HYAS

CASE STUDY
HYAS PROTECT | HYAS INSIGHT

Canadian Credit Union

HYAS Helps a Bank's IT Team Save Time, Thwart Cyber Attacks, and Increase Productivity

Robbing banks is a classic criminal move. Launching an attack on a bank's cyber properties is essentially a modern twist on an age-old crime. Financial institutions like banks and credit unions are especially vulnerable to cyber attacks because they handle massive amounts of sensitive financial information and high volumes of online transactions.

But a virtual heist can have even more wide-ranging implications for a financial institution and its clients. More than just absconding with funds, bad actors can steal or expose the personal information of anyone who does business there as well as other sensitive data the bank may have on its network.

One HYAS client — a Canadian credit union with 1,400 employees and over $11 billion CAD in assets — knew they were at risk. As one of the country's largest financial cooperatives, it is a consistent target for cybercriminals from all over the world.

"Security operations" wasn't even a "known concept" when the credit union's manager of IT cybersecurity arrived in 2014. But times have changed — especially since the COVID-19 pandemic ushered in an escalation of remote work and increased attack surfaces for just about every business.

According to a 2021 report by the Canadian Bankers Association, cyber attacks against Canadian financial institutions increased by 238% in 2020 compared to the previous year. That spike is largely due to the pandemic. But the number and severity of cyber threats continue to rise nearly four years later.

That's why this credit union chose to upgrade its security capabilities with HYAS Protect Protective DNS. In this case study, we'll take a closer look at how the credit union's IT team tackled cybersecurity threats head-on — in some cases, right down to the criminals' doorsteps.

Challenges and Opportunities: Reducing False Positives and the Limits of the Law

The credit union was (and still is) a near-constant target for cybercrime. While its appeal as a target has not changed, its security operations approach has.

Threat Intelligence

For years, the credit union had been using a traditional threat intelligence provider, but when the IT team tried to investigate and understand more about threat actors, their threat intelligence platform fell short.

Phishing

According to the report by the Canadian Bankers Association, phishing attacks were the most common type of cyber attack on Canadian financial institutions, accounting for 41% of all incidents reported. The HYAS client credit union is no exception. With HYAS Protect Protective DNS in place, the IT team has identified (and thwarted) multiple phishing attacks, including direct emails to the organization's employees and Google adware aimed at people searching for credit unions.

Law enforcement

In the United States, the Secret Service, the FBI, the Department of Defense and multiple other agencies have specific divisions that investigate, defend against and prosecute cybercrime.

But as the credit union's manager of IT cybersecurity explains, the Canadian authorities' capabilities for fraud investigation lag behind the U.S.

In the province where the bank is headquartered, he says that "if you walked into a local savings branch with a gun and robbed it and you only got a thousand bucks, you would definitely have a pretty big investigation. But if you send a phishing campaign and defraud the credit union for a hundred thousand dollars — we struggle to get any type of support from the Royal Canadian Mounted Police [RCMP]."

In his province, just two people at the RCMP are dedicated to cyber fraud cases. So the credit union conducts its own investigations. However, they cannot do much more than find and stop bad actors. Only law enforcement can prosecute crimes — so "we needed help," the IT manager says. "When you use threat intelligence as much as we do, you get a large false positive rate because you don't necessarily trust where a lot of that data comes from. We had to demonstrate to them that we had enough intelligence to make a case that could be pursued legally."

Cyber Crime in Canada: A Snapshot

- According to the Canadian Anti-Fraud Centre, there have been over 150,000 reports of fraud in Canada with over $600 million stolen since January 2021.
- Globally, an estimated 400,000 servers were affected by Chinese state-sponsored cyberattack that compromised Microsoft Exchange servers in March 2021. While it is difficult to determine the number of compromises, the Cyber Centre assesses that upwards of 9,000 Canadian servers were very likely vulnerable.
- "State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these specific states. These campaigns target Canada for a variety of reasons, including our association with groups such as NATO and the G7," according to the Cyber Centre's National Cyber Threat Assessment for 2023–2024.

Solutions and Strategies: The Need for Speed (and Fraud Response)

With HYAS Protect and HYAS Insight, the credit union is able to keep its customers safe, defend its own networks and even identify threats toward other financial institutions.

Fraud Response

Fraud response is the number one way the credit union uses HYAS. Here's a real-world example of a cyber attack from the credit union's IT manager:

- A user responds to a phishing
- email and gives the attackers their login credentials.
- Next, the threat actor attempts to log on, trips off the multi-factor authentication
- Without giving it much thought, the user clicks approve' in the login confirmation email
- At this point, the credit union's IT team is alerted because the user opened the email in a Canadian location, while the person trying to log in to the account is in Cyprus

The credit union does have staff working abroad, so the team double-checked to ensure nobody was in Cyprus. (Spoiler alert: This was a real attempt at fraud.)

Speed

"The staff is really quickly able to look up what they need and get the intelligence they need without [having to] sort through a bunch of minutiae and other crap that comes up with other intelligence program products. You don't have to wait for that information. Within the HYAS platform, it's just there. It populates it for you."

Compared to the other solutions the credit union uses, HYAS is much easier to use because "everything is in one window," he adds. HYAS Insight is intuitive, user-friendly, and presents all the necessary information in one place, making it easy to navigate and understand.

Customized Experience

The credit union IT team appreciates the personalized attention they receive from HYAS.

Unraveling an International Cybercrime Ring

It began with a sudden surge in fraudulent losses at the credit union.

Since the lion's share of cyberattacks involve phishing, the IT team suspected phishing was in play. But there hadn't been any reported SMS or email campaigns targeting the credit union's members.

Then, one day, while doing routine administrative tasks, an IT team member stumbled upon a counterfeit ad for the credit union on Google. He didn't know it at the time, but finding that adware was like pulling on a thread that would unravel an international network of cybercrime.

It turned out that the threat actors used (fraudulent) Google Ads to redirect unsuspecting users to phishing sites.

- The team's investigation, with HYAS Insight as a primary tool, proved crucial in identifying the bad actors' patterns.
- The attackers consistently used the same China-based registrar and demonstrated that they had a well-funded operation. Once the bad actors knew they had been spotted, they made a rapid pivot in tactics, with a lag time of only about a day and a half from detection to their next move — a stark contrast to the slower pace of other attackers the IT team encountered.
- HYAS provided unique intelligence, allowing the team to extract WHOIS information and reverse DNS data promptly. This information revealed a pattern in the bad actors' hosting strategy: cycling through compromised WordPress sites hosted on the same service.

"

"The biggest advantage to using HYAS Insight is the speed with which the security team can respond to threats."

– IT Manager

Results — and Reprisals

With the help of HYAS, the credit union has bolstered its security stance as well as its reputation.

In one case, a threat actor launched an email phishing attack that sent credit union members to a fake website. The IT team found the site by using the HYAS Insight reverse lookup feature. They also found four other credit unions that were victims of the phishing scam.

"We advised all four institutions: Hey, there's an active phishing campaign … *This is how you take down the site … Here's all the information you need,*" says the manager.

Three of the four credit unions took the sites down really quickly. But one credit union didn't heed the warning. The threat actor figured out that its employees had weak passwords and pivoted the attack to password spraying. The incident cost that credit union dearly.

> "We're not the biggest client in the world, that's for sure … but even the HYAS CEO makes the time to meet with us and understand what we need to do and where we need to go. HYAS is keenly interested in how we do business and more importantly - how they can help us not only do it better, but help us ensure ongoing resiliency."
>
> **– IT Manager**

The Curious Case of PT Carlos

In another epic takedown, the credit union team identified an actor they dubbed "PT Carlos" and used HYAS tools to gather detailed information on him — like an email address that linked him to Central America.

- By analyzing IP addresses connected to phishing sites, the team recognized a pattern indicating testing infrastructure.
- With HYAS, they pinpointed the threat actor's probable location in Montreal. They also observed his consistent cell phone use, specifically a Samsung Galaxy tab, for domain setup.

"He was very predictable in his approach," says the credit union IT manager. "We found after a while that all of these guys are pretty predictable and you can 'fingerprint' them a little bit. We knew as soon as we'd seen certain hosts, certain IPs, certain exploit kits … Carlos' specifically because we were able to pattern match them."

- Although they were unable to build a national case for the RCMP to investigate, the credit union IT team's proactive takedown requests, based on predictable patterns, apparently became too frustrating for Carlos. A year and a half after he first appeared, the team hasn't seen hide or (virtual) hair of Carlos.

THE MORAL OF THE STORY: Crime doesn't pay — and neither does laziness. Cybercriminals might seem sophisticated and are often well-funded, but that doesn't mean they're particularly smart.

Saving Time Increases Productivity

The credit union IT team hasn't been able to quantify specific cost savings after integrating HYAS into its tech stack. But that doesn't mean they haven't seen a significant shift in productivity.

"What we save is intelligence time. Until HYAS Insight, there weren't a ton of tools that did decent 'whois' lookup," the IT manager notes. "Now, we get all the whois information from the past five years."

> "Because we use HYAS Protect, we are able to act so aggressively that we generally only see attacks for very short periods of time."
>
> **– IT Manager**

Credibility

Another huge benefit of using HYAS: The ability to prove the accuracy of intelligence. Armed with HYAS data, the IT team is able to show its board of directors and executive risk committee that real threats are being identified, pursued, and thwarted.

"It definitely has given us a lot of credibility as an asset in the organization," says the IT manager. This credibility led to two new hires in his department dedicated to cybersecurity.

The IT manager and his team get praise from the credit union CEO and other executives — "when they see you taking names and kicking butt, they say: *You guys are always doing a great job keeping us and our members safe*," he adds.

HYAS Products

HYAS security solutions provide the visibility and observability needed to stay in control of your environment. HYAS solutions are easy to deploy, easy to manage, and integrate seamlessly into any security stack.

PROTECTIVE DNS

HYAS Protect

Protective DNS

Our protective DNS solution combines authoritative knowledge of attacker infrastructure and domain-based intelligence to proactively block malicious communication used by cybercriminals to conduct phishing, ransomware, and other forms of cyberattacks.

Explore HYAS Protect →

THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insights allows you to rapidly discover and investigate any IOC and related indicators. Identify and map out the complete cybercriminal campaign architecture and take a proactive stance against future attacks.

Explore HYAS Insight →

Contact Us For a Demo

hyas.com/contact

HYAS

Protecting Businesses and Solving Intelligence Problems Through Detection of Adversary Infrastructure and Anomalous Communication Patterns

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.