SANS

Analyst Program

Product Review

Applying AI and Automation to Protect Your Internet Attack Surface

Written by Jake Williams

December 2021

BOLSTER

Introduction

The purpose of this document is to provide an independent review of the Bolster product. SANS reviewed the Bolster product to identify the product's capabilities and how they can be useful, primarily for domain monitoring, fraud detection, and brand protection. SANS determined that the Bolster product has strong capabilities for identifying multiple types of infringements and malicious conditions, going much further than simply examining typosquat domains. If your organization is evaluating domain monitoring, brand monitoring, or fraud prevent solutions, consider Bolster a strong candidate.

Internet Attack Surface Continues to Morph

The internet attack surface used to be limited primarily to typosquat domains. It now includes application store attacks, Google Sites, social media, app store submissions, phishing sites, and more. Organizations thinking only about typosquat domains are missing significant portions of their external attack surface.

In the past, a limiting factor in typosquat domains was that there were a very small number of top-level domains (TLDs). That is no longer the case. The rapid explosion in the number of TLDs means that threat actors have far more opportunities to find believable typosquat domains with which to abuse brands.

The Bolster product has strong capabilities for identifying multiple types of infringements and malicious conditions, going much further than simply examining typosquat domains.

The attack surface, however, has expanded significantly beyond just typosquat domains. With the large number of platforms available to serve content without ever registering a domain (think Google Sites), it's easier than ever to publish infringing or malicious content. Additionally, threat actors use the ever-growing number of free webmail platforms to register email addresses that will pass casual inspection and cost an organization reputational loss.

App stores are rife with copycat applications targeting unsuspecting users. At a minimum, a fraudulent app deprives the legitimate publisher of advertising or app store sales revenue. More commonly, threat actors use fraudulent applications to steal accounts and other data from users who install the applications. This is a worst case for victim organizations. Victim users channel their anger at the legitimate organization, believing they are the source of the compromise. The victim organization not only suffers reputation damage, it also loses time dealing with afflicted users.

Organizations also suffer damages from fraudulent listings in the ever-growing number of online marketplaces. Providers of physical goods aren't the only ones hurt by marketplace fraud. Those who sell virtual goods, such as SaaS providers, are also at the mercy of fraudsters causing reputational damage in online marketplaces.

Add to all these the vast impersonation attack surface created by social media platforms, and it's no wonder that Bolster is moving into this space. Because the social media protection features were still in development at the time of the review, we did not include them as part of this product review.

The internet attack surface is certain to continue to change. As new threats emerge, fraudsters and threat actors will move to occupy social media spaces. Organizations without full-time, dedicated teams monitoring the latest advances in social media protection will likely lose this high-stakes game of cat and mouse.

Brand Protection Now an Information Security Priority

Brand protection traditionally has been the job of the organization's legal team, although in some cases the job fell to the marketing team. While some brand protection operations still require intervention from the legal team, the primary duties are rapidly shifting to information security teams. This move makes sense. Even though legal or marketing teams might identify a counterfeit application in an app store, they ultimately must rely on the information security team for capability analysis of the application.

Similarly, when customers complain that they are receiving phishing emails harvesting credentials for your site, the information security team always plays a major role in the investigation. In many cases, information security also receives the initial report for this activity. Although other units in the organization may be involved in remediation of select incidents, practically every online brand protection incident involves the information security team. Put bluntly, brand security is information security. Given this fact, it's no surprise that most forward-leaning organizations have moved online brand-monitoring activities under the purview of the information security team.

Product Review

This section of the paper introduces the Bolster product and highlights the capabilities that were enumerated as part of the SANS product review. To keep the review a manageable length for readers, not all features of the product evaluated are explicitly listed in the review. Also note that social media monitoring features were still in beta at the time of evaluation and are not included in the review. We encourage readers to evaluate the product independently to discover additional features not covered in this document.

How Does Bolster Perform Discovery?

Bolster uses multiple sources for obtaining source data, many of which are proprietary. Some data sources we can discuss publicly include:

- Advanced typosquatting detection in passive DNS
- Domain feeds showing all new domains registered every 24 hours from most TLDs
- Spam and phishing honeypots deployed worldwide (to arm Bolster with links to landing pages)
- Certificate transparency logs
- Threat intelligence feeds

When it discovers a suspicious domain, the Bolster engine uses a headless browser to load the web page, process the document object model (DOM), and take a screenshot. It repeats this process for links discovered in spam and phishing emails caught in email honeypots. This distinction between the domain and links is important because a threat actor may leave the index page free of any infringing or likely malicious data but place this data on specific pages that are only accessible via links provided in the phishing emails.

Another variation of this attack method places the infringing code on the index page but delivers the content only if specific parameters in the URL (delivered through a phishing link) are present. These approaches are why the use of phishing and spam honeypots are such an important differentiator between Bolster and other products that index only newly registered domains. Bolster does that too, but the capability to use phishing and spam honeypots ensures that malicious activity is detected and mitigated.

When it discovers a suspicious domain, the Bolster engine uses a headless browser to load the web page, process the document object model (DOM), and take a screenshot.

Another differentiator is the use of an actual headless browser. A tool retrieving a web page without rendering the DOM is trivial for the site operator to detect. By breaking the page load up across many files (which is typical in most legitimate websites anyway), the threat actor can detect competitors' browser-substitutes and return only non-infringing content. Another trick used by threat actors to evade simplistic detection is to use JavaScript **`GetElementById()`** and **`AppendChild()`** to dynamically build suspicious DOM elements, such as a fake login form. If a fake browser is used that doesn't properly render JavaScript, a higher false negative rate will almost certainly result.

After the data is collected, the Bolster Artificial Intelligence and Machine Learning (AI/ML) engine goes to work processing the data. For those not intimately familiar with AI/ML technologies, it's important to note that optimum results will only be delivered through a combination of good source data and good algorithms. That's why Bolster puts so much work into its data collection: "Garbage in" results in "garbage out."

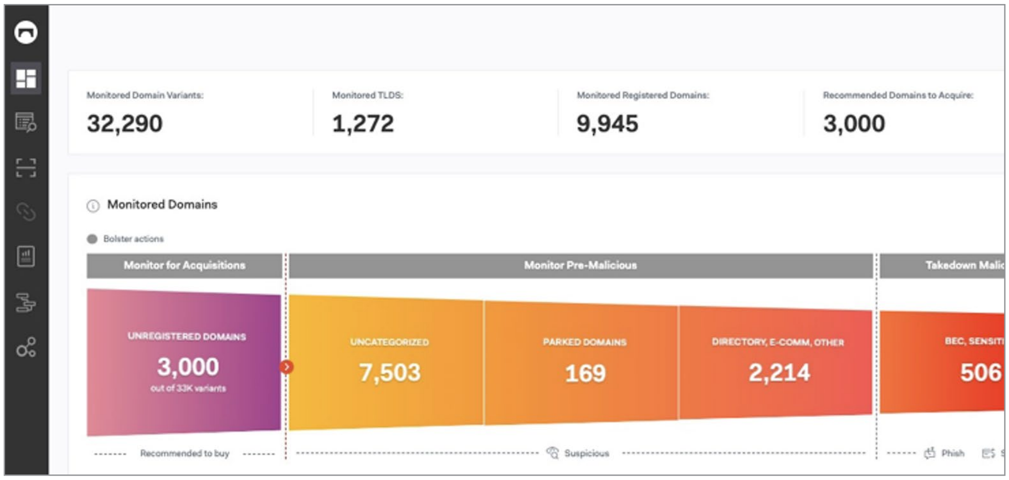
The Bolster AI/ML engine performs natural language processing (NLP), image recognition (to detect logos and other trademarked content), and clustering to identify suspicious and malicious domains. Clustering helps identify patterns that a human might miss. For instance, certificate transparency logs reveal information about the subject of the certificate that might follow a specific pattern, such as particular spacing or consistent misspelling of a city name. While a human *might* notice these, ML doesn't miss any of them—and does so less expensively and at scale with reliable results. Suspicious items are reported in the dashboard, displayed as a funnel of risks.

The Bolster AI/ML engine performs natural language processing, image recognition, and clustering to identify suspicious and malicious domains.

Dashboard

The Bolster dashboard (see Figure 1) is an extremely useful tool for visualizing the attack surface identified, monitored, and remediated. The dashboard paints a picture of the brand protection surface in a way that's consumable by practically any stakeholder.

The dashboard highlights the following items:



Monitored Domain Variants: 32,290

Monitored TLDS: 1,272

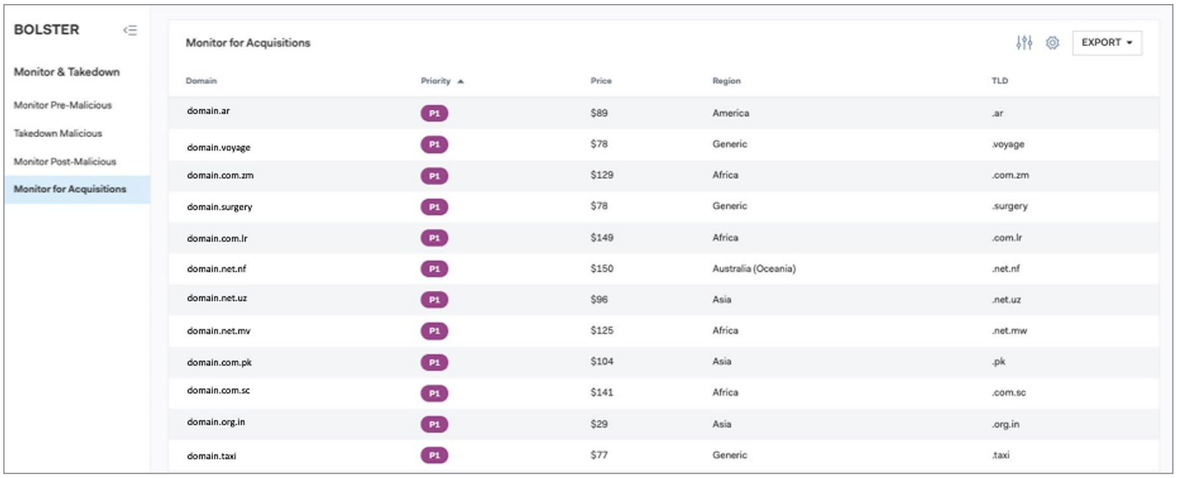
Monitored Registered Domains: 9,945

Recommended Domains to Acquire: 3,000

Monitored Domains

Figure 1. Dashboard

- **Domain names that have been identified as potential typosquats—**These are domains that have not yet been registered.
- **Domain names with typosquats that have already been registered—**These are further separated by domains that are parked with a registrar and have been categorized and those that have not been categorized at all.
- **Domains that are in the takedown process—**These domains may have been observed performing credential-harvesting attacks, sending phishing emails, or performing other infringing behavior.
- **Domains that have previously been taken down but are still being monitored for post-takedown malicious activity—**Sometimes threat actors may reactivate a previously suspended domain, usually through a registrar's abuse appeals process. This number also helps show the value proposition for brand monitoring.



Monitor for Acquisitions

Domain	Priority ▲	Price	Region	TLD
domain.ar	P1	$89	America	.ar
domain.voyage	P1	$78	Generic	.voyage
domain.com.zm	P1	$129	Africa	.com.zm
domain.surgery	P1	$78	Generic	.surgery
domain.com.lr	P1	$149	Africa	.com.lr
domain.net.nf	P1	$150	Australia (Oceania)	.net.nf
domain.net.uz	P1	$96	Asia	.net.uz
domain.net.mv	P1	$125	Africa	.net.mw
domain.com.pk	P1	$104	Asia	.pk
domain.com.sc	P1	$141	Africa	.com.sc
domain.org.in	P1	$29	Asia	.org.in
domain.taxi	P1	$77	Generic	.taxi

Figure 2. Prioritized Unregistered Domain List

Unregistered domains are those that might later be registered by a threat actor and have a high likelihood of infringing use. Depending on the organization's size, it might not have the political will to purchase hundreds or thousands of domains to prevent attacks.[1] That's where Bolster's prioritization scores come into play. Bolster's AI/ML engine automatically prioritizes the unregistered domains based on the likelihood that the given domain will be used maliciously and provides each with a weighted score. This capability allows customers to purchase low-cost, high-risk domains first and monitor the rest. Figure 2 provides an example of a prioritized list of unregistered domains.

[1] Somehow there's always political will to acquire a domain after it has been used maliciously. Proactive actions, however, are better than reactive responses.

Some information security professionals might believe they can prioritize better than ML; in reality, though, they cannot. Bolster has built what is likely the world's largest dataset showing the patterns by which threat actors take unregistered domains, register them, and use them maliciously. Utilizing the prioritization provided by Bolster, organizations can ensure they get maximum value from every penny they spend on proactively acquiring domains to prevent attacks.

Bolster is working to become a domain registrar to ease the process of acquiring domains. This plan will ease workflows and further reduce domain acquisition costs for Bolster customers proactively acquiring domains before they've been used maliciously.

Parked Domains

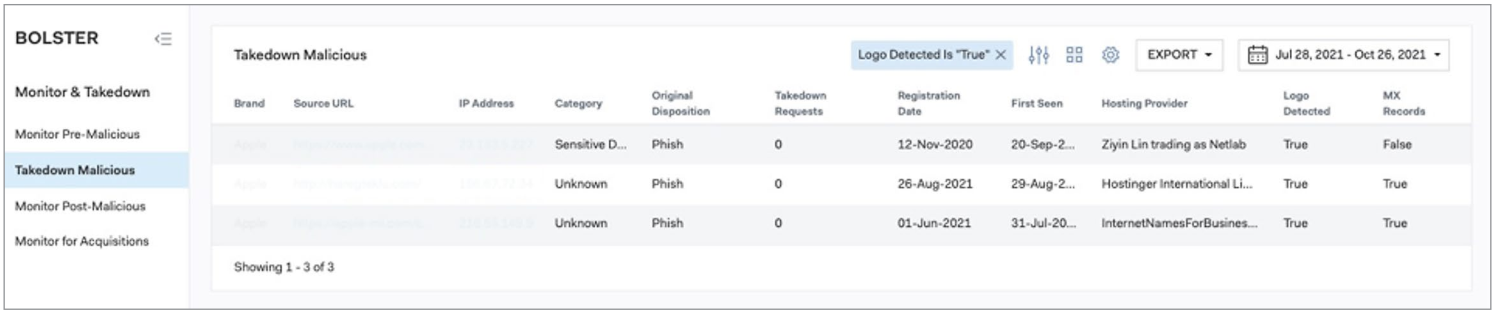
When Bolster identifies a registered domain, it identifies whether it has a high likelihood of becoming malicious in the future and continues to monitor the domain for signs of weaponization. This approach includes detecting whether the domain is no longer parked, then examining DOM elements, and applying NLP and image recognition technologies to discover likely malicious use. All this happens automatically, without the need for analyst involvement.

Contrast this to the manual approach. Suppose the analyst regularly analyzes certificate transparency logs (just one data source Bolster actively monitors) for a few misspellings of their primary domain (Bolster monitors hundreds of such misspellings), finds a new domain, but determines that it is parked. The analyst adds this to a queue in hopes of returning to it in the future. In reality, even if the analyst discovers the newly registered and parked domain, they are unlikely to return to it before it is weaponized.

A registered but parked suspicious domain is a lot like a threatening gang standing idly on public property outside your corporate office. You know they pose a risk, but they haven't broken any laws yet and, at this point, you can't take any action. But that doesn't mean that you can simply ignore them. Vigilant, continuous monitoring is needed—and let's be honest, that's exhausting and time-consuming when done manually. Automation matters here first because of scale, but also because humans simply can't search for the same variety of brand protection issues that the AI/ML engine can. Additionally, brand monitoring isn't a point-in-time problem. It requires consistent application of resources over time. Nowhere is this problem shown more clearly than a registered domain that is parked in a pre-weaponized state.

Domain Lists

Analysts obviously want to gain more details than are present in the dashboard. The Bolster UI makes it easy to see high-level information about domains at a glance (see Figure 3). The information displayed in the table includes the IP address, registration date, whether the domain has been involved in phishing, whether a takedown has been initiated, whether the brand's logos were detected on the site, and many other fields.



Takedown Malicious

Brand	Source URL	IP Address	Category	Original Disposition	Takedown Requests	Registration Date	First Seen	Hosting Provider	Logo Detected	MX Records
[redacted]	[redacted]	[redacted]	Sensitive D...	Phish	0	12-Nov-2020	20-Sep-2...	Ziyin Lin trading as Netlab	True	False
[redacted]	[redacted]	[redacted]	Unknown	Phish	0	26-Aug-2021	29-Aug-2...	Hostinger International Li...	True	True
[redacted]	[redacted]	[redacted]	Unknown	Phish	0	01-Jun-2021	31-Jul-20...	InternetNamesForBusines...	True	True

Showing 1 - 3 of 3

Figure 3. Domain Details List

This information is very valuable to have in a single place during an investigation. Navigating the UI made it clear that the Bolster product was built by people who understand analysts' needs. A feature that really drives this point home is the capability to export data from practically any UI component. Most application developers, unfortunately, think they know what the user will want from the data and that they have included all necessary functions in the user interface. While that would be great, it's almost never a reality. Smart developers include functionality to export data (preserving format), offering maximum flexibility for analysis well beyond the original developer's vision. Figure 4 shows a sample export option.

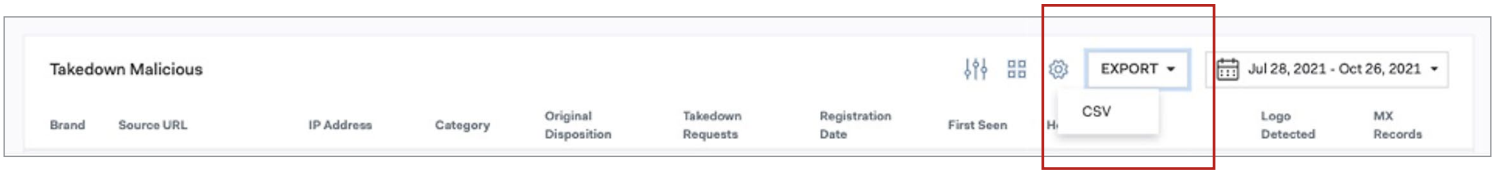
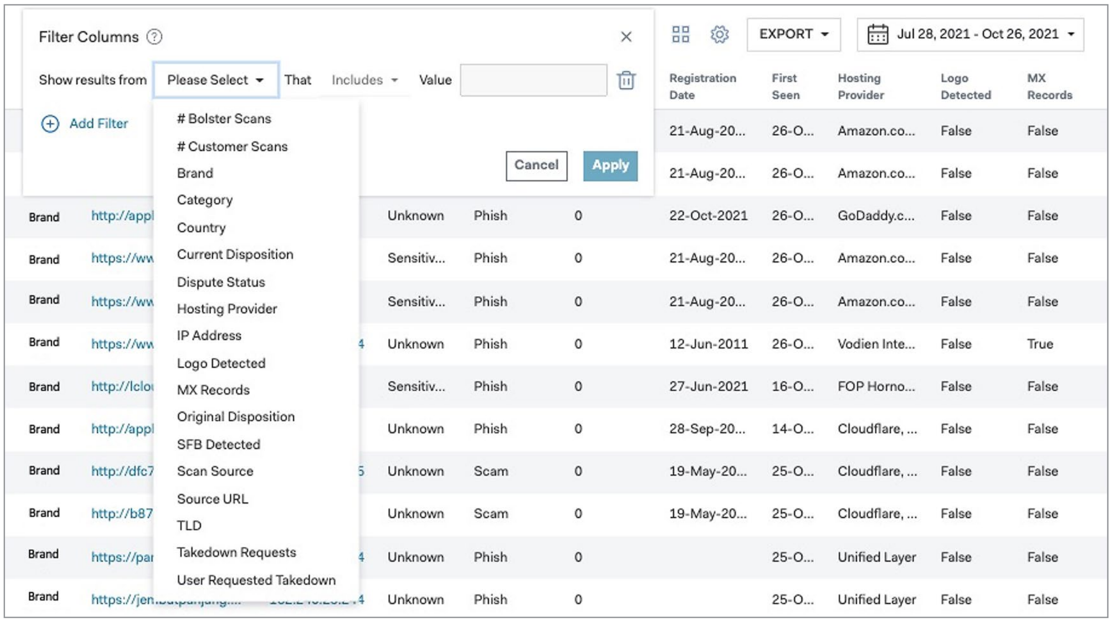


Figure 4. Export Option

In testing, we found less need to export data than we normally do while learning a "new-to-us" product. Not only is the UI fairly easy to navigate, but columns are easy to customize (see Figure 5). Additionally, columns can be filtered individually or combined with other column filters, removing most of the need to export data for analysis.



						Registration Date	First Seen	Hosting Provider	Logo Detected	MX Records
						21-Aug-20...	26-O...	Amazon.co...	False	False
						21-Aug-20...	26-O...	Amazon.co...	False	False
Brand	http://appl		Unknown	Phish	0	22-Oct-2021	26-O...	GoDaddy.c...	False	False
Brand	https://ww		Sensitiv...	Phish	0	21-Aug-20...	26-O...	Amazon.co...	False	False
Brand	https://ww		Sensitiv...	Phish	0	21-Aug-20...	26-O...	Amazon.co...	False	False
Brand	https://ww	4	Unknown	Phish	0	12-Jun-2011	26-O...	Vodien Inte...	False	True
Brand	http://lclo		Sensitiv...	Phish	0	27-Jun-2021	16-O...	FOP Horno...	False	False
Brand	http://appl		Unknown	Phish	0	28-Sep-20...	14-O...	Cloudflare, ...	False	False
Brand	http://dfc7	5	Unknown	Scam	0	19-May-20...	25-O...	Cloudflare, ...	False	False
Brand	http://b87		Unknown	Scam	0	19-May-20...	25-O...	Cloudflare, ...	False	False
Brand	https://pa	4	Unknown	Phish	0		25-O...	Unified Layer	False	False
Brand	https://jen.butpanjang....	102.2 [illegible] 4	Unknown	Phish	0		25-O...	Unified Layer	False	False

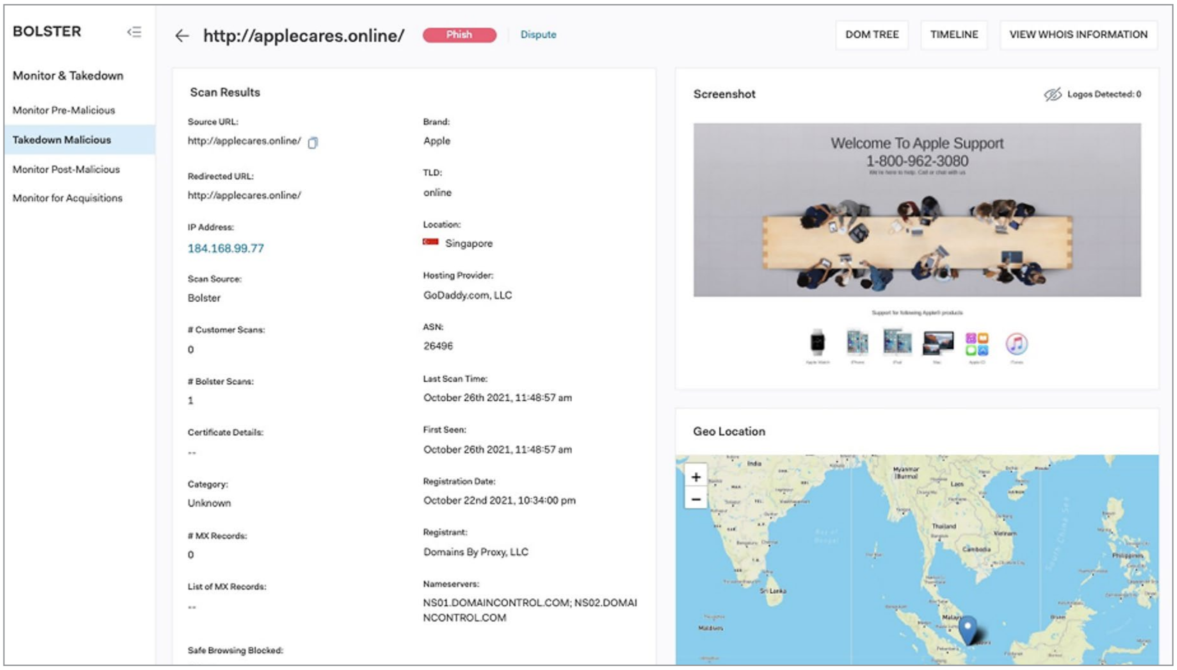
Figure 5. Column Customization

Individual Domain Details

Analysts can drill into information about every registered domain identified. As shown in Figure 6, information provided by the Bolster engine includes:

- Hosting provider
- Geolocation
- Network telemetry about the domain
- Passive DNS
- Screenshots (where applicable)

This data provides evidence supporting the classification for each domain discovered.



Scan Results

Source URL: http://applecares.online/

Brand: Apple

Redirected URL: http://applecares.online/

TLD: online

IP Address: 184.168.99.77

Location: Singapore

Scan Source: Bolster

Hosting Provider: GoDaddy.com, LLC

Customer Scans: 0

ASN: 26496

Bolster Scans: 1

Last Scan Time: October 26th 2021, 11:48:57 am

Certificate Details: --

First Seen: October 26th 2021, 11:48:57 am

Category: Unknown

Registration Date: October 22nd 2021, 10:34:00 pm

MX Records: 0

Registrant: Domains By Proxy, LLC

List of MX Records: --

Nameservers: NS01.DOMAINCONTROL.COM; NS02.DOMAINCONTROL.COM

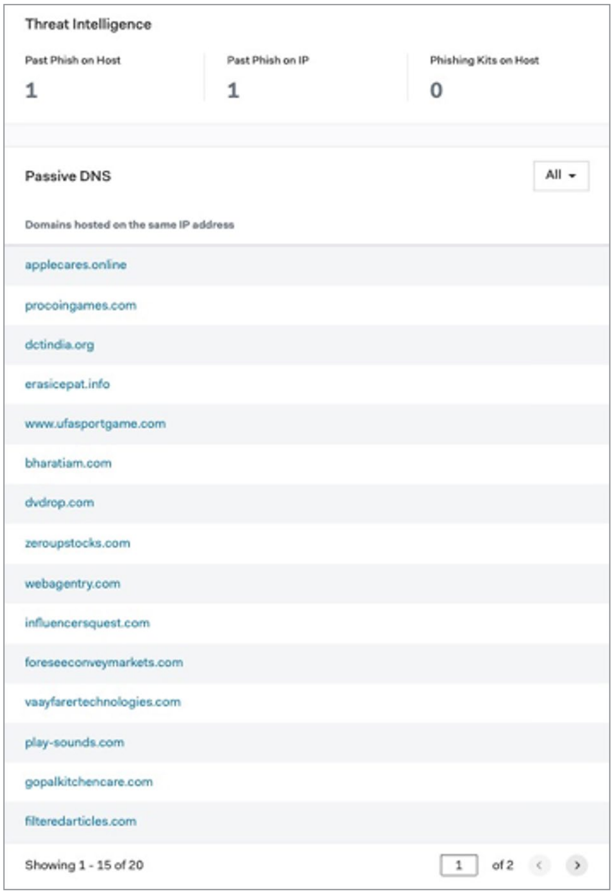
Safe Browsing Blocked:

Figure 6. Individual Domain Details

Some might see this simply as data enrichment, but it goes much further than the typical forms of data enrichment we see for malicious domains. Not only can the analyst see historical information (original disposition), but they can also see whether phishing has been previously observed on the IP address where the domain is now parked. Identifying whether the domain has an MX record (for example, configured for email) is another differentiator that contextualizes the domain.

Showing the source of detection to the analyst is important. High-quality analysis requires source grading[2] for credibility and reliability of data provided. Too many products condescendingly hide behind "proprietary algorithms you wouldn't understand anyway" and say, "Just trust us. This is bad." Bolster shows the original scan source as well as historical disposition of the domains, laying its proverbial cards on the table for all to see. This is both a sign of confidence in the underlying technology and a benefit to analysts who are more prone to trust the resultant data because they understand the process.

Multiple domains observed on the IP address where the domain is now parked may also serve as a discriminator for the analyst in determining how to handle the alert. Passive DNS displays both what domains are presently at the IP address and what domains have previously been there. Because threat actors regularly reuse infrastructure, this data point alone is often sufficient to block an IP address. See Figure 7.



Threat Intelligence

Past Phish on Host	Past Phish on IP	Phishing Kits on Host
1	1	0

Passive DNS

Domains hosted on the same IP address

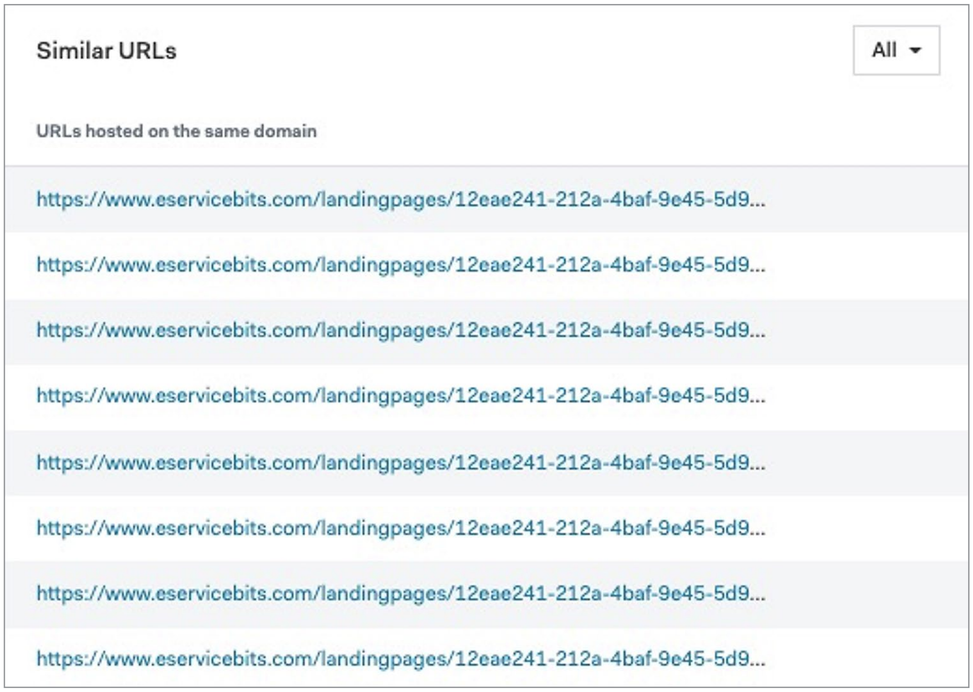
applecares.online
procoingames.com
dctindia.org
erasicepat.info
www.ufasportgame.com
bharatiam.com
dvdrop.com
zeroupstocks.com
webagentry.com
influencersquest.com
foreseeconveymarkets.com
vaayfarertechnologies.com
play-sounds.com
gopalkitchencare.com
filteredarticles.com

Showing 1 - 15 of 20

Figure 7. Passive DNS Listing of Domains on the Same IP

[1] Admiralty code, https://en.wikipedia.org/wiki/Admiralty_code

The Bolster UI also shows other URLs hosted on the same IP address both presently and historically. This is important for analysts because a threat actor may host credential-harvesting landing pages for multiple domains on a single IP address. In this case, the analyst can quickly determine that a domain is likely infringing by observing the number of diverse landing pages it hosts. See Figure 8.



Similar URLs

All ▾

URLs hosted on the same domain

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

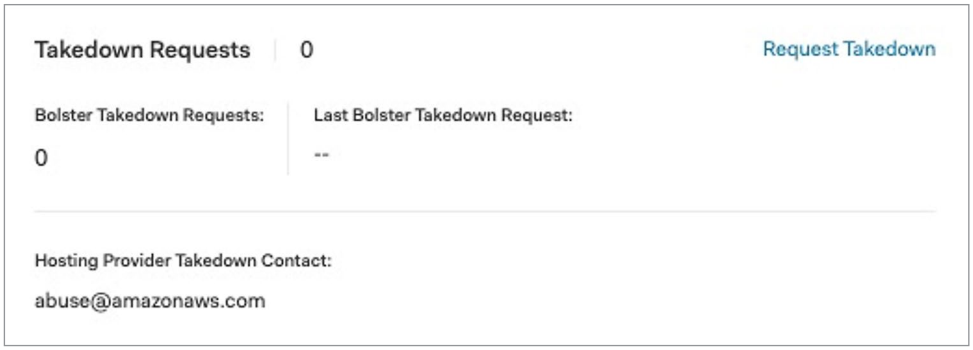
https://www.eservicebits.com/landingpages/12eae241-212a-4baf-9e45-5d9...

Figure 8. Similar URLs on the Same IP

Takedown Requests

Bolster makes the process of takedown requests trivial for customers. Anyone who has tried to get a domain taken down understands the difficulty of finding the correct submission process, gathering the supporting data required for the takedown, submitting it, clarifying the evidence with the registrar, and finally querying for updates on the status of the takedown request. In most situations, the domain takedown process with Bolster requires only a single click. With automation solutions such as SOAR (more on that later), takedowns may require zero clicks.

Bolster submits takedowns to many registrars (and most high-volume registrars) via APIs. Because of Bolster's stellar track record of high-fidelity submissions, most registrars operate on their submissions automatically. This speed and efficiency represent a stark contrast to submissions by individual analysts, where many registrars justifiably (but frustratingly) seek additional evidence to confirm the veracity of the takedown request. This feature is another way the scale of the Bolster platform provides benefits for organizations. See Figure 9.



Takedown Requests | 0

Request Takedown

Bolster Takedown Requests: 0

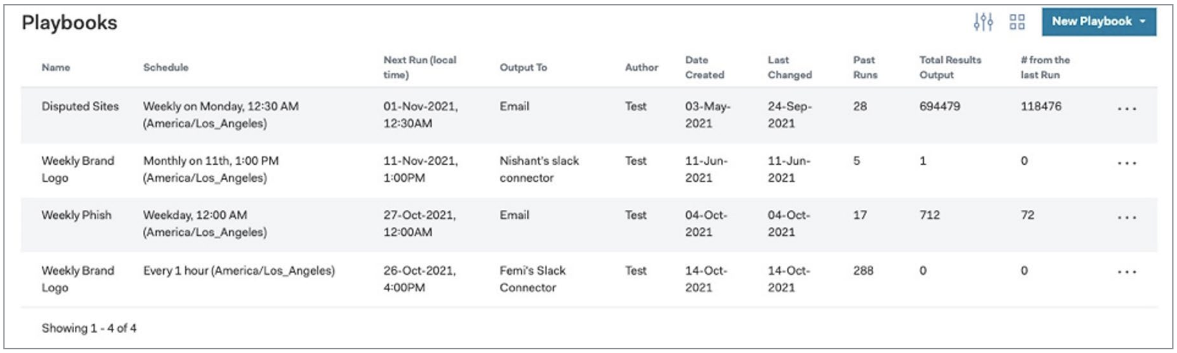
Last Bolster Takedown Request: --

Hosting Provider Takedown Contact: abuse@amazonaws.com

Figure 9. Takedown Requests

Automation Playbooks

Unless you've been living under a rock, you know automation is all the rage in security. Normally, full automation is out of reach for all except those who have invested in SOAR platforms (which are never inexpensive). Bolster provides playbooks for common operations built into its own platform (see Figure 10), a sort of "SOAR-lite." For those with existing investments in SOAR, the platform fully integrates with those solutions through an API.

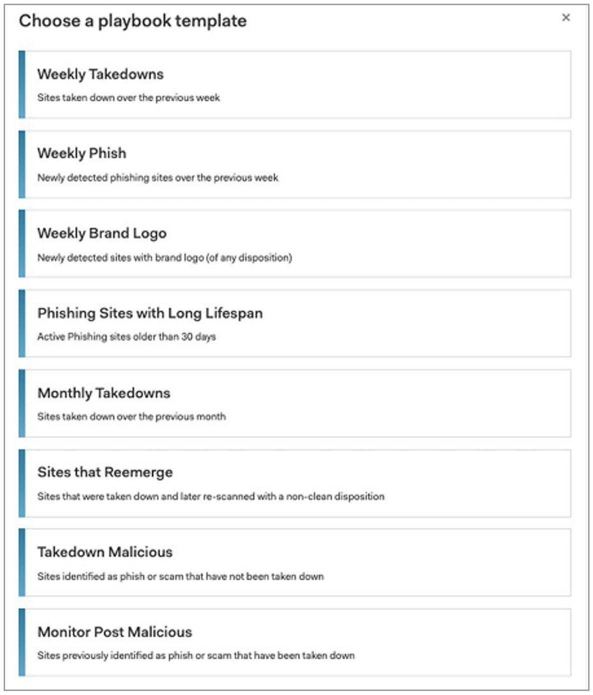


Name	Schedule	Next Run (local time)	Output To	Author	Date Created	Last Changed	Past Runs	Total Results Output	# from the last Run	
Disputed Sites	Weekly on Monday, 12:30 AM (America/Los_Angeles)	01-Nov-2021, 12:30AM	Email	Test	03-May-2021	24-Sep-2021	28	694479	118476	...
Weekly Brand Logo	Monthly on 11th, 1:00 PM (America/Los_Angeles)	11-Nov-2021, 1:00PM	Nishant's slack connector	Test	11-Jun-2021	11-Jun-2021	5	1	0	...
Weekly Phish	Weekday, 12:00 AM (America/Los_Angeles)	27-Oct-2021, 12:00AM	Email	Test	04-Oct-2021	04-Oct-2021	17	712	72	...
Weekly Brand Logo	Every 1 hour (America/Los_Angeles)	26-Oct-2021, 4:00PM	Femi's Slack Connector	Test	14-Oct-2021	14-Oct-2021	288	0	0	...

Showing 1 - 4 of 4

Figure 10. Bolster Playbooks

Creating new automations in the Bolster platform is also relatively easy, owing to a library of playbook templates (see Figure 11). In our evaluation, we found the templates to be readily usable. There wasn't a single playbook we examined where we were left scratching our heads thinking, "Who would ever need that?" This feature stands in stark contrast to other platforms we've evaluated where automation and reporting templates seem to have been written by someone with no subject matter knowledge whatsoever.



Weekly Takedowns
Sites taken down over the previous week

Weekly Phish
Newly detected phishing sites over the previous week

Weekly Brand Logo
Newly detected sites with brand logo (of any disposition)

Phishing Sites with Long Lifespan
Active Phishing sites older than 30 days

Monthly Takedowns
Sites taken down over the previous month

Sites that Reemerge
Sites that were taken down and later re-scanned with a non-clean disposition

Takedown Malicious
Sites identified as phish or scam that have not been taken down

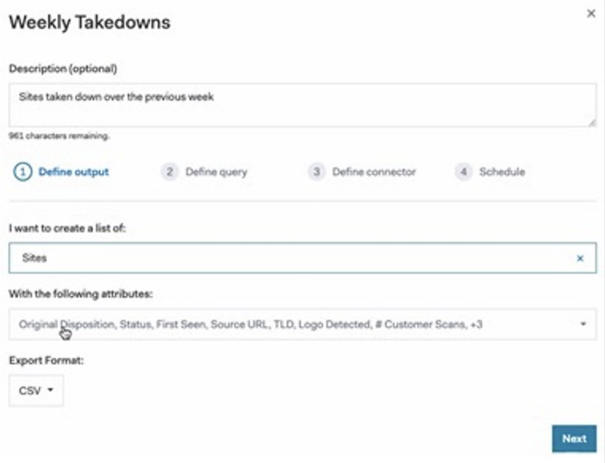
Monitor Post Malicious
Sites previously identified as phish or scam that have been taken down

Figure 11. Playbook Templates

Configuring Playbooks

Building new playbooks is relatively easy and requires no programming experience, significantly expanding the number of personnel who can benefit from the automations offered. Practically any analyst who can use the platform can configure a playbook, extending the usefulness of the data significantly. The analyst simply chooses the columns needed in the output (Figure 12), the output format, and the query they wish to execute (Figure 13).

As shown in the screenshots, automation playbook creation is trivial to complete, even with minimal experience on the platform.



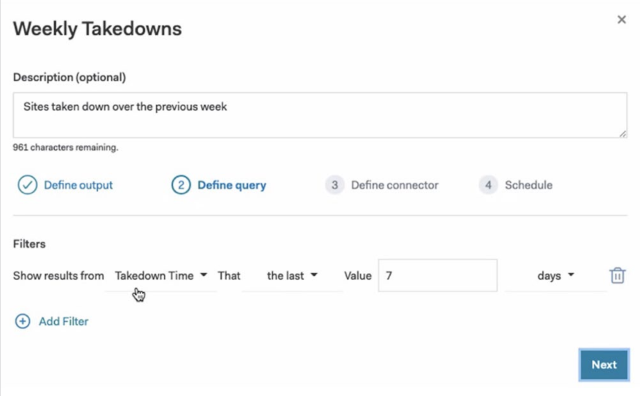
Description (optional)
Sites taken down over the previous week
961 characters remaining.

I want to create a list of:
Sites

With the following attributes:
Original Disposition, Status, First Seen, Source URL, TLD, Logo Detected, # Customer Scans, +3

Export Format:
CSV

Figure 12. Playbook Output Configuration 1



Description (optional)
Sites taken down over the previous week
961 characters remaining.

Filters
Show results from Takedown Time That the last Value 7 days

Figure 13. Playbook Query Configuration 2

Connectors

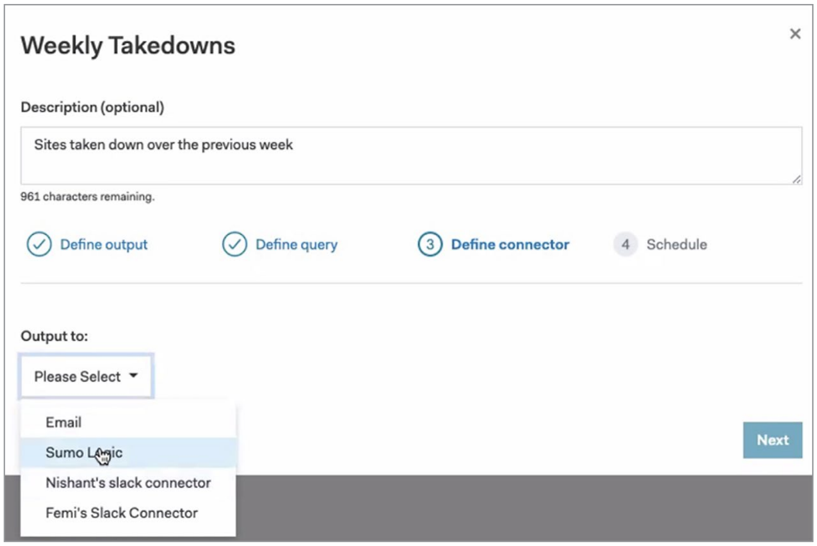
After configuring the output format and query for the playbook, we must configure somewhere to send the data. This is another area where we found the Bolster platform to be maximally flexible. The platform, of course, supports email, which these days is table stakes for any automation, but it also supports export to Sumo Logic and Slack (Figure 14).

What we found particularly exciting, though, was the ease with which we could configure new API connectors, directly from the UI (see Figure 15). This truly sets the standard for all security products going forward. Typically, users are forced to read some partially documented standard, define the interface with some arcane standard, and then call professional services when it doesn't work—only to find out that the only person on the planet who can configure a new connector is a Level 4 engineer who may get to your ticket in six months.

Not so with Bolster. The UI allows you to quickly integrate with any product that supports a **`REST API`** (most products support **`REST`**). The UI supports configuration of:

- API URL
- Request method (usually **`POST`** or **`GET`**, but not limited here)
- HTTP headers (API keys are often supplied through headers)
- HTTP form data (usually **`GET`** or **`POST`** variables)
- HTTP request body (the actual payload data)

The capability to easily extend the platform through these APIs is a key differentiator and sets the gold standard for other products going forward.



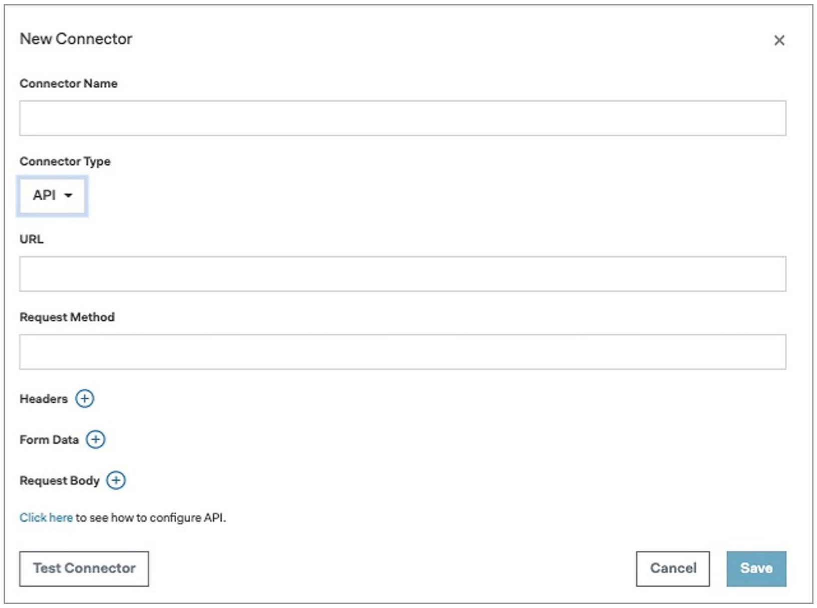
Weekly Takedowns

Description (optional)

Sites taken down over the previous week

961 characters remaining.

Figure 14. Playbook Connector Configuration



New Connector

Connector Name

Connector Type: API

URL

Request Method

Click here to see how to configure API.

Figure 15. Configuring a New Connector

Reporting Tools

Previously, we discussed the analyst dashboard showing malicious domains. While this works well for analysts, other stakeholders need different dashboards. Bolster supplies reporting dashboards that work well for those stakeholders (see Figures 16 and 17). They would also be appropriate for almost any SOC video wall.

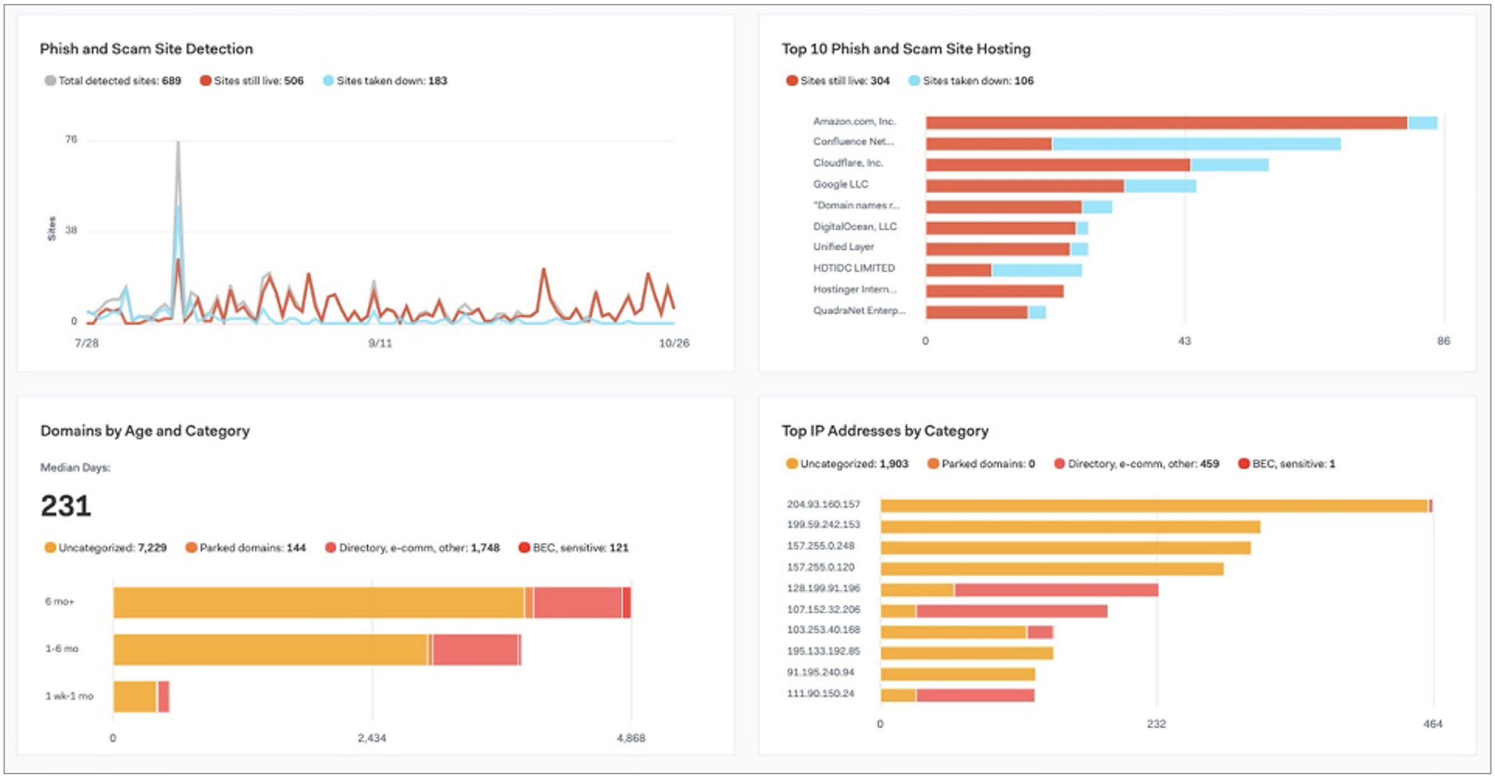


Figure 16. Reporting Dashboard 1

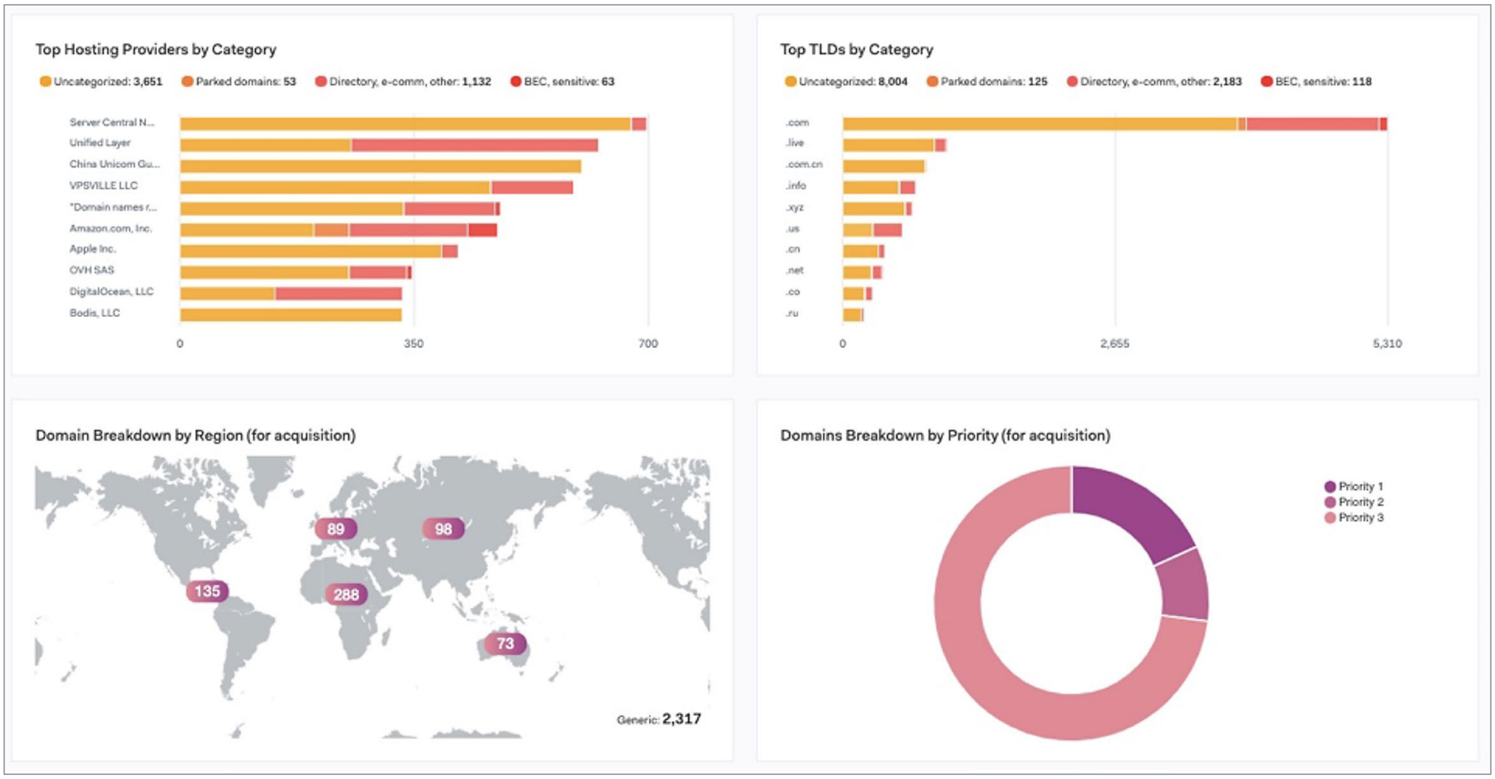
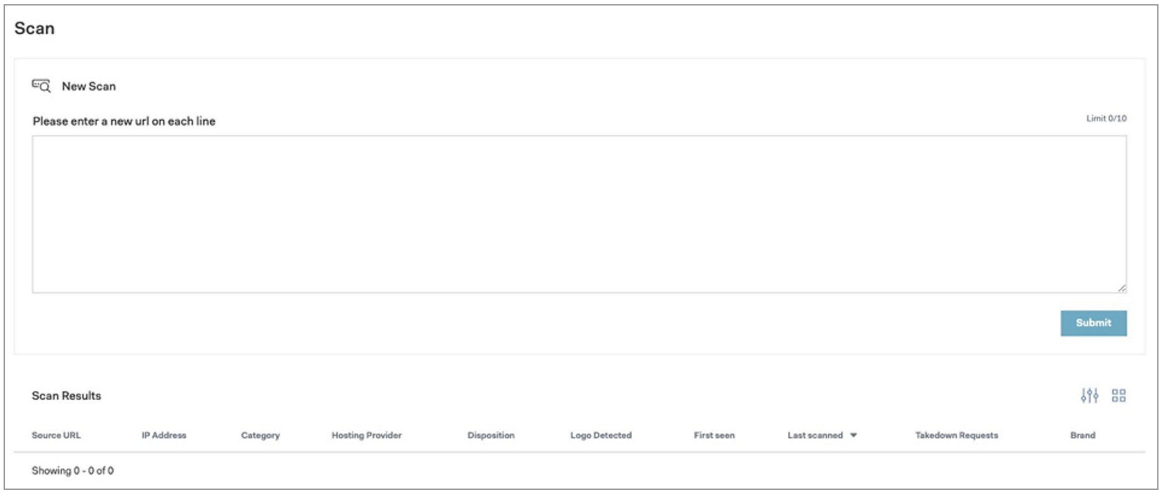


Figure 17. Reporting Dashboard 2

Bulk Threat Intelligence Checks

The Bolster platform also offers bulk checks of domains for threat intelligence. These checks are useful for analysts working with lists of domains obtained outside the platform who want to know how Bolster views these domains. This is another seemingly obvious feature missing from so many platforms. Too often, platform developers build tools that operate only on their data. While they output data, the analyst is often left thinking, “Wouldn’t it be great if I could input data for analysis?” With Bolster, the answer is, “Yes, you can.”

This feature ensures that analysts evaluate domain data the same regardless of whether it originates from inside or outside the platform. See Figure 18.



Please enter a new url on each line

Source URL	IP Address	Category	Hosting Provider	Disposition	Logo Detected	First seen	Last scanned ▾	Takedown Requests	Brand

Showing 0 - 0 of 0

Figure 18. In-Platform URL Scanning

Conclusion

In our evaluation of the Bolster platform, we found it to be easy to use and extremely effective at monitoring and protection. The Bolster platform automates many tasks that would require most organizations to dedicate multiple full-time equivalents to perform, even on a semi-regular basis. The best part of the platform, however, isn’t the automation. It’s the advanced detection and continuous monitoring we haven’t seen in any other platform. Adding takedown automation to the platform is just gravy as far as we’re concerned. If your organization is considering implementing fraud protection, or brand or domain monitoring (or overhauling an existing program), give Bolster a look.

If your organization is considering implementing fraud protection, or brand or domain monitoring (or overhauling an existing program), give Bolster a look.

Sponsor

SANS would like to thank this paper’s sponsor:

BOLSTER