Guardz.

SMB Threat Report

Mid-Year 2025 Edition

Table of Contents

Introduction

This report is based on threat intelligence gathered directly from the Guardz customer base, including telemetry from our platform, active detections, and insights from our threat hunting team.

Unlike generic industry research, the findings here reflect real-world attacks, trends, and incidents observed across thousands of small and medium-sized businesses secured by Guardz worldwide.

Executive Summary

In the first half of 2025, Guardz threat intelligence observed an unprecedented surge in cyber threats targeting SMBs across our customer base. Our platform logged nearly double the weekly incidents compared to last year, providing a unique window into how attackers are adapting.

New data reveals cyberattacks on SMBs have skyrocketed exponentially even as businesses have improved their threat monitoring capabilities. This mid-year threat report highlights how SMBs are now squarely in attackers' crosshairs, often facing enterprise-grade threats without enterprise-level defenses.

Highlights Of The Findings

Ransomware remains a top threat, with more than a hundred types ransomware detections logged among SMBs in H1 2025. Sophisticated criminal gangs continue to target smaller organizations perceived as soft targets, often pairing encryption with data theft for extortion.

Credential abuse is at an all-time high. An overwhelming majority of breaches involve stolen or compromised passwords. Credential-focused attacks surged dramatically year-over-year, the most significant rise among all attack types. Information-stealing malware exploded in use to siphon billions of passwords and session tokens, fueling a booming underground market of logins for sale. With many SMBs not enforcing multi-factor authentication (MFA), adversaries find it trivial to reuse these credentials for easy entry.

Phishing persists as the leading breach vector. Direct phishing incidents have declined as threat actors increasingly bypass “spray-and-pray” emails in favor of using stolen credentials for stealthy logins. Generative AI is supercharging social engineering, enabling attackers to craft eerily realistic phishing messages and deepfake voices at scale, fooling even tech-savvy users.

Cloud assets are under siege. As SMBs migrate data and infrastructure to the cloud, attackers follow. The vast majority of breaches now involve cloud-stored data. Password attacks on cloud accounts spiked tenfold, targeting cloud login portals. Threat actors aggressively seek cloud access tokens and keys. Weakly secured cloud apps and third-party services have contributed to a significant surge in recent cloud intrusions.

Evolving tactics and emerging threats include attackers increasingly leveraging legitimate tools for “living off the land” (LOTL) attacks to bypass antivirus, deepfake content, and AI-driven malware blurring truth and automating hacking tasks, session token hijacking and token theft, ransomware groups pivoting to pure data theft and extortion, and threat actors themselves leveraging generative AI to accelerate attack development.

In summary, the first half of 2025 underscores that SMBs are at the forefront of the cyber threat landscape. Attackers are drawn to SMBs’ valuable data and often limited defenses, employing both tried-and-true methods and cutting-edge techniques to achieve their aims. This report provides a detailed breakdown of key threat trends, targeted industries, attacker tactics, emerging threats, and strategic recommendations. MSPs and MSSPs should use these insights to reassess their risk posture and invest in resilience.

The Current Threat Landscape

Ransomware Rampant as Extortion Grows

Ransomware continues to wreak havoc on organizations of all sizes, with SMBs becoming an increasingly attractive target. Many small businesses falsely assumed they were “too small to target,” only to find that a significant portion suffered from many attempts, many involving ransomware. Ransomware-as-a-Service (RaaS) operations have proliferated, enabling criminals to deploy ransomware at scale.

A few top ransomware gangs are responsible for almost half of all reported attacks, reflecting a concentrated ecosystem. Attackers perceive SMBs as having weaker defenses and limited incident response capabilities, making them easier targets. Many SMB victims lack robust data backups or redundant systems, increasing pressure to pay ransoms to restore operations. Ransomware incidents rose globally and remain steady. Data exfiltration combined with ransomware payloads – the “double-extortion” tactic – is now routine, meaning even organizations with backups face extortion risks. Some threat groups skip encryption altogether, relying solely on data theft extortion, accounting for about one-quarter of breaches.

Downtime from ransomware can cripple daily business, with many SMB leaders saying even one day of outage could shut down their company. Ransom and recovery costs continue to rise, and while many incidents are more minor than enterprise breaches, even a fraction of these costs can be devastating. Public sector entities, including local governments and schools, have seen high-impact attacks. Ransomware remains a top-tier threat in 2025, with adequate backups, network segmentation, and incident response plans being critical to defense.

From the SentinelOne perspective

From the SentinelOne perspective: In the recent SentinelOne threat intelligence classification analysis, a total of 412 distinct threat groups were identified across the monitored environment. The distribution of detections highlights the breadth of malicious activity and the diversity of attack techniques in use.

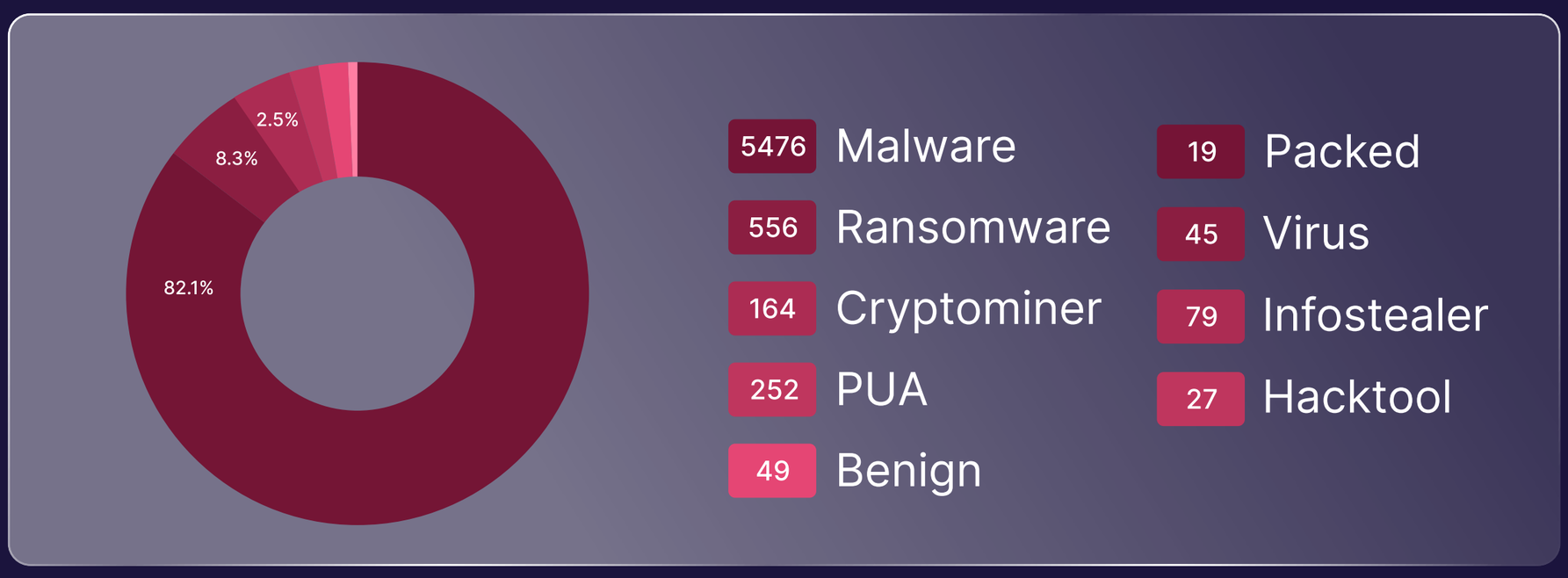
Malware remains the most prevalent category, with 5,476 detections, underscoring its continued dominance as a primary threat vector. Ransomware accounted for 556 detections, reflecting the sustained risk posed by encryption-based extortion campaigns. Potentially Unwanted Applications (PUA) were identified in 252 instances, indicating the presence of software that, while not overtly malicious, poses operational and security risks due to unwanted behavior.

Cryptominer activity was observed in 164 detections, signaling attempts to exploit computing resources for illicit cryptocurrency mining. Infostealer variants appeared in 79 cases, targeting sensitive information and credential theft. In 49 cases, flagged activity was assessed as benign, requiring no immediate remediation.

Additionally, 27 detections involved hack tools, which are often leveraged in the reconnaissance or exploitation phase of an attack chain. Packed binaries accounted for 19 detections, suggesting the use of obfuscation and compression techniques to bypass detection mechanisms.

This classification provides a clear operational picture of the active threat landscape, enabling targeted response measures and informed risk prioritization.

Guardz Data Insights



Phishing & Business Email Compromise (BEC) Adapt with AI

Phishing remains the most prevalent initial attack vector in breaches, accounting for roughly one-fifth of incidents. SMBs are particularly vulnerable due to limited security training and high trust within small teams. However, generic phishing attacks have declined as attackers increasingly use stolen credentials to gain access quietly. Phishing is becoming more targeted and sophisticated.

Business Email Compromise (BEC) scams surged against SMBs, causing significant financial losses globally. BEC attackers impersonate trusted parties to request fraudulent payments or sensitive data. Employees at small businesses face significantly more social engineering attacks than those at larger companies. Generative AI is a game-changer, enabling cybercriminals to craft polished, personalized scam emails and deepfake voice impersonations. This technology increases the scale and believability of attacks, making detection harder. SMBs are responding by increasing security awareness efforts, but gaps remain. Phishing in 2025 remains a shape-shifting threat, still the most common attack vector, but increasingly more complex to detect.

Exchange Online Attack Overview

Attack Category	Total Attempts	Avg. Severity	Primary Industry Target
Phishing	1,876	4.3	Financial Services
Business Email Compromise (BEC)	1,423	4.7	Financial Services
AI-Enhanced Attacks	893	4.8	Professional Services
Credential Harvesting	1,247	4.5	Healthcare
Supply Chain Compromise	682	4.6	Manufacturing

Credential Theft and Abuse at Scale

Stolen credentials have become the center of the cybercriminal playbook, with over 80% of breaches involving compromised credentials. Credential-focused attacks surged dramatically year-over-year. The underground market is flooded with billions of stolen usernames and passwords, primarily harvested by information-stealing malware. These infostealers quietly harvest saved logins, browser cookies, and authentication tokens from infected devices, with usage surging recently.

Alarmingly, a majority of SMBs do not enforce multi-factor authentication, leaving a massive security gap. Attackers leverage stolen credentials for stealthy logins, extended dwell times, privilege escalation, and lateral movement. Session hijacking and token theft techniques have become widespread, allowing attackers to impersonate authenticated users without needing passwords or MFA. Token-based attacks are increasing rapidly, bypassing traditional authentication mechanisms. SMBs and the MSPs that secure them must urgently improve identity security by enforcing MFA, using password managers, monitoring for compromised accounts, and adopting zero-trust principles.

Identity-Based Attacks

Attack Type	Count	% of Total	Avg. Severity (1-5)
Password Spray	576	18.9%	4.6
Credential Stuffing	437	14.4%	4.7
MFA Bypass	312	10.3%	4.9
Legacy Authentication Abuse	298	9.8%	4.3
Account Takeover	267	8.8%	4.8
Subtotal	**1,890**	**62%**	**4.7**

Privilege & Access Abuse

Attack Type	Count	% of Total	Avg. Severity (1-5)
OAuth App Consent	312	10.3%	4.3
Credential Stuffing	243	8.0%	4.1
MFA Bypass	187	6.1%	4.9
Legacy Authentication Abuse	156	5.1%	4.5
Account Takeover	134	4.4%	4.2
Subtotal	**1,032**	**33.9%**	**4.4**

Microsoft 365 Most Targeted Applications

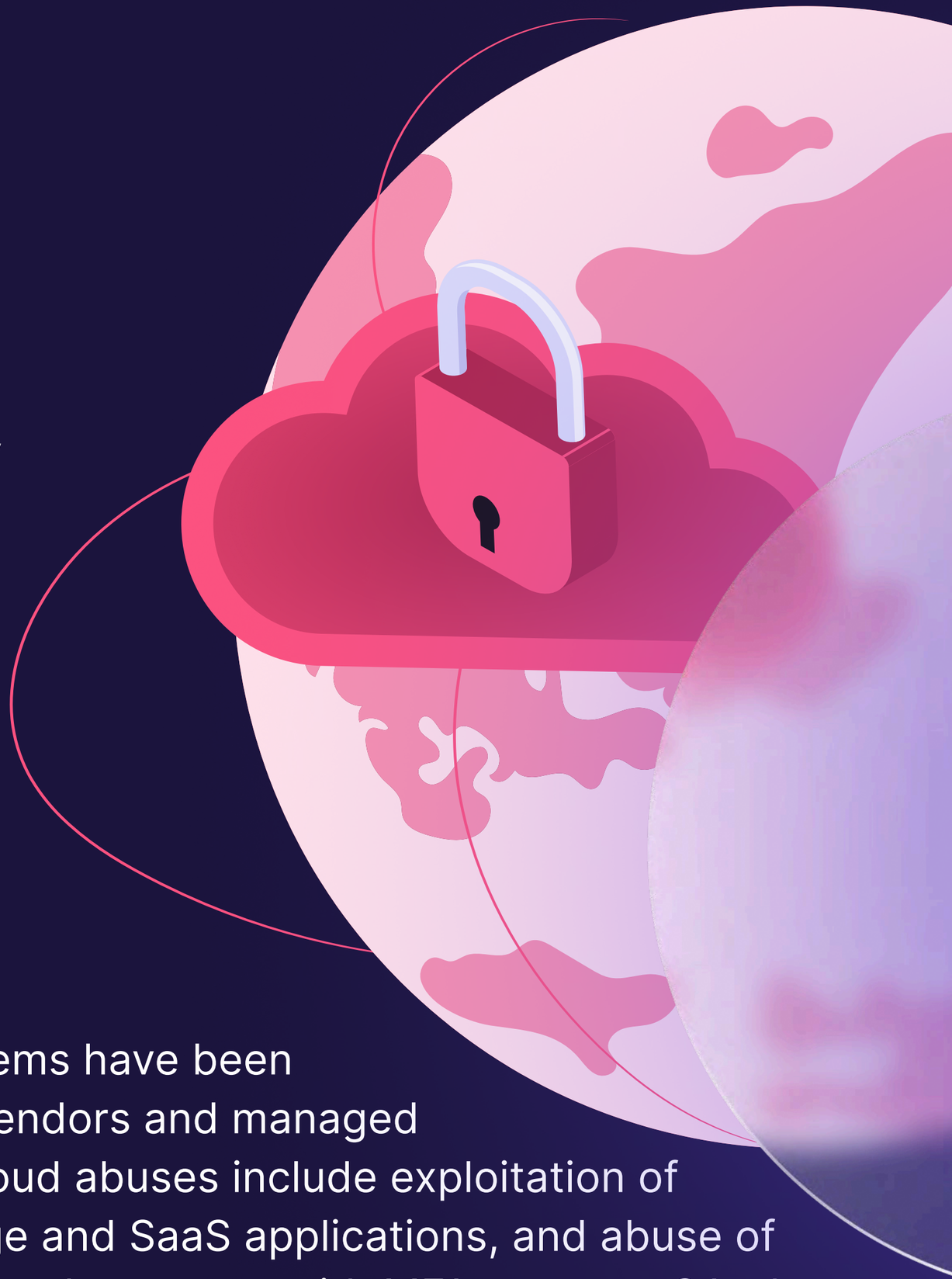
Application	Attack Count	% of M365 Attacks
Outlook/Exchange	1,247	41%
SharePoint	623	20.5%
Teams	532	17.5%
OneDrive	378	12.4%
Power Apps	262	8.6%
Total	**3,042**	**100%**

Google Workspace Attack Distribution

Application	Attack Count	% of M36S Attacks
Phishing	893	38%
Data Exfiltration	632	27%
OAuth App Abuse	421	18%
Drive Sharing Abuse	389	17%
Total	**2,335**	**100%**

Cloud Exploitation and Abuse of Services

Rapid adoption of cloud services has expanded SMB attack surfaces. The majority of data breaches now involve cloud-stored assets. Cloud account takeover attempts have skyrocketed, with automated password attacks reaching thousands of attempts per second. Attackers exploit cloud misconfigurations, steal access keys and tokens, and abuse cloud services for command-and-control or data exfiltration.



Supply chain vulnerabilities in cloud ecosystems have been exploited, with attacks through third-party vendors and managed service providers increasing dramatically. Cloud abuses include exploitation of metadata APIs, malicious use of cloud storage and SaaS applications, and abuse of remote admin features. SMBs must secure cloud accounts with MFA, manage OAuth app permissions, monitor cloud logs, and apply zero-trust principles to third-party connections.

Industries in the Crosshairs

The first half of 2025 has seen concentrated cyberattacks targeting specific industry sectors, with varied attack volumes and severity levels. Below is an overview of the industries most affected by cyber threats, alongside the average severity of attacks and the services most frequently targeted within each sector.

- **Financial Services** represent the largest share of attempts and attacks, accounting for nearly one quarter (24.4%) of all recorded attempts and incidents. These attacks carry a high average severity rating of 4.8 out of 5, reflecting the critical nature of financial data and systems. The primary service targeted within this sector includes email and messaging platforms that support financial communications.

- **Manufacturing** accounts for approximately 13.9% of attempts and attacks with an average severity of 4.4. Attacks in this sector often focus on productivity and office suite software that support operational workflows, reflecting attempts to disrupt manufacturing processes or steal intellectual property.

- **Professional** Services contribute to 10.3% of the attempts and attack volume, with an average severity of 4.2. Similar to financial services, communication and email platforms within this sector are prime attack vectors.

- **Education** saw 9.5% of attempts and attacks with an average severity of 4.3. Educational institutions often experience threats targeting identity management systems, putting student and staff data at risk.

- **Healthcare** follows closely with 18.9% of all attempts and attacks, also experiencing significant impact with an average severity score of 4.7. Healthcare systems that manage patient records and collaboration platforms are common targets, posing risks to sensitive personal health information and operational continuity.

- **Government** entities experienced 12.7% of total attempts and attacks and are among the most severely affected, with an average severity score of 4.9. Identity and access management platforms are the most frequently targeted services, given the critical nature of government systems and citizen data.

- **Retail** comprises 5.9% of the attempts and attacks and an average severity of 4.5. This sector's attacks focus on identity platforms, often aiming at customer and transaction data.

- **Energy & Utilities** account for 4.4% of attempts and attacks with an average severity score of 4.6. Messaging and email servers in this sector remain critical targets, with potential impacts on infrastructure reliability.

Industry Attack Overview

Industry	Total Attacks	% of All Attacks	Avg. Severity (1-5)	Most Targeted Service
Financial Services	742	24.4%	4.8	Microsoft Exchange Online
Healthcare	576	18.9%	4.7	Microsoft SharePoint Online
Manufacturing	423	13.9%	4.4	Microsoft Office Suite
Government	387	12.7%	4.9	Microsoft Entra ID
Professional Services	312	10.3%	4.2	Microsoft Exchange Online
Education	289	9.5%	4.3	Microsoft Entra ID
Retail	178	5.9%	4.5	Microsoft Entra ID
Energy & Utilities	135	4.4%	4.6	Microsoft Exchange Server
Total	**3,042**	**100%**	**4.5**	-

Emerging and Evolving Threats

Notable emerging trends in H1 2025 include:

- **Deepfakes & AI-Driven Impersonation:** AI-generated audio, video, and text used in scams, complicating verification and social engineering defenses.
- **Session Hijacking & Token Theft:** Increasing use of stolen session tokens to bypass authentication controls and escalate attacks.
- **Cloud Abuse & Supply Chain Exploits:** Attackers exploit cloud platform features and third-party vendors to expand reach and persistence.
- **Generative AI Exploitation by Threat Actors:** Attackers leverage AI to automate phishing, malware development, target research, and social engineering.
- **Other Threats:** IoT and remote work vulnerabilities, cryptocurrency-related attacks, and cybersecurity staffing shortages continue to challenge SMB defenses.

Strategic Recommendations

To enhance cybersecurity posture, SMBs should focus on:

- Implementing multi-factor authentication and strong identity management.
- Maintaining reliable offline backups and regularly testing recovery processes.
- Conducting ongoing security awareness training, including phishing simulations.
- Deploying endpoint protection with behavioral monitoring.
- Adopting zero-trust principles, including network segmentation and least privilege.
- Hardening cloud and third-party integrations with strict access controls and monitoring.
- Developing and practicing incident response plans with external expert support.
- Leveraging managed security services and AI-augmented defense tools.
- Securing cyber insurance coverage aligned with organizational needs.

Cybersecurity is an ongoing process requiring continuous risk assessment, employee engagement, and adaptation to evolving threats. With the right approach, SMBs can dramatically reduce risk and enhance resilience against cyber adversaries.

Methodology

All findings are derived from anonymized telemetry across Guardz-managed environments, covering hundreds of thousands of users worldwide.

This includes detections from endpoints, emails, cloud accounts, and identity-related events, supplemented by the Guardz internal threat hunting research.

About the Guardz Threat Hunting Team

Backed by decades of expertise, the Guardz Research team applies advanced techniques to uncover emerging threats and adversarial tradecraft, transforming these insights into automated defenses.

To Learn More Visit Guardz.com