SILENT PUSH

WHITE PAPER

CHANGING FACE OF CYBER BREACHES EXPOSES NEED FOR PREEMPTIVE THREAT INTELLIGENCE

A YEAR IN SUMMARY

2024 marked a transformative year in cyber threat intelligence. Rapidly evolving adversary tactics, novel malware proliferation techniques, and the widespread availability of AI-enabled malicious infrastructure scaling methods has made the jobs of security teams worldwide exponentially more difficult.

Dealing with these threats requires a transformative approach. It is no longer sufficient to approach threats reactively. Indicators of Compromise (IOCs) are stale at best, and so the industry turns towards Indicators of Future Attack (IOFAs) to find the answers they need: preemptive, actionable threat intelligence. The ability to stop attacks before they are weaponized.

THE EVER-EVOLVING THREAT LANDSCAPE

Within this white paper, Silent Push provides a mix of technical information, findings and analysis featuring key trends and an overview of major crimeware families to address the changing threat landscape.

Also available upon request is our 50+ page full report. This is a deeper dive with additional analysis that includes strategic recommendations on preventing an attack and how attackers have swiftly adapted to the rise of artificial intelligence (AI) to scale their operations.

Silent Push is continuously expanding our data collection, processing, and fingerprinting capabilities.

KEY STATISTICS

- Hundreds of thousands of Indicators of Future Attack (IOFAs) are provided by Silent Push on a constantly recurring basis to organizations worldwide alongside a similar number of indicators in our Bulk Data Feeds.
- Dozens of blogs and technical reports are published detailing analysis and mitigation needed to stop activities of multiple APTs and major crimeware groups.
- Ongoing collaboration with worldwide partners in law enforcement and the security industry, leads to the disruption and/or takedown of numerous networks and the blocking of countless cyber attacks.

TOP THREAT TRENDS OF 2024-2025

The cybersecurity environment in 2024 experienced rapid escalation in both the volume and complexity of cyber threats. Silent Push analysts noted considerable increases in activity driven by both state-sponsored advanced persistent threats (APTs) and financially motivated cybercriminal groups, including a dramatic increase in sophistication of phishing kits - with new iterations appearing faster than ever before to shift targeting across all industry verticals (financial, retail, technology, energy, etc.).

AI-POWERED INFRASTRUCTURE SCALING

Threat actors leveraged AI to scale operations, enhancing spear-phishing, automating malware, and obfuscating infrastructure, making detection harder.

A key trend we have coined 'Infrastructure Laundering', involves criminals hiding behind mainstream hosting providers to evade scrutiny. Silent Push's research into Triad Nexus, supported by extensive DNS data, has also uncovered troubling links between cybercrime and real-world criminal gangs, particularly Chinese Triads.

ACCESS-AS-A-SERVICE

"Access-as-a-Service" models continue to grow in prominence as well, exemplified by actors like Raspberry Robin, who facilitated human-operated ransomware campaigns by providing compromised infrastructure to other threat groups. These services streamlined the ability of less sophisticated actors to execute high-profile attacks, further diversifying the threat landscape, and have worrisome ties to Russian threats that the industry should keep in mind when defending against them.

CYBER BREACHES ARE EVER CHANGING AND EXPOSE THE NEED FOR PREEMPTIVE THREAT INTELLIGENCE.

SECURITY TEAMS NEED A BETTER WAY TO REVEAL 98% OF HIDDEN THREAT INFRASTRUCTURE.

IOFAS FROM SILENT PUSH MAP THIS MALICIOUS INTENT—AS IT'S BEING SET UP—ENABLING TEAMS TO PROACTIVELY BLOCK AN ATTACK.

FINANCIALLY MOTIVATED THREAT ACTORS

Financially motivated threat actors dominated the cyber threat landscape for 2024, employing increasingly sophisticated tactics against their targets. Groups like FIN7, Scattered Spider, and Crypto Chameleon, and others exemplified the evolution of crimeware, showing a significant willingness to pivot and innovate while combining traditional methods such as phishing and malware delivery with advanced infrastructure management methods.

Financially motivated threat actors remain one of the most persistent and damaging adversaries facing organizations the world over. Their ability to quickly scale operations and exploit vulnerabilities has led to widespread ransomware attacks, credential theft, and fraud.

Collaborative efforts between organizations and threat intelligence providers, such as Silent Push's work in mapping malicious infrastructure and disrupting criminal networks, have proven essential in mitigating the financial and reputational damage caused by these groups. The need for preemptive intelligence and rapid response capabilities has never been greater, as these adversaries continue to adapt and innovate at an alarming pace.

ADVANCED PERSISTENT THREATS (APTS)

STATE-SPONSORED APT GROUPS

The primary point of concern for governments, organizations, and critical infrastructure managers the world over, state-sponsored APT groups continue to pose a significant challenge to global cybersecurity. APTs remain a driving force behind the evolution and innovation of cyber threats, their actions often paving the way for less sophisticated threats to imitate.

Focusing on mapping adversary infrastructure before weaponization and sharing actionable intelligence underscores the critical need for preemptive threat intelligence in combating these persistent and sophisticated actors.

APT 28 (Fancy Bear), APT 43 (Kimsuky), and Sapphire Sleet have operated with surgical precision throughout the year, targeting individuals and organizations involved in finance, technology, and government across multiple regions.

KNOW THE FACES AND BEHAVIORS OF YOUR ADVERSARIES

FIN7 MALWARE CAMPAIGNS

FIN7 (also known as Sangria Tempest, ATK32, Carbon Spider, Coreid, ELBRUS, G0008, G0046, and GOLD NIAGARA) are a financially-motivated threat group with links to Russia, that has been operating since at least 2013, who were previously thought to have been eliminated by the US Department of Justice.

In 2024, Silent Push analysts received a lead from one of our partners about shell websites being used by FIN7 to age domains. Since our initial public report, we've tracked over 10,000 of these domains and focused considerable efforts on finding new campaigns being launched through these websites.

In late Summer 2024, Silent Push analysts detected a new FIN7 campaign that used a series of AI "deepfake nude generator" websites that were actually honeypots serving malware to unsuspecting visitors.

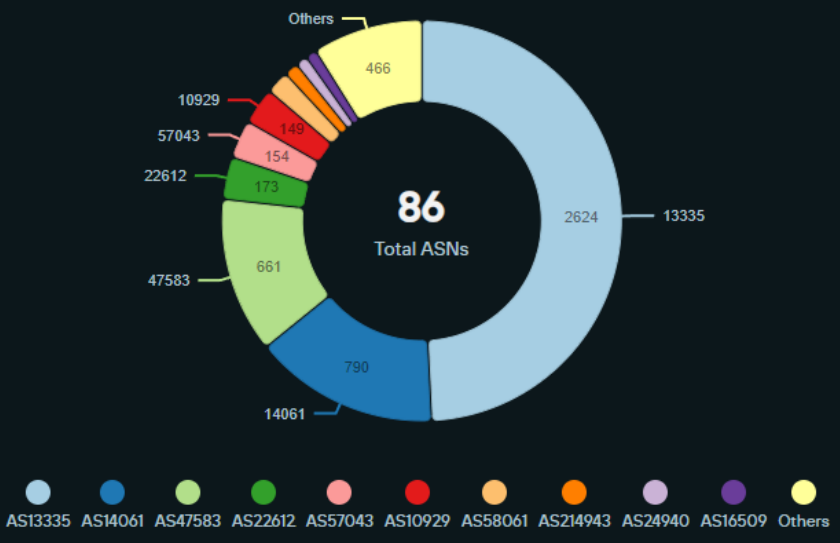
FURTHER FINDINGS

FIN7 SHELL DOMAINS MORPHING INTO PHISHING WEBSITES

A common FIN7 TTP is to take shell domains and morph them into conventional spoofing websites (via redirects or on-page content), targeting users of well-known brands with phishing and malware delivery.

From our analysis, content is served based on a range of user-specific parameters. Domains may populate based on geographic region, IP address, local time, type of connection, or browser settings (such as JavaScript being enabled).

Analysis of the domains used in this campaign indicate a high level of diversity with domain structure, hosting locations, and registrars.



86 ASNs were used across the current FIN7 infrastructure

THE COMM – SCATTERED SPIDER & CRYPTO CHAMELEON

Scattered Spider and Crypto Chameleon are part of "The COMM," a loosely organized group of mostly young threat actors, many based in the U.S. Both have been involved in high-profile financial attacks, leading to multiple arrests.

In 2024, Silent Push analysts received private insights on The Comm, later highlighted in EclecticIQ's September article, *Ransomware in the Cloud: Scattered Spider Targeting Insurance and Financial Industries.* The article exposed Telecom Enemies (aka Telecom Clowns), a "Developer-as-a-Service" (DaaS) group supplying The Comm with tools like Gorilla Call Bot for vishing and Suite's AIO phishing kit.

Silent Push sees AIO as a key link between Scattered Spider and Crypto Chameleon, reinforcing that many Comm members are "script kiddies" relying on pre-built attack tools rather than coding their own.

FURTHER FINDINGS

LINK BETWEEN SCATTERED SPIDER AND CRYPTO CHAMELEON

Our team at Silent Push believes the AIO product is one of the strongest connections between Scattered Spider and Crypto Chameleon. This further highlights that many members of The Comm are “script kiddies” who use the attack methods but often do not code directly themselves. The AIO product includes phishing templates for Coinbase, Gemini, Kraken, Binance, Robinhood, OKX, Trezor, Ledger, Exodus, MetaMask, Trust Wallet, Bitwarden, LastPass, Yahoo!, AOL, Microsoft/MSN, Gmail, and iCloud. Both Scattered Spider and Crypto Chameleon have targeted the companies listed.

It also appears Njalla and Virtuo have become preferred hosting providers for the group in combination with the registrar NiceNIC.

We decided to examine all domains hosted and registered on these services, looking for any names that included characteristic Scattered Spider keywords or typosquat domains featuring the companies mentioned above with new keywords.

Domains search parameters:
nsname = *.my-ndns.com
asnum = 399486;39287
first_seen_min = 2024-08-01

As we analyzed the results, we noticed the response mainly returned:

- Additional Scattered Spider domains
- Crypto Chameleon domains

TRIAD NEXUS

During a 2022 Silent Push investigation into a domain involved in investment fraud, our team uncovered a large cluster of fake trading apps impersonating well-known financial organizations, including the **Australian Securities Exchange (ASX), Coinbase, CoinSmart, eToro, and Nasdaq.**

This same investigation uncovered fake financial job scams employing pig butchering techniques, and this is when our analysts first came across several malicious networks hosted on the FUNNULL CDN infrastructure.

Our **Triad Nexus** research discovered this is not a lone cluster of activity but is, in fact, part of a global financial fraud campaign.

FURTHER FINDINGS

OUR INVESTIGATION CONTINUES TO UNCOVER MORE

When updating our FUNNULL research for 2024, we discovered that this same malicious cluster, while reduced in scope, still has active hostnames, including cmegrouphkpd[.]info, which hosted a fake trading platform abusing CME Group's brand for the past two years.

Until recently, a nearly identical version of this site was hosted at hiflyk47344[.]top.

The timeline can be seen via current and historical CNAME records, which for cmegrouphkpd[.]info shows it had a record pointing to vk6a2rmn-u.funnull[.]vip between February and March 2022, changing to vk6a2rmn-u.funnull01[.]vip between March 2022 and June 2024, and since then, switching to 6ce0a6db.u.fn03[.]vip.

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	TTL	Type
www.cmegrouphkpd.info	-	6ce0a6db.u.fn03.vip	-	2024-06-24 00:23:42	2024-08-04 22:45:59	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull01.vip	-	2022-05-20 19:05:13	2024-06-20 04:27:48	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull.vip	-	2022-02-27 06:55:26	2022-05-07 09:02:13	300	CNAME

The apex domains seen in the Answer fields of these CNAME records – funnull[.]vip, funnull01[.]vip and fn03[.]vip – are all part of FUNNULL's CDN infrastructure.

Read more within our full report (50+ pages) to find out additional insights on FUNNULL. Let us know if you'd like a **free** copy.

THE MISSION

Silent Push spent 2024 tracking millions of hidden malicious domains and IPs, fingerprinting attacker infrastructure both at-scale and as it was stood up, mapped the impact of critical vulnerabilities spread across the web, and worked closely with each of its many partners to disrupt threat actor operations worldwide. We delivered world-first, in-depth technical reporting to our customers, produced IOFA feeds that set the gold standard for preemptive threat intelligence, and continue to iterate upon and improve our rigorously curated, first-party data set and intuitive threat hunting platform.

The insights powering this report are built upon our first-party dataset, which represents the most comprehensive view of the internet available anywhere in the world, to map attacker tactics, techniques, and procedures (TTPs) and infrastructure in real-time. Enabling the tracking and analysis of adversaries' network changes as they occur and stopping them at the gates – before they can get in is critical so you can prevent a breach.

IDENTIFY HIDDEN INFRASTRUCTURE TO PREVENT A BREACH

CONCLUSION

Our preemptive approach to threat intelligence and continuously expanding oversight over global internet architecture backed by game-changing first-party data will play a critical role in helping organizations navigate and mitigate the advanced threats facing them in the coming years. As our industry as a whole shifts to combat a future filled with increasingly resourced and sophisticated cyber threats, the ability to preemptively ruin adversaries' plans by mitigating attacks before they are launched will define the success of cybersecurity strategies in 2025 and beyond.

Read more about these findings within our free 50+ page full report. This is a deeper dive with additional analysis that includes strategic recommendations to preventing an attack and how attackers have swiftly adapted to the rise of artificial intelligence (AI) to scale their operations.

ABOUT US

Silent Push provides preemptive cyber intelligence exposing threat actor infrastructure as it's being set up. Our industry-leading Indicators of Future Attack (IOFA) act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

Get started today.

SILENT PUSH

PREEMPTIVE CYBER INTELLIGENCE WITH INDICATORS OF FUTURE ATTACK

REQUEST A DEMO

silentpush.com