baseVISION TI Report #2

A Looming Menace and Escalating Threat to macOS users

baseVISION

It was once commonly believed that macOS was more secure than any other operating system, with malware being a rare concern. However, the reality today paints a different picture, as macOS is increasingly becoming a prime target for malware, particularly infostealers. At the same time, the adoption of Mac devices in European corporate environments has been steadily rising overtime, with a subsequent increasing exposure to this type of threats.

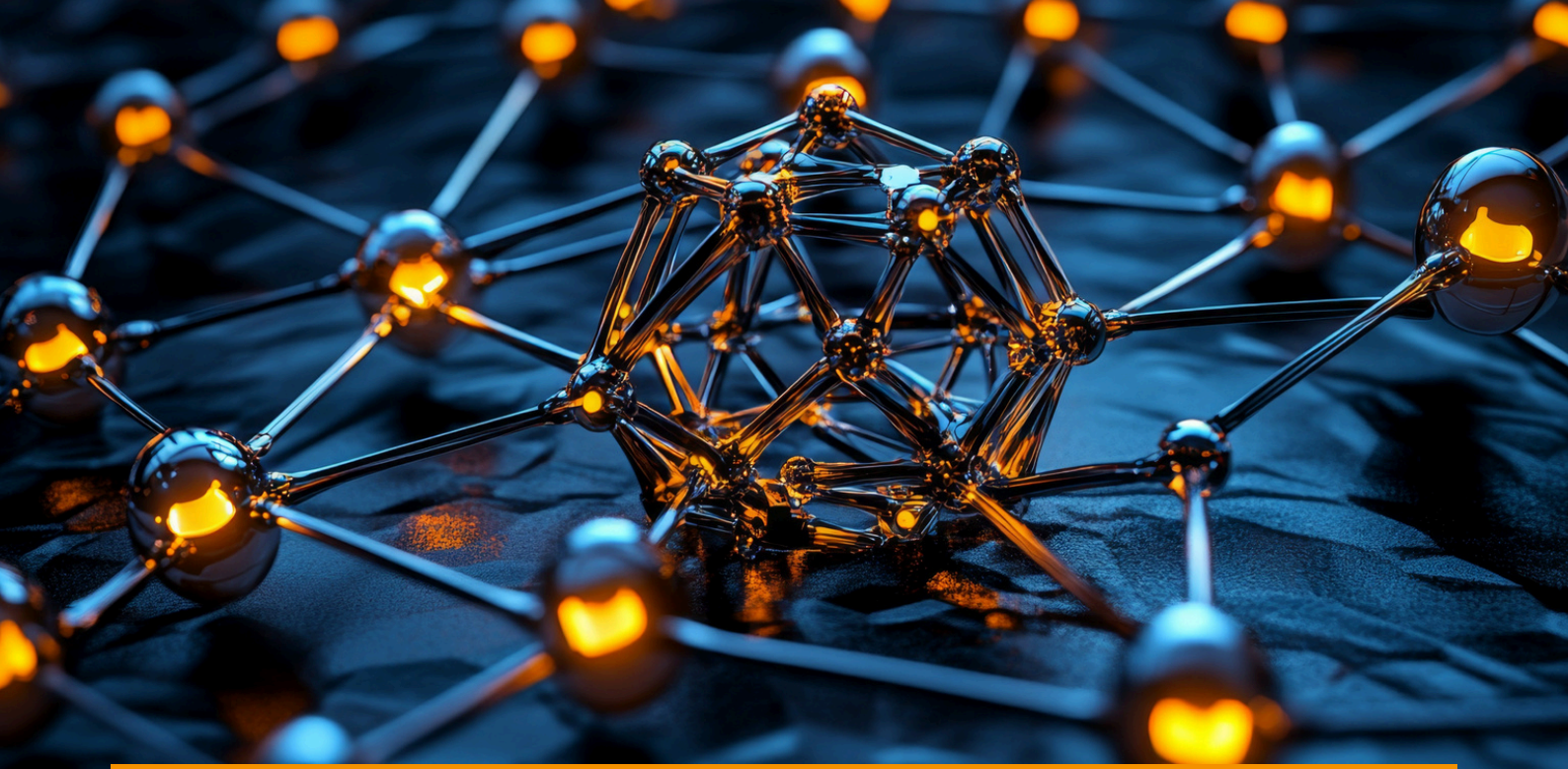
According to Palo Alto Networks Unit42 security researchers, a 101% increase of macOS infostealers was recorded in the last two quarters of 2024, with three mainly predominant infostealer strains: Atomic, Poseidon and Cthulh. This situation has been observed in Switzerland as well, and our monitoring has detected instances of these common macOS infostealer strains among our customer base. In this article, we will recap the observed active deployment and escalating threat posed by macOS infostealers with regards to the recent Swiss cyber threat landscape, in particular for Atomic and Poseidon infostealers.

101%

increase of macOS infostealers

Switzerland

is observing the same trend, with an increase in macOS infostealer activity



Infostealers: What are infostealers?

As the term implies, infostealers are malware types meant to harvest and exfiltrate various data types, including login credentials (passwords, session cookies, 2FA tokens, etc.), personally identifiable information (such as social security numbers and addresses) and other relevant sensitive data such as financial information.

Infostealers are typically spread through different attack vectors, often relying on social engineering techniques to trick users into inadvertently installing them. Some common distribution methods include phishing emails with malicious URLs or attachments, malicious websites to download infected software, malvertising (malicious advertisements that lead users to download malware or visit compromised webpages).

Infostealers represent low hanging fruits, since they can be purchased under the malware-as-a-service (MaaS) model, making them accessible even to individuals with limited technical skills and for a low price. The stolen data typically feeds into an underground criminal economy, with platforms like Telegram serving as markets for harvested credentials. Infostealers are not only the cause of data leaks, but can also set the foothold or provide initial access for future attacks.

baseVISION

Case Study: AMOS (Atomic macOS Stealer) & Poseidon in Switzerland

Concerning trends involving the Atomic macOS Stealer (AMOS) have been observed at the global scale in 2024, and Switzerland is no exception. AMOS is considered the origin of the most prolific macOS infostealer families, whose paternity has been attributed to the unknown threat actor Ping3r, with its first appearance in the hacking scene dating back to April 2023. Initially born as a single offering, AMOS has evolved in different versions, which have disrupted multiple organizations across sectors in 2024.

AMOS propagates with different strategies. For example, our security analysts have observed its diffusion through applications which deceive users to be legitimate. Once those applications are installed, malicious AppleScripts start running to gather and exfiltrate extensive sensitive data. These AppleScripst perform a variety of system-level operations targeting various files, aiming at a thorough data collection from a macOS system for data exfiltration purposes: macOS Keychain data and notes; browser data (cookies, web data and login data), system information and crypto wallets, followed by POST requests to an IP address historically used as a C2 for Aurora Stealer (while now detected as AMOS Stealer). The infostealer tried, for instance to interact with the SQLite database used by Edge to store cookies, attempting to access the file at /Users/$USER$/Library/Application Support/Microsoft Edge /Default/Cookies.

One variant of this malware is the Poseidon infostealer, an AMOS' fork attributed to the threat actor known as "Rodrigo4" At the end of June 2024, cybercriminals launched a large-scale email campaign to distribute Poseidon in the German-speaking region of Switzerland. According to reports from NCSC Switzerland, the attackers lured victims with AGOV (Switzerland's public service login system), redirecting them to a compromised website and prompting to download a malicious application called "AGOV Desktop Access." After downloading and extracting the malicious DMG files, an AppleScript would run to collect sensitive information such as host details, cryptocurrency wallets, credentials, private keys, cookies and VPN configurations. It would then compress the collected data into a zip file and send it to the attacker's command-and-control (C2) server via HTTP, with no further persistence mechanisms observed.

baseVISION

Indicators of Compromise (IOCs)

Here below, you can find an extract of the IoCs tracked for AMOS, as per the latest data provided by SOC Radar. We at baseVISION can help you detect and respond to malicious infostealer activities by leveraging advanced threat intelligence, continuous monitoring and detection tools to identify early signs of compromise with real-time threat analysis. We can also assist with post-infection remediation, to assess the risks of compromise and to ensure that every system is restored to a secure state.

Indicator	Data
HASH	2915b3f8b703eb744fc54c81f4a9c67f
HASH	e6d06bb9afaeb8aa80e62e76a26c7cffd14497f6
HASH	a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91
HASH	7d0e76c7682d33d36225620d3c82e4ddc0f6744baf387a0ea8124f968c18599
Hostname	ndas8m92[.]shop
Hostname	ndm2398asdlw[.]shop
Hostname	Smolcatkgi[.]shop
IP	152.89.198[.]96