



CASE STUDY
HYAS Insight

Large North American Bank

How One of the Largest North American Banks Used HYAS Insight to Stop a Relentless Russian Cyber Attack

Security Showdown

HYAS received a request for assistance from one of the ten largest banks in North America. With more than 13 million customers, the financial services institution was dealing with a persistent and relentless credential stuffing attack targeting customer accounts. The scale and complexity of the attack presented an extraordinary challenge for its seasoned security and fraud teams.

The bank faced three critical threats: the looming specter of significant financial losses, a potential blow to its brand reputation and the indirect costs of fraud, such as lost productivity among its security teams.

The stakes were sky-high.






“

“HYAS provides us with the critical visibility, intelligence, and answers that we can’t get anywhere else”

– Director, Financial Services Company

Snapshot: A Virtual Stickup

The organization, which provides personal, commercial and investment banking, experienced an ongoing, massive credential stuffing attack and turned to HYAS for help. Here's how it played out:

 The Attack	 The Solution	 The Results
25,000 IP addresses • Deployed via botnet, leveraging network of compromised home routers • Global scope, with adversary infrastructure spread across Africa, Asia, North and South America, and Australia.	Identified more than 17,000 (69%) of affected IP addresses • Geolocated over 9,000 IPs • Pinpointed the attack vector, which used a SOCKS proxy protocol • Identified IP ranges used in the attack • Determined the domains owned by adversaries	Attributed the attack to two Russian adversaries • Identified 200+ global enterprises targeted in the same attack • Reported infrastructure intelligence to FS-ISAC and other threat sharing organizations

Game of Codes: How Credential Stuffing Attacks Work

Defending against credential stuffing attacks is a formidable challenge for organizations of every kind. But what is credential stuffing, exactly?

These attacks begin when threat actors use customers' valid, but stolen or leaked, credentials, typically acquired through dark web marketplaces. Criminals exploit the common practice of customers using identical credentials across various online accounts — then swiftly breach them by systematically testing those credentials on numerous websites via readily available automated tools like Sentry MBA and SNIPR.

This particular client's credential stuffing attack employed obfuscation techniques designed to thwart the bank's fraud detection systems. The perpetrators masked their location and identity by concealing the number and location of the IP addresses they used. They also deployed a botnet that hijacked thousands of residential home routers, which made detecting anomalies in IP traffic and login attempts virtually impossible.



Enter the White Hats: HYAS Insight Identifies More Than 17,000 Global IP Addresses

HYAS Insight gives anti-fraud and other security teams an unparalleled view into current and evolving adversary infrastructure, enabling the identification, monitoring, and blocking attacks to reduce business risk; even before attacks are ever launched.

Within days, this client used HYAS Insight to:

- Identification of the adversary's infrastructure, mapping over 17K of the 25K IP addresses
- Determine the botnet in use (Mikrotik RouterOS)
- Geo-locate over 9,000 IPs to their near-exact location in regions across the world
- Identify the attack vector as a SOCKS proxy using three IP ranges
- Analyze the attackers' Mikrotik scripts, including SOCKS proxy setups, crypto mining codes and backdoors
- Connect IP ranges to domains controlled by the threat actors

After the Attack: 200+ Targets, Countless Consequences for Criminals

The HYAS Insight platform surfaced exclusive datasets that allowed the bank, in collaboration with HYAS, to quickly find the attackers and share intelligence with other cybersecurity organizations. HYAS infrastructure intelligence also:

- Attributed the attack to two well-known Russian adversaries
- Enabled proactive blocking and monitoring of the adversaries' infrastructure, including pre-weaponized infrastructure
- Warned other HYAS customers about the adversaries and attacks
- Shared actionable intelligence with the FS-ISAC and other threat-sharing organizations to protect the industry at large
- Empowered other enterprises to adjust their security postures and fraud detection systems accordingly

Detect and Stop Cyber Attacks with Actionable Intelligence No One Else Has

HYAS infrastructure intelligence synthesizes diverse data types with broad reach, providing insight into attacker activity that helps security teams defend the organization from current attacks and preemptively stop future attacks.



HYAS Products

HYAS security solutions provide the visibility and awareness 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 →



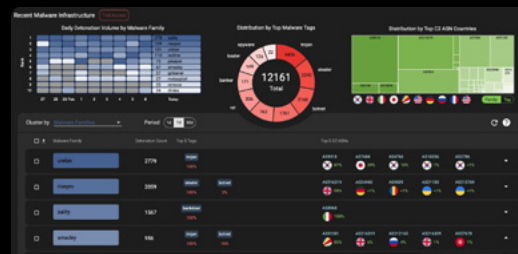
THREAT INTELLIGENCE & INVESTIGATION

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



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.