Sophos Annual Threat Report appendix: Most frequently encountered malware and abused software

These are the tools of the trade Sophos detected in use by cybercriminals over 2024

Written by Sean Gallagher, Anna Szalay

APRIL 16, 2025

SECURITY OPERATIONS | THREAT RESEARCH | ANNUAL THREAT REPORT | ATTACK TOOLS | DUAL-USE TOOLS | MALWARE TRENDS 2024

This appendix to our Annual Threat Report provides additional statistics on incident data and telemetry detailing the tools used by cybercriminals targeting small and midsized businesses (SMBs). For a broader look at the threat landscape facing SMBs, see our main report.

Appendix Contents:

Most frequently-encountered malware types

Small and midsized businesses face a vast set of threats to data—some of which may be precursors to ransomware attacks or may result in other breaches of sensitive information. Ransomware dominates the malware observed in Sophos MDR and Sophos Incident Response cases from 2024, with the top 10 accounting for over 25% of all incidents MDR and IR tracked over the year. But they were not the entire story, and nearly 60% of MDR incidents involved threats not involving ransomware.

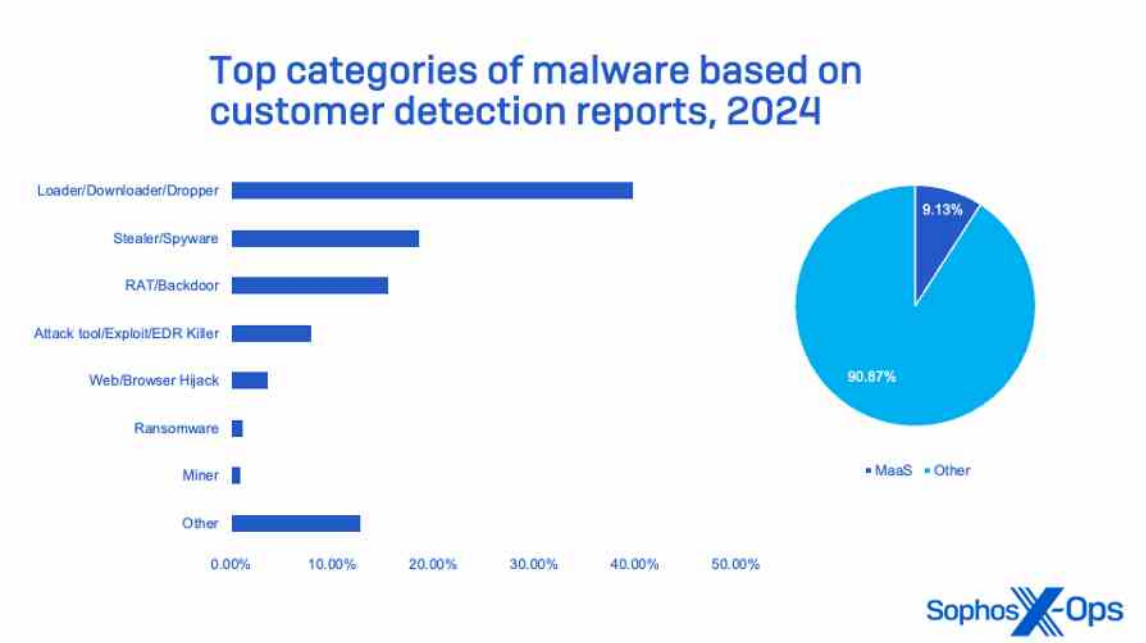

Figure 13: The most commonly seen categories of malware detection seen in 2024, based on customer detection reports

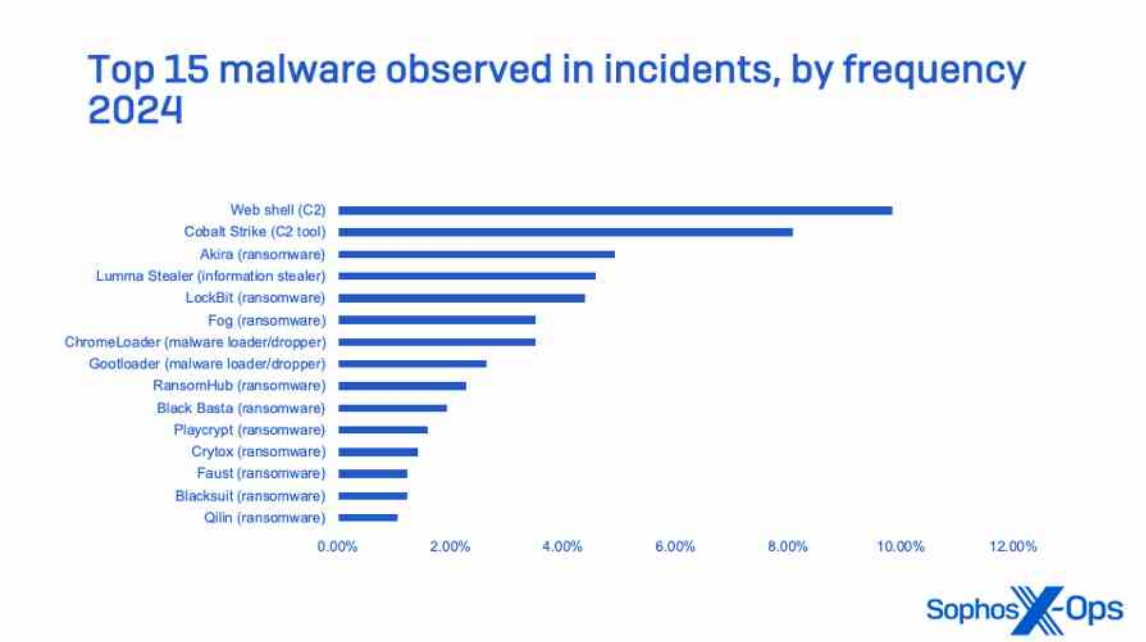

Figure 14: Top 15 malware and attack tools encountered in MDR and IR incidents

Command-and-control tools, malware loaders, remote administration tools, and information-stealing malware make up the majority of the malicious software seen targeting small businesses (aside from ransomware). And these tools, not all of which are technically malware, are used as part of the delivery of ransomware and other cybercriminal attacks.

Only one of the top 10 tools and malware seen in Sophos MDR and IR incidents does not fall into this category: XMRig. It is a cryptocurrency-mining malware often used to passively generate revenue *before* access is sold or otherwise exploited by a ransomware actor.

Figure 20: Top information-stealing malware detections reported by endpoint protection customers

Figure 16: Top non-ransomware malware and tools seen in Sophos MDR and Sophos Incident Response cases specifically in ransomware-related incidents

Dual-use tools

One trend that continues from previous years is the extensive use of generally available commercial, freeware, and open-source software by cybercriminals to conduct ransomware attacks and other malicious activity. Sophos MDR refers to

these as "dual-use tools," as they could be present on networks for legitimate reasons, but are frequently used by cybercriminals for malicious purposes.

Dual-use tools are different from "living-off-the-land binaries" (LOLBins) in that they are full applications deployed and used as intended by malicious actors, rather than operating system-supplied components and scripting engines. Some of the tools that fall into "dual use" are specifically security testing-oriented and intended for red teams—Impacket and Mimikatz are open-source tools that were built specifically for security researchers. Others such as SoftPerfect Network Scanner and Advanced IP Scanner are intended as tools for network administrators, but can be used by cybercriminals for discovery of networked devices and open network ports.

Figure 17: Top 15 "dual use" tools seen in Sophos MDR and Sophos Incident Response incidents, by frequency

Figure 18: Top 9 "dual use" attack tools in Sophos endpoint detections

Commercial remote access tools are collectively the most frequently used dual-use tools encountered in MDR and IR incidents:

Figure 19: Top 15 dual-use tools seen in Sophos MDR and Incident Response incidents, by frequency

With commercial remote access tools, the attackers usually abuse trial account licenses or use pirated licenses for the versions they deploy to targeted machines. In many cases, this is done after initial exploitation through malware droppers, web shells, or other command-and-control tools. In others, it is pushed through social engineering—getting a targeted individual to download

and install the tool themselves, as we have seen in recent Teams "vishing" attacks.

Use of legitimate remote machine management tools, particularly by ransomware actors, has been rising, though remote desktop access tools AnyDesk and ScreenConnect remain the most frequently used commercial IT support tools seen in Sophos MDR and IR incidents. And the most common tool remains PSExec, a Microsoft "lightweight Telnet replacement" used to remotely execute commands and create command shell sessions.

Sophos customers can restrict their usage through Sophos Central using application control policies—and should restrict any tools that are not being used for legitimate IT support.

Attack tools

Cobalt Strike, Sliver, Metasploit, and Brute Ratel are penetration testing tools, and not malware in the legal sense. But they are frequently used to deliver malware and for command and control of malware attacks. Having a well-documented, commercially supported post-exploitation tool like these is a major plus for cybercriminals who would otherwise have to build their own tools to expand their footprint within a targeted organization.

Cobalt Strike remains the most heavily used of these attack tools, present in eight percent of all incidents and nearly 11 percent of ransomware-related incidents. This is a significant decline from 2023, when Cobalt Strike was the third most frequently seen commercial tool used in MDR incidents, ranking only behind the AnyDesk and PSExec remote access tools. Sliver and Metasploit-based tools, which are available as open-source, are seen even less frequently, and Brute Ratel usage by cybercriminals remains extremely rare.

Information stealers

Figure 20: Top information-stealing malware detections reported by endpoint protection customers

Information-stealing malware is often the first step in the access broker's playbook, providing passwords, cookies, and other data that can be used for financial fraud, business email compromise, and ransomware attacks, among other schemes.

Lumma Stealer, sold through Russian-speaking forums as a Malware-as-a-Service (MaaS), was the most frequently encountered information stealer in MDR incidents, and second in overall endpoint detection reports. A major Lumma Stealer campaign beginning in October made it the most reported stealer for the last quarter of 2024, far surpassing last year's MaaS stealer leader RaccoonStealer (which released a new version in 2024 after its infrastructure was disrupted) and by year's end eclipsing Strela Stealer (which was rising in the ranks in 2023; it peaked early in 2024, but trailed off in the second half of the year). No MDR incidents tracked in 2024 involved Strela Stealer.

Figure 21: Lumma Stealer activity in 2024 as observed in customer endpoint detections

Figure 22: Lumma Stealer related MDR incidents in 2024

Figure 23: Strela Stealer activity in 2024 as observed in customer endpoint detections

First tracked in August 2022, Lumma Stealer is believed to be a successor of Mars Stealer, another information stealer purportedly of Russian origin. This stealer primarily targets cryptocurrency wallets, browser session cookies, browser two-factor authentication extensions, stored File Transfer Protocol server addresses and credentials, and other user and system data.

Like some other information stealers (such as Raccoon Stealer), Lumma Stealer can also be used to deliver additional malware—either by launching executables or PowerShell scripts, or by loading malicious DLLs from its own process. Typically, Lumma Stealer is delivered from a compromised website (often a fake CAPTCHA web page) as a download that victims are brought to via malvertising.

Lumma Stealer is generally associated with broader cybercriminal activity. Another MaaS stealer sold on Russian-language forums, StealC, was seen with a much higher correlation to ransomware incidents. Introduced in January 2023, it has been labeled by researchers as a RaccoonStealer and Vidar copycat.

Of regional note is Mispadu Stealer, which continues to target Latin America (and Mexico in particular). In the second quarter of 2024, it was the second-most detected stealer, coming in just behind Strela Stealer, with 74% of those detections coming from Mexico. It has been seen using malicious web and search advertising, notably posing as web ads for McDonald's.

Top ransomware threats

Figure 24: Most frequently detected ransomware families across all Sophos endpoint customers

Figure 25: The top ransomware families encountered in MDR and Incident Response incidents

LockBit, sort of

The most-detected ransomware family in 2024 was LockBit, but not because of the ransomware group that spawned it. In February 2024, US and UK law enforcement claimed to have disrupted the LockBit group by seizing the ransomware-as-a-service group's servers, arresting two of its members, and charging another in an indictment. In the wake of this disruption, numerous variants based on the leaked LockBit 3.0 code became active in the wild, resulting in a spike of LockBit detections in early 2024. However, by March, detections trailed off significantly with a slight rebound in April and early May (though the LockBit gang may not be gone forever).

The groups using LockBit 3.0 frequently used EDR killers and other malware and techniques to attempt to disable endpoint protection. Their initial access was often through VPN accounts that had been compromised (in some cases due to vulnerabilities in the VPN devices themselves), or through the abuse of credentials harvested from unmanaged devices to gain remote access.

Figure 26: LockBit variant detections per day, 2024

Akira and Fog

In terms of actual incidents, the Akira ransomware-as-a-service led the pack in 2024, ultimately stepping in to fill the void left by LockBit. Initially seen in 2022, Akira attacks ramped up in late 2023. The group and its affiliates were steadily active throughout 2024, spiking in August when Akira accounted for 17% of the ransomware detections reported by Sophos customers—doubling from its

position in the first two quarters of the year. By year's end, it still accounted for 9% of ransomware detection reports.

Notably, Sophos observed affiliates tied to Akira also deploying other ransomware variants, including Fog, Frag and Megazord. These attackers (such as those in STAC5881) typically focused on exploiting VPNs for initial access. Typically, Akira's targets had VPNs with no multifactor authentication, or had misconfigured VPN gateways that allowed the attackers to gain access with stolen credentials or brute force attacks.

While Akira remains active, Fog ransomware has occasionally been used as a replacement by affiliates previously connected to Akira, which accounts for its position in third among the top 15 ransomware families encountered in MDR and IR incidents.

RansomHub

RansomHub was another emerging leader in ransomware incidents in 2024. While tied for sixth in overall detections, RansomHub was the fourth most observed ransomware family in actual MDR and IR incidents.

Between February and August 2024, according to a Cybersecurity and Infrastructure Security Agency #StopRansomware advisory, RansomHub had "encrypted and exfiltrated data from at least 210 victims." The majority of Sophos MDR and IR cases involving RansomHub came in the second half of the year, mounting in numbers in November.

Most RansomHub attacks involved abuse of RDP in addition to other legitimate remote desktop tools, including AnyDesk. Initial access in some reported cases came from leveraging the seven-year-old Windows SMB Remote Code Execution Vulnerability (CVE-2017-1444), though this was not observed in the Sophos MDR and IR cases represented in our data. Initial access vectors Sophos X-Ops observed in RansomHub cases included abuse of externally facing Microsoft SQL Servers for command execution, abuse of open RDP and Remote Desktop Web access, and compromise of unmanaged devices.