYArEpK64P4dOzj4fJFjfIdhQcop0Ft27qXNhImE:IAo1nYzj4xBfMK6y
MD5:	92A8BDFC37BA21A5419B51613277EFB6
SHA1:	50BB983B967D1154CFEAF392325C7FA9165D7C89
SHA-256:	89C3AAB4325C99052335B59C3099CF49AC0B81D0082C0B6970C9AF1E3AF1690B
SHA-512:	CD96EE2A3783216E5E1BA8DDA416BE13D18C8E588384C96A75997122E4E3F87F32211DC56C25C89F3DB6D7F17828BD0839F2FFFCF6D23ACC065F0EEA9289A0 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/wp-content/plugins/woocommerce-login-and-registration//assets/css/colorbox.css?ver=5.3.6
Preview:	/*.. Colorbox Core Style:.. The following CSS is consistent between example themes and should not be altered...*/..#colorbox, #cboxOverlay, #cboxWrapper{position:absolute; top:0; left:0; z-index:9999; overflow:hidden;}..#cboxWrapper {max-width:none;}..#cboxOverlay{position:fixed; width:100%; height:100%;}..#cboxMiddleLeft, #cboxBottomLeft{clear:left;}..#cboxContent{position:relative;}..#cboxLoadedContent{overflow:auto; -webkit-overflow-scrolling: touch; }..#cboxTitle{margin:0;}..#cboxLoadingOverlay, #cboxLoadingGraphic{position:absolute; top:0; left:0; width:100%; height:100%;}..#cboxPrevious, #cboxNext, #cboxClose, #cboxSlideshow{cursor:pointer;}...cboxPhoto{float:left; margin:auto; border:0; display:block; max-width:none; -ms-interpolation-mode:bicubic;}...cboxIframe{width:100%; height:100%; display:block; border:0; padding:0; margin:0;}..#colorbox, #cboxContent, #cboxLoadedContent{box-sizing:content-box; -moz-box-sizing:content-box; -webkit-box-sizing:content-box;}..../* ..

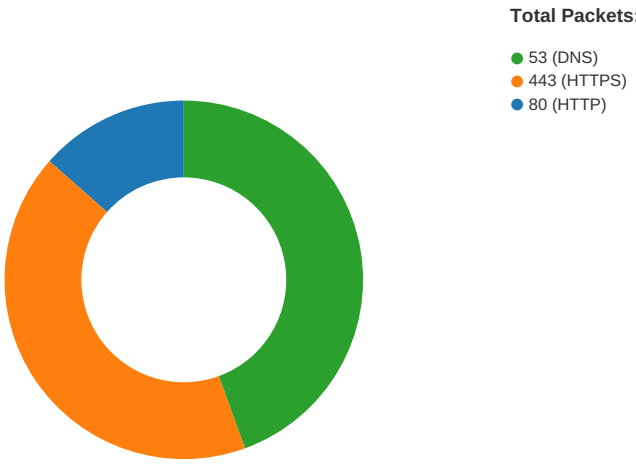
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cropped-logo1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 470 x 110, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	19774
Entropy (8bit):	7.967156268983178
Encrypted:	false
SSDEEP:	384:UZYwv9V3mU6uoy5idCOF+wG0vw1wMHAq6sCvdk:z2Vvoy5iddF+wG0YmbsCvdk
MD5:	B22260B7ED8BF75B9ECB5FD5458D894C
SHA1:	79ACADE1AF545BD5B25B54250B86D7E1B78B09C5
SHA-256:	4526A58671A89EE44E72C05D78BA08F0BA2B11F7ECA815A8E47F524CC784B267
SHA-512:	6D2C0622AE8F8B54AE8CA11E64B690DE2AA87F00ED63FFC9276D34DF7B32867FEFCAD4B2DA7846922A3A74966A37F86349AECD837E8FC8F45ABF8A1766DE1F BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.pukacreations.com/media/cropped-logo1.png
Preview:	.PNG........IHDR.......n.......2.....gAMA......a.....sRGB........ cHRM..z%.............u0...`..:....o._.F....bKGD.............pHYs..............L3IDATx..}w|\...3s......2...l ..1....z.@ .$.NB..G.!..BK ...B(..L.q.]..-.r..|...^..JZyeKf....w..9s.s.9.((.H.........&...B.e.iF<.Y.E....:.....B..z...c.R...ilQ......@..B.B.)...m.Z.9/%..E.=!.......xt.=B.;..&.|..nUPPP8.H.s6.0..u];m...S*&N.....R.<.nR...C0.@mMu....p...^...Zy."V.....84.....]>j..sn...AF...X4.@ ..@.g.^. ...PZZ.....55..y.....fE4.-.z.wUN...@T74+bUPPP...16..KJK....+.._r.....~.-|.r%......Yw[..{t..5...-..'..i......>...a..B...6d.*bUPPP8..9?L.SO9......--..{..o.......UM.i..f..M..!.8.{.N.J).y..._._..&\~.U..k.{K.^..]...8.X....>....G.r..g.....><..s.F..@.QZZ..3f.......{.*..._......a ..!.......@..i..^mg............%Kp......x<~.F...*(((|.!8.5z...c.a.....w..Tsrr0..|\\|..X.p!......B.+.&{..\-.B<.GWW.ZZZ.s.N.Y...~.)...]

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:44.217222929 CET	49715	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:44.217442036 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.226598024 CET	49715	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.226619959 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.426961899 CET	80	49716	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:45.427005053 CET	80	49715	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:45.427094936 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.427151918 CET	49715	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.427608013 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:45.627808094 CET	80	49716	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:45.629122019 CET	80	49716	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:45.629242897 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.144900084 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.145687103 CET	49719	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.345189095 CET	80	49718	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:46.345314980 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.346419096 CET	80	49719	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:46.346563101 CET	49719	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.346599102 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.546845913 CET	80	49718	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:46.549376965 CET	80	49718	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:46.549526930 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.727586031 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.932112932 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:46.932240009 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:46.937553883 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.138529062 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.155530930 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.155572891 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.155606985 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.155625105 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.155667067 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.155697107 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.186561108 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.191780090 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.191987991 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.388151884 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.388252974 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.388403893 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.388465881 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.388911963 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.392920971 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.393050909 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.393146038 CET	49721	443	192.168.2.3	69.163.233.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:47.539486885 CET	80	49716	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:47.539635897 CET	49716	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:47.627130032 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:48.546679974 CET	80	49718	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:48.546775103 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101106882 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101154089 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101191998 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101229906 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101267099 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101313114 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101370096 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101401091 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101439953 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101491928 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101521015 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101562977 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101582050 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101629972 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101667881 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101711035 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.101727009 CET	443	49721	69.163.233.5	192.168.2.3
Jan 11, 2021 18:24:49.101824999 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.174602985 CET	49718	80	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.175060987 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.175478935 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.175952911 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.176299095 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.176629066 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.176958084 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.177278042 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.177849054 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.181488037 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.181826115 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.182264090 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.185630083 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.188694000 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.192142010 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.199932098 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.200437069 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.200978994 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.201402903 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.201767921 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.202219009 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.202610970 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.202986956 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.203381062 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.203727007 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.204073906 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.205280066 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.214749098 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.215178967 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.215522051 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.227783918 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.228945017 CET	49721	443	192.168.2.3	69.163.233.5
Jan 11, 2021 18:24:49.239006996 CET	49721	443	192.168.2.3	69.163.233.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:38.172239065 CET	63492	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:38.223099947 CET	53	63492	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:39.128606081 CET	60831	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:39.188244104 CET	53	60831	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:40.293557882 CET	60100	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:40.344356060 CET	53	60100	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:41.589706898 CET	53195	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:41.637804031 CET	53	53195	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:42.864684105 CET	50141	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:42.924844980 CET	53	50141	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:43.146488905 CET	53023	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:43.194886923 CET	53	53023	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:44.028151989 CET	49563	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:44.206650972 CET	53	49563	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:44.412203074 CET	51352	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:44.460273027 CET	53	51352	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:45.980978966 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:46.117582083 CET	57084	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:46.143296957 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:46.165535927 CET	53	57084	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:47.414110899 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:47.462162971 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:48.368379116 CET	57568	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:48.416637897 CET	53	57568	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.189929962 CET	50540	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.208178997 CET	54366	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.227492094 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.236186028 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.255970001 CET	53	54366	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.256877899 CET	53	50540	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.275295019 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.302508116 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.573491096 CET	55435	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.584631920 CET	50713	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.621916056 CET	53	55435	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.635884047 CET	53	50713	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:49.876015902 CET	56132	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:49.926796913 CET	53	56132	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:50.881527901 CET	58987	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:50.946672916 CET	53	58987	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:52.351856947 CET	56579	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:52.399827003 CET	53	56579	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:52.641239882 CET	60633	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:52.642219067 CET	61292	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:24:52.690689087 CET	53	61292	8.8.8.8	192.168.2.3
Jan 11, 2021 18:24:52.705566883 CET	53	60633	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:02.558336020 CET	58722	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:02.558571100 CET	56596	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:02.558648109 CET	64101	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:02.606421947 CET	53	64101	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:02.606461048 CET	53	56596	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:02.612004995 CET	53	58722	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:03.114521980 CET	63619	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:03.162558079 CET	53	63619	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:05.392510891 CET	64938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:05.457993984 CET	53	64938	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:10.965033054 CET	61946	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:11.024234056 CET	53	61946	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:11.761518002 CET	64910	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:11.819444895 CET	53	64910	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:12.682961941 CET	52123	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:12.733688116 CET	53	52123	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:12.870193958 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:12.920790911 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:13.573169947 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:13.632632971 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:13.865833044 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:13.925028086 CET	53	56130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:25:14.568758011 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:14.616561890 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:14.904500008 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:14.955244064 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:15.736068964 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:15.784019947 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:17.202938080 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:17.254465103 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:17.740168095 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:17.796966076 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:21.196149111 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:21.247013092 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:21.742980003 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:21.790899038 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:29.983738899 CET	59420	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:30.041496038 CET	53	59420	8.8.8.8	192.168.2.3
Jan 11, 2021 18:25:57.819844007 CET	58784	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:25:57.884322882 CET	53	58784	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:01.312844992 CET	63978	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:01.372826099 CET	53	63978	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:05.251375914 CET	62938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:05.310691118 CET	53	62938	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:36.923533916 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:36.983416080 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:36.994399071 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:37.052274942 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:37.936311007 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:37.992932081 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:37.998936892 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:38.046911001 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:38.999383926 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:39.057241917 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:39.138484955 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:39.195580959 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:41.041208982 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:41.098191977 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:41.133327961 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:41.195921898 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:45.152101994 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:45.152196884 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:45.208657026 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:45.208703995 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 18:26:48.929249048 CET	57145	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:26:48.977263927 CET	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:24:44.028151989 CET	192.168.2.3	8.8.8.8	0xe045	Standard query (0)	pukacreations.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:45.980978966 CET	192.168.2.3	8.8.8.8	0x541e	Standard query (0)	www.pukacreations.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.208178997 CET	192.168.2.3	8.8.8.8	0x8726	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.227492094 CET	192.168.2.3	8.8.8.8	0x8004	Standard query (0)	stats.wp.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.573491096 CET	192.168.2.3	8.8.8.8	0x3614	Standard query (0)	s0.wp.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.584631920 CET	192.168.2.3	8.8.8.8	0xfaa3	Standard query (0)	secure.gravatar.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:52.351856947 CET	192.168.2.3	8.8.8.8	0xcffc	Standard query (0)	pixel.wp.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:25:10.965033054 CET	192.168.2.3	8.8.8.8	0x334f	Standard query (0)	www.pukacreations.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:24:44.206650972 CET	8.8.8.8	192.168.2.3	0xe045	No error (0)	pukacreations.com		69.163.233.5	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:46.143296957 CET	8.8.8.8	192.168.2.3	0x541e	No error (0)	www.pukacreations.com		69.163.233.5	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.255970001 CET	8.8.8.8	192.168.2.3	0x8726	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:24:49.255970001 CET	8.8.8.8	192.168.2.3	0x8726	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.275295019 CET	8.8.8.8	192.168.2.3	0x8004	No error (0)	stats.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.621916056 CET	8.8.8.8	192.168.2.3	0x3614	No error (0)	s0.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:49.635884047 CET	8.8.8.8	192.168.2.3	0xfaa3	No error (0)	secure.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:52.399827003 CET	8.8.8.8	192.168.2.3	0xcffc	No error (0)	pixel.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 11, 2021 18:25:11.024234056 CET	8.8.8.8	192.168.2.3	0x334f	No error (0)	www.pukacreations.com		69.163.233.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pukacreations.com
- www.pukacreations.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49716	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:24:45.427608013 CET	89	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: pukacreations.com Connection: Keep-Alive
Jan 11, 2021 18:24:45.629122019 CET	91	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:24:45 GMT Server: Apache Location: http://www.pukacreations.com/ Content-Length: 237 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49718	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:24:46.346599102 CET	92	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.pukacreations.com
Jan 11, 2021 18:24:46.549376965 CET	93	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:24:46 GMT Server: Apache Location: https://www.pukacreations.com/ Cache-Control: max-age=600 Expires: Mon, 11 Jan 2021 17:34:46 GMT Content-Length: 238 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49766	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:25:38.816777945 CET	7242	OUT	GET /product-category/closeouts/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.pukacreations.com Connection: Keep-Alive Cookie: PHPSESSID=be06c56e7553bc39dab597905d8e9510; tk_or=%22%22; tk_r3d=%22%22; tk_lr=%22%22; _ga=GA1.2.1244388716.1610418293; _gid=GA1.2.1245907883.1610418293; _gat_gtag_UA_159680426_1=1
Jan 11, 2021 18:25:39.019879103 CET	7243	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:25:38 GMT Server: Apache Location: https://www.pukacreations.com/product-category/closeouts/ Cache-Control: max-age=600 Expires: Mon, 11 Jan 2021 17:35:38 GMT Content-Length: 265 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 70 72 6f 64 75 63 74 2d 63 61 74 65 67 6f 72 79 2f 63 6c 6f 73 65 6f 75 74 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49767	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:25:49.380736113 CET	9121	OUT	GET /tradeshows/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.pukacreations.com Connection: Keep-Alive Cookie: PHPSESSID=be06c56e7553bc39dab597905d8e9510; tk_or=%22%22; tk_r3d=%22%22; tk_lr=%22%22; _ga=GA1.2.1244388716.1610418293; _gid=GA1.2.1245907883.1610418293; _gat_gtag_UA_159680426_1=1

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:25:49.584307909 CET	9122	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:25:49 GMT Server: Apache Location: https://www.pukacreations.com/tradeshows/ Cache-Control: max-age=600 Expires: Mon, 11 Jan 2021 17:35:49 GMT Content-Length: 249 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 74 72 61 64 65 73 68 6f 77 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49779	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:26:18.145700932 CET	14484	OUT	GET /documents/PERSONAL-GUARANTEE.pdf HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: pukacreations.com Connection: Keep-Alive Cookie: tk_or=%22%22; tk_r3d=%22%22; tk_lr=%22%22; _ga=GA1.2.1244388716.1610418293; _gid=GA1.2.1245907883.1610418293; _gat_gtag_UA_159680426_1=1
Jan 11, 2021 18:26:18.347942114 CET	14484	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:26:18 GMT Server: Apache Location: http://www.pukacreations.com/documents/PERSONAL-GUARANTEE.pdf Content-Length: 269 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 64 6f 63 75 6d 65 6e 74 73 2f 50 45 52 53 4f 4e 41 4c 2d 47 55 41 52 41 4e 54 45 45 2e 70 64 66 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49780	69.163.233.5	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:26:18.560069084 CET	14485	OUT	GET /documents/PERSONAL-GUARANTEE.pdf HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.pukacreations.com Cookie: PHPSESSID=be06c56e7553bc39dab597905d8e9510; tk_or=%22%22; tk_r3d=%22%22; tk_lr=%22%22; _ga=GA1.2.1244388716.1610418293; _gid=GA1.2.1245907883.1610418293; _gat_gtag_UA_159680426_1=1

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 18:26:18.762999058 CET	14486	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 17:26:18 GMT Server: Apache Location: https://www.pukacreations.com/documents/PERSONAL-GUARANTEE.pdf Cache-Control: max-age=600 Expires: Mon, 11 Jan 2021 17:36:18 GMT Content-Length: 270 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 6b 61 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 64 6f 63 75 6d 65 6e 74 73 2f 50 45 52 53 4f 4e 41 4c 2d 47 55 41 52 41 4e 54 45 45 2e 70 64 66 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:24:47.155606985 CET	69.163.233.5	443	192.168.2.3	49721	CN=pukacreations.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Dec 25 17:31:25 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Thu Mar 25 17:31:25 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 11, 2021 18:24:49.359705925 CET	192.0.76.3	443	192.168.2.3	49728	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:49.360075951 CET	192.0.76.3	443	192.168.2.3	49729	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:49.364180088 CET	23.111.9.35	443	192.168.2.3	49724	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 11, 2021 18:24:49.367571115 CET	23.111.9.35	443	192.168.2.3	49725	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 11, 2021 18:24:49.710881948 CET	192.0.77.32	443	192.168.2.3	49732	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

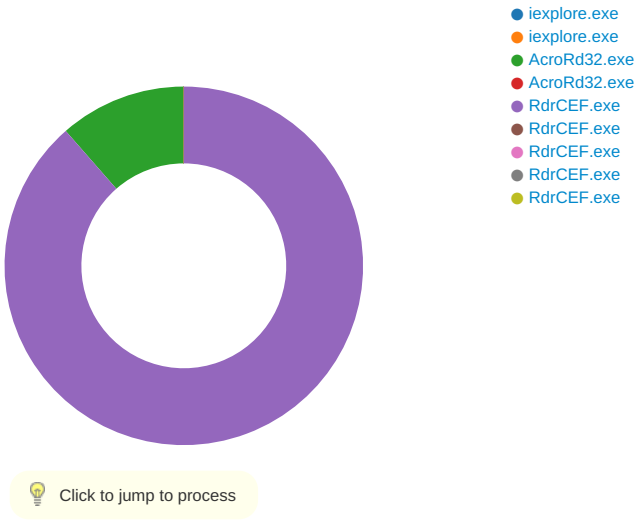
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:49.711522102 CET	192.0.77.32	443	192.168.2.3	49733	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:49.719727993 CET	192.0.73.2	443	192.168.2.3	49735	CN=*.gravatar.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Aug 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Nov 16 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:49.720290899 CET	192.0.73.2	443	192.168.2.3	49734	CN=*.gravatar.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Aug 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Nov 16 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:24:52.485372066 CET	192.0.76.3	443	192.168.2.3	49744	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:24:52.495749950 CET	192.0.76.3	443	192.168.2.3	49743	CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:25:11.457530975 CET	69.163.233.5	443	192.168.2.3	49756	CN=pukacreations.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Dec 25 17:31:25 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Thu Mar 25 17:31:25 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4308 Parent PID: 792

General

Start time:	18:24:42
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff66bb90000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1532 Parent PID: 4308

General

Start time:	18:24:42
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2
Imagebase:	0x1070000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: AcroRd32.exe PID: 4912 Parent PID: 1532

General

Start time:	18:26:19
Start date:	11/01/2021
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' /o /eo /l /b /ac /id 1532
Imagebase:	0xed0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F065C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1okh4cn_kb6hy3_3s4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F2AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4900	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock4912.1.1550807539.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	F52657	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F983C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R9yov03_kb6hy4_3s4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	2	F1EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1xs50aa_kb6hy5_3s4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rvmupmy_kb6hy6_3s4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R81z2u6_kb6hy7_3s4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	F1EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4900	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	F5D405	NtSetInformationFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\AIPC_SRV\AcroSBL_1532_4912	unknown	1040	success or wait	4	F35549	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	F1CF19	RegCreateKeyW

Analysis Process: AcroRd32.exe PID: 4900 Parent PID: 4912

General

Start time:	18:26:20
Start date:	11/01/2021
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 /o /eo /l /b /ac /id 1532
Imagebase:	0xed0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 2156 Parent PID: 4912

General

Start time:	18:26:31
Start date:	11/01/2021
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:	0xba0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	2	C959E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	6	CA83E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	28	CA8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	110	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	6	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	8	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1082	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	29	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	6	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	C959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	4	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	12	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	12	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	28	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	30	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	29	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	10	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	10	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	113	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	144	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	133	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	97	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	3	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	84	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	4	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	8	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	162	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	74	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	6	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	16	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	5	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	C959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	2	C959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	1	C959E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	CA83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 5064 Parent PID: 2156

General

Start time:	18:26:34
Start date:	11/01/2021
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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12005084913169748714 --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=12005084913169748714 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xba0000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 7004 Parent PID: 2156

General

Start time:	18:26:36
Start date:	11/01/2021
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=1716,614424777208045058,2165266707099322910,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9562498448811396969 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xba0000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 5004 Parent PID: 2156

General

Start time:	18:26:37
Start date:	11/01/2021
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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13399235510371959462 --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=13399235510371959462 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xba0000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 7112 Parent PID: 2156

General

Start time:	18:26:39
Start date:	11/01/2021
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=1716,614424777208045058,2165266707099322910,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6053178819435376673 --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=6053178819435376673 --renderer-client-id=5 --mojo-platform-channel-handle=2120 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xba0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis