SOPHOS

Sophos 2024 Threat Report: Cybercrime on Main Street

# Ransomware remains the biggest existential cyber threat to small businesses, but others are growing.

Sophos X-Ops

# Contents

## Background

Cybercrime affects people from all walks of life, but it hits small businesses the hardest. While cyberattacks on large companies and government agencies get a majority of the news coverage, small businesses (broadly speaking, organizations with less than 500 employees) are generally more vulnerable to cybercriminals and suffer more proportionally from the results of cyberattacks. A lack of experienced security operations staff, underinvestment in cybersecurity, and smaller information technology budgets overall are contributing factors to this level of vulnerability. And when they are hit by cyberattacks, the expense of recovery may even force many small businesses to close.

Small businesses are not a small matter. According to the World Bank, more than 90% of the world's businesses are small- and medium-sized organizations, and they account for more than 50% of employment worldwide. In the United States, small and medium businesses account for over 40% of overall economic activity. (In this report, we will use the terms small- and medium-sized businesses or organizations interchangeably, reflecting their similarity in our data.)

In 2023, over 75% of customer incident response cases handled by Sophos' X-Ops Incident Response service were for small businesses. Data collected from these cases, in addition to telemetry collected from customers of our small- and medium-sized business protection software, gives us further unique insight into the threats that are targeting these organizations daily.

## Executive summary

Based on that data and Sophos threat research, we see that ransomware continues to have the greatest impact on smaller organizations. But other threats also pose an existential threat to small businesses:

- Data theft is the focus of most malware targeting small and medium businesses—password stealers, keyboard loggers, and other spyware made up nearly half of malware detections. Credential theft through phishing and malware can expose small businesses' data on cloud platforms and service providers, and network breaches can be used to target their customers as well
- Attackers have stepped up the use of web-based malware distribution—through malvertising or malicious search engine optimization ("SEO poisoning")—to overcome difficulties created by the blocking of malicious macros in documents, in addition to using disk images to overwhelm malware detection tools
- Unprotected devices connected to organizations' networks—including unmanaged computers without security software installed, improperly configured computers and systems running software fallen out of support by manufacturers—are a primary point of entry for all types of cybercrime attacks on small businesses
- Attackers have turned increasingly to abuse of drivers—either vulnerable drivers from legitimate companies or malicious drivers that have been signed with stolen or fraudulently obtained certificates—to evade and disable malware defenses on managed systems
- Email attacks have begun to move away from simple social engineering toward more active engagement with targets over email, using a thread of emails and responses to make their lures more convincing
- Attacks on mobile device users, including social engineering-based scams tied to the abuse of third-party services and social media platforms, have grown exponentially, affecting individuals and small businesses. These range from business email and cloud service compromise to pig butchering (shā zhū pán (殺豬盤)) scams.

## A word about our data

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

- Customer reports—detection telemetry from Sophos protection software running on customers' networks, which gives a broad view of threats encountered, and analyzed within SophosLabs (in this report, referred to as the Labs dataset);
- Managed Detection and Response (MDR) incident data, gathered in the course of escalations driven by detection of malicious activity on MDR customers' networks (in this report, referred to as the MDR dataset);
- Incident Response team data, drawn from incidents on customer networks for business of 500 employees or fewer where there was little or no managed detection and response protection in place (in this report, referred to as the IR dataset).

For a deeper look at data drawn strictly from the cases handled by our external-facing IR team (including cases involving customers with more than 500 employees), please see our sister publication, the Active Adversary Report (AAR). The conclusions in this report are based, unless otherwise stated, on the combined datasets with appropriate normalization.

## Data is the prime target

The greatest cybersecurity challenge facing small businesses—and organizations of all sizes—is data protection. More than 90% of attacks reported by our customers involve data or credential theft in one way or another, whether the method is a ransomware attack, data extortion, unauthorized remote access, or simply data theft.

Business email compromise (BEC), in which email accounts are taken over by a cybercriminal for the purpose of fraud or other malicious purposes, is a substantial problem in the small-to-medium business set. We do not currently cover BEC in our sister publication, the Active Adversary Report, but the authors of the AAR estimate that in 2023, business email compromises were identified by our Incident Response team more often than any other type of incident, save ransomware.

Stolen credentials, including browser cookies, can be used for business email compromise, access to third-party services such as cloud-based finance systems, and access to internal resources that can be exploited for fraud or other monetary gain. They can also be sold by "access brokers" to anyone who cares to exploit them; Sophos has tracked offers on underground forums claiming to provide access to a number of small and medium businesses' networks.

Figure 1: A forum post advertising access to a small US accounting firm

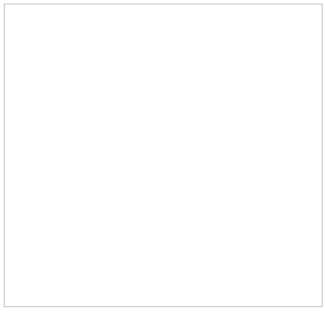

Figure 2: A forum post advertising access to a small business in Belgium

Figure 3: A cybercriminal offering to purchase access to small companies

Figure 4: Access to a small business in Italy being offered for sale on a criminal forum

By category, nearly half of malware detected in 2023 targeted the data of its intended victims. The majority of that is malware we've classified specifically as "stealers"—malware that grabs credentials, browser cookies, keystrokes, and other data that can be either turned into cash as sold access or used for further exploitation.

Because of the modular nature of malware, however, it's difficult to completely categorize malware by functionality—nearly all malware has the ability to steal some form of data from targeted systems. These detections also don't include other credential theft methods, such as phishing via email, text message, and other social engineering attacks. And then there are other targets, such as macOS and mobile devices, where malware, potentially unwanted applications, and social engineering attacks target users' data—especially of the financial kind.

## Malware categories by number of signature updates 2023

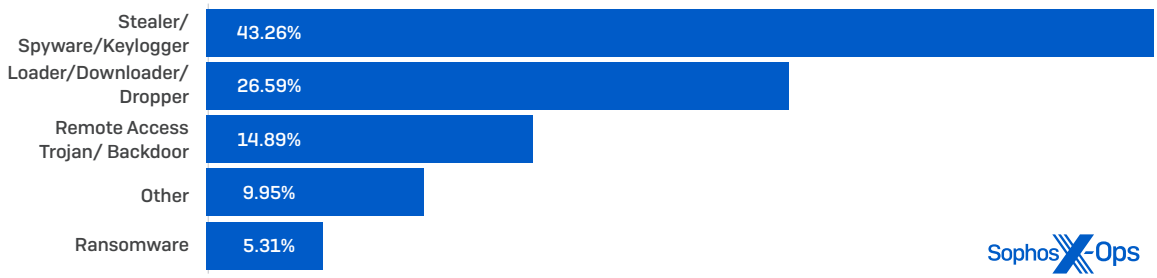


Figure 5: Malware detections by type for 2023, as seen in our Labs and MDR datasets

Nearly 10% of malware detected falls outside of the four major categories shown above. This "other" category includes malware that targets browsers to inject advertisements, redirect search results to earn cash for clicks, or otherwise modifies or collects data for the profit of the malware developer, among other things.

Some stealers are very specific in their targeting. Discord "token" stealers, intended to steal Discord messaging service credentials, are often leveraged to deliver other malware through chat servers or via Discord's content delivery network. But other leading stealers—Strela, Raccoon Stealer, and the venerable RedLine stealer family—are much more aggressive in their targeting, collecting password stores from the operating system and applications as well as browser cookies and other credential data. Raccoon Stealer has also deployed cryptocurrency "clippers" which swap crypto wallet addresses copied to the clipboard with a wallet address controlled by the malware operator.

## Top stealers by number of unique customer reports 2023

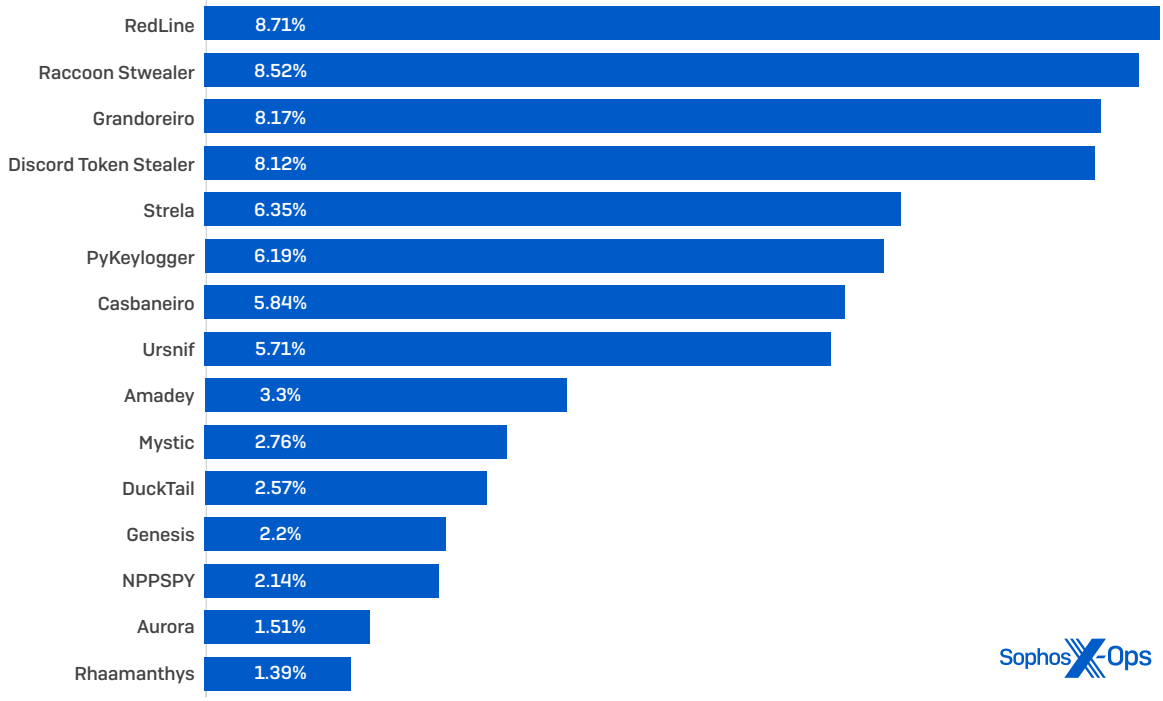


Figure 6: Information stealer malware detections in 2023, drawn from Sophos customer telemetry in the SophosLabs dataset

Sophos has seen an increase in the number of information-stealing malware targeting macOS, and we believe that trend will continue. These stealers—some of which are sold in underground forums and Telegram channels for up to $3,000— can collect system data, browser data, and cryptowallets.

## Ransomware remains a top threat for small businesses

While ransomware makes up a relatively small percentage of overall malware detections, it still packs the biggest punch in terms of impact. Ransomware affects all sizes of businesses across all sectors, but we have seen it hit small- and medium-sized enterprises the most frequently. In 2021, the Institute for Security and Technology's Ransomware Task Force found that 70% of ransomware attacks targeted small businesses. While the overall number of ransomware attacks has varied year over year, that percentage bears out in our own metrics.

LockBit ransomware was the top threat in small business security cases taken on by Sophos Incident Response in 2023. LockBit is a ransomware-as-a-service, delivered by a number of affiliates, and was the most deployed ransomware of 2022 according to Figure 7.

### Small business ransomware incidents handled by Sophos Incident Response, 2023

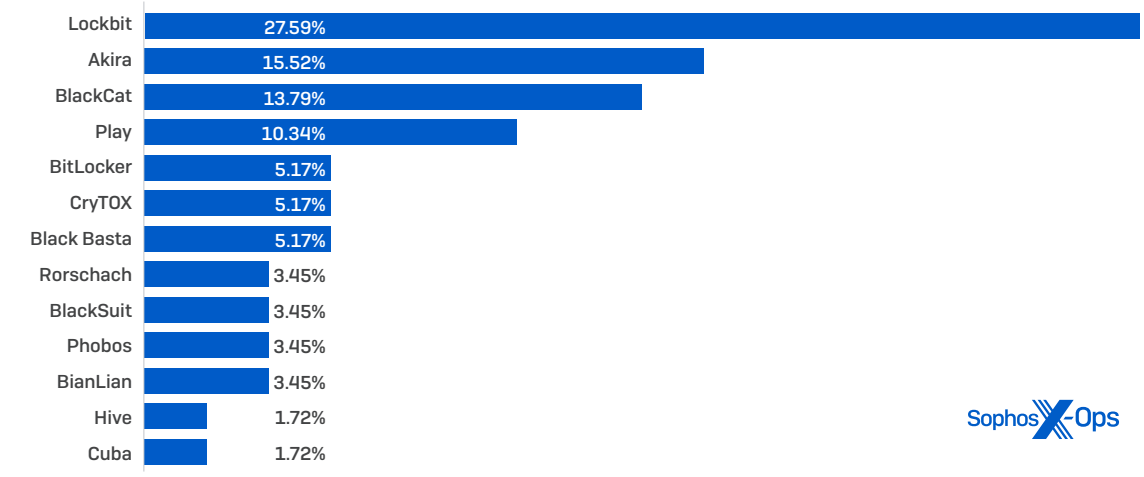


Figure 7: A breakdown of ransomware actors behind the small business incidents Sophos Incident Response investigated in 2023; these numbers reflect the dataset of hands-on IR engagements at customers that generally did not have previous Sophos protections in place

### Top 20 ransomware by number of unique customer reports, 2023

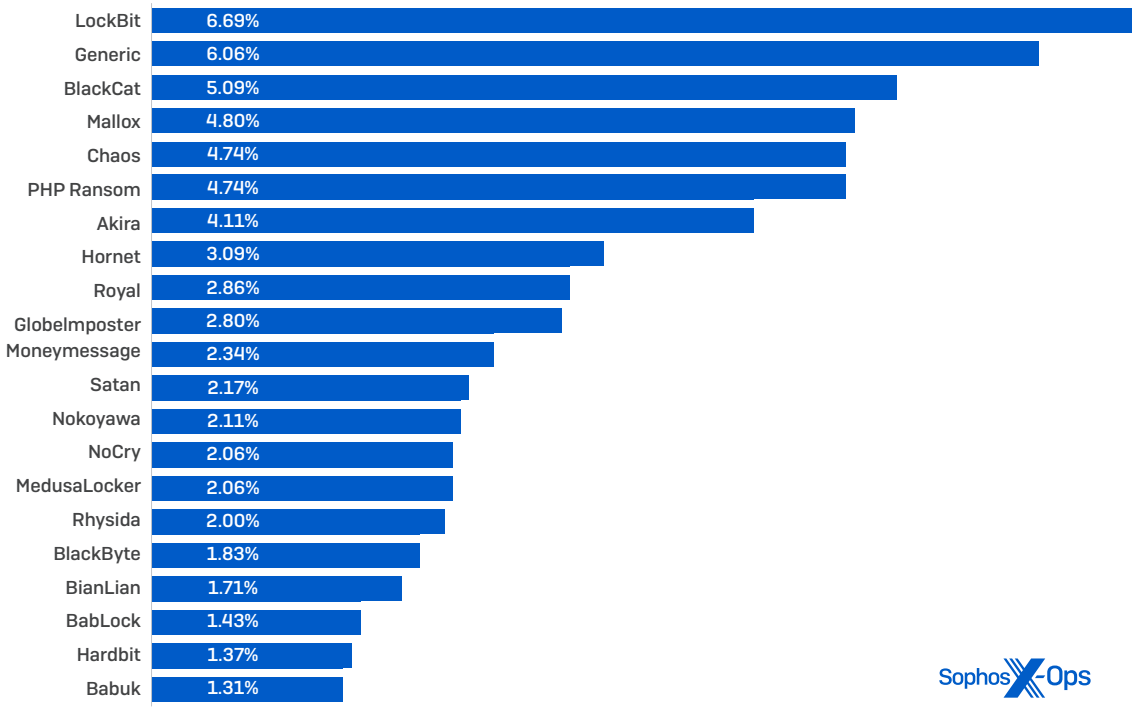


Figure 8: The top attempted ransomware deployments detected by Sophos endpoint protection software and present in our Labs dataset across all customers in 2023, as a percentage of all detected ransomware; "Generic" represents multiple types of ransomware detected with a catch-all signature that were not detected under another definition

LockBit was the malware observed the most by Sophos' Managed Detection and Response (MDR) group (which includes the Incident Response team and its data)—with nearly three times the number of incidents in which ransomware deployment was attempted than its nearest peer, Akira.

## Top malware brands observed in 2023 MDR-handled Incidents, by # of incidents

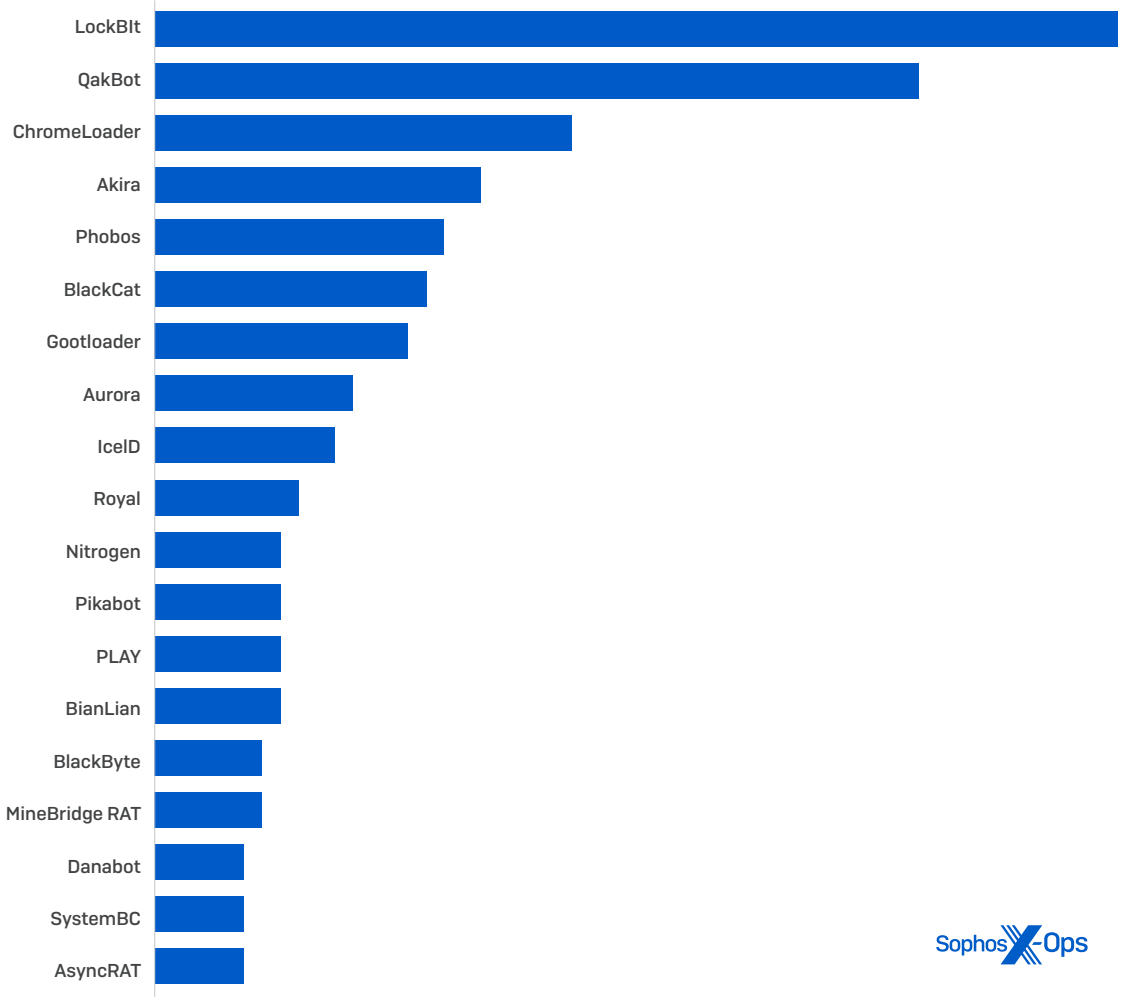


Figure 9: The most-often observed malware in incidents taken on by Sophos Managed Detection and Response in 2023, as seen in the MDR dataset. Note the differences between this chart and the one in Figure 8; aside from the 2023 dominance of LockBit, we see that though there is a wide array of ransomware families that attempt to infect systems. Only a subset of those progress to a stage that requires hands-on MDR assistance. Note that these are non-exclusive; that is, more than one detection may occur in a single incident

As 2023 progressed, we saw an increase in the use of remote execution of ransomware—using an unmanaged device on organizations' networks to attempt to encrypt files on other systems through network file access.

### Remote ransomware incidents, 2022-2023

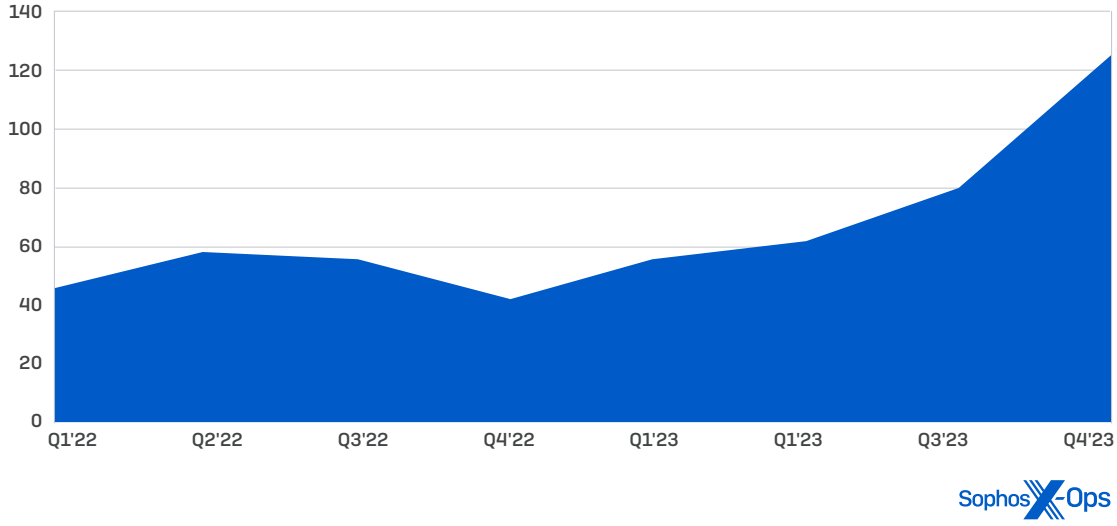


Figure 10: The last two years' worth of data from customer telemetry gathered by Sophos shows an overall increase in the proportion of attempted ransomware attacks involving remote ransomware – an ongoing problem that's taken on new life, especially in the latter half of 2023

These types of attacks are able to gain footholds by exploitation of unprotected servers, personal devices, and network appliances that connect to organizations' Windows-based networks. Defense in depth can prevent these attacks from taking entire organizations offline, but they can still leave organizations vulnerable to data loss and theft.

Windows systems aren't the only ones targeted by ransomware. Increasingly, ransomware and other malware developers are using cross-platform languages to build versions for macOS and Linux operating systems and supported hardware platforms. In February of 2023, a Linux variant of Cl0p ransomware was discovered to have been used in a December 2022 attack; since then, Sophos has observed leaked versions of LockBit ransomware targeting macOS on Apple's own processor and Linux on multiple hardware platforms.

## Cybercrime as a service

The malware world continues to be dominated by what we've referred to as "Malware as a Service" (MaaS)—the use of malware delivery frameworks provided by cybercriminals through underground marketplaces to other cybercriminals. But a combination of improvements in platform security and takedown operations by industry and law enforcement have had some impact on the shape of the MaaS landscape.

After a decade of dominance in the malware delivery business, Emotet has receded since being taken down by Europol and Eurojust in January 2021. So, to a lesser degree, have Qakbot and Trickbot, after being disrupted by law enforcement in August 2023. While Qakbot has returned in some limited form, it has been largely supplanted by its would-be successors, Pikabot and DarkGate.

None of this has impacted the venerable remote access trojan AgentTesla, which has moved to the top of the MaaS market. It was the malware most often detected by endpoint protection in 2023 overall in endpoint (aside from generic malicious .LNK files and obfuscated malware), and made up 51% of the malware delivery framework detections in our telemetry last year.

### Top malware delivery frameworks by number of unique customer reports, 2023

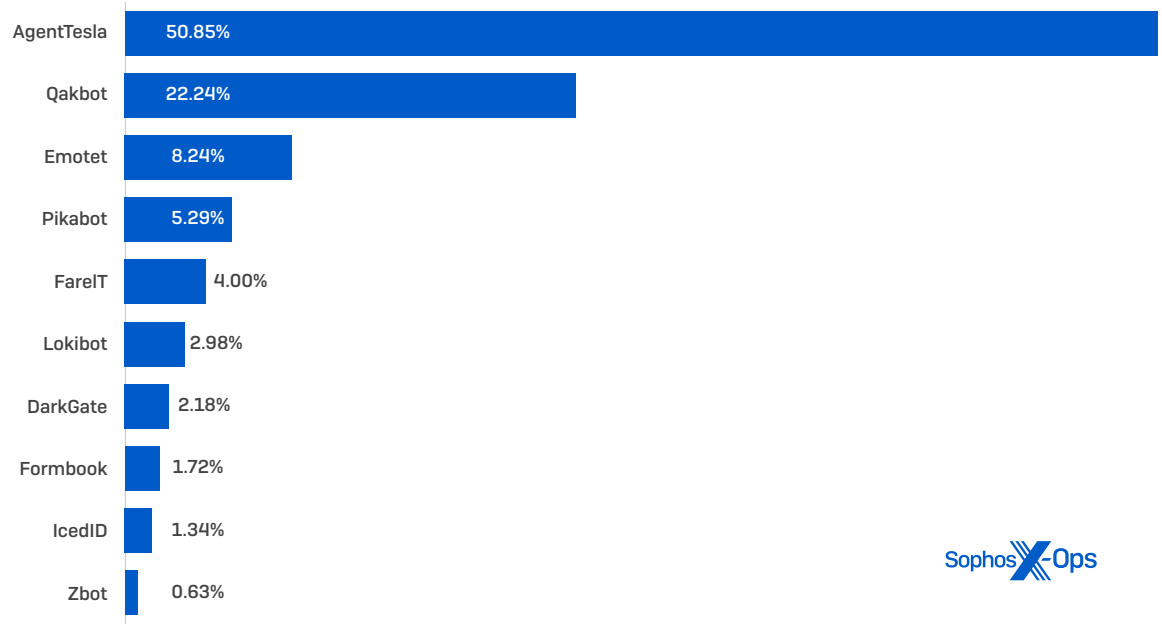


Figure 11: A breakdown of the common frameworks used to deliver malware by attackers, based on the number of endpoint detections from Sophos-protected customer networks; Qakbot numbers represent detections prior to the August 2023 international law enforcement action against its infrastructure

## Finding a different delivery route

Malware attacks require some form of initial access. Typically, that involves one of the following:

- Phishing emails
- Malicious email attachments
- Exploits of vulnerabilities in operating systems and applications
- Fake software updates
- Exploitation and abuse of Remote Desktop Protocol
- Credential theft

MaaS operators have in the past been largely reliant on malicious email attachments for that initial foothold. But changes to the default security of the Microsoft Office platform have had an impact on the MaaS market. As Microsoft has rolled out changes to Office applications that block by default Visual Basic for Applications (VBA) macros in documents downloaded from the Internet, it has become more difficult for MaaS operators to use their favored method of spreading malware.

That has led to some changes in the types of file attachments attackers use—attackers have moved to PDF file attachments almost exclusively. However, there have been some notable exceptions. In early 2023, Qakbot operators turned to using malicious OneNote documents to get around changes being pushed out to Excel and Word, concealing within the document links to script files that were activated when the target clicked on a button within the OneNote notebook file.

In 2021, we noted that "malware-as-a-service" offerings such as the RaccoonStealer backdoor had begun to rely heavily on web delivery, often using search engine optimization (SEO) tricks to fool targets into downloading their malware. In 2022, we saw "SEO poisoning" used as part of a SolarMarker information stealer campaign. These methods are on the rise again, and the actors behind them have grown more sophisticated.

We saw several notable campaigns using malicious web advertising and SEO poisoning to target victims. One of these was by an activity group using malware we dubbed "Nitrogen"; the group used Google and Bing advertisements tied to specific keywords to lure targets into downloading a software installer from a fake website, using a legitimate software developer's brand identity. The same malvertising technique has been used in connection with a number of other initial access malware, including the Pikabot botnet agent, IcedID information stealer, and Gozi backdoor malware families.

In the case of Nitrogen, the ads targeted IT generalists, offering downloads including well-known remote desktop software for end-user support and secure file transfer utilities. The installers carried what was advertised, but they also delivered a malicious Python payload that, when launched by the installer, pulled down a Meterpreter remote shell and Cobalt Strike beacons. Based on other researchers' findings, this was likely the first step in a BlackCat ransomware attack.

## "Dual use" tools

Cobalt Strike, the well-worn "adversary simulation and red team operations" software kit, continues to be used by actual adversaries as well as legitimate security testing organizations. But it is by no means the only commercially developed software used by attackers—and it is no longer the most common.

Remote desktop tools, file compression tools, common file transfer software, other utilities, and open-source security testing tools are commonly used by attackers for the same reason that they're used by small and medium enterprises—to make their jobs easier.

Sophos MDR has observed these utilities, which we refer to as "dual-use tools", abused as part of the post-exploitation process by attackers:

- **Discovery:** Advanced IP Scanner, NetScan, PCHunter, HRSword
- **Persistence:** Anydesk, ScreenConnect, DWAgent
- **Credential Access:** Mimikatz, Veeam Credential Dumper, LaZagne
- **Lateral Movement:** PsExec, Impacket, PuTTy
- **Data Collection & Exfil:** FileZilla, WinSCP, megasync, Rclone, WinRar, 7zip

AnyDesk and PsExec were both seen in more incidents by Sophos MDR than was Cobalt Strike, as seen below:

### Top "dual-use" tools observed in 2023 MDR-handled incidents, by number of incidents

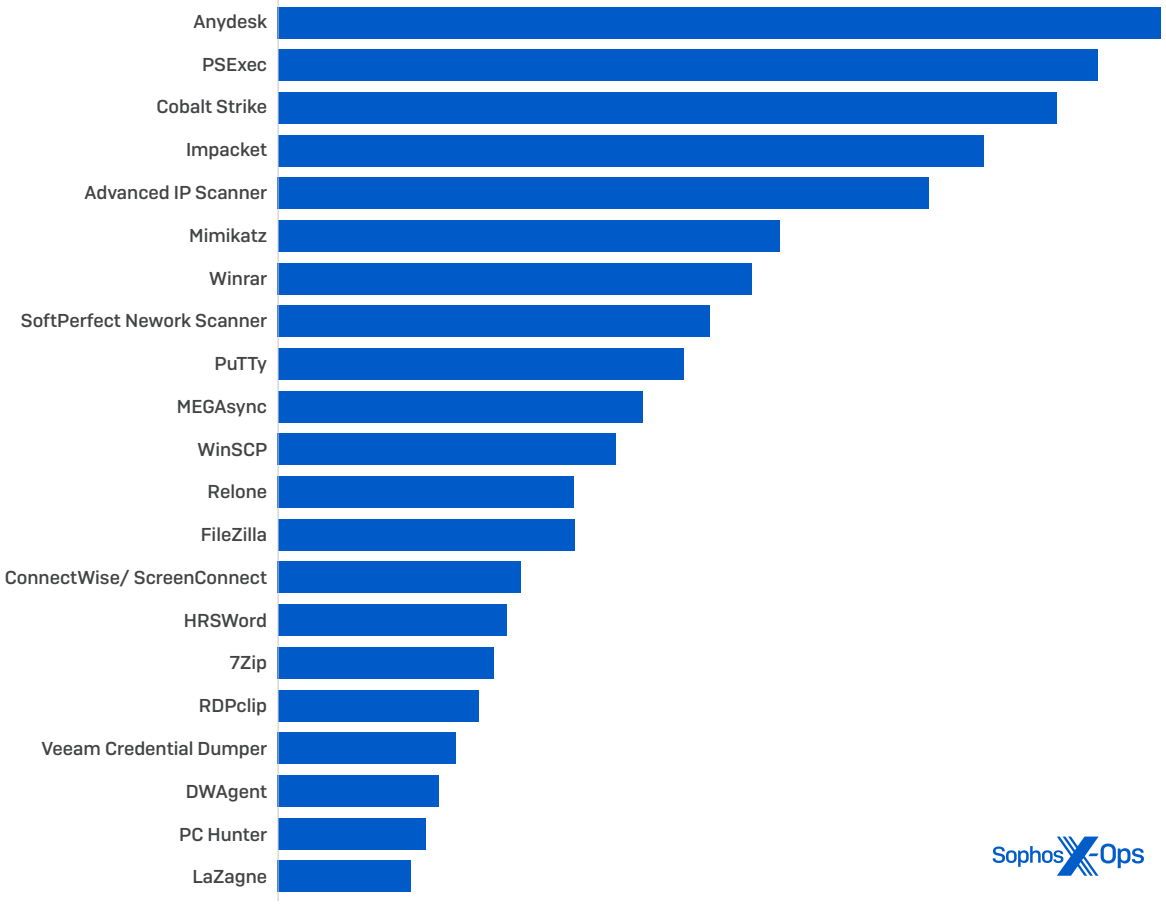


Figure 12: The most-frequently encountered "dual use" tools in cybersecurity incidents, based on the number of cases where each was seen in the Sophos MDR dataset

## Zero-day attacks and non zero-day attacks

In May 2023, Progress Software reported vulnerabilities in the company's widely used secure managed file transfer platform, MOVEit—including one that had been exploited by at least one set of malicious actors. Subsequently the company would reveal multiple additional vulnerabilities and issue multiple patches to fix them.

The attacks were attributed to actors associated with the Cl0p ransomware ring. The attackers used the vulnerability to deploy web shells on the public-facing web interfaces to MOVEit Transfer servers—web shells that in some cases persisted after the vulnerabilities were patched by Progress customers

MOVEit was just one of a number of "zero day" vulnerabilities that challenged defenders in 2023. GoAnywhere, another managed file transfer system, disclosed a vulnerability in February that another CL0p-affiliated group attempted to exploit. And a remote code execution vulnerability in the PaperCut MF and NG print server software products was exploited by the Bl00dy ransomware gang in March and April after being reported to the developers in January.

In some cases, these vulnerabilities simply can't be patched. For example, a vulnerability in Barracuda Email Security Gateway appliances, found in June, was so severe that it could not be patched and required complete replacement of physical or virtual appliances. A Chinese threat group continued to exploit the vulnerable appliances throughout the rest of 2023.

Vulnerabilities in software and devices don't have to be new to be leveraged by attackers. Threat actors frequently seek out software that has fallen out of support, such as older network firewalls and web server software, to target— knowing that no patch will be coming.

## Supply chain attacks and digitally signed malware

Small businesses also have to be concerned about the security of the services they depend upon to manage their business—and their IT infrastructure. Supply chain attacks are not just for nation-state actors; we've seen attacks against managed service providers become an enduring part of the ransomware playbook.

In 2023, Sophos MDR responded to five cases in which small business customers were attacked through an exploit of a service provider's remote monitoring and management (RMM) software. The attackers used the NetSolutions RMM agent running on the targeted organizations' computers to create new administrative accounts on the targeted networks, and then deployed commercial remote desktop, network exploration and software deployment tools. In two of the cases, the attackers successfully deployed LockBit ransomware.

It's hard to defend against attacks that leverage trusted software, especially when that software gives attackers the ability to disable endpoint protection. Small businesses and the service providers who support them need to be vigilant to alerts that endpoint protection has been turned off on systems on their networks, because this may be a sign that an attacker has gained privileged access through a supply chain vulnerability—or through other software that at first glance may seem legitimate.

For example, in 2023, we saw a number of instances of attackers using vulnerable kernel drivers from older software that still had valid digital signatures, and of intentionally created malicious software that used fraudulently obtained digital signatures—including malicious kernel drivers digitally signed through Microsoft's Windows Hardware Compatibility Publisher (WHCP) program—to evade detection by security tools and run code that disables malware protection.

Kernel drivers operate at a very low level within the operating system, and are typically loaded before other software during the operating system's start-up. That means that they execute in many cases before security software can start up. Digital signatures act as a license to drive, so to speak—in all versions of Windows since Windows 10 version 1607, kernel drivers need to have a valid digital signature or Windows operating systems with Secure Boot enabled won't load them.

In December 2022, Sophos notified Microsoft of the discovery of malicious kernel drivers that carried Microsoft-signed certificates. Because these drivers had Microsoft-signed certificates, they were by default accepted as benign software, allowing them to be installed—and then disable endpoint protections on systems that they were installed on. Microsoft issued a security advisory, and then in July 2023 revoked a host of malicious drivers' certificates that had been obtained through WHCP.

Drivers don't have to be malicious to get exploited. We've seen multiple cases of drivers and other libraries from older and even current versions of software products leveraged by attackers to "side load" malware into system memory.

We've also seen Microsoft's own drivers used in attacks. A vulnerable version of a driver for Microsoft's Process Explorer utility has been used multiple times by ransomware operators in efforts to disable endpoint protection products; in April 2023, we reported on a tool dubbed "AuKill" that used this driver in multiple attacks in attempts to deploy Medusa Locker and LockBit ransomware.

Sometimes we get lucky and catch vulnerable drivers before they can be exploited. In July, Sophos behavioral rules were triggered by activity from a driver for another company's security product. The alert was triggered by a customer's own attacker simulation test, but our investigation of the event uncovered three vulnerabilities that we reported to the software vendor and were subsequently patched.

## Spammers push social engineering boundaries

Email may seem like an old-school communication method in an era of encrypted end-to-end mobile chats, but spammers didn't seem to notice (or care) about that. While the traditional BEC method of simply posing as an employee and asking another employee to send gift cards persists, spammers have gotten far more creative.

In the past year, Sophos' messaging security team came across a slew of new social engineering tricks and techniques designed to evade conventional email controls. Messages in which the attacker emails an attachment or link out of the blue are now passé: The more effective spammers are more likely to strike up a conversation first, then move in for the kill in follow up emails.

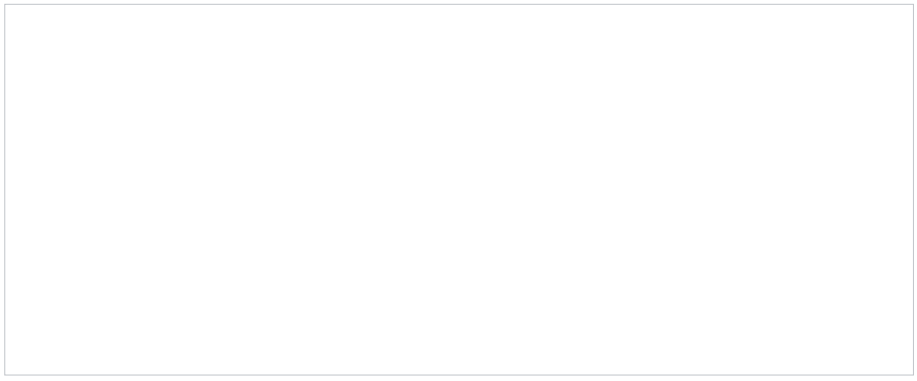

Figure 13: Only after receiving a reply from the target, the spammer sends the target an email with a link to a malicious file inside a password-protected Zip archive

We observed this methodology in attacks in which spammers posing as delivery service workers called enterprise customers on the phone and asked them to open a weaponized email. We also saw spammers initially email a solicitation for business or complaint, in attacks targeting a variety of industries in 2023, followed by a link to download a disguised, weaponized file after the business responded to the first email.

Conventional spam prevention involves processes inspecting message content and making decisions based on that content. Spammers experimented with a variety of methods of replacing any text content in their messages with embedded images: Sometimes the pictures appeared to be a written message, while others experimented with the use of QR codes or images that appear to be invoices (with telephone numbers the attackers prompt victims to call) as a way to evade detection.



Figure 14: A PDF attachment from a spam message embeds a blurry, unreadable thumbnail of a billing invoice and a link to a website hosting a malicious payload

Malicious attachments even pushed boundaries, with weaponized PDFs making something of a comeback, linking to malicious scripts or sites, sometimes using embedded QR codes. The Qakbot malware family expansively abused Microsoft's OneNote document format, the notebook (or .one file), to deliver payloads before being shut down later in the year in a coordinated takedown. Attackers also latched onto the MSIX file format – a type of archive file format used by Microsoft to distribute apps through the Windows App Store – as a way of bypassing detection.



Figure 15 A malicious PDF attachment, emailed to Sophos employees, embeds a QR code image that leads to a phishing page

And attackers abused Microsoft's services as well: By the year's end, about 15% of the total spam Sophos blocked had been sent using email accounts created in Microsoft's business-oriented onmicrosoft.com messaging system.

## Mobile malware and social engineering threats

Small businesses depend heavily on mobile devices as part of either approved or ad-hoc information systems. Text messages, messaging and communications applications, and apps connecting to cloud services—including mobile point of sale applications—are mission-critical systems for distributed small enterprises. Cybercriminals know that, and continue to find ways to target mobile device users to gain access to data or to defraud.

Spyware and "bankers" are a group of Android malware of particular concern, and which we believe will continue to be a threat. Spyware is used to harvest data on the phone—and sometimes will even subscribe the device's user to premium-rate services for direct monetary gain. They harvest personal data, including SMS messages and call logs from the affected device, which is then sold to fraudsters or used for blackmail—or both. There have been several cases where victims have taken their own lives as a result of threats from spyware operators.

These malicious mobile applications are distributed in a number of ways. They may masquerade as legitimate applications on the Google Play app store or third-party app store sites—often as mobile lending applications. They are also spread through links sent via text messages.

Bankers are malware that target financial applications, including cryptocurrency wallets, to harvest account data to gain access to funds—using accessibility permissions to gain access to sensitive data on the phone.

Then there's the phenomenon of "pig butchering," or sha zhu pan. We began tracking fake applications on both the iOS and Android platform tied to a form of scam we first referred to as "CryptoRom" in early 2021; since then, the scams have become increasingly more sophisticated.

The crime rings that operate these scams— frequently operated out of scamming compounds staffed with people who have essentially been kidnapped by organized crime—have taken billions of dollars from victims worldwide, and often focus on people tied to small businesses. In 2023, a small bank in Kansas failed and was seized by the FDIC after the bank CEO sent over $12 million from deposits to scammers in an effort to recover funds he had lost reportedly in one of these scams. This tragic example shows how a scam usually associated with an individual's personal life can have ramifications and impact on small businesses.

Sha zhu pan scammers lure victims through social media sites, dating apps, other apps and community platforms, and even "inadvertent" SMS messages. They tend to target individuals who are looking for a romantic connection or friendship. After moving the target to a secure messaging app such as WhatsApp or Telegram, they gain their trust and introduce a money-making idea that they claim to have inside knowledge about—and that usually involves cryptocurrency.

Over the past year, we've seen the fake applications used by these scams making their way into the Google Play and iOS App stores. They evade store security review by presenting as a benign app until the review process is over, and then change remote content to turn it into a fake crypto trading app. Any crypto deposited through these apps is immediately pocketed by the scammers.

Recently, we've also seen these scams adopt a tactic from another type of crypto scam that requires no fake apps—instead, they use the "Web3" functionality of mobile crypto wallet apps to directly tap into wallets created by the victims. We have identified hundreds of domains associated with these "DeFi (Decentralized Finance) mining" variants of sha zhu pan, and as with the fake apps we identify, we continue to report them and work to get them taken down.

## Conclusions

Small businesses face no shortage of threats, and the sophistication of those threats is often on par with those used to attack large enterprises and governments. While the amount of money that can be stolen is less than available from a larger organization, the criminals are happy to steal what you have and make up for it in volume.

Criminal syndicates are counting on smaller companies to be less well-defended and to not have deployed modern, sophisticated tools to protect their users and assets. The key to successfully defending against these threats is to prove their assumptions wrong: Educate your staff, deploy multifactor authentication on all externally facing assets, patch servers and network appliances with the utmost priority and consider migrating difficult to manage assets like Microsoft Exchange servers to SaaS email platforms.

The primary difference in our experience between the companies that were impacted the most by cyberattacks and those who suffered the least is time to respond. Having security experts to monitor and respond 24/7 is table stakes for an effective defense in 2024. Staying safe isn't impossible; it just takes comprehensive planning and layered defenses to buy you time to respond and minimize damages.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com



24-04-11 EN (NP)

SOPHOS