

CASE STUDY

Hunting in The Home Lab: Putting Cyber Threat Intelligence into Practice

Arch Cloud Labs implements hobbyist-friendly solutions like Pulsedive Community and Pro to research, track, and share wide-ranging personal security projects, from investigating cryptojacking malware actors to hunting for CVEs.

Threat Intelligence for the Community

Home lab enthusiasts experience a frustrating lack of access to key threat intelligence tools and services used by professional security analysts, incident responses, hunters, and reverse engineers.

Often, limited or out-of-range pricing and licensing options set by intelligence vendors exclude independent researchers and home users from the benefits of the latest threat intelligence research.

Arch Cloud Labs set out to find, evaluate, and share affordable (including 100% free!) resources. The goal was to help all security enthusiasts interested in threat intelligence know where to look and share best practice examples to get the most out of the top cybersecurity community resources.



Coffee Meets Feedback

Pulsedive and Arch Cloud Labs first met virtually for a Pulsedive Pro user feedback session. We bonded over our shared appreciation of great Black Friday deals and strong coffee.

KEY INFORMATION



Arch Cloud Labs is a personal security home lab and blog run by Jared, a Professional Security Engineer.

Currently hosting a handful of honeypots, SIEMs, and various virtual machines, Jared uses Arch Cloud Labs as a space to test new technologies, investigate ongoing threats, share tutorials, and openly disseminate findings with the security community.

Follow Arch Cloud Labs

www.archcloudlabs.com

Github: [archcloudlabs](https://github.com/archcloudlabs)

Twitter: [@DLL_Cool_J](https://twitter.com/DLL_Cool_J)

Pulsedive features used:

-  **Indicator** lookup, enrichment, and pivoting
-  **Threat** infrastructure research
-  **Pro Tier API** for automated & on-demand scanning

“ What I love most about Pulsedive is that it gives me, a home lab enthusiast, the ability to use **threat intelligence data I would not otherwise have access to.**”
- Jared, Arch Cloud Labs

CASE STUDY

Hunting in The Home Lab: Putting Cyber Threat Intelligence into Practice

Maximizing Pulsedive's Threat Intelligence Platform

Arch Cloud Labs first came across Pulsedive in the buzz of Infosec Twitter and discovered its value for multiple threat research workflows. On one hand, Pulsedive provides convenient manual lookup and automated enrichment for domains, URLs, and IPs observed in home lab honeypots to perform deeper investigation and analysis. On the other, the Pulsedive platform helps track known and current threats - supporting new research and correlation. Below are a few key use cases.

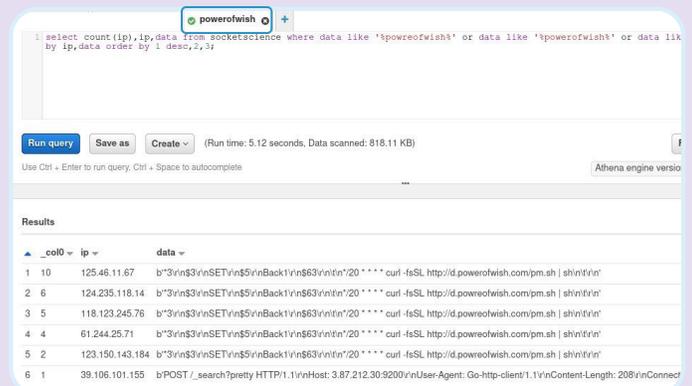
USE CASE 1

Contextualizing Honeypot Data

Context: Arch Cloud Labs hosts multiple honeypots for data collection, storing logs in an S3 bucket, and obtaining data insights via Amazon Athena queries. Athena treats S3 like a SQL backend enabling SQL queries to obtain information from an S3 bucket.

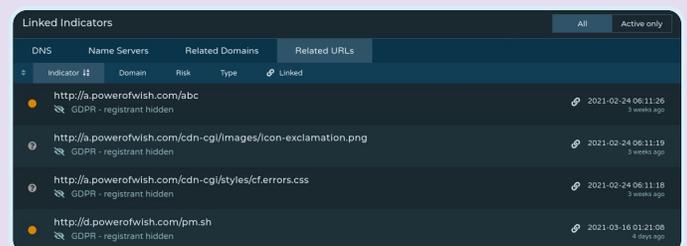
Indicator Enrichment: Arch Cloud Labs found other files hosted on target domains through Pulsedive's **Linked Indicators** section available on every indicator page. By pivoting through other hosts associated with a target domain (in this case, [powerofwish\[.\]com](http://powerofwish.com)), Arch Cloud Labs identified further infrastructure and artifacts.

Running Samples: Arch Cloud Labs subsequently reached out via a download host to see if the files are still hosted externally. Used in conjunction with other free solutions like URL analysis sites and malware sandbox solutions, any home enthusiast can obtain and run samples - even those no longer publicly hosted - to gain insight on process execution without the need to set up their own environment.



Querying the honeypot

Top hits of a particular payload listed in the data column



Enrichment in Pulsedive

Two artifacts of interest related to the domain powerofwish[.]com: pm[.]sh and abc, along with the time the resource was linked to the domain

CASE STUDY

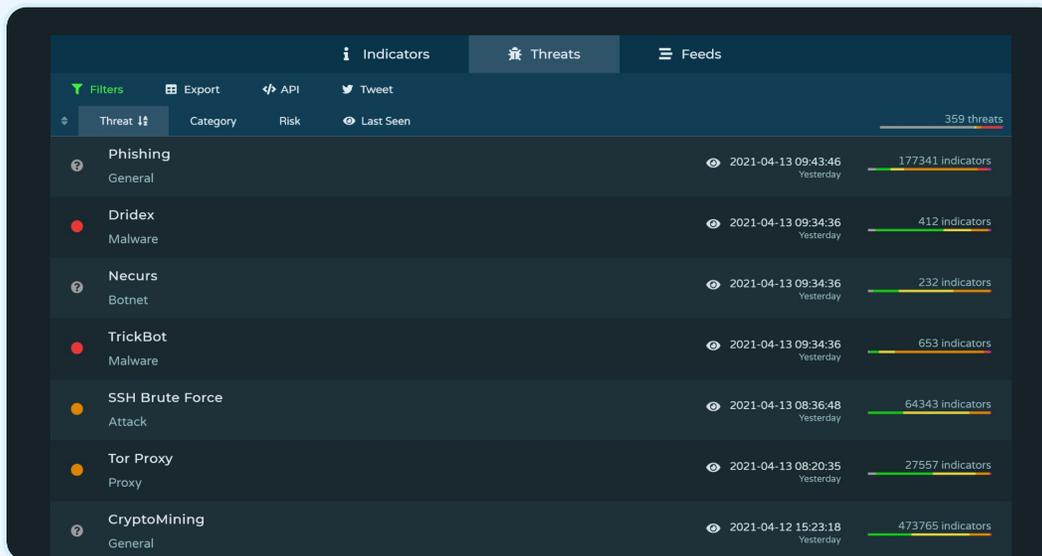
Hunting in The Home Lab: Putting Cyber Threat Intelligence into Practice

USE CASE 2

Hunting For Known Threats

Staying Sharp by Staying Informed: Hobbyists like Arch Cloud Labs keep skills sharp by tracking and researching current threats found in security news headlines, Infosec Twitter feeds, and Reddit /netsec posts. This allows Arch Cloud Labs to recreate existing industry analysis, understand and compare different threats, and contribute to community knowledge.

However, in-depth practical research benefits from access to many levels of threat intelligence - from high-level summaries and news to detailed technical data points. While security enthusiasts are often eager to learn more about the current threat landscape, there are limited free and affordable channels to access comprehensive threat information.



Threat	Category	Risk	Last Seen	Indicators
Phishing	General		2021-04-13 09:43:46 Yesterday	177341 indicators
Dridex	Malware		2021-04-13 09:34:36 Yesterday	412 indicators
Necurs	Botnet		2021-04-13 09:34:36 Yesterday	232 indicators
TrickBot	Malware		2021-04-13 09:34:36 Yesterday	653 indicators
SSH Brute Force	Attack		2021-04-13 08:36:48 Yesterday	64343 indicators
Tor Proxy	Proxy		2021-04-13 08:20:35 Yesterday	27557 indicators
CryptoMining	General		2021-04-12 15:23:18 Yesterday	473765 indicators

Threat Database

Pulsedive Threats are categorized and tagged with various indicators that enable end-user filtering and investigation

pulsedive.com/explore/threats

Arch Cloud Labs uses Pulsedive's free and open threat database to search, filter, and track the latest threats, ranging from general phishing attacks to specific malware variants like **Dridex** and **TrickBot**. Access to Pulsedive's threat profiles provides any security enthusiast with knowledge of reported C2 IPs, malware hosting domains, related news, shared infrastructure characteristics, and additional helpful context for further investigation.

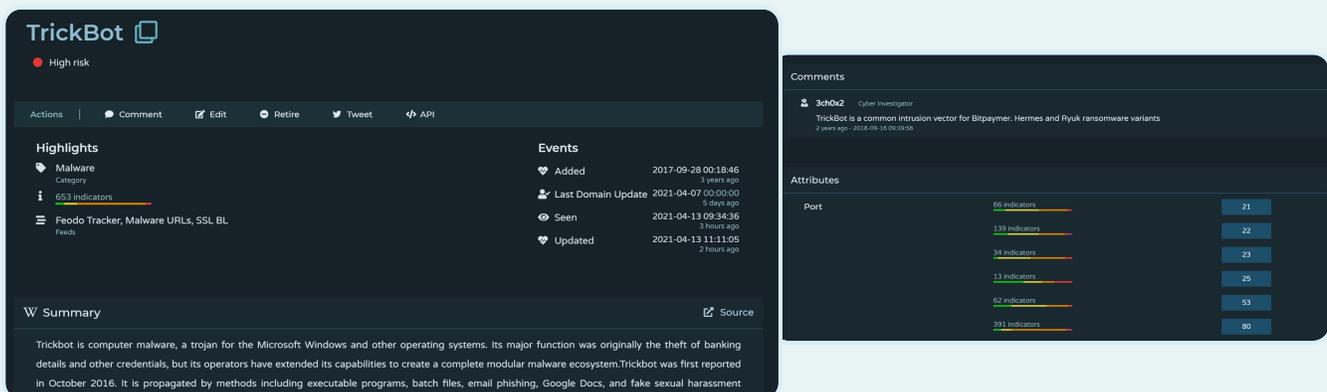
CASE STUDY

Hunting in The Home Lab: Putting Cyber Threat Intelligence into Practice

USE CASE 2, CON'T.

Hunting For Known Threats

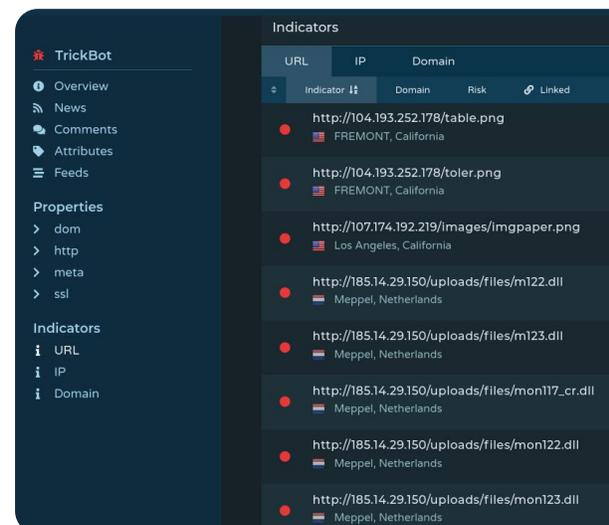
Tackling Trickbot: Most commonly distributed via phishing emails against targeted businesses, a home lab enthusiast typically lacks the visibility into TrickBot that enterprise security operation teams possess. Arch Cloud Labs uses Pulsedive to pivot within living threat profiles to gain unique insights into ongoing activity to bridge this gap.



Trickbot Threat Profile: Summary, overview, user comments and attributes (observed shared infrastructure).

Diving into 'Risky' Business: A favorite pastime of Arch Cloud Lab - identifying odd and overly descriptive file names related to known threats to kick off an investigation. In one particular case, Arch Cloud Labs generated a list of recent TrickBot domains based on risk level and uncovered a series of high-risk URLs resembling files from a college group project.

While the domain was no longer hosting the files when identifying associated IPs, Arch Cloud Labs successfully recovered the files, downloaded samples, and ran analyses by pivoting to complementary free file analysis tools. This combination of tools allows users to recreate analysis in other blogs/reports and find slight differences in prolifically distributed malware samples like **Cryptojacking** variants.



CASE STUDY

Hunting in The Home Lab: Putting Cyber Threat Intelligence into Practice

USE CASE 3

Automated Enrichment & Detection

By leveraging the Pulsedive's scan API endpoint, Arch Cloud Labs has also automated on-demand scanning of IPs from home lab honeypots to rapidly identify if a host is known to be malicious.

Threat Intelligence for All

At Pulsedive, we believe home lab hobbyists like Arch Cloud Labs deserve affordable means to access, pivot on, and integrate with comprehensive sets of timely threat intelligence.

As a community- and user-driven platform, Pulsedive will continue supporting individual user research and intelligence sharing efforts - and look forward to contributing to many projects to come.

```
{
  "iid": 22422369,
  "indicator": "http://helpdeskserver.epelcdn.com/dd210131/init.sh",
  "type": "url",
  "risk": "medium",
  "stamp_linked": "2021-04-05 13:50:40",
  "summary": {
    "domain": "epelcdn.com",
    "properties": {
      "geo": {
        "country": "United States of America",
        "countrycode": "US",
        "region": "AZ"
      },
      "content": [],
      "http": {
        "++code": "200",
        "++content-type": "text/html"
      },
      "whois": {
        "++privacy": "1"
      }
    },
    "domainiid": 19891969
  },
}
```

Automated Scanning

Hit on an indicator returned from Pulsedive API showing risk, known to host malware

Follow & Support Arch Cloud Labs



Learn More

Upgrade

More Data, Fewer Tabs.

Designed for individual security users, Pulsedive Pro provides even more data built right into the Pulsedive interface and integrated with other tools. Pro adds screenshots, higher API limits, critical-risk feeds, third-party integrations, and more - complete functionality to streamline threat intelligence investigation and analysis. The result?

Easy triage, research, and integration, *without* the enterprise price tag.