

— SEPTEMBER 2026

THREAT RESEARCH ROUNDUP

SIX INVESTIGATIONS FROM THE SILENT PUSH RESEARCH
TEAM, JUNE TO SEPTEMBER 2026

FOUR MONTHS, SIX PUBLIC INVESTIGATIONS

Thanks for downloading this report. I'm Michael Sweeney, Director of Preemptive Cyber Defense at Silent Push. I've spent over 15 years in cyber operations and intelligence, much of it on APT attribution and threat actor tracking, and my team's job is turning what we see in adversary infrastructure into intelligence you can act on.

Between June and September we published six public investigations. Some tracked threat actors ahead of an attack: we flagged a Cobalt Strike C2 IP 76 days before it appeared in a DFIR report on The Gentlemen, and mapped infrastructure naming Amgen as a target seven months before its SEC filing. Other investigations were hands-on. We simulated subdomain takeover at scale, joined a bandwidth-sharing network, chatted with a suspected North Korean IT worker on Telegram, and bought a fast-flux subscription to see how it works from the inside.

You lead busy lives, so we have condensed that work here to keep you in the loop. Each section links to the full research, and the final section collects what defenders can act on.

[VISIT OUR RESEARCH HUB →](#)



MICHAEL SWEENEY

Director of Preemptive Cyber Defense Team, Silent Push

TABLE OF CONTENTS

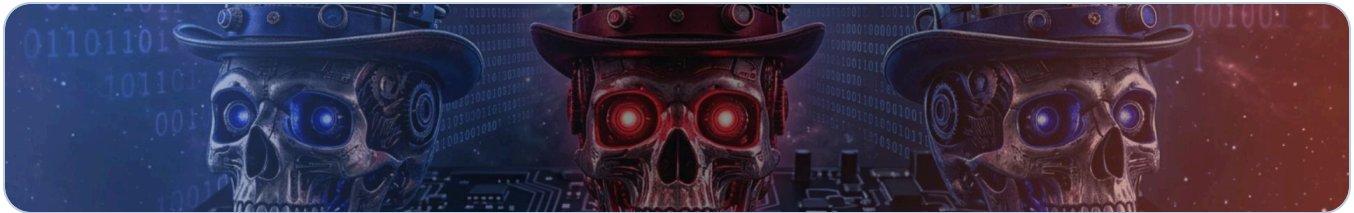
01	THE GENTLEMEN RAAS	04
	The affiliate trail, from CountLoader to The Gentlemen	05
	What the infrastructure picture adds	06
02	DANGLEGEDDON	07
	Our approach	09
	The impact, sector by sector	10
03	THE AMGEN BREACH	11
	What Silent Push saw in January	13
04	PEER2PROFIT AND ASTROPROXY	14
	What are residential proxies	16
	The risk	17
05	NORTH KOREAN IT WORKER FACILITATORS	18
	Primary tactic: identity and proxy theft	20
06	MASS PHISHING THROUGH FAST FLUX	21
	Why threat actors love fast flux	23
07	DEFENDER RECOMMENDATIONS	24
	DNS and infrastructure	25
	Identity, people, and endpoints	26
—	SOURCES	27

THE GENTLEMEN RAAS

What public reporting gets right, and what Silent Push learned months earlier.

THE AFFILIATE TRAIL, FROM COUNTLOADER TO THE GENTLEMEN

Brian Krebs of KrebsOnSecurity published a piece identifying the person allegedly behind The Gentlemen ransomware operation. It is good work, and puts a spotlight back on the Ransomware-as-a-Service group that expanded quickly from mid-2025.



We covered The Gentlemen in an April blog, “No Place to Hide: Following a Serial Ransomware Affiliate from LockBit, Black Basta, and Qilin to The Gentlemen,” based on our deep research in 2025. The blog focuses on the infrastructure and affiliate activity underpinning the operation, specifically an affiliate we had been tracking across four ransomware groups for the better part of three years.

In July and August 2025, Silent Push Preemptive Cyber Defense Analysts identified a previously undocumented malware loader we named CountLoader, observed in three distinct versions: .NET, PowerShell, and JScript. The more significant finding was what CountLoader led to: two Cobalt Strike watermarks, 1473793097 and 1357776117, fingerprinted to a single ransomware affiliate with verifiable ties to Black Basta, LockBit, and Qilin activity.

We published those findings in an exclusive client-facing report in August 2025, followed by our public blog, “CountLoader: Silent Push Discovers New Malware Loader Being Served in Three Different Versions,” on 18 September 2025.

Cobalt Strike licenses carry unique identifiers. When an affiliate uses the same licensed instance across campaigns and RaaS platforms, those watermarks follow them. A RaaS affiliation is replaceable, but the tooling fingerprint is not. That is what makes Cobalt Strike watermarks a reliable tracking mechanism across brand changes.

On 8 February 2026, Silent Push flagged 91.107.247[.]163 as a Cobalt Strike C2, issuing an IOFA alert to customers. Blocking was pushed automatically to firewalls, SIEMs, and EDR platforms that day.

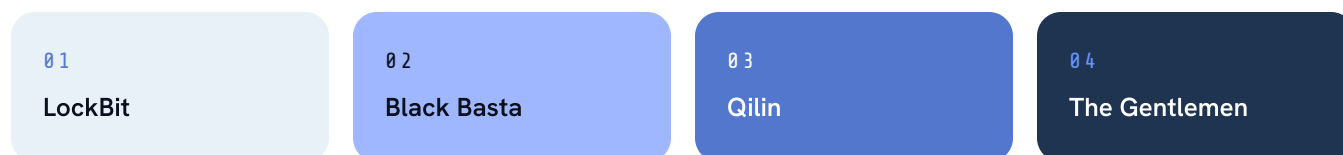
WHAT THE INFRASTRUCTURE PICTURE ADDS TO THE OPERATOR PICTURE

On 20 April 2026, Check Point published a DFIR report on an intrusion by The Gentlemen. The report identified 91.107.247[.]163 as the Cobalt Strike C2 used in the attack. Silent Push had flagged that IP 76 days earlier, and customers had blocks in place across the board. That 76-day window is where preemptive cyber defense operates.

While Krebs answers who is running the operation, infrastructure attribution answers what they are running it on, and how to detect the same actor even when they move between ransomware groups.

The affiliate tracked in our research has worked across LockBit, Black Basta, Qilin, and The Gentlemen. The RaaS group they operate under is interchangeable, and the Cobalt Strike watermarks follow them regardless.

Such persistence is what allows Silent Push to maintain a high-confidence trail across three years of activity spanning four ransomware programs.



WHAT TO BLOCK AND MONITOR

Cobalt Strike is well known to be used by many threat actors and Advanced Persistent Threat groups. Our IOFA for Cobalt Strike C2 Domains and C2 IPs, as well as Cobalt Strike Domains and Cobalt Strike IPs, are available for enterprise clients.

Initial access: The Gentlemen affiliates favor internet-facing VPN and firewall appliances as entry points. Auditing and patching those surfaces should be treated as a priority.

IOFA feeds: Exclusive to enterprise clients, Silent Push Cobalt Strike IOFA feeds are available via API and STIX/TAXII for direct integration into your firewall, SIEM, or EDR. That integration is what put our customers ahead of this intrusion by 76 days.

[READ THE FULL RESEARCH →](#)

DANGLEGEDDON

A Silent Push simulation demonstrates why dangling DNS domains continue to pose global threats.

WHAT IF WE LOOKED AT IT THE SAME WAY A TRAINED NATION-STATE ATTACKER WOULD?



KEY FINDINGS

- 01 Our research team conducted a simulation examining dangling DNS infrastructure across four industry sectors: government, banking, automotive manufacturing, and pharmaceuticals.
- 02 We applied simple, agent-based instrumentation and AI workflows to find, enumerate, and uncover subdomains that could be exploited.
- 03 Using the same single technique over and over produced successful results, leading us to determine we were only scratching the surface of an immense scale of takeover possibilities.
- 04 We named the project “Danglegeddon.”

EXECUTIVE SUMMARY

There are billions of forgotten, abandoned, and misconfigured subdomains on the internet that point to nowhere. Seemingly harmless on the surface, they aren't necessarily an imminent cyber threat warranting an immediate call to arms from analysts, agents, or defenders.

Looking at this “dangling DNS” infrastructure, the Silent Push research team asked a simple question: what if we looked at it the same way a trained nation-state attacker would?

And what if we simulated a scaled exploit of this “highly exploitable” infrastructure that the world has not yet seen? What would the impact be? How widespread could it become, and how quickly could a massive-scale takeover be possible?

Our analysts conducted this threat research initiative specifically against a sample group that included government and Fortune 500 companies, initially targeting Microsoft infrastructure. We named the project “DANGLEGEDDON.”

OUR APPROACH

We targeted 12,500 total domains as our initial infrastructure sample size. Silent Push selected into each target organization's VDP (Vulnerability Disclosure Program) and Bug Bounty Program, and safe harbor for passive vulnerability testing.

12,500

apex domains sampled

16,000

dangling subdomains
found

4,000

takeovers automated

5,000

safe via provider
safeguards

ONE SINGULAR TECHNIQUE: DNS TAKEOVER

In this simulation, we exposed various DNS misconfigurations and broad cookie session scoping to allow credential harvesting and OAuth redirection from a successfully deployed phishing campaign, employing the singular technique of dangling DNS takeover, one of many techniques that has been around for years and is well known in the industry.

Then, simple, agent-based instrumentation and AI workflows were applied to expand the range of DNS domains and subdomains, which proved to be a force multiplier for leveraging this technique at scale and at an accelerated pace across domain and subdomain discovery and enumeration.

USING AI TO ACCELERATE

We continued to leverage AI's ability to find, enumerate, and uncover subdomains as our research progressed. The Claude model Opus 5 quickly enabled script generation after enriching the context with in-scope Bug Bounty programs and the VDP.

The process mapped the targets' 12,500 domains to known vulnerable providers' CNAMEs in EdOverflow's Can-I-take-over-xyz GitHub project.

TIME TO WEAPONIZATION

Within hours, we had a fully developed takeover script to mass-exploit all vulnerable domains.

THE IMPACT

During our simulation, we examined organizations across various industry sectors, including automotive, banking and financial services, energy, government, health care, pharmaceutical, manufacturing, transportation, utilities, and beyond.

GOVERNMENT

Targeting a single U.S. federal government entity, we modeled the downstream effect if applied to all possible systems and accessible employee credentials using Microsoft infrastructure. The immediate impact would affect thousands of systems and millions of employees, causing multiple disruptions. The downstream impact, for example in the Department of Defense, could affect its \$66 billion budget.

BIG PHARMA

An estimated 75% to 85% of major global pharmaceutical enterprises utilize Microsoft Azure for their operations. The speed of a takeover cascading into a magnitude involving multiple global pharma organizations would undermine high-performance R&D, disrupt clinical trials, and pose even more serious consequences for the supply chain necessary to deliver drug and therapeutic solutions on a global scale.

BANKING

Azure serves as a cloud provider for an estimated 80% or more of the world's largest banks and 75% or more of major financial institutions; a disruption could cause serious complications and potential panic. The downstream impact on the global financial sector would include paralysis of online banking and real-time payments, as well as the blocking of trading platforms.

AUTOMOTIVE

Targeting a Fortune 500 manufacturer, we successfully took over a subdomain from a historic American automotive company. The 2025 Jaguar Land Rover cyberattack shut down production for five weeks, cost the company \$350 million directly, and drove an estimated \$2.5 billion in broader UK economic damage, impacting more than 5,000 supplier and dealer organizations.

\$66B

DoD budget within downstream scope

2M+

employees using affected systems

80%+

of the world's largest banks on Azure

It was clear that the same single technique, applied over and over, produced the same successful returns. At that point, we realized we were **only scratching the surface** of the scale of takeover possibilities.

[READ THE FULL RESEARCH →](#)

THE AMGEN BREACH

What our January warning tells defenders.

SEVEN MONTHS BETWEEN THE WARNING AND THE FILING

WHAT HAPPENED, AND WHEN

In January 2026, the Silent Push research team mapped a cluster of adversary infrastructure staged for takeover of single sign-on accounts across more than 100 large organizations. Amgen was one of the named targets, grouped with other pharmaceutical and biotech companies.

On 31 July, Amgen filed a Form 8-K with the SEC confirming that attackers had stolen patient protected health information and proprietary data from cloud environments run by its third-party vendors.

Seven months passed between the January infrastructure findings and Amgen's July disclosure. That is enough time for a targeted organization to block the infrastructure, watch the named accounts, and tighten identity controls before an attack lands. In Amgen's case, the disclosure came at the end of it.

WHO IS SHINYHUNTERS

ShinyHunters is a data theft and extortion group that operates as part of Scattered LAPSUS\$ Hunters, an alliance that also includes Scattered Spider and LAPSUS\$. The group gets in through social engineering, moves through connected cloud platforms, and uses the stolen data to pressure its victims into paying. Its focus is identity and SaaS access, which is what makes a single compromised SSO account so valuable to it.

The targets are large enterprises with heavy cloud footprints, the kind of organizations that run day-to-day operations through platforms like Salesforce, Microsoft 365, and SharePoint. The infrastructure behind this campaign has pointed at more than 100 such organizations across several industries, and the campaign's later activity concentrated on healthcare, medical technology, and pharmaceutical companies. Amgen sits squarely in that profile.

IOC VS IOFA

An Indicator of Future Attack® names a threat while it is still being staged, early enough for a team to respond. An Indicator of Compromise is the older, well-known kind of signal: the forensic evidence collected after a breach that helps with investigation once the loss has already happened.

JAN 2026

Infrastructure mapped

7 MONTHS

Window to act

31 JUL 2026

Form 8-K filed

SOURCE: SILENT PUSH RESEARCH AND SEC EDGAR

WHAT SILENT PUSH SAW IN JANUARY

The Silent Push platform maps adversary infrastructure by watching for the setup work that happens before an attack: the domains a group registers, the certificates and hosting it stands up, and the tooling it stages while preparing to move against a target. We turn that activity into Indicators of Future Attack® (IOFA), which give a security team a named threat and a timeframe to act on before anything reaches their environment.

In January 2026, that work identified the Scattered LAPSUS\$ Hunters campaign while it was still being built, months before any of it was used against a target. In Silent Push research, the average lead time between spotting this kind of infrastructure and an attack landing is 154 days. In Amgen's case, the public timeline ran to about seven months.

HOW THE ATTACK CHAIN WORKS

Health-ISAC, the information-sharing group for the healthcare sector, published an advisory on 24 July 2026 describing the pattern in detail. The short version is that the attack runs on social engineering aimed at a vendor's helpdesk. Someone calls posing as internal IT and persuades a representative to reset multi-factor authentication on a chosen employee's account. That reset hands over a single signed-in session, and that session reaches the cloud apps the account can open.

Amgen's disclosure places the unauthorized activity in cloud environments run by third-party service providers, and the company reported no impact to its products, manufacturing operations, or financial reporting systems. The exposed records sat with outside vendors contracted to store and process patient data on Amgen's behalf, in infrastructure Amgen does not run or directly monitor. An organization can operate a mature security program across its own estate and still inherit the risk carried by every vendor that holds its regulated data.

WHAT SECURITY TEAMS CAN DO

The first control to adopt is a no-same-call rule, which stops a helpdesk from resetting a password, resetting MFA, or enrolling a new device on the same call that requests it. The request goes into a ticket and gets a callback to a number already on file for the account. That single step breaks the part of the chain the group relies on most.

For higher-risk accounts such as administrators, security staff, and finance employees, the advisory recommends a second approval and an out-of-band identity check before any credential change. It also points to phishing-resistant MFA such as FIDO2 keys or passkeys, which cannot be talked out of a person over the phone.

[READ THE FULL RESEARCH →](#)

PEER2PROFIT AND ASTROPROXY

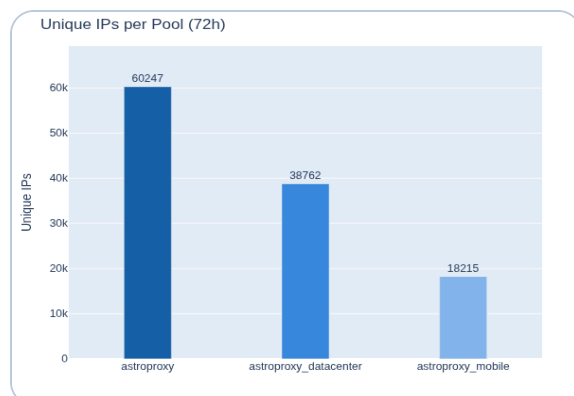
How bandwidth-sharing apps turn a corporate IP address into someone else's product.

WE JOINED A BANDWIDTH-SHARING NETWORK TO SEE WHAT HAPPENS TO YOUR IP ADDRESS



KEY FINDINGS

- 01 Residential proxies are almost invisible to security teams, yet they can expose organizations' valuable internal resources to anyone with a proxy subscription.
- 02 PEER2PROFIT directly feeds ASTROPROXY. Silent Push confirmed an operational relationship between the two: PEER2PROFIT recruits everyday users and pays them for bandwidth, while ASTROPROXY resells that bandwidth commercially, at up to 27 times what the user was paid.
- 03 Over a 72-hour enumeration window, we identified 117,224 unique IPs across ASTROPROXY's residential, mobile, and datacenter pools, with the residential pool alone adding over 1,000 new IPs every hour.
- 04 These apps are not malware. PEER2PROFIT installs through official channels with full user consent, which means standard antivirus tools and threat intelligence feeds don't flag it, and any employee can install it on a corporate device without triggering a single alert.
- 05 A DNS record was enough to reach internal networks. ASTROPROXY blocks direct requests to internal IP ranges, but our team determined the filter could be bypassed with nothing more than a domain name resolving to an internal IP address. This was responsibly disclosed before publication; the provider did not remediate.



UNIQUE IPS ACROSS ALL THREE POOLS. SOURCE: SILENT PUSH ENUMERATION, 72-HOUR WINDOW

WHAT ARE RESIDENTIAL PROXIES, AND WHY DO THEY MATTER?

To understand how one of these proxy networks was built, we did what any curious researcher would do: we joined one. We became a proxy node in the PEER2PROFIT network, a bandwidth-sharing program that pays users for their internet connection, and then tracked to see what would happen to our IP address.

These programs are easy to install, their infrastructure isn't flagged, and yet they pose a real risk to organizations, since any employee can run them. In doing so, they hand their organization's IP space to a proxy network, potentially causing reputational damage and even exposing internal corporate assets.

DATA CENTER

IP addresses specifically allocated to commercial servers. Easy to provision, inexpensive to operate, and straightforward to block since they are static.

MOBILE

Sourced from real user devices or SIM farms. Traffic exits through carrier-grade NAT or mobile gateways, often sharing IP addresses across many legitimate users, making blocking ineffective.

RESIDENTIAL

The hardest to deal with and the most attractive to threat actors. The IPs belong to real users, assigned by their ISPs, and the devices can be anywhere. Proxy traffic is indistinguishable from an ordinary user browsing the internet.

RESIDENTIAL PROXIES: THE GOOD AND THE BAD

Legitimate businesses might use residential proxies to test how their services appear across different geographies and verify ad placements. We have found threat actors abusing residential proxy networks for large-scale credential stuffing operations, malspam campaigns, financial and banking fraud, geo-restriction bypass, and rate-limit evasion.

The dual-use nature makes it difficult to block residential proxy traffic without significant collateral damage. The second problem is how fast these networks change: a given IP can be a clean residential connection one hour and an active proxy exit node the next, with no abuse history or reputation signal to reflect that change.

Over a 72-hour enumeration window, we identified 117,224 unique IPs across ASTROPROXY's residential, mobile, and datacenter pools, with the residential pool alone adding over 1,000 new IPs every hour.

THE RISK

Bandwidth-sharing programs such as PEER2PROFIT are not malware. They are legitimate applications distributed through official channels that users knowingly install. This distinction has significant consequences for corporate security.

ANY EMPLOYEE CAN INSTALL ONE

There is no technical barrier to an employee installing a bandwidth-sharing client on a corporate device or on a personal device connected to a corporate network. Common antivirus solutions do not flag these programs, and the infrastructure they connect to is not listed as malicious in standard threat intelligence feeds or reputation systems.

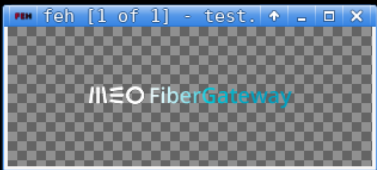
A CORPORATE IP BECOMES A PROXY EXIT NODE

Once installed, the device's internet connection, and by extension the organization's IP space, becomes available as a proxy exit node in a commercial proxy service. Any traffic routed through that node will appear to originate from a corporate IP address.

A DNS RECORD WAS ENOUGH TO REACH INTERNAL NETWORKS

Direct access to internal IP addresses is blocked, but this filter could be easily bypassed with a simple DNS entry resolving to internal IPs. Using a node enrolled in the PEER2PROFIT network and available via ASTROPROXY, we successfully reached the router management interfaces of Portugal's largest ISP and downloaded a PNG file from the router as proof of access. A user running a bandwidth-sharing client is not only giving away the public IP address, but potentially exposing every device on that network to anyone with access to the proxy service.

```
user:~/ $ curl -sw '%{http_code}' \
-x http://node-de-74.astroproxy.com:10108 \
--proxy-user "$PROXYPW" \
app.192-168-1-254.nip.io/external/styles/img/logo.png \
--output test.png
200
user:~/ $ feh test.png
```



FILTER BYPASS: DOWNLOADING A PNG FROM A MEO FIBER GATEWAY ROUTER

RESPONSIBLE DISCLOSURE

We responsibly disclosed this finding before publication, and the provider was given significant time to investigate and remediate. With no meaningful remediation forthcoming, we are disclosing this publicly to raise awareness of the risk that a bandwidth-sharing program can pose to the networks it operates on.

[READ THE FULL RESEARCH →](#)

NORTH KOREAN IT WORKER FACILITATORS

Exposing a recruiting scheme run through Discord servers and Telegram.

A JOB ADVERTISEMENT ON A COMPUTER MOUSE REVIEW SERVER



KEY FINDINGS

- 01 Silent Push identified a North Korean fake job recruitment scam channel hosted on a Discord server by a defender colleague, and we engaged the recruitment representative to ask about their offering and determine whether the individual was actually a North Korean IT worker.
- 02 After connecting via Telegram, we asked the suspect NK persona “Tec Guru” about virtual private networks; they advised us to use Astrill VPN, a VPN often used by North Korean IT workers.
- 03 We identified the threat actor's primary tactic as identity and proxy theft, under the guise of a front and facilitator recruitment scheme.
- 04 Based on technical reference indicators pointing to the persona being a North Korean IT worker, and on their speech patterns, among other flags, we believe they are North Korean.

EXECUTIVE SUMMARY

A cybersecurity colleague spotted an odd job advertisement being promoted on a Discord server named “Mouse Review,” a server channel created to find and write computer mouse reviews. Discord servers are free, often invitation-only virtual meeting places divided into smaller text and voice rooms called channels.

We began investigating the job advertisement on the Mouse Review channel. The Discord account tecguru113, ID 1453753519436861505, is responsible for spreading the fake job advertisement in the server.

One of our principal threat research analysts created a fake persona and contacted the Telegram account Tecguru0618 mentioned in the job ad. What follows details our interaction with the representative, whom we believe with moderate to high confidence is a North Korean IT worker.

Organizations engaging with North Korean IT workers face severe sanctions risks and are advised to verify applicants' physical locations during job interviews. Silent Push developed a detection method for these operations.

PRIMARY TACTIC: IDENTITY AND PROXY THEFT

The North Korean IT worker's primary goal is proxy hiring, using Western or Latin American citizens as the “face” and legal identity to bypass sanctions, identity verification controls, and regional hiring restrictions.

GEOGRAPHIC TARGETING

The threat actor explicitly solicited individuals based in the U.S., E.U., and LATAM to serve as proxies who can bypass geographic IP and location blocks and regional tax compliance checks.

FACE RENTAL

The advertisement explicitly requests a proxy to “turn on your camera during interviews,” “communicate with clients,” and “represent the necessary skills confidently.”

REVENUE SHARING

The job ad scam offers a financial incentive split, 35% to the proxy and 65% to the North Korean IT worker, to incentivize foreign nationals to serve as financial and identity mules.

KEY RISK TAKEAWAYS FOR ORGANIZATIONS

- 01 Remote identity fraud:** Candidates hired for remote roles may be sitting on camera while a completely different entity writes code, answers technical queries via chat, or controls the machine via remote desktop.
- 02 Insider threat and data exfiltration risk:** Once hired, these workers often use their corporate access to exfiltrate proprietary source code, steal sensitive intellectual property, and extort victim organizations by threatening to leak corporate data in exchange for ransom payments.
- 03 Sanctions compliance:** Companies that unknowingly hire or pay North Korean IT workers, even through a proxy, risk sanctions from the Office of Foreign Assets Control, a financial intelligence and enforcement agency of the U.S. Department of the Treasury.

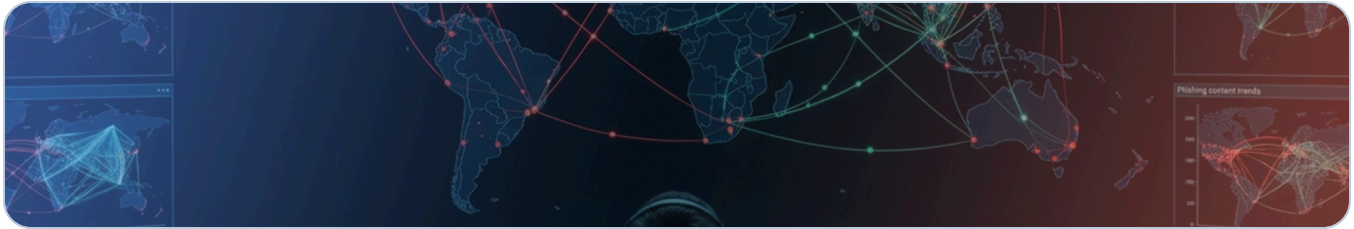
The U.S. Department of State issued an alert on 31 July 2026, “Countries, Companies, and Other Entities Regarding North Korean IT Workers,” outlining North Korean IT workers' modus operandi and warning the international community and private sector of the threat they pose.

[READ THE FULL RESEARCH →](#)

MASS PHISHING THROUGH FAST FLUX

We became a customer to watch the infrastructure behave from the inside.

THOUSANDS OF LIVE PHISHING DOMAINS FROM A SINGLE QUERY



KEY FINDINGS

- 01 The fast-flux technique has evolved, making it easier for threat actors to use in phishing campaigns and harder for defenders to detect and apprehend cybercriminals.

- 02 Silent Push became a fast-flux customer to watch how the infrastructure behaves from the inside, and then turned what we learned into detection analytics.

- 03 From a single query in our platform, we identified thousands of live phishing domains, including a large, Canada-first banking campaign that hides behind commercial traffic-distribution cloaking.

- 04 Beyond CISA's recommendations to protect against fast-flux attacks, our platform detects fast-flux infrastructure to provide proactive protection.

EXECUTIVE SUMMARY

While the fast flux technique of rapidly rotating a domain's DNS records across many IP addresses and networks to avoid detection dates back to at least 2007, it has become more sophisticated and easier for threat actors to use in phishing campaigns and other malicious activities.

Going deeper into our research on fast flux, we became a customer to see its inner workings. We identified a large global phishing operation from a single query in our platform. The infrastructure's structure is quite effective, making it nearly impossible for most defenders to detect.

Organizations should develop fast-flux detection analytics and blocking capabilities. Our platform enables security teams to protect against fast-flux infrastructure.

In April 2025, CISA, jointly with the NSA, FBI, and international partners, published **FAST FLUX: A NATIONAL SECURITY THREAT**, warning that fast flux “exploits a gap commonly found in network defenses.” The advisory explicitly encourages service providers to develop accurate, reliable, and timely fast-flux detection analytics and blocking capabilities.

WHY THREAT ACTORS LOVE FAST FLUX

When The HoneyNet Project first documented the fast-flux technique in 2007, the rotating IP address pool was the attacker's own botnet. That same capability has since become a subscription service, rented, openly marketed on cybercrime forums, and sold by providers, including at least one sanctioned bulletproof hoster. Phishing operators simply point their domains at the service, and the provider rotates the underlying infrastructure.

IP blocking is fast, but fast flux is built to defeat it: a single domain rotates across a constantly changing pool of IPs spread over different networks and often various countries. Block one IP, and the domain resolves to another within minutes. For phishing, command and control, and scam infrastructure, this turns IP blocking into a losing game and leaves the domain as the only durable point of failure.

BECOMING A CUSTOMER TO SEE INSIDE

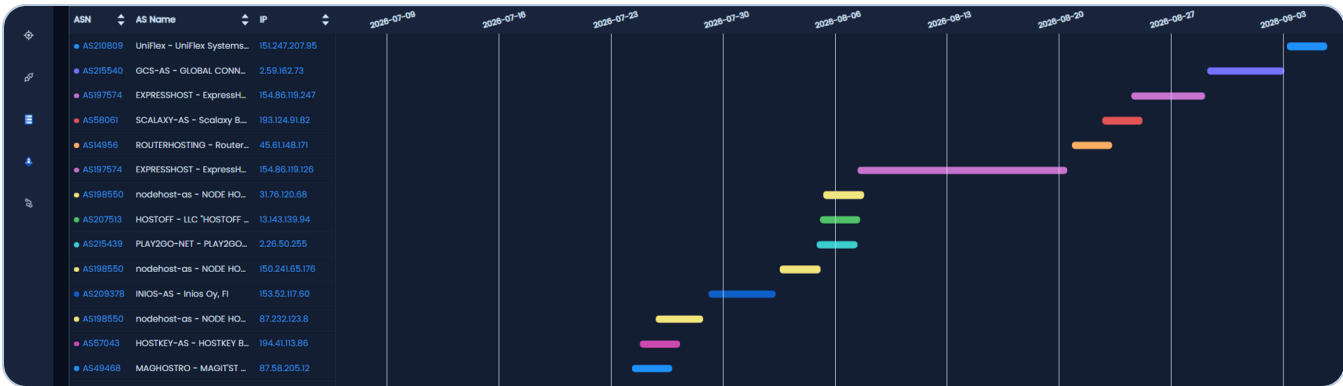
To better understand how to detect this layer, our team of researchers did what defenders rarely can: we became a customer. We purchased a fast-flux service from a provider on the market, watched how the infrastructure behaves from the inside, and turned what we learned into detection analytics.

FAST FLUX AS A SERVICE: A MATURE CRIMINAL MARKET

We paid, and within hours we had what any hosting customer gets: a client portal, a support ticket system, and provisioning instructions directing customers to delegate their domain to a specific DNS provider: the exact delegation signature our detections key on.

KNOWING WHERE TO LOOK

Every fast-flux provider we have tracked protects itself the same way: the provider's own domains never touch the customer infrastructure. Instead, each customer delegates to provider-controlled DNS, which then hands out the rotating IP addresses. That delegation layer is the detection opportunity, and it is invisible unless you know where to look.



IP DIVERSITY VIEW OF CANADA-POST11[.]COM IN TOTAL VIEW: 20 IPS ACROSS 13 ASNS OVER 90 DAYS

[READ THE FULL RESEARCH →](#)

DEFENDER RECOMMENDATIONS

Consolidated from all six investigations.

DNS AND INFRASTRUCTURE

- 01 Work dangling record types in order of blast radius: NS first, then MX, then external CNAMEs, then internal. For each record, delete it from the authoritative zone. Re-point it only if the service behind it is genuinely still in use.
- 02 Sequence decommissioning so the DNS record dies before the cloud resource does. Most of the exposure in the Danglegeddon study came from teams deprovisioning a storage account, a web app, or a VM and leaving the record behind.
- 03 Prefer providers that require domain ownership verification before accepting a custom hostname. In Azure, that means a TXT verification record such as asuid. The 4,925 records we found to be not claimable were protected by exactly this kind of provider-side safeguard.
- 04 Assign an owner and a review date to every DNS record. Employee attrition, layoffs, and merged infrastructure ownership after M&A activity are what produce orphaned zones, and none of those events trigger a DNS review at most organizations.
- 05 Publish CAA records to restrict which certificate authorities can issue for your namespace, and monitor certificate transparency logs for issuance you did not request.
- 06 Audit any security control that allows lists by domain suffix or TLD. A subdomain taken over from a trusted brand passes those filters.
- 07 Implement fast-flux detection analytics at the DNS level. Alert on domains with high IP and ASN diversity, abnormally low TTLs, and inconsistent IP geolocation, and validate that your Protective DNS provider actually blocks fast-flux behavior rather than assuming coverage.
- 08 Block traffic to and from domains and IPs associated with known bulletproof and abuse-tolerant networks, including infrastructure tied to sanctioned hosting providers. Block the confirmed bulletproof ASNs and monitor the rest.

IDENTITY, PEOPLE, AND ENDPOINTS

- 09 Adopt a no-same-call rule at the helpdesk. No password reset, MFA reset, or new device enrolment on the same call that requests it. The request goes into a ticket and gets a callback to a number already on file. That single step breaks the part of the chain ShinyHunters relies on most.
- 10 For administrators, security staff, and finance employees, require a second approval and an out-of-band identity check before any credential change. Move those accounts to phishing-resistant MFA such as FIDO2 keys or passkeys, which cannot be talked out of a person over the phone.
- 11 Extend that scrutiny to vendors. Amgen's own operations were unaffected while patient data held by third-party providers was exposed. An organization inherits the risk carried by every vendor that holds its regulated data.
- 12 Verify applicants' physical locations during job interviews. Organizations engaging with North Korean IT workers face severe sanctions risks, including through a proxy who sits on camera while another party does the work.
- 13 Treat bandwidth-sharing clients as a corporate risk even though no antivirus flags them. Once installed, a corporate IP becomes a proxy exit node, and the proxy network can reach internal resources on the same network through nothing more than a DNS record pointing at an internal IP.
- 14 Audit and patch internet-facing VPN and firewall appliances. The Gentlemen affiliates favor them as entry points, and auditing and patching them should be treated as a priority.
- 15 Monitor continuously rather than periodically. Silent Push IOFA feeds and the Dangling DNS API return these findings programmatically via API and STIX/TAXII, so this becomes a scheduled job that alerts SecOps and IT instead of a quarterly project.

Across these six investigations, the infrastructure was observable before it was used in a targeted attack. The controls above shorten the distance between when it appears and when someone acts on it.

THE FULL RESEARCH

Each section in this report reproduces a Silent Push research publication. The full posts, including all supporting detail and links to primary sources, are on the Silent Push blog.

11 JUN **What Recent Reporting Gets Right About The Gentlemen RaaS and What Silent Push Learned Months Earlier**

silentpush.com/blog/the-gentlemen-raas/

30 JUL **Welcome to Danglegeddon**

silentpush.com/blog/danglegeddon/

03 AUG **Amgen Breach: What Our January Warning Tells Defenders**

silentpush.com/blog/amgen-breach-what-our-january-warning-tells-defenders/

20 AUG **How Peer2Profit and Astroproxy Turn Your Bandwidth Into Someone Else's Product**

silentpush.com/blog/peer2profit-astroproxy/

14 SEP **Silent Push Exposes North Korean IT Worker Recruiting Facilitators Through Discord Servers**

silentpush.com/blog/nk-it-worker/

15 SEP **Silent Push Tracks a Mass Phishing Operation Through Fast Flux**

silentpush.com/blog/fast-flux-phishing/

All screenshots in this report are taken from the original publications.
Product screenshots show the Silent Push platform as it appeared at the time of each investigation.



SEE THE INFRASTRUCTURE BEFORE IT IS USED AGAINST YOU

Start a conversation with one of our platform experts to learn how preemptive cyber defense gives your team more lead time on adversary infrastructure, before an attack is launched.

BOOK A DEMO

COMMUNITY EDITION

NEUTRALIZE BEFORE COMPROMISE

© 2026 SILENT PUSH, INC.
ALL RIGHTS RESERVED