TEAM CYMRU

CASE STUDY

Threat Reconnaissance Lessons from the Private Sector

How government agencies can optimize security and stay ahead of nation state threat actors.

Threat Reconnaissance Lessons from the Private Sector

How government agencies can optimize security and stay ahead of nation state threat actors

TEAM CYMRU

"[Before Team Cymru,] we only had visibility into what was happening within the enterprise perimeter."

State and Federal agencies continue to be targeted by sophisticated, nation-state-sponsored threat actors. The Banking and Finance sectors are similarly targeted by state-sponsored threat actors, and while the motivations may differ, the means necessary to defend against these threats is the same.

This case study details how analyst teams at leading financial institutions are using Team Cymru's Pure Signal™ threat reconnaissance solution and what State and Federal agencies can learn from these banks' game-changing approach to security. The following explores the recon methodology necessary to get ahead of sophisticated threat actors who are looking to disrupt democratic process, interrupt critical services and steal citizen data.

"We were able to see the infrastructure stood up before the phishing emails even went out."

Challenges...

Limitations of Traditional Threat Intelligence Feeds & Reports

"Traditional threat intelligence feeds are a snapshot in time, and they seem to be curated to report some of the older data, while holding back on some newer information," explained a lead analyst. Organizations need freedom to derive their own answers and not rely solely on third-party determinations, which may not be current or appropriate for them. Context is key.

Inability to get ahead of malicious campaigns:

Like most organizations, these firms only had visibility into what was happening within the enterprise perimeter. This meant that network defenders and incident responders had to wait for alerts or hunt for indicators of compromise (IOCs) within their enterprise. Many call the latter threat hunting, but when you discover IOCs within your perimeter, that's no longer a threat. That's a reality.

- APT campaigns are always evolving, highly obfuscated and they come at you repeatedly and relentlessly.
- Financially motivated threat actors find human behavior easy to exploit and difficult to correct, even with extensive security awareness training.
- Given the retrospective nature of traditional threat intelligence services and inherently reactionary security solutions, preventing recurrence post incident is a huge challenge.

Detecting scanning and determining intent:

Vulnerability probing is usually extremely difficult to detect, and it's even more difficult to determine what threat actors are probing for.

sales@cymru.com

TEAM CYMRU

Proactively seek cyber threats at internet scale.

The financial organisations we researched decided to leverage their threat analysts in a more proactive and strategic way. Implementing the Pure Signal™ platform gave these analysts the ability to apply network forensics to the Internet as a whole.

Instead of solely searching within the enterprise for IOCs and chasing down security alerts, analysts are now able to take a bit of intelligence gathered from a previous security incident or from other sources and trace threats back to their origins. Despite relays and other obfuscation measures the perpetrators have taken, these teams can backtrack to the origin IP address(es) and map out the malicious infrastructures. They are able to monitor their high-priority threats and block them indefinitely. This is what threat hunting is supposed to be.

With internet-scale visibility, the analysts can watch network communications outside their own infrastructure, allowing them to see when their partners and peers are being scanned or are potentially compromised. They can also watch outside systems scanning their own assets, observing this behavior to determine what the threat actors are scanning for.

> "Team Cymru gives us a **10-fold increase** in the amount of threat intelligence we can use."

Outcomes...

Benefits of mapping threat actor infrastructure

Now, these banks have on demand access to global network flows, PDNS and 50 other data types via the Pure Signal™ threat reconnaissance solution. This allows them to monitor state-sponsored threat actors that have historically targeted the financial industry.

During the surge after General Soleimani was killed, one team discovered new command and control servers (C2s) associated with APT 33 and 34. "Our discoveries, in a way, helped defend a lot of the financial institutions out there," explained an analyst.

Monitoring these threat actors in the wild allows Pure Signal users to stay ahead of these types of campaigns by blocking new infrastructure as it is being stood up.

> **"It's a force multiplier and a career enabler."**

Building a complete picture out of the fragments received from other vendors

Malware vendors reported a unique signature indicative of C2 infrastructure. An analyst team is able to monitor that infrastructure via the Pure Signal™ portal and discover new C2s as they are being stood up. "We discover a handful of C2s a month," stated a lead analyst. With this information the bank is able to preemptively block this group and its attacks.

Traditional threat intelligence sources are not only retrospective and fragmented in nature, they can also be inaccurate. This is another reason banks are choosing to gain access to the source of this intelligence, in order to make their own determinations as to what a threat is and its level of criticality. For example, one analyst team had open source intel on a UDP DDoS attack.

After accessing Pure Signal data to investigate, analysts realized that it was not actually a DDoS attack and were able to drill deeper to understand what was really going on.

Gaining ground against phishing attacks

A MageCart phishing attempt was made on an employee. The bank conducted malware analysis, then searched for the malware hash and attributes via the Pure Signal solution to identity the IP addresses associated with that malware sample and related malware samples. This allowed them to see those threat actors accessing specific ports and registering domains, which allowed the financial institution to get the upper hand.

In another example, there was a COVID-19 phishing campaign, and the team was able to attribute it to an Iranian threat actor and block it before the emails were sent.

Detecting and determining the objectives of scanners

When a suspect IP showed up on one bank's radar, the analyst team used Pure Signal intelligence to determine that this person had been probing for a sensitive remote vulnerability execution. "We saw him pulling on the thread until we discovered what he was looking for," explained the analyst. "We would not have been able to get a picture of what he was doing globally without this platform." The team could see that he was probing others in their industry as well.

No touch monitoring of their supply chain

As command and control (C2s) servers are identified, these banks will monitor them to see who they are communicating with worldwide. This allows them to determine whether any of their trusted partners have been compromised.

Business Benefits

The Power of Pure Signal™

Team Cymru puts **50+ types** of Internet data into the hands of elite analyst teams.

> **"Global network flow is really difficult to get access to. Some other vendors do that somewhat, but Team Cymru allows us to easily access it on demand."**

The value of threat reconnaissance to public sector agencies...

90%

of the active signatures detected by the government's intrusion prevention system in June 2020 were associated with three specific threats: a remote access tool, click fraud malware and a cryptominer.[1]

How Threat Recon Helps: You can use the signatures of these threats to trace the malicious communications through proxies to their origins, then map and monitor the extended infrastructures. This will allow you to block bad emails before they're sent and detect C2 calls faster.

Shadow IT

is a big problem for US government agencies. As a result of the OMB changing the definition of data center in 2019, the GAO estimated that 2000 IT facilities would continue to operate as access points to federal systems without proper oversight.[2]

How Threat Recon Helps: You can use the beyond-the-perimeter visibility of the Pure Signal™ reconnaissance solution to map your own attack surface, illuminating shadow IT and indications of compromise across your supply chains and extended network of IT facilities.

197 Days

is how long it takes, on average, for companies to identify a breach.[3]

How long does it take government agencies? Traditional network monitoring, endpoint detection and threat intel solutions are leaving you exposed. In most instances, the C2s referenced in the examples herein were not flagged by other tools or feeds.

How Threat Recon Helps: Close detection gaps, accelerate compromise assessments, ensure comprehensive remediation, and prevent recurrence. By seeing your attack surface from the perspective of your attacker, viewing anomalous communications from the outside in, you can identify malicious activity that traditional tools will miss. This also allows you to block more of the extended threat infrastructure, so attackers can't simply use a new malware variant or pivot to the next C2.

[1] Robert Lemos. July 1,2020. DHS Shares Data on Top Cyber Threats to Federal Agencies. Dark Reading.

[2] Larry Dignan for Between the Lines. March 5, 2020. US government agencies have shadow IT infrastructure problem, cybersecurity risks, says GAO. ZDNet

[3] Ponemon Institute. 2020. Cost of a Data Breach Report. IBM

sales@cymru.com

TEAM CYMRU

Prioritize

Which alerts should we focus on?

In a few pivots you can gain context, gauge criticality, and see whether you're dealing with a targeted attack and if others in your industry are being targeted.

Assess

Which systems are compromised?

See all beaconing assets across your organization, including remote workers, cloud servers, and even supply chain IPs that are communicating with malicious IPs.

Trace

Where do these bad IPs and malware lead?

Get an initial view into additional IPs staged to pick up where a blocked IP left off. This also allows you to gain context into the nature of the threat and prioritize efforts.

Map

Where will they hit us from next?

Map out additional IPs across the globe that are part of the extended threat infrastructures, and identify additional malware associated with the threats you're observing.

Enrich

How can we use this to improve SecOps?

Feed additional IOCs into your SIEM/ SOAR to refine alerting rules and operationalize your extended visibility.

Monitor

How do I stay ahead of these threat actors?

Continuously monitor threat infrastructures as they evolve to preemptively block new attacks.

CONTACT US
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

EMERGENCY CONTACT
+1 847-378-3301
support@cymru.com

TEAM CYMRU