Take Down Service

BENEFITS AND BUSINESS VALUE

- Having identified the takedown, security teams can focus on protecting the business
- Simple process to request the takedown of identified websites
- From request to conclusion, the Anomali Takedown Service handles everything
- Anomali Takedown is a global service - relevant languages and structure for communication in the takedown are handled
- Anomali Takedown Service analyses the site and determines the best course of action for takedown
- The status of all takedown requests is monitored and displayed in a dashboard
- The service monitors and confirms when the site is no longer in operation

Take Down Fraudulent or Malicious Websites

Fraudsters, criminals, and malicious actors host their content on the internet so it can be accessed by victims and/or their own malware once deployed on a victim's infrastructure. In some cases, these sites may be mimicking legitimate websites to commit direct fraud to your customers or other malicious activities against your brand's trust. In other cases, these sites have come to your attention as they have been identified as part of an attack or incident involving your organization. In these situations, but particularly the first, you want to get the site taken down.

Anyone who has pursued takedowns will know that this can often be a complex and time-consuming process. The Anomali Take Down service takes care of all this complexity and removes the time overhead, allowing your security teams to get on with protecting your business and organization. From a simple 'click' the takedown request is instantiated and then its status is tracked to conclusion.

Anomali's specialist partner for this service is dedicated to achieving effective takedowns. Together we review the service and add features to maintain a comprehensive cover of all effective methods available to achieve success for customers.

The Anomali Takedown Service is straightforward - a 12 month subscription with a chosen number of Takedown tokens valid for the duration. It is available to all Anomali customers from the Anomali App Store.

The Threat from Fraud and Malicious Websites

Threat actors and criminals often target brands and produce websites designed to trick end users into parting with their information or credentials or to trick them into downloading malware into their environments. This brand abuse could involve one of yours, the brand of a partner you do business with, or a well-known brand.

In other scenarios, threat actors simply set up sites to host and deploy their malware - almost like their malware 'app store'. You may become aware of this as you understand communication that has happened from an initial phishing attack or malware infection as it communicates with this 'app store' to download further malware.

Sometimes the sites threat actors use are legitimate sites that, due to some security flaw, have been hijacked to host their malware. Your network protection allows this communication as it's a legitimate site.

The problem defenders face is that in all these situations and especially if the site is abusing their own brand, they need these sites taken off-air or get the legitimate site cleaned up. That's when defenders discover how complex and time-consuming this can be. Achieving a successful takedown is no easy task.

Takedowns are Complex and Time-Consuming

The task of building the takedown request, figuring out who to send it to, what content/evidence is required, what format and language to use, and then tracking and chasing for progress is often complex and always time-consuming.

The Anomali Takedown Service handles all of this end to end:

Provides a simple 'click' user experience to request a takedown

Analyses the site and determines the fraudulent and/or malicious nature

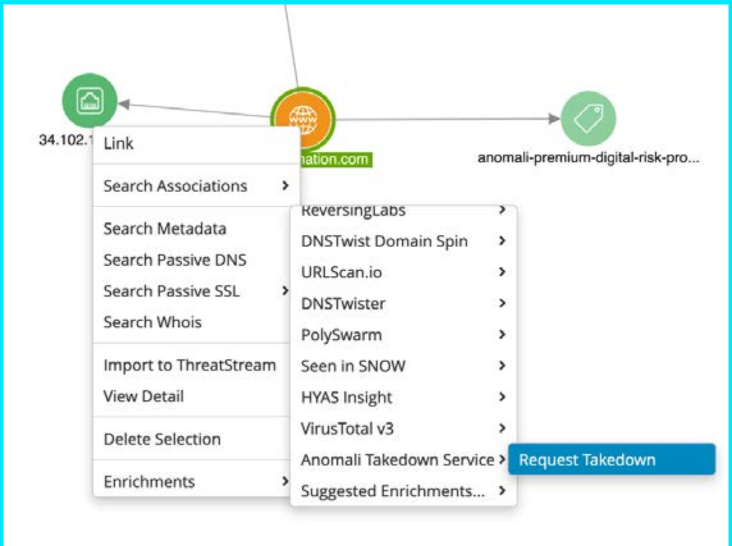
Gathers the necessary evidence and adds any further justification from you

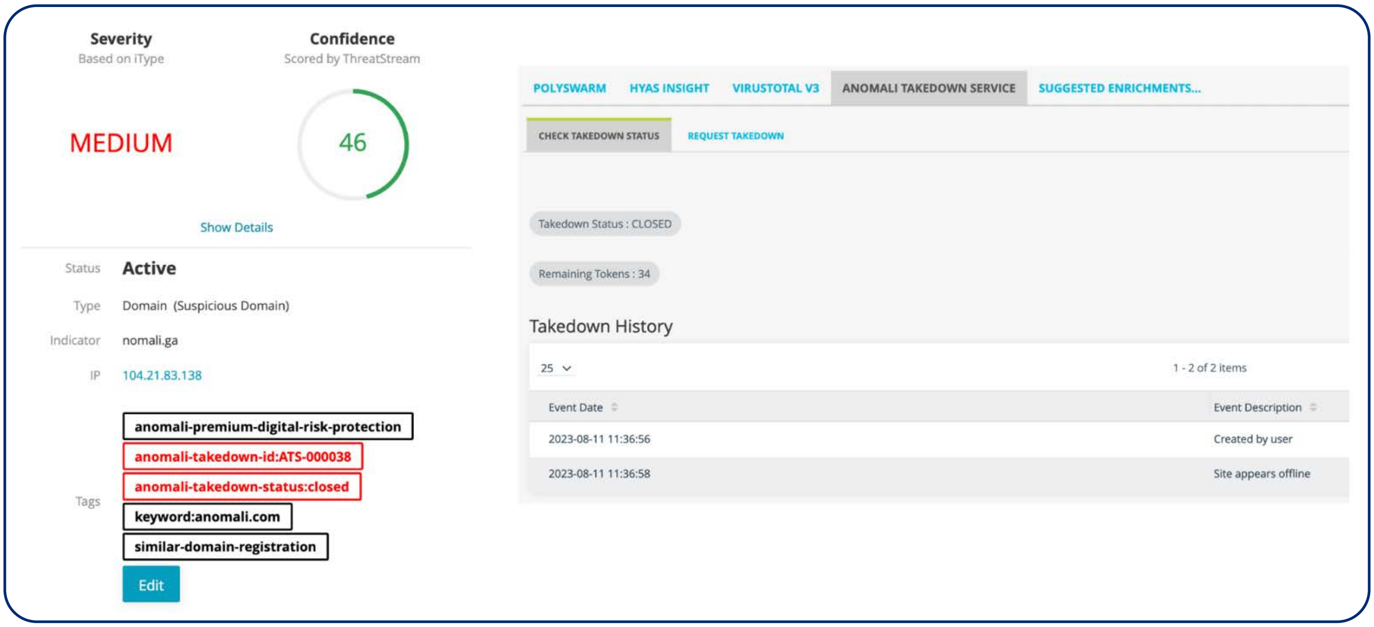
Identifies the site owner, hosting company, and domain registrar as appropriate

Formulates the communications required for each, including content, language, and method for delivery

Sends the takedown communications and initiates tracking and follow-up

Provides a dashboard and request level detail in ThreatStream to show the status and progression of all takedowns





Status Active

Type Domain (Suspicious Domain)

Indicator nomali.ga

IP 104.21.83.138

Tags
anomali-premium-digital-risk-protection
anomali-takedown-id:ATS-000038
anomali-takedown-status:closed
keyword:anomali.com
similar-domain-registration

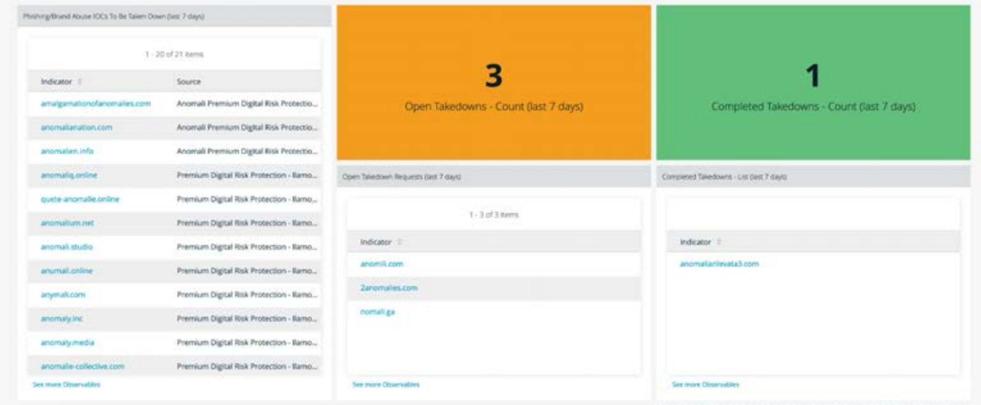
Takedown Status : CLOSED

Remaining Tokens : 34

Takedown History

25 1 - 2 of 2 items

Event Date	Event Description
2023-08-11 11:36:56	Created by user
2023-08-11 11:36:58	Site appears offline


3
Open Takedowns - Count (last 7 days)
1
Completed Takedowns - Count (last 7 days)
See more Observables
See more Observables
See more Observables

Phishing/Brand Abuse IOCs To Be Taken Down (last 7 days)

1 - 20 of 21 items

Indicator	Source
amalgamationofanomalies.com	Anomali Premium Digital Risk Protectio...
anomalianation.com	Anomali Premium Digital Risk Protectio...
anomalien.info	Anomali Premium Digital Risk Protectio...
anomaliq.online	Premium Digital Risk Protection - Bamo...
quete-anomalie.online	Premium Digital Risk Protection - Bamo...
anomalium.net	Premium Digital Risk Protection - Bamo...
anomali.studio	Premium Digital Risk Protection - Bamo...
anumali.online	Premium Digital Risk Protection - Bamo...
anymali.com	Premium Digital Risk Protection - Bamo...
anomaly.inc	Premium Digital Risk Protection - Bamo...
anomaly.media	Premium Digital Risk Protection - Bamo...
anomalie-collective.com	Premium Digital Risk Protection - Bamo...

Open Takedown Requests (last 7 days)

1 - 3 of 3 items

Indicator
anomili.com
2anomalies.com
nomali.ga

Completed Takedowns - List (last 7 days)

Indicator
anomalianlevata3.com

With the simple user experience to request and track takedowns, the pressure and stress of getting malicious sites off the internet has been removed. Defenders can rest easy knowing that the takedown they've identified is being pursued to conclusion on their behalf. They can focus their efforts on continuing to protect their business.

ANOMALI