Bitdefender

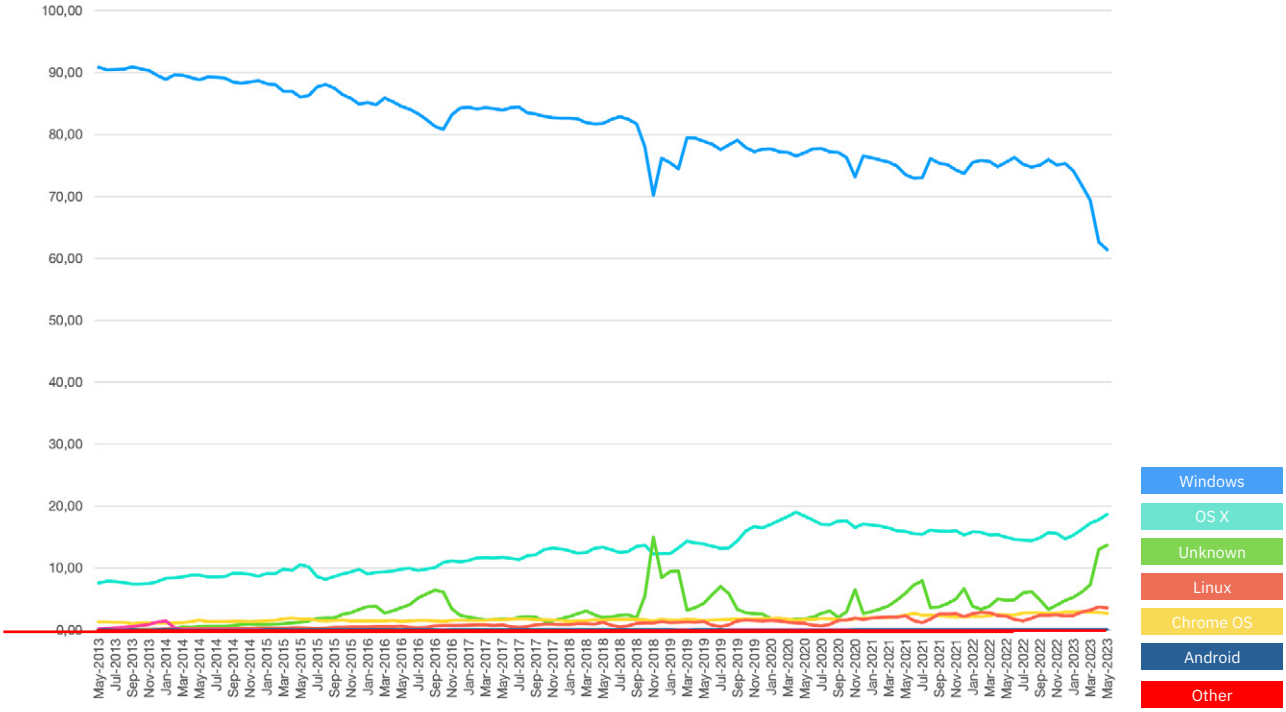
REPORT

macOS Threat Landscape Report

Contents

Executive Summary

Apple's desktop operating system has been steadily gaining ground in the past decade, and currently commands almost 18% of desktops worldwide – a 10% increase from 2013, according to Statcounter.



Macs are far less targeted than Windows computers, as Microsoft still rules the land with 63% of the desktop market. Threat actors are devoting time and resources to exploit the larger attack surface provided by Microsoft.

But while Apple users enjoy less risk due to the platform's smaller footprint, Macs aren't bulletproof. Apple finds itself consistently having to patch actively exploited vulnerabilities as threat actors employ social engineering vectors and spray-and-pray techniques.

Moreover, spyware vendors are increasingly targeting Apple's iOS, which shares many common components with macOS, like the web rendering engine WebKit. As a result, threat actors are starting to attack Macs more efficiently with threats designed to exploit unpatched flaws and lax cybersecurity hygiene.

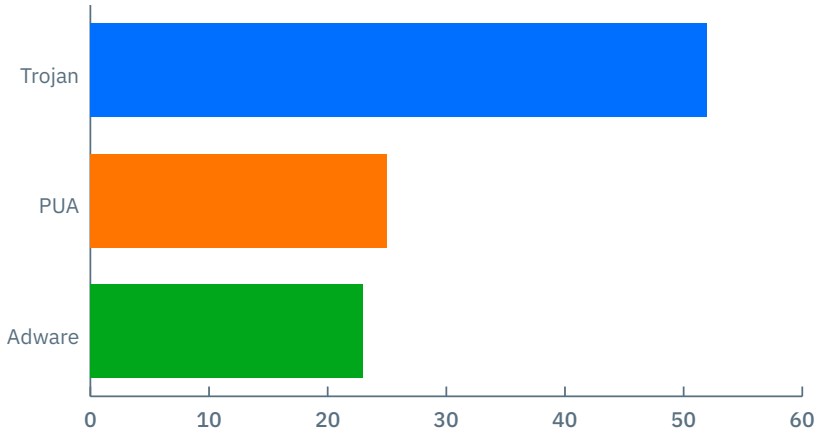
Key findings

- → Mac users are targeted by three key threats: Trojans, Adware and Potentially Unwanted Applications (PUAs)
- → Trojans are the biggest single threat to Macs, accounting for more than half of threat detections followed by PUAs and Adware
- → EvilQuest remains the single most common piece of malware targeting Macs at 52.7%
- → Trojans designed to exploit unpatched vulnerabilities present a real danger to users who typically postpone installing the latest security patches from Apple
- → With a 25.3% share, PUAs represent a quarter of “executable” threats to Macs
- → 8% of PUA detections on Macs are crypto miners and 1% are jailbreak utilities
- → Trojans designed to exploit unpatched vulnerabilities present a real danger to users who typically postpone installing the latest security patches from Apple
- → Threats designed to infect Macs typically require victims to manually run an executable
- → Threat actors put effort into making malware packages look and feel like legitimate applications

Top threats targeting Macs

Data gathered annually by Bitdefender shows that Mac users are mainly targeted by three key threats: **Trojans**, **Adware** and **Potentially Unwanted Applications (PUAs)**. While named differently, these hazards share one trait: they require victims to manually run the threat, meaning their authors try hard to make their malware look like legitimate applications.

2022 was no different, as most malware infections on Macs were predictably spread across these three categories of threats.



Trojan	PUA	Adware
51.8%	25.3%	22.6%

Just like the years prior, **Trojans** remain the biggest single threat to Macs, accounting for more than half of the threats detected. **PUAs** occupy the second spot, with more than a quarter of detections. **Adware** follows closely, at just over a fifth of threats targeting Mac computers.

Trojans

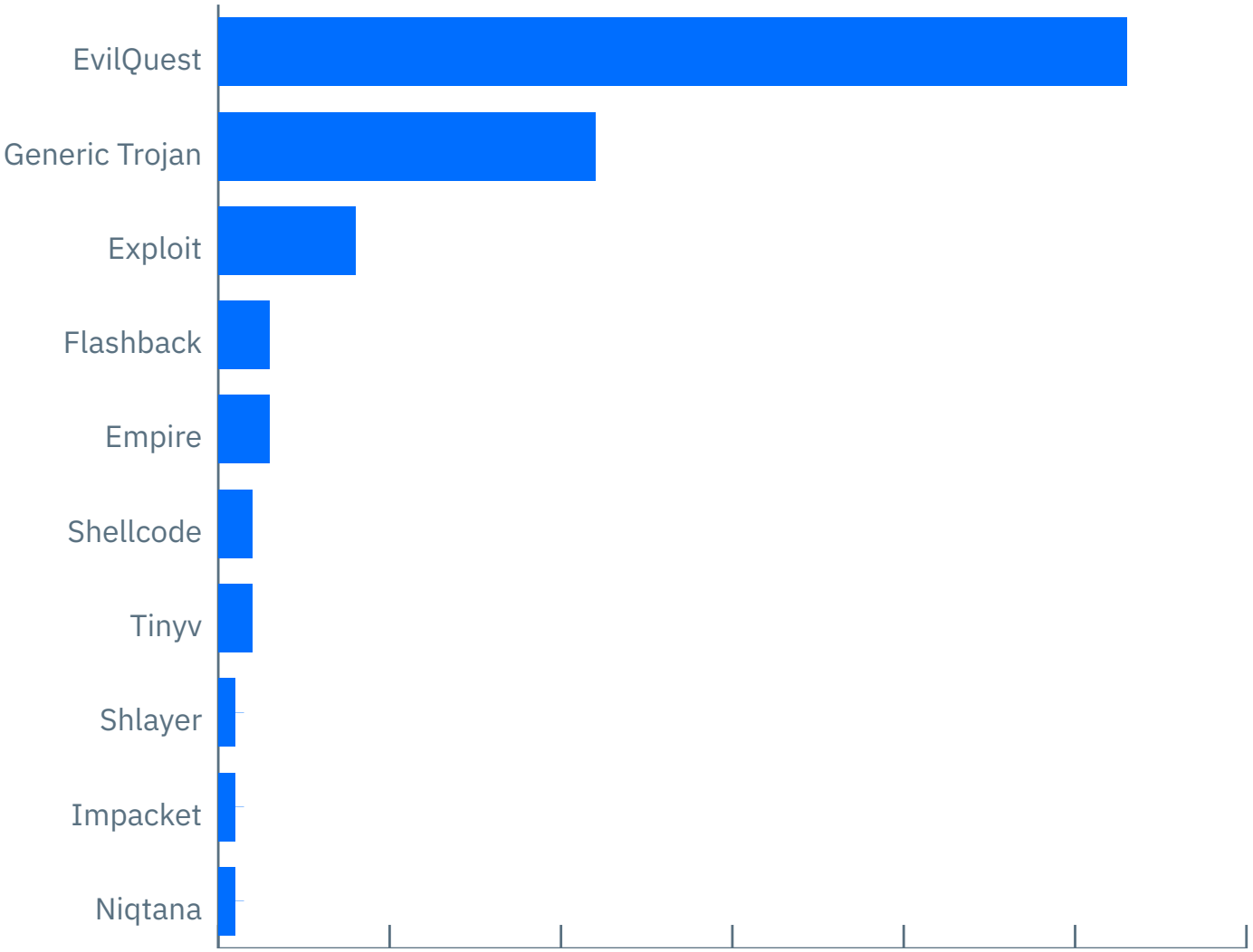
Trojans remain the most prolific form of malware targeting Macs. Threat actors use every trick in the book to infect systems , including:

→ Socially engineered communications (spam, phishing, social media)

→ Rigged advertisements served via social media or websites (malvertising)

→ Tainted file downloads via torrent or warez websites

Most Trojan families listed in this report are household names in the macOS threat landscape. While some can be considered legacy malware, threat actors still use them, with some degree of success, as many users are careless and don't configure proper security settings and/or deploy a dedicated security solution.



EvilQuest	Generic Trojan	Exploit	Flashback	Empire	Shellcode	Tinyv	Shlayer	Impacket	Niqtana
52.7%	22.4%	8.2%	2.7%	2.6%	1.9%	1.7%	1.4%	0.8%	0.6%

EvilQuest

First discovered in mid-2020, **EvilQuest** remains the single most common Trojan targeting Macs, with a 52.7% share. The malware bundles a ransomware component designed to encrypt and pilfer the victim's files, as well as a keylogger to record keystrokes and steal personal or financial data.

While most antivirus vendors recognize and block EvilQuest, its continued abundance indicates that attackers are still using it in a spray-and-pray fashion, hoping to catch unprotected systems in their nets.

Generic Trojans

Twenty-two percent of detections include several **Generic** Trojans whose characteristics are similar, if not identical, and therefore don't get their own name on the list.

Exploit Trojans

Taking third place with an 8.2% detection rate, **Exploit** Trojans leverage known / unpatched flaws in macOS and are designed to deploy timely payloads (additional malware components) without the user's knowledge. Exploit-centric Trojans present a real danger to users who don't run an antivirus on their Mac or, as is typical, postpone installing their security patches from Apple.

Flashback

With a relatively small 2.7% detection rate, **Flashback** represents a type of Trojan that disguises itself as a legitimate app or installer (update) to trick users into running the threat with their own hands.

Flashback marked the beginning of sustained malware development for the Mac when it emerged more than a decade ago. It's enough to warrant it a mention as it still makes the rounds 12 years after it was originally detected by security researchers.

Empire

Empire is a partially defunct threat, but still emerges in our telemetry with a 2.6% detection rate years after inception. Its rapidly-deployable post-exploitation modules include keyloggers and data stealers, and it boasts adaptable communications to evade network detection.

Shellcode

Shellcode is an instruction set that can be leveraged to execute a command and take control of or exploit a vulnerable machine. Trojans that run **Shellcode** on the target system to launch malware or download additional payloads had a considerably low detection rate of 1.9% during the tracked period (Jan-Dec 2022).

Shlayer

Typically disguised as installers and various cracking tools, **Shlayer** continues to emerge 1.4% of the time and delivers adware, unwanted applications, and promotes fake search engines. Most infections come from warez and torrent sites.

Potentially Unwanted Applications

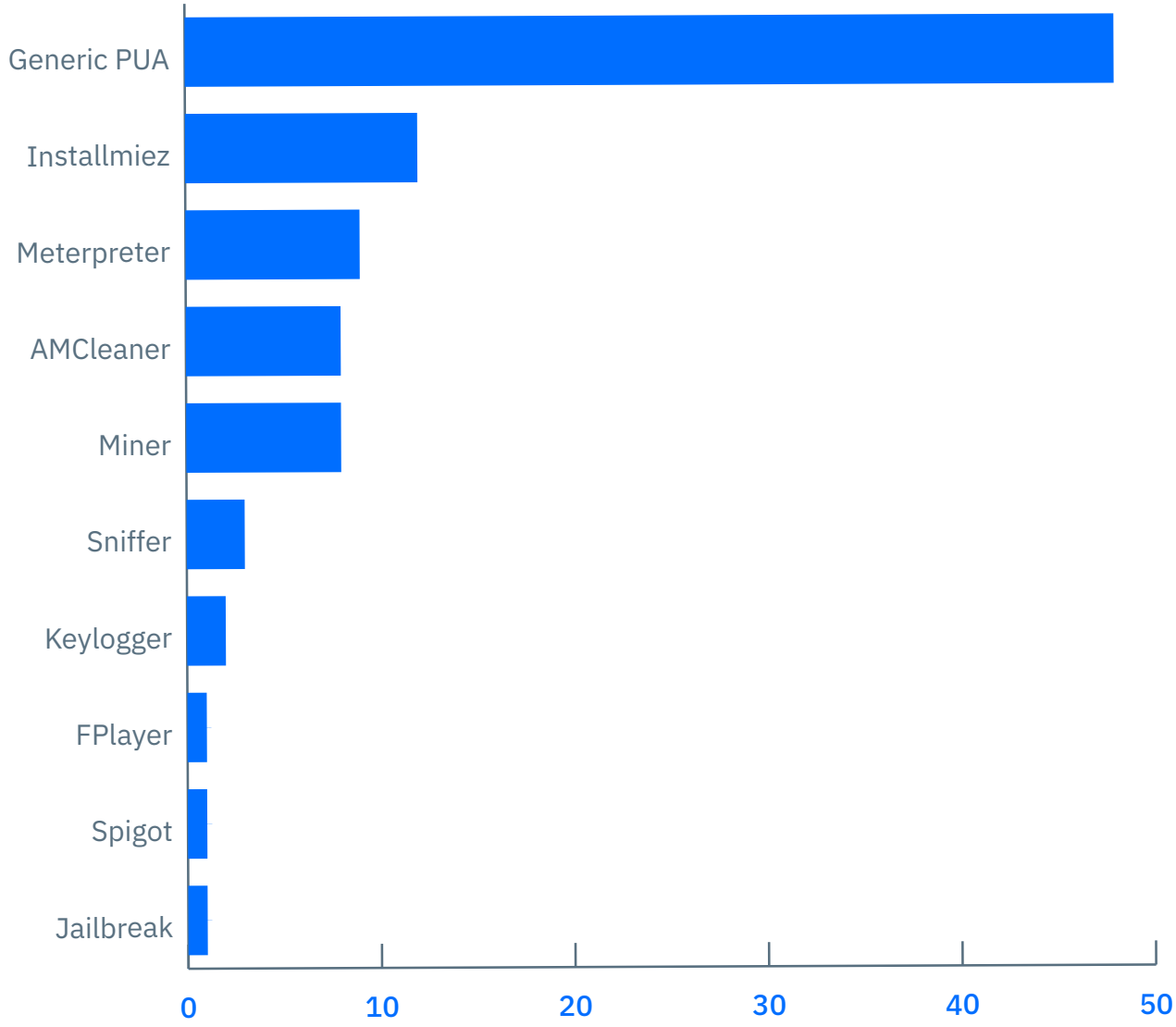
Walking the thin line between nuisance and threat , PUAs are commonly found as freeware, repackaged applications or utility apps (i.e. system cleaners) with hidden functionality like data tracking and coin mining.

Some PUAs hijack the user's browser, changing the default search engine and installing plugins without consent. Highly aggressive PUAs can modify third-party apps, download additional (unsolicited) software, and alter system settings. With a 25.3% share, PUAs represent a quarter of "executable" threats to Macs.

Many of apps in the macOS ecosystem check the boxes that describe a PUA program, including:

→ remote admin tools
→ system cleaners
→ (fake) virus scanners
→ battery life savers
→ memory utilities

Even with Apple keeping close tabs on the ecosystem, developers have flooded the market with 'shady' apps, some persuasive enough to get users to disable restrictions and run apps from any source. While most PUA detections are generic in nature, common names still crop up in our telemetry.



Generic PUA	Installmiez	Meterpreter	AMCleaner	Miner	Sniffer	Keylogger	FPlayer	Spigot	Jailbreak
47.8%	11.7%	9.2%	8.0%	8.0%	3.3%	1.5%	1.1%	1.1%	1.0%

Installmiez

Installmiez is one of the oldest PUA detections recorded on Macs. Delivered as fake installers through pop-ups or downloaded by other shady apps, this threat harbors a secondary payload that can be anything from adware to data stealing malware. Attackers constantly update the second payload, meaning Installmiez often drops a different threat.

Meterpreter

Part of the Metasploit Project and Framework, Meterpreter is a penetration testing tool designed to help security teams address vulnerabilities on targeted apps. It's mostly used for beneficial hacking, but it can also be used by unethical hackers eager to exploit vulnerable targets.

AMCleaner

We detect AMCleaner as fake optimization tools or bogus security software that try to trick users into purchasing a paid version of a system utility or an antivirus – typically one that doesn't work as advertised. "Cleaner" apps are common threats in the macOS landscape and often exhibit scareware behavior.

Miners

Crypto mining is not too common on Macs, but some PUAs are designed to do just that – without the user's consent. Unwary users often do the legwork for crypto-hungry threat actors after getting infected with mining software. Miners make their way onto Macs through many different avenues, including browser pop-ups and plugins, freeware apps, software downloaded through warez or torrent sites, and more. Coin miners are not technically considered "malware" but they do hog computing power and eat away at battery life, which wears down the system.

Spigot

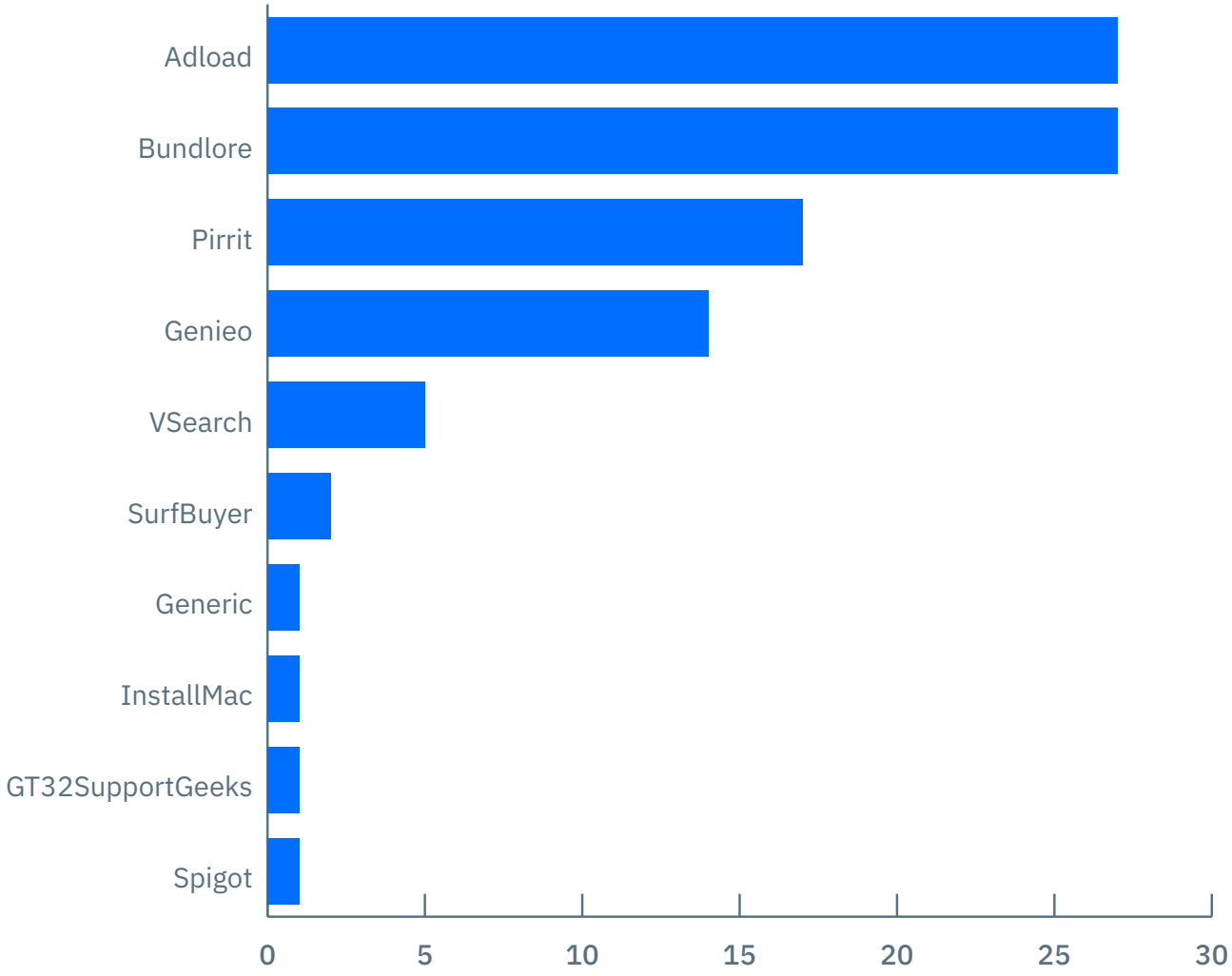
Spigot is the detection name for applications that install themselves as extensions on your web browser and display ads – essentially making them adware. Developers use clever application names to trick users into downloading and installing what appears to be a reputable, legitimate app.

Jailbreak

Once a popular practice among iOS aficionados, jailbreak assistants designed to 'unlock' iPhones are now less common with a meager 1% of all PUA detections. Common jailbreak utilities represented in this detection can include the likes of PaleRa1n, Blizzard Jailbreak, ayakurume, Dopamine, Fugu15, and others.

Adware

Adware enables developers to make money out of advertising other products, sometimes in an aggressive way and with spyware-like behavior. Adware accounts for more than a fifth of threats targeting Macs. Like most file-based threats, adware ends up on computers after users willfully run freeware programs, fake installers, software downloaded from torrents and wares sites, pirated programs, malicious links, malvertising, and others.



Adload	Bundlore	Pirrit	Genieo	VSearch	SurfBuyer	Generic	InstallMac	GT32SupportGeeks	Spigot
27.2%	26.5%	16.6%	14.2%	5.5%	1.8%	0.8%	0.6%	0.6%	0.6%

Adload

Known to impersonate popular video players and other common applications, Adload hijacks browsers and forces victims to visit potentially malicious websites, enabling cyber criminals to make money. It's mostly served through malicious links and makes up the bulk of adware detections (27.2%) by Bitdefender solutions.

Bundlore

Bundlore accounts for more than a quarter of adware detections on Macs and represents a family of adware droppers. As its name suggests, the threat 'bundles' multiple threats . After installation, Bundlore apps deliver intrusive advertisements (coupons, banners, pop-ups, etc) and gather data from the system, including the user's personal information.

Apps from the Bundlore family often infiltrate the target system as browser extensions capable of collecting data entered into forms, meaning they can also access sensitive data like usernames, passwords, or credit card numbers.

Pirrit

Pirrit is the third-most-abundant form of adware found on Macs. It displays intrusive and deceptive advertisements and gathers data from the infected system. Ads served include coupons, surveys and pop-ups. If clicked, users are taken to shady websites or scripts that automatically download additional unwanted payloads.

Genieo

At 14.2% , this piece of adware is notorious for making it hard for the user to remove the threat. After it installs itself, Genieo hijacks the user's browser and mines information. Because it behaves like a virus, Genieo is considered borderline malware. When it emerged almost a decade ago, Genieo became a catalyst for adware development and deployment on macOS.

VSearch

Although ranked in the single digits, VSearch is a fairly common piece of adware that hijacks web browsers after masquerading as a legitimate software download. VSearch fetches intrusive ads and serves questionable content from unknown servers. It often changes sources to thwart detection.

Top 15 families

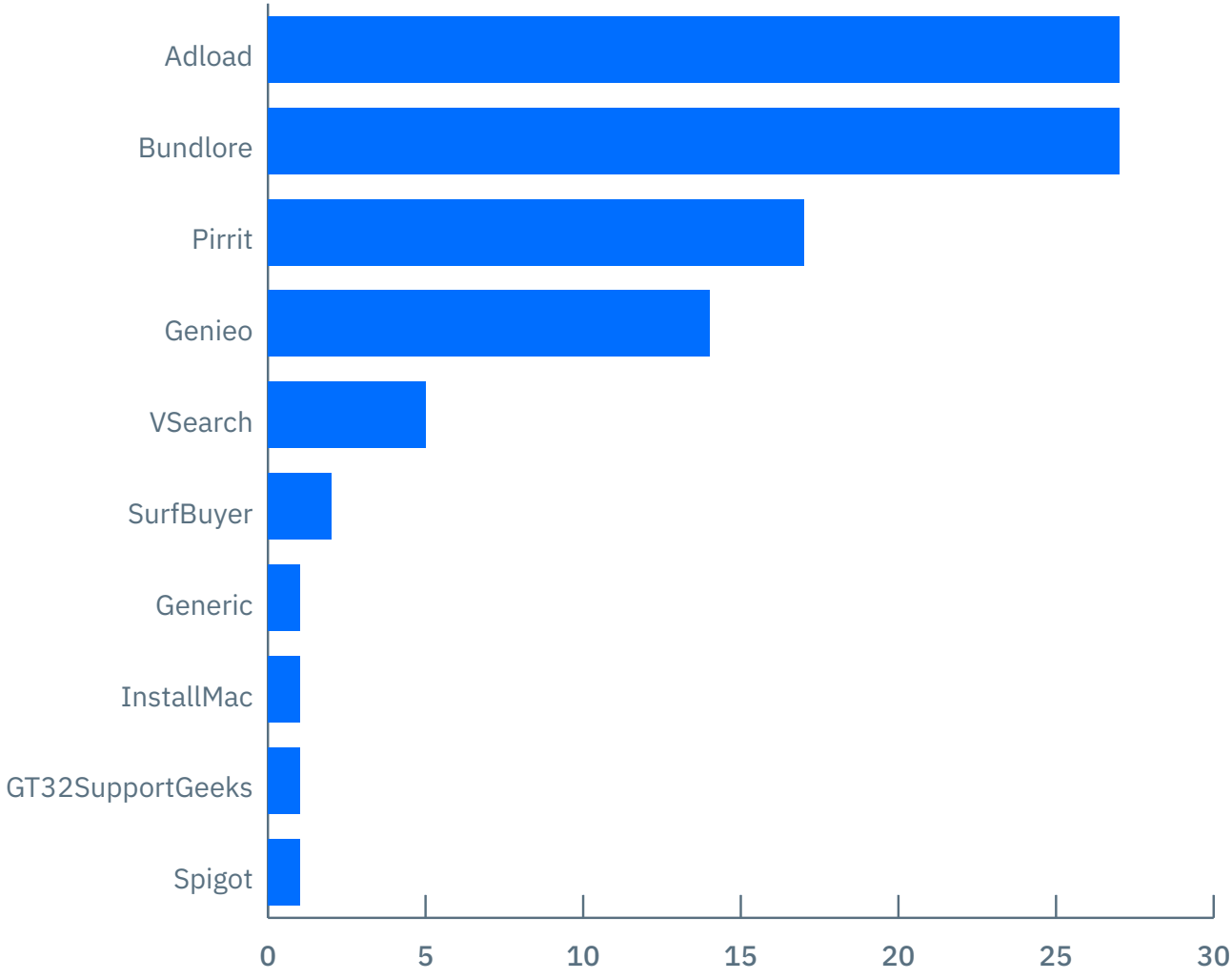
For extra visibility into the key threats making the rounds in the Mac ecosystem, these are the top 15 detections (designated as “families” of threats) aggregated from all three main categories (Trojan, PUA and Adware). Some key findings:

→ The ransomware-laden **EvilQuest** trumps every other threat on the board, scoring over **27%** just by itself

→ In second place, **Generic** detections from all categories come together to account for some **23.9%** of all file-based (executable) threats on macOS

→ Moving into the single digits, **Adware** leads the pack with considerable activity from the likes of **Adload**, **Installmiez** and **Bundlore**

→ **Shellcode**-centric Trojans, with a small **1%** share, were the least-detected threat targeting Macs in 2022



EvilQuest	27.3%	**Meterpreter**	2.3%
Generic	23.9%	**Miner**	2.0%
Adload	6.1%	**AMCleaner**	2.0%
Bundlore	6.0%	**Flashback**	1.4%
Exploit	4.3%	**Empire**	1.3%
Pirrit	3.8%	**VSearch**	1.2%
Genieo	3.2%	**Shellcode**	1.0%
InstallMiez	3.0%		

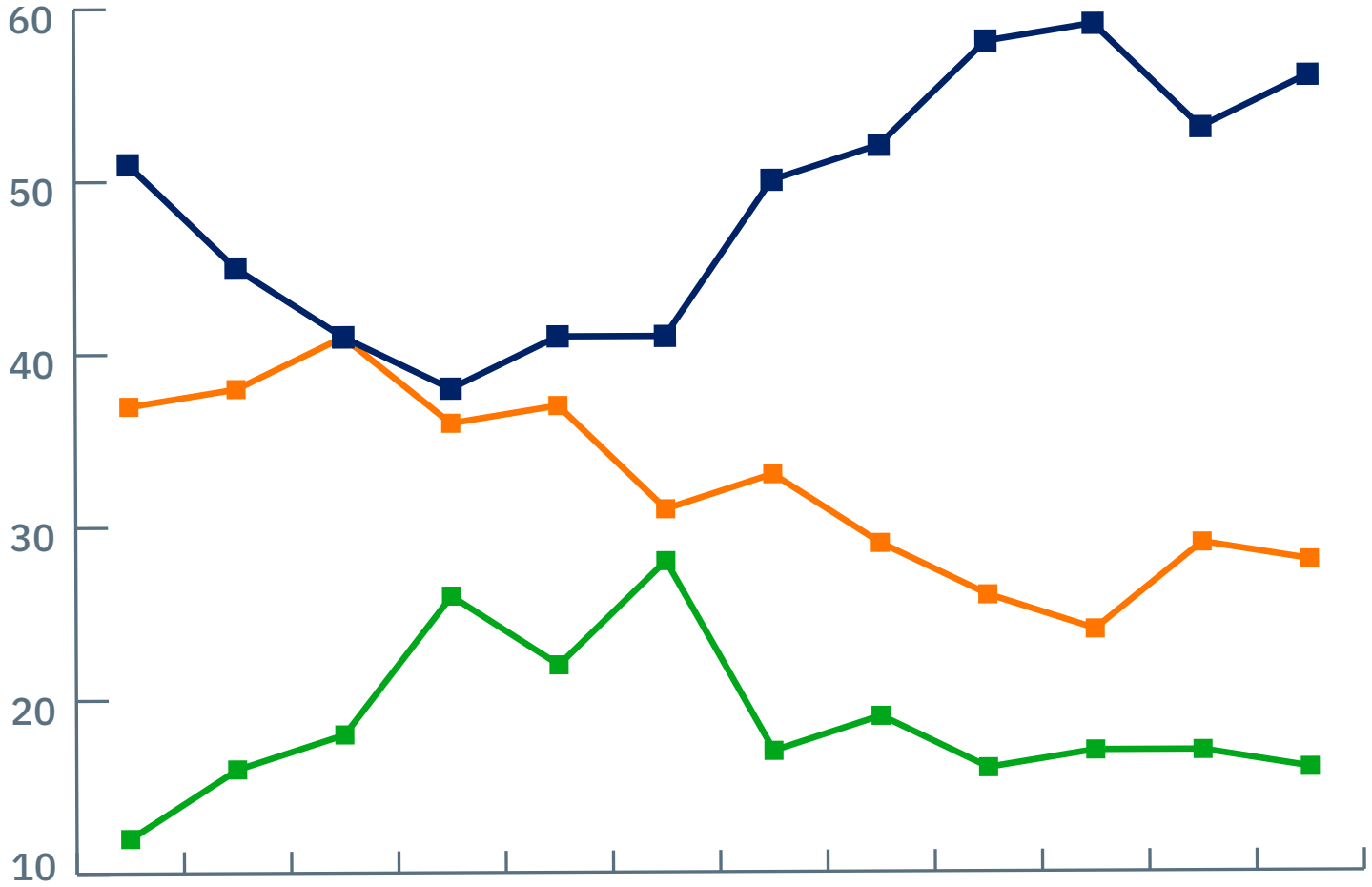
Threat evolution

In the 12-month period tracked in this report, Trojan activity oscillated the most, registering the lowest activity in April-May (38.18%) and the highest in October (59.3%). Trojan activity at the end of the year was 55.59%, only a few points above the annual average, indicating that 2023 is on track to record similar activity. As the chart shows, Trojan activity in the June – December period (H2) was considerably higher than other threats.

By contrast, PUA and Adware infections dwindled in H2 and even more so towards the end of the year.

PUA and Adware activity was considerably lower in December than at the start of the year. Adware detections registered their lowest point at the start of the year (12.42%), while the lowest detection rate for PUA activity was in October (23.61%).

Adware activity peaked in June (28.02%) while PUA detections peaked in March (40.79%), matching Trojan detections decimally around that point.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Trojan	50.68%	45.29%	41.08%	38.18%	40.95%	41.21%	49.98%	52.14%	57.87%	59.30%	53.45%	55.59%
PUA	36.86%	38.32%	40.79%	36.11%	36.84%	30.67%	32.54%	28.97%	25.83%	23.61%	29.35%	27.87%
Adware	12.42%	16.19%	18.06%	25.63%	22.15%	28.02%	17.44%	18.85%	16.27%	17.04%	17.09%	16.40%

Conclusion

It's true that Apple's ecosystem – often touted as a walled garden safe from malware – enjoys a narrower range of threats than Microsoft's or Google's ecosystems. However, our research shows that this apparent safety net isn't impenetrable. In fact, this false sense of protection often means malware tailored to infect Macs is better suited to its goals. Threat actors have less attack surface to exploit, so they are forced to optimize their techniques and procedures to ensure better success.

In recent years, Apple has issued a multitude of security patches to address critical weaknesses that were said to be "actively exploited" by threat actors. Many of those flaws were found in key components shared by both Macs and iPhones. Many (if not most) users procrastinate updating software and deploying security fixes. And statistics show that the vast majority of Mac owners use older generations of macOS.

Bitdefender recommends that Mac users stay up to date with the latest OS version and always apply the newest security patches. Equally important, never download software from unofficial sources, like torrents and warez sites. These hubs harbor most of the threats discussed in this report.

Our findings send a clear signal that Mac users are becoming more vulnerable to online threats, making it important to deploy a dedicated security solution to keep watch over any potential malicious activity.

Bitdefender Total Security boasts unbeatable multi-layered protection to keep your Mac safe from all-new and existing threats with minimal impact on system performance. Learn more at bitdefender.com/solutions/total-security.html.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com