

Bandura Cyber GMC Release Notes

This document provides release notes for the Bandura Cyber Global Management Center (GMC).

The complete GMC User Manual can be retrieved from the Bandura Cyber Support Center, located here: <https://helpdesk.banduracyber.com/hc/en-us>.

RELEASE NOTES

Release: GMC Build 69, August 26, 2021

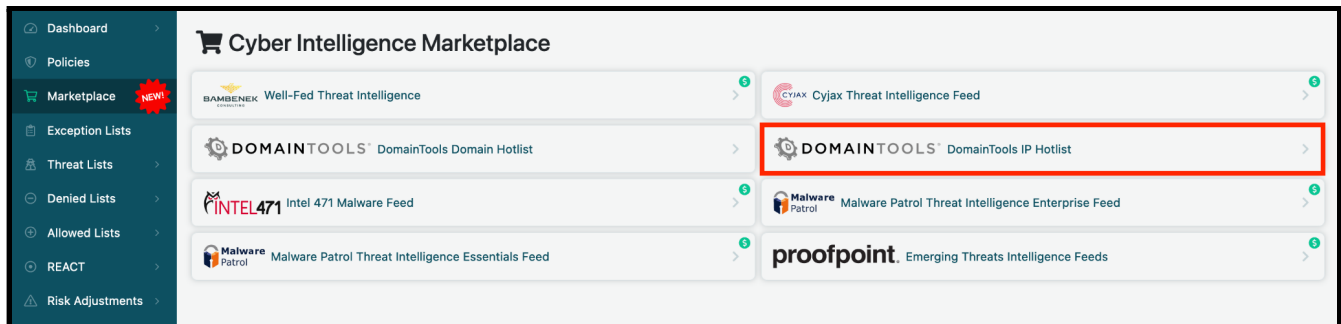
New Features:

New Marketplace Feed - DomainTool IP Hotlist

The Cyber Intelligence Marketplace has a new, FREE offering available to all customers: DomainTools IP Hotlist.

To enroll:

1. Select Marketplace from the left-hand navigation menu. All available offerings will display.
2. Select the DomainTools IP Hotlist Listing



3. Select Subscribe

The cost to add the DomainTools IPs feed to your subscription is:

FREE!

Subscribe



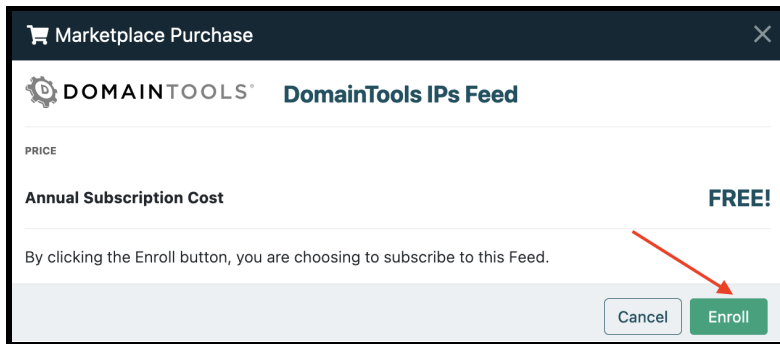
DomainTools IPs

Description

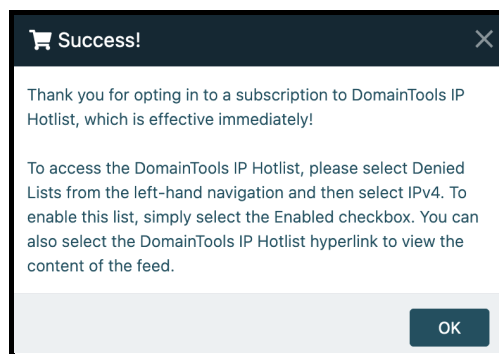
From a network defense perspective, a substantial area of risk involves traffic from the protected environment to threat-actor-controlled assets. Connections from trusted users to hostile IP addresses enable malware downloads or command and control, data exfiltration, espionage, and other threat activities. Preventing users from reaching dangerous infrastructure, while supporting necessary business functions, is a major component of any network defense strategy. Most of those connections are directed toward domains, and not hard-coded IP addresses. This makes the population of domains on a hosting IP address an ideal basis for determining how risky the IP is.

The DomainTools IP Hotlist is designed to identify the riskiest population of hosting IP addresses. Two main criteria define this list: the average Domain Risk Score of the hosted domains, and the level of traffic the address is receiving, as measured in Internet-wide passive DNS collection. The Hotlist is an ideal database for high-confidence block list and detection rule creation. Typical Hotlist size is between 40,000 and 50,000 IP addresses.

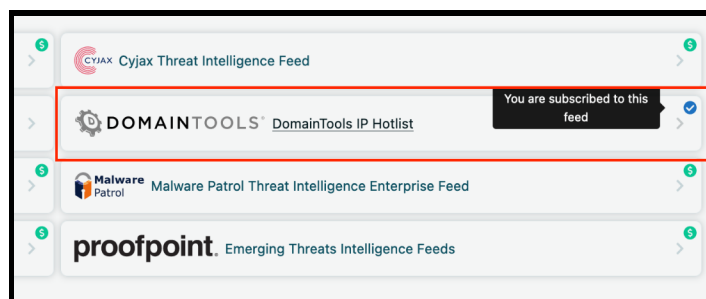
4. Select Enroll



5. A Success Toast will display



6. On the main Marketplace screen, the listing will be updated to show you are subscribed to the feed



To Enable the list:

1. From the left-hand navigation menu, select IPv4 under Denied Lists
2. Select the checkbox under the Enabled column for the DomainTools IP Hotlist

IPv4 Denied Lists

Enabled	Type	Name	Description	Entries	Last Sync	Last Update
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	IP RBL (all)	30,959	07/10/20 11:44:06 AM	07/10/20 11:44:06 AM
<input checked="" type="checkbox"/>	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000	07/10/20 12:03:36 PM	07/10/20 12:03:36 PM
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	DHS Information Sharing	0	07/10/20 12:30:03 PM	07/10/20 12:30:03 PM
<input type="checkbox"/>	Automatic	DomainTools	DomainTools IP Hotlist	57,827	08/26/21 12:52:12 PM	08/26/21 11:50:16 AM
<input type="checkbox"/>	Automatic	ET Compromised IPs	Emerging Threats Compromised IPs	553	07/10/20 11:44:02 AM	07/09/20 6:58:26 PM
<input type="checkbox"/>	Automatic	Feodo	Feodo feed from abuse.ch	534	07/10/20 11:56:40 AM	07/10/20 11:56:40 AM

3. After enabling the list, navigate to Policies
4. Select the Denied Lists icon in the applicable policy row

Policies

Name	Description	Default Inbound	Default Outbound
Default Inbound	Default Inbound Policy	—	—
Default Outbound	Default Outbound Policy	—	—

5. Select the DomainTools checkbox
6. Select Save in the top-right corner

IPv4 Denied Lists Default Inbound

Inherit Defaults

Public IPv4 Denied Lists

- Bambenek DGA
- Bambenek Sinkhole
- Bandura Healthcare Ransomware
- Blocklist.de
- CINS Army list
- Cyjax
- DHS Information Sharing
- DomainTools
- ET Block IPs
- ET Compromised IPs
- Feodo
- Intel471 High Confidence Feed
- Intel471 Medium Confidence Feed
- Malware Patrol Enterprise
- Malware Patrol Essentials
- OpenDBL TOR List
- SolarWinds Compromised IPs
- State of Missouri SOC
- Talos IP RBL
- US-CERT Cloud Services
- US-CERT Healthcare Ransomware
- US-CERT OnePercent Ransomware
- Zoom

Cancel Save

NOTE: If you have Inherit Defaults selected, you will need to unselect that checkbox first.