

How to: Threat hunting and threat intelligence

blog.apnic.net/2021/10/21/how-to-threat-hunting-and-threat-intelligence/

James Shank

October 21, 2021



This APNIC [network security series](#) on threat hunting has so far covered a range of great and necessary tools/rules to help you with your threat hunt — it is hard to consider a hunt complete without using at least one of these techniques.

But what does a complete hunt look like? And how does a successful hunt get incorporated into a completed intelligence product? In this post, I'm going to introduce these lofty topics and show some examples.

First, let's define our target. [Finished intelligence](#) is the product of intelligence processes, the end game, the goal. It leverages assessments of data by subject matter experts (SMEs) to help provide context to inform decisions. These are delivered via a report, which contains judgments on possible decisions, including how they were determined and whether they are trusted.



The Intelligence Cycle

Figure 1 — The intelligence cycle is the process of developing raw information into finished intelligence for consumers, including policymakers, law enforcement executives, investigators, and patrol officers. ([Source](#))

Creating completed intelligence that serves a useful purpose requires well-defined intelligence requirements. The end output then informs decision makers on relevant topics. This is what threat hunting should aim to do — find threats of concern and provide data that informs decisions.

What are intelligence requirements?

Intelligence requirements could get their own blog post! Good requirements help the analyst understand their objective and ensure the objective aligns with business needs. To illustrate intelligence requirements, consider the following two examples.

BAD: ‘Alert management each time advanced actors target us using zero-days.’

This is a poorly defined requirement. It is too vague, poorly scoped, and unlikely to inform decisions in a meaningful way.

GOOD: 'Provide a report to management within three days of a detected incident. The report should include details of when and how an attack happened. Include an assessment of the impact of the attack. Include suggestions on what changes may improve detection and prevention of similar attacks in the future.'

This provides a clear scope and clear expectations. It is specific and the output will help to inform decisions. It sets an expectation for the SMEs to guide the audience by asking for suggested changes.

Requirements should be clear in scope and objective and be possible! They should be orientated towards improving the understanding of a topic, situation, or concern.

Before we hunt

To start a hunt, you'll require four things: data, a hypothesis, a why (intelligence requirements), and a time limit.

Data can be many different things — system logs, proxy logs, application logs, binary files, DNS — the list goes on and on. Without data, you do not have anything to hunt.

A hypothesis needs to be clear and testable. It should start with something concrete. This could be a vulnerability, a bit of intelligence, odd behaviour, or anything that might lead to finding unknown threats. This is broad in what it can be but needs to be well defined.

All threat intelligence work requires intelligence requirements. These will help align the output to a business objective or something your organization finds valuable. Hunters may need to extrapolate a purpose from the higher scope requirements. Make sure you can justify the extrapolation, though, or you may end up with a hunt that does not add any value!

All experienced hunters will be very familiar with wasted time and effort. This is part of threat hunting. To ensure things do not run unbounded, set a time limit on your activity. If a hunter thinks success is around the corner and runs out of time, they should discuss it with their peers. A second opinion often helps.

Beginning our example hunt

To take a recent example, Apache 2.4.49 had a vulnerability described by [CVE202141773](#). Team Cymru [published a blog about the total number of systems running this version](#).

Our data for this hunt will be Twitter, GitHub, Shodan, and system logs.

This vulnerability is trivial to exploit. It requires a simple GET or POST request that can exfiltrate data or allow remote code execution.

Our hypothesis will be: ‘Our organization has compromised systems and needs to start Digital Forensics and Incident Response (DFIR)’.

Given that the data for this hunt is at our fingertips, we can set **our time limit** to one day. For this hunt, **our intelligence requirement — our why —** is to answer a simple set of questions. Please spend one day to create a report that answers the following questions, to the degree possible given a one-day time constraint:

- Is there reason to believe we have been impacted by the CVE-2021-41773 vulnerability?
- Should we start DFIR activities?
- What defensive actions should, if any, should we take in response to CVE202141773?

Twitter search

Twitter often provides useful near real-time information as researchers discover things about software bugs. For this search, we can use ‘CVE202141773’.

We find a clear and simple example of a one-line command to exploit this vulnerability:

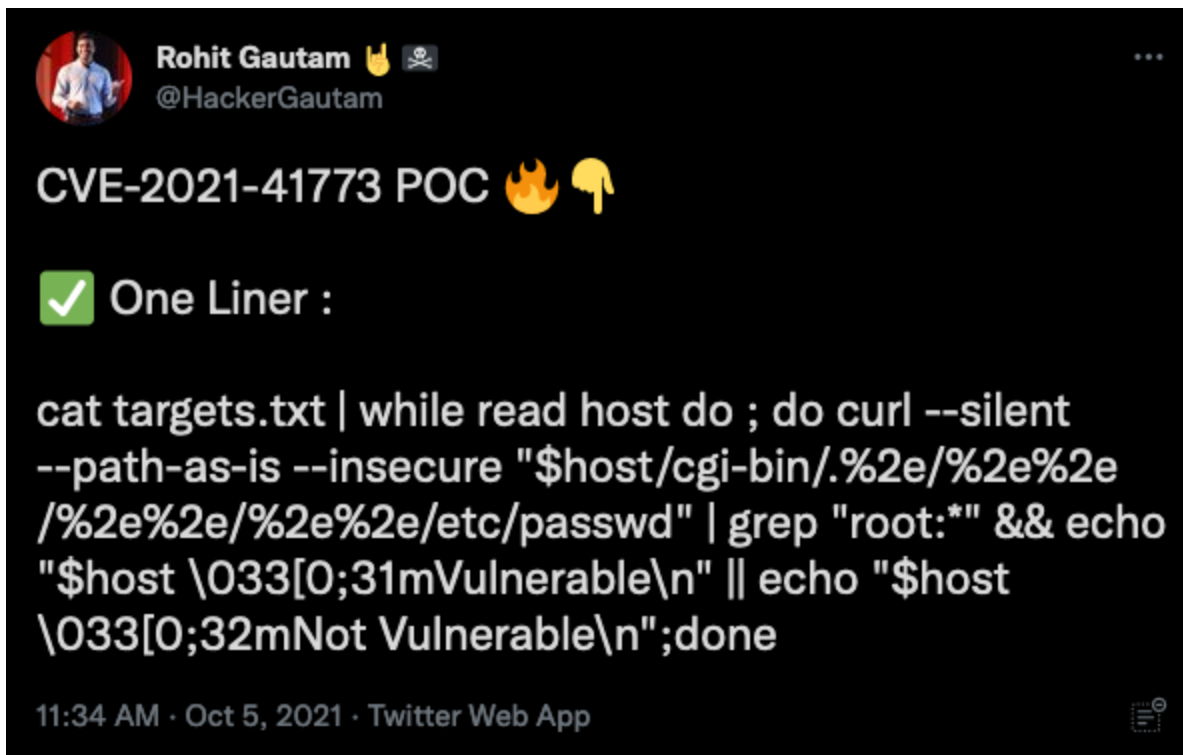


Figure 2

— Tweet showing method to scan hosts and determine vulnerability to CVE202141773.

([Source](#))


We find several other tweets showing similar easy-to-use commands for this vulnerability.

We also see a US CISA post tying CVE202141773 to CVE202142013. The following tweet links to an article explaining that the v2.4.50 patch introduces another vulnerability:



US-CERT  @USCERT_gov · 3d



 Active scanning of Apache HTTP Server **CVE-2021-41773** & CVE-2021-42013 is ongoing and expected to accelerate, likely leading to exploitation. Please patch immediately if you haven't already—this cannot wait until after the weekend. Read more: us-cert.cisa.gov/ncas/current-a...



 8  291  291 

Figure 3 — Tweet linking CVE202141773 and CVE202142013. ([Source](#))

We also find a tweet showing a Shodan screenshot. This shows 112,756 worldwide service ports listening with this version.



CyberDyn999
@CDyn999



CVE-2021-41773 > Shodan Results.

Ouch



5:56 PM · 10/5/21 · [Twitter Web App](#)



Figure 4 — Tweet showing Shodan search for Apache 2.4.49. (Source)

Shodan search

Our first search is for Apache/2.4.49. This shows a count of 67,891 services listening as of 11 October 2021. Previous counts seen in tweets were higher! This is a good sign of patching progress worldwide. Shodan counts represent listening services counts, not host counts. The number of affected systems is less than this count, as many systems running Apache listen on 80 and 443, with some listening on several other ports.

Shodan presents an interface to query different host details exposed across the Internet. We will use this to assess the general scope of concern.

Next, we can search for 'Apache/2.4.50' and get a count of 13,568 listening services. These services are vulnerable to the second vulnerability, CVE202142013.

TOTAL RESULTS

13,568

TOP COUNTRIES

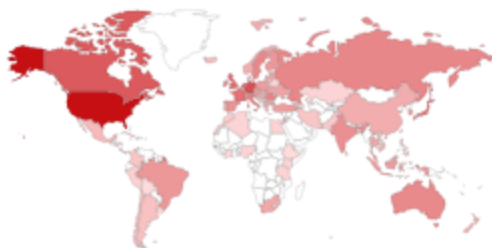


Figure 5

United States	5,724
Germany	1,251
Canada	935
Netherlands	820
United Kingdom	574

[More...](#)

— Shodan search for Apache/2.4.50 from 11 October 2021.

NOTE: These counts are for worldwide services that are vulnerable. Paid Shodan allows filtering to a specific network.

GitHub search

GitHub is often the place researchers share code that demonstrates vulnerabilities. We'll search GitHub for 'CVE202141773'. We can then sort by 'Least recently updated'. This should give us an idea of when public Proof of Concept (POC) code became available.

Note: In our environment, we were not vulnerable to this flaw. These logs simulate how a successful retrieval of /etc/passwd would look.

Time to report

We've so far shown how to perform the hunt. This alone does not get us to a finished intelligence state. We have refined data now that helps us to form conclusions.

We now need to create a finished intelligence product. For this, use a template to match your intended audience. The example report included offers a simplified format suitable for executives and technicians.

[Example_Threat_Intelligence_Report for CVE-2021-41773Download](#)

Organizations today are struggling to keep up with the modern-day threat environment. It takes time, it takes talent, and it takes tools to be successful. We covered some tools and techniques here that can get you started. Happy hunting and stay safe out there!

James Shank is Chief Architect of Community Services and Senior Security Evangelist at Team Cymru.

Rate this article

The views expressed by the authors of this blog are their own and do not necessarily reflect the views of APNIC. Please note a [Code of Conduct](#) applies to this blog.