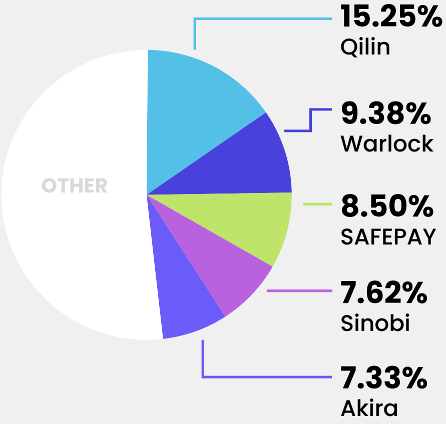
BYER–NICHOLS THREAT BRIEF

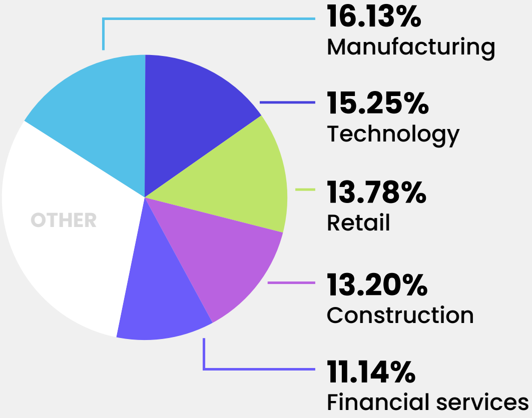
SECOND HALF AUGUST 2025

We all knew that sooner or later we would start to see malware that leverages generative AI. PromptLock, which was recently discovered by ESET, makes use of GenAI to analyze files on victim systems to work out whether to encrypt or exfiltrate the files. We are also seeing more active malware that is targeting MacOS and Linux. In fact, half of the trending malware variants that we focus on in this brief specifically target Linux and MacOS—a firm reminder that no matter which OS you are running, you should ensure that you have strong endpoint protection and detection capabilities in place.

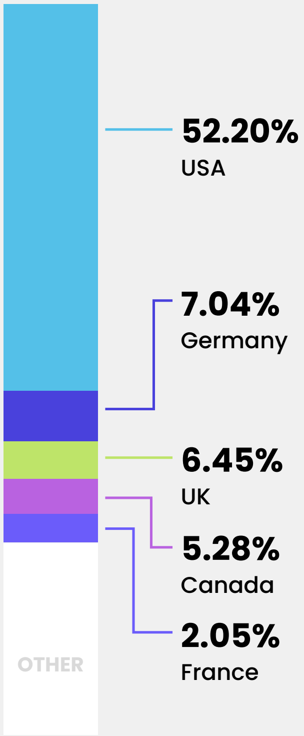
Top ransomware



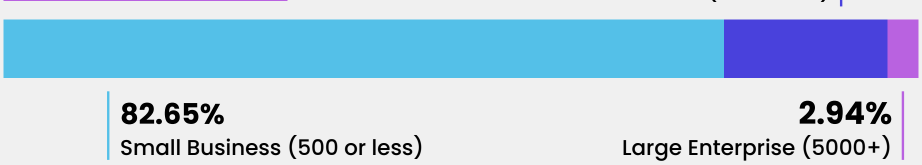
Victim sector



Victim locations



Victim org size



Trending malware

DripDropper

DripDropper is a perfect example of the fact that malware doesn't only affect Windows and MacOS systems - Linux is vulnerable too. The malware exploits a vulnerability in Apache ActiveMQ (CVE-2023-46604). After establishing persistence, it patches the vulnerability to secure exclusivity and disguise its initial access path. Once it has established persistence, it communicates with an adversary-controlled Dropbox account for command and control.

PromptLock

We knew it was only a matter of time until malware would also start to use generative AI. Promptlock, which was recently discovered by ESET, creates Lua scripts which can operate on MacOS, Windows and Linux. It uses GenAI to analyze local files, and depending on their content either encrypts or exfiltrates them.

MixShell

Mixshell is a sophisticated threat actor who engages in phishing activities by contacting target entities via their "Contact us" forms on their public web sites. Through social engineering they trick company representatives to click on malicious links which trigger the installation of malware. Their primary targets are industrial supply chain companies in the US.

RingReaper

Yet another example of Linux malware is Ringreaper, which uses the Linux io_uring interface, which is normally used for asynchronous I/O, to evade EDR software. By using io_uring for file and network operations, Ringreaper reduces the traces which EDR tools can use to detect malware, making itself almost invisible.

Shamos

A sophisticated malware campaign that targets MacOS users, Shamos lures Mac users to fake tech support websites and tricks users who are looking for solutions to technical issues into downloading malware which captures the user's password and downloads the SHAMOS executable which establishes persistence by installing a malicious Plist in the user's LaunchDemons directory.

TamperedChef

This cybercrime campaign uses malvertising tactics to trick users into going to fraudulent websites which lure users into downloading the TamperedChef infostealer. It masquerades as a free PDF editor called AppSuite PDF Editor. Once installed it enumerates installed security tools and attempts to stop web browsers to gain access sensitive data such as credentials and cookies.

Top news

- US seizes $2.8 million in crypto from Zeppelin ransomware operator, sanctions Grinex crypto-exchange
- DOJ charges 22-year-old man behind RapperBot botnet used in over 370,000 DDoS attacks
- Scattered Spider hacker gets sentenced to 10 years in prison
- Dev gets 4 years for creating kill switch on ex-employer's systems
- Massive anti-cybercrime operation leads to over 1,200 arrests in Africa
- Malicious Android apps with 19M installs removed from Google Play
- New AI attack hides data-theft prompts in downscaled images
- Malware devs abuse Anthropic's Claude AI to build ransomware

Trending adversaries

APT36 **Salt Typhoon** **Silver Fox**

Blind Eagle **Silk Typhoon** **Storm-0501**

Active vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2024-8068	Citrix	Session Recording
CVE-2024-8069	Citrix	Session Recording
CVE-2025-20265	Cisco	Secure Firewall Management Center
CVE-2025-43300	Apple	iOS, iPadOS, and macOS
CVE-2025-48384	Git	Git
CVE-2025-52970	Fortinet	FortiWeb
CVE-2025-54948	Trend Micro	Apex One
CVE-2025-57819	Sangoma	FreePBX
CVE-2025-7775	Citrix	NetScaler
CVE-2025-9074	Docker	Desktop

Qilin continues to maintain its top spot amongst ransomware actors, albeit with a slightly lower percentage of infections. Akira and Sinobi continue to make their presence known. SafePay, which initially surfaced in late 2024, has now made its way into the top 5. Warlock, which only made its public debut in June 2025, is notable for exploiting vulnerabilities in unpatched Microsoft SharePoint servers.

Cyber-attacks often mirror real-world rivalries. APT36 is a Pakistani cyber espionage group which is using sophisticated phishing campaigns to target Indian defense personnel. The group sends phishing emails containing malicious PDFs, with a blurred background, along with a button that emulates the login interface of the Indian National Informatics Centre (NIC). Users who click the button are redirected to a URL which downloads a ZIP archive, posing as a legitimate application. The campaign is focused on credential theft and establishing long-term persistence inside Indian defense networks. Another 2 trending adversaries who are believed to be nation state actors are Salt Typhoon and Silk Typhoon, both of whom are believed to be engaged in espionage activities. Both are suspected of having links to China's Ministry of State Security (MSS).

In this period, we are seeing a particularly high number of trending and actively exploited vulnerabilities. Of particular concern are 3 vulnerabilities impacting Citrix technologies (CVE-2024-8086, CVE-2024-8069 and CVE-2025-7775). It is worth noting that the first 2 of these date back to 2024 and are not new. CVE-2025-43300, which is related to an out of bounds write issue, is of worrying because of its broad impact across iOS, IpadOS and MacOS. Apple believes this vulnerability may have been exploited in a sophisticated attack against specifically targeted individuals.

BYER CO

WRITTEN BY JEREMY NICHOLS, FORMER DIRECTOR OF THE GLOBAL THREAT INTELLIGENCE CENTER

EXECUTIVE SUMMARIES & ADVERSARY BIO'S BY GEOFF REHMET, CYBERSECURITY EXPERT

PRODUCED & DISTRIBUTED BY BYER CO'S CYBERSECURITY MARKETING DIVISION