SILENT PUSH

SILENT PUSH RESEARCH / 2026

DANGLEGEDDON

WHY DANGLING DNS DOMAINS POSE A GLOBAL THREAT

TABLE OF CONTENTS

SECTION 01

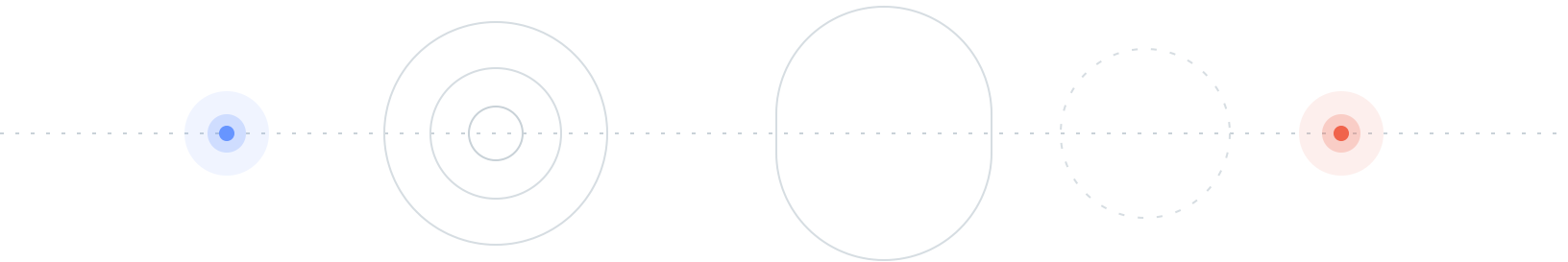
EXECUTIVE SUMMARY

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 massive-scale 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, and named the project “DANGLEGEDDON.”



THE SAMPLE

ONE STUDY, IN FIVE NUMBERS

12,500 apex domains targeted as the initial infrastructure sample size

16,000 dangling subdomains isolated across those apex domains

4,000 subdomain takeovers automated

7,000 required additional steps to determine whether they met the conditions for takeover

5,000 of those were safe due to the provider's safeguard measures

SECTION 02

OUR APPROACH

SAMPLE SIZE OF DANGLING DNS INFRASTRUCTURE

We targeted 12,500 total domains as our initial infrastructure sample size. This represented a small sample of the total companies and infrastructure changes we see daily in the Silent Push data set. Silent Push selected into each target organization's VDP (Vulnerability Disclosure Program)/BBP (Bug Bounty Program) programs and safe harbor for passive vulnerability testing.

Every record we observed was dangling and represented a liability for each company. However, among the 12,500 apex domains, we isolated 16,000 dangling subdomains and automated the takeover of 4,000 subdomains. There were 7,000 subdomains that required additional steps to determine whether they met the conditions for takeover. Upon review, 5,000 of those were safe due to the provider's safeguard measures.

12,500	16,000	4,000	5,000
apex domains sampled	dangling subdomains found	takeovers automated	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's 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 Vulnerability Disclosure Program (VDP). The process mapped the targets' 12,500 domains to known vulnerable providers' CNAMEs in EdOverflow's Can-I-take-over-xyz GitHub project.

Using Silent Push's Dangling DNS API, we further filtered to those resources that lacked allocation or DNS registration. This technique isolated several hundred domains that we further cross-validated against the providers for availability.

Next, the process rapidly enabled the discovery of new registers and platforms that support customizable CNAMEs without DNS domain verification. After this discovery process, we were able to extract several unknown vulnerable providers.

TIME TO WEAPONIZATION

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

As security providers, we are mindful of our legal exposure when conducting these investigations. Advanced threat actors could simply broaden to all resolvable domains in the beginning to start Dangleggedon in time for their morning coffee.

EXPLOITATION OF VULNERABLE CONDITIONS AND BAD IT HYGIENE

Most of the victim networks simply had old resource calls, receiving inbound referrals or XSS (cross-site scripting) directly from the corporate websites and scripts. This allowed the simulated attack not only to be possible but also to demonstrate that it could cut across any industry, any piece of dangling organizational infrastructure, anywhere in the world.

Employee attrition, merged infrastructure ownership (via M&A activity), and large-scale layoffs created highly exploitable conditions, making organizations even more vulnerable to exploitation when IT hygiene is not adhered to comprehensively and immediately during change control and employee termination processes.

MICROSOFT INFRASTRUCTURE = EASIEST AND MOST ACCESSIBLE

Our work focused on Microsoft Azure Blobs, Azure VMs, Web Apps, APIs, and Power Pages instances as a starting point.

As an initial sample size of real-world takeover in mission-critical industries, the team randomly selected infrastructure in the Government, Banking, Pharma, and Automotive industries.

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.

01
Azure Blobs

02
Azure VMs

03
Web Apps & APIs

04
Power Pages

SECTION 03

THE IMPACT

During our simulation, we examined organizations across industry sectors, including Automotive, Banking/Financial, Energy, Government, Health Care, Pharmaceutical, Manufacturing, Transportation, Utilities, and beyond.

GOVERNMENT

SECTOR 01 / 04

Targeting a single U.S. federal government entity, using the techniques described above, we modeled the downstream effect if applied to all possible government 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 the Department of Defense (DoD), for example, could affect its $66 billion IT budget.
- With over 31% of DoD IT infrastructure within the Federal government, the takeover could involve thousands of systems used by over 2 million employees.
- Given the interdependence of departments and the documented cybersecurity oversight gap, the attack surface could grow monumentally.
- A cascading attack could extend far beyond the DoD, involving different branches of the military and national security systems, with the potential impact on national security arguably being severe.

$66B

DoD budget in the downstream impact model

31%

of DoD infrastructure sits within the Federal government

2M+

employees using systems in scope

BANKING

SECTOR 02 / 04

Targeting a large international bank with the same simulated action using the identical technique, the downstream modeling shows a massive impact on the broader banking industry, given the industry's hyper-reliance on Microsoft infrastructure:

80%+

Azure serves as a cloud provider for an estimated 80+% of the world's largest banks and 75+% of major financial institutions; a disruption could cause serious complications and potential panic.

GLOBAL

Applied globally, these disruptions would affect high-performance risk modeling, secure data workloads, and the deployment of generative AI capabilities across multinational firms, including Bank of America, UBS, and the Bank of Montreal.

HALT

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. Customer account lockouts, transaction processing delays, and widespread communication breakdowns across institutions would be felt by global consumers.

BIG PHARMA SECTOR 03 / 04

Targeting a global pharmaceutical organization, our downstream model projected an enormous impact from a takeover because many pharmaceutical organizations use Azure Cloud.

An estimated 75% to 85% of major global pharmaceutical enterprises utilize Microsoft Azure for their operations. This means Fortune 500 companies in the sector, and non-Fortune 500 companies globally.

PRECEDENT / NOTPETYA, 2017

As an example, the 2017 NotPetya attack (estimated at $10 billion worldwide) on Merck downed 40,000 systems within minutes and caused reported losses of $1.4 billion, prompting pushback from insurers. In addition to outages and cascading issues, it also resulted in landmark insurance decisions that were drawn out over more than 10 years of litigation.

In 2026, there has been a rise in sophisticated cyberattacks and ransomware incidents targeting Abbott Laboratories, Novo Nordisk, West Pharmaceutical Services, and others.

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.

ESTIMATED LOSSES ACROSS ORGANIZATIONS COULD BE IN THE HUNDREDS OF BILLIONS.

AUTOMOTIVE

SECTOR 04 / 04

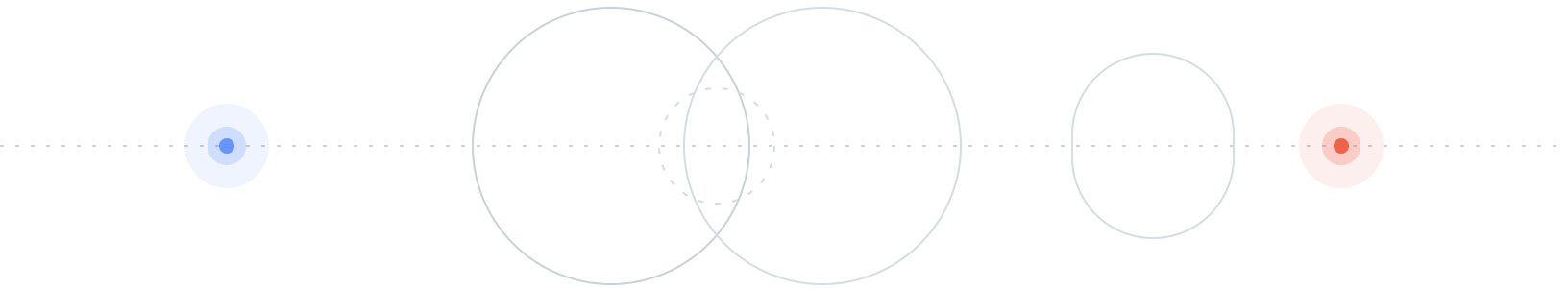
Targeting a Fortune 500 manufacturer, we successfully took over a subdomain from a historic American automotive company.

Historically, a single cyberattack on a top-tier automaker can cost billions and paralyze national supply chains within days.

5	$350M	$2.5B	5,000+
weeks of production shut down	direct cost to the company	broader UK economic damage	supplier and dealer organizations impacted

The 2025 Jaguar Land Rover (JLR) 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 and prompting an unprecedented government-backed loan to keep the supply chain solvent.

Disruption compounded fast and hit beyond the automaker: JLR's shutdown was cited by the Bank of England as a factor in a UK GDP contraction that quarter, illustrating how a single manufacturer's IT outage can ripple into national economic indicators, a dynamic that scales with how deeply operations, from production scheduling to supply-chain logistics, are impacted.



AN ATTACKER WHO WAS ABLE TO TAKE OVER THIS AUTOMAKER'S SUBDOMAIN COULD:

01 Host malicious content and serve phishing pages, malware, or other malicious content under the legitimate car maker’s domain.

02 Cause reputational damage by abusing the trusted brand’s subdomain.

03 Steal user credentials to create convincing phishing pages that appear to be legitimate services.

04 Perform cookie theft and potentially steal session cookies if scoped to the parent domain.

05 Bypass security controls if the legitimate brand’s subdomain is whitelisted in security tools, allowing malicious content to bypass filters.

This vulnerability poses a significant security risk, as attackers can leverage the trust associated with the brand's domain to carry out malicious activities.

SECTION 04

DETAILS ON THE SIMULATED ATTACK

As described in our AI research above, we checked the accounts in multiple ways to determine the best methods for taking over a domain. This workflow highlighted the key industries and government entities we feared were vulnerable due to turnover and infrastructure dependencies. All takeovers were disclosed responsibly.

The 12,500 domains were a small sample of the total companies we see in our daily data, selected for their VDP (Vulnerability Disclosure Program)/BBP (Bug Bounty Program) programs and safe harbor for passive vulnerability testing. Every one of those records is dangling and a liability for the companies, but of those 12,500 apex domains, we isolated 16,000 dangling subdomains and automated the takeover of 4,000 subdomains. There were 7,000 subdomains that required additional steps to determine whether they met the conditions for takeover. Upon review, 5,000 were safe due to the provider's safeguard measures in place to protect its customers.

16,000	4,000	7,000
dangling subdomains isolated	takeovers automated	needed further validation

In each instance, our researchers successfully took over the abandoned resource associated with the identified organization's dangling DNS infrastructure. The organization then redirected its subdomain to our site to serve whatever content we wanted. For each of the organizations involved, we reached out to alert them of the exposed domain(s)/dangling DNS infrastructure through VDPs, among other methods.

Based on the vulnerable DNS infrastructure list we identified, we chose an organization from each sector and assessed its willingness to be tested. Our goal was to demonstrate that virtually any organization with dangling DNS infrastructure is vulnerable to a subdomain takeover.

> A taken-over subdomain isn't itself an intrusion; it's a start, or a trusted launchpad.

Because it inherits the parent organization's reputation and can obtain a TLS certificate, an attacker typically uses it to host convincing phishing pages or credential-harvesting forms, or, in some misconfigured cases, to intercept shared session tokens directly.

From there, reaching internal systems or causing real operational disruption requires the organization to have made additional, separate mistakes beyond the dangling DNS record itself, such as weak multi-factor authentication, overly broad internal trust between systems, or third-party relationships that extend trust further than they should. The dangling DNS is the initial foothold, but the ultimate severity of impact depends heavily on how many additional layers of security hygiene fail after that foothold is gained. Much of it depends on the location of the former valid device and the internal trust that the device the former DNS record pointed to remains in place.

BELOW IS A BREAKDOWN OF THE SIMULATION DETAILS, SECTOR BY SECTOR.

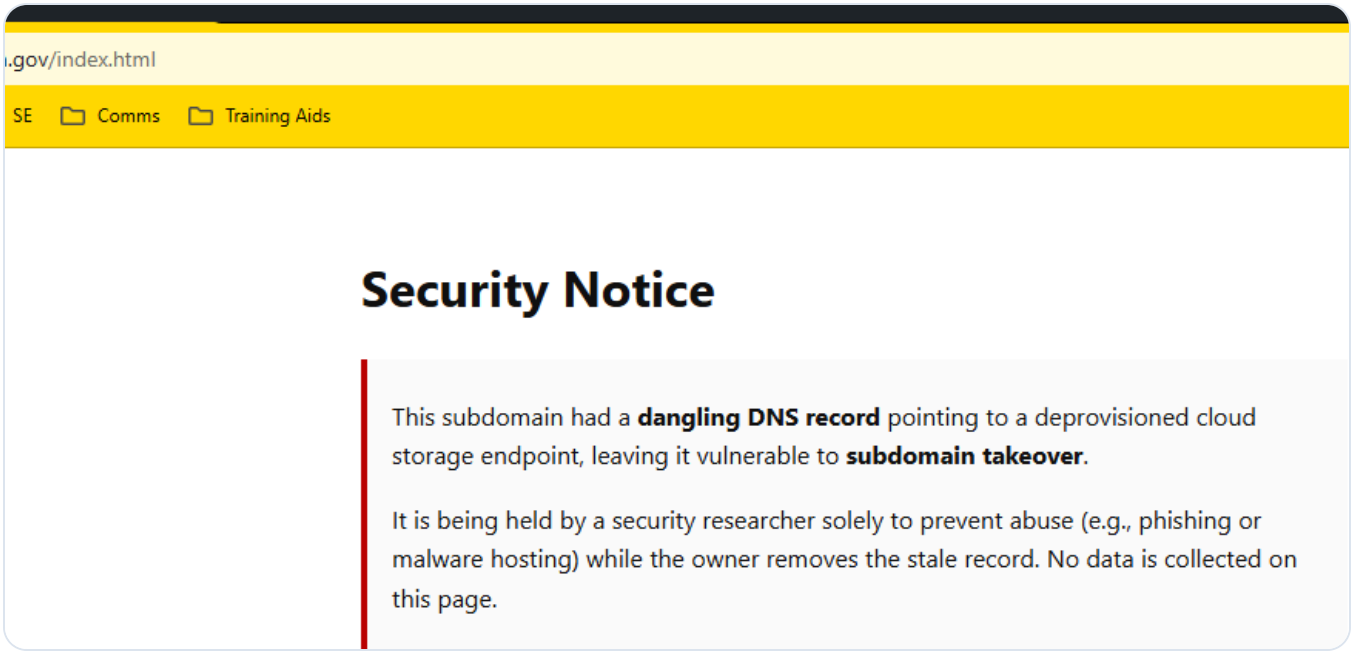
SECTION 05

HOW THE SILENT PUSH PLATFORM WAS APPLIED

From raw domain enumeration to a working proof of takeover, here is how the Silent Push Platform surfaced and confirmed each exposure, sector by sector.

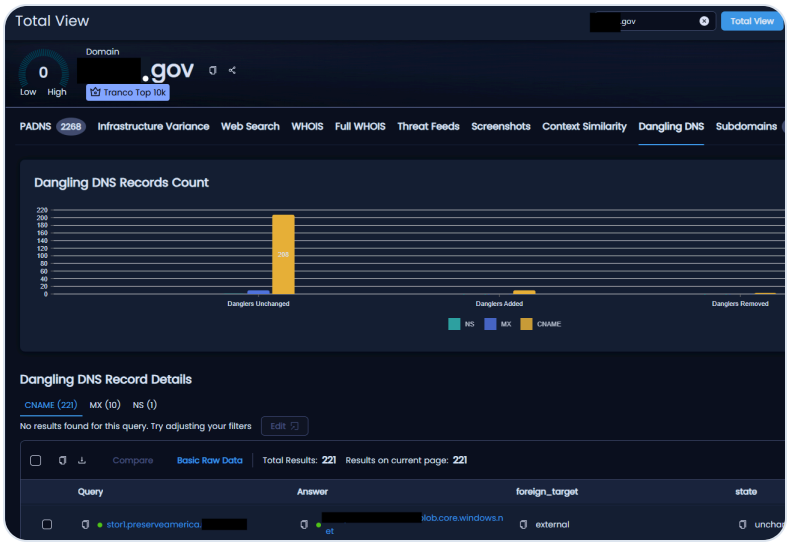
GOVERNMENT SIMULATION 01 / 04

In this simulation, we selected a U.S. federal entity from our sample size. This organization was vulnerable because its DNS record pointed to an unassigned Azure Blob Storage resource.



After hosting the site, the nautical-themed subdomain can be integrated seamlessly into a spearphishing topic. In addition to being hard to detect during human inspection, the domain can now bypass automated safeguards by leveraging the trust associated with .gov domains.

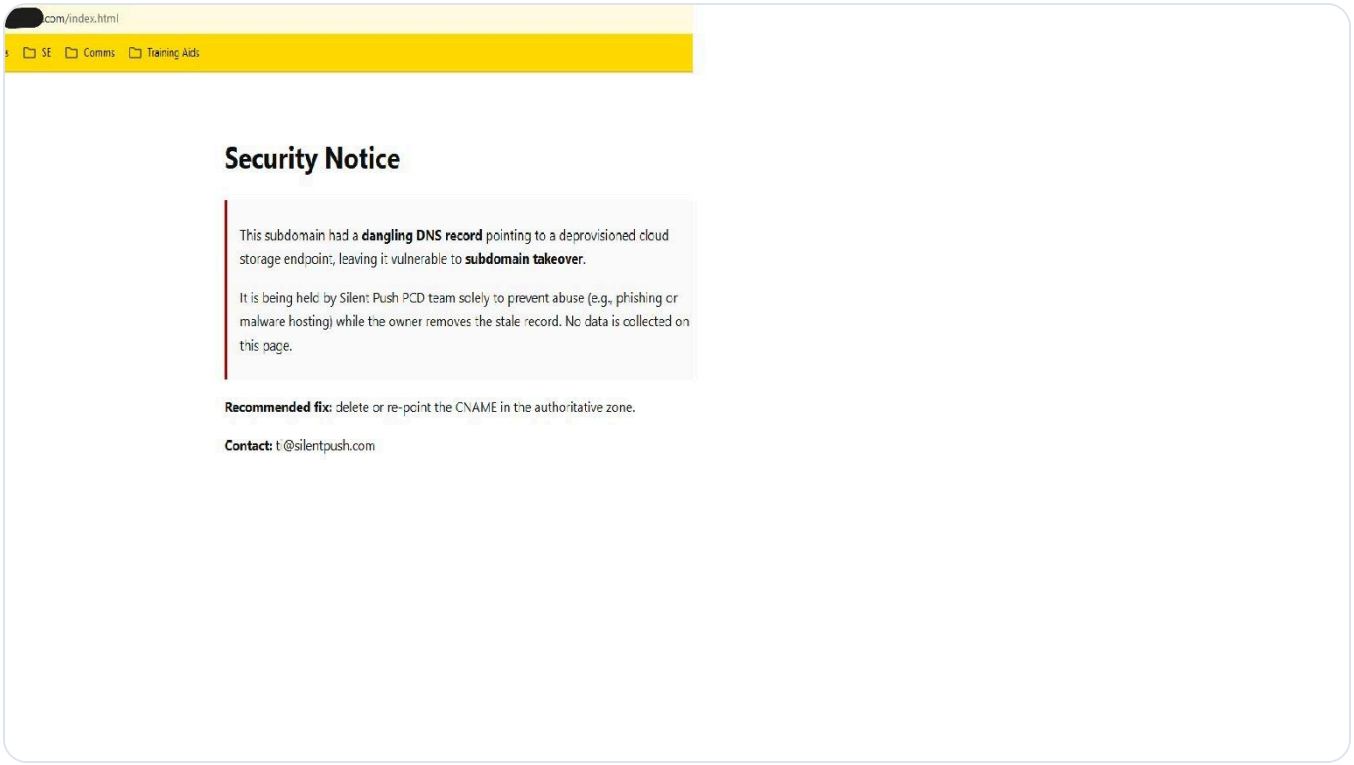
It is fairly obvious to see how a phishing domain leveraging the public trust of a federal organization, current events, and valid TLS certifications can lead to mass exploitation of U.S. citizens and beyond.

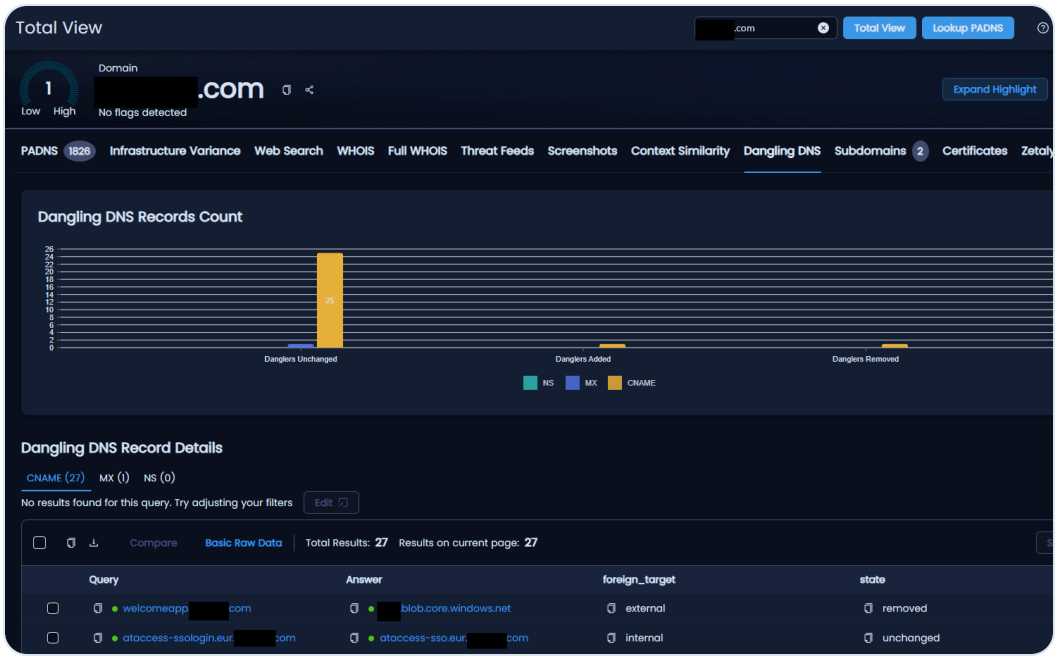


SILENT PUSH TOTAL VIEW QUERY FOR FEDERAL AGENCY INFRASTRUCTURE

BANKING SIMULATION 02 / 04

In our second sampling, we isolated a large French global bank. This company faced the same IT hygiene issue as its U.S. sibling. It had left an unassigned Azure Blob storage resource pointing to an application.

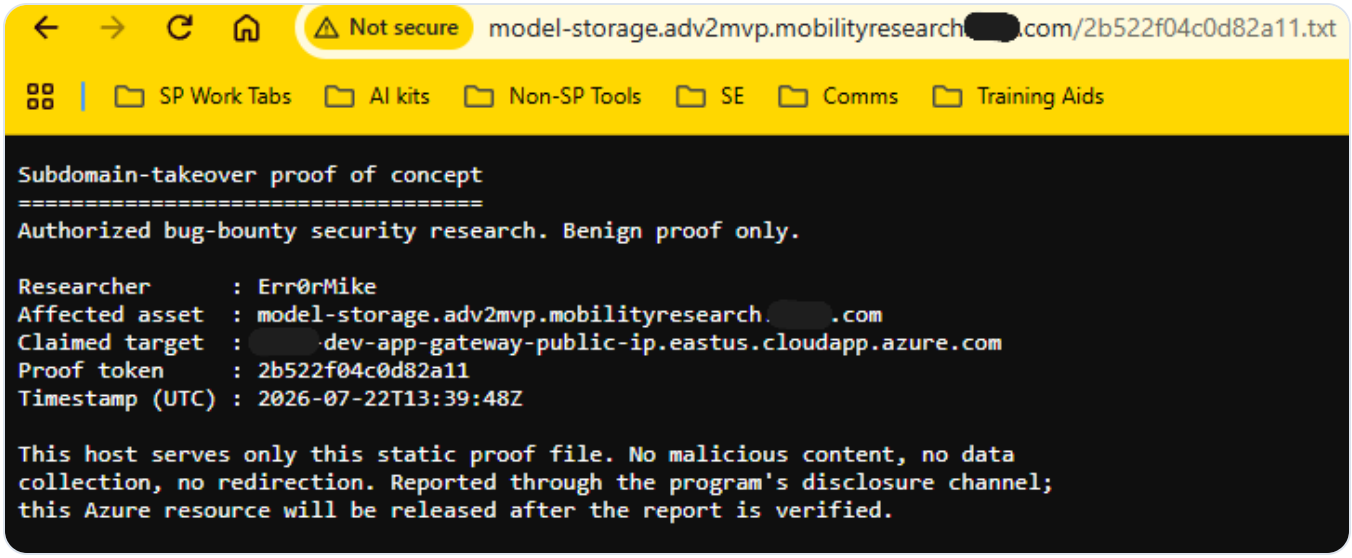




SILENT PUSH TOTAL VIEW QUERY FOR FINANCIAL ORGANIZATION INFRASTRUCTURE

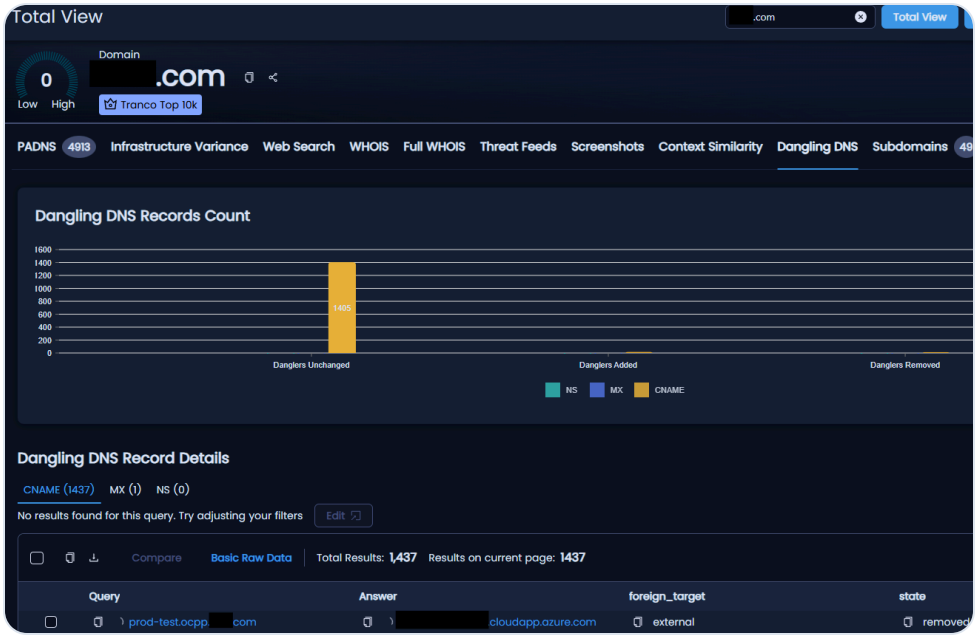
AUTOMOTIVE MANUFACTURING SIMULATION

Our third simulation is a beloved Fortune 500 U.S. automotive manufacturing titan.



The company left a dangling DNS record pointing to a developmental application gateway hosted by an Azure virtual machine (VM). This device can potentially be operationalized and passively receive stored XSS from internal scripts and API calls.

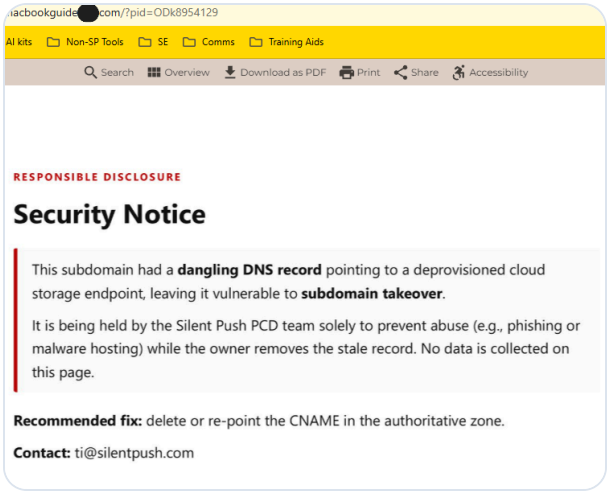
Developer's credentials, like API keys and authentication headers, could be harvested for reuse to expand access into the company. In addition, this VM is fully capable of providing a platform for malware hosting with the coveted TLS lock.



SILENT PUSH TOTAL VIEW QUERY FOR AUTOMOTIVE ORGANIZATION INFRASTRUCTURE

PHARMACEUTICAL SIMULATION 04 / 04

A major pharmaceutical company we identified left a record pointing to an Apple device guide. This presented a strong thematic which could allow an attacker to focus on a specific set of targets and events.



As proof of the discovery process, we found an online publishing platform, Paperturn, that allowed for custom CNAME assignment. The platform can host and convert files, such as PDFs.

SILENT PUSH TOTAL VIEW QUERY FOR PHARMACEUTICAL ORGANIZATION INFRASTRUCTURE

SECTION 06

USING THE PLATFORM: A PROACTIVE HUNTING MECHANISM WITH AI INSTRUMENTATION

Claude excelled at bulk data summarization coupled with Silent Push's DNS dangling records search:

SP enablement — the stats worth showing off

Metric	Result
Danglers surfaced per SP API call	5.88
Wasted calls avoided by counts-precheck	10,547 of 12,527 apexes (84%)
Reduction, raw SP records → triage queue	85,254 → 258 (330:1)

Coupled with some simple availability checks to see if the resource could be taken over:

Verdicts

Sweep	Rows	🔴 Confirmed claimable	🟢 Not claimable	🟡 Manual verify
Internet-wide (91 fingerprints)	16,544	4,066	4,925	7,393

> The hypothetical scenario of a Danglegeddon became a very real threat in minutes.

After clearing the context window and the agent team swapping in Claude, the automation of the infrastructure build-out was a simple task, bypassing any CVP flags and setting us one button away from Dangle Day.

AN ANALYSIS ENGINE TO INFORM MITIGATIONS

Everything described so far was possible because of how the underlying data is collected. Most subdomain takeover hunting starts with a guess. An analyst picks a target, runs a wordlist against it, resolves what comes back, and checks whether any of the answers point at an unclaimed resource. That approach only finds hostnames someone thought to guess, for the one organization being tested, and at the moment the scan runs.

> Silent Push doesn't guess. We re-resolve every hostname in our dataset every day.

When a CNAME's target stops resolving, when an MX host disappears, when a delegated name server goes quiet, we see the answer change the day it happens, across the entire namespace we observe rather than one target at a time. Dangling records surface as a byproduct of continuous resolution, rather than as a scan you have to launch.

That distinction matters more for defenders than for attackers. Records that get an organization compromised are the ones nobody remembers creating. They do not appear in the CMDB, they were not in scope for the last pentest, and they belong to a team that reorganized two years ago. Asking an organization to scan its own infrastructure only finds what it already knows it owns. Our discovery process has no such dependency, which is why the 12,527 apex domains in this study yielded 85,254 raw dangling records and 16,544 rows worth reviewing.

12,527	85,254	16,544
apex domains in this study	raw dangling records yielded	rows worth reviewing

READING THE DANGLING DNS VIEW

The screenshots in their respective sections below show the Dangling DNS tab inside Total View, our single-pane record for a domain. Note the tab strip across the top: PADNS, WHOIS, Certificates, Subdomains, and Threat Feeds. Dangling DNS sits beside them because it is one facet of the same record; anything found here pivots directly into passive DNS history, certificate issuance, and the rest of the organization's footprint without leaving the page.

TWO PANELS DO THE WORK.

NS MX CNAME

The Dangling DNS Records Count chart buckets findings into Danglers Unchanged, Danglers Added, and Danglers Removed, with record type color-coded: teal for NS, blue for MX, and yellow for CNAME. Because we re-resolve daily, this is a change ledger rather than a snapshot. Unchanged is a standing exposure that has survived at least one collection cycle. Added is new exposure created since the last one, which is the bar a defender should be alerting on. Removed shows records that were cleaned up or that stopped resolving entirely.

The Dangling DNS Record Details table below breaks out the same findings out by type, with a count on each tab, and four columns per row. “Query” is the organization's own hostname. “Answer” is where that hostname still points. Foreign_target marks the answer as internal or external, telling whether the broken pointer lands somewhere the organization still controls, or somewhere it does not. External is where takeover risk lives. State carries the same unchanged or removed status as the chart.

SCREENSHOT OF SILENT PUSH TOTAL VIEW AS SEEN IN THE PLATFORM

The volumes in these four screenshots are the point. A financial organization with 27 dangling CNAMEs and a dangling MX. An automotive manufacturer with 1,437 dangling CNAMEs on a single apex. A pharmaceutical company with 271, including the Paperturn record we used in the simulation. A federal agency with 221 dangling CNAMEs, 10 dangling MX records, and a dangling NS delegation, several of them pointing at unclaimed Azure Blob Storage. None of these organizations knew. Every one of them was reachable through a public disclosure channel.

FINANCIAL

27

dangling CNAMEs, plus a dangling MX

AUTOMOTIVE

1,437

dangling CNAMEs on a single apex

PHARMACEUTICAL

271

including the Paperturn record

FEDERAL AGENCY

221

CNAMEs, 10 MX, one NS delegation

WHY CNAME, MX, AND NS EACH CARRY A DIFFERENT KIND OF RISK

DANGLING CNAME

The hostname still answers, but the service it aliases has been deprovisioned. Whoever claims the resource name at the provider inherits the hostname, the parent brand's reputation, and, in most cases, a valid TLS certificate through automated domain validation. This is the condition we exploited in every simulation. It is also the most common by a wide margin, which is why the yellow bar dominates all four charts.

DANGLING MX

Mail addressed to the domain is being routed to a host that no longer exists. Two consequences follow. Legitimate mail fails silently, including DMARC reports and anything routed through that exchanger. More seriously, an attacker who can claim or re-register that mail host receives inbound mail addressed to the organization. That means password reset links, invoices, vendor correspondence, and the email-based verification step that gates certificate issuance and account recovery at most providers.

DANGLING NS

This is the worst of the three and the least common, which is exactly why it gets missed. A dangling NS record means a zone or subzone has been delegated to a name server that no longer answers, usually because a domain lapsed or a hosted DNS zone was deleted. Anyone who takes control of that name server controls the entire zone beneath it. Not one hostname: every hostname, plus the ability to create records that never existed, including A, MX, and the TXT records used for wildcard certificate validation. One dangling NS record can be worth more to an attacker than a thousand dangling CNAMEs.

SECTION 07

WHAT TO DO ABOUT IT

ORDER OF BLAST RADIUS

NS → MX → EXTERNAL CNAME → INTERNAL

Work the record types in order of blast radius. NS first, then MX, then external CNAMEs, then internal.

For each record, the fix is to delete it from the authoritative zone. Re-point it only if the service behind it is genuinely still in use. Where a hostname is still referenced by live pages or scripts and the underlying resource is still claimable, reclaim the resource defensively first, then remove the reference and the record.

The process fix is a sequencing rule: the DNS record dies before the cloud resource does. Most of the exposure in this study exists because teams deprovisioned a storage account, a web app, or a VM and left the record behind. Reversing that order in decommissioning runbooks eliminates the condition at the source.

THE DNS RECORD DIES BEFORE THE CLOUD RESOURCE DOES.

RECOMMENDATIONS

01 Prefer providers that require domain ownership verification before accepting a custom hostname. In Azure, that means the asuid TXT verification record specifically. The 4,925 records we found to be unclaimable could be protected by exactly this kind of provider-side safeguard.

02 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 currently trigger a DNS review at most organizations.

03 Publish CAA records to restrict which certificate authorities can issue for your namespace, and monitor certificate transparency logs for issuance you did not request.

04 Audit any security control that allows lists by domain suffix/TLD. A subdomain taken over from a trusted brand passes those filters.

05 Monitor continuously rather than periodically. Our Dangling DNS API returns these findings programmatically, so this becomes a scheduled job that alerts the SecOps and IT teams instead of a quarterly project.

SECTION 08

CONCLUSION

The objective of this research initiative was to develop a few simple ways for organizations to better identify vulnerabilities and defend against attackers who leverage existing internet infrastructure against them.

To achieve this, it was necessary to run the attack simulation to analyze infrastructure samples from organizations across a few key industry sectors. We used the same set of techniques throughout the simulation to successfully take over “dangling” infrastructure associated with each targeted organization and, within a safe and controlled environment, redirect it to demonstrate how easily it could be exploited on the open internet.

Our intent with this initiative is to raise awareness of how extremely dangerous dangling DNS domains and subdomains can be when organizations are not practicing secure IT hygiene across their networks.

As evidenced by our approach scoping, the downstream impact of dangling DNS takeovers, assessed across a small but significant sample of global infrastructure, paints a clear picture of how quickly and easily organizations can be exploited, especially since attackers can simply stand up third-party infrastructure for exactly this purpose.

In addition to adhering to consistent IT hygiene practices, organizations can use the Silent Push Platform to identify dangling infrastructure and other assets, among other proactive measures, to preemptively protect their networks.

> Despite the significant business and critical service disruptions in this scenario, Microsoft is just one cloud provider among many carrying this same exposure. The substantial non-Microsoft infrastructure still out in the wild represents an enormous attack surface we'll explore in a follow-up to this report.

SECTION 09

ABOUT SILENT PUSH RESEARCH

The Silent Push Research team is spearheaded by Mike Sweeney. Michael Sweeney is the Director of Preemptive Cyber Defense at Silent Push, where he leads the team in delivering proactive cyber defense through actionable intelligence on emerging threat infrastructure and adversary tradecraft.

Michael brings over 15 years of experience in cyber operations and intelligence, with deep expertise in APT attribution, threat actor tracking, and translating complex technical data into strategic intelligence.

He has directed multi-disciplinary teams, designed detection and intelligence systems, established intelligence production standards and governance frameworks, and built cross-functional partnerships across government, law enforcement, and industry.

VISIT OUR RESEARCH PAGE.

MICHAEL SWEENEY

Director of Preemptive Cyber Defense, Silent Push

SILENT PUSH

FIND YOUR DANGLING INFRASTRUCTURE BEFORE SOMEONE ELSE DOES

Silent Push is a Preemptive Cyber Defense Platform. We re-resolve the namespace every day, so exposure surfaces the day it appears.

REQUEST A DEMO

VISIT WEBSITE

NEUTRALIZE BEFORE COMPROMISE

Silent Push, Inc.
12020 Sunrise Valley Drive, Suite 100
Reston, VA 20191

+1 (703) 860-6398 / info@silentpush.com