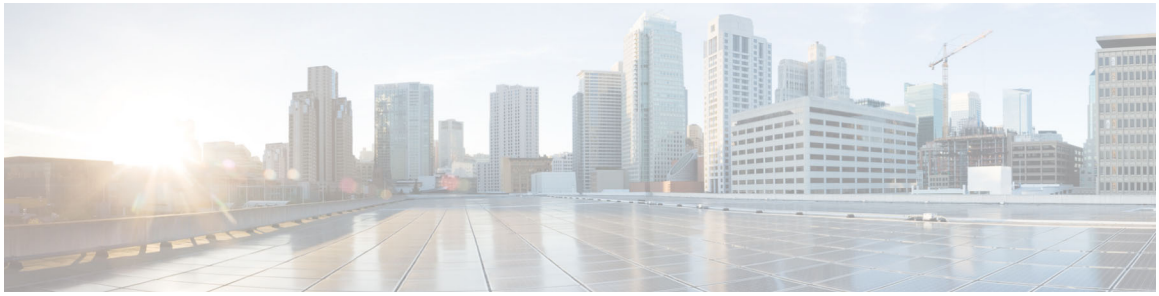

Release Notes for URL Category and Threat Category Updates for Cisco Web and Email Security Appliances

Published Date: May 4, 2017
Last Updated: April 25, 2019

Contents

URL Category Update

Release Date

Release Date: April 3, 2019

Changes

New URL Category added:

- Not Actionable - Sites that have been inspected but are unreachable or do not have enough content to be assigned a category.

The new URL category specified above will now be available while configuring access control by URL category.

Release Date

Release Date: May 8, 2017

Changes

New URL categories added:

- Online Meetings - online meetings, desktop sharing, remote access, and other tools that facilitate multi-location collaboration.
- Paranormal - UFOs, ghosts, cryptid, telekinesis, urban legends, and myths.
- Personal VPN - Virtual Private Network (VPN) sites, or tools that are usually for personal use, which may or may not have been approved for corporate use.
- DIY Projects - guidance and information to create, improve, modify, decorate and repair objects, articles, without the aid of experts or professionals.
- Hunting - professional or sport hunting, gun clubs, and other hunting related sites.
- Military - military, armed forces, military bases, military organizations, anti-terrorism.

This is the only change in this release. The six new URL categories specified above will now be available while configuring access control by URL category.

Threat Category Update

Threat Categories

The available threat categories are:

- Malware Sites - Websites that are known to contain, serve, or support malware in its delivery, propagation, or in carrying out its malicious intent
- Spyware and Adware - Sites that are known to contain, serve, or support Spyware and Adware activities.
- Phishing - Phishing and other fraudulent sites that copy or mimic legitimate sites for the purposes of surreptitiously acquiring sensitive information, such as user names, passwords, credit card numbers, etc, for use in malicious activities.
- Botnets - Known to participate in a Bot network. These include Command and Control (CNC, C2) Servers and sites that deliver or receive data as part of the malicious transaction (bots, zombies).
- Spam - Known to serve, deliver or aide in the propagation of Spam
- Exploits - Sites that are known to host or aide in exploits, drive-by-downloads and other activities that identifies and compromises vulnerable systems.
- Mobile Threats - Threats that are designed to infect or adversely affect mobile devices such as phones and tablets.
- High Risk Sites and Locations - Domains and hostnames that match against the OpenDNS predictive security algorithms from security graph.

- Bogon - Bogons are IP Addresses that are known to belong to reserved IP address spaces that is supposedly unallocated or undelagated. Sites in this category are bogons that are known to be sending traffic.
- Malware Node - Sites that use Peer-to-Peer sharing as a method to carry out malware related activities.
- Ebanking Fraud - Known to engage in fraudulent activities that relate to electronic banking.
- Indicators of Compromise (IOC) - Hosts that have been observed to engage in Indicators of Compromise.
- Domain Generated Algorithm - Domains that are extracted from malware that employ algorithms that generate domains for potential use in future malicious activities such as hosting malware or as an ex-filtration destination.
- Open HTTP Proxy - Hosts that are known to run Open Web Proxies and offer anonymous web browsing services.
- Open Mail Relay - Commonly used by Spam and Phishing attackers, sites in this category are hosts that are known to offer anonymous email relaying services.
- TOR exit Nodes - Hosts known to offer exit node services for the Tor Anonymizer network.
- Potential DNS Rebinding - Public DNS entries that resolve to your network space. These are sometimes associated with DNS rebinding attacks, which allow malicious scripts to access your internal network resources.
- DNS Tunneling - Sites that provide DNS Tunneling as a service. These services can be for PC or mobile and create a VPN connection specifically over DNS to send traffic that may bypass corporate policies and inspection.
- Dynamic DNS - Sites that are hosting dynamic DNS services. Attackers can use this technology as an evasion technique against IP blacklisting.
- Newly Seen Domains - Domains that have recently been registered, or not yet seen via telemetry. The behavior of these URLs has not been observed enough to establish the appropriate reputation. Spammers and malicious actors may rely on newly registered, or previously unused domains to disguise their activities, and avoid interdiction due to low reputation. Some legitimate URLs may briefly appear in this threat category as they become visible.
- Cryptojacking - Websites with embedded scripts to mine cryptocurrency which use the visitor's web browser. The script may belong to the owner of the web site, or injected by a malicious third-party, and is used as a method of generating revenue.
- Linkshare - Websites that share copyrighted files without permission. The web site may be compromised, or otherwise involved in illegal file sharing.
- Malicious Sites - Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category.

Support

Related Documentation

See the chapter for URL categories in the user guides for AsyncOS for Cisco Web Security Appliances and Cisco Email Security Appliances:

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

Customer Support

Cisco TAC: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.
