flare

ADFS, Ransomware, and Identity: The New Frontier for Cybersecurity

Cybercriminals are opportunists. In most cases ransomware groups and threat actors aren't targeting specific industries or sectors, but instead are following the path of least resistance in an effort to maximize their profitability. Infostealer logs represent perhaps the clearest and easiest of those paths today for threat actors to gain access to corporate systems.

Infostealer malware is specialized malicious software designed specifically to harvest sensitive credentials, personal information, and authentication data from infected systems. Once deployed, these threats silently monitor user activity, extract passwords from browsers and system memory, and exfiltrate the stolen information to command-and-control servers controlled by threat actors. The resulting "stealer log" contains all the user's session cookies, credentials, and many files from the computer. To date, over 100 million stealer logs have been distributed in the cybercrime ecosystem.

Infostealers and Active Directory Credentials

For the purpose of this short report, we wanted to look at the prevalence of credentials and session cookies specifically for Active Directory that have been traded in the infostealer ecosystem. Active Directory (AD) is Microsoft's directory service for Windows domain networks that centralizes network management. AD stores information about objects on the network such as users, computers, and security groups, and enables administrators to manage permissions and access to resources across the enterprise.

AD serves as the authentication and authorization system that validates user credentials and determines their access rights to network resources. When compromised, it can lead to attackers gaining full control over an organization's entire IT infrastructure since it manages identity and access control across the network.

For this reason, Active Directory compromise is often a key step in the ransomware attack chain. Active directory represents the "keys to the kingdom" for attackers, granting them the ability to move laterally across the network, escalate privileges, and ultimately deploy ransomware or exfiltrate sensitive data.

At a high level, the sheer degree of active directory credentials is astonishing. We reviewed Flare data and found **almost 3% of all infostealer logs had credentials to Active Directory**, encompassing access (and potentially session cookies) that would allow threat actors to log directly into Active Directory environments.

3%
of Stealer Logs contain Active Directory Credentials

1.9M+
logs contain ADFS Credentials

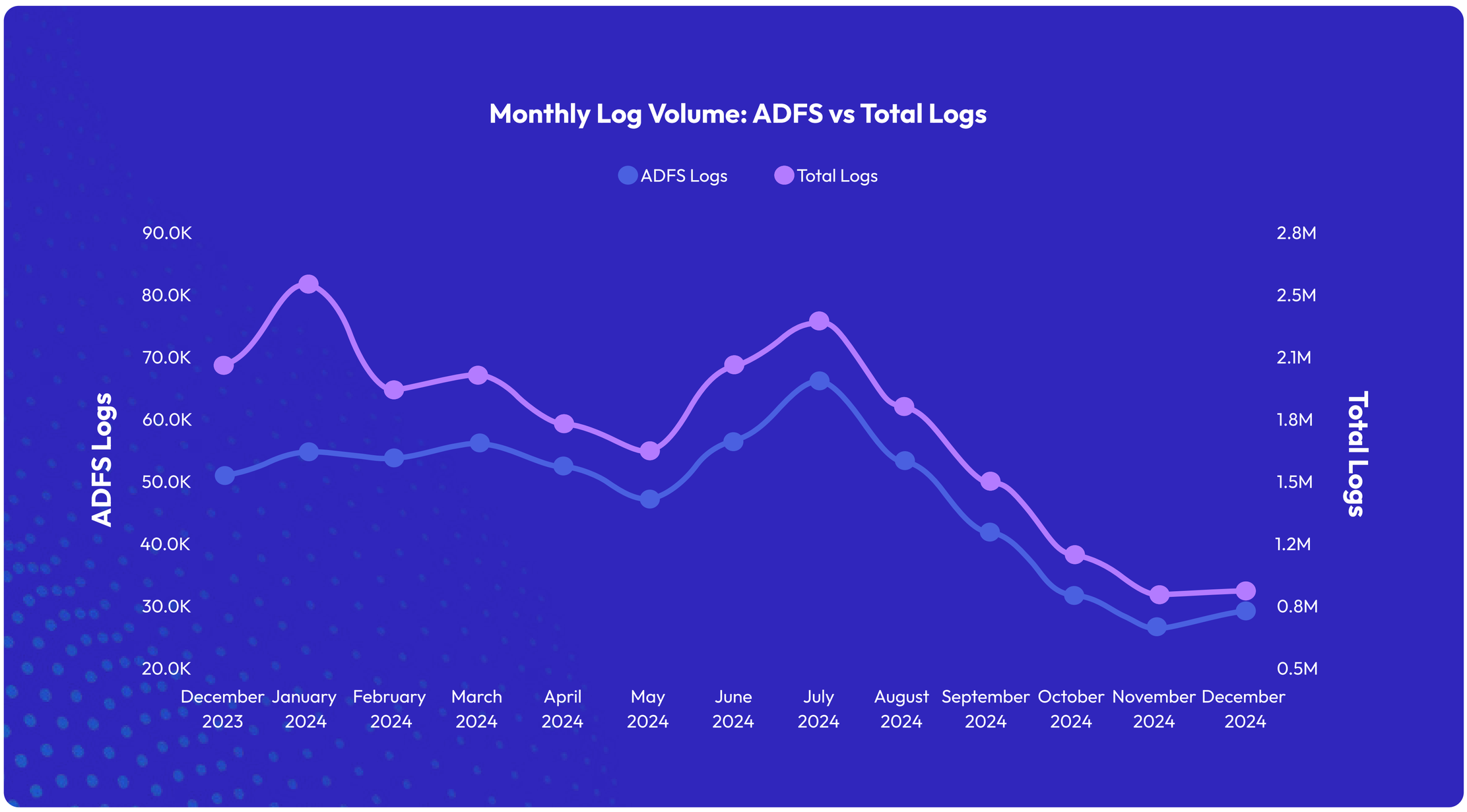
9,459
ADFS credentials entered the ecosystem in the past month

For Logs with ADFS

In 2024, Flare identified **569,892** stealer logs containing at least one ADFS access credential, roughly 2.75% of all logs from that year. **Over 13,000** unique organizations had their ADFS access credentials compromised in 2024. Alarmingly, nearly **4% of these ADFS logs also included credentials for another corporate SSO/identity provider like JumpCloud, Ping Identity, Verify.ibm, Okta Preview, or AWS Apps.** And over 80% of 2024 logs with Active Directory credentials contained other SSO credentials such as sso, SAML, or OAuth2, with almost half exhibiting two or more.

13,000
Unique Organizations Affected

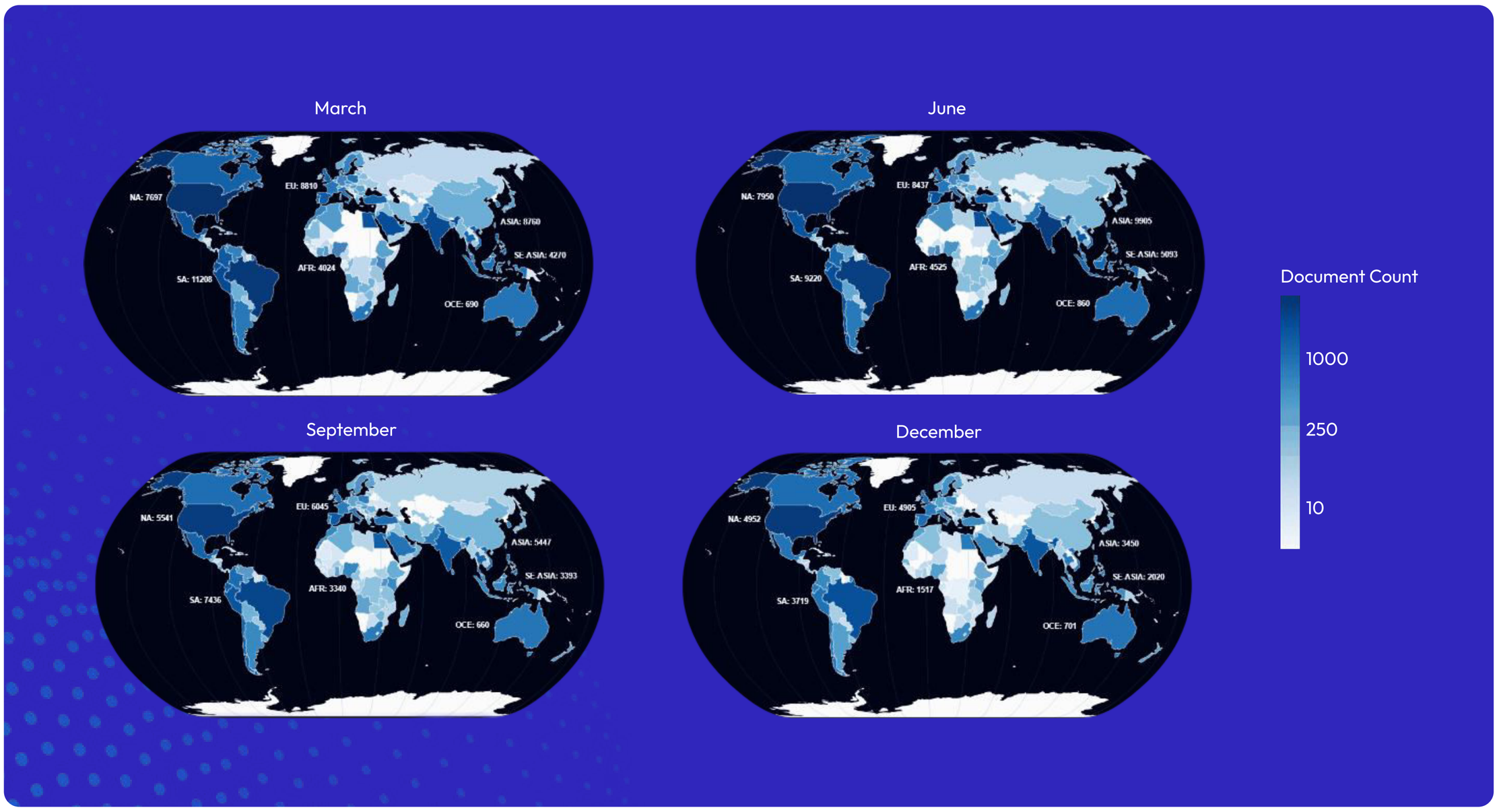
The ADFS log volume shows a clear pattern throughout the year: a steady rise during the first quarter, a slight dip in April-May, followed by a sharp increase starting in June that culminates in July's peak. After this peak, we observe a sharp decline beginning in August and continuing through the end of the year.



Our analysis comparing total log volume and ADFS log volume over a two-year period reveals a striking correlation. ADFS log dynamics appear primarily driven by overall log volume fluctuations, consistently representing approximately three percent of total logs (ranging from 2.15% in January 2024 to 3.26% in December 2024).

Regional examination shows Europe, North America, and Oceania closely mirror the overall trend with increased volumes from June through July before declining in August. Africa, South America, Asia, and Southeast Asia maintain more stable volumes without the dramatic summer increase. However, all regions show significant volume reduction during August-September.

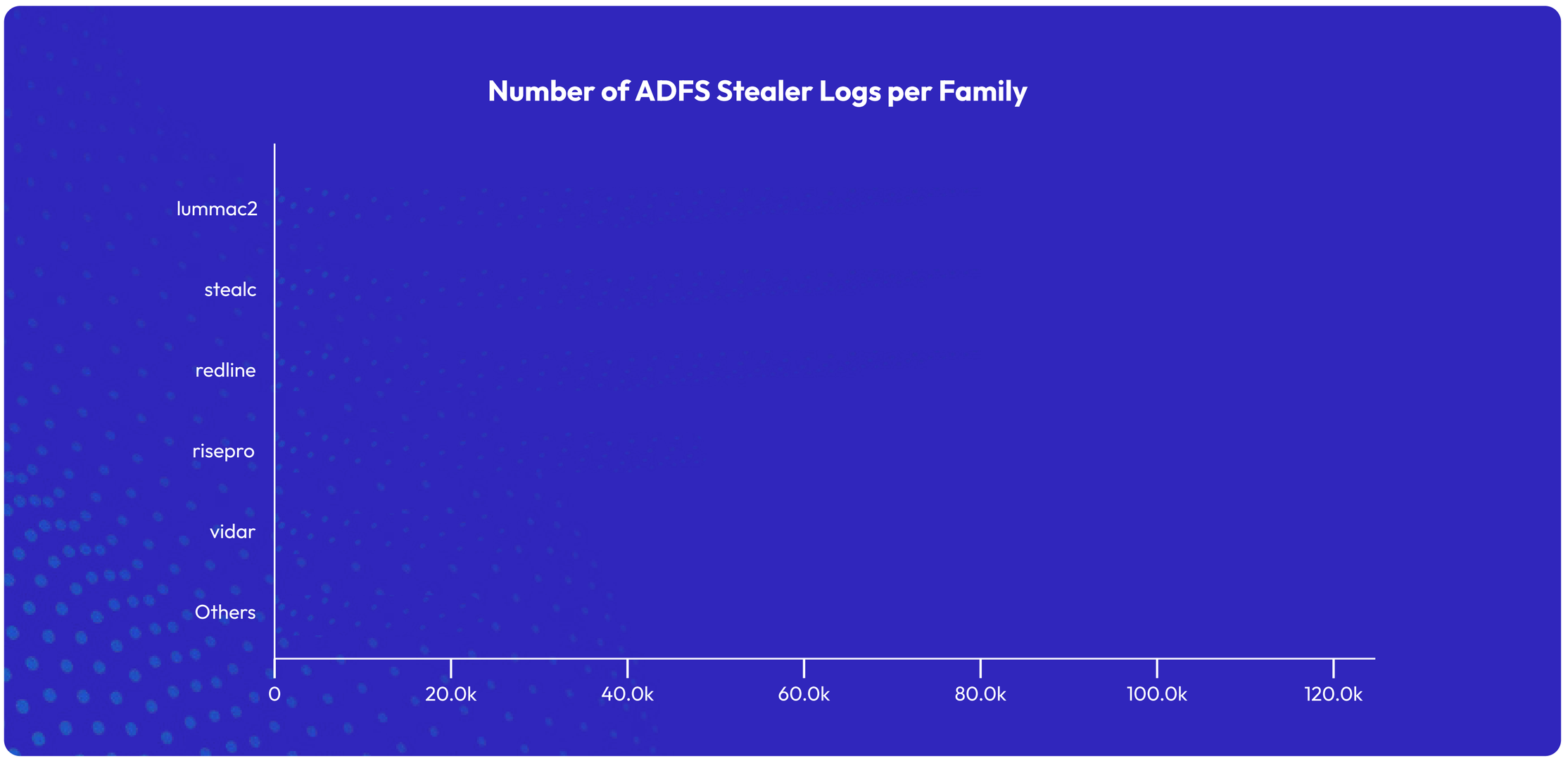
This suggests that while the summer spike in ADFS log volume seems to be primarily driven by Europe and North America, the subsequent worldwide decline appears to be influenced by broader factors. While the root cause for such variation remains under investigation, evidence indicates ADFS log volume changes primarily follow total log volume dynamics within this evolving ecosystem.



Additional contributing factors may include seasonal changes in device usage. Summer months typically see increased home computer access, both by children during school breaks and adults on vacation. Children often gain unsupervised access to devices that may have enterprise credentials, creating security vulnerabilities, as they are more likely to engage in high-risk online behaviors that could lead to malware infections or credential compromises. Additionally, adults may also access corporate environments through personal devices during vacation, inadvertently exposing systems to risks. The surge in May may be influenced by the end of the school year, when children's computer usage spikes, while the August decline aligns with the return to classrooms and structured schedules for adults. These explanations, however, remain hypothetical pending further investigation.

Infostealers Leading to ADFS Access

Three malware families **dominate** our 2024 ADFS logs: Lumma, StealC, and Redline collectively account for 82.5% of all recorded infections. While Lumma, StealC, and Redline dominate the threat landscape, our analysis also identifies significant activity from Risepro, Vidar, and Bradmax, all following remarkably similar seasonal patterns. Starting in July, we observe a universal decline affecting all malware families, though with varying trajectories.



Risepro drops almost completely below detection thresholds, while StealC, Redline, and Vidar show a more gradual reduction in volume over subsequent months. StealC emerges as the most prevalent threat vector, displaying both the most aggressive growth during peak summer months and the steepest subsequent decline.

The New Infostealer Reality

Most security teams have not caught up to the reality of massive-scale and broad based infostealer exposure. Most major companies today have significant infostealer exposure, and infostealers go beyond credential pairs. An infostealer contains an individual's entire life, often disclosing everything from what airlines they fly, what password combinations they use, and what they think are good secret questions.

A single ADFS credential disclosure is bad. A disclosure of almost everything about the identity of a key employee is far far worse. Companies need to rapidly adjust to the new reality that threat actors likely have enormous amounts of information on some employees, including board members and executives in addition to possible direct access to accounts. As organizational security increases, the attacks of the future will be driven by increasingly sophisticated Identity based attacks enabled by artefacts such as leaked credentials and stealer logs disclosing key information.

> The future is here - it's just not evenly distributed yet.
>
> - William Gibson

Gartner Peer Insights™ 4.9 ★★★★★

AICPA SOC 2 TYPE II Thoropass™

Sign Up for a Free Trial →

flare

flare.io hello@flare.io