

# Operation Endgame Quakes Rhadamanthys

**p** [proofpoint.com/us/blog/threat-insight/operation-endgame-quakes-rhadamanthys](https://proofpoint.com/us/blog/threat-insight/operation-endgame-quakes-rhadamanthys)

November 12, 2025

[Blog](#)

[Threat Insight](#)

Operation Endgame Quakes Rhadamanthys



The Proofpoint Threat Research Team

## Key takeaways

- Rhadamanthys is a prominent malware observed since 2022, used by multiple cybercriminal threat actors.
- The malware has been observed delivered via email, web injects, and malvertising campaigns.
- It is a modular information stealer with multiple pricing plans, and the creators sell it alongside Elysium Proxy Bot and a Crypt Service.
- International [law enforcement disrupted](#) Rhadamanthys and affiliates' infrastructure as part of ongoing Operation Endgame efforts.

## Overview

Rhadamanthys malware has evolved significantly over time, reflecting ongoing advancements in cybercriminal techniques. First observed in 2022, Rhadamanthys emerged as a sophisticated information stealer, primarily targeting sensitive user data such as login credentials, financial

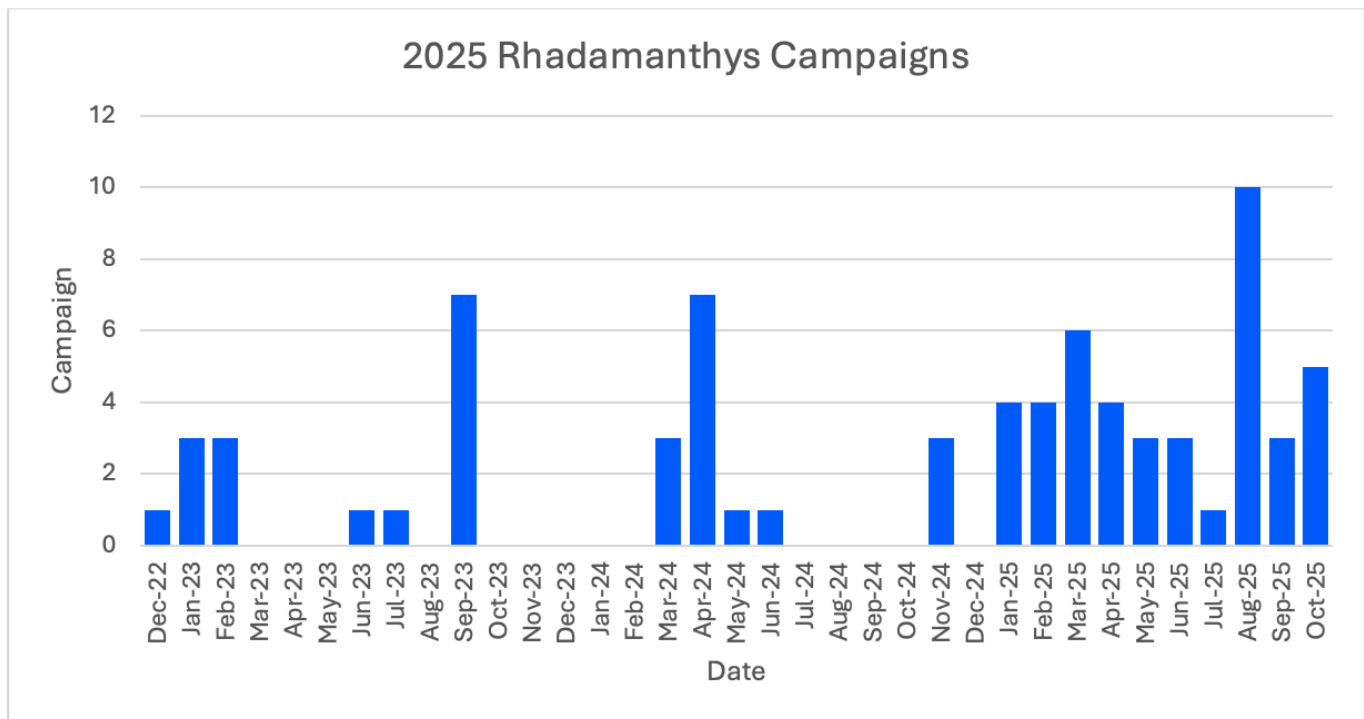
information, and system details. It quickly gained popularity on underground forums, where its capabilities and ease of customization attracted various cybercriminals.

Throughout its development, Rhadamanthys updates include new features, improving its evasion tactics and adaptability. Updates often allow it to avoid detection by security and detection controls more effectively, often through techniques involving obfuscation and anti-analysis. The malware authors introduced multi-stage payloads, which enabled the malware to bypass security layers by spreading across stages in discrete steps. Additionally, it became more modular, allowing threat actors to tailor capabilities to specific attacks or targets.

The operators sell access to Rhadamanthys for between \$300 to \$500 a month, with options for a higher price point for customized uses. Notably, some cybercriminal forums banned the sale of Rhadamanthys because it allowed the targeting of Russian and Commonwealth of Independent States countries.

Proofpoint observes Rhadamanthys delivered via email campaigns conducted by multiple threat actors. Techniques for payload delivery include leveraging the ClickFix social engineering technique, pairing URLs and aggressive filtering with instructions that advise people to copy, paste, and run PowerShell scripts to infect themselves with malware. Threat actors including TA585, TA2541, TA547, TA571, TA866, and numerous unattributed threat clusters have used Rhadamanthys in campaigns.

Proofpoint observed more Rhadamanthys campaigns so far in 2025 than previous years, in part due to more threat actors leveraging compromised websites to deliver malware, including Rhadamanthys. (Analyst note: it is possible there was additional low-volume activity observed in email threat data that was not campaigned by threat researchers.)



**Figure 1.** Timeline of Rhadamanthys campaigns.

## Operation Endgame

On 13 November 2025, law enforcement disrupted Rhadamanthys’s infrastructure – specifically taking down multiple servers associated with the management and operation of the malware – as well as infrastructure associated with affiliates using the malware. This disruption was part of [Operation Endgame](#), a collaboration between global law enforcement and private sector partners. Additional services like Elysium Proxy Bot were also affected. Notably, law enforcement also posted a video on the [operation’s main website](#) that suggested that the threat actor behind Rhadamanthys was not only facilitating information stealer operations but also stealing sensitive data from Rhadamanthys affiliates. In addition to the infrastructure disruption, it’s likely that this operation will also negatively affect the criminals’ reputation, leading affiliates to mistrust them.

Operation Endgame is a widespread effort conducted by global law enforcement and private sector partners, including Proofpoint, to disrupt malware and botnet infrastructure and identify the alleged individuals associated with the activity. In May 2024, the first Operation Endgame disruption effort targeted multiple malware families including IcedID, Bumblebee, SystemBC, Pikabot, SmokeLoader, and more, and [Europol called it](#) the “largest ever operation against botnets, which play a major role in the deployment of ransomware.” The second major Operation Endgame action occurred in May 2025 and targeted additional malware families and their creators, including [DanaBot](#), WarmCookie, Trickbot, and Hijack Loader. The major malware-as-a-service Lumma Stealer has also been [targeted by law enforcement](#).

Operation Endgame disruptions have significantly affected the overall email threat landscape, specifically disrupting activity attributed to known initial access broker (IAB) payloads and supporting malware families delivered via email-based campaigns. For example, in March 2023, 17% of email-based malware campaigns in Proofpoint data were associated with malware targeted by Operation Endgame, while that number had dropped to 1% by September 2025.

## History

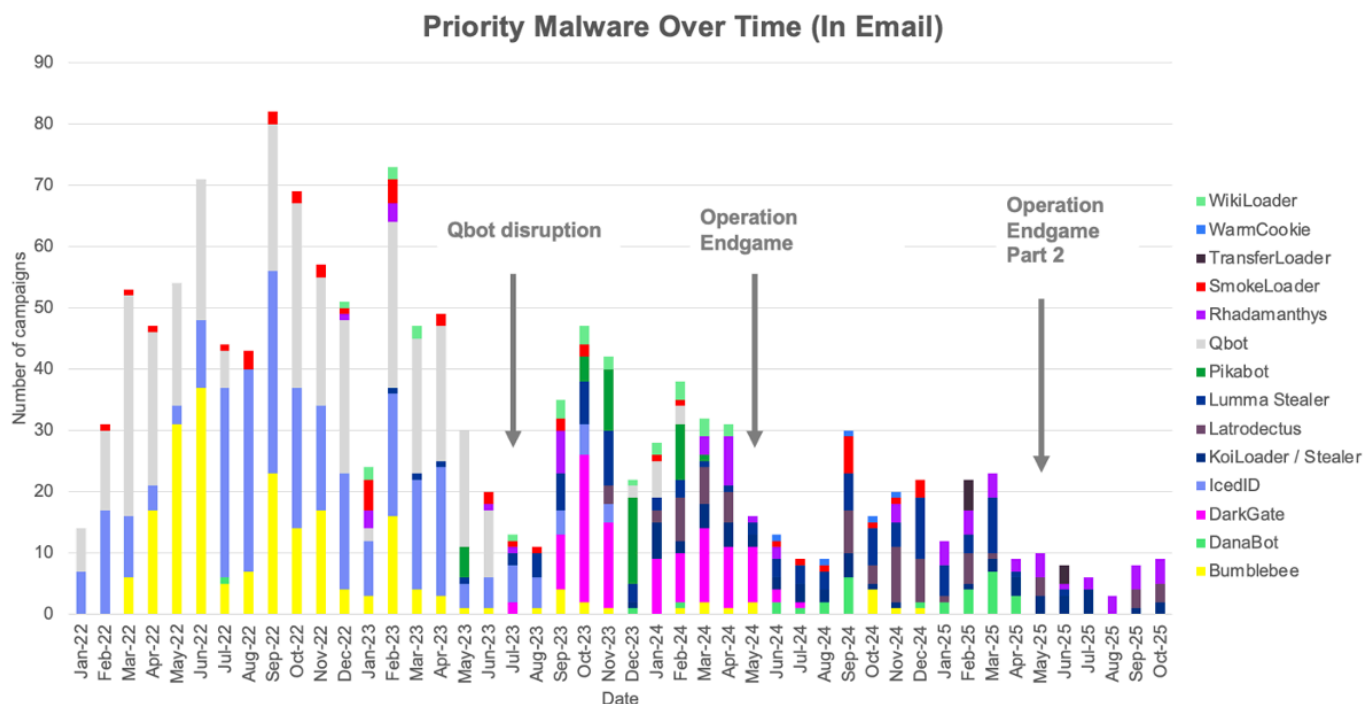
---

When Rhadamanthys first emerged in 2022, it was a commercially marketed information-stealer sold via underground forums by the alias “kingcrete2022”. It swiftly evolved from a simple malware to a modular Malware-as-a-Service (MaaS) offering as developers added plugins and staged loader architecture to make analysis and detection harder. Early development ascended into a cadence of rapid releases.

By 2024, the malware was shipped with a notable update that added AI-driven OCR capabilities to automatically identify and extract cryptocurrency seed phrases from images. This version included new evasion and encryption upgrades. The operator also offered new conveniences for customers that reflected popular trends in the threat landscape, one of which was MSI installer execution to assist in bypassing security detections.

In late 2024 through 2025, researchers noted an increase in Rhadamanthys campaigns which leveraged the malware’s modularity to tailor to threat actors with different objectives and levels of sophistication. In 2025, the developers pushed a new 0.9.X series that hardened network and packing obfuscation, expanded device and browser fingerprinting, reintroduced PNG steganography for hiding payloads, and adopted marketing changes. These changes included tiered pricing updates, enhanced features, and rebranding. The rebranding was reflected in a modernized site emphasizing a more professional MaaS business model, rapid feature growth, more useful distribution and monetization techniques, and an ecosystem that makes Rhadamanthys a favored malware of choice.

The takedown and disruption of many prominent loaders and top tier malware by Operation Endgame primed the market for Rhadamanthys to rise. Evidence suggests the malware is maintained and improved by capable developers. New releases have correlated to current and coveted resources and landscape trends, delivered in a way that makes it easy to utilize for customers.



**Figure 2.** Priority malware in campaign data and the impact of Operation Endgame.

## Affiliations

As a MaaS, different affiliates may license the malware, attach custom plugins, and run campaigns independently. It is advertised on multiple forums, meaning it is not exclusive to a group of trusted affiliates but is instead available to a larger market. It is notable the creators developed the malware to be used by threat actors with varying expertise. As a result, Rhadamanthys has been observed in campaigns as simple as compressed executables attached to emails, and more sophisticated campaigns using distribution techniques like Google Ads, ClickFix, compromised websites, and priority threat actors' more targeted campaigns.

## Threat actors

Proofpoint first began tracking Rhadamanthys in December 2022 when it was distributed in a campaign attributed to priority cybercriminal threat actor [TA571](#) with post exploitation activities attributed to [TA866](#). TA571 has used both exclusive and more freely available malware, but TA866 has historically been observed using more exclusive and distinct malware. The actors' use of Rhadamanthys immediately designated it as a priority malware to tracked.

Proofpoint subsequently observed [TA2541](#), a capable actor classified on a lower tier who favors off-the-shelf RATs, use Rhadamanthys in February 2022. [TA547](#), a priority threat actor who has used sophisticated banking malware and loaders, leveraged Rhadamanthys throughout 2024. [TA585](#), a newly designated actor suspected of operating their entire attack chain through malware delivery, utilized Rhadamanthys frequently in 2025. In addition to the designated threat actors tracked by Proofpoint, the malware has been used in a large number of unattributed activity

clusters in Proofpoint data, including the threat actor tracked by third-parties as “[Aggah](#)”, and by other threat actors tracked externally in distributing malware via other mediums like malvertising or SEO poisoning.

Actors across the crimeware spectrum from low-level actors to sophisticated operators using Rhadamanthys consistently over time demonstrates the apparent success of the malware as a product, the malware’s evolution and evasion efforts, and the successful MaaS strategy employed by its operators.

## Malware

---

Threat actors may distribute Rhadamanthys as the sole malware payload, a companion malware delivered with others, or as a follow-on payload. In Proofpoint data, Rhadamanthys is frequently used in campaigns distributed by loaders. For example, we’ve seen the following drop Rhadamanthys as a follow-on payload:

- SystemBC
- DarkGate
- GuLoader
- SmartLoader
- Resident Backdoor
- DoubleLoader
- DOILoader / Hijack Loader
- Latrodectus
- CastleLoader
- Amadey

Proofpoint researchers have also observed Rhadamanthys delivered in campaigns as a companion to other malware, including:

- Remcos
- zgRAT
- Screenshotter / AHK Bot
- BitRAT
- XWorm
- Lumma
- XLoader

In these campaigns, Rhadamanthys is either delivered at the same time as other payloads, or is distributed to a limited target set within a broader campaign that drops multiple payloads to different recipients.

## Recent attack chains

---

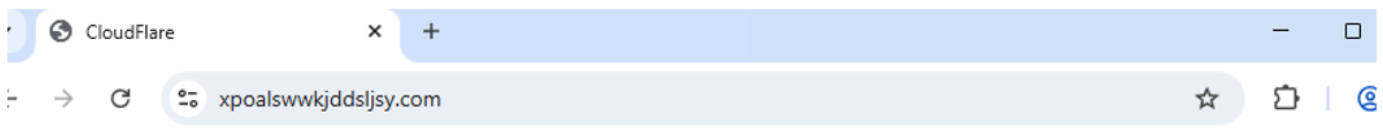
Rhadamanthys is currently distributed by multiple threat actors using many different attack chains to deliver malware. The following are a small sample of some of the most interesting campaigns Proofpoint researchers observed in recent months.

## Compromised websites

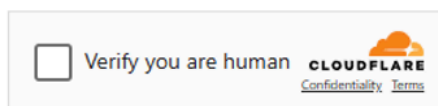
---

Multiple threat clusters use compromised websites to distribute Rhadamanthys. In email data, we observe these messages because they contain links to compromised websites. Although neither the sender nor the site owner may intend harm, the websites have been compromised with a malicious injection.

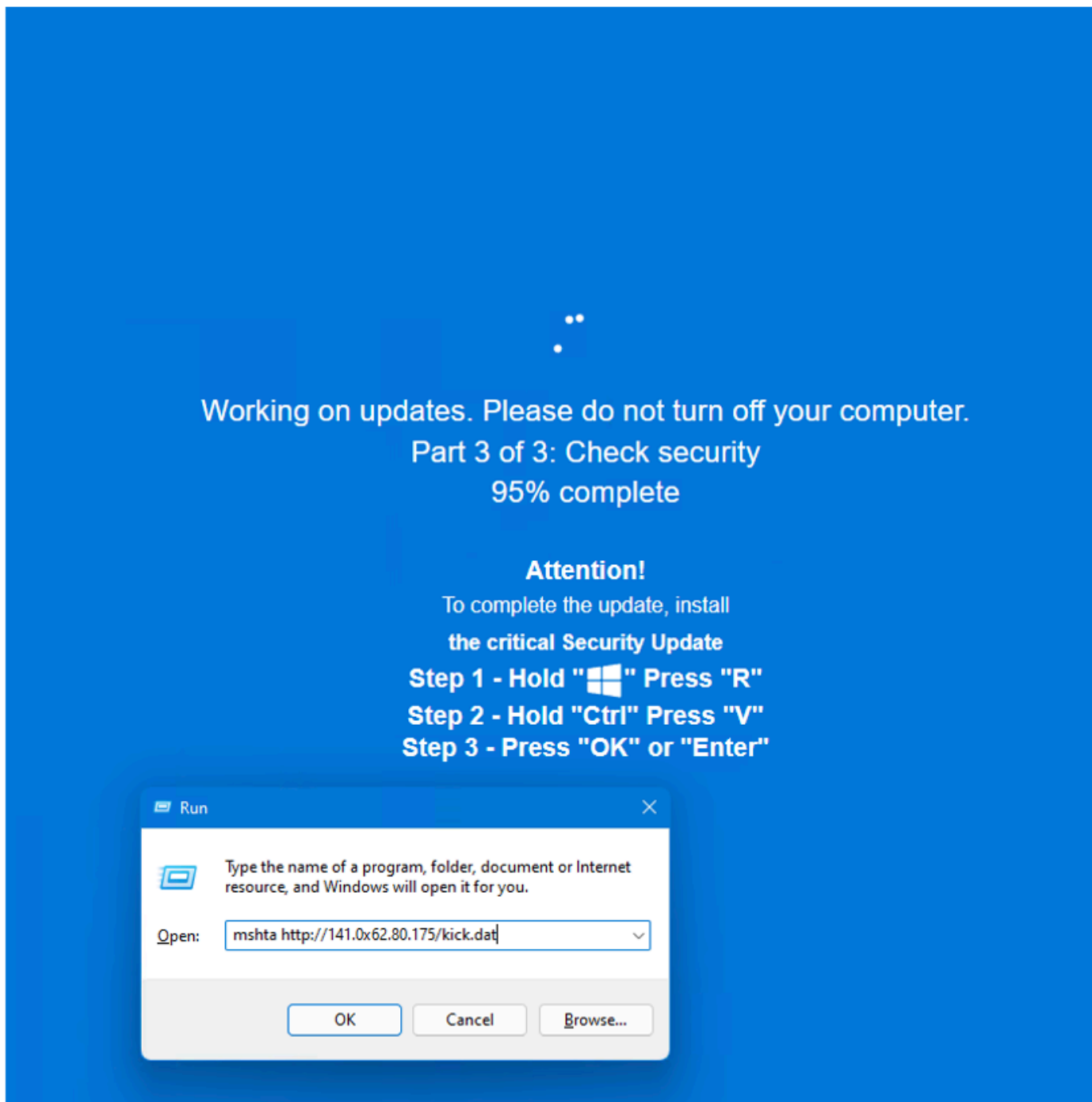
In a campaign observed in October 2025, the injection prompted the website to load a malicious script which was hosted on actor-operated infrastructure, which, in turn loaded a counterfeit Cloudflare turnstile. Upon validation the browser switched to full screen and display a fake security update lure.



Verify you are human by completing the action below.



**Figure 3.** Cloudflare verification.



**Figure 4.** Fake update ClickFix instructions.

This attack chain used a technique called "Clickfix" which instructs the user to copy and paste a malicious command in the run box. In this way, the attacker is essentially tricking the user to infect themselves with malware. Many web inject campaigns use this technique. In this case, if the command was run, it would lead to the installation of Rhadamanthys.



## URLs

Rhadamanthys payload delivery via URLs in emails is also common. For example, Proofpoint identified a campaign in October impersonating a logistics company. Messages contained URLs leading to a website instructing the recipient to sign a form and click “submit”. Then, the user would be redirected to a ClickFix landing page.


dpeforms

apps.englandlogistics.tenderloads.com/dpeformseN12foikjdw.html

Please fill out and submit

Note: Please fill out the highlighted fields on the document below, then click the submit button at the end

England LOGISTICS



Carrier Rate Confirmation

Page 1

FOR LOAD QUESTIONS

AFTER LOAD IS DELIVERED

Contact:

Order No: 12722586

Authorized Agent:

Please include order number in subject line of email

CARRIER

SG Transport BG Inc

Phone:

Date:

10/17/2025

DETAILS

Commodity:

Temp:

Cases/Pieces:

Cycle Type:

Trailer: F

Weight: 10.000

Pallets:

PU 1

St. Louis, Missouri

Date:

10/18/2025

UNTIL 8 PM

SO 2

Chicago, Illinois

Date:

10/22/2025

24/7 FCFS

Pick-up and delivery addresses, contact info and specific load information will be provided separately

PAYMENT

Carrier Freight Pay:

Load Tracking Tool Used

Total Carrier Pay:

\$1400

Please note: If paid by either piece count or weight, payment will be adjusted based on actuals.

Please Sign:

☐ Accept

☐ Decline

SUBMIT

Driver Name:

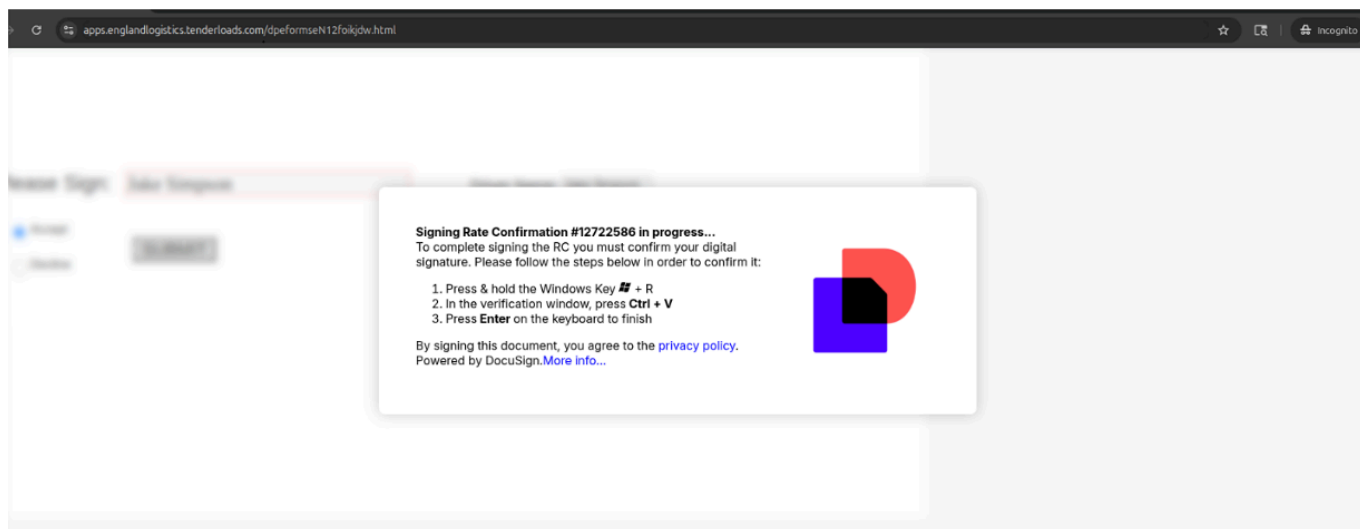
Driver Cell:

Driver Email:

Tractor #:

Trailer #:

Figure 5. Impersonated company landing page with a fake confirmation.



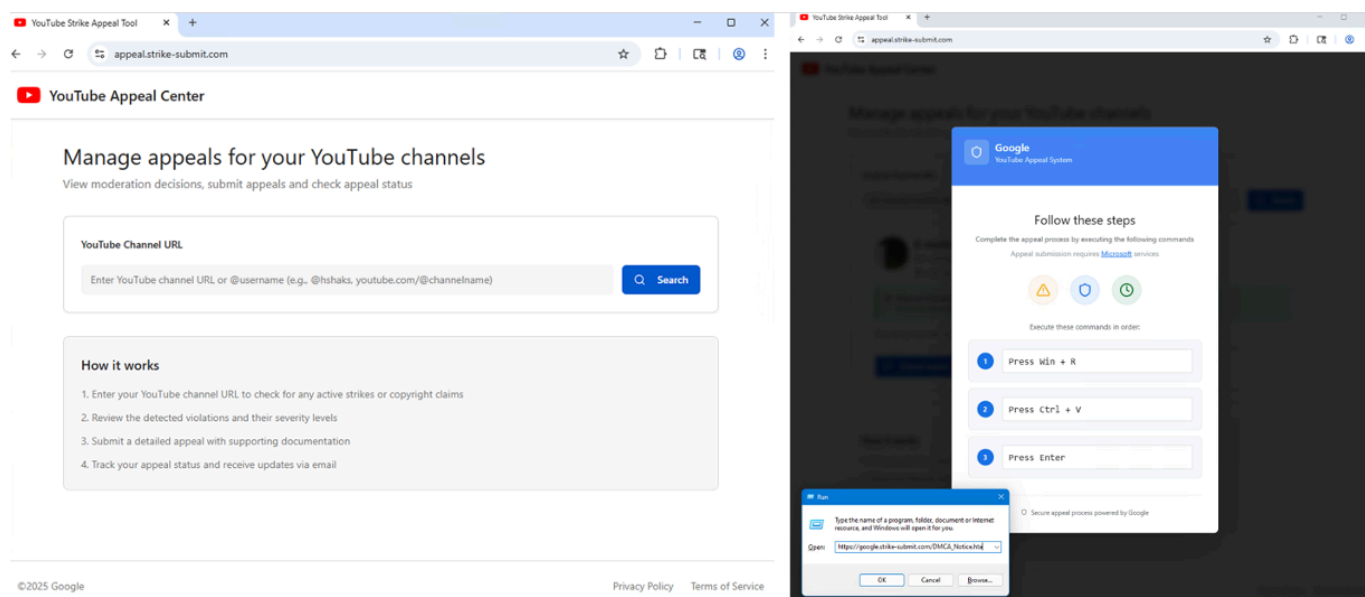
**Figure 6.** ClickFix instructions.

If the target completed the ClickFix steps as instructed, a command was initiated to download a tar archive and run CastleLoader. CastleLoader was observed loading DOILoader and Rhadamanthys. DOILoader was observed loading zgRAT.

This campaign aligns with an increase in threat actors [targeting the surface transportation industry](#) to deliver malware or remote monitoring and management (RMM) tools.

## PDFs

Another interesting campaign in August and September impersonated YouTube and targeted organizations in the entertainment and media industries. The messages contained a PDF with a link to a fake "Youtube DMCA" themed website built with [Lovable App](#) and used the ClickFix technique.



**Figure 7.** Fake YouTube “copyright appeal” website created by threat actors.

The app instructed recipients to enter their YouTube URL, retrieved real-time metadata for any submitted YouTube channel, and claimed that an appeal is needed. If the instructions were followed and the user copied and pasted the PowerShell script as directed, it executed an HTA script. The HTA enabled VBA macros via registry changes and built an Excel workbook via COM in-memory, opening it silently without user interaction. The workbook contained an AutoOpen macro, which the HTA constructed from split Base64 strings. This macro downloaded a .bin file containing shellcode and executed it via classic shellcode injection using VirtualAlloc + RtlMoveMemory + CreateThread into the Excel process to run Rhadamanthys in memory. While the macro included logic for both 32- and 64-bit Office, it only downloaded and ran 64-bit shellcode, so it crashed on 32-bit Excel.

The payload chain from HTA to shellcode execution was likely built with the commercial toolkit MacroPack Pro which is sold to red teams and "ethical hackers".

## Impact

---

In general, disruptions to cybercrime threat actors and their malware have ripple effects across the ecosystem. Threat actors who rely on Rhadamanthys will have to find a new malware for distribution and spend time and money retooling their attack chains. It is possible that threat actors may pivot to newer malware such as Amatera Stealer, Monster V2, or CastleRAT. But while there may be other options tooling-wise, disruptions also sow distrust among the criminal ecosystem, [and in some cases](#), lead to more restrictive policies and tighter controls about who can buy malware from certain brokers.

Proofpoint will continue to monitor where Rhadamanthys threat actors go next and continue defending against cybercriminal threats.

## Conclusion

---

As law enforcement disruptions continue to alter threat actors' behavior, it's important to be aware of emerging trends and behaviors from prominent cybercriminal threat actors, such as the use of [remote monitoring and management](#) software (RMMs), increase in use of [information stealers](#), and [new social engineering techniques](#) that target people not technology. By understanding the landscape, organizations can implement defenses against emerging trends and anticipate what decisions threat actors will make to stay ahead of them.

Proofpoint's mission is to provide the best human-centric protection for our customers against advanced threats. Whenever it is possible and appropriate to do so, and as is the case with Operation Endgame, Proofpoint uses its team's knowledge and skills to help protect a wider audience against widespread malware threats. Proofpoint was proud to assist in the law enforcement investigations into Rhadamanthys activity.

Through its unique vantage point, Proofpoint is able to identify the largest and most consequential malware distribution campaigns, providing the authorities with much-needed insight into the biggest threats to society, affecting the greatest number of people around the world.

Proofpoint Threat Research would like to thank Pim Trouerbach for his collaboration on investigations into Rhadamanthys and related malware.

## Emerging Threats signatures

---

<a href="#">2864521</a>	Rhadamanthys CnC Domain in DNS Lookup
<a href="#">2864523</a>	Observed Rhadamanthys CnC Domain in TLS SNI
<a href="#">2864294</a>	Observed Malicious SSL Cert (Rhadamanthys)
<a href="#">2862244</a>	Observed Malicious SSL Cert (Rhadamanthys)
<a href="#">2862245</a>	Observed Malicious SSL Cert (Rhadamanthys)
<a href="#">2054665</a>	Win32/Rhadamanthys CnC Activity (GET)
<a href="#">2854802</a>	Suspected Rhadamanthys Related SSL Cert
<a href="#">2043202</a>	Rhadamanthys Stealer - Payload Download Request
<a href="#">2853001</a>	Rhadamanthys Stealer - Payload Response
<a href="#">2853002</a>	Rhadamanthys Stealer - Data Exfil

## Example indicators of compromise

---

Indicator	Description

13f0bf908679bea560806fd3c14ef581b3cadbab2ff07a6adf04d97995924707	shielders.msi SHA256
b0c9d619256fdf220fbb39945fac5a040b5e836f1eae0459b4fcfb2b451420a7	DpiChrysler.exe SHA256
hxxps://84[.]200[.]80[.]8/gateway/53c06hop.fp0g1	Rhadamanthys C2
security[.]flacergurad[.]com	Actor-Controllec Intermediate Domain
security[.]flaegrudad[.]com	Actor-Controllec Intermediate Domain
security[.]flaezguerad[.]com	Actor-Controllec Intermediate Domain
security[.]flaezguered[.]com	Actor-Controllec Intermediate Domain
security[.]flavregurads[.]com	Actor-Controllec Intermediate Domain
security[.]flheregurend[.]com	Actor-Controllec Intermediate Domain
security[.]flqaergwaard[.]com	Actor-Controllec Intermediate Domain

security[.]flsaregursd[.]com	Actor-Controllec Intermediate Domain
security[.]gueradflwre[.]com	Actor-Controllec Intermediate Domain
theguardshield[.]com	Actor-Controllec Intermediate Domain
flheregurend[.]com	Actor-Controllec Intermediate Domain
flsaregursd[.]com	Actor-Controllec Intermediate Domain
flaezguerad[.]com	Actor-Controllec Intermediate Domain
flaezguered[.]com	Actor-Controllec Intermediate Domain
flcreagurade[.]com	Actor-Controllec Intermediate Domain
theguardshield[.]com	Actor-Controllec Intermediate Domain
flnaresgurard[.]com	Actor-Controllec Intermediate Domain

flaxergaurds[.]com	Actor-Controllec Intermediate Domain
cloudwardena[.]com	Actor-Controllec Intermediate Domain
flenieregurd[.]com	Actor-Controllec Intermediate Domain
Budparbanjarnegara[.]com	ClickFix Payload Domain
hxxps://google[.]strike-submit[.]com/DMCA_Notice.hta	Payload URL
hxxps://google[.]strike-submit[.]com/DMCA_Notice[.]hta	ClickFix Payload URL
hxxps://google[.]strike-submit[.]com/agreeses[.]bin	ClickFix Payload URL
bc2508708feb0ccc652494f8e28620bd871a8b6e1d26c7cdd61ab070f2594bbc	ClickFix Payload SHA256
ccdd8a6dc97eeba07e586f059eae7944dd767519f2c3b2233ff90d3dc4e8e3f0	ClickFix Payload SHA256
hxxps://85[.]192[.]61[.]140/gateway/h2u7sp2d[.]ab87a	Rhadamanthys C2

hxxps://policy[.]video	Optional Initial Redirecror in PDFs
hxxps://support-review[.]org/	Optional Initial Redirecror in PDFs
hxxps://appeal[.]strike-submit[.]com	ClickFix Landing Example
support-review[.]org	Actor-Controllec Domain
trust-review[.]org	Actor-Controllec Domain
compliance-review[.]org	Actor-Controllec Domain
channel-review[.]org	Actor-Controllec Domain
application-review[.]org	Actor-Controllec Domain
strike-submit[.]com	Actor-Controllec Domain
submit-appeal[.]com	Actor-Controllec Domain



policy[.]video	Actor-Controlled Domain
tdsworkout[.]com	Example Web Inject
103[.]136[.]68[.]61	Example Web Inject
cashorix[.]xyz	Web Inject Domain
xpoalswwwkjddsljsy[.]com	Filtered Landing Page
galaxyswapper[.]pro	Filtered Landing Page
193[.]24[.]211[.]233	Filtered Landing Page
hxxp://141[.]0x62[.]80[.]175/kick[.]dat	ClickFix Payload (HTA)
141[.]98[.]80[.]175	ClickFix Payload (HTA)
ff14b28408121ebe4a5d0c2f14b9dc99e987e89b56392dc214481197d4815456	ClickFix Payload (HTA) SHA256

http://xoiiasdpsdoasdpojas[.]com/	ClickFix Payload (PS1)
xoiiasdpsdoasdpojas[.]com	ClickFix HTA Payload (PS1)
141[.]98[.]80[.]175	ClickFix HTA Payload (PS1)
c9026ffc02f11204ac1eb1183376a5cee74f7897d948bdcd59c06f31de2671fa	ClickFix HTA Payload (PS1)  SHA256
193[.]221[.]200[.]93	Rhadamanthys C2

[Previous Blog Post](#)

[Next Blog Post](#)

**Subscribe to the Proofpoint Blog**