HYAS

CASE STUDY

HYAS INSIGHT IDENTIFIES RUSSIAN THREAT ACTORS BEHIND MASSIVE CREDENTIAL STUFFING ATTACK

QUICK FACTS

SITUATION

North American bank targeted by massive global credential stuffing attack

CHALLENGES

- Scale: Large > 25,000 IPs
- Distribution: Global
- Other Factors: Botnet of hacked home routers

SOLUTION – HYAS INSIGHT

- Identification of > 17,000 of 25K IPs (69%)
- Geo-location of 9K IPs
- Identification of SOCKS proxy as attack vector, the IP ranges used, and domains owned by adversaries

RESULTS

- Attribution of the attack to two Russian adversaries
- Identification of > 200 global enterprises also being targeted by the same attack
- Communication of adversary and attack intel to FS-ISAC and other threat sharing organizations

Complex globally-distributed attack targeting over 200 of the largest financial institutions and global brands highlights the need for a pre-zero-day approach to cybersecurity

SITUATION

In November 2018 HYAS was contacted by a large North American banking and financial services firm to help with an ongoing credential stuffing attack against the bank's customer accounts. While the company's security and fraud teams were familiar with and had responded to credential stuffing attacks in the past, this attack was of a scale and level of complexity the team had not seen. With the potential to create substantial direct losses, in-direct fraud-related costs, and damage to brand reputation, the attack had also become a huge drain on productivity for the bank's security and fraud teams.

CHALLENGE

Defending against credential stuffing attacks is very challenging for most organizations because customer accounts are targeted using valid credentials which have been stolen or leaked in a data breach, and usually obtained by threat actors via dark web marketplaces. Knowing that many customers use the same credentials for multiple online accounts, adversaries gain access to customer accounts by rapidly testing credentials on hundreds of websites using publicly available automated tools like Sentry MBA and SNIPR.

The credential stuffing attack against this financial institution was massive, distributed, and employed obfuscation techniques designed to reduce the effectiveness of the bank's fraud detection systems and mask the location and identity of the adversaries orchestrating the attack - most notably:

Number of IPs Used

The attack was distinguished by the use of well over 25,000 unique IPs making it next to impossible for the bank to detect and block specific IPs related to the attack.

Geographic Distribution of IPs

The majority of the IPs used in the attack were located in Africa, Asia, South America, North America, and Australia. As a global operation with customers around the world making geo-IP-based blocking not an option.

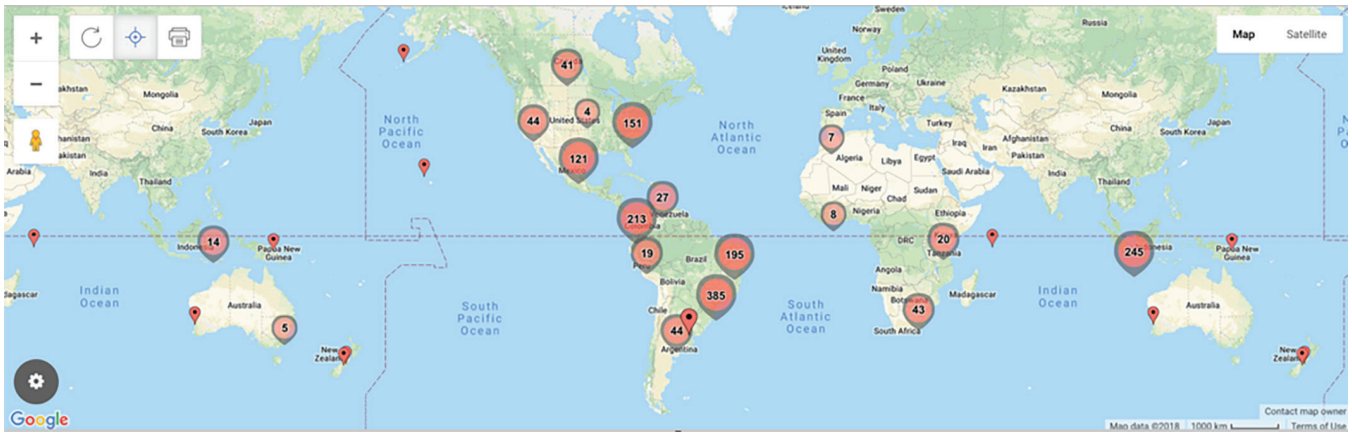
Use of Botnet to Proxy Traffic

The threat actors' use of a botnet comprised of thousands of compromised residential home routers added to the bank's difficulty in detecting anomalies in IP traffic and account login attempts.

SOLUTION – HYAS INSIGHT

HYAS Insight gives cybersecurity teams an unparalleled view into current and evolving adversary infrastructure, enabling the identification, monitoring, and blocking of attacks before they are launched and in many cases the tracking of adversaries to their physical doorsteps. Within days HYAS Insight quickly enabled:

- Identification of over 17K of the 25K IPs as running the Mikrotik RouterOS indicating use of an Botnet
- Geo-location of over 9K IPs to their near-exact location showing the broad geographic distribution of the attack
- Analysis of several Mikrotik attack scripts - socks proxy setup scripts, crypto mining codes, and backdoors
- Identification of the attack vector as a socks proxy allowing instructions from 3 IP ranges
- The tying of the IP ranges to domains controlled by the threat actors



HYAS Insight's Precision IP visualization of the global distribution of the IPs being used in the attack

RESULTS

With access to the Insight platform's exclusive datasets, HYAS and the bank were able to quickly:

- Attribute the attack to two Russian adversaries including names, email addresses, and phone numbers, enabling proactive blocking of any future attacks using the other domains and infrastructure tied to the threat actors
- Communicate the adversary and attack intel to HYAS customers, and share high level details to the FS-ISAC, and other threat sharing organizations, enabling many enterprises to adjust their security posture and fraud detection systems to mitigate this attack

FOR MORE INFORMATION OR TO SCHEDULE A DEMO, PLEASE CONTACT US AT:

Email: info@hyas.com
Web: hyas.com/demo
Phone: +1-888-610-4927

ABOUT HYAS

HYAS provides attribution intelligence and solutions that help cybersecurity teams identify the specific threats targeting their organization and the adversaries behind them. The Insight threat attribution platform gives cybersecurity teams an unparalleled view into current and evolving adversary infrastructure, enabling the identification, monitoring, and blocking of attacks before they happen and in many cases the tracking of adversaries to their physical doorsteps. With it's unique focus and capability of quickly pinpointing the perpetrators of digital attacks, HYAS customers include some of the world's largest financial services, technology, media, and manufacturing enterprises.