censys

How to Find Hacked Web Servers with Censys Search

A Step-by-Step Guide for Cybersecurity Practitioners & Researchers

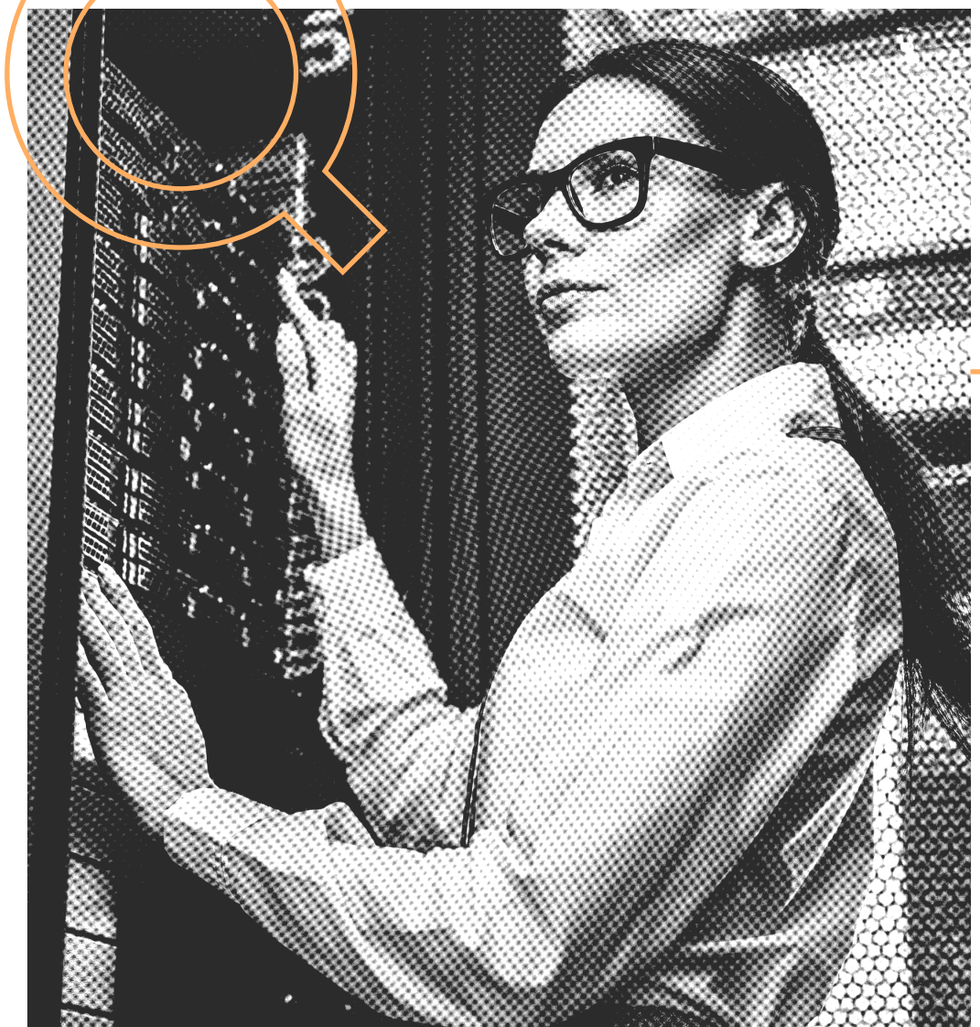
Web servers have long been popular targets for cybercriminals. If successfully hacked, web servers can be valuable gateways for criminals to exploit, disrupt, or steal from organizations. Hack into a web server, and you may also be able to distribute malware, acquire user credentials, and launch attacks on other systems to create a ripple effect of chaos and harm.

Web servers are likely to remain prime targets for hackers going forward because organizations are increasingly leveraging web-based applications and running on servers to do business.

Cybersecurity teams must therefore remain vigilant about how they protect their servers and identify traces of a successful hack.

Just as hacked web servers are a highly relevant area of focus for cybersecurity teams, they can also be appealing subjects for researchers. By digging deeper, researchers can identify hacked web servers on a macro level to understand more about trends across the global threat landscape and understand where adversaries are focusing their efforts.

In this ebook we set out to provide both cybersecurity practitioners and researchers a step-by-step guide for how to identify and track hacked web servers quickly and accurately. **Though there are a variety of methods for hunting for hacked web servers, we'll focus on how to launch an investigation with the user-friendly Censys Search tool.**



What We'll Cover:

- VI. Accessing Ground Truth Internet Intelligence with Censys Search
- VII. For Defenders: Hunting for Hacked Web Servers During a Zero-Day
    - A. A 3-Step Guide to Identifying Hacked Servers
    - B. Response: What to Do If Your Web Server Has Been Hacked
- VIII. A Censys Search Case Study: Investigating CVE -2023 -21554: MSMQ
- IX. For Researchers: Tracking Hacked Web Server Trends
- X. Wrap-Up: Gaining a Global Perspective on Internet Security

Let's start with a few words about what Censys Search is and why it can be a valuable tool for practitioners and researchers alike!

Accessing Ground Truth Internet Intelligence with Censys Search

If you're setting out on a search for hacked web servers, you're going to need a reliable source of internet intelligence. A ground truth source of internet intelligence is not only essential for facilitating an investigation into hacked servers (you need to look somewhere for evidence of a hack, after all), it can also help you claim with reasonable confidence that a hack has, in fact, occurred. The last thing you want after sounding the alarm that a hack has occurred is to discover you've been dealing with a false positive.

With this in mind, consider internet intelligence sources that are:

Comprehensive:

You can see all servers on the public-facing internet.

Up-to-date:

You're looking at a near real-time view of activity on servers.

Accurate:

You won't need to waste time with false positives.

Contextualized:

It's easy to understand the details about web servers and related activity.

Where can teams find this kind of ground truth intelligence? Meet Censys Search. Censys Search, powered by the Censys Internet Map, is the leading source of internet intelligence available. Our proprietary scanning engine empowers users with the most breadth and depth of information of any vendor.

In fact, Censys is the only vendor to:

- Conduct daily comprehensive scans of the top 100+ ports
- Conduct proprietary ML-based discovery across all 65K ports
- Refresh all services daily to eliminate false positives
- Provide detailed visibility into open ports and running protocols, regardless of standard port assignment, to understand host intent

Censys also maintains the world's largest x.509 certificate repository that users can leverage to identify related infrastructure and suspicious hosts.

Unlocking Insights with Censys Search

Practitioners and researchers can access Censys Search to conduct investigations into all corners of the internet, including hacked web servers.

Censys Search is just what it sounds like: a tool used to run searches on our internet database. Search is designed as a toolbar into which users can enter queries. While our search toolbar presents a simple UI, on our results pages, users can drill down into findings with thousands of parsing and indexing fields to learn more about what was found and pivot their investigations.

In fact, each asset we discover is enriched with data from multiple third-party sources providing the most complete picture of what the asset is. **Censys Search unlocks all of this information with a simple query language that allows you to nimbly search through mountains of data and find exactly what you're looking for.**

You can read more about Censys Search and how to get started by visiting our website or exploring our Quick Guide to Queries. And to learn how to use Censys Search to launch an investigation into hacked web servers, keep reading!

For Defenders: Hunting for Hacked Web Servers During a Zero-Day

Let's paint a picture: It's 6 a.m. and you've just rolled out of bed. Your coffee is brewing and you're about to hop in the shower as you get ready for another day as a SecOps practitioner. You're running through the day's list of to-do's when...

There it is. A message from your team pops up, and it's the kind that quickens your heartrate in an instant. You learn a dreaded zero-day has hit, and your CISO needs to know (right now) if your company is at risk of exploitation.

Zero-days can throw security teams into tailspins of investigative chaos. Business-as-usual goes out the window as teams scramble to determine, with certainty, whether or not their organization is, or is not, impacted by a zero-day.

Knowing where to look for signs of compromise, and knowing which tools to find them, can make or break your team's ability to respond quickly and accurately. Which brings us to finding hacked web servers.

According to the 2022 Verizon Data Breach Investigations Report, **web servers are the most commonly impacted asset in breaches.** This isn't exactly surprising. After all, web servers often make up the bulk of an organization's internet-facing infrastructure, and therefore are more likely to be exposed as compared to other types of digital assets.

Recent examples of zero-days involving hacked web servers have included:

Log4j CVE-2021-44338:

In late 2021, a severe remote code exploit was deployed against Log4j, an open sourced Java-based logging tool. Attackers created a malicious payload that tricks a server into loading executable code from an attacker-controlled location, resulting in remote code execution (RCE) with the permission levels of the user running the service. This means attackers could execute malware, extract sensitive information like passwords, and other nefarious actions. You can read about how the Censys Research Team tracked the Log4j zero-day using Censys Search in their rapid response article.

ProxyNotShell: CVE-2022-41082:

Attackers launched another remote code execution attack in 2022 against Microsoft Exchange Servers 2013, 2016, and 2019. Attackers were able to intercept users' credential requests and insert their own, thereby taking control of servers and gaining access to organizations' sensitive information. You can learn more about the zero-day and how the Censys Research Team tracked its impact, including through the establishment of queries and a tracking dashboard, here.

Knowing how to quickly and accurately investigate web servers for signs of compromise is therefore a highly useful skill for security teams responsible for responding to zero-days to acquire. Finding hacked web servers gives security teams the ability to track threat actors as they're working, so that they can locate affected hosts and immediately take action before any further damage is done.

Finding hacked web servers can empower teams to:

Prevent Data Loss

Hacked web servers can serve as a platform for data theft or exfiltration. By finding compromised servers, cybersecurity teams can prevent sensitive data from being stolen or leaked.

Halt Malicious Activity

Hacked web servers can be used to distribute malware, launch phishing campaigns, or host malicious content. Discovering these compromised servers enables teams to shut down an in-progress attack and prevent further harm.

Gather Threat Intelligence

Recognizing attack patterns, tools, and techniques deployed by threat actors against servers can be used to improve the organization's overall security posture.

Prevent Recurrence

By investigating and addressing hacked web servers, cybersecurity teams can learn from past incidents and take steps to prevent similar attacks from occurring in the future.

With these benefits in mind, let’s get into how to find these hacked servers using Censys Search.

For Defenders:
3 Steps to Identify Hacked Web Servers

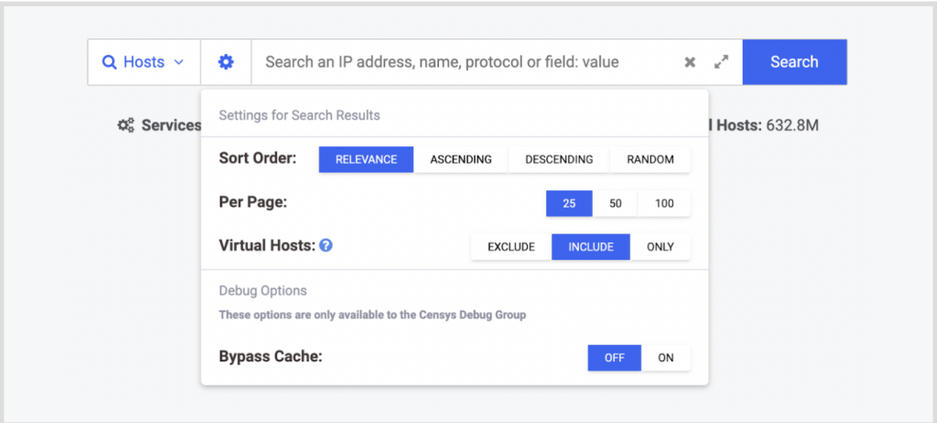
Navigate to search.censys.io and create a free Community User account, if you don't already have one. Censys Search is available as a free community tool, but users can access advanced features like robust historical lookups, regular expression queries, matched services, and a higher monthly query limit with an upgraded package.

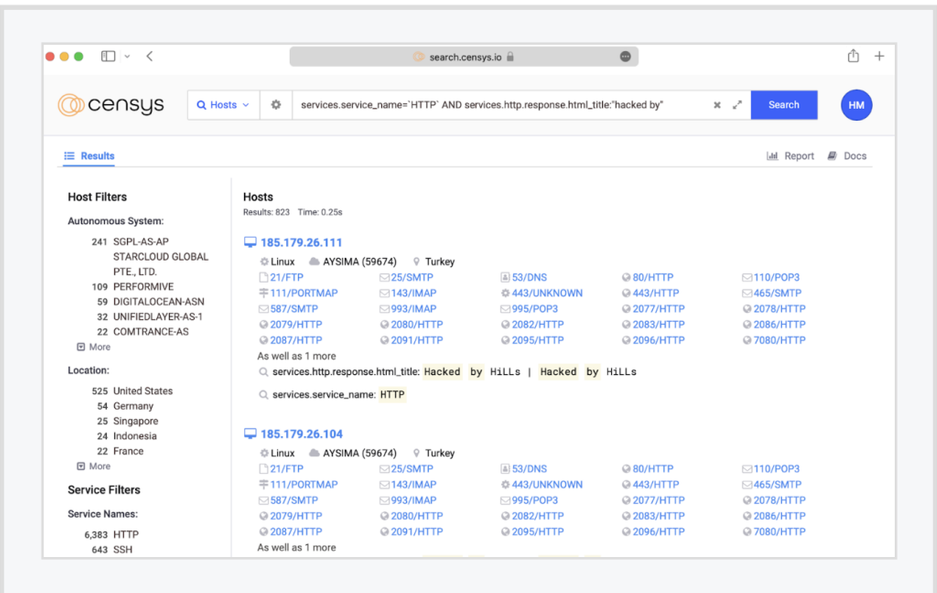
1 Looking for "Hacked By" Tags

We'll begin with one of the simplest ways that security teams can find defaced web servers: searching for the string "hacked by". Threat actors commonly "sign their work" by leaving a message on a website, such as "Hacked by [actor handle]". You can think of it like an artist's signature on a work of graffiti.

Luckily these signatures are convenient bread crumbs for defenders who are hunting for affected web servers. We can use Censys to search for these affected sites all over the world simply by looking for defacements.

Our simple query will restrict results to Censys-visible HTTP servers that include the string "hacked by" on their web interface. We can include virtual hosts in these search results by first toggling the gear icon on the search homepage and selecting "Virtual Hosts: Include" as seen below.





2 Evaluate All Censys-Visible Hosts Running HTTP

Next we can run our search by typing in this query:

services.service_name=`HTTP` and services.http.response.html_title:"hacked by"

and clicking **"search"**

This will grab all Censys-visible hosts running HTTP, regardless of which TCP port it's running it on. Based on the search results that come back and the highlighted text, you can immediately see that we're uncovering some gems with this approach.

Spot-checking the search results can be used to confirm the value of this approach — it has a high true positive rate. When accessing these hosts be sure to use a secure method such as a VPN, proxychains, or Tor.

3 Apply Filters Based on Your Specific Use Case

We can narrow down these results further based on what we're interested in. Here are some additional filters you may want to add in specific use cases:

- If you run a network (for example a university, a hosting company, or an Internet Service Provider) or need to triage reports for your clients, you can constrain this query — for example, if you work at a national CSIRT organization you can filter by the "location.country" attribute (e.g. just add "AND location.country: [your country]" to the above query).

- If you're working for a state government and helping your organization identify successful hacking events, you can filter by the "location.city" attribute.

- If you're running an Internet Service Provider, you can filter by your autonomous system number using the "autonomous_system.asn: [your asn]" attribute. Using the API you can make these calls on a regular basis and keep updated as we find these servers.

And there you have it! With constraints in place, you can narrow your search for hacked web servers based on the parameters of your investigation. For further illustration of how Censys Search can be used to find hacked web servers in response to a zero-day, consider the following case study from the Censys Research Team.

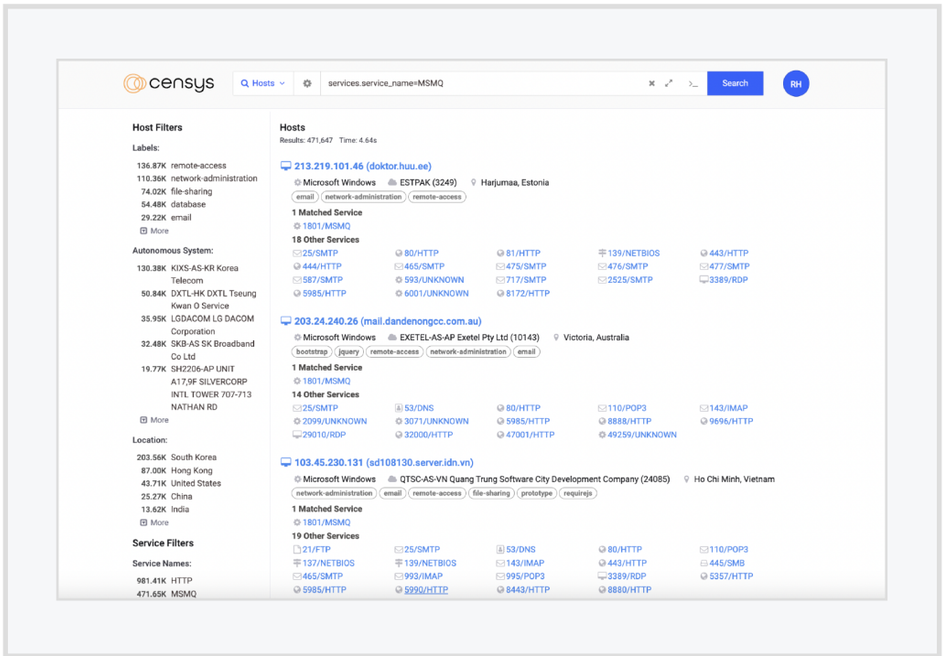
A Censys Search Case Study: Investigating CVE -2023-21554: MSMQ

In April 2023, a critical vulnerability for Microsoft's Messaging Queuing (MSMQ) service was announced. The vulnerability creates opportunities for attackers to hack MSMQ web servers and facilitate remote code execution. The Censys Research Team took a closer look at this critical vulnerability, observing the number of MSMQ servers open to the internet and providing search queries organizations could use to determine if their MSMQ servers had been hacked.

Censys' Guidance for Determining MSMQ Vulnerability

Whether the MSMQ service is firewalled from the internet or exposed publicly for a good reason, Censys recommended that individuals and organizations check whether the service was running on their servers.

Organizations could use Censys Search to determine if they had been affected by this critical vulnerability using the query: services.service_name=MSMQ



Additionally, Censys advised that administrators ensure the latest Microsoft patches have been applied if the service is intentionally enabled. By default, this service listens on TCP port 1801. It uses a proprietary binary protocol for data communication, but Microsoft documentation luckily includes examples of an MSMQ connection request and an MSMQ connection response. Using this information, an analyst could quickly check to determine if there is a valid MSMQ service listening on the other end by using "netcat", with the following command:

Unset

```
$ echo
H4sIAAAAAAAACAxM4wM3g4+kfZMPEwPAfCBgYmBguRhSHBkycOtVz
+rZngq/UjrF3n
nX2sRTsd3GdUDFh3oI/fqfuyQowM4yCEQ4AzGv6OzwCAAA= \
|base64 -d|zcat -|\
netcat $IP_ADDRESS 1801 |\
hexdump -C
```

If the output looks similar to the following hex dump, then the server is running MSMQ:

Unset

```
00000000 10 5a 0b 00 4c 49 4f 52 3c 02 00 00 ff ff ff ff
|.Z..LIOR<.......|
00000010 00 00 12 00 d1 58 73 55 50 91 95 95 49 97 b6 e6
|.....XsUP...I...|
00000000 10 5a 0b 00 4c 49 4f 52 3c 02 00 00 ff ff ff ff
|.Z..LIOR<.......|
00000010 00 00 12 00 d1 58 73 55 50 91 95 95 49 97 b6 e6
|.....XsUP...I...|
```

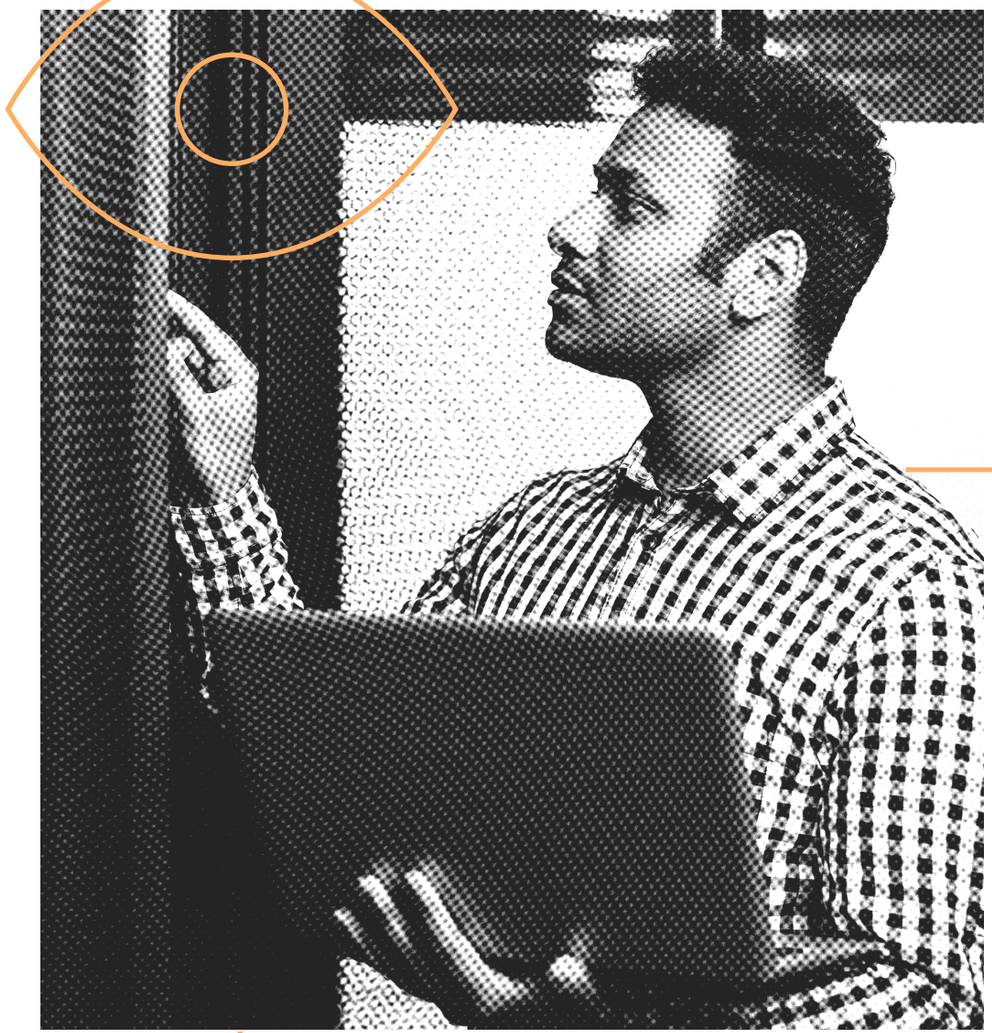
Alternatively, a user could check the local Windows system to determine whether the service is running by going to the Start Menu, then Control Panel, and clicking on the "Programs and Features" section. There should be an option to "Turn Windows features on or off." From this window, we can scroll down to find an entry labeled "Microsoft Message Queue (MSMQ) Server." If these checkboxes are enabled, this means the service is running.

What Censys Sees

Censys has found that since deploying its MSMQ scanner, **over 465,000 hosts have been observed** running the MSMQ service. Censys is able to parse results by continents and countries, and could therefore observe that Hong Kong is the most significant user of MSMQ, with over 35% (167,418 hosts) of the total MSMQ hosts running this service on the internet.

As for the types of networks this service has been observed running in, Censys saw a mix of enterprises, cloud hosting providers, and general broadband internet service providers.

You can find the Censys Research Team's full response to the MSMQ critical vulnerability affecting web servers here.



For Defenders: Our Web Servers Have Been Hacked. What Do We Do?

If your Censys Search investigation has turned up evidence of a hacked server, you may have a bit of a challenge ahead of you. However, there are a great deal of helpful guides and tools from people who've been in your shoes (and there are many who have, you aren't alone!) which may prove useful if you're reacting to a breach. Dreamhost and Sucuri both offer guides on cleaning up after a website hack, which are both great first steps. You may also want to:

1 Minimize the Damage

Initially, you'll need to remove the problematic content, restore the site from a backup, close security gaps that you've uncovered after tracking the attack(s), and add some security tooling around the site in order to prevent future issues.

Ideally, you'd want to react by reinstalling your breached systems onto an updated, secured platform, but we realize that's very often not a realistic option for most companies.

2 Identify Possible Adversary Routes

As Censys never attempts to gain access to any of the hosts across the internet (we strongly believe in good internet citizenship) we don't collect any data on how a server is hacked. However, Censys data can help you identify the possible routes that an adversary took to access your system.

An example would be that perhaps an attacker left FTP on, which you would be able to see with a bit of forensic analysis. This creative analysis is key so that you can determine what happened to close the security gap and prevent it from happening again.

Censys can give you the critical visibility into Internet-exposed services that you need in your threat hunting efforts, and help you find attacker trails and behaviors in order to track, pivot, and protect your organization.

3 Remember: Knowledge Is Power

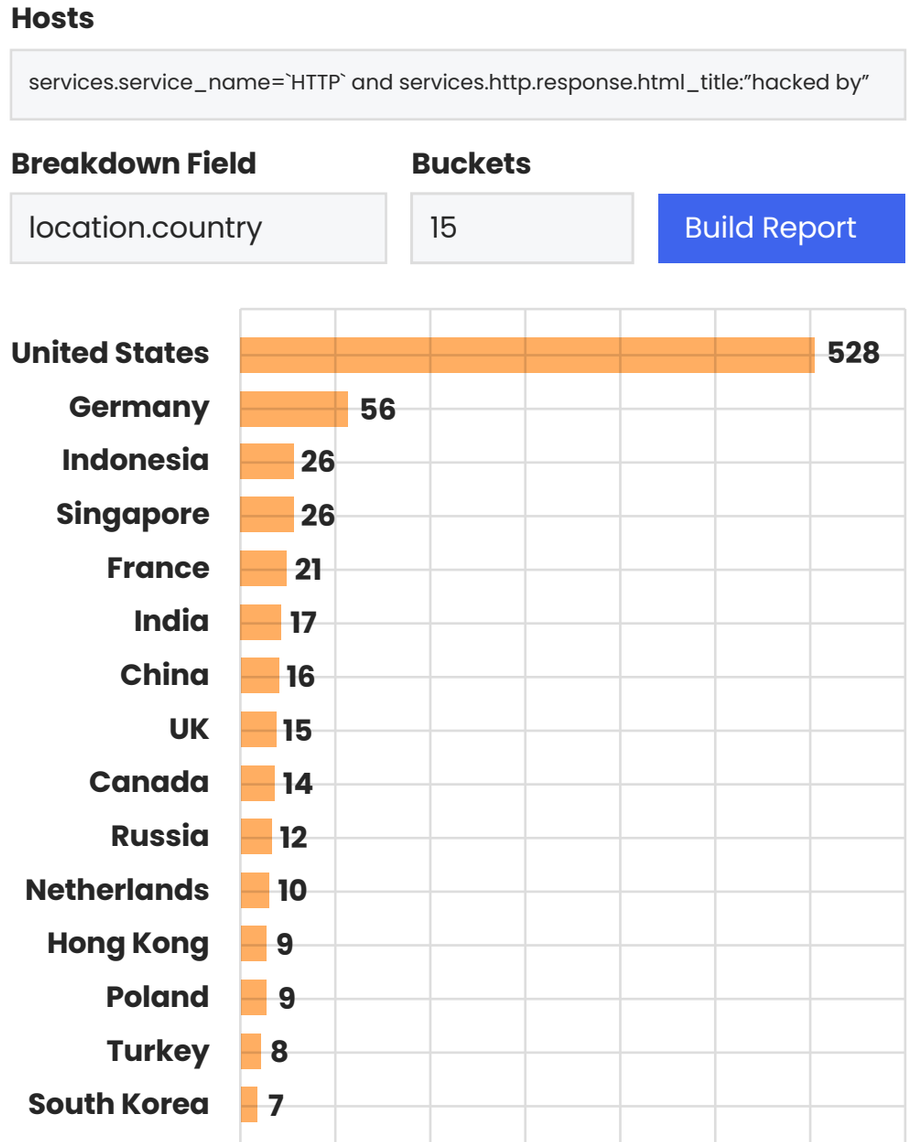
Even though finding that you've been affected by adversaries can feel like a defeat, you've still done the work to locate those problematic hosts and address the security gap before it gets any bigger. Without the knowledge that you have hacked web servers tied to your organization, threat actors could continue damaging your systems for years to come.

For Researchers: Discovering and Tracking Hacked Server Trends

Now let's turn to how researchers can use Censys Search to identify and understand hacked web servers! If you're a researcher, the types of security trend data you can uncover in Censys can be highly useful for supporting existing research projects and brainstorming new projects. To get started, a suggested first step is to analyze data on a global scale with Censys searches, relying on our report builder function.

Step 1: Building a Report

Let's build a report from the search results we uncovered earlier in this ebook, aggregating by the country each web server is hosted in using the "location.country" field. We can make the data more or less granular by adjusting the "Number of Buckets" field. This report reveals that the United States dominates, with 3.46% of hacked servers hosted in the U.S.

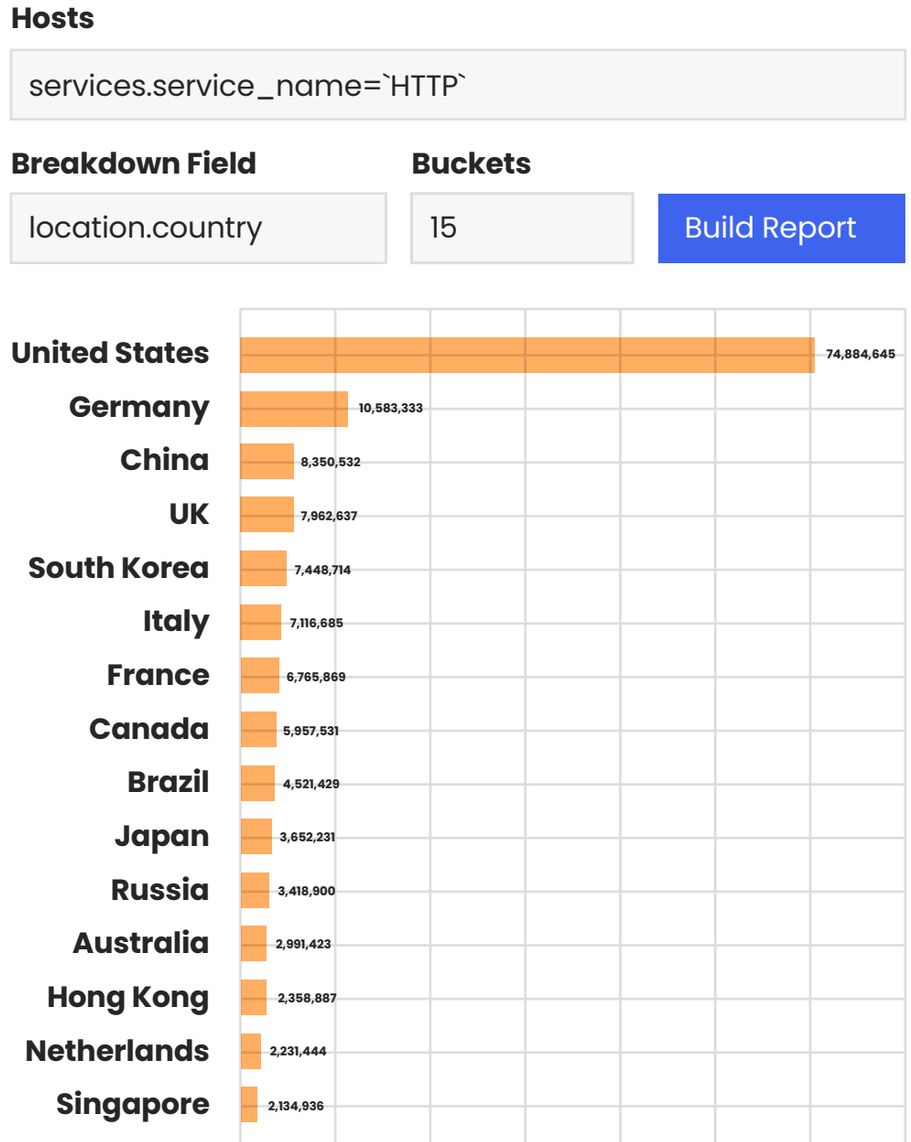


But this chart on its own is misleading. If all you were to do is to take those results at face value and make interpretations around it, you'd likely draw some false conclusions. An important distinction to make in this report is that hosts aren't distributed evenly around the world. The U.S. hosts a good deal of the IPv4 address space, so this trend data may be unfairly skewed toward that country. Think about it this way: if two countries each have 20 servers reporting "hacked by", but the first country has 100 servers and the second has 10000, that's a 20% rate vs a 0.2% rate of "hacked by" instances.

Step 2: Gain More Context

What we need to do next is start adding context into the picture. In this example, we'll tie together two sets of results from Censys:

1. The number of HTTP servers with the string "hacked by" by country
2. The number of total hosts running HTTP by country (see the figure right)



When we scale the “hacked by” values (the first data set) by the number of web servers in each country (the second set), filtering out countries where the former value is trivially small (n<5), we see a different picture.

Tables 1 and 2 break down the top 10 and bottom 10 instances of “hacked by” per capita web servers for those countries. Surprisingly, Indonesia leads the pack as a percentage of population at a rate of about triple the second-place country Singapore, but that may be due to the smaller web server population in that country compared to Singapore.

Italy, by contrast, has the lowest rate of defaced web servers from our perspective. It’s interesting to study various factors that may explain these findings, which may point to the opportunity for a broader study.

Table 1: Most Hacked Servers by Country

Top 10 Affected Countries per Capita Web Servers

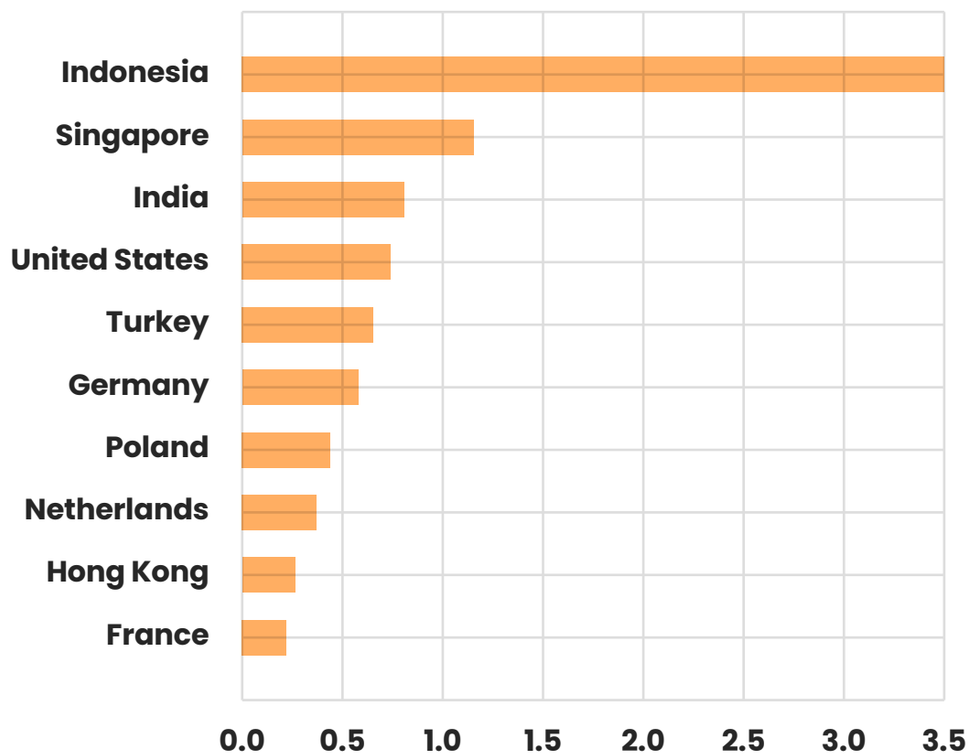
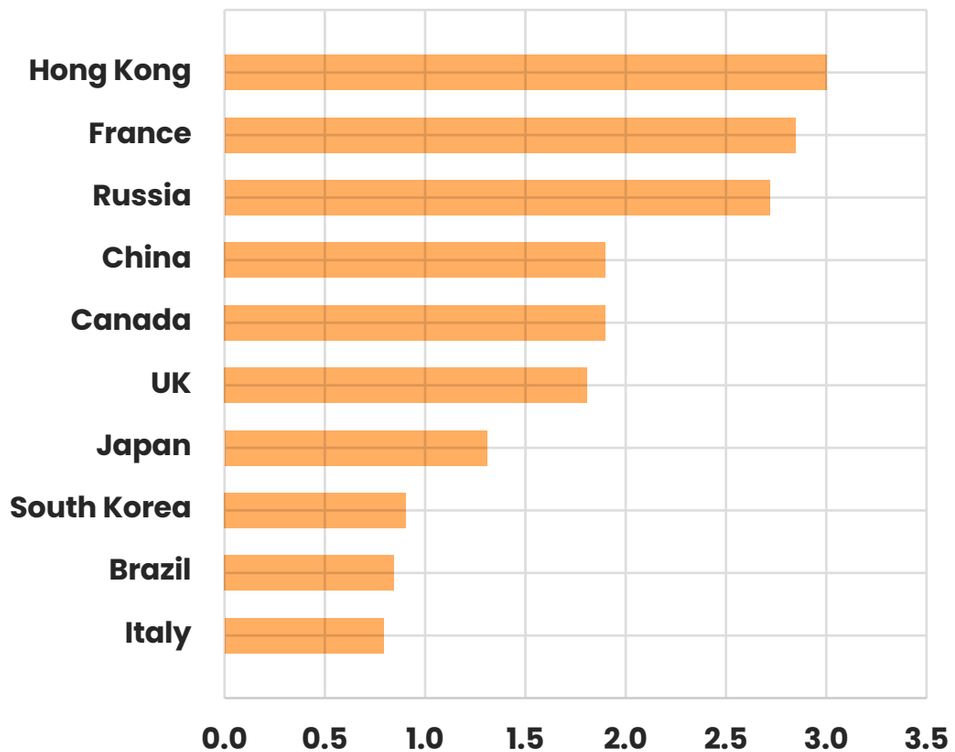


Table 2: Least Hacked Servers by Country

Bottom 10 Affected Countries Per Capita Web Servers



Step 3: Continue Asking Questions

These data points can lead to a larger question: what attributes, regulations, and social trends could potentially impact why Indonesia or Iceland, for instance, would have more hacked websites per capita than other countries. As you can imagine, internet data alone isn't enough to demonstrate causation, but it can be used to pull together interesting data trends to support a huge variety of research projects.

Gaining a Global Perspective on Internet Security

Internet intelligence can uncover what we don't know about our own organization, while also illuminating real-time data trends that tell a bigger story about global internet security.

Finding hacked web servers is just one simple example that we hope will get you thinking creatively about how you can explore our leading internet intelligence with Censys Search. With our broad, global perspective and the depth of relevant security data we make searchable, users have a wealth of intel at their fingertips that they can apply to their own cybersecurity and research efforts.

Next Steps with Censys

Start your own search by visiting our Censys Search tool at http://search.censys.io! Interested in learning more about how Censys can support your cybersecurity or research efforts? We'd love to talk. Reach out to us today to start a conversation at http://censys.com/contact.

The one place to understand everything on the internet.

Censys is the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. We provide governments, enterprises, and researchers with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats. Censys scans 63% more services than the nearest competitor across the world's largest certificate database (>10B), reducing the likelihood of a breach by 50%.

Founded by the creators of ZMap, trusted by the U.S. Government and over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the Internet.

censys