ID: 1397431
Cookbook: browseurl.jbs
Time: 05:53:37
Date: 23/02/2024
Version: 40.0.0 Tourmaline

Table of Contents

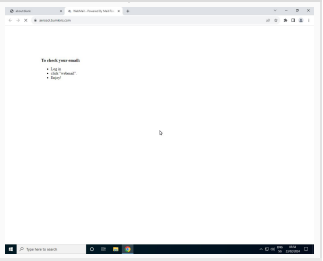
Windows Analysis Report

http://aerosol.bumkins.com/

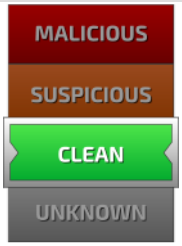
Overview

General Information

Sample URL:	http://aerosol.bumkins.com/
Analysis ID:	1397431
Infos:	



Detection

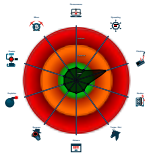


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Creates files inside the system direc…
- Detected clear text password fields …
- HTML body contains low number of …
- HTML page contains hidden URLs o…
- HTML title does not match URL
- Invalid T&C link found
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4900 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 3720 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2348 --field-trial-handle=2284,i,10209318467324837293,7950406128623755245,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6468 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://aerosol.bumkins.com/ MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

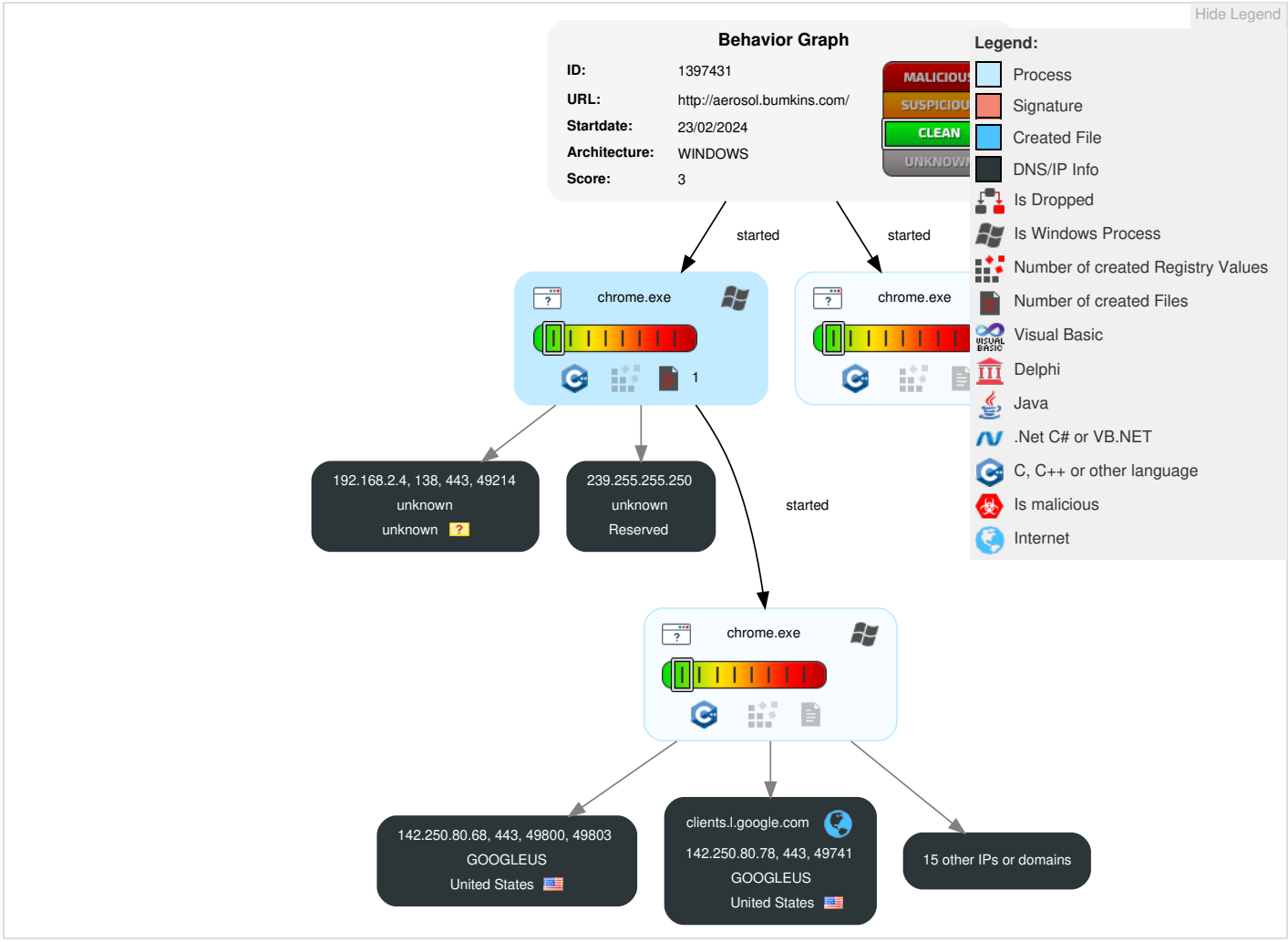
Joe Sandbox Signatures

There are no malicious signatures

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	4 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	5 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	3 Ingress Tool Transfer	Traffic Duplication	Data Destruction

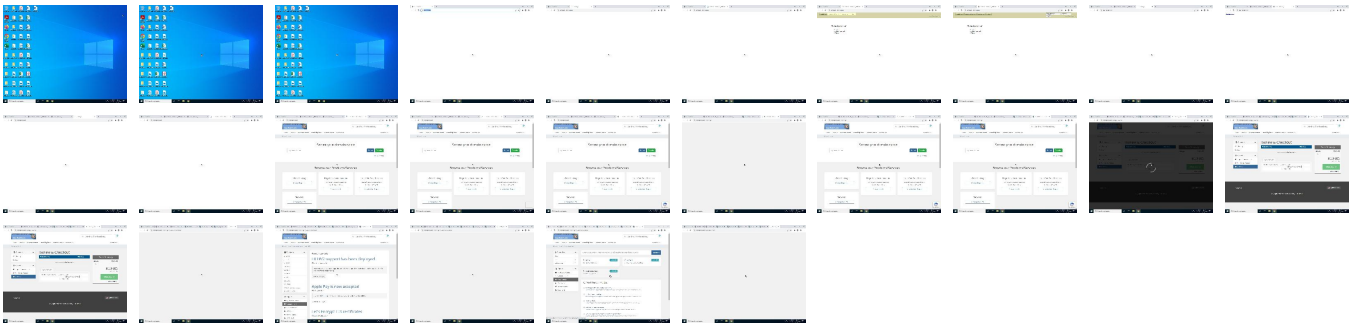
Behavior Graph

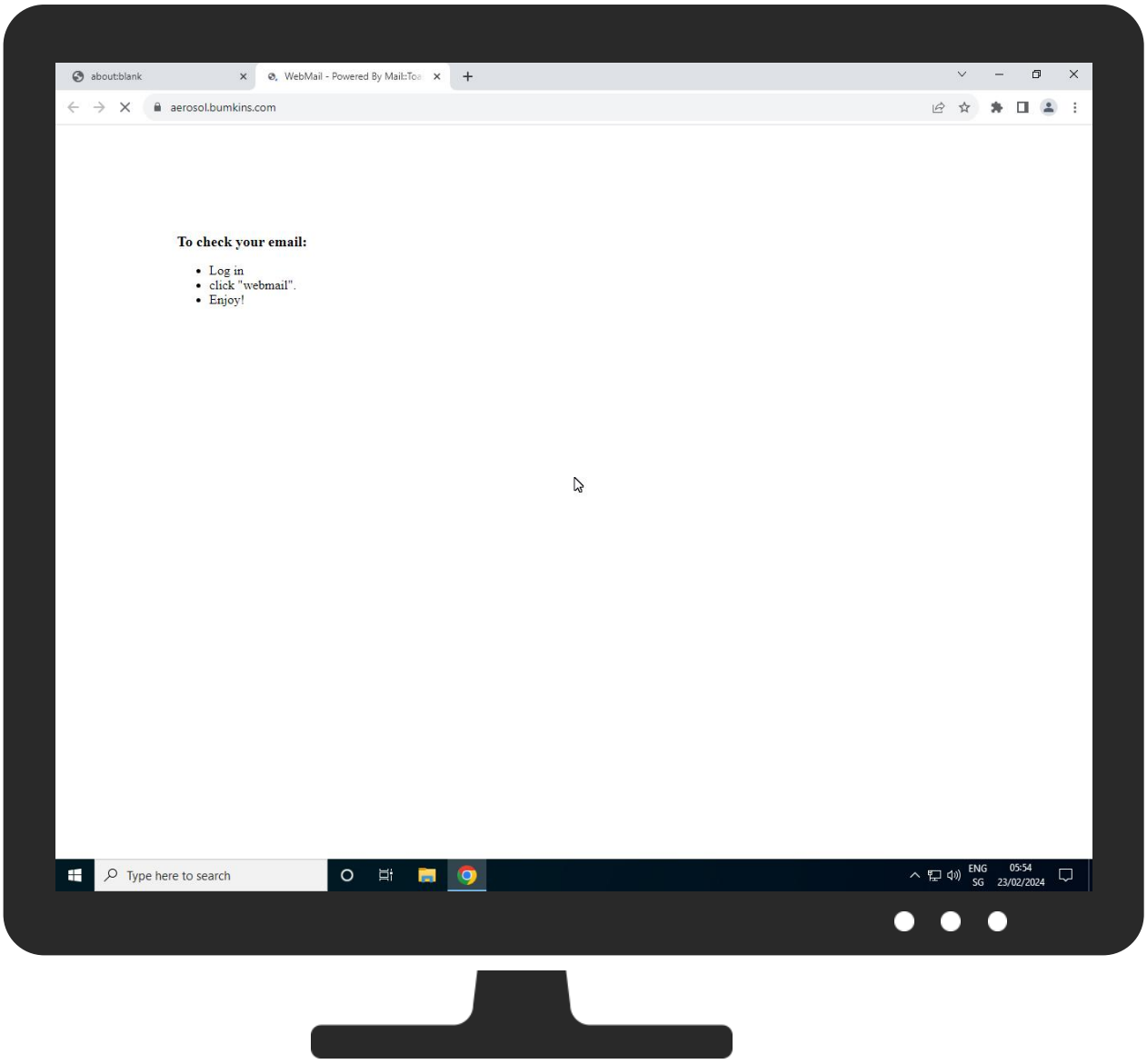


Screenshots

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://aerosol.bumkins.com/	0%	Avira URL Cloud	safe	
http://aerosol.bumkins.com/	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.theartfarm.com	0%	Virustotal		Browse
mail-toaster.org	0%	Virustotal		Browse
stripecdn.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorAutocomplete-dc62d89d9e2121e48baf.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCarouselNavItem-fd5a8f8fac232f661b3	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/StripeSet-423109ad4bf57a2a011c.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CheckoutFormGraphic-b2509d821651cbc82709.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/PaymentLinksReceiptGraphic-68e48fc32d105e52ee0c.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/AnimatedIcon-0b7478e1f9234aae8838.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/BackgroundGlobe-64953aedea5f231d07b7.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/BackgroundGlobe-64953aedea5f231d07b7.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorStatusBar-24c7c84123b2b6e4f091.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorStickyAnimation-4ea4d6a5e9b414987337.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/List-d4c6ad06c173a7dca2ed.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Field-ea906aa31d4012757deb.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorAsciiLoader-c1a350cb85f7a989f599.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Frontdoor-118109a04e95921931d9.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Icon-646136cd9e336d8c18d7.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/DevelopersCodeEditor-eadbd8bbcdedd8edbbe3.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/GraphicFormFieldInput-3d704dfad5ff81d0e80b.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCarouselNavTrack-1380f9c2e275695c5e	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/GraphicFormFieldList-5317148749a9268ec04d.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/EnterpriseCarouselAside-b05102a0b81de0c11406.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCardBackground-853f685776c80eaa0089	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Stripe-b3679504f08482f96a0d.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorConnectAnimation-f4ce77b995975fa55335.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Global-f1eeffae1de3242fcca9.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/f965fdf4.woff2	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorGraphic-ab42746a2bb65d850037.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/Prelude-Q2U7OZHZ.js	0%	URL Reputation	safe	
http://https://www.theartfarm.com/assets/img/logo.png	0%	Avira URL Cloud	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CardField-739e285edeecea986ed0.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/GridLayout-0b90e779a89c0243e739.css	0%	URL Reputation	safe	
http://mail-toaster.org/	0%	Avira URL Cloud	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/HorizontalOverflowContainer-0b85e8f46a0db21a6ef9.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/StripeProductUsed-448c2bc0913c408517f4.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorSuiteAnimation-683958a93f82ca151ea7.css	0%	URL Reputation	safe	
about:blank	0%	Avira URL Cloud	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorSubanimation-b9163916332f2a67d464.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/StartUp-3ebb94fdaa25d9c5cfc2.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorCursor-517911b19e66c94dafbb.css	0%	URL Reputation	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/ProductListing-3e17d7acee941b127dd1.css	0%	URL Reputation	safe	
http://https://mail-toaster.org/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.theartfarm.com/assets/js/StatesDropdown.js	0%	Avira URL Cloud	safe	
http://mail-toaster.org/	0%	Virustotal		Browse
http://https://www.theartfarm.com/templates/orderforms/standard_cart/css/all.min.css?v=0d4099	0%	Avira URL Cloud	safe	
http://www.communitymx.com/content/article.cfm?cid=E0989953B6F20B41	0%	Avira URL Cloud	safe	
http://https://www.theartfarm.com/templates/twenty-one/img/flags.png	0%	Avira URL Cloud	safe	
http://https://www.theartfarm.com/templates/orderforms/standard_cart/js/scripts.min.js?v=0d4099	0%	Avira URL Cloud	safe	
http://https://www.theartfarm.com/assets/webfonts/fa-regular-400.woff2	0%	Avira URL Cloud	safe	
http://https://b.stripecdn.com/mkt-statics-srv/assets/GlobalizationPicker-cb59e0de1d5c3aeaa184.css	0%	Avira URL Cloud	safe	
http://www.communitymx.com/content/article.cfm?cid=E0989953B6F20B41	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.theartfarm.com	66.128.51.172	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	172.253.122.84	true	false		high
m.stripe.com	34.212.84.166	true	false		high
stripe.com	54.186.23.98	true	false		high
www.google.com	142.251.35.164	true	false		high
aerosol.bumkins.com	162.213.38.147	true	false		high
mail-toaster.org	66.128.51.170	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.80.78	true	false		high
stripecdn.map.fastly.net	151.101.0.176	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
m.stripe.network	unknown	unknown	false		high
js.stripe.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://js.stripe.com/v3/fingerprinted/js/m-outer-15a2b40a058ddff1cffdb63779fe3de1.js	false		high
http://mail-toaster.org/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.theartfarm.com/assets/img/logo.png	false	• Avira URL Cloud: safe	unknown
about:blank	false	• Avira URL Cloud: safe	low
http://https://mail-toaster.org/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://www.theartfarm.com/assets/js/StatesDropdown.js	false	• Avira URL Cloud: safe	unknown
http://https://www.theartfarm.com/templates/orderforms/standard_cart/css/all.min.css?v=0d4099	false	• Avira URL Cloud: safe	unknown
http://https://aerosol.bumkins.com/images/mt_background.png	false		high
http://https://js.stripe.com/v3/m-outer-3437aaddcdf6922d623e172c2d6f9278.html#url=https%3A%2F%2Fwww.theartfarm.com%2Fcart.php%3Fa%3Dview&title=Shopping%20Cart%20-%20The%20Art%20Farm&referrer=&muid=NA&sid=NA&version=6&preview=false	false		high
http://https://js.stripe.com/v3/	false		high
http://https://aerosol.bumkins.com/favicon.ico	false		high
http://https://www.theartfarm.com/assets/webfonts/fa-regular-400.woff2	false	• Avira URL Cloud: safe	unknown
http://https://www.theartfarm.com/index.php?rp=/announcements	false		unknown
http://https://stripe.com/	false		high
http://https://www.theartfarm.com/templates/twenty-one/img/flags.png	false	• Avira URL Cloud: safe	unknown
http://https://www.theartfarm.com/templates/orderforms/standard_cart/js/scripts.min.js?v=0d4099	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/js/bg/nGv8TnQEbG7rxu27zBphhV5oFwnrYjnPSH4XjNT2aQ8.js	false		high

URLs from Memory and Binaries

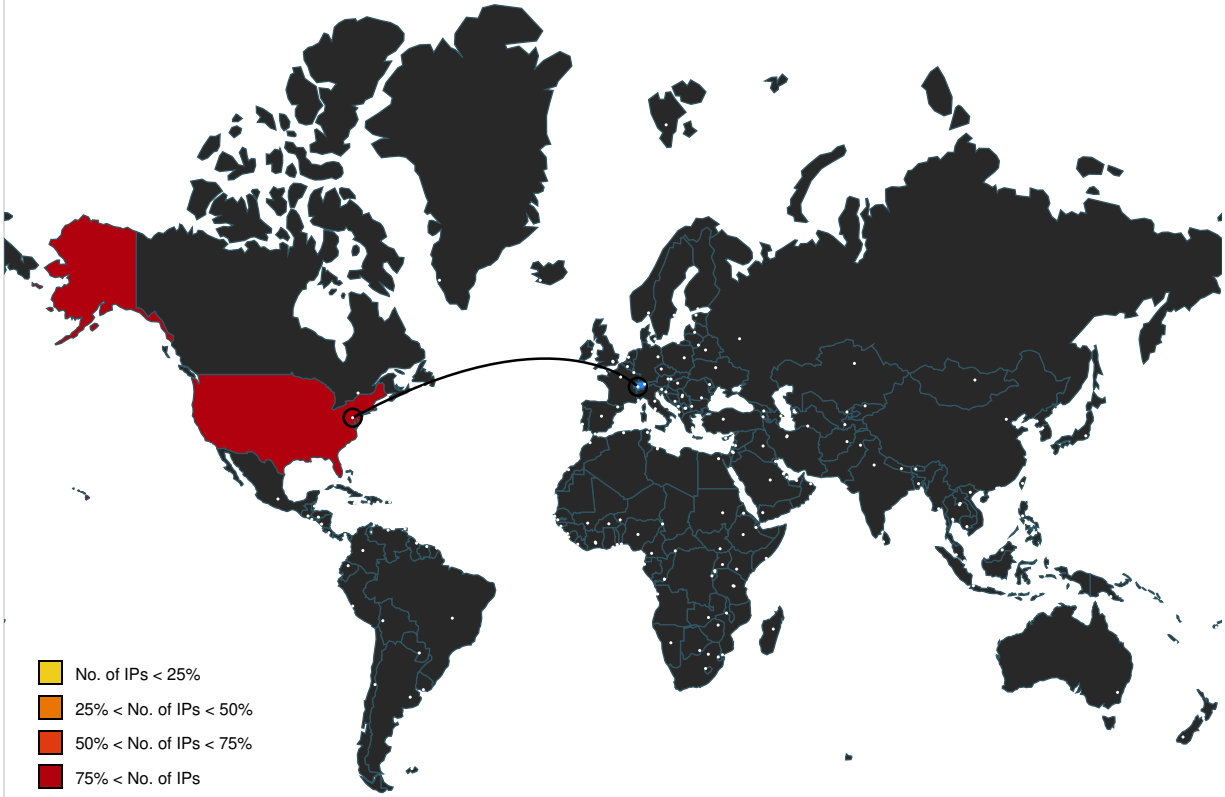
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images.ctfassets.net/fzn2n1nzq965/7szA8TJHWKDIEuCbu6Yblm/4548db61648d063fb7e7dddfca04ab79/ho	chromecache_94.2.dr	false		high
http://https://developers.google.com/recaptcha/docs/faq#localhost_support	chromecache_82.2.dr, chromecache_103.2.dr	false		high
http://https://stripe.com/spc/licenses	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorAutocomplete-dc62d89d9e2121e48baf.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCarouselNavItem-fd5a8f8fac232f661b3	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/StripeSet-423109ad4bf57a2a011c.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/CheckoutFormGraphic-b2509d821651cbc82709.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/de-ch	chromecache_94.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stripe.com/en-li	chromecache_94.2.dr	false		high
http://https://press.stripe.com/	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/PaymentLinksReceiptGraphic-68e48fc32d105e52ee0c.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://images.ctfassets.net/fzn2n1nzq965/2EOOpI2mMZgHYBlbO44zWV/5a6c5d37402652c80567ec942c733a43/fa	chromecache_94.2.dr	false		high
http://https://stripe.com/en-lu	chromecache_94.2.dr	false		high
http://https://stripe.com/en-lt	chromecache_94.2.dr	false		high
http://https://stripe.com/en-lv	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/AnimatedIcon-0b7478e1f9234aae8838.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/BackgroundGlobe-64953aedea5f231d07b7.css	chromecache_94.2.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorStatusBar-24c7c84123b2b6e4f091.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://fontawesome.com	chromecache_104.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorStickyAnimation-4ea4d6a5e9b414987337.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://assets.ctfassets.net/fzn2n1nzq965/01hMKr6nEEGVfOuhsaMIXQ/c424849423b5f036a8892afa09ac38c7/fa	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/List-d4c6ad06c173a7dca2ed.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/docs/payments/checkout	chromecache_94.2.dr	false		high
http://https://stripe.com/en-my	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/Field-ea906aa31d4012757deb.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://support.google.com/recaptcha/#6175971	chromecache_82.2.dr, chromecache_103.2.dr	false		high
http://https://stripe.com/ie	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorAsciiLoader-c1a350cb85f7a989f599.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/Frontdoor-118109a04e95921931d9.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/Icon-646136cd9e336d8c18d7.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://validator.w3.org/check?uri=referer	chromecache_96.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/DevelopersCodeEditor-eadbd8bbcdedd8edbbe3.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/GraphicFormFieldInput-3d704dfad5ff81d0e80b.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://m.stripe.network	chromecache_100.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCarouselNavTrack-1380f9c2e275695c5e	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/en-mx	chromecache_94.2.dr	false		high
http://https://support.google.com/recaptcha	chromecache_103.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/GraphicFormFieldList-5317148749a9268ec04d.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/en-mt	chromecache_94.2.dr	false		high
http://https://stripe.com/pricing	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/EnterpriseCarouselAside-b05102a0b81de0c11406.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/CustomersCaseStudyCardBackground-853f685776c80eaa0089	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/Stripe-b3679504f08482f96a0d.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorConnectAnimation-f4ce77b995975fa55335.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/Global-f1eeffae1de3242fcca9.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/en-no	chromecache_94.2.dr	false		high
http://https://stripe.com/docs/payments	chromecache_94.2.dr	false		high
http://https://stripe.com/in	chromecache_94.2.dr	false		high
http://https://stripe.com/en-nl	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/f965fdf4.woff2	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://images.ctfassets.net/fzn2n1nzq965/5F0uhf7cRg9vhR6NmgWzzl/664e14ddebb91375f89f8dcc75242dc0/ho	chromecache_94.2.dr	false		high
http://https://stripe.com/it	chromecache_94.2.dr	false		high
http://https://developers.google.com/recaptcha/docs/faq#my-computer-or-network-may-be-sending-automated-que	chromecache_82.2.dr, chromecache_103.2.dr	false		high
http://https://stripe.com/docs/upgrades#api-versions	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorGraphic-ab42746a2bb65d850037.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/guides	chromecache_94.2.dr	false		high
http://https://images.ctfassets.net	chromecache_94.2.dr	false		high
http://www.communitymx.com/content/article.cfm?cid=E0989953B6F20B41	chromecache_131.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/Prelude-Q2U7OZHZ.js	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/jp	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/CardField-739e285edeecea986ed0.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/GridLayout-0b90e779a89c0243e739.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://dashboard.stripe.com/	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/GlobalizationPicker-cb59e0de1d5c3aeaa184.css	chromecache_94.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stripe.com/en-hu	chromecache_94.2.dr	false		high
http://https://stripe.com/th	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/HorizontalOverflowContainer-0b85e8f46a0db21a6ef9.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/StripeProductUsed-448c2bc0913c408517f4.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/sv-fi	chromecache_94.2.dr	false		high
http://https://www.google.com/log?format=json&hasfast=true	chromecache_82.2.dr, chromecache_103.2.dr	false		high
http://https://stripe.com/en-hk	chromecache_94.2.dr	false		high
http://https://support.stripe.com/?referrerLocale=en-us	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorSuiteAnimation-683958a93f82ca151ea7.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/FrontdoorSubanimation-b9163916332f2a67d464.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://stripe.com/en-hr	chromecache_94.2.dr	false		high
http://https://stripe.com/it-hr	chromecache_94.2.dr	false		high
http://https://cloud.google.com/contact	chromecache_82.2.dr, chromecache_103.2.dr	false		high
http://https://images.ctfassets.net/fzn2n1nzq965/6iLtU8qBUtE42tshpmZxY2/ac5b7b7a181524237b942e43620fceef/ch	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/StartUp-3ebb94fdaa25d9c5cfc2.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://b.stripecdn.com/mkt-statics-srv/assets/CodeEditorCursor-517911b19e66c94dafbb.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown
http://https://fontawesome.com/license	chromecache_104.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images.ctfassets.net/fzn2n1nzq965/4WjxT85Wi0tNWOJie0L7LW/233ec6bd0738bc0fb86ed1ea0a12515a/Po	chromecache_94.2.dr	false		high
http://https://b.stripecdn.com/mkt-statics-srv/assets/ProductListing-3e17d7acee941b127dd1.css	chromecache_94.2.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.80.68	unknown	United States		15169	GOOGLEUS	false
66.128.51.172	www.theartfarm.com	United States		7819	GLOBAL-IP-NETWORKSUS	false
151.101.0.176	stripecdn.map.fastly.net	United States		54113	FASTLYUS	false
66.128.51.170	mail-toaster.org	United States		7819	GLOBAL-IP-NETWORKSUS	false
142.251.40.228	unknown	United States		15169	GOOGLEUS	false
172.253.122.84	accounts.google.com	United States		15169	GOOGLEUS	false
162.213.38.147	aerosol.bumkins.com	United States		50837	CLOUDSIGMA-ASCH	false
54.186.23.98	stripe.com	United States		16509	AMAZON-02US	false
142.250.80.78	clients.l.google.com	United States		15169	GOOGLEUS	false
151.101.128.176	unknown	United States		54113	FASTLYUS	false
34.212.84.166	m.stripe.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
44.240.51.134	unknown	United States		16509	AMAZON-02US	false
142.251.35.164	www.google.com	United States		15169	GOOGLEUS	false
151.101.192.176	unknown	United States		54113	FASTLYUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1397431
Start date and time:	2024-02-23 05:53:37 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://aerosol.bumkins.com/
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	8
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:	clean3.win@29/111@38/16
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: http://mail-toaster.org/ • Browse: http://www.theartfarm.com/ • Browse: https://www.theartfarm.com/index.php • Browse: https://www.theartfarm.com/cart.php?a=view • Browse: https://www.theartfarm.com/index.php?rp=/announcements • Browse: https://www.theartfarm.com/index.php?rp=/knowledgebase • Browse: https://www.theartfarm.com/serverstatus.php

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 142.250.80.99, 34.104.35.123, 142.250.80.106, 142.251.40.106, 142.250.80.42, 142.250.65.202, 142.251.40.234, 142.250.65.170, 142.250.176.202, 142.250.81.234, 142.251.40.170, 142.250.80.74, 142.251.41.10, 142.250.65.234, 142.251.35.170, 142.251.40.202, 142.251.40.138, 142.251.32.106, 40.68.123.157, 20.166.126.56, 52.165.165.26, 13.85.23.206, 142.250.80.3, 142.250.64.106, 142.250.72.106, 142.250.176.195, 142.251.40.131, 142.250.80.67, 142.251.40.163, 40.127.169.103, 20.12.23.50
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, slscr.update.microsoft.com, fonts.gstatic.com, clientservices.googleapis.com, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, edgedl.me.gvt1.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, update.googleapis.com, umwatson.events.data.microsoft.com, www.gstatic.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 100

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (526), with no line terminators
Category:	downloaded
Size (bytes):	526
Entropy (8bit):	4.844995662196588
Encrypted:	false
SSDEEP:	12:c4GJ0k2lvgyT6d1uOMXUZsCxYADLsdfPw3CgrR5jddeU7nu:c5D2BtT67uOMXUZjxYOLsOCgrN80u
MD5:	D96C709017743C0759CF3853D1806BA5
SHA1:	72E21587610C49C8305A55E71F73FA88ED618205
SHA-256:	BA2338AA6670580269C762F51C4291DAEF913201AA8F4D4FD166C1A878262652
SHA-512:	974E260ED8BD1D99628FC3248F07179F6EA228E37A6B9D3EF906DBA57571F2DF54D73F93D1F3460902D28A90BD4793BCA35477B2EF8FBF424B9112147F04BCC
Malicious:	false
Reputation:	low
URL:	http://https://js.stripe.com/v3/fingerprinted/js/m-outer-15a2b40a058ddff1cffdb63779fe3de1.js
Preview:	!function(){"use strict";var e="https://m.stripe.network",n=window.location.hash,t=/preview=true/.test(n)?"inner-preview.html":"inner.html",o=document.createElement("ifra me");o.src="".concat(e,"/").concat(t).concat(n);var i=function(n){if(n.origin===e){var t=window.opener||window.parent||window;if(!t)return;t.postMessage(n.data,"*")}else o.contentWindow.postMessage(n.data,"*")};window.addEventListener?window.addEventListener("message",i,!1):window.attachEvent("onMessage",i),document.bo dy&&document.body.appendChild(o)}();

Chrome Cache Entry: 101

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	519
Entropy (8bit):	4.536758771950739
Encrypted:	false
SSDEEP:	12:t9Afm3vqCOnftAJHOhKCxzw5NW6duZ4FIrGwdpwk8zqAKcdM7J5:t9AfWAnSNCxKNxuZDqwwvxc
MD5:	C6B234719965CC10DF0F8D12C1F438DD
SHA1:	386F533083A450BB34F87DAB852E495195A7FDDB
SHA-256:	686D81E030899B477865D67A01FE34E83D8E68AA8DA91A59205AD3E901A3EC71
SHA-512:	F5902DED64A6ECE6015686924BBC6796AF1FE50B527A40B920B45D499DA2EDBDAEF5B2A87C56CB61A89CD174876F64790AF18B9BD1C838D285FD62B20FCDC D2
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/img/clippy.svg

Preview:	<svg height="1024" width="896" xmlns="http://www.w3.org/2000/svg">. <path d="M128 768h256v64H128v-64z m320-384H128v64h320v-64z m128 192V448L384 640l192 192V704h320V576H576z m-288-64H128v64h160v-64zM128 704h160v-64H128v64z m576 64h64v128c-1 18-7 33-19 45s-27 18-45 19H64c-35 0-64-29-64-64V192c0-35 29-64 64-64h192C256 57 313 0 384 0s128 57 128 128h192c35 0 64 29 64 64v320h-64V320H64v576h640V768zM128 256h512c0-35-29-64-64-64h-64c-35 0-64-29-64-64s-29-64-64-64-64 29-64 64-29 64-64 64h-64c-35 0-64 29-64 64z" />.</svg>.

Chrome Cache Entry: 102	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65202)
Category:	downloaded
Size (bytes):	203943
Entropy (8bit):	5.079195518191298
Encrypted:	false
SSDEEP:	1536:Ug3wIJtTP82BjhCkDEBi8yNcuSE3qRqenzq3SYiLENM6HN26Jv4/LmhI9cmJhB3o:l3nQ1zq3SYiLENM6HN26zSLpY
MD5:	0B4B334A1CF7F72040D69A99208C274E
SHA1:	56BD4B7B30F8E16DAB5EE8862BF5A87C190CA78D
SHA-256:	A2F330CBDEE9CA0CD9AD7D76DF9CF06066C2D42C8CE55752862CA479852898FC
SHA-512:	4E4375DFD230DD2B247E40A206C71595F022FE0689AE2C3E79DA1977E0EB82C1372DC545FC120BF12EB1A4EA07E61FB312A07A93D1053FDF1041F6146B4048B
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/twenty-one/css/theme.min.css?v=0d4099
Preview:	/*!. * WHMCS Twenty-One Theme. * Global Stylesheet. * Copyright (c) 2020 WHMCS Limited. * https://www.whmcs.com/license/. *//*!. * Bootstrap v4.5.3 (https://getbootstrap.com/). * Copyright 2011-2020 The Bootstrap Authors. * Copyright 2011-2020 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#336699;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"Noto Sans",sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-fami

Chrome Cache Entry: 103	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (568)
Category:	downloaded
Size (bytes):	503430
Entropy (8bit):	5.708119764112345
Encrypted:	false
SSDEEP:	6144:HEYt9e4UlnQyfZLsIB74RSHywNGte2fp0YROQVZT+DSUAZqH/:Hi9fpj140SwQz0YRO+ZSj/
MD5:	3E528C5BD4E8985F914F84BC5F86DF5F
SHA1:	34104EA645A6789DD9CB58C264E20ED6855EA1DE
SHA-256:	E51E616D124133B0FB24968469097A4D311B972F78455143D940703EA0639BA6
SHA-512:	C59A1D40F649446F33FF0FF3FA9A8E997D3CFF10F968D35226BA08BB91C9013AE937460CF2DAB0888848ABE1B693D4377FBD6904E3E03360B15035A8C3E9BC9
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2005, 2007 Bob Ippolito. All Rights Reserved.. Copyright The Closure Library Authors.. SPDX-License-Identifier: MIT.*/./*. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var C=function(){return[function(f,q,S,Z,P,X,U){return(f|((X=[1,6,4],(f+X[1]&X[2])<X[0]&&3<=((f^17)&7))&&(this.X=S,this.N=q),X[1]))>>3||(P=0,P=void 0===P?0:P,U=I[16](14,q,L[13](26,Z,S),P)),U},function(f,q,S,Z,P,X,U,b,k,E,J,K,B,n,F,c){if(1<=((f|(F=(f-7>>3||(c=q instanceof qd&&q.constructor===qd?q.N:"type_error:SafeUrl"),["T","call",0]),72))==f&&(c=u[22](26,function(r,g,m){m=["could not contact reCAPTCHA.",15,(g=[2,3,6],"recaptcha::2fa")];switch(r.N){case 1:if(!U.C)throw Error(m[0]);if(!U.X)return r.return(I[19](72,.g[0]));if("string"!==typeof X||X.length!=g[2])return r.return(I[19](32,P));return u[10]((r.C=g[0],m[1]),P,U.C,r);case P:C[2

Chrome Cache Entry: 104	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65393)
Category:	downloaded
Size (bytes):	156472
Entropy (8bit):	4.711296987922954
Encrypted:	false
SSDEEP:	1536:hgvcfQ4aNi7HHQZD0bMSPCDTdV8dWGFlibo3+8leiy6BauXZG81UfgFSkAmYdAT/:lcl4aY7QN0bjPerbxHuXdz
MD5:	28B5623458ED1AAFAFF6B3C0B63ED250
SHA1:	3B3F8B4FE4235068639740973FA86FE34A7F7986
SHA-256:	2C694CFAFD5C00BA4A7A2110060EB937AFCCFC1D7B745A319C49764FE4EF017C
SHA-512:	80BD40A6677578A7911933BFE271438C44362F8CA6BE21D5C67F3C3450B741363492CABD7BC6EE6485F2F5459B62E9210518B7240E71C90336995A83015ECF78
Malicious:	false

Reputation:	low
URL:	http://https://www.theartfarm.com/assets/css/fontawesome-all.min.css
Preview:	/*! * Font Awesome Pro 5.10.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license (Commercial License). */..fa,.fab,.fad,.fa l,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-heigh t:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{f ont-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{t ext-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2e m;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pull-left{float:left}.fa-pull-right{float:rig

Chrome Cache Entry: 105	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 288 x 67, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	34200
Entropy (8bit):	7.975336386324512
Encrypted:	false
SSDEEP:	768:ntqMAdrVeINhOSC+9cQXLUzPpYF596D76to6qD7eABspw3:tq9PNR30Pe96vlBuc
MD5:	2133E51A99B613053214019946B6986B
SHA1:	31FA4C478417BCD6ABFA285362EB2B8CF3534A91
SHA-256:	8B4267932D551E822315C6F054A84E3B29E7DC9503299DC3FCE50971C85F3BA5
SHA-512:	EBD51D897A71A191B0318B8845C4F04046E2D796847DAB1330680DBB8264D4E07509D3121F5853FAEF803013808B0A5EEC2F83C5521B5CA88534FD5C68C3F755
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/img/logo.png
Preview:	.PNG.....IHDR... ...C.....<.....sRGB.....pHYs.....wiTXtXML:com.adobe.xmp.....<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:photoshop="ht tp://ns.adobe.com/photoshop/1.0/". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/". xmlns:dc="http://purl.org/ dc/elements/1.1/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">. <tiff:ResolutionUnit>2</tiff:ResolutionUnit>. <tiff:Orientation>1</tiff:Orie ntation>. <tiff:NativeDigest>256,257,258,259,262,274,277,284,530,531,282,283,296,301,318,319,529,532,306,270,271,272,305,315,33432;CFAEEC7FCD3 3378A4A71D49676881A17</tiff:NativeDigest>. <photoshop:ICCProfile>sRGB IEC61966-2.1</photoshop:ICCProfile>. <photoshop:ColorMode>3</pho

Chrome Cache Entry: 106	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1288), with no line terminators
Category:	downloaded
Size (bytes):	1288
Entropy (8bit):	5.803547307207809
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZJlX6+KVCLTLv138EgFB5vtTGJTlWtZ1v8lgsLqo40RWUnYN:VKEcixKonR3evtTA871v8lhLrwUnG
MD5:	D35A5B9D50FFD75F75F2AE733FE486C0
SHA1:	CD9BD666D9E47C5C3E62936F5CFA46F012719E09
SHA-256:	6B5293BDC08B1E6D6DCA10429F493C178AB594918B4A93F0792AA7DE7B56455F
SHA-512:	68242889117B119F5E2E2691DC2E7BD454DA71609111E4652936191CA95C6DD79AAF236A2D7F864AB27BA1125F6FB940BFD629AF185A8E22EC459C59EFAE01F
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api.js?onload=recaptchaLoadCallback&render=explicit&_=1708664121772
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.r eady=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('explicit');(c fg['onload']=cfg['onload']||[]).push('recaptchaLoadCallback');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po .async=true;var m=d.createElement('meta');m.httpEquiv='origin-trial';m.content='Az520Inasey3TAyqLyojQa8MnmCALSEU29yQFW8dePZ7xQTvSt73pHazLFTK 5f7SyLUJSo2uKLesEtEa9aUYcgMAAACPeyJvcmlnaW4iOiJodHRwczovL2dvb2dsZS5jb206NDQzIiwiZmVhdHVyZSI6IkRpc2FibGVUaGlyZFBhcnR5U3RvcmFnZVBhcn RpdGlvbmluZyIsImV4cGlyeSI6MTcyNTQwNzk5OSwiaXNTdWJkb21haW4iOnRydWUsImlzVGhpcmRQYXJ0eSI6dHJ1ZX0=';d.head.prepend(m);po.src='https:// www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js';po.crossOrigin='anonym

Chrome Cache Entry: 107	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHl1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832

SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D9
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PIP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"lc.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...l.a....*+....(...S..\h....@.....I.$..%.2....l.....a.|.....U...y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

Chrome Cache Entry: 108	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	96
Entropy (8bit):	5.034422459779062
Encrypted:	false
SSDEEP:	3:HCNCkuDKthCsRu/mRKq2Hr2iuC/yYn:QuqICemR3Y29C/yY
MD5:	FEE0E3DFCFD96E86242F6E08280F2DA2
SHA1:	33C374DC1C410884D1D627B2C4159207B445BA1C
SHA-256:	882EB29C00779A07104AD176E00D8F2B62821B16DC8D4EAA8F6A4694435B6865
SHA-512:	181982BC7D4C02E942D2745D9B3D811F0A539D34B5357A776262FBA2394D205DAFD16017A3D592818A3A558B3644A1BBF6516194141A9868C3EBD917302DBD28
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAlV4_8xSKzOihIFDWdns_4SEAkMVBz6GkRKHBIFDY6nFnMSHgmWFEiNDKiwbBIFDaDIjiUSBQ1Vu_VvEgUNoHnZphIXCa4fVe6_qVEEEgUN2-_OEhIFDXOST1k=?alt=proto
Preview:	CgkKBw1nZ7P+GgAKCQoHDY6nFnMaAAobCgcNoMiOJRoACgcNVbv1bxoACgcNoHnZphoAChIKBw3b784SGgAKBw1zkk9ZGgA=

Chrome Cache Entry: 109	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 200 x 25
Category:	dropped
Size (bytes):	2658
Entropy (8bit):	7.835838708462061
Encrypted:	false
SSDEEP:	48:nuRRgtdBqIKpw3OE2/0lqoYv6ktQHobuqxWw01REQ9OcA:uRRg70H+3OE2/0soYvmob9Rgr9lA
MD5:	41880FA22172966FC2F080135F0ADAE7
SHA1:	26F5BDD7196D1D0A96D1D76D971CC0B3738115AA
SHA-256:	27CE260D2294E252FA98722E0B2D1C0F750F6024AA2DB5082EA6E5B48910C7A4
SHA-512:	80D45528EDC16FFEB4BDD386A18F858008E5890982E1567816D6C5BE865B7FA148F3B0BF52094EAE2E279DF4C33C61FF5AB3641F433F5C7185F0BB213E254FE2
Malicious:	false
Reputation:	low
Preview:	GIF89a.....|..i..v.....i....}..p..n..i.....u..{.....i..m.....q.....{.....v..v....q.....v.....l..q.....m.....|....{..m....{.....|.....l..r..r.....l .....m.....r..|.....w....l.....h..p..w....q....z.....y.....f!.....,.....@... .. x.....Ay..4...Z..\e.....Z,,..e.,.],.4.....\].....e,.....\.....,....44.....X ...J...dj\h1Cl.....B&.fdl....3(..P....`(Bd.R!C..%Rd.p..%J..\.qd...+.....!~|..'.-..I.1..&-k.....%o.`zsgG.#1*9...J.8..Xu.B.,-f.....G"....~.+V.x...#K>.x.d.'K..9qg.A...yt..9.V....=z(..-.6 ..m.][.....v..h.#'.<....G.....[....{..]|8x.e.P.A...[.....,.....^}...._.Q...|.....A.=`!a{.b..~Q@.a.2.w.|..(..... .....b...g... ...X...^._.....h$.! .....FZ..m..gT..Yd.a..c.u.e...)..\.y.d.l...0 @...6da..p.'.6....D....

Chrome Cache Entry: 110	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	44
Entropy (8bit):	4.678419619169109
Encrypted:	false
SSDEEP:	3:HCNCkuWDTcXx9+n:QuWDgXxg
MD5:	3E85EFC275216B4BCA69346E53FF6E1C
SHA1:	6CAF4C664A2109AEB27C016A749887FC7AD9EE24
SHA-256:	BA638690C2E939838FB5BD416348393E6D13686CDD3DB3A6FE855E03A5FC3F20

SHA-512:	91FF73FDD796322594A2D9D1FF82E1E1F7CB792B8DA318729E8DCD5104526782965ED76E6972F71B0EDBE14BA3815C9DC874640BC090A8B2BDE099A5FB7A78 1
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAlV4_8xSKzOihIFDWdns_4SFwmuH1Xuv6lRBBIFDdvvzhISBQ1zkk9Z?alt=proto
Preview:	CgkKBw1nZ7P+GgAKEgoHDdvvzhIaAAoHDXOST1kaAA==

Chrome Cache Entry: 111

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 288 x 67, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	34200
Entropy (8bit):	7.975336386324512
Encrypted:	false
SSDEEP:	768:ntqMAdrVeINhOSC+9cQXLUzPpYF596D76to6qD7eABspw3:tq9PNR30Pe96vlBuc
MD5:	2133E51A99B613053214019946B6986B
SHA1:	31FA4C478417BCD6ABFA285362EB2B8CF3534A91
SHA-256:	8B4267932D551E822315C6F054A84E3B29E7DC9503299DC3FCE50971C85F3BA5
SHA-512:	EBD51D897A71A191B0318B8845C4F04046E2D796847DAB1330680DBB8264D4E07509D3121F5853FAEF803013808B0A5EEC2F83C5521B5CA88534FD5C68C3F755
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR... ...C.....<.......sRGB.........pHYs...............wiTXtXML:com.adobe.xmp.....<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">. <tiff:ResolutionUnit>2</tiff:ResolutionUnit>. <tiff:Orientation>1</tiff:Orientation>. <tiff:NativeDigest>256,257,258,259,262,274,277,284,530,531,282,283,296,301,318,319,529,532,306,270,271,272,305,315,33432;CFAEEC7FCD33378A4A71D49676881A17</tiff:NativeDigest>. <photoshop:ICCProfile>sRGB IEC61966-2.1</photoshop:ICCProfile>. <photoshop:ColorMode>3</pho

Chrome Cache Entry: 112

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 1 icon, -128x-128, 32 bits/pixel
Category:	dropped
Size (bytes):	69694
Entropy (8bit):	6.0166748491726025
Encrypted:	false
SSDEEP:	768:82MlSe1oXPzHhrocJm231dfLxSMO88888888888808IxgrgY5sm0Tr:85lloXrH+gm419kSEgY5smo
MD5:	471B468AABE292CD2099B2E04047527A
SHA1:	038BF470AD04E7BCBE7FC58B3ADBC221A0021E0E
SHA-256:	63C8B75B2DBF22560921E6239030D7132AD5A3D15F051D10A378EA79E8420C75
SHA-512:	32F4090A28739ED0BCCCD7BE1B31AFCF31E52686B1C4096CF0B7FE53DDBC4C0E996EAF108FAE598835807D14C8E824F8619C09B8B8CC796586A58F9EFBB7E 35
Malicious:	false
Reputation:	low
Preview:	....(.......(............. ....

Chrome Cache Entry: 113

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 48236, version 1.0
Category:	downloaded
Size (bytes):	48236
Entropy (8bit):	**7.994912604882335**
Encrypted:	**true**
SSDEEP:	768:uj6JxavgLx5rjTH3CdZ3y11o4uMb2IVEhiB6z6GAAHJApICtBgso6HaOjTXHRWK:ujoa4LxZPCdm3B2IVEhiB62apApISxos
MD5:	015C126A3520C9A8F6A27979D0266E96
SHA1:	2ACF956561D44434A6D84204670CF849D3215D5F
SHA-256:	3C4D6A1421C7DDB7E404521FE8C4CD5BE5AF446D7689CD880BE26612EAAD3CFA
SHA-512:	02A20F2788BB1C3B2C7D3142C664CDEC306B6BA5366E57E33C008EDB3EB78638B98DC03CDF932A9DC440DED7827956F99117E7A3A4D55ACADD29B006032D9 5C

Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/opensans/v40/memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTS-muw.woff2
Preview:	wOF2.....I.....D.....O..B..h?HVAR.x.`?STAT.$'...0+...\|.../V.....+..2.0..6.6.$..`. ..~.....[B4q.....t..P.M_.z...1..R.S*...u.#..R....fR.1.N.v.N.P...;.2.....!Z.....Qs ...5f.G.K.an2&....2...*.....C.H.t..N!.....nh.<(.vN.....j.._.L.P.t..Ai.%....._I.i,..o,C.].H.X9.....a.=N....k.....n.L..k.f.u..{...:.}^\[..~5...Z`.....`!...%4.,...K0..&.a/....P....S....m .Z.....u...D.j.F...f.0`I.`.`.h#..)(FQ.F!o$.....S.).MV8%Rh...r...x...T]$.=.....Y...!.3.&U..."....Q....{.I/0..d..4iJ/..}...3....i[Z..NG.WD...>.[U..Q.h..@m.=..S...1C2...d...<..v.?.q.f..n.. .OUz.....&Z.....Z."..N.....n...9.B..C..W....}...W..6Zs.i.+Z.....jB.n..x.8M.....q..@I....-.%..,C,..K..#.2...4)/.v_..x.<....t.....%[.4?.=j.V..jj"..W.u..q....I.L.=.....E...\.M.7{.>.....W.....C. `...,9$.....\..o.....y...4A..m.P.,X..=?.:.....wF`..+.P.....M!.4.....I.>M..t.ff5r..^..Z.g...!fA,hIIQ...e.R>B.AH.VuX..>..\.=.ky...1>C....>C.c.;...6D.

Chrome Cache Entry: 114

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 15344, version 1.0
Category:	downloaded
Size (bytes):	15344
Entropy (8bit):	7.984625225844861
Encrypted:	false
SSDEEP:	384:ctE5KIuhGO+DSdXwye6i9Xm81v4vMHCbppV0pr3Ll9/w:cqrVO++tw/9ClCFbQLlxw
MD5:	5D4AEB4E5F5EF754E307D7FFAEF688BD
SHA1:	06DB651CDF354C64A7383EA9C77024EF4FB4CEF8
SHA-256:	3E253B66056519AA065B00A453BAC37AC5ED8F3E6FE7B542E93A9DCDCC11D0BC
SHA-512:	7EB7C301DF79D35A6A521FAE9D3DCCC0A695D3480B4D34C7D262DD0C67ABEC8437ED40E2920625E98AAEAFBA1D908DEC69C3B07494EC7C29307DE49E91C2 EF48
Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2
Preview:	wOF2.....;.....H..;.....d..@..J.`..L.T..<.....x.....^...x.6.$..6. ..t. ..I.h\|.I....A....b6.....(.....@e.]...*:..-.0..r.)..hS..h...N.).D.....b.].....^..t?.m{...."84...9.....c...?..r3o.. ..}...S]....zbO.../z..{.....~cc....I...#.G.D....#*e.A..b...b`a5P.4.....M....v4..fI#X.z,.,...=avy..F.a.\9.P\|.[....r.Q@M.I..._.9..V..Q..].....[{u..L@...]..K.....]C....I$.Z.Z...Zs.4..... x..... ..F.?.7N..].|.wb\....Z{1L#..t....0.dM...$JV...{..oX...i....6.v.~.....)\|.TtAP&).KQ.]y.....'...:.d..+..d..."C.h..p.2.M..e,.*UP..@.q..7..D.@....,.....B.n. r&.....F!....\...;R.?-.i...,7..cb../I...E g...!X.)5.Aj7...Ok..l7.j.A@B`".}.w.m..R.9..T.X.X.d....S..`XI..1... .$C.H.,.\. ..A(.AZ.....`Wr.0]y..-..K.1.....1.tBs..n.0...9.F[b.3x...*$....T..PM.Z-.N.rS?I.<8eR'.3..27..? ;..OLf*.Rj.@.o.W.....j~ATA....vX.N:.3dM.r.)Q.B...4i.f..K.l..s....e.U.2...k..a.GO.}..../.'..%$..ed.*.'..qP....M..j...../.z&.=...q<....-..?.A.%..K..

Chrome Cache Entry: 115

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (65529), with no line terminators
Category:	downloaded
Size (bytes):	88751
Entropy (8bit):	5.414296471740167
Encrypted:	false
SSDEEP:	1536:2sHx8vawlWe2XzbStiSc6q1jboAmKum7EqIZ7d+/:2sHx8vzWe2jOtiSg1jboAmKum7EqCp+/
MD5:	69CB7809B5011312E716F29B3D19DCE6
SHA1:	833DABFB546D57065AEBA7190B5EE5A2428DFA47
SHA-256:	E039E607C78306C7E029A7FD0ECDB14F86456F16E1A5CE65AA26B4FDF1D38A3C
SHA-512:	4259C8F940CFE4B7EC384E5ABD855713DA7792A955A7B737B75E45E6559A90292ADE59D7CCAB381EA4C2D0FA5109B4ABD9BFA0887C05C9FB1A27469D5E198A 69
Malicious:	false
Reputation:	low
URL:	http://https://m.stripe.network/out-4.5.43.js
Preview:	var StripeM=function(e){var t={};function n(r){if(t[r])return t[r].exports;var _=t[r]={i:r,l:!1,exports:{}};return e[r].call(_.exports,_,_.exports,n),_.l=!0,_.exports}return n.m=e, n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.def ineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"ob ject"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var _ in e)n.d(r,_,function(t){return e[t]}.bind(null,_));return r},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=fu nction(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=30)}([function(e,t,n){"use strict";(function(e){n.d(t,"a",(function(){retur

Chrome Cache Entry: 116

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (49872), with no line terminators
Category:	downloaded
Size (bytes):	49876
Entropy (8bit):	4.968959236387818
Encrypted:	false
SSDEEP:	384:nS4Hwc+RBhisQgv/HBL98FmnX+rXNycLBLSxnW3PKiwd:nS4HwvjhisQgnHBL98FmX+UyPKTd
MD5:	8358948054955F371FEE5614C83CBD45

SHA1:	AC88DC3399A3F20E9B1D651B231422B2C65C9DF3
SHA-256:	11FA640F6B541E1CF45B55179E5567F70419745DFA01D10768590CE18E32E735
SHA-512:	5B3719708C08CFE25B90B2F37C42C74560944B9171951E61DABDCA0B9ABE32CFD586B150DCF9400A3E9FCA8F90996AA8B52656BC511EC115839E45C1961BE26 7
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/twenty-one/css/all.min.css?v=0d4099
Preview:	@charset "UTF-8";.intl-tel-input{position:relative;display:inline-block}.intl-tel-input *{box-sizing:border-box;-moz-box-sizing:border-box}.intl-tel-input .hide{display:none}.intl-tel-input .v-hide{visibility:hidden}.intl-tel-input input,.intl-tel-input input[type=tel],.intl-tel-input input[type=text]{position:relative;z-index:0;margin-top:0!important;margin-bottom:0!important;padding-right:36px;margin-right:0}.intl-tel-input .flag-container{position:absolute;top:0;bottom:0;right:0;padding:1px}.intl-tel-input .selected-flag{z-index:1;position:relative;width:36px;height:100%;padding:0 0 0 8px}.intl-tel-input .selected-flag .iti-flag{position:absolute;top:0;bottom:0;margin:auto}.intl-tel-input .selected-flag .iti-arrow{position:absolute;top:50%;margin-top:-2px;right:6px;width:0;height:0;border-left:3px solid transparent;border-right:3px solid transparent;border-top:4px solid #555}.intl-tel-input .selected-flag .iti-arrow.up{border-top:none;border-bottom:4px solid #555}.intl-tel-input .co

Chrome Cache Entry: 117

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	56
Entropy (8bit):	4.743358334102714
Encrypted:	false
SSDEEP:	3:HCNCkuDKthb42mCGSxgN/mFjvy:QuqBTxgoF2
MD5:	6C4D19F6118B88915FCFA881F276CD7B
SHA1:	84DFB56C581D0A6E2397A8165E81256FEC927AE9
SHA-256:	B4C73B832B4E2345297CE6EB89B55B0B7623FB224F60CA7696086221D75127E2
SHA-512:	6D65D2271EA99A56E5E22252F2A676535131092059E9D7005C5C573A8B1D9CFF8D9A8E5873F26335F29006DA88ED6FA929ADA6EB7540E78EE7DFED6C3D8B005 B
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAlV4_8xSKzOihIFDWdns_4SEAlC7Bobt3SUbxIFDZ7ugoISFwmuH1Xuv6lRBBIFDdvvzhISBQ1zkk9Z?alt=proto
Preview:	CgkKBw1nZ7P+GgAKCQoHDZ7ugoIaAAoSCgcN2+/OEhoACgcNc5JPWRoA

Chrome Cache Entry: 118

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 10 x 25
Category:	dropped
Size (bytes):	637
Entropy (8bit):	7.25568542333341
Encrypted:	false
SSDEEP:	12:NfuKOCUPikeU1CWa2eh1ukRlJx1qIeKkXs2BPW+N6X2BOUpEdjGsXyCbujLl4XPG:NfuKqPB1C1JSAIelfBPWiOww7XyCbu/0
MD5:	E1238FDD48300132FA813F695FAA47F5
SHA1:	C20EF511ACCC8F9ABBE58229F5DB4B0B95D05C2C
SHA-256:	C6261F3A3317C6F047505C5C48092CDB2711759F2E70B8414FE8555B9AB0BFB7
SHA-512:	CD7B91AA5A355D41CF7A7A8D518D46C5215B0EDA9046F5829513B8052FA9D37B4778AC4CD4FD51684DC560EB59EE68B2909B4306E6E2F82D0E7A34B5069314E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....|....i....m..{..n.....p....r....v.....i.....h....m..l..t..q..j....i..n..t.....}..l.....|..y....m..x..{..q..k..q.....o.....o.....q.....j..{..y.....r..v..z..z..o..}.....v..z..|.....h.....k..s....h..l....x.....m..g..f.....l.....,.....@..S>|...Nn....''k.|...ZRCz..{..{z.t..)D&7....h...2.p..y-Pl..0%5Y....e.l.sG..='[T i.B4..@bf.zWw.V]. .''z_...z...v...<.....^|F.#M#.@..D.....A.C.0LPT..F....V.@.q... >`..a.%.bT.c...(...1A....!t.P....&. 1....zfP8..H.@.;

Chrome Cache Entry: 119

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 152192, version 330.15794
Category:	downloaded
Size (bytes):	152192
Entropy (8bit):	**7.99813044764158**
Encrypted:	**true**
SSDEEP:	3072:BHUC6F7WQApb6jtQnEIFAEbO7D9C08x+c7XGNLZeQ:b6F7ZpjpIFAEbO9L8xn7XIn
MD5:	D3D31317D040F3DD097BFA4401941D28

SHA1:	FCB010CD53F3ABE885C47AAA5CE5A667EC130F18
SHA-256:	E689270B831964B3FBFF3E17FDC3BE952CD831CEF717BD5EF39BCF0199C4FEAE
SHA-512:	D3AAA8B4C622C9DA060AEF1714E216B47D394AECEB4FE8AEDAA0B7F9427211916C410285F11184E41120851D1F08F9F2D358E602BF8AF1879418EB22DBD07171
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/webfonts/fa-regular-400.woff2
Preview:	wOF2.....R.....|..R#.J=.....?FFTM....`.....8.6.$..J..P.. ..F...a[.....nC....;...Q.6...]..!...l.,..PLu...5.....W&_.wK^./.].k.6a....@E..B1'...J.l....s...9...K.jU.[.D,.NZ.2.. .I..y.g.....T.T..k...T....N.. ..\e.Y....G..\..xw..c...X9....g../.AS.....f.h4@..g7df.B....i...A.....TFe....."MzS/..z..}..>...&..z.....!.....l...u.v(.r/py...Mb\|?*..SfJ.1._.....!.9....x....g....I..?. F._....1....0.j....Z.=.e..O.../=w>... {.....$.d.....q-...o.....9>.b.,.....W.;!.c...v.XM....`..nk..k...t].].Lv...n....{.....-..R.}.+3...L!.3x.W.T.....v.k....CV..._...v..Q.>)c..P$ .c.."pUY.AY.3....E-P.....f.=.Uw.u|..w..p]...@.....H`.#7.^.....F.=.....Fa.Q.....f.4Gh..% .vx.,.....rL<..I7...$..2.+.@.B.0E.I ....$..'C$(Up.D.q..\..:Ql..m..X..U.....-/.....z.7....UUooUonI....I.. ....J.p!.....U..Q.iSZ...KF|..[..q...x.n.k<s.....}M..3.....M..H.!e.....?O.a..].X..B.T)..b.cfN4.n.#q..'p[v..`Jaac..P..}_o.?."..J.....

Chrome Cache Entry: 120	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	18664
Entropy (8bit):	4.794460397487593
Encrypted:	false
SSDEEP:	384:JuOe0Vq06ZYLC9qNCUKbh3GE/M83wZGZNY0phDapIJp:xq0DcqNeh3GE/M8gZ2phDNp
MD5:	BAB3356ED6BB6A026937B3930E8A8DFE
SHA1:	097E395616D61543B79CF8FEAD8C06D9E78C6ECD
SHA-256:	0C916FAD3EB51C4AC4B65EB51B0EEDA029B4CAD9C84F56F76E43BC93D4D99286
SHA-512:	9ADA82CD1EAB6A4F53D65E911A2B97DBC6D720434CFA3F2B76557E09A8F59B379E091EBE42ED00101F54ADC4AB66E08270F384217640E75E96FA20CAA3C159DC
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/mt-script.js
Preview:	// <script language="JavaScript" type="text/javascript">.// note that we cuddle our elses in here, this is required for some .// browsers according to: http://en.wikipedia.org/wiki/JavaScript_syntax..var mailhost = 'https://aerosol.bumkins.com'../* If you want a default webmail application launched when a user. clicks on "webmail", then set this value to the name of the . webmail application as shown in the launch_selected_web_app. function below. */. .// var default_webmail = "squirrel";.// var default_webmail = "roundcube";.var default_webmail = "windex"; // the webmail index page../* A default destination for the "admin" link. Since the most common. admin function will be in qmailadmin, that is the default. You can. simply remove qmailadmin and leave a double quoted empty string . there ("") instead. The same applies for statistics. */..var default_admin = "qmailadmin";.var default_statistics = "munin";.// these color selectors determine the color of

Chrome Cache Entry: 121	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 5630 x 15, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	65960
Entropy (8bit):	**7.992139037271912**
Encrypted:	**true**
SSDEEP:	1536:bZPHu0UAVHiKwJom57/ec4WK9r76icNoW80bG1q6P9Jgr:lPHWiHVEokSN19r7dpWVG46PTgr
MD5:	AE33ACAE404631E997EF8D91DAE08CCD
SHA1:	19FAE9A6AA4BB419EBA378B0D0573906DC1BE38A
SHA-256:	38025784BEDEB5E4CAE496B131C85CABBD95AE0B1C0A3C9D9CB474D7262DB04B
SHA-512:	C1F0C98BCC1EA2D28A01CC7A14C2F77D8C4C99F7B00D10773E4F40BC7FC7703341AA89BCFA3927FD67EA10FCC6516D2532EDC1B43E7D788DE16309C8251DCBB9
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/twenty-one/img/flags.png
Preview:	.PNG.....IHDR.....d...oIDATx..u.\.....;>...=!.!..S.H.@...;u(V.....NB @.u..u..r~...&...&.....fv....y..<...Q.....5.....E.....N/b./....."T.)....._...:..T)..w..+...4..'4h~..._..;>.Mm_..$t."....".u.7I.?.....}&p;....?^....V.?.....;S...F/.....,.\|&...lg./.;.....t.X...[u..#..^[.=.`;.....Z.....`.....D...}.....=....;.<.~.....31[0{.....9.._...qs.u.Y[?...o...N,.U.l}..K..p.. .....N*..\|.F.Z.].u...b.C.....%.4..0.n..~.....w$...../..e.F.7...'.9..NEK>.~....~.Y6.....%...98fR..Y^|..|...0...i..#"....u-.?....u.....>^K...vs..>.t.:l.n.....?....u...~.r....?^.....Lb.h....Z.k .E..:.^....m.I.:...m.&..+.._).I...i...b....t....zPzC&Mw....>.....#/...?G.?O.....{...../...X..+.!kS.....r./..qk.....+.....O/!.M#.....4{.L..DQU,..Z.i..@...).J0..V..@....8@(.. X}./].3.A.I.P:..I..}.....E...u..^...n,....[.d.<..W....p.e../.m.....O..VI.cB...h.....=...(....7k<<..:.....o.q..Fw....A].?\V....

Chrome Cache Entry: 122	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (17213), with no line terminators
Category:	downloaded
Size (bytes):	17213
Entropy (8bit):	5.537850058572444

Encrypted:	false
SSDEEP:	384:QufhppYQthhqB9qANUYUnIFAr5au0GtFsy:1fh1th8BDNz/ArrDsy
MD5:	DE07DB035125277742B4B8DB60D234DE
SHA1:	CFF1BB46A450C1CEDCB6015655595EA97E11A1C3
SHA-256:	9C6BFC4E74046C6EEBC6EDBBCC1A61855E681709EB6239CF487E178CD4F6690F
SHA-512:	5F49F96213F5A173698CAD4FFB1EB5BA33224DC23E0E22D85FE20C5781FF68B7C86BC688D7F0D06DC0540B8526B26405B04B0145571B753575DDEE5208D57E5
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/js/bg/nGv8TnQEbG7rxu27zBphhV5oFwnrYjnPSH4XjNT2aQ8.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var n=function(y,e){if(!(y=(e=null,P.trustedTypes),y)||!y.createPolicy)return e;try{e=y.createPolicy("bg",{createHTML:b,createScript:b,createScriptURL:b})}catch(r){P.console&&P.console.error(r.message)}return e},b=function(y){return y},P=this||self;(0,eval)(function(y,e){return(e=n())&&1===y.eval(e.createScript("1"))?function(r){return e.createScript(r)}:function(r){return""+r}}(P)(Array(7824*Math.random()|0).join("\n")+'(function(){var x=function(e,y){if(e.P)return y5(e,e.v);return(y=f(true,e,8),y)&128&&(y^=128,e=f(true,e,2),y=(y<<2)+(e|0)),y},Mt=function(e,y,P,n,b,W,G){for(W=((b.Ki=iC,b.z_=(b.m9=eU,b[J]),b).hq=r2(b.l,{get:function(){return this.concat()}}),b.B8=T[b.l](b.hq,{value:{value:{}}}),[]),G=0;288>G;G++)W[G]=String.fromCharCode(G);k(true,(F(b,(F(b,(I((I(297,b,(q(function(r,A,D,N,O){I((O=(N=(A=(N=(O=(D=x(r),A=x(r),x(r)),x)(r),p(A,r)),p)(N,r),p)(O,r),D),r,GI(A,r,N,O))},b,((q(fun

Chrome Cache Entry: 123

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	711
Entropy (8bit):	5.148910519181866
Encrypted:	false
SSDEEP:	12:trz9k41+WEgs9jrL1ufWjjhKPw6wPUCIUfezqLti5LSdEupOF:t/9k41YnjhKPFwsgfMvLTupQ
MD5:	C76E793FF15BBB2D2722E3F457DE7605
SHA1:	29D5F44485C0021066A305CF7D4C8C0A02166D0C
SHA-256:	78972E26A47CE2F3FE151170B4E1270DEBCC9FEC0D1E56F88F3898F77C905405
SHA-512:	35FC7B9A32A481B464B71CDD30EA593616D9AFD11F9B3ADE50AF176E37DC7B350271F97718E3DB21914A462A5C7CE6BB76112CDD5C1AFDF74BCF93A83C502181
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/img/overlay-spinner.svg
Preview:	<svg width="115px" height="115px" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 100 100" preserveAspectRatio="xMidYMid" class="lds-dual-ring" style="background: none;"><circle cx="50" cy="50" ng-attr-r="{{config.radius}}" ng-attr-stroke-width="{{config.width}}" ng-attr-stroke="{{config.stroke}}" ng-attr-stroke-dasharray="{{config.dasharray}}" fill="none" stroke-linecap="round" r="40" stroke-width="4" stroke="#c2c2c2" stroke-dasharray="62.83185307179586 62.83185307179586" transform="rotate(166.292 50 50)"><animateTransform attributeName="transform" type="rotate" calcMode="linear" values="0 50 50;360 50 50" keyTimes="0;1" dur="1s" begin="0s" repeatCount="indefinite"></animateTransform></circle></svg>

Chrome Cache Entry: 124

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 200 x 25
Category:	downloaded
Size (bytes):	2658
Entropy (8bit):	7.835838708462061
Encrypted:	false
SSDEEP:	48:nuRRgtdBqIKpw3OE2/0lqoYv6ktQHobuqxWw01REQ9OcA:uRRg70H+3OE2/0soYvmob9Rgr9lA
MD5:	41880FA22172966FC2F080135F0ADAE7
SHA1:	26F5BDD7196D1D0A96D1D76D971CC0B3738115AA
SHA-256:	27CE260D2294E252FA98722E0B2D1C0F750F6024AA2DB5082EA6E5B48910C7A4
SHA-512:	80D45528EDC16FFEB4BDD386A18F858008E5890982E1567816D6C5BE865B7FA148F3B0BF52094EAE2E279DF4C33C61FF5AB3641F433F5C7185F0BB213E254FE
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/images/mt_tab-left-off.gif
Preview:	GIF89a.....|..i..v.....i....}..p..n..i.....u..{.....i..m.....q.....{.....v..v....q.....v.....l..q.....m.....|....{..m....{.....|.....|..r..r.....l.....m.....r..|.....w....l.....h..p..w....q....z.....y.....f!.....,.....@... .. x.....Ay..4...Z..\e.....Z,,..e.,.],.4.....\].....e,.....\.....,....44.....X...J...dj\h1CI.....B&.fdl....3(..P....`(Bd.R!C..%Rd.p..%J..\.qd...+.....!~|..'.-..I.1..&-k.....%o.`zsgG.#1*9...J.8..Xu.B.,-f.....G"....~.+V.x...#K>.x.d.'K..9qg.A...yt..9.V....=z(..-.6..m.][.....v..h.#'.<....G.....[....{..]|8x.e.P.A...[.....,.....^}...._.Q...|.....A.=`!a{.b..~Q@.a.2.w.|..(..... .....b...g... ...X...^._.....h$.! .....FZ..m..gT..Yd.a..c.u.e...)..\.y.d.l...0@...6da..p.'.6....D....

Chrome Cache Entry: 125

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (56398), with no line terminators
Category:	downloaded

Size (bytes):	56398
Entropy (8bit):	5.907604034780877
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKYlebyB5lxRx54PHSGdXXwW7MFWwXVuE2:4UcW6v+0B5chXwW49z2
MD5:	EB4BC511F79F7A1573B45F5775B3A99B
SHA1:	D910FB51AD7316AA54F055079374574698E74B35
SHA-256:	7859A62E04B0ACB06516EB12454DE6673883ECFAEAED6C254659BCA7CD59C050
SHA-512:	EC9BDF1C91B6262B183FD23F640EAC22016D1F42DB631380676ED34B962E01BADDA91F9CBDFA189B42FE3182A992F1B95A7353AF41E41B2D6E1DAB17E87637A0
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(

Chrome Cache Entry: 126

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, ASCII text
Category:	downloaded
Size (bytes):	345
Entropy (8bit):	5.23939483518923
Encrypted:	false
SSDEEP:	6:TMVBdoIUnWn8FX0wa9Fgc4svquXsLwFcn4mc4sVI/iHIF0GzFFRBAEdOqkswFFt+:TMHdoIWWnMEwKFcuX4wp57fGpFRjdOLU
MD5:	AB99593EFDF397078F11D9C37DD218A1
SHA1:	34540FFC5331CC545C1035B06A72B4F8D375973D
SHA-256:	BEAB79184BF1FCA1F52FF3761F8A533827106FEF3749C6C9C9A3E7EEC619A226
SHA-512:	A392A7302AB5E859485363D6DAD05AF64A1AF11FCA0F113184CB13EE14263F9C0F1EB8A0FC456C7D033383F7880B2DFFECE63D284192A6D903ACD2197274E140
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/favicon.ico
Preview:	<?xml version="1.0" encoding="iso-8859-1"?>.<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">. <head>. <title>404 - Not Found</title>. </head>. <body>. 404 - Not Found . </body>.</html>.

Chrome Cache Entry: 127

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	784
Entropy (8bit):	5.07253324905626
Encrypted:	false
SSDEEP:	12:BMQti6QclfhzFymDRZc+wE0xXhhNHC2pQfavBjBd27LUAio5B9jL:WCispzcaZ8xZCCdZ9dmUI9v
MD5:	E8BB2D5A7EAFD393748F52C6FA72F583
SHA1:	F6A86F462B82711395644206AE96C156BEA378FB
SHA-256:	38BD595734A715A7CBE28DF4AA887C8D5CE88EB137DDA3EC5AD0A7B96FFBA777
SHA-512:	1B42AAE7F9FB5FB13D8C12093F435248F90AE87FDD204D33C8165ACB909C99FBCA25DC9F34AFB5A84417A4A9B8A2B8E096F329F45A3BF3758F2D65FF6F55D20A
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">..<html lang="en">.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<title>WebMail - Powered By Mail::Toaster</title>..<meta name="generator" content="TextMate http://macromates.com/">..<meta name="author" content="Matt Simerson">..<link rel="stylesheet" href="mt-style.css" type="text/css" media="screen" title="no title" charset="utf-8" />.. Date: 2006-08-12 -->.</head>..<frameset rows="60,92%">.<frame src="mt-top.html" name="mt-head" id="mt-head" scrolling="no" noresize="noresize" frameborder="0"/>.<frame src="mt-login.html" name="mt_body" id="mt_body" scrolling="auto" noresize="noresize" frameborder="0"/>.<noframes>.. #include virtual="mt-login.html" -->..</noframes>.</frameset>..</html>.

Chrome Cache Entry: 128

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	28
Entropy (8bit):	4.208966082694623
Encrypted:	false
SSDEEP:	3:iMCnSoICkY:ESckY
MD5:	E42D89C5C5A44797E0B79ED1E489CF5B
SHA1:	F2939E3F99A4F5565F0C5DA11FB8364D97276A7E
SHA-256:	7766B07BB1CA49EB740B2F6B55D0AE1148312156CF1A12F877813B2C5D2CCCD6
SHA-512:	86704CBB82D12B515E03B66FA5DCEECE30BBBF1396B33BBD5D157CA94385EF4B9352EA4DB2125818F29D4DDA60FB77120A18DB9B131186272003688048160700
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISFwkCrS8BwjLoIxIFDZ7ugoISBQ1TWkfF?alt=proto
Preview:	ChIKBw2e7oKCGgAKBw1TWkfFGgA=

Chrome Cache Entry: 129

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 123132, version 330.15794
Category:	downloaded
Size (bytes):	123132
Entropy (8bit):	**7.998045700567174**
Encrypted:	**true**
SSDEEP:	3072:8DgGlpde8rM7EYqTOAlaS0ySo2OxgYxeyIpmF8Mvx5lh:8flfen7nqTOAF0Do2O2YoyYmF8Mp5f
MD5:	ED0564F6AC76FA57DF8A5A1F142F4157
SHA1:	2B4337D89FFF7D9F9C4CC4A92FE9039AD378EFE9
SHA-256:	550F1AE5D566AFED493AB8B5F1DD1B4D5A777EF19D1B3C57BF7B01025FEFD38C
SHA-512:	64C6056EFF382497EB44FB5DA080F5C2996BBB8C69C8F74E9DAB9BF3B5BE36F80CF44447F7C2BB4A4C1B257CDC2E9EA11A8959A926C550B92E4A264FC3D2CI 22
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/webfonts/fa-solid-900.woff2
Preview:	wOF2.....+.....J=.....?FFTM....`.....`..._.6.$..J..P.. .....a[...C..oC.....`Z...}..e....::4V.+O>..\.<1chW.....J.1.f...8.;!..W.D....d.....3.D..l(buO5.....[7..C .#NoS....c..[.d...>b.8....(.....K)'3...9.....C.....^#].]....m.%\|.Tl.f..(.q.\|...+.FO".R.?...^F....$.....,&"#"#++&I.....%.J...d..1A...I.B._.e..O...NN...G<Q...k.^w..;..w..k..._..RJ<.K. ws._...Z+..m...H.....I...1....JT...Xx.....6c...^.V.:....."..).4..}....&.?..>.g.?...-..+.j.v.+Z6j].U..Do.....Z.E/`Dm.....d*.0.E.0.(..H.....J.W./+>.....-d.`mC...9^.)....@...?...`a.`E.dO..X ~.....@>...V...2..ZX.M...4.y....K..M.R.YYYV.h&..$...PU. [U.(.dO...9....k....4.....zO.n.vL.....\|v....g.....$m...B./+...]..H.BM..n.....B;.A..y.....6.....QS."....$..3H.....&.....8... ".....%.....5*8VQ.k.m..i[..h.`.j._..]...U.[....;}..d;,..w..lS.....tB....J....f.$.%S..I....5.....!.]e;l.4.fAg.....}..&..KC0t...F.....+b...|[

Chrome Cache Entry: 130

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.098952451791238
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezocKqD:J0+oxBeRmR9etdzRxGez1T
MD5:	62962DAA1B19BBCC2DB10B7BFD531EA6
SHA1:	D64BAE91091EDA6A7532EBEC06AA70893B79E1F8
SHA-256:	80C3FE2AE1062ABF56456F52518BD670F9EC3917B7F85E152B347AC6B6FAF880
SHA-512:	9002A0475FDB38541E78048709006926655C726E93E823B84E2DBF5B53FD539A5342E7266447D23DB0E5528E27A19961B115B180C94F2272FF124C7E5C8304E7
Malicious:	false
Reputation:	low
URL:	http://https://mail-toaster.org/favicon.ico
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .</body></html>.

Chrome Cache Entry: 131

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded

Size (bytes):	4801
Entropy (8bit):	5.226064337345134
Encrypted:	false
SSDEEP:	96:fn2oGwfJ4lZmLOaclKlsyPl0yMl8Q0l5ZbVoHEILn2YPlGMKfILhN:f2rwhSwOdgsU0y+G7pYrd7ZhN
MD5:	D31F08737561CED0EC7E24FEDBC534A8
SHA1:	8A888F5C4ACF039B6DA4BCA8D323D1B68BCB60B4
SHA-256:	35CA691F111F34897AB5E3C685C19BA712A729114719D42A43B6666C0FB4311E
SHA-512:	DD97F735980122420DCE18643333465E3E1A5CF5BE378B2AA82A42DB95E125B4106191CCCB3F0EDCDEE25734B1B8367FAFA84D037DD70CAC3EC0AAB603410F4F
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/mt-style.css
Preview:	/* . Author: Matt Simerson (matt@tnpi.net).. Version: 1.1...Date: 2006.10.17.....colors in use:... dark grey: #333333 text.. light grey: #666666 active text... .tan bg: #FFFFCC active/middle bar. .tan bg: #CCCC99 background page color.*/.* html div#header {./* "tan hack", for IE box model positioning bug ..http://www.communitymx.com/content/article.cfm?cid=E0989953B6F20B41.*/..width: 97%; /* IE 5 win */..w\idth: 98%; /* IE 6 & IE5 mac */.}.body {..margin-left: 0px;..font-family: Verdana, Helvetica, Arial, sans-serif;..font-size: 11px;..background-color: #CCCC99;..background-image: url("images/mt_background.png");.}.div#header {..position: absolute;..top: 0px;..left: 10px;..right: 10px;..padding-right: 10px;..padding-left: 10px;..padding-top: 5px;..height: 25px;./*..background-color: #ffffff;..color: #666666;.*/.}..div#top_level_links {..height: 24px;..margin: 0px;..width: 550px;./*..background-color: #FFFFCC;.*/.}.div#top_level_links span {./* these are the t

Chrome Cache Entry: 132	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 200 x 25
Category:	dropped
Size (bytes):	2583
Entropy (8bit):	7.84269204717794
Encrypted:	false
SSDEEP:	48:nrT5iepOXhvoTEF4R2+7LjNS/oaJ975v9eKg90z9e/woJd2uH/uzqiAmLs3:n/tER2A4R2+RhafhUKg90z9e/woaknvR
MD5:	E757CB3BB9D9AA01962887657915D947
SHA1:	F0C7636684B921B5B31AF4FB50ECBD18E64FD15F
SHA-256:	56DE3FA10EEE464527BB9A439C672389635EF9F782A8404033F955CA0FB6A152
SHA-512:	473C59EF6CE45964EE5B3633B5346B06AADDA03051755FF09AC639EEF74C4568B05263928C2ED64FF4D77570F1F41D054B8EBD11018A77B01DEEEEEB57F5805E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....|....v....v..r..j..i..q..i..g....t..o.....{..y.....x..m.....i.....q.....{.....v.....v..q.....l.....q..m.....i.....|..{..m.....{.....|..l.....m..h..r.....l..n.....r....|.....s..l..g..y.....k..l.....f!.....,.....@...4.2....r.....9B00(.p.^.Du,,.ci.0,.,g99,i.90d.....g.0..,cd...B,...i9...0....c.....BB.....^.:3.W.W..}..a..q,..R.F.*=x... E...y...Qc...4.H...J..Sh.Ae%..1_.)S.G.$7..H.dM..W.....LA.l...(k..HT&.....R.L.HK:u.....6.K...x...s@.....a.....+^....#K.L.r...4...gN....Lz...z.....:j.[.fm....o....i.G...:8o..^..uq..[..].9n.z.(..d....<x@'..a...n>H....`.^.....~G..Alw.}.).D...~.]._....._...8!~....z.!..y.....a~,.....&(.}..w..h..^.w.!k..AeD.i.H&.$.b6...y.q....A..6....\...6...P....R.I&.Z....YB..m..&.Z...Z.i..Y.9..

Chrome Cache Entry: 133	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	28
Entropy (8bit):	4.2359263506290326
Encrypted:	false
SSDEEP:	3:QQinPt:+Pt
MD5:	1505E9BB79B4C3F51AEC072BFF0E4F1D
SHA1:	C2229235760065DD7708E3D63A718B05FF209F37
SHA-256:	C3E80C02DBB99150A42F8867CFC2BD1565E9B7DE84EB4F3D75C9AF0A674566D1
SHA-512:	C0B996819ED4D93E5D5158867080BC16B479FD2EE651FD4F56453ABCEF6F5B5C67BB6E313D29971A61BE963BE67F4483939B89DDBB711B647453F7A0B966D47C
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISFwllImeng_eGLRIFDXhvEhkSBQ3OQUx6?alt=proto
Preview:	ChIKBw14bxIZGgAKBw3OQUx6GgA=

Chrome Cache Entry: 134	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded

Size (bytes):	200
Entropy (8bit):	4.942373347667344
Encrypted:	false
SSDEEP:	3:qTkIDZxVsJYkup3XyHFeTrAyTKTWKMrBKblbJ4ZNDpVbz2USrGXI9kBbZ6iF4:qTjxVgYkYv3J/14QpcUAVuB965
MD5:	3437AADDCDF6922D623E172C2D6F9278
SHA1:	F69066CF20141AC93418102D3EEE7C0225B8A623
SHA-256:	35DCC382EB69D00369D708708CDC545F3968B68FA5BBE3E728D11FEDD04F93BB
SHA-512:	2DAE5C5C30C6A0E763D8128F2CE1D467EAD432E582AB4EBB68E23991DB08F57490ABC0EED805FD33FAB5503C1737D9D47D4CC1090AE15D7391593FBB295D6E7
Malicious:	false
Reputation:	low
URL:	http://https://js.stripe.com/v3/m-outer-3437aaddcdf6922d623e172c2d6f9278.html
Preview:	<!doctype html><html><head><meta charset="utf-8"/><script defer="defer" src="https://js.stripe.com/v3/fingerprinted/js/m-outer-15a2b40a058ddff1cffdb63779fe3de1.js"></script></head><body></body></html>

Chrome Cache Entry: 135

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (3087)
Category:	downloaded
Size (bytes):	11195
Entropy (8bit):	5.033925961026424
Encrypted:	false
SSDEEP:	192:1LExtwS2bcy8PgItVs8y8xlN0DdbATTJ8g/TpCz9YTc4csc8DoBAlNX:1oxtwSQcZPDVsCcUZrpCzZ378Do+z
MD5:	11F6FC38E1E5C535960FC8E78910C1BA
SHA1:	E591D8B955528A733632A231C82DCBFB7B4D481E
SHA-256:	414881D00CA6A4C27551564A8F0B5C82A6E3335592D89A4C24D96E28B1C5AB10
SHA-512:	18ACDEC2E90910F4BB63C2AD7E676575924A7BB5FD9324DB1DADEAABBFD98251150A4A07276D1287C3C8A2BAE1D574A5F72979AE71848592DA84367B3DEE853D
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/js/StatesDropdown.js
Preview:	var states = new Array();.states['AU'] = ["Australian Capital Territory","New South Wales","Northern Territory","Queensland","South Australia","Tasmania","Victoria","Western Australia","end"];.states['BR'] = ["AC","AL","AP","AM","BA","CE","DF","ES","GO","MA","MT","MS","MG","PA","PB","PR","PE","PI","RJ","RN","RS","RO","RR","SC","SP","SE","TO","end"];.states['CA'] = ["Alberta","British Columbia","Manitoba","New Brunswick","Newfoundland","Northwest Territories","Nova Scotia","Nunavut","Ontario","Prince Edward Island","Quebec","Saskatchewan","Yukon","end"];.states['FR'] = ["Ain","Aisne","Allier","Alpes-de-Haute-Provence","Hautes-Alpes","Alpes-Maritimes","Ard.che","Ardennes","Ari.ge","Aube","Aude","Aveyron","Bouches-du-Rh.ne","Calvados","Cantal","Charente","Charente-Maritime","Cher","Corr.ze","Corse-du-Sud", "Haute-Corse", "C.te-d'Or", "C.tes-d'Armor", "Creuse", "Dordogne", "Doubs", "Dr.me", "Eure", "Eure-et-Loir", "Finist.re", "Gard", "Haute-Garonne", "Gers", "Gironde", "H.rault",

Chrome Cache Entry: 136

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	68
Entropy (8bit):	4.750173179933465
Encrypted:	false
SSDEEP:	3:HCNCkuWy2Fx42K21GSxgN/mFjvy:QuWTFxfKaxgoF2
MD5:	B4BB0FCEDB4B32FF3B54014916956868
SHA1:	F44B8F48D7DFBCF02368911CFF8401516A910365
SHA-256:	25CF9C0820B01F3507B02376D3011D5EA28A0956F3BB5BB9258CACB1F15C3A44
SHA-512:	16D5D196B581211C9E875AC2574379E27E2BBC7C5EBFEAC4D9E42306AF4AFAA7CCF88E97B58722DAD6EE85E5105DFCC074BF9CBC164436A3EE04E63C62576346
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAlV4_8xSKzOihIFDWdns_4SFwmJRNoVCidCmRIFDVNVgbUSBQ3OQUx6EhcJrh9V7r-pUQQSBQ3b784SEgUNc5JPWQ==?alt=proto
Preview:	CgkKBw1nZ7P+GgAKEgoHDVNVgbUaAAoHDc5BTHoaAAoSCgcN2+/OEhoACgcNc5JPWRoA

Chrome Cache Entry: 76

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1288), with no line terminators

Category:	downloaded
Size (bytes):	1288
Entropy (8bit):	5.803547307207809
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZJIX6+KVCLTLv138EgFB5vtTGJTlWtZ1v8IgsLqo40RWUnYN:VKEcixKonR3evtTA871v8IhLrwUnG
MD5:	D35A5B9D50FFD75F75F2AE733FE486C0
SHA1:	CD9BD666D9E47C5C3E62936F5CFA46F012719E09
SHA-256:	6B5293BDC08B1E6D6DCA10429F493C178AB594918B4A93F0792AA7DE7B56455F
SHA-512:	68242889117B119F5E2E2691DC2E7BD454DA71609111E4652936191CA95C6DD79AAF236A2D7F864AB27BA1125F6FB940BFD629AF185A8E22EC459C59EFAE01F
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api.js?onload=recaptchaLoadCallback&render=explicit&_=1708664105623
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('explicit');(cfg['onload']=cfg['onload']||[]).push('recaptchaLoadCallback');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;var m=d.createElement('meta');m.httpEquiv='origin-trial';m.content='Az520Inasey3TAyqLyojQa8MnmCALSEU29yQFW8dePZ7xQTvSt73pHazLFTK5f7SyLUJSo2uKLesEtEa9aUYcgMAAACPeyJvcmlnaW4iOiJodHRwczovL2dvb2dsZS5jb206NDQzIiwiZmVhdHVyZSI6IkRpc2FibGVUaGlyZFBhcnR5U3RvcmFnZVBhcnRpdGlvbmluZyIsImV4cGlyeSI6MTcyNTQwNzk5OSwiaXNTdWJkb21haW4iOnRydWUsImlzVGhpcmRQYXJ0eSI6dHJ1ZX0=';d.head.prepend(m);po.src='https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js';po.crossOrigin='anonym

Chrome Cache Entry: 77

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (30442), with no line terminators
Category:	downloaded
Size (bytes):	30442
Entropy (8bit):	4.925189241178507
Encrypted:	false
SSDEEP:	384:DOHCYV0WfqiMuiN0RKrDCsgspL4T9lgz56y/j1:Dy6CBNTT9K6s1
MD5:	E0C6FD59657DBC6DB1DB4E067133E30C
SHA1:	0E418AC6F7FD1E07F5B6BC66B296AB72E9242CA7
SHA-256:	2D83A5ED4615A183FECA72A12F5A33478571BDE7C7E8916A9BB5BA7011AE8DA5
SHA-512:	070C8AAC9E4443CAC419B115EB813B5949BCE971C681A2D732B9C6AAFD1D357949789B5133A55AD8B212366DCA02CE48C55BD9411DF22C46125A5940B1BC3FF
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/orderforms/standard_cart/css/all.min.css?v=0d4099
Preview:	#order-standard_cart{margin:0;padding:0 0 40px 0;font-size:14px}#order-standard_cart .cart-sidebar{float:left;width:25%;position:relative;min-height:1px;padding-right:15px;padding-left:15px}#order-standard_cart .cart-body{float:right;width:75%;position:relative;min-height:1px;padding-right:15px;padding-left:15px}#order-standard_cart .secondary-cart-body{float:left;width:65%;position:relative;min-height:1px;padding-right:15px;padding-left:15px}#order-standard_cart .secondary-cart-sidebar{float:right;width:35%;position:relative;min-height:1px;padding-right:15px;padding-left:15px}@media only screen and (max-width:1199px){#order-standard_cart .cart-sidebar{display:none}#order-standard_cart .cart-body{width:100%;float:none}#order-standard_cart .secondary-cart-body{width:69%}#order-standard_cart .secondary-cart-sidebar{width:31%}}@media only screen and (max-width:991px){#order-standard_cart .secondary-cart-body{width:100%;float:none}#order-standard_cart .secondary-cart-sidebar{margin:0 auto;

Chrome Cache Entry: 78

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 200 x 25
Category:	downloaded
Size (bytes):	2583
Entropy (8bit):	7.84269204717794
Encrypted:	false
SSDEEP:	48:nrT5iepOXhvoTEF4R2+7LjNS/oaJ975v9eKg90z9e/woJd2uH/uzqiAmLs3:n/tER2A4R2+RhafhUKg90z9e/woaknvR
MD5:	E757CB3BB9D9AA01962887657915D947
SHA1:	F0C7636684B921B5B31AF4FB50ECBD18E64FD15F
SHA-256:	56DE3FA10EEE464527BB9A439C672389635EF9F782A8404033F955CA0FB6A152
SHA-512:	473C59EF6CE45964EE5B3633B5346B06AADDA03051755FF09AC639EEF74C4568B05263928C2ED64FF4D77570F1F41D054B8EBD11018A77B01DEEEEEB57F5805E
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/images/mt_tab-middle-off.gif
Preview:	GIF89a.....|....v....v..r..j..i..q..i..g....t..o.....{..y.....x..m.....i.....q.....{.....v.....v..q.....l.....q..m.....i.....|..{..m.....{.....|..l.....m..h..r.....l..n.....r....|.....s..l..g..y.....k..l.....f!.....,.....@...4.2....r.....9B00(.p.^.Du,,.ci.0,.,g99,i.90d.....g.0..,cd...B,...i9...0....c.....BB.....^.:3.W.W..}..a..q,..R.F.*=x... E...y...Qc...4.H...J..Sh.Ae%..1_.)S.G.$7..H.dM..W.....LA.l...(k..HT&.....R.L.HK:u.....6.K...x...s@.....a.....+^....#K.L.r...4...gN....Lz...z.....:j.[.fm....o....i.G...:8o..^..uq..[..].9n.z.(..d....<x@'..a...n>H....`.^.....~G..Alw.}.).D...~.]._....._...8!~....z.!..y.....a~,.....&(.}..w..h..^.w.!k..AeD.i.H&.$.b6...y.q....A..6....\...6...P....R.I&.Z....YB..m..&.Z...Z.i..Y.9..

Chrome Cache Entry: 79	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	112
Entropy (8bit):	4.387569884524225
Encrypted:	false
SSDEEP:	3:qVvjNAGDEtvOqL/rb63XADyiJS4UEOmRHngkXj4YUv5c4NGL:qFjSGDEdOq+nA2ic4d/gkfUvC4QL
MD5:	17C1752B115CE245FC16F12C376066EA
SHA1:	A51E0AB60069B90FD5240299B2E80A385BB2A599
SHA-256:	AB329942EC7599ABBE6B56BAE982FCAF758F4C36D9792E2095CB41F75DF62635
SHA-512:	00761A53F7A271BC0F650CB42625F0F7D9C091E27B40093CE4337F612AC61280DBF867CBDC6396AFAFDBCC5C7939D8F378FB09E202DCD13C36DDB84D9D1AC5D
Malicious:	false
Reputation:	low
URL:	http://https://mail-toaster.org/
Preview:	<html>. <head>. </head>. <body>. The Art Farm . </body>.</html>.

Chrome Cache Entry: 80	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.954234440752388
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKPMwmIknZSSZgWaee:PLKdXNQKss6gL
MD5:	7E005BC0107FE8DD6255D4253228EF02
SHA1:	718501672A9B00AFFE1D688D7B3F2F6202E3E96E
SHA-256:	80663B7D03F283B27D8D833CA725A43D5CD3D5B5A7DD6487970DCA9469F9C139
SHA-512:	3F17B8CCEF75B49E01343A33D14744D589C87EC2A574B529E7EC65ED921C47D6D4A6F768CA4229B4A0B9E87D6624D76E0B4241AD214014305A9AA8E76643315
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=1kRDYC3bfA-o6-tsWzIBvp7k
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js');

Chrome Cache Entry: 81	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 164724, version 330.15794
Category:	downloaded
Size (bytes):	164724
Entropy (8bit):	**7.998653023534962**
Encrypted:	**true**
SSDEEP:	3072:33CPheB5wPws0xJ8VvY5ZzQ/ogbAihfu4wvTbpNuHZSdF25iBCW/5:EhYagx6euoN4w7TuHZh5q3x
MD5:	50EF43C2FFD372CE035948A55FFCEA13
SHA1:	884852A7EAFD498F8EA55A2DAB6AE4521388E0DD
SHA-256:	F8CDFE0414EAC9A2380C093C8F3DE44E1298E2EF2F9FCDF3A999F86C357AB5E2
SHA-512:	FAD4152770105B2B21823CE64595819F83BECEB43F11B1128670A653A0F9F94BA738AA6640B3AE80E95CCA50BAB70B89AFD169DD6B7683FB1616AA28B477DB80
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/assets/webfonts/fa-light-300.woff2
Preview:	wOF2.....t.....J=.....?FFTM....`.....j.6.$..J..P.. .....a[`8...."(..@...3)E..m.7.c3...R.ln.....x.;.*..* .....[2....K.%)((L.N7u~.G(..Wi`V.W#(.....J#.<.I.[Y.e.....`.....(.m..B.<h..1""f.....L.P.P.....f/...v.....I.U?.7}./....._.Qh4@.C$$.....65..V.....I....(..UN.tE..#.!..S&...L.. c.b.....Zk.>.....FDD.....I..Sk.j.....{....prwu,.;..g....y.*.i..'@.6.n.t.....$.-...zp....h:...c..-.a+Q..Q.....m....r+.%.d.F..#..pp...P.....J@...q.u.j.W.c.....nZ.....j..K.o....^...+n(F.AH...R.?."i...c.E....Y..,...9..f3.....2.T.~.2fX..U..=.R.....mz..[...Ov.{.x0.D...K..G.....5@s...I...=.....v.F*)C.7.a&hc.Q`%.`...+b./....fw.j..>.L.....:..M7..M.....F:....X..c...J.B.7...{....z4i.....U..u-,.&.....0.s.]5_ ....._*.I].@8..*d.H.'.."......($K..f.z..d.s...}=..%x02#...M|6.M....c._... R%...IE.<....x^wP.6C....Zs`-W.y.R.i....`:.?|..T..z..~ht...x....$..>^.V.$.0.<.....8...x.....}_..r>..R..*.a...p'.

Chrome Cache Entry: 82	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with very long lines (568)
Category:	downloaded
Size (bytes):	503430
Entropy (8bit):	5.708119764112345
Encrypted:	false
SSDEEP:	6144:HEYt9e4UlnQyfZLsIB74RSHywNGte2fp0YROQVZT+DSUAZqH/:Hi9fpj140SwQz0YRO+ZSj/
MD5:	3E528C5BD4E8985F914F84BC5F86DF5F
SHA1:	34104EA645A6789DD9CB58C264E20ED6855EA1DE
SHA-256:	E51E616D124133B0FB24968469097A4D311B972F78455143D940703EA0639BA6
SHA-512:	C59A1D40F649446F33FF0FF3FA9A8E997D3CFF10F968D35226BA08BB91C9013AE937460CF2DAB0888848ABE1B693D4377FBD6904E3E03360B15035A8C3E9BC9
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2005, 2007 Bob Ippolito. All Rights Reserved.. Copyright The Closure Library Authors.. SPDX-License-Identifier: MIT.*/./*. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var C=function(){return[function(f,q,S,Z,P,X,U){return(f|((X=[1,6,4],(f+X[1]&X[2])<X[0]&&3<=((f^17)&7))&&(this.X=S,this.N=q),X[1]))>>3||(P=0,P=void 0===P?0:P,U=l[16](14,q,L[13](26,Z,S),P)),U},function(f,q,S,Z,P,X,U,b,k,E,J,K,B,n,F,c){if(1<=((f|(F=(f-7>>3||(c=q instanceof qd&&q.constructor===qd?q.N:"type_error:SafeUrl"),["T","call",0]),72))==f&&(c=u[22](26,function(r,g,m){m=["could not contact reCAPTCHA.",15,(g=[2,3,6],"recaptcha::2fa")];switch(r.N){case 1:if(!U.C)throw Error(m[0]);if(!U.X)return r.return(l[19](72,.g[0]));if("string"!==typeof X||X.length!=g[2])return r.return(l[19](32,P));return u[10]((r.C=g[0],m[1]),P,U.C,r);case P:C[2

Chrome Cache Entry: 83

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 10 x 25
Category:	downloaded
Size (bytes):	637
Entropy (8bit):	7.25568542333341
Encrypted:	false
SSDEEP:	12:NfuKOCUPikeU1CWa2eh1ukRlJx1qIeKkXs2BPW+N6X2BOUpEdjGsXyCbujLl4XPG:NfuKqPB1C1JSAIelfBPWiOww7XyCbu/0
MD5:	E1238FDD48300132FA813F695FAA47F5
SHA1:	C20EF511ACCC8F9ABBE58229F5DB4B0B95D05C2C
SHA-256:	C6261F3A3317C6F047505C5C48092CDB2711759F2E70B8414FE8555B9AB0BFB7
SHA-512:	CD7B91AA5A355D41CF7A7A8D518D46C5215B0EDA9046F5829513B8052FA9D37B4778AC4CD4FD51684DC560EB59EE68B2909B4306E6E2F82D0E7A34B5069314E
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/images/mt_tab-right-off.gif
Preview:	GIF89a.....|....i....m..{..n.....p.....r....v.....i.....h....m..l..t..q..j....i..n..t.....}..l.....|..y....m..x..{..q..k..q.....o.....o.....q.....j..{..y.....r..v..z..z..o..}.....v..z..|.....h.....k..s....h..l.....x.....m..g..f.....!.....,.....@..S>|...Nn...."k.|...ZRCz..{..{z.t..)D&7....h...2.p..y-Pl..0%5Y....e.l.sG..=.'[T i.B4..@bf.zWw.V]. ."z_...z...v...<.....^|F.#M#.@..D.....A.C.0LPT..F....V.@.q... >`..a.%.bT.c...(...1A....!t.P....&. 1....zfP8..H.@.;

Chrome Cache Entry: 84

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (65530), with no line terminators
Category:	downloaded
Size (bytes):	614540
Entropy (8bit):	5.355923798751124
Encrypted:	false
SSDEEP:	12288:ks7/FZduSMJSl3pHfHsH3HzBj4fRif+QUBXSD+s0avTkNcGaIs0a1l3lIyzaTEv/:72RiDrI4yIMQ5D8hlvk
MD5:	F9EC2D86FDC73DFEEE3C098C160118FB
SHA1:	B36549959DCDE7870E9F12F2E37196943548C9BF
SHA-256:	198FE8FFABD1262C5D7D80807B7002F21D36C045E2ADE244496EBC1EF394B716
SHA-512:	D0E19C834E1198014CAF3F6AD33926180FD7966ABF9CA9AE7EA1FF6E7988F35B7CF2AA79A5F6A2EBC0EF3DB88472812B4079435BECA01FAABCF464C8386E88A6
Malicious:	false
Reputation:	low
URL:	http://https://js.stripe.com/v3/
Preview:	!function(){function e(t){var n=o[t];if(void 0!==n)return n.exports;var a=o[t]={id:t,loaded:!1,exports:{}};return r[t](a,a.exports,e),a.loaded=!0,a.exports}var t,n,r={723:function(e,t,n){"use strict";function r(e){l.length||(i(),!0),l[l.length]=e}function o(){for(;d<l.length;){var e=d;if(d+=1,l[e].call(),d>1024){for(var t=0,n=l.length-d;t<n;t++)l[t]=l[t+d];l.length-=d,d=0}}l.length=0,d=0,!1}function a(e){return function(){function t(){clearTimeout(n),clearInterval(r),e()}var n=setTimeout(t,0),r=setInterval(t,50)}}e.exports=r;var i,c,s,u,l=[],d=0,p=void 0!==n.g?n.g:self,m=p.MutationObserver||p.WebKitMutationObserver;"function"==typeof m?(c=1,s=new m(o),u=document.createTextNode(""),s.observe(u,{characterData:!0}),i=function(){c=-c,u.data=c}):i=a(o),r.requestFlush=i,r.makeRequestCallFromTimer=a},5937:function(e,t,n){e.exports=n.p+"fingerprinted/img/abnamro-4445e65420800f96f68cfc67a273f66b.svg"},1520:function(e,t,n){e.exports=n.p+"fingerprinted/img/asn-3d9b1bbff2f8f12105510992dbb37ae8.svg

Chrome Cache Entry: 85	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D9
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PIP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\..._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"lc.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...l.a....*+....(...S..\h....@.....I.$..%.2....I.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e...,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

Chrome Cache Entry: 86	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 5630 x 15, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	65960
Entropy (8bit):	**7.992139037271912**
Encrypted:	**true**
SSDEEP:	1536:bZPHu0UAVHiKwJom57/ec4WK9r76icNoW80bG1q6P9Jgr:lPHWiHVEokSN19r7dpWVG46PTgr
MD5:	AE33ACAE404631E997EF8D91DAE08CCD
SHA1:	19FAE9A6AA4BB419EBA378B0D0573906DC1BE38A
SHA-256:	38025784BEDEB5E4CAE496B131C85CABBD95AE0B1C0A3C9D9CB474D7262DB04B
SHA-512:	C1F0C98BCC1EA2D28A01CC7A14C2F77D8C4C99F7B00D10773E4F40BC7FC7703341AA89BCFA3927FD67EA10FCC6516D2532EDC1B43E7D788DE16309C8251DCBB9
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....d...oIDATx..u.\.....;>...=!.!..S.H.@...;u(V.....NB @.u..u..r~...&...&.....fv....y..<...Q.....5.....E.....N/b./....."T.)....._...:..T)..w..+...4..'4h~..._. ;>.Mm_..$t."....".u.7I.?.....}&p;....?^....V.?.....;S...F/.....,.|&...lg./.;.....t.X...[u..#..^[.=.`;.....Z.....`.....D...}.....=.....;.<.~.....31[0{.....9.._...qs.u.Y[?...o...N,.U.l}..K..p.. .....N*..|.F.Z.].u...b.C.....%.4..0.n..~.....w$...../..e.F.7...'.9..NEK>.~....~.Y6.....%...98fR..Y^|..|...0...i..#"....u-.?....u.....>^K...vs..>.t.:l.n.....?....u...~.r....?^.....Lb.h....Z.k .E..:.^....m.I.:...m.&..+..._).I...i...b....t....zPzC&Mw....>.....#/...?G.?O.....{...../....X..+..!kS.....r./../.qk.....+.....O/!.M#.....4{.L..DQU,..Z.i..@...).J0..V..@....8@(.. X}./].3.A.I.P:..I..}.....E...u..^...n,....[.d.<..W....p.e../.m.....O..VI.cB...h.....=...(....7k<<..:.....o.q..Fw....A].?\V....

Chrome Cache Entry: 87	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32033)
Category:	downloaded
Size (bytes):	637772
Entropy (8bit):	5.605037220552038
Encrypted:	false
SSDEEP:	6144:clbtX+kIsGZXbM9XYNYA6vNgOcWXlkteDgQ+SvtK28+zRQgy4qZVjaVjuh5:Tqswg7xktP1SvtKAzRyxYA5
MD5:	5A291C3AA07DB4473B89CFD375140758
SHA1:	5A167520F01FAED0EF401D1AA897E6EAB29BA796
SHA-256:	0945E6D555033D10E1C91A03EA5480492BDBF3DB070DB6E7CD732BE5C152DB4F
SHA-512:	0A3E360CA4BCC2F8235000229D39F17ECC964B0C8E933A2A04E0ED2EBA282E78C8A42A520B6EE9ECCDE53DB2D49D60A43AFAD139B59F90B0213ECF803D03E981
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/twenty-one/js/scripts.min.js?v=0d4099

Preview:	function scrollToGatewayInputError(){var e=jQuery(".gateway-errors,.assisted-cc-input-feedback").first(),t=e.closest("form");t||(t=jQuery("form").first()),t.find('button[type="submit"],input[type="submit"]').prop("disabled",!1).removeClass("disabled").find("i.fas,i.far,i.fal,i.fab").removeAttr("class").addClass("fas fa-arrow-circle-right").find("span").toggle(),e.length&&elementOutOfViewPort(e[0])&&jQuery("html, body").animate({scrollTop:e.offset().top-50},500)}function elementOutOfViewPort(e){var t=e.getBoundingClientRect(),n={};return n.top=t.top<0,n.left=t.left<0,n.bottom=t.bottom>(window.innerHeight||document.documentElement.clientHeight),n.right=t.right>(window.innerWidth||document.documentElement.clientWidth),n.any=n.top||n.left||n.bottom||n.right,n.any}function disableFields(e,t){"."!==e[0]&&(e="."+e);var n=jQuery(e);n.prop("disabled",t),t?n.addClass("disabled"):n.removeClass("disabled")}function checkAll(e,t){"."!==e[0]&&(e="."+e),jQuery(e).removeAttr("checked"),jQuery(t).is(":

Chrome Cache Entry: 88	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	706
Entropy (8bit):	5.430509054751938
Encrypted:	false
SSDEEP:	12:BMQbwuOiEX1ReQ8lf1KgHwjF9cscuKOtfMR4xw+VofgVe/qiWdJ4swxLQL:WaG1RgV8vcafmXgUUJzw2
MD5:	7C331E5D1D95FCA3E79820AEAC41F934
SHA1:	9D24DCA2DB5A8F8557F19FED6449D350B2340C7E
SHA-256:	897093802465F8AD6323A78DB3DC21C94A7C31E1D02972C06DCBEEBD6D5D1065
SHA-512:	B4F141151FBFFBB866FF6FA801DA74BDA9DF59702E784C4A957F48B0EA6F2D7E24E092CD5D687244F9546093290CB87E9D57235E7FE4D6EB07C931542F97FDF
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/mt-login.html
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">.<html>.<head>.<title>Mail::Toaster Webmail Login</title>.<meta http-equiv=Content-Type content="text/html; charset=ISO-8859-1">.<style type="text/css">. .body { margin-left:0px; margin-right:0px; margin-top:0px; background-color:#fff }.p:first-child { margin-top:0px }.h1 { font-size:18px; }.h3 { font-size:18px; }.-->.</style>.</head>.<body>.. .... To check your email: .... - Log in .... - click "webmail". .... - Enjoy! ... .. .</body>.</html>.

Chrome Cache Entry: 89	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 100 x 100, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	163
Entropy (8bit):	5.025279476306441
Encrypted:	false
SSDEEP:	3:yionv//thPlpbtqrK9Ag9RthwkBDsTBZtjjmpS/AlD+/qkltmfwk/t6S/ljp:6v/lhPt9AgjnDspjypiAU1tLsTtjp
MD5:	72B020240027209A169A7008BAE0084E
SHA1:	C5D5807AF53A4689971A46B363C642BD55613071
SHA-256:	938565F22323C33D0C80745EDFB364D38A445F6E51C1FEF7961AAF269F897170
SHA-512:	E676CF68332A2929137851F3D50539DFD544BDE2944F15EC1E2487E9FE2A563029A08021BC2C547F608A70A8196E958D16B08BFC9D9D91E2526562D0B66C86BE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...d...d.....G<ef....gAMA.....OX2....tEXtSoftware.Adobe ImageReadyq.e<....PLTE...../......#IDATx.....S_..U.....0.'t.....IEND.B`.

Chrome Cache Entry: 90	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (930), with no line terminators
Category:	downloaded
Size (bytes):	930
Entropy (8bit):	5.12292712843304
Encrypted:	false
SSDEEP:	24:0jHQfOuH41YiLY3WL3QquM32EhEcx+Ps2P2pCgrsLHOII:0EJpNqycBxWACgrsDOt
MD5:	06BFCD88AF438673A8BF9B845A11AA6E
SHA1:	D024A745032CBE115526ABE648D9FA0F0A10A681
SHA-256:	947AC0903521F5ECEEFC90637C066306A8CA67466CCC188BB0107FB7CFB532D1
SHA-512:	6A37EA27F3AD16DE6BCB4C386D9F09962902AE2F2FDF76B6723CFF8155CD0B9D4504D1EA6ED3C4D5C9D49BE9C636EB9386BB13C9A787A71F02640A8EC939D80
Malicious:	false
Reputation:	low
URL:	http://https://m.stripe.network/inner.html

Preview:	<!doctype html><html><head><meta charset="utf-8"><title>StripeM-Inner</title></head><body><script>!function(){var e=document.createElement("script");e.defer=!0,e.src="out-4.5.43.js",e.onload=function(){var e;window.StripeM&&(e=window.location.hash,/ping=false/.test(e)||(e=(e=e.match(/version=(4|6)/))?e[1]:"4",window.StripeM.p({t:!0,v:e}))},e=function(e){if(window.opener||window.parent||window)try{var i=((t=JSON.parse(e.data)).message||t).action,t=t.message?t.message.payload:t;switch(i){case"ping":window.StripeM.p({t:!0,o:{muid:t.muid,sid:t.sid,referrer:t.referrer,url:t.url,title:t.title,v2:t.v2},v:t.version||"4"});break;case"track":if(!t.source||!t.data)return;window.StripeM.b({muid:t.muid,sid:t.sid,url:t.url,source:t.source,data:t.data},t.version||"4")}}catch(e){}},window.addEventListener?window.addEventListener("message",e,!1):window.attachEvent("onMessage",e))},document.body.appendChild(e)}()</script></body></html>

Chrome Cache Entry: 91

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1572)
Category:	downloaded
Size (bytes):	17451
Entropy (8bit):	5.358172817248659
Encrypted:	false
SSDEEP:	192:f/Pz+qSc6uy9rbqGIwYGV1pi/KWbqXV6uyErbqGIwYjc1Yk/MoBqNf6uyCrbqGIN:nb8q9DaHq904Zq9r
MD5:	431D9EF3CD1EBE80081AD636F9737911
SHA1:	50E55E699B03E38362A308FB73B55D7EEC741DB8
SHA-256:	5489D34C6FAF46A989BE459CC0A3A28BE86FB219AEF6750C69D1410DDB9FE7AC
SHA-512:	65560DF0E5C71B2E4FECA69D2CFC0C2B0BD5E9068B7BCE74002D66FBA498AC81DE0330A044AAEE0C21A38166A83AD44E32BA38682133C2BBE1807A96AC9C69C7
Malicious:	false
Reputation:	low
URL:	http://https://fonts.googleapis.com/css2?family=Open+Sans:wght@300;400;600&display=swap
Preview:	/* cyrillic-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. font-stretch: 100%;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v40/memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTSKmu1aB.woff2) format('woff2');. unicode-range: U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;.}./* cyrillic */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. font-stretch: 100%;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v40/memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTSumu1aB.woff2) format('woff2');. unicode-range: U+0301, U+0400-045F, U+0490-0491, U+04B0-04B1, U+2116;.}./* greek-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. font-stretch: 100%;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v40/memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTSOmu1aB.woff2) format('woff2');. unicode-range: U+1F00-1FFF;.}./* greek

Chrome Cache Entry: 92

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	711
Entropy (8bit):	5.148910519181866
Encrypted:	false
SSDEEP:	12:trz9k41+WEgs9jrL1ufWjjhKPw6wPUCIUfezqLti5LSdEupOF:t/9k41YnjhKPFwsgfMvLTupQ
MD5:	C76E793FF15BBB2D2722E3F457DE7605
SHA1:	29D5F44485C0021066A305CF7D4C8C0A02166D0C
SHA-256:	78972E26A47CE2F3FE151170B4E1270DEBCC9FEC0D1E56F88F3898F77C905405
SHA-512:	35FC7B9A32A481B464B71CDD30EA593616D9AFD11F9B3ADE50AF176E37DC7B350271F97718E3DB21914A462A5C7CE6BB76112CDD5C1AFDF74BCF93A83C50281
Malicious:	false
Reputation:	low
Preview:	<svg width="115px" height="115px" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 100 100" preserveAspectRatio="xMidYMid" class="lds-dual-ring" style="background: none;"><circle cx="50" cy="50" ng-attr-r="{{config.radius}}" ng-attr-stroke-width="{{config.width}}" ng-attr-stroke="{{config.stroke}}" ng-attr-stroke-dasharray="{{config.dasharray}}" fill="none" stroke-linecap="round" r="40" stroke-width="4" stroke="#c2c2c2" stroke-dasharray="62.83185307179586 62.83185307179586" transform="rotate(166.292 50 50)"><animateTransform attributeName="transform" type="rotate" calcMode="linear" values="0 50 50;360 50 50" keyTimes="0;1" dur="1s" begin="0s" repeatCount="indefinite"></animateTransform></circle></svg>

Chrome Cache Entry: 93

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 1 icon, -128x-128, 32 bits/pixel
Category:	downloaded
Size (bytes):	69694
Entropy (8bit):	6.0166748491726025
Encrypted:	false
SSDEEP:	768:82MlSe1oXPzHhrocJm231dfLxSMO88888888888808IxgrgY5sm0Tr:85lloXrH+gm419kSEgY5smo
MD5:	471B468AABE292CD2099B2E04047527A
SHA1:	038BF470AD04E7BCBE7FC58B3ADBC221A0021E0E
SHA-256:	63C8B75B2DBF22560921E6239030D7132AD5A3D15F051D10A378EA79E8420C75

SHA-512:	32F4090A28739ED0BCCCD7BE1B31AFCF31E52686B1C4096CF0B7FE53DDBC4C0E996EAF108FAE598835807D14C8E824F8619C09B8B8CC796586A58F9EFBB7E735
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/favicon.ico
Preview:	....(.......(............. ....

Chrome Cache Entry: 94

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (7783)
Category:	dropped
Size (bytes):	2227025
Entropy (8bit):	5.114652635787882
Encrypted:	false
SSDEEP:	6144:hktq7fjfZZU6NvHa61kUyJ8FoyJMOhZfiyJ8dIyJYElR/Tff4NE:R7fR1kUyJ+oyJwyJKIyJ8E
MD5:	E324D23112B7B17FE10CF7D580A3B583
SHA1:	3AB00D67F81D387335B7BD7DCAD9287E822E3284
SHA-256:	BF4E74B73756BA564C47EAA75B3B051EE77C57AEA5C40BE64CE2AC863AAC706F
SHA-512:	11F84FA39167D93D9B2561487F95F23474196824BFB71E958A0BCB5F55C575A28413E46D787E0249F92F4BB9927626752E41C94DCE9F25F9E35DEBEDD352851C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html. class="MktRoot". lang="en-US". data-js-controller="Page". data-page-id="Home". data-page-title="Stripe | Financial Infrastructure for the Internet". data-experiments-loading. data-loading.>. <head>. <script>window.__capturedErrors = [];.window.onerror = function (message, url, line, column, error) { __capturedErrors.push(error); };.window.onunhandledrejection = function(evt) { __capturedErrors.push(evt.reason); }.</script>.<meta. name="sentry-config". data-js-dsn="https://7cd38b0eb2b348b39a6002cc768f91c7@errors.stripe.com/376". data-js-release="85bcb45cbc6d5e8e4bda5bbdee7b072765c69279". data-js-environment="production". data-js-project="mkt".>.. <meta name="experiment-treatments" content="wpp_site_header_solutions_nav_redesign.control.ursula.aeae0952-35f0-4b1d-8bb3-ff7f407ab1f7,wpp_globalized_aa_homepage.control.ursula.2f125cad-d5d0-41f0-a10a-6aea426908ea">.. . .. <template class="TrackingSandboxTemplate">. <iframe . class="Tracking

Chrome Cache Entry: 95

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 15552, version 1.0
Category:	downloaded
Size (bytes):	15552
Entropy (8bit):	7.983966851275127
Encrypted:	false
SSDEEP:	384:HDKhlQ8AGL0dgUoEGBQTc7r6QYMkyr/iobA2E4/jKcJZI7lhzi:jslQ+LhUoTB0Qr6Qjkg/DmcJufzi
MD5:	285467176F7FE6BB6A9C6873B3DAD2CC
SHA1:	EA04E4FF5142DDD69307C183DEF721A160E0A64E
SHA-256:	5A8C1E7681318CAA29E9F44E8A6E271F6A4067A2703E9916DFD4FE9099241DB7
SHA-512:	5F9BB763406EA8CE978EC675BD51A0263E9547021EA71188DBD62F0212EB00C1421B750D3B94550B50425BEBFF5F881C41299F6A33BBFA12FB1FF18C12BC7FF1
Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Preview:	wOF2......<...........<Z.........................d..z..J.`..L.\..<.....<.....^...x.6.$..6. .... ..S..}%.......\|....x..[j.E...d..-A...]=sjf$X.o.5......V....i?}.\...;...V......5..mO=,[.B..d'..=..M...q...8..U'..N..G...[..8....Jp..xP...'.?....}.-.1F.C.....%z..#...Q...~.~..3............r.Xk..v.*.7t.+bw...f..b...q.W..'E.....O..a..HI.....Y.B..i.K.0.:.d.E.Lw....Q..~.6.}B...bT.F.,<./....Qu....|...H....Fk.*-..H..p4.$......{.2.....".T'..........Va.6+.9uv....RW..U$8...p...........H5...B..N..V...{.1....5}p.q6..T...U.P.N...U...!.w..?..mI..8q.}.... >.Z.K.....tq..}.><Ok..w.. ..v....W...{....o...."+#+,..vdt...p.WKK:.p1...3`. 3.......Q.].V.$}.......:.S..bb!I...c.of.2uq.n.MaJ..Cf.......w.$.9C...sj.=...=.Z7...h.w M.D..A.t.....]..GVpL...U(.+.)m..e)..H.}i.o.L...S.r..m..Ko....i..M..J..84.=............S..@......Z.V.E..b...0.....@h>...."$.?....../..?.....?.J.a,..|..d...|`.m5..b..LWc...L...?.G.].i...Q..1.:..LJV.J...bU.2.:\.kt.......t.....k....B..i.z+...........A.....

Chrome Cache Entry: 96

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	11621
Entropy (8bit):	4.90064070134424
Encrypted:	false
SSDEEP:	96:4/hgUYVT8gB5QSqglyvIv0MzkRTz44iC5xfQHwEbcu+Lpit+DskAMfu:yhgUYvcKlQHMzGTz4vGJRaV+Lk+xu
MD5:	DB59DE965782B8266BAE6AA3CE5E6E80

SHA1:	3D2FA1A9924C3562A2A802E147A587B3395893C1
SHA-256:	89470495B29CDA5097D336FF1E2C9CA97D0AA0B6CFD92B27F0A066CE981D5CF1
SHA-512:	465D77DE69EB4806DEB24A606B6B9E39B572E9C74CCF42E1F825FEAF7C5E5E98A47D3863413F684BC4B823D752DC3AD62A0C814CABCAB348E318867FA9C5AC48
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/mt-top.html
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html>.<head>. <meta http-equiv="Content-Type" content="text/html" />..<title>Webmail - Powered By Mail::Toaster</title>..<meta name="author" content="Matt Simerson" />..<link rel="stylesheet" href="mt-style.css" type="text/css" media="screen" />..<script src="mt-script.js" type="text/javascript"></script> .. Date: 2006-08-12 -->.</head>..<body onload="read_auth_settings_from_cookies(false)">.. . .. . webmail ....administration... ....statistics.. ....<a onclick="sele

Chrome Cache Entry: 97

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32049)
Category:	downloaded
Size (bytes):	63648
Entropy (8bit):	5.209275328602241
Encrypted:	false
SSDEEP:	768:xXWMhyM9qJLt9EE0+JV6tJJTkMn/OF9DXUGJWsAzO0lBx4d1gtDmmncIZU7Z4iYK:xBKJV6r+Mn/OF9DnAh4d1gAmX7E
MD5:	485EE9AC8DFD187450A11D72913E110A
SHA1:	BCA775A5BDDB98A209058E772AF158BE1AB99AF6
SHA-256:	D10D75C9839BF3A1902D17ED377B3A4595BB84B056E0F3033DD023B796135B18
SHA-512:	4D9C86976B4FB3C69D324E12B6E5498A18791A5C44CF10A03F17D4CF9318293B396529CEF88681B634BDCB6E59E5404319EA67E611F5B58CF346085B40FD1397
Malicious:	false
Reputation:	low
URL:	http://https://www.theartfarm.com/templates/orderforms/standard_cart/js/scripts.min.js?v=0d4099
Preview:	function scrollToGatewayInputError(){var e=jQuery(".gateway-errors,.assisted-cc-input-feedback").first(),t=e.closest("form");t||(t=jQuery("form").first()),t.find('button[type="submit"],input[type="submit"]').prop("disabled",!1).removeClass("disabled").find("i.fas,i.far,i.fal,i.fab").removeAttr("class").addClass("fas fa-arrow-circle-right").find("span").toggle(),e.length&&elementOutOfViewPort(e[0])&&jQuery("html, body").animate({scrollTop:e.offset().top-50},500)}function elementOutOfViewPort(e){var t=e.getBoundingClientRect(),n={};return n.top=t.top<0,n.left=t.left<0,n.bottom=t.bottom>(window.innerHeight||document.documentElement.clientHeight),n.right=t.right>(window.innerWidth||document.documentElement.clientWidth),n.any=n.top||n.left||n.bottom||n.right,n.any}function validateCheckoutCreditCardInput(e){var t=jQuery('input[name="ccinfo"]:checked').val(),n=checkoutForm.find('*[type="submit"]'),i=null,a=!0,r=checkoutForm.find('input[name="paymentmethod"]:checked'),o=r.hasClass("is-credit-

Chrome Cache Entry: 98

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	519
Entropy (8bit):	4.536758771950739
Encrypted:	false
SSDEEP:	12:t9Afm3vqCOnftAJHOhKCxzw5NW6duZ4FlrGwdpwk8zqAKcdM7J5:t9AfWAnSNCxKNxuZDqwwvxc
MD5:	C6B234719965CC10DF0F8D12C1F438DD
SHA1:	386F533083A450BB34F87DAB852E495195A7FDDB
SHA-256:	686D81E030899B477865D67A01FE34E83D8E68AA8DA91A59205AD3E901A3EC71
SHA-512:	F5902DED64A6ECE6015686924BBC6796AF1FE50B527A40B920B45D499DA2EDBDAEF5B2A87C56CB61A89CD174876F64790AF18B9BD1C838D285FD62B20FCDCD2
Malicious:	false
Reputation:	low
Preview:	<svg height="1024" width="896" xmlns="http://www.w3.org/2000/svg">. <path d="M128 768h256v64H128v-64z m320-384H128v64h320v-64z m128 192V448L384 640l192 192V704h320V576H576z m-288-64H128v64h160v-64zM128 704h160v-64H128v64z m576 64h64v128c-1 18-7 33-19 45s-27 18-45 19H64c-35 0-64-29-64-64V192c0-35 29-64 64-64h192C256 57 313 0 384 0s128 57 128 128h192c35 0 64 29 64 64v320h-64V320H64v576h640V768zM128 256h512c0-35-29-64-64-64h-64c-35 0-64-29-64-64s-29-64-64-64-64 29-64 64-29 64-64 64h-64c-35 0-64 29-64 64z" />.</svg>.

Chrome Cache Entry: 99

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 100 x 100, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	163
Entropy (8bit):	5.025279476306441

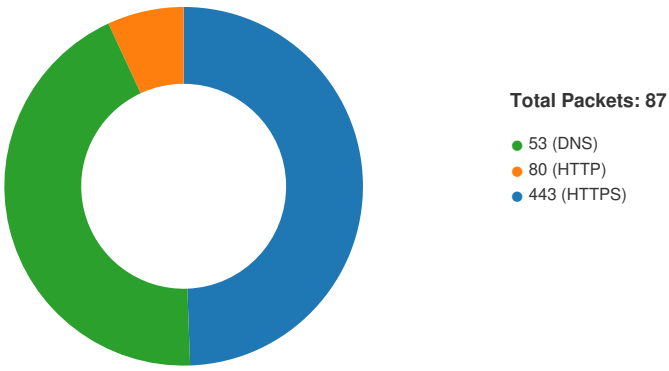
Encrypted:	false
SSDEEP:	3:yionv//thPlpbtqrK9Ag9RthwkBDsTBZtjjmpS/AID+/qkltmfwk/t6S/ljp:6v/lhPt9AgjnDspjypiAU1tLsTtjp
MD5:	72B020240027209A169A7008BAE0084E
SHA1:	C5D5807AF53A4689971A46B363C642BD55613071
SHA-256:	938565F22323C33D0C80745EDFB364D38A445F6E51C1FEF7961AAF269F897170
SHA-512:	E676CF68332A2929137851F3D50539DFD544BDE2944F15EC1E2487E9FE2A563029A08021BC2C547F608A70A8196E958D16B08BFC9D9D91E2526562D0B66C86BE
Malicious:	false
Reputation:	low
URL:	http://https://aerosol.bumkins.com/images/mt_background.png
Preview:	.PNG.....IHDR...d...d.....G<ef....gAMA.....OX2....tEXtSoftware.Adobe ImageReadyq.e<....PLTE...../.....#IDATx.....S_..U.....0.'t.....IEND.B`.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2024 05:54:20.562169075 CET	443	49737	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.562200069 CET	443	49737	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.562268019 CET	443	49737	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.562542915 CET	49737	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.562881947 CET	49737	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.562881947 CET	49737	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.562944889 CET	443	49737	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.562978983 CET	443	49737	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.584393024 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.584472895 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.584671021 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.584737062 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.584754944 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.876627922 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.877226114 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.877300978 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.877773046 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:20.877773046 CET	49738	443	192.168.2.4	20.190.151.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2024 05:54:20.877790928 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:20.877826929 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:21.082777977 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:21.082807064 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:21.082901955 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:21.083127022 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:21.083420992 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:21.083421946 CET	49738	443	192.168.2.4	20.190.151.9
Feb 23, 2024 05:54:21.083483934 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:21.083520889 CET	443	49738	20.190.151.9	192.168.2.4
Feb 23, 2024 05:54:22.342637062 CET	49675	443	192.168.2.4	173.222.162.32
Feb 23, 2024 05:54:30.974932909 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:30.974972963 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:30.975080967 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:30.975245953 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:30.975274086 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:30.976443052 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:30.976521969 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:30.976593971 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:30.976747036 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:30.976771116 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.205449104 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.205641031 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.205657959 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.206195116 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.206268072 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.207602024 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.207655907 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.208565950 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.208648920 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.208770990 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.208786964 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.210609913 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.210867882 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.210927010 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.212379932 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.212454081 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.213350058 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.213440895 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.213546991 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.213563919 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.357321978 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.357425928 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.416358948 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.416695118 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.417222977 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.417263985 CET	49741	443	192.168.2.4	142.250.80.78
Feb 23, 2024 05:54:31.417284012 CET	443	49741	142.250.80.78	192.168.2.4
Feb 23, 2024 05:54:31.449747086 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.450082064 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.450375080 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.451004028 CET	49742	443	192.168.2.4	172.253.122.84
Feb 23, 2024 05:54:31.451062918 CET	443	49742	172.253.122.84	192.168.2.4
Feb 23, 2024 05:54:31.982043028 CET	49675	443	192.168.2.4	173.222.162.32
Feb 23, 2024 05:54:32.766666889 CET	49745	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:32.767498016 CET	49746	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:32.921514988 CET	80	49745	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:32.921751976 CET	49745	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:32.922188044 CET	80	49746	162.213.38.147	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2024 05:54:32.922282934 CET	49746	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.077332020 CET	80	49745	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:33.077389002 CET	80	49746	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:33.077502012 CET	49746	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.232933998 CET	80	49746	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:33.280445099 CET	49746	80	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.329020023 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.329107046 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:33.329227924 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.329653978 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:33.329735041 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.279867887 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.311377048 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:34.311409950 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.315351963 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.315443039 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:34.372318983 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:34.372824907 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.374207973 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:34.374253988 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.419626951 CET	49749	443	192.168.2.4	162.213.38.147
Feb 23, 2024 05:54:34.530177116 CET	443	49749	162.213.38.147	192.168.2.4
Feb 23, 2024 05:54:34.530267954 CET	443	49749	162.213.38.147	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2024 05:54:30.885962009 CET	64111	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:30.886353970 CET	58701	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:30.887478113 CET	61956	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:30.887888908 CET	63839	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:30.951118946 CET	53	57695	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:30.974265099 CET	53	58701	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:30.974325895 CET	53	64111	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:30.975244999 CET	53	61956	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:30.975959063 CET	53	63839	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:31.556786060 CET	53	53476	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:32.656754971 CET	51811	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:32.657004118 CET	51160	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:32.746437073 CET	53	51811	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:32.878684998 CET	53	51160	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:33.237411976 CET	62106	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:33.237550020 CET	49717	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:33.327569962 CET	53	62106	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:33.328260899 CET	53	49717	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:34.798592091 CET	55332	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:34.799572945 CET	50780	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:34.887330055 CET	53	55332	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:34.887558937 CET	53	50780	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:37.519253969 CET	53	57793	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:38.353436947 CET	51486	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:38.354151011 CET	62973	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:38.444897890 CET	53	62973	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:38.508033037 CET	53	51486	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:48.696386099 CET	53	59588	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:50.581373930 CET	138	138	192.168.2.4	192.168.2.255
Feb 23, 2024 05:54:53.159852028 CET	55340	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:53.160336018 CET	60705	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:53.507288933 CET	53	55340	1.1.1.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2024 05:54:54.108833075 CET	53	60705	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:54.224303007 CET	59628	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:54.224641085 CET	60653	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:54:54.313829899 CET	53	59628	1.1.1.1	192.168.2.4
Feb 23, 2024 05:54:54.645407915 CET	53	60653	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:03.162518024 CET	65523	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:03.162959099 CET	54871	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:03.316766977 CET	53	54871	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:03.399532080 CET	53	65523	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:03.695652962 CET	65004	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:03.695991993 CET	59646	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:03.784866095 CET	53	65004	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:03.872222900 CET	53	59646	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:05.310141087 CET	53	49602	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:05.980782032 CET	53	52644	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:06.891930103 CET	59661	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:06.892399073 CET	63050	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:06.979775906 CET	53	59661	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:06.980357885 CET	53	63050	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:06.987190962 CET	53	53261	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:06.994777918 CET	60308	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:06.995131969 CET	57108	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:07.201937914 CET	53	60308	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:07.715423107 CET	53	65194	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:07.760278940 CET	53	55639	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:07.895643950 CET	53	57108	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:08.690291882 CET	49214	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:08.690618038 CET	54937	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:08.778561115 CET	53	49214	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:08.778611898 CET	53	54937	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:09.315933943 CET	53	60780	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:10.681261063 CET	53	52903	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:11.700097084 CET	53	54989	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:28.503551960 CET	51987	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:28.504036903 CET	54704	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:28.592581987 CET	53	51987	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:28.593018055 CET	53	54704	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:29.850594997 CET	57770	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:29.850996017 CET	62033	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:29.938750029 CET	53	57770	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:29.939661980 CET	53	62033	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:30.260411978 CET	53	53977	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:30.714510918 CET	62718	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:30.714874983 CET	61577	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:30.802886963 CET	53	61577	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:30.803596020 CET	53	62718	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:30.868151903 CET	53	56488	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:33.334405899 CET	56720	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:33.334877014 CET	52660	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:33.426104069 CET	53	52660	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:33.426134109 CET	53	56720	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:34.337451935 CET	52647	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:34.337994099 CET	63519	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:34.426784039 CET	53	52647	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:34.427440882 CET	53	63519	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:35.540636063 CET	62608	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:35.541151047 CET	56818	53	192.168.2.4	1.1.1.1
Feb 23, 2024 05:55:35.628568888 CET	53	62608	1.1.1.1	192.168.2.4
Feb 23, 2024 05:55:35.629774094 CET	53	56818	1.1.1.1	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 23, 2024 05:54:32.878870010 CET	192.168.2.4	1.1.1.1	c223	(Port unreachable)	Destination Unreachable
Feb 23, 2024 05:54:54.108954906 CET	192.168.2.4	1.1.1.1	c225	(Port unreachable)	Destination Unreachable
Feb 23, 2024 05:54:54.645567894 CET	192.168.2.4	1.1.1.1	c225	(Port unreachable)	Destination Unreachable
Feb 23, 2024 05:55:03.872369051 CET	192.168.2.4	1.1.1.1	c21b	(Port unreachable)	Destination Unreachable
Feb 23, 2024 05:55:07.900435925 CET	192.168.2.4	1.1.1.1	c21b	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 23, 2024 05:54:30.885962009 CET	192.168.2.4	1.1.1.1	0xead5	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:30.886353970 CET	192.168.2.4	1.1.1.1	0xd912	Standard query (0)	clients2.google.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:30.887478113 CET	192.168.2.4	1.1.1.1	0xe873	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:30.887888908 CET	192.168.2.4	1.1.1.1	0x3a64	Standard query (0)	accounts.google.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:32.656754971 CET	192.168.2.4	1.1.1.1	0x9169	Standard query (0)	aerosol.bumkins.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:32.657004118 CET	192.168.2.4	1.1.1.1	0x21d6	Standard query (0)	aerosol.bumkins.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:33.237411976 CET	192.168.2.4	1.1.1.1	0x658c	Standard query (0)	aerosol.bumkins.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:33.237550020 CET	192.168.2.4	1.1.1.1	0xe16c	Standard query (0)	aerosol.bumkins.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:34.798592091 CET	192.168.2.4	1.1.1.1	0x78cc	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:34.799572945 CET	192.168.2.4	1.1.1.1	0x2a4d	Standard query (0)	www.google.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:38.353436947 CET	192.168.2.4	1.1.1.1	0x7eba	Standard query (0)	aerosol.bumkins.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:38.354151011 CET	192.168.2.4	1.1.1.1	0x50	Standard query (0)	aerosol.bumkins.com	65	IN (0x0001)	false
Feb 23, 2024 05:54:53.159852028 CET	192.168.2.4	1.1.1.1	0xe696	Standard query (0)	mail-toaster.org	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:53.160336018 CET	192.168.2.4	1.1.1.1	0x4ef6	Standard query (0)	mail-toaster.org	65	IN (0x0001)	false
Feb 23, 2024 05:54:54.224303007 CET	192.168.2.4	1.1.1.1	0xc44	Standard query (0)	mail-toaster.org	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:54.224641085 CET	192.168.2.4	1.1.1.1	0x4340	Standard query (0)	mail-toaster.org	65	IN (0x0001)	false
Feb 23, 2024 05:55:03.162518024 CET	192.168.2.4	1.1.1.1	0xc109	Standard query (0)	www.theartfarm.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:03.162959099 CET	192.168.2.4	1.1.1.1	0x1860	Standard query (0)	www.theartfarm.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:03.695652962 CET	192.168.2.4	1.1.1.1	0x7f71	Standard query (0)	www.theartfarm.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:03.695991993 CET	192.168.2.4	1.1.1.1	0xdd1e	Standard query (0)	www.theartfarm.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:06.891930103 CET	192.168.2.4	1.1.1.1	0x8ab6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:06.892399073 CET	192.168.2.4	1.1.1.1	0x8f22	Standard query (0)	www.google.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:06.994777918 CET	192.168.2.4	1.1.1.1	0x183c	Standard query (0)	www.theartfarm.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:06.995131969 CET	192.168.2.4	1.1.1.1	0x24b2	Standard query (0)	www.theartfarm.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:08.690291882 CET	192.168.2.4	1.1.1.1	0x8936	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:08.690618038 CET	192.168.2.4	1.1.1.1	0x375d	Standard query (0)	www.google.com	65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 23, 2024 05:55:28.503551960 CET	192.168.2.4	1.1.1.1	0x4e9d	Standard query (0)	js.stripe.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:28.504036903 CET	192.168.2.4	1.1.1.1	0x1ae0	Standard query (0)	js.stripe.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:29.850594997 CET	192.168.2.4	1.1.1.1	0xe72b	Standard query (0)	js.stripe.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:29.850996017 CET	192.168.2.4	1.1.1.1	0x7ecc	Standard query (0)	js.stripe.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:30.714510918 CET	192.168.2.4	1.1.1.1	0x7f4d	Standard query (0)	m.stripe.network	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:30.714874983 CET	192.168.2.4	1.1.1.1	0x48ef	Standard query (0)	m.stripe.network	65	IN (0x0001)	false
Feb 23, 2024 05:55:33.334405899 CET	192.168.2.4	1.1.1.1	0x632	Standard query (0)	m.stripe.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.334877014 CET	192.168.2.4	1.1.1.1	0xfadd	Standard query (0)	m.stripe.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:34.337451935 CET	192.168.2.4	1.1.1.1	0x1358	Standard query (0)	m.stripe.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.337994099 CET	192.168.2.4	1.1.1.1	0x45a8	Standard query (0)	m.stripe.com	65	IN (0x0001)	false
Feb 23, 2024 05:55:35.540636063 CET	192.168.2.4	1.1.1.1	0x86ed	Standard query (0)	stripe.com	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:35.541151047 CET	192.168.2.4	1.1.1.1	0x9de8	Standard query (0)	stripe.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 23, 2024 05:54:30.974265099 CET	1.1.1.1	192.168.2.4	0xd912	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:54:30.974325895 CET	1.1.1.1	192.168.2.4	0xead5	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:54:30.974325895 CET	1.1.1.1	192.168.2.4	0xead5	No error (0)	clients.l.google.com		142.250.80.78	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:30.975244999 CET	1.1.1.1	192.168.2.4	0xe873	No error (0)	accounts.google.com		172.253.122.84	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:32.746437073 CET	1.1.1.1	192.168.2.4	0x9169	No error (0)	aerosol.bumkins.com		162.213.38.147	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:33.327569962 CET	1.1.1.1	192.168.2.4	0x658c	No error (0)	aerosol.bumkins.com		162.213.38.147	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:34.887330055 CET	1.1.1.1	192.168.2.4	0x78cc	No error (0)	www.google.com		142.251.35.164	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:34.887558937 CET	1.1.1.1	192.168.2.4	0x2a4d	No error (0)	www.google.com			65	IN (0x0001)	false
Feb 23, 2024 05:54:38.508033037 CET	1.1.1.1	192.168.2.4	0x7eba	No error (0)	aerosol.bumkins.com		162.213.38.147	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:53.507288933 CET	1.1.1.1	192.168.2.4	0xe696	No error (0)	mail-toaster.org		66.128.51.170	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:54:54.313829899 CET	1.1.1.1	192.168.2.4	0xc44	No error (0)	mail-toaster.org		66.128.51.170	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:03.399532080 CET	1.1.1.1	192.168.2.4	0xc109	No error (0)	www.theartfarm.com		66.128.51.172	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:03.784866095 CET	1.1.1.1	192.168.2.4	0x7f71	No error (0)	www.theartfarm.com		66.128.51.172	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:06.979775906 CET	1.1.1.1	192.168.2.4	0x8ab6	No error (0)	www.google.com		142.251.40.228	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 23, 2024 05:55:06.980357885 CET	1.1.1.1	192.168.2.4	0x8f22	No error (0)	www.google.com			65	IN (0x0001)	false
Feb 23, 2024 05:55:07.201937914 CET	1.1.1.1	192.168.2.4	0x183c	No error (0)	www.theartfarm.com		66.128.51.172	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:08.778561115 CET	1.1.1.1	192.168.2.4	0x8936	No error (0)	www.google.com		142.250.80.68	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:08.778611898 CET	1.1.1.1	192.168.2.4	0x375d	No error (0)	www.google.com			65	IN (0x0001)	false
Feb 23, 2024 05:55:28.592581987 CET	1.1.1.1	192.168.2.4	0x4e9d	No error (0)	js.stripe.com	stripecdn.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:28.592581987 CET	1.1.1.1	192.168.2.4	0x4e9d	No error (0)	stripecdn.map.fastly.net		151.101.0.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:28.592581987 CET	1.1.1.1	192.168.2.4	0x4e9d	No error (0)	stripecdn.map.fastly.net		151.101.128.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:28.592581987 CET	1.1.1.1	192.168.2.4	0x4e9d	No error (0)	stripecdn.map.fastly.net		151.101.64.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:28.592581987 CET	1.1.1.1	192.168.2.4	0x4e9d	No error (0)	stripecdn.map.fastly.net		151.101.192.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:28.593018055 CET	1.1.1.1	192.168.2.4	0x1ae0	No error (0)	js.stripe.com	dexeqbeb7giwr.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:29.938750029 CET	1.1.1.1	192.168.2.4	0xe72b	No error (0)	js.stripe.com	stripecdn.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:29.938750029 CET	1.1.1.1	192.168.2.4	0xe72b	No error (0)	stripecdn.map.fastly.net		151.101.128.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:29.938750029 CET	1.1.1.1	192.168.2.4	0xe72b	No error (0)	stripecdn.map.fastly.net		151.101.0.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:29.938750029 CET	1.1.1.1	192.168.2.4	0xe72b	No error (0)	stripecdn.map.fastly.net		151.101.192.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:29.938750029 CET	1.1.1.1	192.168.2.4	0xe72b	No error (0)	stripecdn.map.fastly.net		151.101.64.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:29.939661980 CET	1.1.1.1	192.168.2.4	0x7ecc	No error (0)	js.stripe.com	stripecdn.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:30.802886963 CET	1.1.1.1	192.168.2.4	0x48ef	No error (0)	m.stripe.network	d1tcqh4bio8cty.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:30.803596020 CET	1.1.1.1	192.168.2.4	0x7f4d	No error (0)	m.stripe.network	stripecdn.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 23, 2024 05:55:30.803596020 CET	1.1.1.1	192.168.2.4	0x7f4d	No error (0)	stripecdn.map.fastly.net		151.101.192.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:30.803596020 CET	1.1.1.1	192.168.2.4	0x7f4d	No error (0)	stripecdn.map.fastly.net		151.101.0.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:30.803596020 CET	1.1.1.1	192.168.2.4	0x7f4d	No error (0)	stripecdn.map.fastly.net		151.101.64.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:30.803596020 CET	1.1.1.1	192.168.2.4	0x7f4d	No error (0)	stripecdn.map.fastly.net		151.101.128.176	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		34.212.84.166	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		52.10.34.124	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		44.238.48.240	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		35.160.61.92	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		44.240.235.135	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		34.211.107.203	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		54.202.109.213	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:33.426134109 CET	1.1.1.1	192.168.2.4	0x632	No error (0)	m.stripe.com		44.237.70.166	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		44.240.51.134	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		50.112.176.46	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		35.82.187.64	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		34.211.107.203	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		34.213.123.46	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		44.240.111.178	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		44.237.70.166	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:34.426784039 CET	1.1.1.1	192.168.2.4	0x1358	No error (0)	m.stripe.com		34.212.84.166	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:35.628568888 CET	1.1.1.1	192.168.2.4	0x86ed	No error (0)	stripe.com		54.186.23.98	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:35.628568888 CET	1.1.1.1	192.168.2.4	0x86ed	No error (0)	stripe.com		54.187.159.182	A (IP address)	IN (0x0001)	false
Feb 23, 2024 05:55:35.628568888 CET	1.1.1.1	192.168.2.4	0x86ed	No error (0)	stripe.com		54.187.119.242	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- login.live.com
- clients2.google.com
- accounts.google.com
- aerosol.bumkins.com
- https:
  - mail-toaster.org
  - www.theartfarm.com
  - www.google.com
  - js.stripe.com
  - m.stripe.network
  - m.stripe.com
- fs.microsoft.com
- stripe.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: **4900**, Parent PID: **3748**

General

Target ID:	0
Start time:	05:54:24
Start date:	23/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: chrome.exe PID: **3720**, Parent PID: **4900**

General

Target ID:	2
Start time:	05:54:28
Start date:	23/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2348 --field-trial-handle=2284,i,10209318467324837293,7950406128623755245,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6468**, Parent PID: **3748**

General

Target ID:	3
Start time:	05:54:31
Start date:	23/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://aerosol.bumkins.com/
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly