ID: 715097
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 16:18:15
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

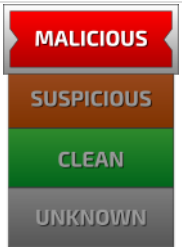
http://www.optimumsource.net

Overview

General Information

Sample URL:	http://www.optimumsource.net
Analysis ID:	715097
Infos:	

Detection

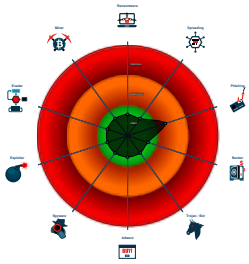


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 3088 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://www.optimumsource.net/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2312 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=2044 --field-trial-handle=1740,i,12436308146909054526,16182453480135305632,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN TA569 Domain in DNS Lookup (skambio-porte .com) - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1

Timestamp:	192.168.2.31.1.1.163979532039030 10/03/22-16:18:46.390588
SID:	2039030
Source Port:	63979
Destination Port:	53

Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN TA569 Domain in DNS Lookup (skambio-porte .com) - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1	
Timestamp:	192.168.2.31.1.1.149858532039030 10/03/22-16:20:28.061920
SID:	2039030
Source Port:	49858
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking

Snort IDS alert for network traffic

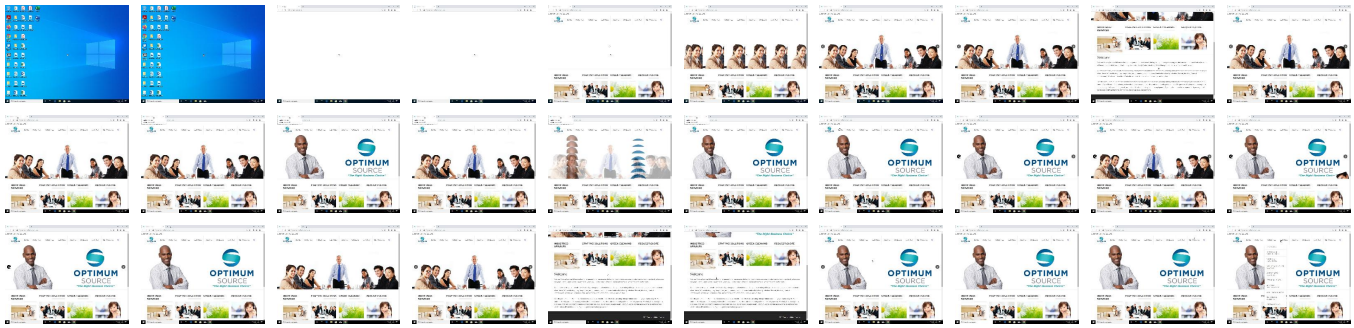
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.optimumsource.net	0%	Avira URL Cloud	safe	
http://www.optimumsource.net	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/large_left.png	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/css/settings.css?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-migrate-3.3.2.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.3dflow-2.0.js?ver=2.0	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-sliderAccess.js?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-3.6.0.min.js?ver=3.6.0	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/shadow2.png	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.transit.min.js?ver=0.9.9	0%	Avira URL Cloud	safe	
http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/12/slider_bg.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/12/home_banner3.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/modules/wip-content-manager/assets/js/content.manager.lib.min.js?ver=1.0	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/timer.png	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/css/font-awesome.min.css?ver=3.2.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/custom-css.php?ver=1648301343&c=1&theme=wip_theme	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/12/home_page_banner2.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/font/fontawesome-webfont.woff?v=3.2.1	0%	Avira URL Cloud	safe	
http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/11/home_bg_section.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/modernizr.custom.js?ver=2.6.2	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/loader.gif	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.6	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/slider.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/base.css?ver=1.0.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/resquestquote_homepage.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/comment-reply.min.js?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.easing.1.3.js?ver=1.3	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.css?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.js?ver=2.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/global.min.js?ver=1.0.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/mouse.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/Optimum-Source-Logo-Web.png	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/style.css?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/hoverIntent.min.js?ver=1.10.2	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/light.css?ver=1.0.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/button.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/js/jquery.themepunch.revolution.min.js?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/css/captions.css?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/industriesserved_homepage.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/reset.css	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/responsive.css?ver=1.0.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.5.6	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/greencleaning_homepage.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/large_right.png	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.isotope.min.js?ver=1.5.25	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/controlgroup.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/jquery/ui/checkboxradio.min.js?ver=1.13.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.optimumsource.net/wp-content/uploads/2013/11/services_homepage.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.js?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-includes/js/wp-emoji-release.min.js?ver=5.9.4	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/wip-megamenu.js?ver=1.1	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/favicon.ico	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/services/	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/Banner-Home2.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/12/slider_bg.jpg	0%	Avira URL Cloud	safe	
http://www.optimumsource.net/wp-content/uploads/2013/11/Business-meeting-Supplier-Management1.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

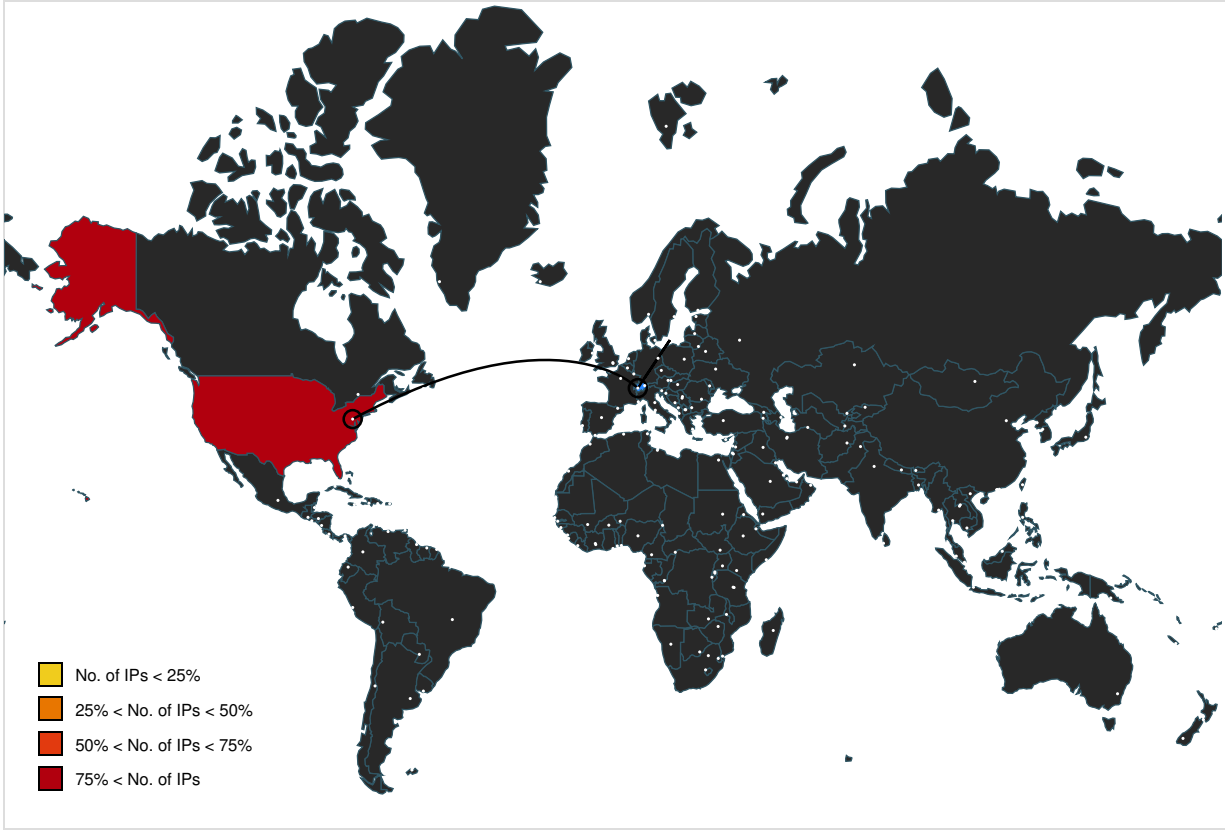
Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.18.13	true	false		high
www.optimumsource.net	160.153.91.65	true	false		unknown
s174710176.onlinehome.us	74.208.236.114	true	false		unknown
www.google.com	142.250.74.196	true	false		high
clients.l.google.com	172.217.18.14	true	false		high
s.w.org	192.0.77.48	true	false		high
skambio-porte.com	91.228.56.183	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.optimumsource.net/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/large_left.png	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-migrate-3.3.2.min.js?ver=3.3.2	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/Banner-Home2.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/css/settings.css?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.3dflow-2.0.js?ver=2.0	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-sliderAccess.js?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-3.6.0.min.js?ver=3.6.0	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/shadow2.png	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.transit.min.js?ver=0.9.9	false	• Avira URL Cloud: safe	unknown
http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/12/slider_bg.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/12/home_banner3.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/modules/wip-content-manager/assets/js/content.manager.lib.min.js?ver=1.0	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/timer.png	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/css/font-awesome.min.css?ver=3.2.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/custom-css.php?ver=1648301343&c=1&theme=wip_theme	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/12/home_page_banner2.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/font/fontawesome-webfont.woff?v=3.2.1	false	• Avira URL Cloud: safe	unknown
http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/11/home_bg_section.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/modernizr.custom.js?ver=2.6.2	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/loader.gif	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.6	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/slider.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/12/slider_bg.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/base.css?ver=1.0.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/	false		unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/resquestquote_homepage.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/comment-reply.min.js?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/clients/	false		unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.easing.1.3.js?ver=1.3	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.css?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.js?ver=2.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/global.min.js?ver=1.0.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/mouse.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/Optimum-Source-Logo-Web.png	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/clients/	false		unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/style.css?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/hoverIntent.min.js?ver=1.10.2	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/css/captions.css?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/	false		unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/button.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/light.css?ver=1.0.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/js/jquery.themepunch.revolution.min.js?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/industriesserved_homepage.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/reset.css	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/responsive.css?ver=1.0.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/Business-meeting-Supplier-Management1.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.5.6	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/greencleaning_homepage.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/large_right.png	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.isotope.min.js?ver=1.5.25	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/controlgroup.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/jquery/ui/checkboxradio.min.js?ver=1.13.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/services_homepage.jpg	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/services/	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.js?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-includes/js/wp-emoji-release.min.js?ver=5.9.4	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/wip-megamenu.js?ver=1.1	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/wp-content/uploads/2013/11/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://www.optimumsource.net/services/	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
142.250.186.170	unknown	United States		15169	GOOGLEUS	false
172.217.18.13	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.18.14	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.18.3	unknown	United States		15169	GOOGLEUS	false
74.208.236.114	s174710176.onlinehome.us	United States		8560	ONEANDONE-ASBrauerstrasse48DE	false
91.228.56.183	skambio-porte.com	unknown		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.186.164	unknown	United States		15169	GOOGLEUS	false
172.217.18.10	unknown	United States		15169	GOOGLEUS	false
160.153.91.65	www.optimumsource.net	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
142.250.186.74	unknown	United States		15169	GOOGLEUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715097
Start date and time:	2022-10-03 16:18:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://www.optimumsource.net
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	12
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@25/0@10/151

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.68, 20.190.159.0, 20.190.159.2, 20.190.159.73, 40.126.31.71, 40.126.31.67, 40.126.31.69, 20.190.159.64, 142.250.186.99, 34.104.35.123, 142.250.186.74, 142.250.74.202, 142.250.186.170, 142.250.185.234, 172.217.18.106, 142.250.185.106, 142.250.184.202, 172.217.18.10, 216.58.212.170, 142.250.181.234, 172.217.16.138, 216.58.212.138, 142.250.184.234, 172.217.16.202, 142.250.185.138, 172.217.23.106, 142.250.186.138, 142.250.185.170
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prda.aadg.msidentity.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, slscr.update.microsoft.com, login.live.com, ajax.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/11/home_bg_section.jpg
- VT rate limit hit for: http://s174710176.onlinehome.us/optimumsource/wp-content/uploads/2013/12/slider_bg.jpg
- VT rate limit hit for: http://www.optimumsource.net/
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-sliderAccess.js?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.css?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/contact-form-7-datepicker/js/jquery-ui-timepicker/jquery-ui-timepicker-addon.min.js?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.6
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.5.6
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-3.6.0.min.js?ver=3.6.0
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/jquery-updater/js/jquery-migrate-3.3.2.min.js?ver=3.3.2
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/large_right.png
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/loader.gif
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/shadow2.png
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/assets/timer.png
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/css/captions.css?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/revslider/rs-plugin/js/jquery.themepunch.revolution.min.js?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.3dflow-2.0.js?ver=2.0
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/idangerous.swiper.js?ver=2.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/plugins/wip-mega-menu/assets/js/wip-megamenu.js?ver=1.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/base.css?ver=1.0.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/css/font-awesome.min.css?ver=3.2.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/font-awesome/font/fontawesome-webfont.woff?v=3.2.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/light.css?ver=1.0.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/reset.css
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/css/responsive.css?ver=1.0.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/global.min.js?ver=1.0.1
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.easing.1.3.js?ver=1.3
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.isotope.min.js?ver=1.5.25
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/jquery.transit.min.js?ver=0.9.9
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/assets/js/modernizr.custom.js?ver=2.6.2
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/custom-css.php?ver=1648301343&c=1&theme=wip_theme
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/modules/wip-content-manager/assets/js/content.manager.lib.min.js?ver=1.0
- VT rate limit hit for: http://www.optimumsource.net/wp-content/themes/pantherhead/style.css?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/Optimum-Source-Logo-Web.png
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/favicon.ico
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/greencleaning_homepage.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/industriesserved_homepage.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/resquestquote_homepage.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/11/services_homepage.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/12/home_banner3.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-content/uploads/2013/12/home_page_banner2.jpg
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/comment-reply.min.js?ver=5.9.4
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/hoverIntent.min.js?ver=1.10.2
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/button.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/checkboxradio.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/controlgroup.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/mouse.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/jquery/ui/slider.min.js?ver=1.13.1
- VT rate limit hit for: http://www.optimumsource.net/wp-includes/js/wp-emoji-release.min.js?ver=5.9.4

Created / dropped Files

No created / dropped files found

Static File Info

No static file info