Beyond the Web:
Non-Web Attack Surface Report

Table of Contents

Executive Summary_

Cyberthreats continue to evolve as attackers weaponize non-web protocols to evade detection and stage sophisticated attacks across industries. Protocols like SSH, SMB, and SMTP are increasingly manipulated to launch covert communications, maintain persistence, and exfiltrate sensitive data—all while escaping traditional network defenses.

ThreatLabz uncovered that DNS attacks are among the most prominent, leveraging techniques like tunneling and dynamic domain generation to disguise malicious activity within legitimate queries. Tools like Cobalt Strike are used to establish stealthy command-and-control (C2) connections, demonstrating how attackers continue to innovate within traditional systems.

Retail, manufacturing, healthcare, and energy industries are especially vulnerable, with complex supply chains and legacy systems presenting attackers with exploitable gaps. Emerging abuse of SMTP and SSH is creating opportunities for credential theft, ransomware delivery, and lateral movement within networks. Meanwhile, P2P applications like Torrent have proven effective for malware distribution, botnet operations, and discreet data exfiltration using steganographic techniques.

Legacy vulnerabilities remain a major risk factor, with attackers exploiting gaps in protocols like SMB and NTP. Additionally, tunneling tools like Chisel and anonymizer networks such as TOR are enabling attackers to bypass detection and maintain footholds across compromised environments.

Zscaler ThreatLabz dives deep into this hidden attack surface, charting the methods and motivations driving non-web threats and providing industry-specific insights to counter the rising tide of protocol exploitation.

Key_ Findings

DNS emerges as the most abused non-web protocol and is exploited via tunneling, dynamic records, and algorithmic domains to bypass security, supporting C2, data exfiltration, and evasive communications.

Retail, manufacturing, healthcare, technology and energy sectors are under siege by exploited protocols and face persistent attacks exploiting protocols like DNS, SSH, SMTP, and SMB.

Critical infrastructure is experiencing widespread SSH abuse and used in covert communication, lateral movement, and anonymized malicious operations through tunneling and identity obfuscation tools.

Legacy CVEs fuel persistent exploits as outdated vulnerabilities continue to be favored entry points, allowing threat actors to execute remote commands, achieve lateral movement, and compromise networks with alarming success.

Brute force attacks targeting RDP and SMB are the most exploited.

Cobalt Strike is the preferred C2 tool for a majority of threat actors across all observed C2 communications.

Protocols_Under Fire: DNS Leads Non-Web Threats

DNS plays a pivotal role in internet connectivity, but it is also a top target for threat actors who want to exploit its inherent accessibility and weaknesses. As shown in Figure 1, DNS accounts for an overwhelming 83.8% of observed non-web threats, making it the most exploited protocol by attackers. Because DNS traffic is almost always permitted through firewalls, attackers use it as an entry point to conceal malicious operations. By blending harmful activity with legitimate queries, DNS has been turned into a key enabler for covert communication and data theft.

One of the most concerning techniques is DNS tunneling, which allows attackers to exfiltrate data or sustain C2 communication under the guise of normal DNS traffic. Tools like Cobalt Strike leverage tunneling methods to bypass detection and establish lasting footholds. Firewall configurations that lack deep DNS inspections enable these stealth techniques, leaving organizations exposed to unnoticed exploitation. Compounding the problem, standard defenses like IP blacklisting fail when attackers use dynamic domains or constantly update DNS A records to evade detection.

Further amplifying the threat are activities like DNS hijacking, poisoning, amplification, and rogue server exploitation. Unpatched DNS vulnerabilities add additional layers to the risks faced by organizations. The ubiquity of these protocols, combined with their tactical value to threat actors, highlights the growing imperative for robust DNS security measures.

As DNS continues to be a favorite among cybercriminals for its versatility, organizations face mounting pressure to secure this critical protocol. Without vigilance and advanced tools to detect and neutralize DNS abuse, the consequences—from data theft to C2 persistence—could be catastrophic.

Besides these, ThreatLabz observed various malicious activities in other non-web protocols, such as RDP, SMB, FTP, NTP, SSH, SMTP, LDAP, and DHCP, which are detailed throughout this report.

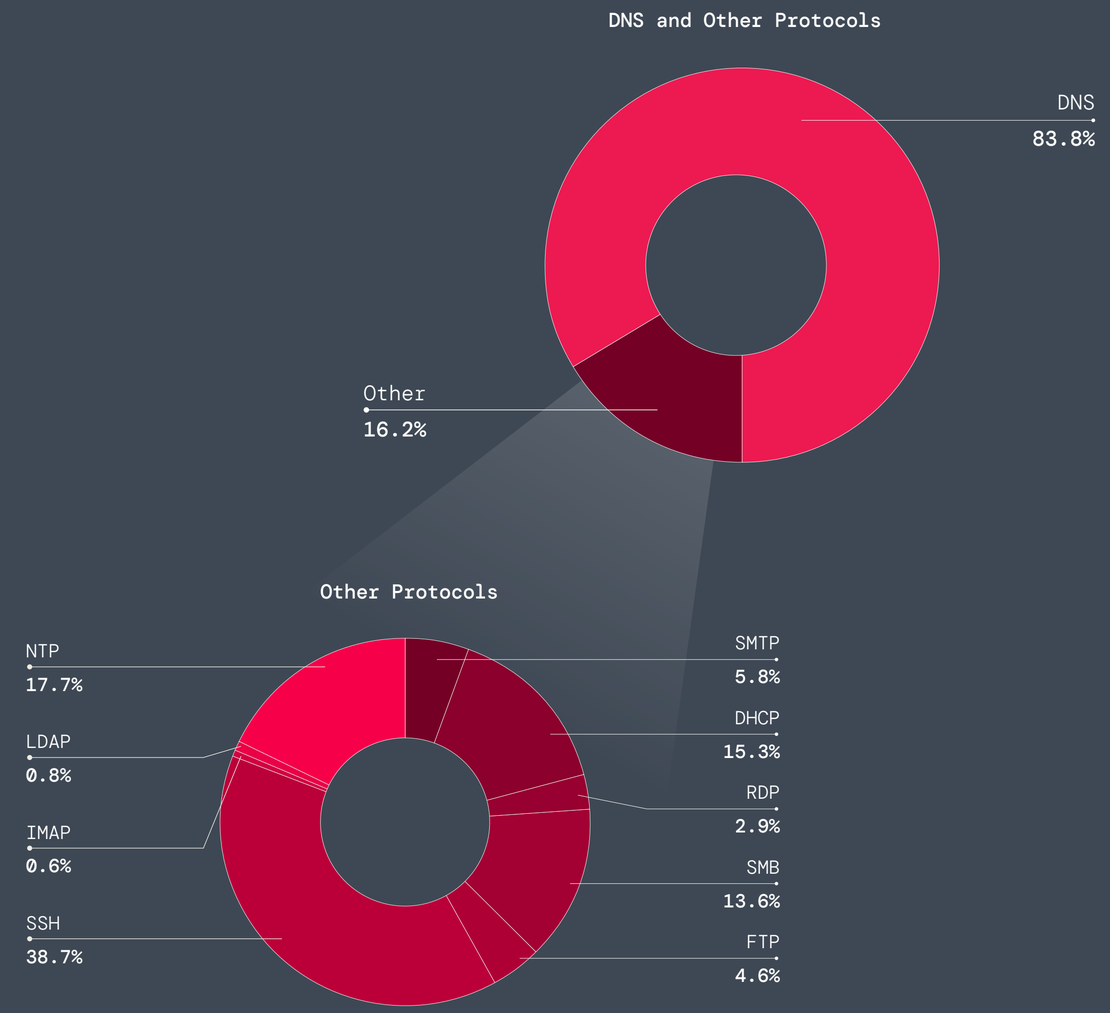


Figure 1: Top targeted sectors overall (top) and a detailed breakdown of the "other" category (bottom)

Critical Industries_Under Attack: Sector Insights on Non-Web Threats

ThreatLabz uncovered that retail emerged as the most targeted industry, receiving 62% of all observed threats, yet industries like manufacturing (8.4%), technology (7.2%), services (4.1%), and communication (4%) exhibit significant threat activity as well (Figure 2).

The retail sector is an ideal target due to their operational dependency and expansive attack surface. ThreatLabz identifies several malware categories targeting this sector including trojans, backdoors, spyware, stealers, and ransomware, with exploitation often beginning through unpatched systems. Seasonal peaks and the necessity for uninterrupted operations exacerbate the impact on retail organizations, incentivizing ransom payments during ransomware attacks.

Other industries are also encountering a notable volume of threat activity, each presenting distinct vulnerabilities ripe for exploitation. Manufacturing has become an increasing focus for attackers, particularly due to inherent weaknesses in industrial control systems (ICS) and operational technologies, which can result in production delays and pose safety hazards.

Similarly, technology firms are consistently targeted for their intellectual property and proprietary assets, with attackers leveraging gaps in code repositories, cloud environments, and development systems to steal critical data or disrupt operations. Services and communication sectors are also facing significant risks due to their reliance on interconnected and decentralized ecosystems, where disruptions can cascade across multiple processes and stakeholders, causing widespread operational impacts.

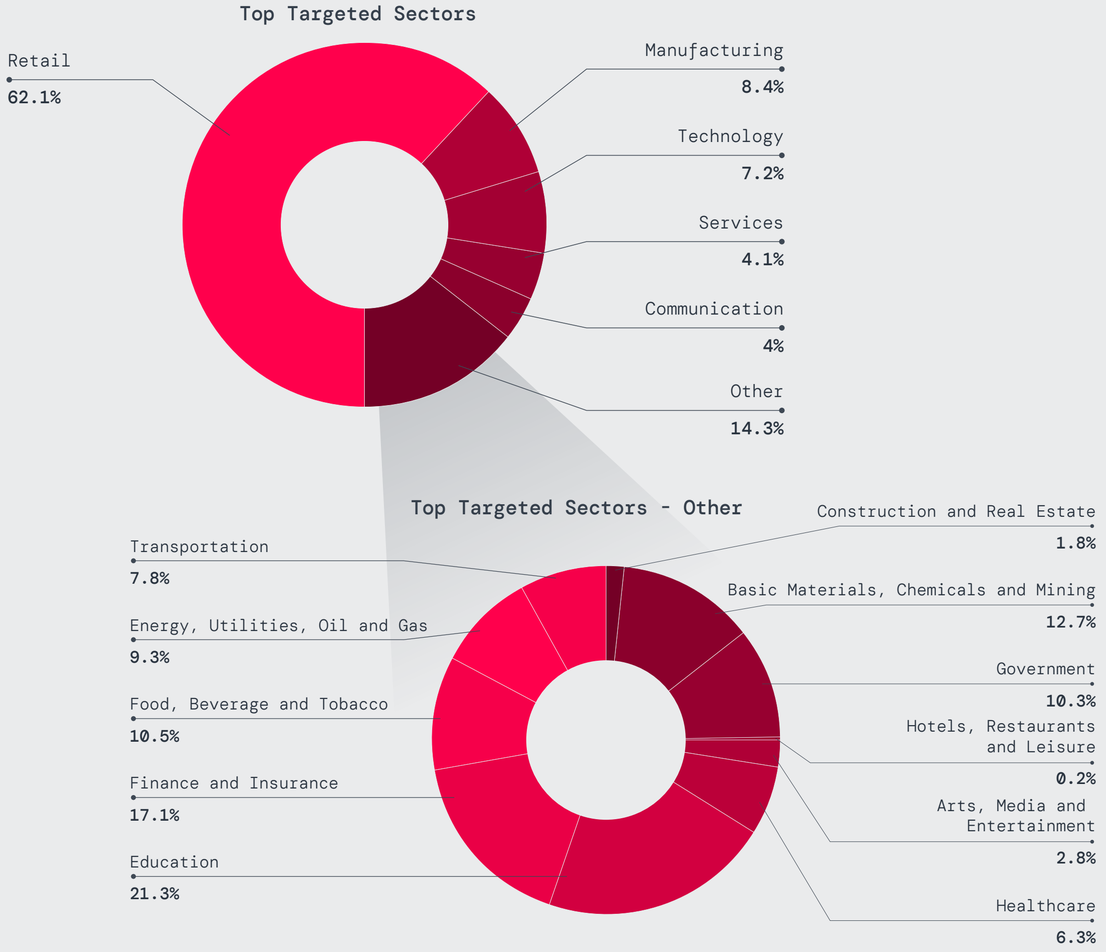
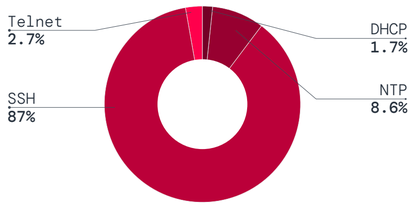
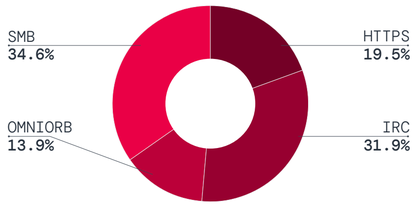


Figure 2: Top targeted sectors overall (top) and a detailed breakdown of the "other" category (bottom)

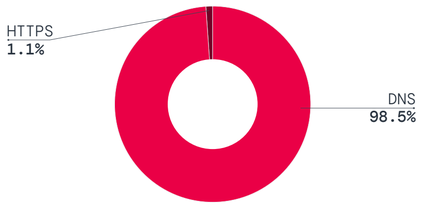
Exploiting_Protocols: DNS and SSH Dominate the Industry Landscape



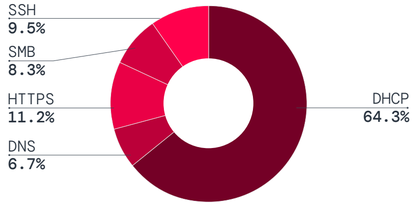
Basic Materials, Chemicals and Mining



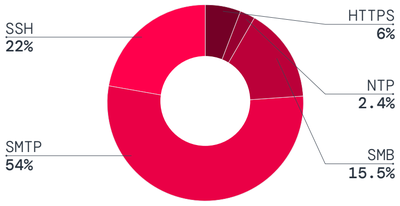
Arts, Media and Entertainment



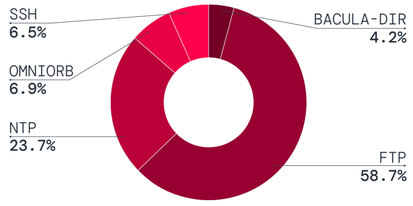
Communication



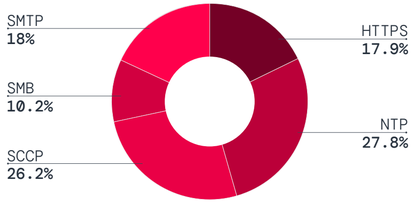
Finance and Insurance



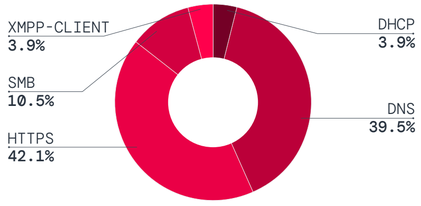
Food, Beverage and Tobacco



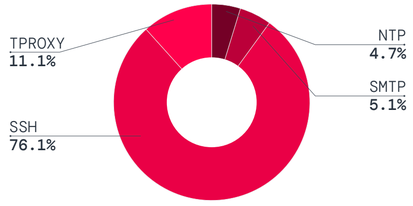
Government



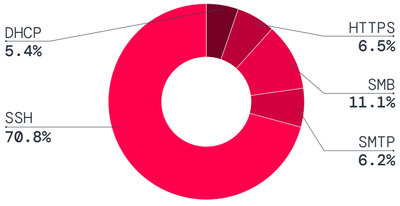
Healthcare



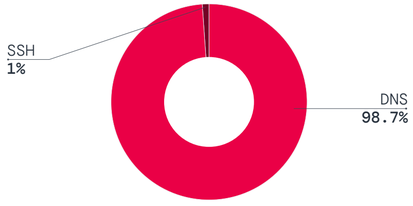
Hotel, Restaurants and Leisure



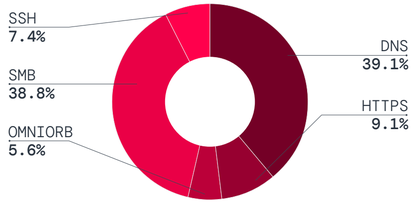
Manufacturing



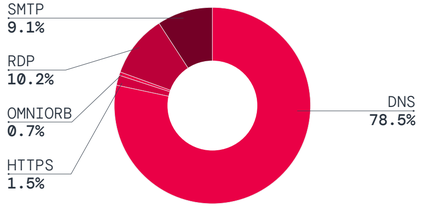
Others



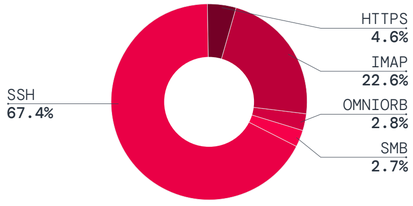
Retail



Services



Technology



Transportation

Figure 3: Industry and threat protocol distribution

Threat actors are systematically exploiting the weakest links within each industry, transforming tailored vulnerabilities into high-stakes battlegrounds. ThreatLabz revealed that DNS is one of the most heavily abused protocols across multiple industries, serving as a primary vector for tunneling malicious payloads and enabling data exfiltration. The retail sector is particularly vulnerable, with 98.7% of attacks leveraging DNS, as seen in Figure 3.

Technology also faces significant DNS exploitation (78.5%), as attackers capitalize on its critical reliance on operational connectivity and cloud-based ecosystems. Similarly, communication (98.5%) and services, along with hotels, restaurants, and leisure sectors, experience notable DNS abuse due to tunneling, phishing campaigns, and malicious payload delivery.

In resource-intensive industries, attackers focus heavily on abusing SSH, exploiting its pivotal role in system administration to gain unauthorized access to sensitive environments. The manufacturing sector (76.1%) sees widespread SSH misuse, while transportation (67.4%) has also emerged as a target. A significant factor driving SSH-based threats, as observed by ThreatLabz, is the strategic use of anonymizers, which allow threat actors to obscure their identities and origins. This obfuscation complicates attribution and mitigation, enabling attackers to conduct malicious operations such as unauthorized access, malware deployment, and data exfiltration—solidifying SSH as the most exploited protocol across all analyzed sectors.

Meanwhile, finance and insurance sectors stand out for DHCP abuse (64.3%), where attackers exploit network misconfigurations to disrupt connectivity and provide unauthorized entry points. Legacy protocols such as FTP remain a persistent vulnerability, especially in the government (58.7%), underscoring the risks posed by outdated infrastructure. Additionally, healthcare faces notable activity over protocols like NTP and HTTPS, where real-time synchronization and secure communications remain vulnerable without adequate defenses.

It's clear that securing commonly exploited protocols across industries is no longer optional but essential. As attackers continue to refine their methods, targeted security strategies addressing commonly exploited protocols must be prioritized to safeguard operations and minimize risks.

Inside the_Attack Chain: Exploits, Anonymizers, and Backdoors Driving Non-Web Threats

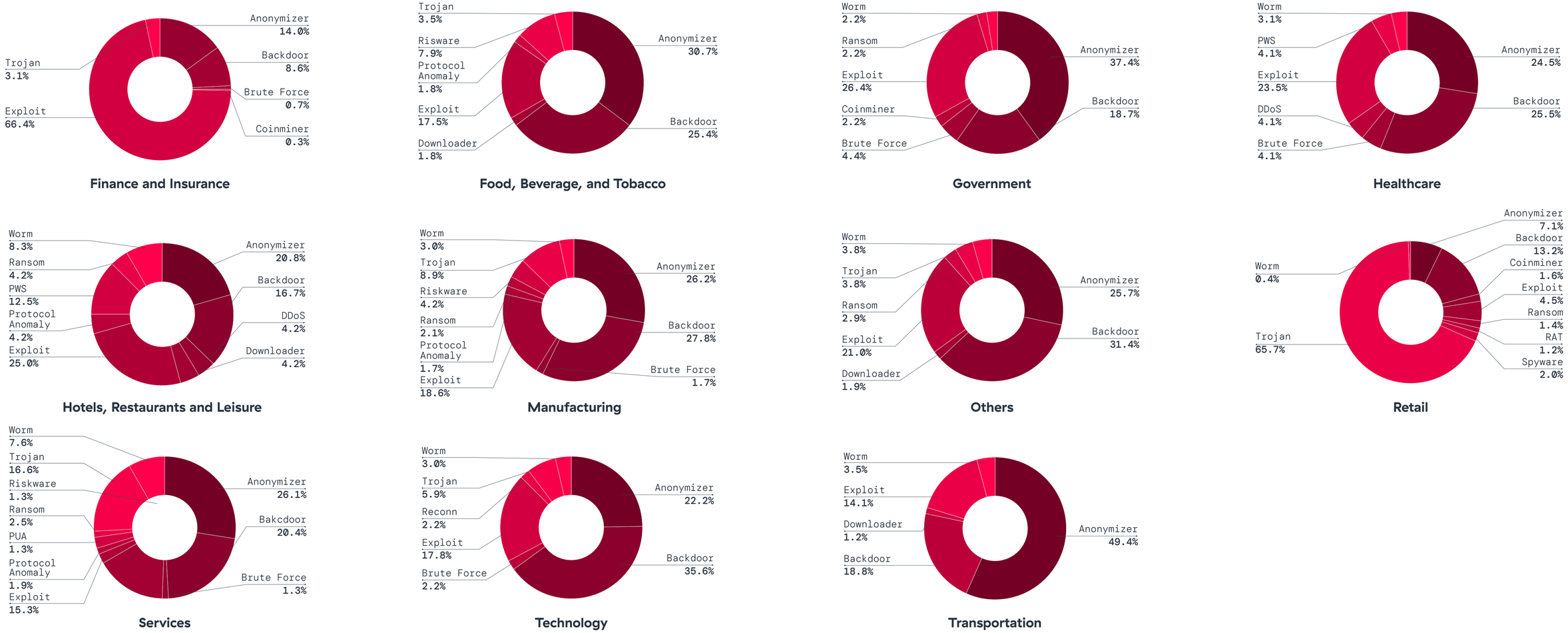


Figure 4: Industry and threat categories distribution

Threat actors are systematically exploiting the weakest links within each industry, employing tailored non-web threat categories to compromise systems and evade detection. ThreatLabz has uncovered that exploits and anonymizers dominate the threat landscape, reflecting the diverse approaches attackers use to infiltrate operational environments. Exploits are especially prevalent in sectors like finance and insurance (66.4%) as shown in Figure 4, and allow cybercriminals to target unpatched vulnerabilities and misconfigurations for unauthorized access and data exfiltration.

In contrast, anonymizers are heavily abused in industries such as transportation (49.4%), allowing attackers to mask identities, evade attribution, and persist within compromised systems. These tools facilitate advanced malicious operations like lateral movement and malware deployment.

Beyond these top threat categories, backdoors also pose substantial risks, particularly in transportation (18.8%) and technology (35.6%),, where attackers leverage persistent access to deploy payloads under the radar. Meanwhile, trojans and backdoors dominate the DNS threat landscape in the retail sector, where malicious DNS activities leverage tools such as CobaltStrike, LemonDuck Coinminer, and spyware like Hermit.

Government, food, beverage, and tobacco sectors face persistent brute force attacks and ransomware threats tied to legacy infrastructure vulnerabilities, making them attractive targets for exploitation. Similarly, brute force activity is heavily observed in the technology sector, where attackers target open RDP ports to gain remote access and establish footholds within critical systems. These attacks underscore the importance of addressing outdated infrastructure and implementing robust defensive measures to mitigate the risk of unauthorized access and system compromise.

As cybercriminals are increasingly tailoring their non-web attack strategies to exploit sector-specific weaknesses, businesses must prioritize layered security approaches, such as endpoint detection, protocol-specific monitoring, and continuous patch management, to mitigate risks effectively and safeguard operations from evolving attacker techniques.

Unseen_Pathways: How Malware Is Redefining Cyberattacks with Non-Web Protocols

Malware leveraging non-web protocols has become a hallmark of modern cyber campaigns, allowing attackers to infiltrate networks while bypassing traditional web-based defenses. By utilizing specialized protocols and advanced techniques, these malicious tools enable data exfiltration, persistence within compromised environments, and the execution of devastating ransomware attacks. ThreatLabz found the most prominent malware families exploiting non-web protocols, providing deep insight into their capabilities and examining their growing impact on the global threat landscape.

Agent Tesla — Backdoor

Agent Tesla is a spyware/backdoor malware designed for credential theft via screen-capturing, keystroke-logging, and targeting browsers, email clients, and FTP applications. Distributed through phishing emails, it uses non-web protocols such as SMTP to exfiltrate stolen data to attacker-controlled mailboxes and FTP for remote uploads. Consistently adapting, Agent Tesla is heavily used in attacks on industries like manufacturing and healthcare, leveraging geopolitical tensions and tax season phishing campaigns to maximize impact. Its affordability and evolving evasion tactics make it a key tool for attackers seeking sensitive data across global targets.

Gh0st RAT — Remote Access Trojan (RAT)

Gh0st RAT is a versatile remote access trojan (RAT) widely used for cyber espionage. It enables attackers to manipulate files, monitor user activities, intercept webcams, and capture keystrokes. Distributed through phishing campaigns or bundled software, Gh0st RAT provides attackers with full control over victim systems. It communicates with C2 servers via raw TCP/IP sockets, often using encrypted data exchanges, reverse-shell connections, or peer-to-peer (P2P) protocols for anonymity. Its newer variants, including SugarGh0st and Gh0stGambit, have made a resurgence since 2024, targeting human rights groups, journalists, and AI researchers across Southeast Asia and the U.S. threat actors, such as Chinese-linked APTs like Nexus, have used Gh0st RAT to steal sensitive information, with notable campaigns like “Operation Diplomatic Specter” employing DNS exfiltration techniques.

XMRig — CoinMiner

XMRig is an open source cryptomining software weaponized by cybercriminals to hijack victim systems and mine Monero, a cryptocurrency known for its strong privacy features. By exploiting CPU and GPU resources, XMRig slows down devices and often causes overheating. It is typically deployed via compromised websites, phishing emails, or exploit kits targeting software vulnerabilities. XMRig communicates directly with cryptocurrency mining pools using Stratum protocols or HTTP-based algorithms, bypassing traditional C2 channels. From late 2024 into 2025, XMRig has been tied to major campaigns, including exploits of cloud vulnerabilities and botnets like LemonDuck. Its adaptability and ease of integration into other malware make it a preferred tool for cryptojacking attacks globally.

AsyncRAT — Remote Access Trojan (RAT)

AsyncRAT is an open source trojan that enables attackers to control infected machines remotely, offering features like keystroke logging, remote file management, and screen monitoring. Deployed primarily through phishing emails, it leverages encrypted TLS communication and DNS tunneling to avoid detection by network defenses. In 2025, AsyncRAT gained traction in multi-step attacks targeting small to mid-sized businesses, often paired with tools like RedLine Stealer or Cobalt Strike for expanded access. Its ease of customization and ability to evade detection make it a widely used tool among cybercriminals and state-sponsored groups alike.

ValleyRAT — Remote Access Trojan (RAT)

ValleyRAT is a lightweight remote access trojan (RAT) commonly deployed via spear phishing emails to grant attackers control over victim systems, including file access and command execution. It uses both unencrypted protocols like HTTP and TCP sockets for basic operations and encrypted SSL/TLS channels for secure C2 communications. Known for advanced evasion tactics such as DLL sideloading and anti-VM checks, ValleyRAT has been tied to espionage campaigns targeting sectors like finance, healthcare, manufacturing, and critical infrastructure. In 2025, it was leveraged in several high-profile attacks, including ransomware-linked campaigns and medical software exploits.

LockBit — Ransomware

LockBit remains a highly dangerous ransomware family operating under the ransomware as a service (RaaS) model, relying on its double-extortion tactics to encrypt files and exfiltrate data for ransom negotiations. Leveraging TOR-based encrypted communication, alongside TCP/IP and P2P mechanisms, LockBit ensures stealth and persistence in its operations. While Operation Cronos in 2024 disrupted its dominance, LockBit 4.0 introduced faster encryption, decentralized infrastructure, and enhanced evasion methods. Healthcare and finance sectors remain prime targets, with attacks underlining its continued threat to global organizations. Leaks from its affiliate network have exposed critical data while aiding investigations, yet LockBit persists as a key player in the evolving ransomware landscape, collaborating with groups like ClOp.

Top Attack Tools Used By Threat Actors

Threat actors are escalating their use of specialized attack tools, weaponizing non-web protocols to bypass detection and breach systems with precision. ThreatLabz has identified a broad toolkit utilized by cybercriminals, ranging from free open source utilities to highly refined commercial platforms. These tools fall into categories such as tunneling mechanisms that embed malicious activities within legitimate traffic streams, anonymizers designed to conceal operational footprints, and reconnaissance tools that meticulously identify vulnerabilities ahead of an attack.
C2 utilities are also heavily leveraged to grant attackers persistent and remote control over compromised environments. The effectiveness of these tools lies in their ability to exploit gaps in traditional web-focused security frameworks, providing attackers with stealth, scale, and efficiency.

Tunneling Tools

Chisel	Chisel is highly favored for its stealth, utilizing tunneling over HTTP/S to mimic legitimate web traffic while employing SSH encryption to obscure payloads. Its lightweight, in-memory binary footprint further enhances its ability to evade detection, making it an effective tool for bypassing security mechanisms.
PageKite	PageKite allows local servers to be exposed to the internet by bypassing firewalls and NAT configurations, creating persistent public URLs. Threat actors leverage it for stealthy communication, security evasion, and data exfiltration, making it an attractive option for advanced persistent threats (APTs).
Zrok	Zrok enables secure and private connections by creating tunnels between devices that are otherwise inaccessible, bypassing network restrictions and firewalls. This functionality is often exploited to facilitate seamless communication, covert data transfers, and unauthorized operations across restricted environments, making it an effective tool for malicious activities.
Jprq	Jprq enables instant access to local web servers by assigning them public URLs, bypassing firewalls and network restrictions. This functionality is exploited to expose internal systems to the internet, allowing for covert communication, unauthorized data exfiltration, and testing malicious payloads directly on compromised environments.
Tunwg	Tunwg leverages end-to-end SSL encryption to securely forward TCP streams to a locally running Tunwg instance. Its encryption capabilities and ability to bypass network restrictions make it an effective tool for concealing malicious activity, enabling covert data transfers and facilitating unauthorized communication channels.
SISH	SISH uses SSH to expose local development servers to the internet, bypassing firewalls and network restrictions. Its secure tunneling capabilities are exploited to enable remote access to localhost services, facilitate covert data exfiltration, and establish unauthorized communication channels in compromised environments.
SSH_J	SSH_J operates as a public SSH jump and port-forwarding server, enabling secure redirection of connections across networks. Its functionality is often exploited to bypass security controls, establish hidden communication channels, and facilitate unauthorized access, making it a valuable tool for malicious activities in restricted environments.

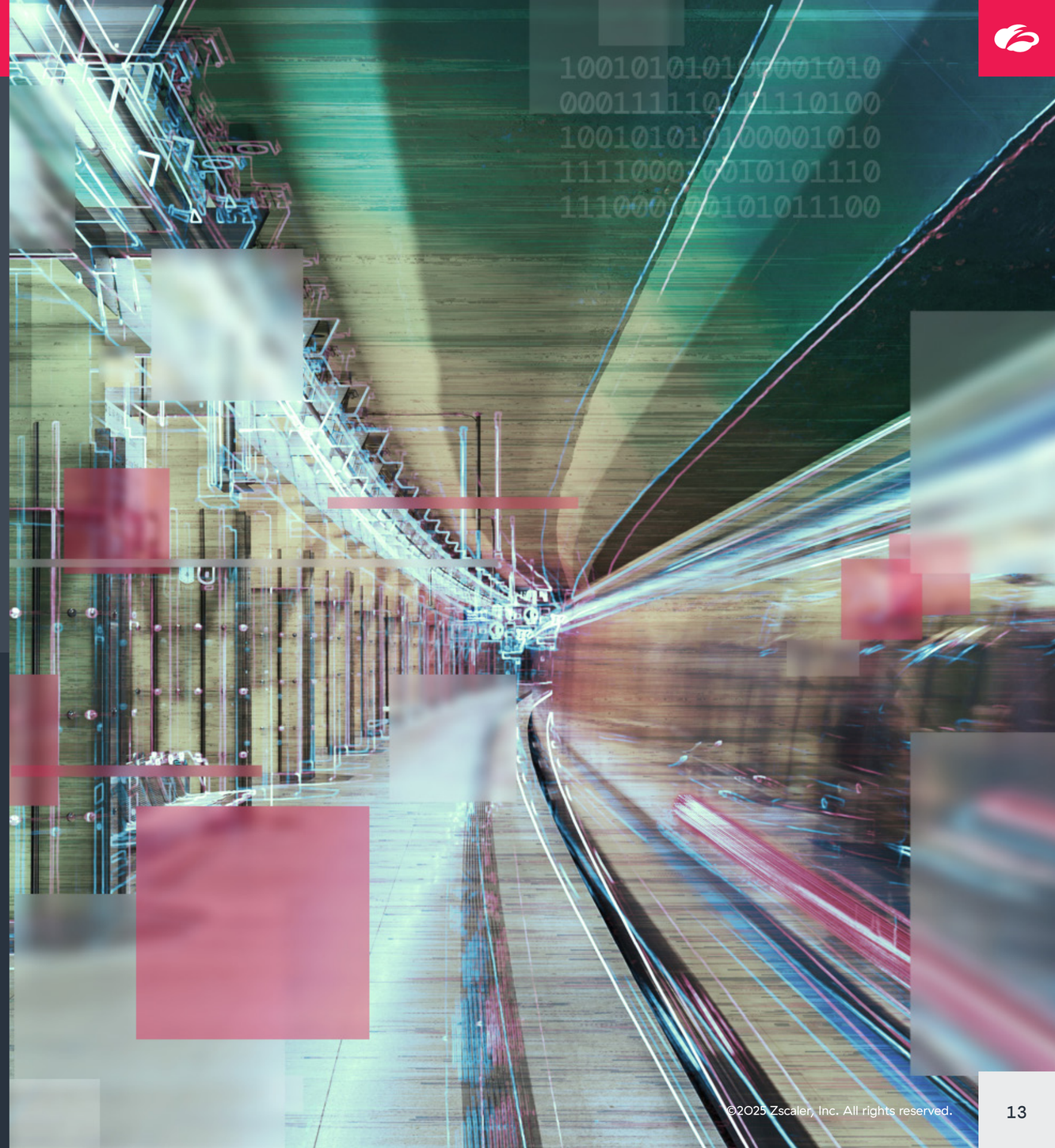
ThreatLabz found Chisel accounts for 98% of tunneling tool traffic, indicating its frequent use by attackers to bypass security. They also observed suspicious communications to endpoints known for distributing CryptoMiners, Trojans, and malware (via PageKite). Less common tunneling tools like Jprq, Tunwg, SISH, and SSH_J were identified, but their malicious use couldn't be confirmed.

Command and Control Tools

Cobalt Strike	Cobalt Strike, a commercial penetration testing tool designed for red teams, is widely used by attackers to conduct sophisticated cyberattacks including ransomware and espionage. Its powerful capabilities, such as Beacon payloads, covert communication, post-exploitation modules, malleable C2 profiles, and flexible payload generation, enable advanced threat operations.
Metasploit	Metasploit, an open source cybersecurity framework, is widely abused by attackers to identify and exploit system vulnerabilities. With features like exploit databases, payload generation, automated exploitation, post-exploitation tools, and multi-platform support, it enables threat actors to simulate attacks, configure payloads, and execute sophisticated exploitation techniques.

ThreatLabz observed significant use of Cobalt Strike for C2 operations, including increased beaconing and malicious activities. DNS TXT records were utilized for stealthy communication, with multiple DNS requests to Cobalt Strike C2 domains and endpoints interacting with historical Cobalt Strike shellcode. Additionally, ThreatLabz detected DNS requests to domains hosting Cobalt Strike's Teardrop, a memory-only dropper, potentially indicating downloads of loaders used for data exfiltration, keylogging, screenshots, and payload deployment.

Metasploit exploitation attempts were also prevalent, with live session beaconing, BIND and reverse shells, and communications with known IOCs targeting enterprise endpoints and critical infrastructure. Adversaries leveraged Metasploit's interactive shell for enumeration, file system interaction, and network manipulation on compromised systems. These observations underscore Metasploit's ongoing relevance in attack chains, where it is often used to exploit vulnerabilities and provide security testing framework for different environments.



Anonymizer Tools

Tor	Tor, short for "The Onion Router", is an open source privacy network that facilitates anonymous communication and browsing. It enhances user privacy by making it difficult to trace online activities and locations. Consequently, threat actors also leverage Tor to conceal their identities and carry out malicious activities.
Psiphon	Psiphon is a free, open source internet circumvention tool that helps users bypass censorship and access blocked websites. It creates a secure tunnel using VPN, SSH, and proxies to provide access to information in countries with internet restrictions and is designed to resist blocking.
Touch	Touch VPN enables users to mask their real IP addresses, encrypt internet traffic. While primarily used for privacy and unrestricted browsing, threat actors may leverage Touch to conceal their identities during cyberattacks, evade detection, and facilitate illicit activities across borders.

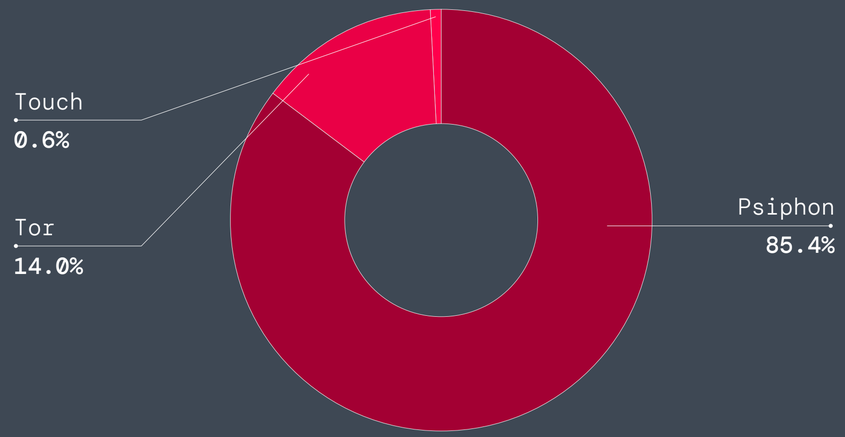


Figure 5: Anonymizer tool usage

ThreatLabz uncovered the extensive use of anonymizers in malicious activities, revealing that Psiphon accounts for 85.4% of anonymizer traffic compared to Tor at 14%, highlighting Psiphon's popularity for both legitimate and malicious purposes. Psiphon implementations using GQUIC protocol have been exploited for persistent C2 connections that bypass security measures. ThreatLabz also identified weak or predictable cryptographic tags in GQUIC communications, presenting vulnerabilities that attackers can exploit.

As seen in Figure 5, Tor remains a key anonymizing tool for covert C2 communications, with adversaries often utilizing Obfs4 to obfuscate traffic. Despite these efforts, ThreatLabz identified anomalies in the TLS handshake, particularly within the Client Hello message, as indicators of compromise.

ThreatLabz also observed njRAT (Bladabindi/Njw0rm), a .NET-based remote access trojan, in targeted campaigns leveraging Psiphon. Attackers are repackaging Psiphon with njRAT to exploit its trusted reputation, tricking users into downloading a malicious version. The infected Psiphon executable operates both legitimate censorship circumvention and njRAT, which establishes a reverse backdoor for credential theft, surveillance, and data exfiltration. Distribution methods include phishing emails and compromised websites using social engineering tactics. Psiphon's encrypted communication does not interfere with njRAT's C2 traffic, typically unencrypted or base64-encoded.

Socks5System proxy malware was also identified, infecting systems to turn them into subscription-based proxy exit nodes. These nodes facilitate anonymous and malicious traffic, enabling attackers to conceal origins, bypass restrictions, and execute illegal activities. Such proxy services add layers of anonymity that complicate detection and attribution of malicious operations.

Probe/Probe_Attempts

Threat actors are escalating their use of specialized attack tools, weaponizing non-web protocols to bypass detection and breach systems with precision. ThreatLabz has identified a broad toolkit utilized by cybercriminals, ranging from free open source utilities to highly refined commercial platforms. These tools fall into categories such as tunneling mechanisms that embed malicious activities within legitimate traffic streams, anonymizers designed to conceal operational footprints, and reconnaissance tools that meticulously identify vulnerabilities ahead of an attack. C2 utilities are also heavily leveraged to grant attackers persistent and remote control over compromised environments. The effectiveness of these tools lies in their ability to exploit gaps in traditional web-focused security frameworks, providing attackers with stealth, scale, and efficiency.

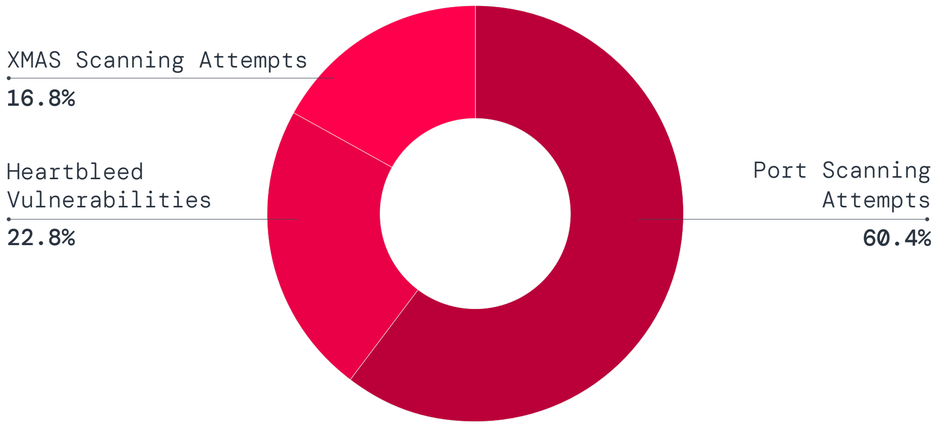


Figure 6: Distribution of probe attempts

Brute Force_Attacks

Brute force attacks remain a persistent and versatile threat, extending far beyond web-based environments. These attacks rely on systematically guessing credentials or keys to gain unauthorized access to systems, devices, and services, often exploiting weak or default passwords or overlooked security configurations. Threat actors use advanced automation tools to target vulnerable endpoints, creating entry points for ransomware, data theft, and other malicious activities. As the techniques evolve, brute force methods are increasingly tailored to compromise non-web platforms, including IoT devices, servers, and remote access tools.

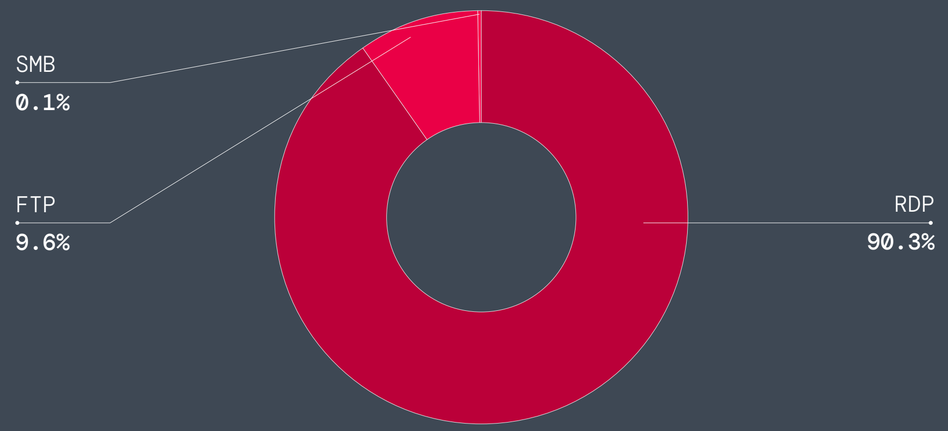


Figure 7: Brute force distribution per protocol

ThreatLabz observed that certain non-web protocols experienced significantly more brute force attempts than others—with RDP, SMB, and FTP leading the list. As shown in Figure 7, RDP accounts for 90.3% of overall brute force traffic. RDP brute force attacks are a significant security threat, where attackers use automated tools to repeatedly guess username and password combinations, targeting exposed RDP services to gain unauthorized access to sensitive systems. These attacks often rely on weak, default, or reused credentials and are marked by numerous failed login attempts.

ThreatLabz has also identified FTP brute force activity, comprising 9.6% of overall brute force traffic. Despite its limited use today, FTP remains vulnerable to bruteforcing attempts, with attackers scanning open ports for initial access, viewing it as easy to exploit.

Similarly, SMBv1 brute force attacks highlight active targeting of this legacy protocol, with threat actors systematically attempting username and password combinations to establish footholds within networks.

DNS_Tunneling Techniques

ThreatLabz uncovered the use of DNS tunneling techniques to conceal malicious network traffic within legitimate DNS requests and responses. By leveraging DNS, which is often allowed through firewalls due to its essential role in internet communication, attackers can create covert channels to bypass security controls, enabling activities such as data exfiltration and C2.

One noteworthy tool is Mythic, an open source, cross-platform C2 platform. Its DNS profile facilitates highly customizable DNS tunneling, allowing operators to embed encrypted and Base64-encoded C2 messages within DNS traffic. This approach disguises communication and data theft within normal DNS queries, making detection significantly harder.

DanaBot, an advanced banking trojan, similarly exploits DNS tunneling techniques. Known for its financial data theft capabilities, DanaBot uses a dual-stack DNS channel in its C2 protocol, employing both IPv4 A records and IPv6 AAAA records alongside HTTP-based communication mechanisms. This layered approach enables attackers to exfiltrate sensitive data while maintaining access to infected systems.

As DNS tunneling continues to gain traction among threat actors, its ability to evade traditional security measures underscores a critical challenge for defenders. C2 frameworks like Mythic and Advanced Trojans like DanaBot demonstrate how DNS can serve as a stealthy vector for malicious activities, particularly in advanced attack campaigns.

P2P_Applications - Torrent Protocol

While the Torrent protocol is widely recognized as a legitimate and efficient file sharing technology, its decentralized design also makes it a favored tool for cybercriminals. Legitimate uses include distributing large updates for software and open source projects, while threat actors exploit its resilient structure to deliver malicious files without a central server, making it challenging to trace sources or shut down operations.

ThreatLabz discovered that approximately 13% of total Torrent traffic is malicious, highlighting its widespread abuse in P2P applications. Cybercriminals leverage torrents for key purposes:

1. **Malware Distribution:** The most common misuse involves bundling malware—such as ransomware, cryptominers, trojans, spyware, or adware—with popular content, including cracked software or games. Malicious files are disguised as desired downloads.

2. **C2 Operations:** Advanced botnets use P2P networks to overcome the single point of failure inherent in traditional C2 models. Botmasters inject commands into private P2P networks, propagating them through infected bots and blending malicious activity seamlessly with legitimate traffic.

3. **Malicious Data Exfiltration:** Attackers break stolen data into smaller chunks, creating private torrents and "seeding" it to attacker-controlled nodes. This tactic mimics standard P2P traffic, avoiding detection while transferring large volumes of sensitive information.

4. **Steganography and Hidden Payloads:** Threat actors embed malicious code within large, seemingly benign files like HD videos. Specialized droppers extract and execute the hidden payload after downloading, making detection significantly more difficult.

The Torrent protocol's dual-use nature underscores the importance of continuous monitoring and robust security controls in P2P environments.

Top Vulnerabilities_ Exploited Over Non-Web Protocols

Exploitation attempts targeting vulnerabilities in non-web protocols are on the rise, spanning both recent CVEs from 2024 and older, unpatched flaws. Threat actors are focusing on critical weaknesses in protocols like SMB, RDP, FTP, and DNS to enable lateral movement, data theft, and ransomware attacks. These vulnerabilities remain a significant risk to organizations, especially when combined with sophisticated techniques to evade detection and bypass security controls. This section analyzes the top vulnerabilities exploited over non-web protocols, their impact on enterprise environments, and the importance of addressing these weaknesses through timely patching and layered security strategies.

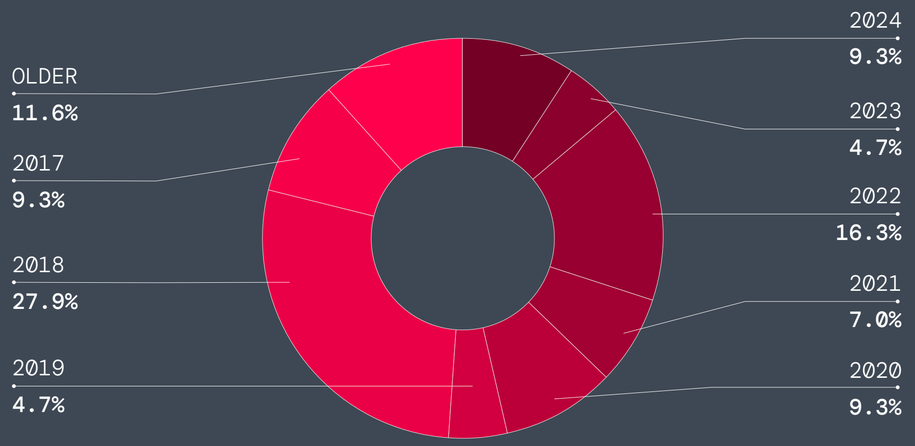


Figure 8: CVE distribution 2017-2024

As shown in Figure 8, even older vulnerabilities—some dating back several years—remain a significant threat. CVEs from as far back as 2017 continue to be actively exploited by attackers for initial access, lateral movement, and executing malicious campaigns. This dispels the misconception that legacy flaws are “low risk” simply due to their age; unpatched vulnerabilities remain high-value targets for threat actors aiming to bypass defenses. Notably, CVE-2019-6443 (NTPsec ntpd ctl_getitem Out of Bounds Read) ranked highest in exploitation attempts, with a large volume of triggers. A surprising number of internet-facing unpatched systems remain accessible, enabling attackers to exploit them for malicious activities.

Top vulnerabilities

CVE-2024-45519

CVE-2024-45519 is a critical unauthenticated OS command injection vulnerability impacting the Zimbra Collaboration software suite. The flaw resides in the postjournal service, responsible for email archiving and compliance. Attackers can exploit this vulnerability by sending specially crafted SMTP messages to the server, triggering the execution of embedded commands with system-level privileges upon processing.

Successful exploitation grants attackers full control of the compromised server, allowing them to deploy web shells, exfiltrate sensitive data, and pivot laterally to compromise additional systems within the network. This vulnerability highlights the severe risks posed by unpatched systems within widely-used enterprise communication platforms.

Citing evidence of active attacks, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its Known Exploited Vulnerabilities (KEV) **catalog**, underscoring the urgency for remediation.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2022-30136

The Windows Network File System (NFS) vulnerability in the NFSv4.1 protocol handler allows remote code execution due to improper size calculations when processing COMPOUND requests. This flaw causes an undersized memory buffer, leading to a buffer overflow when response data is copied. An unauthenticated attacker can exploit this vulnerability to execute arbitrary code with SYSTEM privileges, resulting in full system compromise or a system crash (denial of service) if exploitation fails. Threat actors can use this access to deploy ransomware, steal data, move laterally, and establish persistent access across the targeted network.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2022-28054

CVE-2022-28054 is an OS command injection vulnerability in the VanDyke VShell Server caused by improper neutralization of user-supplied input in the trigger action command functionality. Remote attackers can submit crafted payloads containing shell metacharacters, which are executed by the system's command interpreter. Successful exploitation enables arbitrary code execution (ACE) under the security context of the VShell Server, resulting in a complete compromise of system confidentiality, integrity, and availability (CIA). ThreatLabz has observed a high volume of exploitation attempts targeting this CVE, highlighting the ongoing risk posed by unpatched, internet-facing systems vulnerable to malicious activities.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2022-35742

CVE-2022-35742 is a denial of service (DoS) vulnerability in Microsoft Outlook caused by improper handling of MIME headers. Attackers can exploit this flaw by sending specially crafted emails that trigger automatically when retrieved and processed by the email server, creating a DoS condition before being viewed in the Preview Pane. Successful exploitation can result in persistent service disruption, performance degradation, and system failures, ultimately impacting email communications and business operations. This vulnerability highlights the potential operational risks posed by MIME Header parsing flaws in widely used application platforms.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2021-28325

An information disclosure vulnerability in the SMBv2 component of the Microsoft Windows SMB service is caused by improper handling of uninitialized memory during read operations. A remote, authenticated attacker can exploit this flaw by sending a crafted SMB2 CREATE request, granting access to kernel memory. Using even low-privilege credentials, attackers can repeatedly extract small, random chunks of kernel memory, potentially exposing sensitive data like password hashes or cryptographic keys. Exploitation may enable lateral movement and deployment of malicious backdoors and trojans, highlighting the critical impact of unpatched SMB vulnerabilities on Microsoft Windows.

More information about this vulnerability can be found in the NVD description and the Zscaler Threat Library.

CVE-2021-36754

CVE-2021-36754 is a critical vulnerability in the PowerDNS Authoritative Server that enables remote attackers to trigger a denial-of-service condition. Exploitation occurs when a specially crafted DNS query with QTYPE 65535 causes an uncaught out-of-bounds exception, crashing the server process. Successful attacks can disrupt essential online services, leading to operational downtime, financial losses, and reputational damage. ThreatLabz observed exploitation attempts targeting multiple PowerDNS servers, originating from endpoints previously associated with malicious activities such as malware distribution, highlighting the continued threat posed by unpatched systems in sensitive infrastructure environments.

More information about this vulnerability can be found in the NVD description and the Zscaler Threat Library.

CVE-2020-1350

CVE-2020-1350, known as SIGRed, is a critical "wormable" vulnerability in Windows DNS Server that poses a severe risk to network infrastructure. An unauthenticated attacker can exploit this flaw by sending a malicious DNS query, resulting in code execution with LocalSystem privileges—the highest authority on the server. Due to its wormable nature, the malware can autonomously spread between vulnerable servers without requiring user interaction, enabling rapid and widespread compromise across networks. As Windows DNS is a core service, this vulnerability highlights the need for immediate patching to prevent large-scale exploitation and disruption.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalog.

More information about this vulnerability can be found in the NVD description and the Zscaler Threat Library.

CVE-2020-0601

The Windows CryptoAPI (Crypt32.dll) contains a spoofing vulnerability in its validation of Elliptic Curve Cryptography (ECC) certificates, allowing attackers to bypass trust mechanisms. Adversaries can exploit this flaw to make malicious software appear signed by trusted organizations, enabling man-in-the-middle (MiTM) attacks and bypassing security warnings. Attackers can issue fraudulent certificates, exploiting browsers reliant on Windows CryptoAPI to decrypt traffic, modify communications, and steal sensitive user data. While ThreatLabz has observed limited exploitation attempts tied to malicious endpoints, CISA's inclusion in the KEV catalog highlights the critical need for immediate patching to mitigate risks.

More information about this vulnerability can be found in the NVD description and the Zscaler Threat Library.

CVE-2019-0787

A remote code execution vulnerability in the Windows Remote Desktop Client can be exploited when users connect to malicious servers, allowing attackers to execute arbitrary code. Successful exploitation grants adversaries control to install programs, alter or delete data, and create accounts with administrative privileges. Threat actors employ techniques such as social engineering, DNS poisoning, or MiTM attacks to lure victims into initiating connections. Microsoft has issued a security update to address this flaw, but some attackers continue exploiting unpatched RDP clients to deploy trojanized malware installers, stealers, and droppers, and exfiltrate sensitive data. Immediate patching is strongly recommended.

The continued exploitation of this legacy vulnerability highlights the persistence of unpatched systems in active environments. More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2019-6443

NTPsec's ntpd contains an out-of-bounds read vulnerability due to insufficient validation of NTP packet message lengths. This flaw allows unauthenticated remote attackers to send specially crafted packets, resulting in memory reads outside the allocated buffer. Such vulnerabilities can trigger program crashes, erratic behavior, or security breaches. ThreatLabz observed a significant spike in exploitation attempts targeting this CVE, indicating that many unpatched, internet-facing NTP servers remain vulnerable. These servers are actively being leveraged by threat actors for malicious activities, underscoring an urgent need for updates and remediation.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2018-2628

Oracle WebLogic Server is impacted by a remote code execution vulnerability in its Core Components subcomponent, stemming from unsafe deserialization of Java objects via the RMI registry. Threat actors can exploit this flaw by sending crafted Java objects to execute arbitrary code, resulting in server takeover. CISA has added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalog due to active exploitation in the wild. Observed attacker behaviors include deploying backdoors, webshells, and malicious scripts for remote administration, data exfiltration, and expanding control over compromised systems. Immediate patching is critical to mitigate this risk.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2018-7074

A stack buffer overflow vulnerability in HPE Intelligent Management Center (iMC) PLAT arises from improper validation of user-supplied data in TFTP packet handling. Specifically, the vulnerability stems from overly large block size parameters improperly copied to a fixed-length, stack-based buffer. Threat actors exploiting this flaw can execute arbitrary code on affected systems, potentially leading to full compromise of the HPE iMC server.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2017-0143

CVE-2017-0143 is a remote code execution vulnerability in Microsoft Server Message Block 1.0 (SMBv1) caused by improper handling of specific requests. An attacker can exploit this flaw by sending a specially crafted packet to the target SMBv1 server, potentially executing arbitrary code. In most scenarios, exploitation requires authentication, enabling the attacker to gain control over the server and perform unauthorized actions. The vulnerability underscores the importance of disabling SMBv1 or applying available patches to reduce exposure to potential exploitation,

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its KEV **catalog**. Multiple critical vulnerabilities in SMBv1, from CVE-2017-0143 till CVE-2017-0148, are known to be exploited by WannaCry and NotPetya ransomware campaigns.

ThreatLabz observed a large number of probes for SMBv1 which suggests that Threat Actors are still actively looking for unpatched systems running SMBv1 for exploiting a set of known vulnerabilities existing in it.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

CVE-2017-10986

A denial of service vulnerability in FreeRADIUS, identified as CVE-2017-10986, allows a remote attacker to crash the server. The flaw originates in the dhcp_attr2vp() function, which enters an infinite read loop when processing a malformed DHCP request. By sending a crafted packet, a threat actor can exploit this bug to trigger a server crash. A successful exploit would disrupt essential authentication and network services, leading to significant operational outages, financial repercussions, and reputational damage for the affected organization.

ThreatLabz observed a few attempts exploiting the vulnerability for multiple FreeRADIUS servers. Attempts were made from the endpoint which had a history of malicious activities of spreading malware.

More information about this vulnerability can be found in the **NVD description** and the **Zscaler Threat Library**.

How Zscaler Zero Trust Firewall Protects Against Non-Web Threats

Non-web threats continue to pose significant challenges to traditional security measures. Attackers weaponize the most common protocols like DNS, DoH, SSH, SMB, RDP and many others often in concert with encrypted web to evade detection and conduct mutli-stage attack operations. Zscaler's Zero Trust Firewall provides a robust capability to address these emerging threats, leveraging advanced inspection capabilities based on zero trust principles and architecture to safeguard global organizations against protocol exploitation, lateral movement, and communication with malicious entities.

1. Advanced Policy Enforcement with Least Privilege Access

Zero trust enforces least-privilege access across all protocols and applications, eliminating unnecessary exposure to malicious activity for all corporate users, devices, server, and workloads no matter where they are located. By segmenting access based on user roles, device identity, and contextual risk, the Zscaler Zero Trust Exchange ensures only authorized users access sensitive resources. Targeted defenses include:

- RDP and SMB Security: User and application-specific segmentation prevents unauthorized access to services, minimizing avenues for brute-force or automated attacks.
- SMTP Protections: Email protocols are fortified with strict filters preventing credential harvesting, phishing payload delivery, and ransomware distribution attempts.

2. DNS Security

The Zscaler Zero Trust Firewall ensures all traffic is inspected by the Zero Trust Exchange including all DNS traffic—whether standard or encrypted—and secures the content of all DNS communications through the following capabilities:

- Ability to monitor and apply policies to all DNS requests and responses, irrespective of the protocol and the encryption used. This includes UDP, TCP, and DNS over HTTPS (DoH) via a variety of conditions such as per user, group, department, DNS request/response type, resolver used, etc.
- Enforce condition-based actions on DNS traffic, such as allowing or blocking traffic, redirecting requests to specific DNS servers, redirecting users by overwriting DNS responses, or otherwise interacting within the DNS protocol standards for graceful error coding etc.
- Detect DNS tunneling and domain generated algorithms (DGAs) by analyzing query and response patterns, including encrypted DNS such as DoH. Queries deviating from legitimate activity are flagged and blocked, effectively disrupting C2 connections and unauthorized exfiltration attempts.
- Translate unencrypted traffic into encrypted DNS (or other translations) and send to any third party protective DNS (PDNS) resolver if desired, while still protecting and enforcing all DoH traffic regardless of destination.

3. Cloud IPS and Cloud Custom IPS

Adversaries increasingly exploit protocols like DNS, RDP, SSH, and SMB to bypass centrally deployed legacy IPS and NDR systems and various perimeter or point defenses. This leaves much traffic uninspected for routing and visibility and capacity reasons, creating security and visibility gaps. Zscaler Cloud IPS and Custom IPS capabilities extend intrusion prevention into the cloud and gives security teams the ability to author and deploy Snort-compatible signatures unique to their environment. SecOps teams can also benefit from the global security coverage of included managed security and updated signatures. Detections in all cases are distributed on a real-time basis and deployed inline across the Zero Trust Exchange. The Zscaler Zero Trust Firewall's IPS Control offers immediate, continuous protection against existing, emerging, and targeted threats and exploits. This comprehensive security extends to all users, devices, servers, and workloads across all traffic.

4. Inline AI-Powered Threat Detection

The Zscaler Zero Trust Firewall integrates AI-driven threat intelligence to detect evolving malware, ransomware delivery, and protocol abuse in real time. This proactive approach enables security teams to identify and block emerging threats, such as, malicious DNS records or brute force SMB/RDP attacks, before attackers can achieve persistence. Key capabilities include:

- Dynamic Identification of Legacy CVEs: known vulnerabilities exploited within protocols like SMB and NTP are identified and blocked, even when attackers attempt to cloak their activity in encrypted or segmented traffic.
- C2 Traffic Recognition: Using behavioral analytics, Zscaler Zero Trust Firewall identifies and disrupts stealthy communications facilitated by tools like Cobalt Strike, Chisel tunneling apps, or TOR anonymizers.

5. Integrated ThreatLabz Intelligence

The Zscaler Zero Trust Firewall continuously incorporates the latest updated threat intelligence from Zscaler ThreatLabz, ensuring that evolving attack techniques—such as P2P application abuse, steganographic malware distribution, and dynamic records exploitation—are quickly identified and mitigated on all user, device, server, and workload traffic globally. This intelligence provides granular visibility into attacker tactics, techniques, and procedures (TTPs) to protect environments across retail, healthcare, manufacturing, critical infrastructure, and more.

6. Mitigating Anonymizer Usage and Evasion Strategies

CVEs from as far back as 2017 continue to be actively exploited by attackers for initial access, lateral movement, and executing malicious campaigns. This dispels the misconception that legacy flaws are "low risk" simply due to their age; unpatched vulnerabilities remain high-value targets for threat actors aiming to bypass defenses. Notably, CVE-2019-6443 (NTPsec ntpd ctl_getitem Out of Bounds Read) ranked highest in exploitation attempts, with a large volume of triggers. A surprising number of internet-facing unpatched systems remain accessible, enabling attackers to exploit them for malicious activities.

Conclusion

Non-web protocols have emerged as a covert battleground for cybercriminals, transforming tools like DNS and SMB into weapons for data theft, ransomware delivery, and persistent C2 communication. Attackers exploit the inherent trust and accessibility of these protocols, leveraging techniques such as DNS tunneling, anonymizers, and brute force attacks to bypass traditional security defenses. Organizations that fail to secure these hidden attack surfaces face dire consequences, including operational disruption, reputational damage, and irreversible data loss.

As cyberthreats grow more sophisticated, protecting non-web protocols is critical for maintaining operational integrity in the face of evolving attacks. Zscaler Zero Trust Firewall is essential in defending against the non-web threats outlined in this report. Delivered inline across 160+ data centers, it protects organizations by blocking DNS tunneling, preventing exploitation of protocols such as RDP and SMB with IPS, and accelerating incident response through detailed logging. This ensures that even the most exploited non-web attack surfaces are continuously monitored and secured at cloud scale.

Adopt these best practices to strengthen defenses against non-web threats:

- Enforce zero trust for all traffic with strict authentication, least-privileged access, and continuous inspection
- Secure DNS to detect tunneling, dynamic domain attacks, and command-and-control callbacks
- Patch legacy vulnerabilities, including SMB, RDP, and NTP
- Leverage cloud-delivered IPS and firewall controls to block exploitation attempts across non-web traffic
- Restrict unnecessary protocols to reduce your attack surface
- Monitor anonymizer tools to track obfuscation attempts
- Enable detailed logging and unified visibility across non-web traffic to accelerate detection, investigation, and response

In today's threat landscape, securing web traffic alone is no longer enough—non-web protocols demand the same zero trust scrutiny. Organizations that act now will be far better positioned to close blind spots and eliminate one of the most exploited attack surfaces in the modern cyber domain.

ThreatLabz_Research Methodology

The Zscaler global security cloud is a massive operation, processing over 500 trillion daily signals and blocking more than 9 billion threats and policy violations each day. This robust system also provides Zscaler customers with over 250,000 security updates daily, ensuring continuous protection.

For the purpose of this report, Zscaler ThreatLabz conducted an in-depth analysis of millions of non-web transactions between November 2024 and April 2025. This research delved into critical areas such as the most frequently targeted non-web protocols and industry verticals, prominent vulnerability-based exploits, and the top tools used by threat actors for tunneling, anonymizing, and bruteforcing. Additionally, ThreatLabz meticulously tracked and examined significant malware distributions that occurred via non-web protocols.

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, **research.zscaler.com**.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit **www.zscaler.com**.

zscaler™ | Zero Trust Everywhere

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**