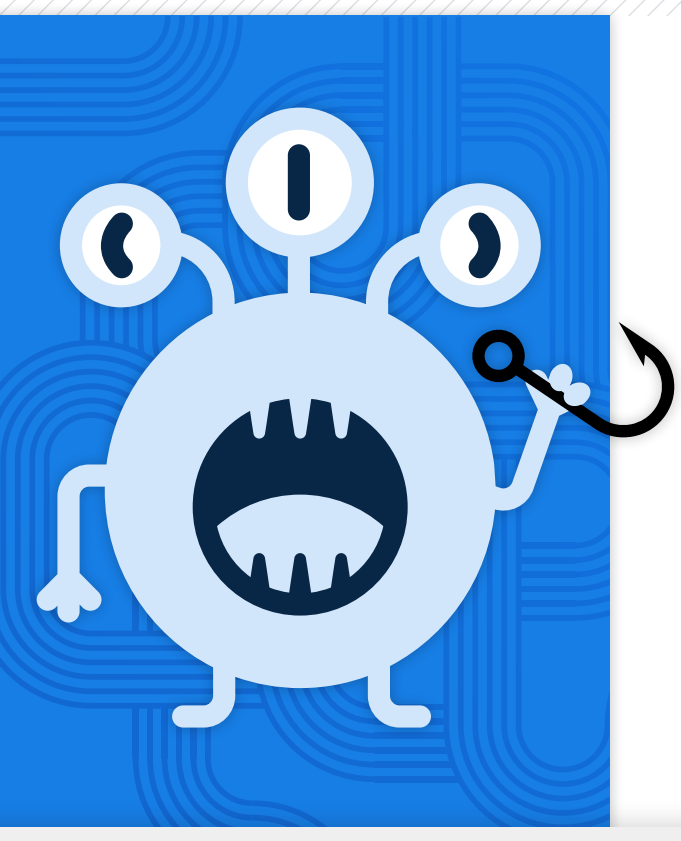
SOC SNAPSHOT: Q2 2023

What we're seeing:

Malware families linked to pre-ransomware operations shifting gears to commodity malware



Understanding types of malware

A malware incident occurs when it reaches a managed asset.

Pre-ransomware involves allowing ransomware–likely malware–to persist, often with initial and remote access tools.

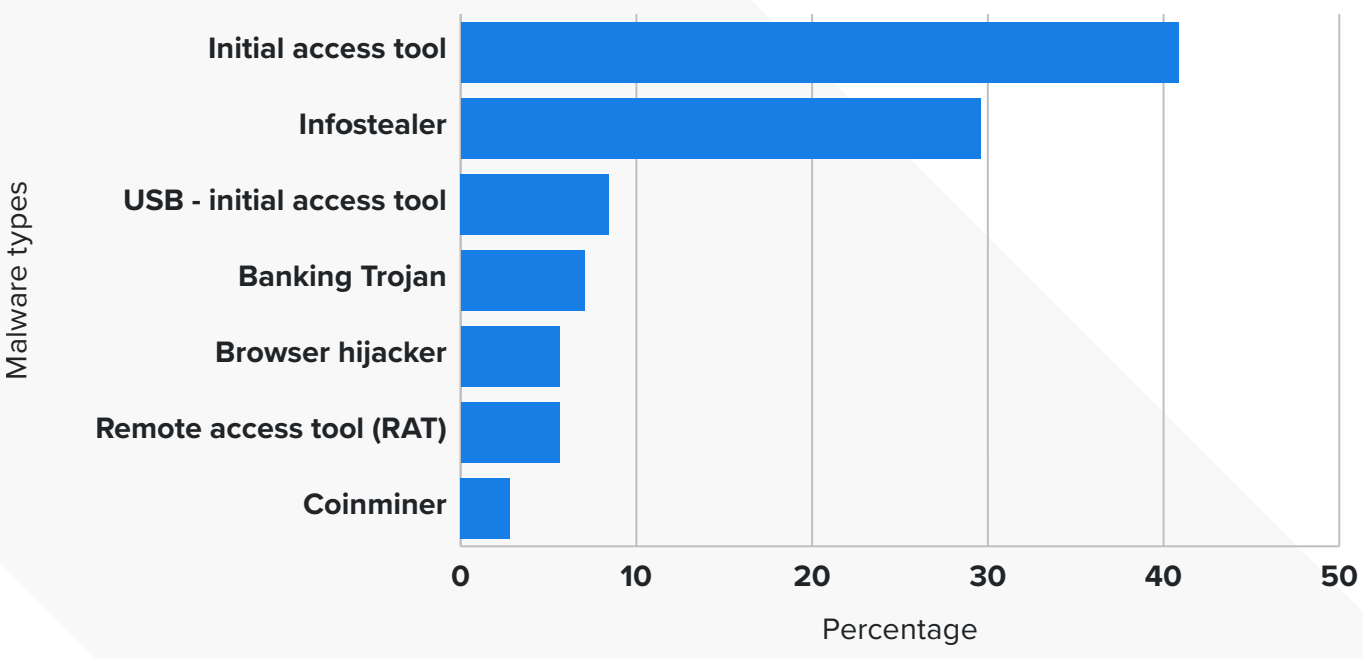
Commodity malware is malware available for purchase, so it's easy for bad actors to access it with a low lift (and a credit card).

What does commodity malware attempt to do?

- ✅ **Infostealer:** accesses sensitive data stored in the user's browsers or on their device
- ✅ **Banking Trojan:** steals or intercepts financial information from the user's browser
- ✅ **Browswer hijacker:** redirects the user to ads or malicious websites
- ✅ **Coinminer:** uses the browser's computer resources to generate cryptocurrency for the attacker

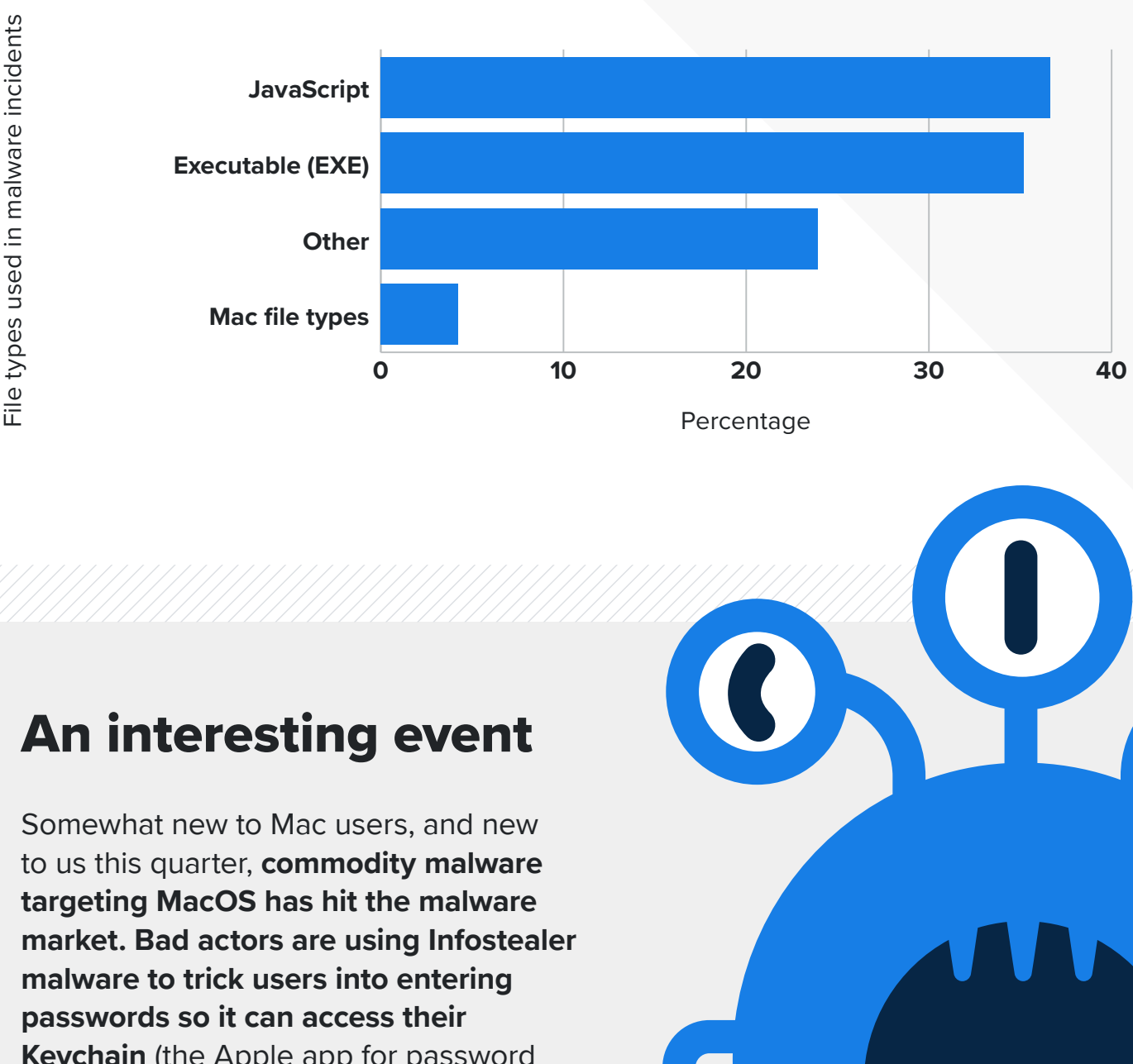
What did our SOC see?

Commodity malware accounted for 23% of all incidents we saw in Q2. The malware families selling these commodities were also linked to pre-ransomware operations we've previously seen.



How'd they get in?

Elusive malware continues to use JavaScript files, LNK, and HTA files to gain entry.



An interesting event

Somewhat new to Mac users, and new to us this quarter, **commodity malware targeting MacOS has hit the malware market. Bad actors are using Infostealer malware to trick users into entering passwords so it can access their Keychain** (the Apple app for password storage).

How can I protect my organization?

Your IT team needs a list of remote access tools allowed in your organization's environment. If you don't have a list, get one. Knowing how your employees access your network can improve your ability to identify unauthorized access.

Want more insights from our SOC?
Get your copy of the full Q2 2023 Threat Report

Read it now

www.expel.com