



## CASE STUDY

# 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 North American banks by assets. 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 insidious, often overlooked indirect costs of fraud, such as lost productivity among its security teams.

The stakes were sky-high.



“HYAS provides organizations unparalleled visibility, protection and security against all kinds of malware and attacks to ensure business continuity.”

## 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

- 25,000 IPs affected
- Deployed via botnet, which itself used hacked home routers
- Global scope, appearing to emanate from locations in Africa, Asia, South America, North America and Australia



#### HYAS Insight as a Solution

- 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



#### The Results

- Attributed the attack to two Russian adversaries
- Identified 200+ global enterprises targeted in the same attack
- Reported adversary and attack intel 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?

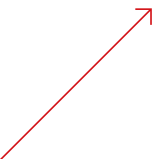
These attacks begin when threat actors use customers' valid, but stolen or leaked credentials, typically acquired through dark web marketplaces. Criminals exploit the common practice of customers using identical credentials across various online accounts – then swiftly breach them by systematically testing 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 threat intelligence and investigation platform provides cybersecurity teams with an unmatched perspective on adversary infrastructure. This intelligence empowers teams to proactively identify, monitor, and thwart attacks before criminals even initiate them. HYAS' tools can even be used to track adversaries right down to their doorsteps in the real world.



Within days, this client used to HYAS Insight to:

- Identify more than 17,000 of the 25,000 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:

- Attributed the attack to two distinct Russian adversaries, including their names, email addresses and phone numbers
- Enabled proactive blocking of domains and infrastructure tied to the threat actors
- Warned HYAS customers about the adversaries and attacks
- Shared high-level details with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other threat-sharing organizations
- Empowered other enterprises to adjust their security postures and fraud detection systems accordingly



## **Detect and stop cyber attacks** **instantly with data and intelligence** **no one else has.**

HYAS provides organizations unparalleled visibility, protection and security against all kinds of malware and attacks to ensure business continuity - independent of any new attack vector, surface, or technique that may be used to breach their environment.

**CONTACT US FOR A DEMO**  
[hyas.com/contact](https://hyas.com/contact)

INVESTIGATE ATTACK  
INFRASTRUCTURE FURTHER  
AND IDENTIFY FRAUD FASTER



### **HYAS INSIGHT**

An efficient and expedient investigation is the best way to protect your enterprise. HYAS Insight provides threat and fraud response teams with unparalleled visibility into everything you need to know about the attack. This includes the origin, current infrastructure being used and any infrastructure.



**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.