

0 0 0 0 0  
X 0 0 X

THE THREAT PROFILER'S PLAYBOOK

# 6 Steps to Uncovering Ransomware

(& Other Nefarious Activity)



0 0 → 0 X

# Introduction

In the Wild West that is the global internet, it can sometimes feel as though nefarious activity lurks in every corner. [Nation state-sponsored cybercrime is on the rise](#), ransomware is being used to target even the most neutral of parties, like schools, and hackers are finding new and creative ways to breach systems.

For as much good as the internet has to offer (and we know there's plenty), it's terrain not without risks to the average organization or agency. And that is, of course, why threat profilers have such an important role to play.

But as you know, threat profiling is easier said than done. Not only do you have to figure out where to look for threats, but once you find one, you must determine whether or not it is actually a threat at all. This is where things can get tricky. Teams tight on time and resources (and which team isn't?) don't want to waste effort investigating dead ends. So how do you tell with reasonable confidence that what you're looking at is actually nefarious?

## Embarking on a Proactive Profiling Strategy

We think about this question a lot here at Censys, and it drives our quest for better data and context about internet activity.

In fact, it's one of the reasons the Censys team decided to launch its own proactive search for bad threat actors using our Censys Search tool. We wanted to further explore how we could use our powerful internet scanning data to quickly identify threats and correctly profile them with a high degree of confidence.

With timely geopolitical and cybersecurity trends top of mind, we focused our search on potential threats located in Russia. What we uncovered was a series of hosts with ransomware that we assessed were likely being used for nefarious purposes. In a relatively short period of time, we were able to arrive at some pretty significant findings; and though our efforts were just for exploratory purposes, for other organizations and agencies, these kinds of discoveries can have major implications.

That's why throughout this playbook, we'll be connecting takeaways from our Russian ransomware expedition into broader tactics and strategies threat profilers can use to guide their own threat profiling efforts. Find step-by-step details about how we uncovered Russian ransomware using the Censys Search tool, along with key tips and tricks you can generalize to inform your own approach.

Let's dive in.

## How Does Censys Empower Threat Profilers?

Our powerful internet-scanning capabilities make Censys the one place cybersecurity pros can go to understand everything on the internet. Our industry-leading [Censys Search](#) tool helps threat profilers protect their organizations from advanced threat actors with comprehensive, contextual internet intelligence that enables complex and custom searches.

## STEP 1

# Getting Started: How Do We Profile Threats?

What does a threat look like if it's just hanging out on the internet? That's the question we asked ourselves as we set out on our search for potential threats.

Profiling nefarious threats is tricky. Judging a book by its cover is almost never a good idea, whether it be in law enforcement, military, or online. And discovering all of the makings of an online crime BEFORE it happens does not necessarily mean that the crime would have taken place.

That being said, as you begin a threat profiling expedition, you can follow factual observations from the Censys Search data set to more accurately identify suspicious hosts, capable of criminal activity. By looking at the objective behavior of various entities, we can draw informed conclusions about their likely intent. The goal here is to not just arrive at answers, but to arrive at answers that are critically understood and actionable.

## Access to the Best Data

However, to make these reliable observations, we need accurate, robust data that can provide ample context about what we see. The Censys Universal Dataset, which powers our Censys Search tool, does just that. This dataset offers the most comprehensive view of the internet available, continuously scanning 101 protocols across the top 3,500+ ports on the full IPv4 address space and the top 100 IPv4 ports daily to produce a high-resolution map of the public internet.

If you're going to embark on your own hunt for malicious actors, a fresh data set with the right UX layered on top is also imperative. Coming up short on the ability to use parsing fields or reporting functions could mean investigation delays and dead ends. For context, the Censys Search tool has over 2100 parsed fields.

With the right data at your fingertips, you'll be able to begin your search with confidence.



## STEP 2

# Choose Your First Search Filter

Given recent foreign cybercrime activity and other geopolitical events, Censys wanted to begin our proactive search for threats using geography as a first filter; in particular, we focused on Russia. Though you can start your search by choosing from a number of different filters (ex: operating system, host DNS, software), if you have a region in mind, parsing out by location can be a useful first step.

We began with a large pool of potential threat actors by looking at all hosts in Russia. By searching [location.country=`russia`] on [search.censys.io](https://search.censys.io), we saw that there were over 4.7 million hosts located in the country. You can substitute any country of interest into this same search query when conducting your own search for hosts.

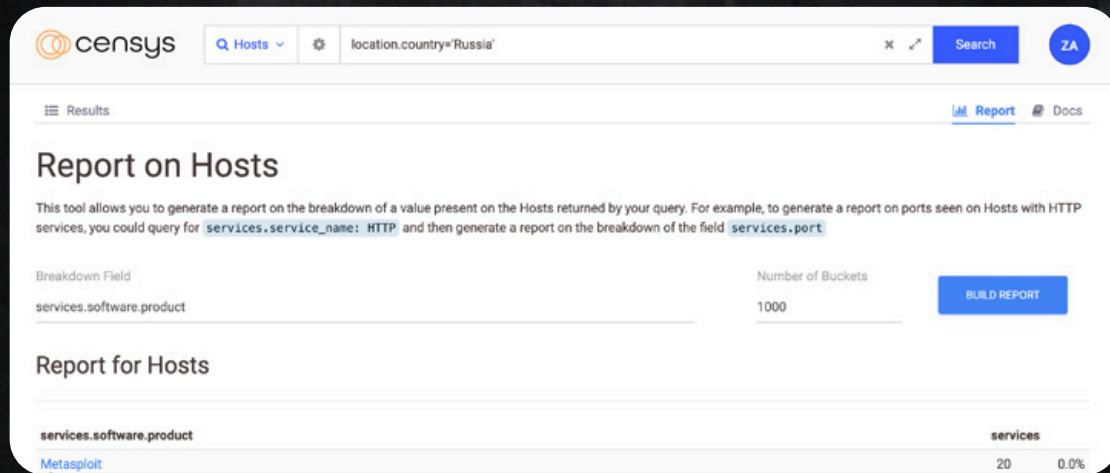
Censys collects a number of different data points about each host it observes, as shown below. This is the information that threat profilers can use to further refine their search and pivot toward interesting or unusual findings when relevant. That's exactly what the Censys team did after their initial host search by location.



## STEP 3

# Keep Your Eyes Peeled for Unusual Host Attributes

Combing through over 4.7 million hosts is beyond a needle-in-a-haystack endeavor, which is why our research team narrowed their focus by looking for potential nefarious software on the hosts. A quick software browse using the Censys “Reports” function shows that there were 10 hosts in Russia with the pentest tool Metasploit.



## Why Was Metasploit Relevant?

Metasploit in and of itself is by no means a smoking gun. It's essentially the software version of a lock picking kit, however its presence doesn't necessarily mean a lock has been picked. But by identifying the presence of Metasploit on these 10 hosts, the research team was able to pivot, and with a seemingly larger group of threat actors using open source penetration testing tools like Metasploit, investigate hosts with this tool.

*This is a worthwhile strategy threat profilers can use in any search: look for commonalities in the data across your set of target observations, and use that to further guide your investigation.*

Our team continued looking at the data that accompanied these 10 hosts, specifically TLS and PROTOCOLS data, and saw that those two of those hosts also contain a “Deimos C2” tool, located in Russia.



## What Is Deimos C2?

Deimos C2 is a command and control tool, which pen testers use to make their jobs easier by allowing them to automate commands to hosts they've compromised. Presence of C2 tools could indicate that a host can or is controlling other hosts, or that the host itself is controlled by a "command" host. Threat profilers who come across Deimos C2 on their profiling expeditions are wise to give it a second look. Again, this is not necessarily an indicator that a crime has been committed since legitimate pen testers use the tool; however, a C2 tool in the wrong hands could mean a compromised or nefarious host.

At the very least, we took it as a sign to keep digging.

Using our data, we were then able to fingerprint the Deimos C2 tool with JARM and pivot to a host in Ohio ("Host D") with Deimos C2. Leveraging Censys' history function, we wound back the clock to uncover `pss.exe` on the host, which is associated with the Karma Ransomware group.

### See For Yourself:

Run This Query: `services.jarm.fingerprint:`

`1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687`



## STEP 4

# Go Back in Time with Historical Perspectives

Learning about a host's current attributes is one thing, but being able to look back at how that host evolved over time can unlock a whole new ball game. Historical data views can allow threat profilers to make connections that would have previously gone unnoticed.

After leveraging Censys' historical data to locate ransomware executables on Ohio "Host D," Censys revisited the original Russian "Host A" for other indicators of nefarious activity. Because the data that's accessible on Censys Search goes back about two years, we were able to take a look back in time at our prime suspect: "Host A."

A historical view can be useful to keep in mind as you conduct your own search, particularly if you've uncovered a suspicious host and have run into a wall about the current state of data, want to observe the host at the time of an incident, or want to see changes in its posture to uncover anomalies or attempts to hide indicators of nefarious activity.

In our case, pulling the historical view of "Host A" ultimately led us to our discovery of ransomware.

5.101.5.196

Summary Explore History WHOIS

May 30, 2022 08:49 PM UTC | Hurricane Electric

Service Observed

31001/TCP/HTTP

Changed Fields

- banner\_grab.tls.certificates.leaf\_fp\_sha\_256
- http.tls.certificates.leaf\_data.names
- http.tls.certificates.leaf\_data.subject.organizational\_unit
- http.response.body

Historical Port Discovery

Odd Certificate

PoshC2 IOC

Certificate Pivot

While looking at this host from a historical view, we came across a port that had appeared on the host for the very first time around May 30, 2022, but then was gone just as quickly as it had turned up. What to make of this anomalous port? Our team noticed that on this same day, a new certificate with odd descriptions had also appeared. The certificate's location was also listed as Minnetonka, Minnesota, which seemed odd for a Russian host. The nonsensical words used for other certificate fields prompted a Google search of these fields, which revealed that this certificate was an indicator for PoshC2, another Command and Control tool.

XXO



## What Is PoshC2?

PoshC2 is a C2 framework worth a threat profiler's second glance. It's a free and open source "proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement," developed by Nettitude Labs. PoshC2 documentation also directs that a Python programming language kit be installed on target hosts, serving as another probable Indicator of Compromise (IOC) as well as identifying probable threat actors, should Python software be found on hosts also possessing the PoshC2 certificate.

### See For Yourself:

Run This Query: `services.jarm.fingerprint:`

`1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687`

00X



PoshC2



XX0X



## STEP 5

# Pivot on Interesting Findings

You never know where an unusual observation may lead you. In our case, by focusing on the PoshC2 certificate, we made a breakthrough discovery. We queried the Censys Search tool to pivot and show us all of the other hosts that had this same certificate on them. We found almost a dozen other hosts, the most significant of which were two Russian hosts (“Host F” and “Host G” in the diagram on the next page).

Of the hosts we pulled with PoshC2 certificates, we learned that:

- “Host F” and “Host G” contained a malware kit
- “Host E” contained a malware kit
- “Host K” presented the PoshC2 certificate as well as the Python version mentioned by the manufacturer
- “Host K” through “Host O” contained only the PoshC2 certificate

### See For Yourself:

Run This Query: `services.tls.certificates.leaf_data.subject_dn=`C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=PI8055077``

“Host F,” located in Russia, contained executables to disarm or disable antivirus software, as well as a Trojan. But more interestingly, it contained a callback to Bitcoin “Host I” and “Host J.” The fact that this is set up for the collection of Bitcoin payment is yet another clue that suggests nefarious behavior (possible

cash repositories for Bitcoin payouts during a ransomware attack), but it doesn’t prove it.

However, in the historical host information for “Host F,” we can see the domain, `decorous.cyou` appended to the nefarious executables that indicated ransomware capabilities. This domain was identified in CISA Alert (AA22-181A) as an IOC for the MedusaLocker group as an actor in previous ransomware attacks. This is where referencing trusted, external references like CISA Alerts pays off. The CISA Alert confirmed that the `decorous.cyou` address was used to accept payments from the victims the ransomware had affected.

With this, we had our smoking gun.


```
HTML Title Directory listing for /
Response Body EXPAND
# Directory listing for /
* * *
* [ANY_DESK.bat.restoreassistance_net@decorous.cyou] (ANY_DESK.bat.restoreassis
tance_net%40decorous.cyou)
* [defender+malwar.bat.restoreassistance_net@decorous.cyou] (defender%2Bmalwar.
bat.restoreassistance_net%40decorous.cyou)
* [NG.bat.restoreassistance_net@decorous.cyou] (NG.bat.restoreassistance_net%40
decorous.cyou)
* [ngrok.exe.restoreassistance_net@decorous.cyou] (ngrok.exe.restoreassistance_
net%40decorous.cyou)
* [VmManagedSetup.exe.restoreassistance_net@decorous.cyou] (VmManagedSetup.exe.
restoreassistance_net%40decorous.cyou)
* * *
```

# Link Analysis Diagram

## SYMBOL LEGEND

-  Exploit/Initial Access Tool
-  Command & Control (C2) Tool
-  Forward/Proxy Tool
-  Possible Malware Kit
-  Confirmed Malware Kit
-  Ransomware Package
-  Bitcoin Host

## FLAG LEGEND

-  Russia
-  China
-  Ohio, U.S.
-  Virginia, U.S.
-  California, U.S.
-  New Jersey, U.S.
-  Taiwan, U.S.
-  Netherlands, U.S.



## STEP 6

# Bring It All Together

What did we determine from all of our digging? Based on our findings, we concluded that the initially discovered Russian “Host A” and “Host B” with Metasploit and Deimos C2 are possible initial command hosts used to set up ransomware architectures. Russian “Host F” and “Host G” possess malware that’s capable of disabling anti-virus and performing a ransomware attack, with beacons to two Bitcoin nodes that likely receive ransomware payment from victims; they are likely the hosts that initiate compromises of either proxy victims or ransomware victims. The link of “Hosts F” and “Host G” to initial “Host A” is circumstantial based only on the existence of the PoshC2 certificate and being hosted in Russia – further analysis with other data types is required to conclude or rule out any direct connection.

Though our threat profiling research was purely exploratory in nature, you can see how government agencies, private corporations, and other organizations prone to attacks have much to gain from uncovering these kinds of threats. The ability to profile threats with a high degree of confidence makes it possible to identify similar behaviors to proactively defend against future attacks, and in some cases, even obstruct attackers from acting in the first place.



# Plays for Any Threat Profiler

Let's review how any threat profiler can use a tool like Censys Search to identify threats and gain the context they need to draw conclusions with confidence.

### 1. Choose the Right Search Filter

Where do you want to look for bad actors? Once in the Censys Search tool, we started with geographic location, which we found was an easy way to make the scope of our search more manageable. However, if you're unsure about region, you can also search by host type, protocols, etc. Based on the kinds of threats your organization has seen in the past, you'll likely know which filter makes the most sense for your efforts.

### 2. Keep an Eye Out for Unusual Host Attributes

We used the Censys "Report" function to browse software instances and determine what was on the hosts we pulled from Russia. There are a number of different attributes you can look at using this Report function, including operating system, DNS, protocols, etc. Looking at software, however, will usually be the quickest way to determine if a host is home to nefarious activity.

### 3. Get a Historical Perspective

Because Censys data goes back two plus years, we were able to take a look at the original Russian hosts to discover it also had a PoshC2 certificate. You can use the Search tool's historical view to understand how activity on a host may have changed over time.

### 4. Pivot on Interesting Findings

By choosing to focus on the PoshC2 certificate we uncovered with our historical view, we unlocked a path to the Medusa locker hosts (ransomware) and the Bitcoin payout hosts, which was the smoking gun we needed to make our conclusion. Don't be hesitant to follow new leads as you conduct your profiling.

### 5. Bring It All Together

Use the data you've collected to make an informed hypothesis about your findings. Keep in mind that what you've found may not lead to a definitive conclusion, and it may warrant additional exploration. If you do feel confident that you've uncovered something nefarious, be sure to identify the right stakeholders as needed. To report anomalous cyber activity and/or cyber incidents 24/7 email [report@cisa.gov](mailto:report@cisa.gov) or call (888) 282-0870. To report an IT Vulnerability, please use this form: <https://www.kb.cert.org/vuls/report/>

## Tips to Keep in Mind

- Don't underestimate interesting findings; if something seems unusual, there's good reason to follow its trail. Be patient as you explore multiple leads.
- Use Open Source Intelligence Tools (OSINT) as a complement to Censys Search to dig further into the host data when needed.
- If your suspicions are raised, keep looking! There's always a parsed field or a data type that you can look for within the Censys Search data set.

# Proactive Threat Profiling with Censys Search

Access the best internet intelligence on the market with Censys Search. Our global scanning infrastructure collects information on more of the internet (and at a higher frequency) than any other tool, and our ground truth scan data is enriched with multiple internal and external sources to provide complete context on each asset's configuration and level of exposure. And, your threat hunting exercises can become more pointed with an easy-to-use query language and 2100+ parsable data fields, giving you the flexibility you need to locate attack infrastructure, write risk detections, and identify compromised hosts.

Censys Search also continuously scans 101 protocols across the top 3,500+ ports on the full IPv4 address space and the top 100 IPv4 ports daily (that's 2x more than the nearest competitor) to produce a high-resolution map of the public internet, providing best-in-class visibility to threat hunters, attack surface managers, and other security professionals. With Censys Search, your team can understand and investigate threats with greater accuracy.

## Why Is Censys Search Data Superior?

- **Structured data and advanced search:**  
Find structured data with detailed information that's indexed and searchable about each protocol and certificates associated with hosts. Ingest data into whichever workflows already exist within your organization, whether you're leveraging the UI or API.

- **More internet hosts and services:**  
Automatic protocol detection, through which Censys identifies services independently of ports, means your team will have visibility into services running on non-standard ports.
- **Multi-perspective scanning:**  
Censys data gives you visibility into 99% of active IPv4 hosts on the internet, thanks to scanning from five Tier-1 service providers from separate locations around the world.
- **Detailed historical host data:**  
All users have access to historical data via UI and API, with significantly more detailed information than our competitors.
- **Fast lookup API:**  
Utilize Censys data programmatically via the Censys API, which provides detailed information about current or historical assets.

When it comes to your next threat profiling expedition, up your game with access to the best internet data available anywhere. Gain more visibility, get more context, and uncover more insights so that you can critically understand and take action on the threats facing your organization. Learn how Censys Search can empower your efforts at <https://censys.io/data-and-search/>.

X00  
00

0

0X X0

0



## The one place to understand everything on the internet.

For security pros who protect the organization, Censys is the best at finding exposures attackers will exploit. Our industry-leading Internet scanning platform and >9.1B certificate database (the world's largest) enable us to provide 63% more service coverage than our nearest competitors. Founded by the creators of ZMap, at Censys we've made it our mission to make the Internet a more secure place for everyone.

[hello@censys.io](mailto:hello@censys.io)

[www.censys.io](http://www.censys.io)