The Sophos Annual Threat Report: Cybercrime on Main Street 2025

Ransomware remains the biggest threat, but old and misconfigured network devices are making it too easy

Written by Sean Gallagher

APRIL 16, 2025

SECURITY OPERATIONS | THREAT RESEARCH | ANNUAL THREAT REPORT | FEATURED | MIDSIZE BUSINESSES | SMALL BUSINESSES

Small businesses are a prime target for cybercrime, as we highlighted in our last annual report. Many of the criminal threats we covered in that report remained a major menace in 2024, including ransomware–which remains a primary existential cyber threat to small and midsized organizations.

Ransomware cases accounted for 70 percent of Sophos Incident Response cases for small business customers in 2024—and over 90 percent for midsized organizations (from 500 to 5000 employees). Ransomware and data theft

attempts accounted for nearly 30 percent of all Sophos Managed Detection and Response (MDR) tracked incidents (in which malicious activity of any sort was detected) for small and midsized businesses.

While ransomware attacks overall have declined slightly year over year, the cost of those attacks overall has risen, based on data from Sophos' State of Ransomware report. And though many of the threats observed in 2024 were familiar in form, other data-focused threats continue to grow, and new tactics and practices have emerged and evolved:

- Compromised network edge devices—firewalls, virtual private network appliances, and other access devices—account for a quarter of the initial compromises of businesses in cases that could be confirmed from telemetry, and is likely much higher.
- Software-as-a-service platforms, which were widely adopted by organizations during the COVID pandemic to support remote work and to improve overall security posture, continue to be abused in new ways for social engineering, initial compromise, and malware deployment.
- Business email compromise activity is a growing proportion of the overall initial compromises in cybersecurity incidents—leveraged for malware delivery, credential theft, and social engineering for a variety of criminal purposes.
- One of the drivers of business email compromise is the phishing of credentials with adversary-in-the-middle multifactor authentication (MFA) token capture, a constantly evolving threat.
- Fraudulent applications carrying malware, or tied to scams and social engineering through SMS and messaging applications, lead to mobile threats for small and midsize businesses.
- Other less-technical threats leveraging the network continue to be a threat to small businesses, again with evolving patterns of scams.

This report focuses on the trends seen in cybercriminal attack patterns faced by small and midsized organizations. Details of malware and abused software most frequently encountered in endpoint detections and incidents is provided in an appendix to this report, which can be found here.

Table of Contents

A word about our data

The data used in our Annual Threat Report analysis comes from the following sources:

- Customer reports—this consists of detection telemetry from Sophos endpoint software running on customers' networks, which gives a broad view of threats encountered, and analyzed within SophosLabs (in this report, referred to as endpoint detection data)
- Incident data—this consists of both data gathered in the course of escalations driven by detection of malicious activity on MDR customers' networks, data gathered by MDR Incident Response from customer incidents, and data gathered by Sophos Incident Response from incidents on customer networks for organizations of 500 employees or fewer where there was little or no managed detection and response protection in place. These datasets are treated as a combined set of incident data in this report.
- SecureWorks incident and detection data is not included in this report, as it was based on pre-acquisition telemetry.
- All data is from the 2024 calendar year, unless otherwise noted.

Customer report data is a firehose of all detections from endpoints, which in most cases result in malware being blocked. Incident data, on the other hand, includes data collected from any event where malicious activity was detected on an MDR customer network or uncovered as part of an Incident Response case, and offers a somewhat deeper picture in many cases of the intent of activity and connections to other threat intelligence.

This report focuses on data specific to small and midsized organizations. Deeper dives on the data gathered from Sophos Incident Response and Sophos MDR Operations, including data on larger organizations, can be found in our Active Adversary Report (AAR) series.

Broken Windows (and gateways)

Whether simply misconfigured, using weak credential policies, or running on vulnerable software or firmware, systems on the network edge are the initial point of compromise for over a third of all incidents involving intrusion into smaller organizations. As Sophos CEO Joe Levy pointed out recently, obsolete and unpatched hardware and software constitutes an ever-growing source of security vulnerabilities, a phenomenon he referred to as "digital detritus."

While zero-day attacks on vulnerabilities are relatively rare in cybercrime targeting small and medium businesses, published vulnerabilities can be very quickly weaponized by access brokers and other cybercriminals. This was the case when the backup software provider Veeam released a security bulletin on CVE-2024-40711 in September 2024—within a month, cybercriminals had developed an exploit for the vulnerability, and paired it with gaining initial access through VPNs.

The Veeam vulnerability and similar documented vulnerabilities that remained unpatched by customers—some of them recent, but some over a year old—played a role in nearly 15 percent of the cases Sophos MDR tracked involving malicious intrusions in 2024. In nearly all cases, the vulnerabilities were reported for weeks if not longer before they were exploited by attackers, frequently in connection to ransomware attacks. In other cases, they were used to gain initial access by cybercriminals for other purposes—including gaining access to potentially sell to ransomware actors.

Top published vulnerabilities as observed in Sophos MDR / IR intrusion incidents

CVE	Description	% of intrusions exploited	Date of CVE publication*
CVE-2024-1709	ConnectWise ScreenConnect authentication bypass	4.70%	2024-02-21
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway buffer overflow vulnerability	2.78%	2023-10-10
CVE-2023-27532	Veeam Backup & Replication Cloud Connect unauthenticated access to encrypted credentials stored in the configuration database	2.35%	2023-03-10

CVE-2024-3400	Palo Alto Networks PAN-OS command injection vulnerability, allows an unauthenticated attacker to execute commands with root privileges on the firewall	1.28%	2024-04-12
CVE-2024-37085	VMware ESXi contains an authentication bypass vulnerability	0.85%	2024-06-25
CVE-2024-40711	Veeam deserialization of data vulnerability, allows remote code execution	0.85%	2024-09-07
CVE-2023-48788	Fortinet FortiClient EMS SQL injection vulnerability, allows an unauthenticated attacker to execute commands as SYSTEM	0.64%	2023-03-12
CVE-2024-27198	JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform admin actions	0.43%	2024-03-04
CVE-2024-21762	Fortinet FortiOS out-of-bound write vulnerability, allows a remote unauthenticated attacker to execute code or commands via HTTP requests	0.43%	2024-02-09
CVE-2021-34473	Microsoft Exchange Server contains an unspecified vulnerability that allows for remote code execution	0.21%	2021-07-14
Total		14.53%	

* Vulnerability dates from cvedetails.com

Figure 1: Top published vulnerabilities as observed in Sophos MDR / IR intrusion incidents

In some cases, even when patches have been deployed for known vulnerabilities, devices may remain vulnerable because they have already been compromised. For example, web shells or other methods of post-exploit access malware may have been deployed before the vulnerability was patched. In other

cases, the patching process may have not been fully completed. In one Sophos MDR case, a Citrix Netscaler gateway was used to establish initial access by an attacker by exploiting sessions that were not reset after the “Citrix Bleed” patch was deployed.

Many of the intrusions to which Sophos MDR and IR responded involved other sorts of vulnerabilities not necessarily covered by the Common Vulnerabilities and Exposures database: default configurations, misconfigurations, weak two-factor authentication (name and password), and other issues with internet-facing devices that leave them vulnerable to attack, as well as vulnerabilities that may have been fixed in later updates by vendors but were never assigned CVE identifiers. Others were potentially related to much older vulnerabilities in unpatched or end-of-life’d devices that had been left in service.

Network edge devices in particular—including virtual private network (VPN) appliances, firewalls with VPN capabilities, and other remote-access appliances—are a major contributor to cybercrime incidents. These devices collectively account for the largest single source of initial compromise of networks in intrusion incidents tracked by Sophos MDR.

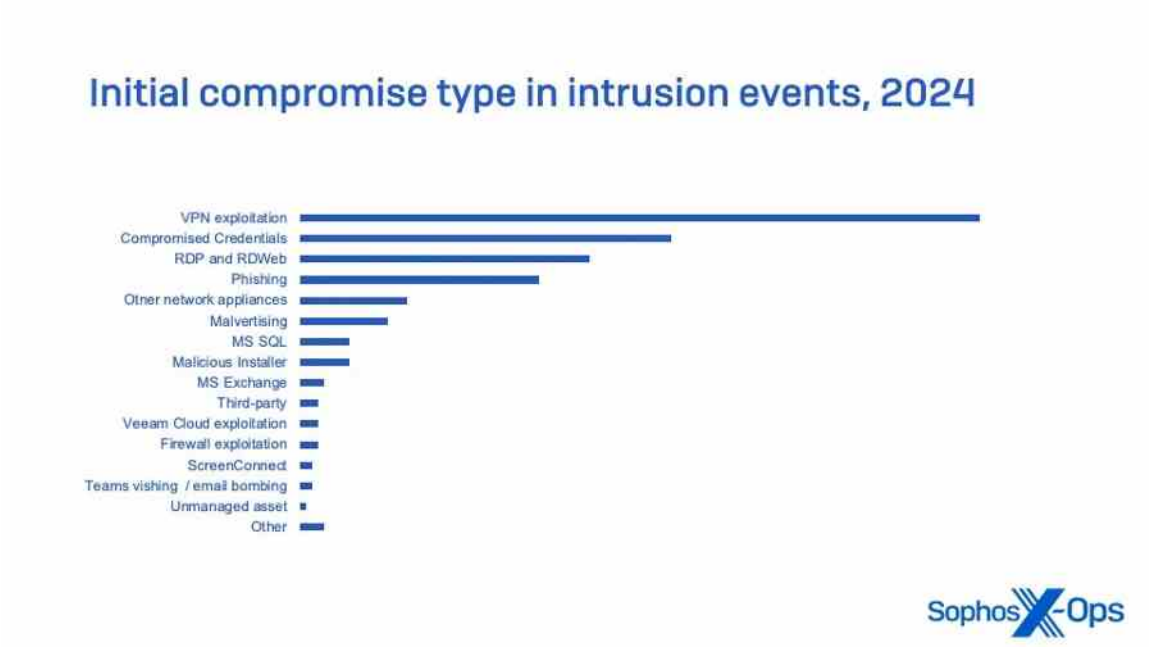

Figure 2: Relative frequency of initial compromise points by cybercriminals against small and medium businesses, based on all incident data. Initial compromise causes overlap in some cases

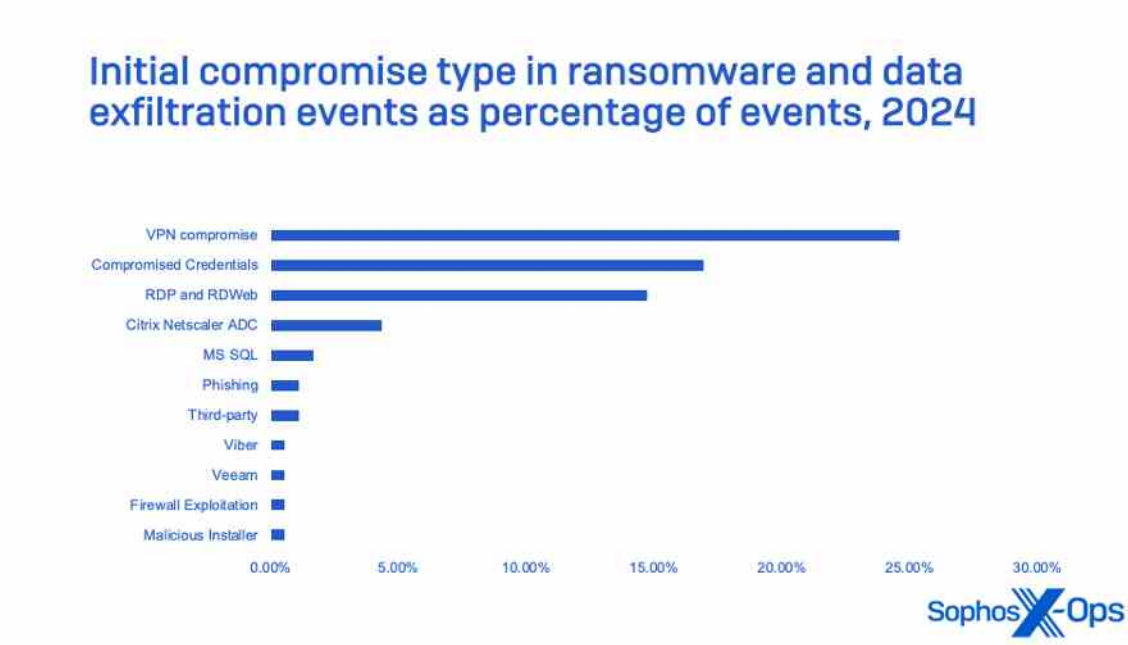

Figure 3: Relative frequency of initial compromise points specifically observed in ransomware and data exfiltration/extortion attacks by cybercriminals against small and midsized businesses, based on Sophos MDR and Incident Response incident data

These figures do not include incidents where ransomware execution or data exfiltration never occurred because of blocking of C2 and other post-exploitation tools.

These statistics highlight the need for even small organizations to deploy MFA for all user accounts, and especially those with remote access rights via a VPN or other means. They also show the necessity of auditing devices used for remote connection to networks and updating their software or firmware regularly—and replacing software and operating systems that no longer receive regular security update support.

STACs: Packaged playbooks, tactics, tools and procedures

Rather than tracking "threat groups," Sophos MDR focuses on identifying specific patterns of behavior to track a set of actors across multiple incidents. These include tools, tactics and procedures (TTPs), support infrastructure, and other characteristics that reflect the use of a shared playbook or set of scripted tools. We refer to these as Security Threat Activity Clusters (STACs) and track their activity as campaigns.

STACs represent not just a single set of actors, but a shared playbook—tactics, tools, and procedures (TTPs), including attack scripts and similar methods for targeting victims. These playbooks may have been packaged for use by multiple affiliates of a ransomware organization, sold on underground marketplaces, or outright stolen by individuals moving from one criminal activity to another.

For example, while hunting for threats leveraging the Veeam vulnerability CVE-2024-40711, Sophos MDR Threat Intelligence identified a specific threat activity cluster using it, along with VPN exploitation, and nearly identical TTPs. The cluster is tracked as STAC5881. In this campaign, the Veeam vulnerability was used to create identically named administrator accounts (named "point"). However, the ransomware deployed in these cases varied: Akira, Fog, and a new ransomware named Frag.

Figure 4: Frag Ransomware note associated with a STAC5881 attack

Frag appears to be a "junk gun" ransomware—crudely coded, cheap ransomware produced as an alternative to ransomware-as-a-service, and either

developed by the cybercriminals themselves or obtained from an underground marketplace at an average price of $375.

The most active STAC campaigns tracked by Sophos MDR in 2024 were ransomware-related in all but one case—and that campaign was the long-running malware-as-a-service platform DanaBot, which can be a precursor to ransomware attacks.

Most active security threat activity clusters in 2024

STAC4265	DanaBot campaign using Facebook social engineering, with links to “uncl aimed money” sites that redirect to deliver malware that attempts to steal browser data and exfiltr ate it via the Tor anonymizing network
STAC4529	Authentication bypass using RCE of ConnectWise Screen Connect prior t o 23.9.8
STAC4556	Crytox ransomware deployed, uTox messenger application dropped, use of a deployed vulnerable kernel driver to disable EDR software. The attackers in the cluster also us ed legitimate “dual use” tools: Advanced Port Scanner for network discovery, and Mimikatz and La zagne tools for credential discovery and dumping
STAC6451	Mimic ransomware affiliates, using Cloudflare to mask command and co ntrol domains, exploiting Microsoft SQL Server for unauthorized access, and deploying Impacket fo r backdoor creation with common credentials. They also exhibit proficiency in network evasion by redirecting probing domains to legitimate sites and exfiltrating data via well-known file trans fer services.
STAC5881	A cluster leveraging Akira, Fog, and Frag ransomware attacks, exploiting VPNs and CVE-2024-4071 (described above)
STAC5464	A ransomware-related cluster linked to Hunters International, using the s ame SFTP exfiltration server across incidents as well as NTDS credential dumping and use of n etwork proxying through Plink, SystemBC malware, and other tools

STAC5397	A threat actor or set of actors associated with Akira and Fog ransomware. Creates backdoor accounts with a common password. The cluster has been observed deploying “dual use” legitimate tools: AnyDesk for execution and lateral movement, and Rclone and FileZilla for data exfiltration.
STAC4663	A ransomware-related cluster that utilizes custom, obfuscated malware to perform intrusions. The group often uses CVE-2023-3519 to exploit Citrix NetScaler appliances for initial access, and uses the legitimate OpenSSH library for network traffic tunneling in victim environments.
STAC5304	A RansomHub ransomware affiliate first identified in summer 2024 that has reused exfiltration IP addresses across multiple incidents, leveraging legitimate tools (Atera Agent remote machine management software, FileZilla for data exfiltration) and a script named HideAtera.bat for defense evasion

Figure 5: Most active security threat activity clusters in 2024 ordered by number of incidents

Trends in cybercrime techniques, tactics and practices

Remote ransomware continues to grow

While the overall number of incidents in 2024 was slightly down—in part because of better defenses and the disruption of some major ransomware-as-a-service operators—ransomware-related crime is not fading away. If anything, the tactics of ransomware actors are evolving to be faster on the attack and more willing to extort the victim over stolen data when they fail to encrypt victim’s files. Sometimes the attackers don’t even bother trying to encrypt the files.

When attackers do run ransomware, it’s often done from outside of the detection range of endpoint protection software—that is, from an unmanaged

device either remotely or directly connected to the targeted network. These "remote" ransomware attacks use network file-sharing connections to access and encrypt files on other machines, so the ransomware never executes on them directly. This can conceal the encryption process from malware scans, behavioral detection, and other defenses.

Sophos X-Ops found in an examination of telemetry that use of remote ransomware increased 50 percent in 2024 over last year, and 141 percent since 2022.

Figure 6: Remote ransomware attacks from 2022 to 2024 by quarter

Social engineering via Teams vishing

In the second half of 2024, and particularly in the fourth quarter, we saw the adoption of a combination of technical and social engineering attacks used by threat actors to target organizations using Microsoft 365 (formerly Office 365). One of these attacks was successful in data exfiltration but failed to progress to ransomware execution. Several others were blocked during attempts to gather credentials and move further into the targeted organizations' network (and potentially, into their software-as-a-service instance and its data).

These attacks by two different threat groups used "email bombing"—the sending of a large volume of emails to targeted people within the organizations they attacked—followed by a fake technical support call over Microsoft Teams to those people, using their own 365 account to send Teams messages and make Teams voice and video calls into the targeted organizations.

MFA phishing

Criminals have also adjusted their deception techniques for gathering user credentials. MFA has made it more difficult to convert usernames and passwords into access. The cybercriminal marketplace has responded with new ways to capture both credentials and multifactor tokens in real time to overcome that obstacle.

MFA phishing relies on an "adversary-in-the-middle" approach, where the phishing platform acts as a proxy to actual authentication process for the multifactor-protected service. The platform then passes captured credentials and the session cookie returned from the login to the cybercriminal over a separate channel, which in turn allows them to pass the credentials and token to the target's legitimate service site and gain access.

An MFA phishing platform called Dadsec emerged in the fall of 2023, and would later be linked to campaigns in 2024 by a phishing-for-hire platform known as Tycoon. But Tycoon was not the only phishing ring using Dadsec-derived tools. Rockstar 2FA and FlowerStorm both appear to be based on updated versions of the Dadsec platform, using Telegram as a command-and-control channel. Rockstar 2FA was highly active in the middle of 2024 and appeared to suffer from technical failures in November, but was quickly supplanted by FlowerStorm.

Intelligence collected from both platforms revealed a large volume of compromised accounts, but it was unclear how many had actually been used for access by cybercriminals.

Figure 7: A developer browser view of a FlowerStorm phishing page

Adversarial AI usage

Cybercriminals engaged in intrusion-style attacks have made limited use of artificial intelligence. Most of the use of generative AI by cybercriminals has focused on social engineering tasks: creating images, videos and text for fake profiles, and for use in communication with targets to mask language fluency issues and identity. They also use it to make their own tools look more professional—as RaccoonStealer developers did for a graphic for their portal login page.

Figure 8: The login screen for a RaccoonStealer Office365-focused credential theft portal

Figure 9: The source of the image, on the generative AI site OpenArt

One area where there has been emergent use of generative AI is in phishing emails. Large Language Models (LLMs) such as ChatGPT can be used to create grammatically correct content in a format that varies from target to target—defeating content filters that identify signatures in spam and phishing emails.

SophosAI demonstrated that an entire campaign of targeted emails could be created using AI-orchestrated processes based on information gathered from targeted individuals' social media profiles, using existing tools.

Sophos X-Ops expects use of these capabilities by cybercriminals to expand in the future. Currently, (based on our research into discussions of LLMs on criminal forums, including an initial investigation in late 2023, followed by an update in early 2025), there remains a considerable amount of skepticism among some threat actor communities. Some are experimenting and using AI for routine tasks, but malicious applications remain largely theoretical—though in our most recent update we noted that a handful of threat actors are beginning to incorporate generative AI into spamming services and similar tools.

Quishing

Around the same time that RockStar was peaking, Sophos X-Ops discovered a "quishing" campaign targeting Sophos employees (none of whom fell for the lure). Emails with QR codes alleged to provide secure access to a document were embedded in a PDF attachment; the QR code in fact contained a link to a fraudulent document-sharing site that was, in fact, an adversary-in-the-middle phishing instance, with characteristics very similar to Rockstar 2FA and FlowerStorm.

Figure 10: A phishing email with a QR code targeting Sophos employees

Figure 11: The fake authentication window for the phishing site the QR code directed targets to, with a Cloudflare security check to validate the target

Malvertising and SEO poisoning

Malvertising is the use of malicious web advertisements, including paid listings on search results. It continues to be a favored method of distributing malware. Long used by droppers such as ChromeLoader, malvertising has become the distribution method of choice for information-stealing malware, but Sophos MDR has observed other malware injection mechanisms leveraging malvertising as well.

A malvertisment can either link to a malicious web page or directly to a malicious script that is downloaded and launched by the victim, resulting in the installation of malware or other tools giving the attacker persistence on the victim's computer. For example, in the second half of 2024, Sophos X-Ops observed a browser hijacking campaign associated with Google search malvertising leveraging keywords that targeted users searching for a PDF tool download. The advertisements led to downloads of malicious Microsoft installer (.MSI) files which installed what appeared to be an actual functioning PDF tool—but also created a system task, a startup item, and registry keys to establish persistence for malware that hijacks browsers, redirecting targets' web searches to sites controlled by the malware's operators.

Malvertising has been observed by Sophos MDR in cases associated with some of the other most active malware campaigns of 2024: DanaBot, Lumma Stealer, and GootLoader. Other attack vectors were also observed using malvertising, including backdoors and remote administration trojans (including SectopRat), the Cobalt Strike attack tool set, and abused legitimate remote access software such as AnyDesk.

EDR killers

Sophos X-Ops has observed a variety of malicious software tools developed for the criminal marketplace over the past two years referred to as "EDR killers." These tools are intended to exploit kernel drivers to gain privileged access to the operating system and kill targeted protected processes—specifically, endpoint security software—so that ransomware or other malware can be deployed unimpeded. Increasingly, we have seen the developers of these tools rely on a collection of legitimate but vulnerable drivers to power them, in what are known as "bring your own vulnerable driver" (BYOVD) attacks.

Sophos X-Ops saw a variety of would-be EDR killers used by ransomware actors in 2024. The most frequently seen of these was EDRSandBlast, a tool used by multiple actors. Seen in both MDR and Incident Response cases, EDRSandBlast variants were detected in waves of attempted ransomware attacks throughout the year, including a dramatic peak around the US Thanksgiving holiday in November.

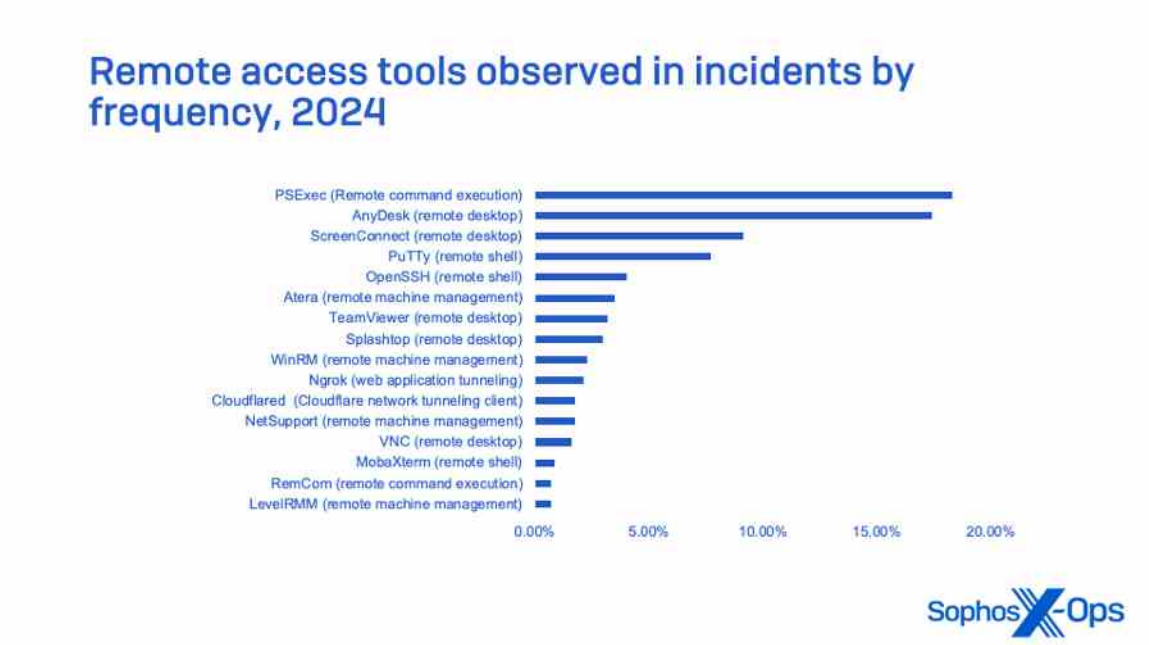

Figure 12: Top 10 EDR-killer malware detected by Sophos endpoint protection

Sophos tamper protection, behavioral detection, and specific detections of malicious use of kernel drivers for disabling defenses help prevent these tools from making ransomware attacks more damaging. But the constant evolution of these tools puts even more pressure on defenders to detect and stop attackers before they can deploy them.

Conclusion

The threat landscape for small and midsized businesses remains highly dynamic, with criminals constantly adapting their tactics to new defensive measures and exploiting vulnerabilities new and old alike as opportunities emerge. Responding to this environment is more than most small organizations can handle without external support and is a strain even on organizations with dedicated IT teams.

Lifecyle management of all systems, including Internet routers, firewalls, VPN appliances, and Internet-facing applications and servers, is an essential part of deterring a significant percentage of attacks. Devices left in service without patches or after the end of their support by vendors can act as a beacon for access brokers and ransomware actors who perform wide network scans of the Internet for vulnerable systems to attack.

This year's data shows that criminals are increasingly attacking where we aren't looking.

- Sophos MDR is increasingly seeing the exploitation of vulnerabilities and misconfigurations of network edge devices, which are used to obtain and disguise criminal access to networks.
- If there is a risk of their ransomware encryption tool being detected by your endpoint security protection, attackers simply use "remote ransomware" techniques from under-defended assets.
- If they can find a way to elevate their privileges, they bring along a vulnerable device driver with the aim of blinding your security tools from their malicious intent.

Whether stealing MFA codes, using QR codes to trick users into visiting malicious logins from their phones, or convincing users to invite them in through email bombing and vishing attacks, cybercriminals continually adapt and evolve to our defenses.

When taken as a whole, the data and trends in this report illustrate the need to take a defense-in-depth approach to protecting any size organization. Many of these don't require a deeper investment in security, as much as a change in mindset to match the evolving threat. Small and midsized organizations can reduce their risk profile with these steps:

- Migrate from passwords to passkeys for account credentials. Passkeys are stored digital keys assigned to specific devices and can't be intercepted by adversary-in-the-middle phishing kits.
- For accounts that can't be secured with passkeys, use multifactor authentication, and migrate to passkey protection when possible.

- If accounts cannot be secured by either method, closely monitor them through an identity threat detection and response strategy—either internally or with a managed service provider.
- Prioritize patching edge devices such as firewalls and VPN devices, and following through on all required steps for patching (including device resets).
- Make sure endpoint security software is deployed across all your assets so that unmanaged devices can't be leveraged by attackers.
- Enlist outside help to audit and monitor your external attack surfaces regularly to ensure you don't have exploitable entry points for attackers scanning for targets.

Acknowledgements

Sophos X-Ops thanks Anna Szalay, Colin Cowie and Morgan Demboski of Sophos MDR Threat Intelligence and Chester Wisniewski, Director, Global Field CISO for their support in the production of this report.

About the Author

Sean Gallagher

Sean Gallagher is Principal Threat Researcher, Sophos X-Ops. Prior to joining Sophos, he was an information security and technology journalist for over 30 years, including 10 as information security and national security editor for Ars Technica.

Read Similar Articles