Intelligence Insights: July 2025

By chris.brook@redcanary.com

Published: 2025-07-24 · Archived: 2026-04-06 00:25:59 UTC

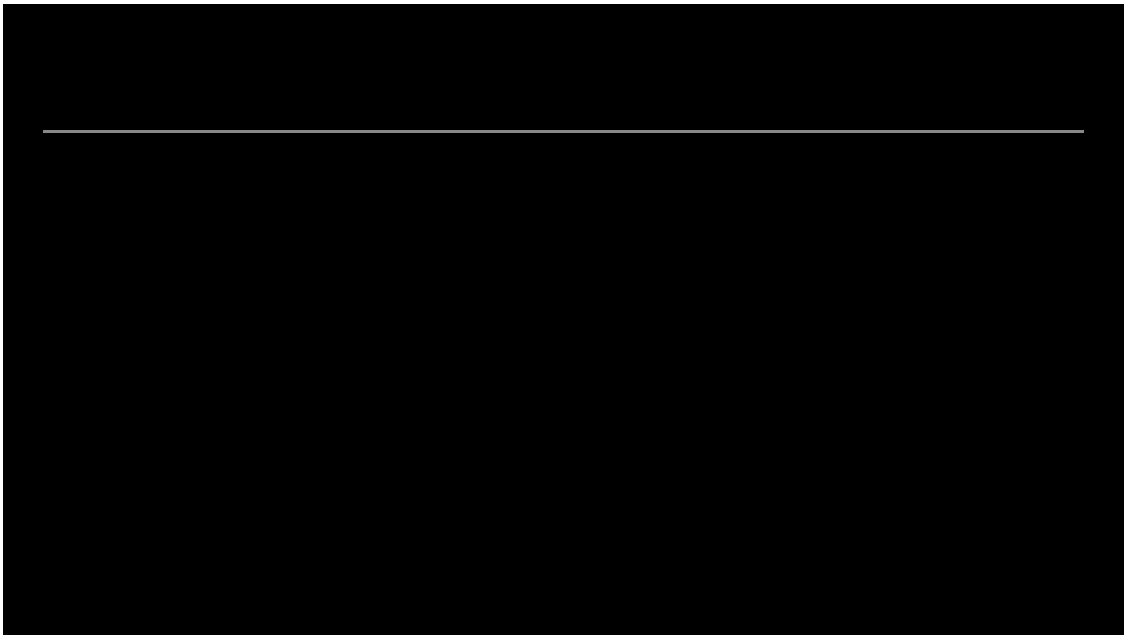
Intelligence Insights: July 2025

CleanUpLoader compromises, Poseidon Stealer debuts, and LummaC2 lives again in this month's edition of Intelligence Insights

July 24, 2025

Highlights from June

Amber Albatross kept its number 1 spot on our top 10 most prevalent threat list this month. Amber Albatross is Red Canary's name for a cluster of activity that starts from an adware program and leads to a pyInstaller EXE with stealer-like capabilities. This month it shares a tie with Mimikatz, a credential dumping tool often used by red teams—although after additional review, Mimikatz's increased detection volume appears to be due to unmarked testing and security researcher use.



Tying for third with SocGholish and making its debut in the top 10 is CleanUpLoader. Also known as Oyster/Broomstick, CleanUpLoader is a loader designed to maintain persistence and deliver additional threats. It has previously been leveraged by ransomware-linked actors, reportedly including adversaries that have deployed Rhysida ransomware. Red Canary and other researchers saw a significant uptick in CleanUpLoader activity early this June due to its use as a payload in malvertising campaigns. You can read more about this threat below.

Also making its debut on our top 10 list, tying for eighth place, is Poseidon Stealer. Poseidon, an information stealer, targets macOS systems to obtain sensitive data from browsers, extensions, and other applications using AppleScript code. It's a member of the macOS stealer family that shares similarities with Atomic Stealer (aka AMOS) both in its codebase and functionality. We began tracking the activity as Poseidon at the beginning of June 2025.

Our research is ongoing, and it may be that after additional assessment, some of the activity we tracked as Poseidon will be better tracked as Odyssey retroactively due to Poseidon's recent sale and rebrand. Numerous versions and frequent rebranding make differentiating between variations in the malware family challenging for defenders. That said, the similarities also lend to similar detection analytics working across variations on the theme. Based on our observations and third-party reporting, the recent uptick in activity is driven by an increase in the use of the macOS version of paste and run for initial access and execution.

Absent from last month's list, LummaC2 reappeared on the top 10 list as another tie for eighth. Our observations indicate some LummaC2 infrastructure remains functional after the takedown earlier this year, and other researchers have seen continued low-level use of LummaC2 since late May 2025. As has been the case after other high-profile takedowns, some return of a threat at a lower volume is not atypical, and this appears to be the case for LummaC2 as well.

This month's top 10 threats

To track pervasiveness over time, we identify the number of unique customer environments in which we observed a given threat and compare it to what we've seen in previous months.

Here's how the numbers shook out for June 2025:

Month's rank	Threat name	Threat description
Month's rank: ➡ 1*	Threat name: Amber Albatross	Threat description : Red Canary-named cluster of activity that starts from an adware program and progresses through several stages to a pyInstaller EXE with stealer capabilities
Month's rank: ⬆ 1*	Threat name: Mimikatz	Threat description : Open source tool that dumps credentials using various techniques
Month's rank: ⬆ 3*	Threat name: CleanUpLoader	Threat description : A loader designed to maintain persistence and deliver additional threats

Month's rank	Threat name	Threat description
Month's rank: ⬆ 3*	Threat name: SocGholish	Threat description : Dropper/downloader that uses compromised WordPress sites to redirect users to adversary infrastructure posing as necessary browser updates to trick users into running malicious code
Month's rank: ⬆ 5*	Threat name: Charcoal Stork	Threat description : Suspected pay-per-install (PPI) provider that uses malvertising to deliver installers, often disguised as cracked games, fonts, or desktop wallpaper
Month's rank: ⬆ 5*	Threat name: Metasploit Framework	Threat description : Penetration testing framework used to probe systematic vulnerabilities on networks and servers to conduct post-exploitation activity on compromised hosts
Month's rank: ⬇ 5*	Threat name: Scarlet Goldfinch	Threat description : Activity cluster that uses a distribution scheme similar to SocGholish and uses JScript files to drop NetSupport Manager onto victim systems
Month's rank: ⬇ 8*	Threat name: Conficker	Threat description : Ancient NetBIOS and USB worm that has plagued the internet since 2008. What is dead may never die.
Month's rank: ⬆ 8*	Threat name: Impacket	Threat description : Collection of Python classes to construct/manipulate network protocols
Month's rank: ⬆ 8*	Threat name: LummaC2	Threat description : Information stealer sold on underground forums and used by a variety of adversaries; may also be used as a loader for additional payloads

Month's rank	Threat name	Threat description
Month's rank: ⬇ 8*	Threat name: NetSupport Manager	Threat description : Legitimate remote access tool (RAT) that can be used as a trojan by adversaries to remotely control victim endpoints for unauthorized access
Month's rank: ⬆ 8*	Threat name: Poseidon Stealer	Threat description : Stealer targeting macOS systems to obtain sensitive data from browsers, extensions, and other applications using AppleScript code
Month's rank: ⬇ 8*	Threat name: Tangerine Turkey	Threat description : Red Canary's name for a VBS worm that is delivered via an infected USB and uses a printui DLL hijack to deliver a cryptomining payload

⬆ = trending up from previous month
⬇= trending down from previous month
➡ = no change in rank from previous month

*Denotes a tie

CleanUpLoader makes a mess with malvertising

CleanUpLoader (aka Oyster/Broomstick) is a loader designed to maintain persistence and deliver additional threats. It made its first appearance in our top 10 this month due to a major malvertising campaign in June 2025. It's previously been leveraged by adversaries that went on to deploy Rhysida ransomware, which makes it important to detect and remediate as early as possible. This is not the first time CleanUpLoader has been distributed in widespread malvertising and search engine optimization (SEO) poisoning operations; a similar campaign in June 2024 used malicious ads for fake downloads of Microsoft Teams and Google Chrome.

The activity we observed in June 2025 was primarily due to users attempting to download PuTTY or WinSCP, legitimate and widely used Windows tools for secure remote access and file transfer. By targeting IT personnel, the adversaries could possibly have higher privileges if they were to gain access to an endpoint via this campaign. After searching for the legitimate software, users are tricked into clicking on an SEO-optimized advertisement or typo-squatted link that leads to a copied version of the legitimate website.

Screenshots from Arctic Wolf

One example we observed directed users to this malicious site at `putty[.]run`, a copy of `putty[.]org`.

putty[.]org above, putty[.]run below

The malicious website feeds users an executable with a name like `putty.exe`, masquerading as the requested software, then unpacks and executes CleanUpLoader malware. It's typically distributed as DLL files that are executed using `rundll32.exe`, and when executed, leads to a number of behaviors including:

- establishing persistence via scheduled task, for example: `schtasks.exe /Create /SC MINUTE /MO 3 /TN "Security Updater" /TR "C:\windows\System32\rundll32.exe C:\users[redacted]\AppData\Roaming\HQXYOCnhJRyac\twain_96.dll DllRegisterServer"`
- system and domain reconnaissance commands
- outbound netconns, often by `rundll32.exe`, to external C2 infrastructure

Recent CleanUpLoader campaign at-a-glance

Fortunately for defenders, this behavior has not changed significantly, meaning prior detection analytics for CleanUpLoader should still be effective. One example is CleanUpLoader's use of `rundll32.exe` in the scheduled task it creates, which gives us a detection opportunity.

Detection opportunity: Scheduled tasks that use `rundll32.exe`

The following pseudo-detection analytic identifies scheduled tasks using `rundll32.exe`. Adversaries, like those behind CleanUpLoader, abuse Rundll32 because it can make it hard to differentiate malicious activity from normal operations. Scheduled tasks do not normally use `rundll32.exe`.

```
 process ==  (schtasks)
&&
command_includes ('/create' || 'rundll32')
```
