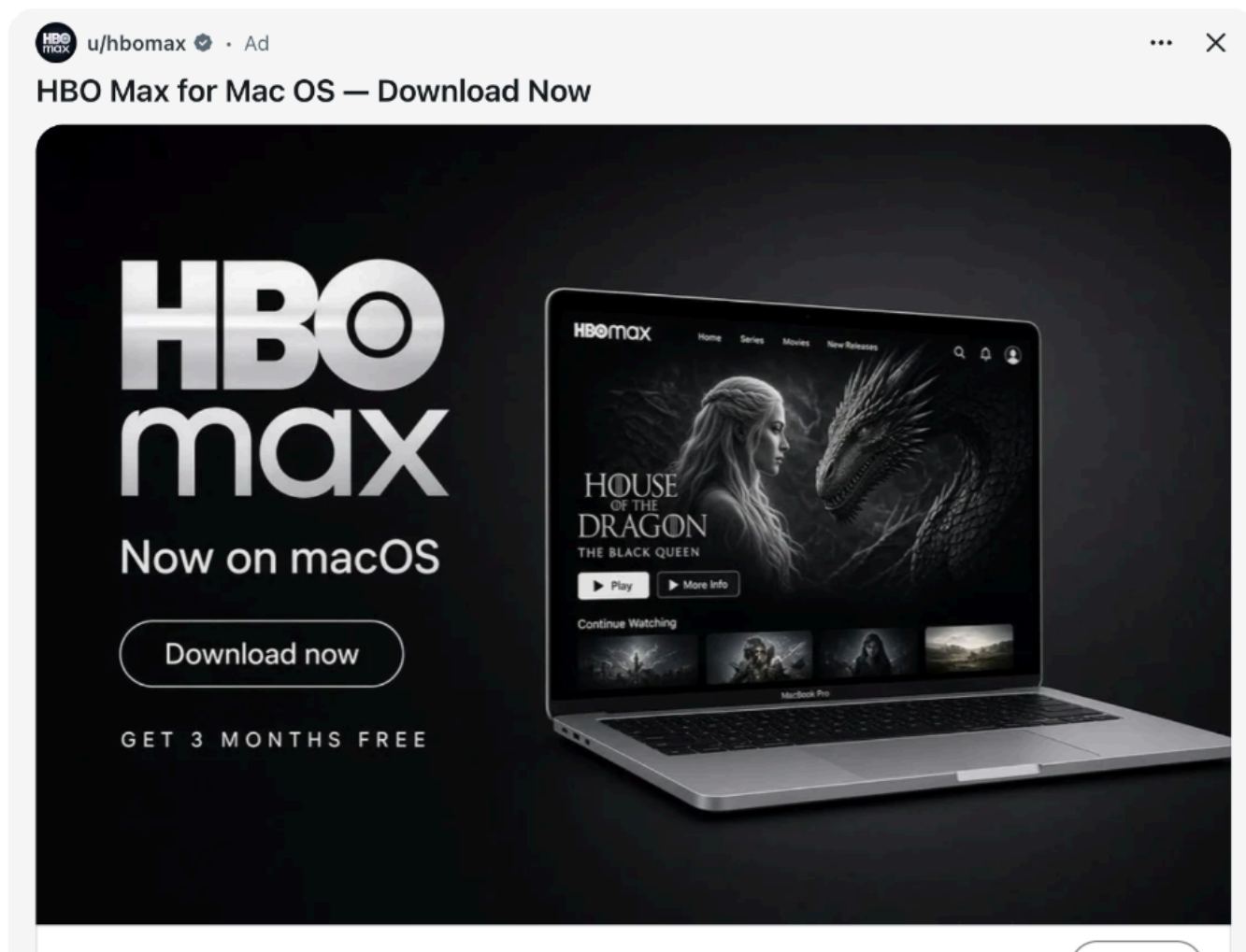


HBO Max ads on a compromised Reddit account exposed a massive PasteSwitch ClickFix operation

 hudsonrock.com/blog/hbo-max-ads-on-a-compromised-reddit-account-exposed-a-massive-pasteswitch-clickfix-operation

Hudson Rock

September 14, 2026



In September 2026, the cybersecurity community uncovered a massive, highly coordinated malvertising campaign leveraging the official, verified HBO Max Reddit account (u/hbomax).

Over a frantic 48-hour period, the compromised account pushed 108 distinct “ClickFix” advertisements to users across the platform.

Through joint research conducted by [Hudson Rock](#) and [Kirk from ADAMnetworks](#) (with additional thanks to Tuxxin from Whack.sh and Emiliano from The Matrix Project), we can confirm this incident is part of a massive, cross-platform delivery operation we are dubbing **PasteSwitch**. This operation spans macOS stealers, Windows loaders, deceptive TLS tactics, and contract-controlled cryptocurrency clippers.

Initial Discovery

The incident was brought to light by Alex Cutts in the r/cybersecurity subreddit. While browsing the platform, they encountered an official Reddit advertisement authored by the verified u/hbomax account. The ad aggressively promoted a native macOS application for HBO Max, a standalone application that does not currently exist.

Intrigued, the user followed the advertisement to a highly convincing landing page. Upon clicking the download button, the site did not initiate a standard file transfer. Instead, it triggered a classic “ClickFix” social engineering prompt, instructing the visitor to copy and paste a terminal command to install the software.



r/cybersecurity
u/Unhappy-Capital-1464 • 5d

Reddit Infostealer Adverts

Personal Support & Help!

I was browsing Reddit and saw an ad displaying u/hbomax as the author - this advertised a macOS HBO Max app which I'd not heard of and was interested in. The user is verified and appears to have posted many times in the official HBO Max subreddits.

The advert takes you to hbomaxx[.]us which looks somewhat legitimate, and has a join button / download. Clicking these opens up the classic infostealer/clickfix paste this command to download. Having checked, this downloads an executable with other capabilities for account compromise (obviously all done in a full sandbox - inspecting the output only, not running anything).

My guess is that the reddit account is compromised - I did consider some sort of character substitution in the username but clicking it took me to the profile - but I'm trying to think if there is any other explanation for this as I'd be very surprised for it to actually be a HBO Max issue.

I've reported to Reddit / HBO but just interested in any viewpoints (My role is cybersecurity adjacent but not a technical specialist)

Screenshots:

<https://files.catbox.moe/q0ee7d.png>
<https://files.catbox.moe/6nw1vc.png>
<https://files.catbox.moe/v1ycvm.png>

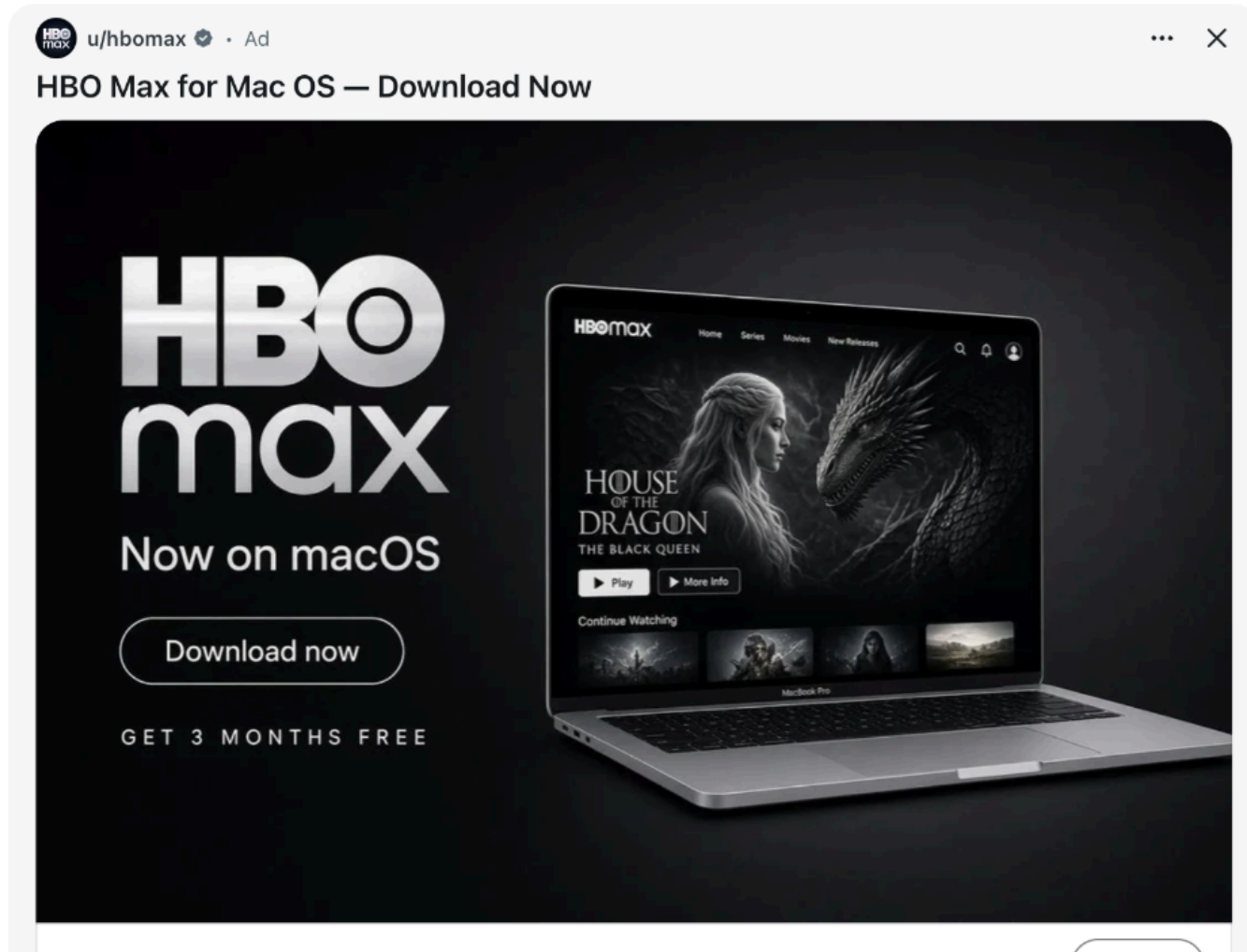


The initial report on r/cybersecurity detailing the suspicious official u/hbomax advertisement, first discovered by Alex Cutts.

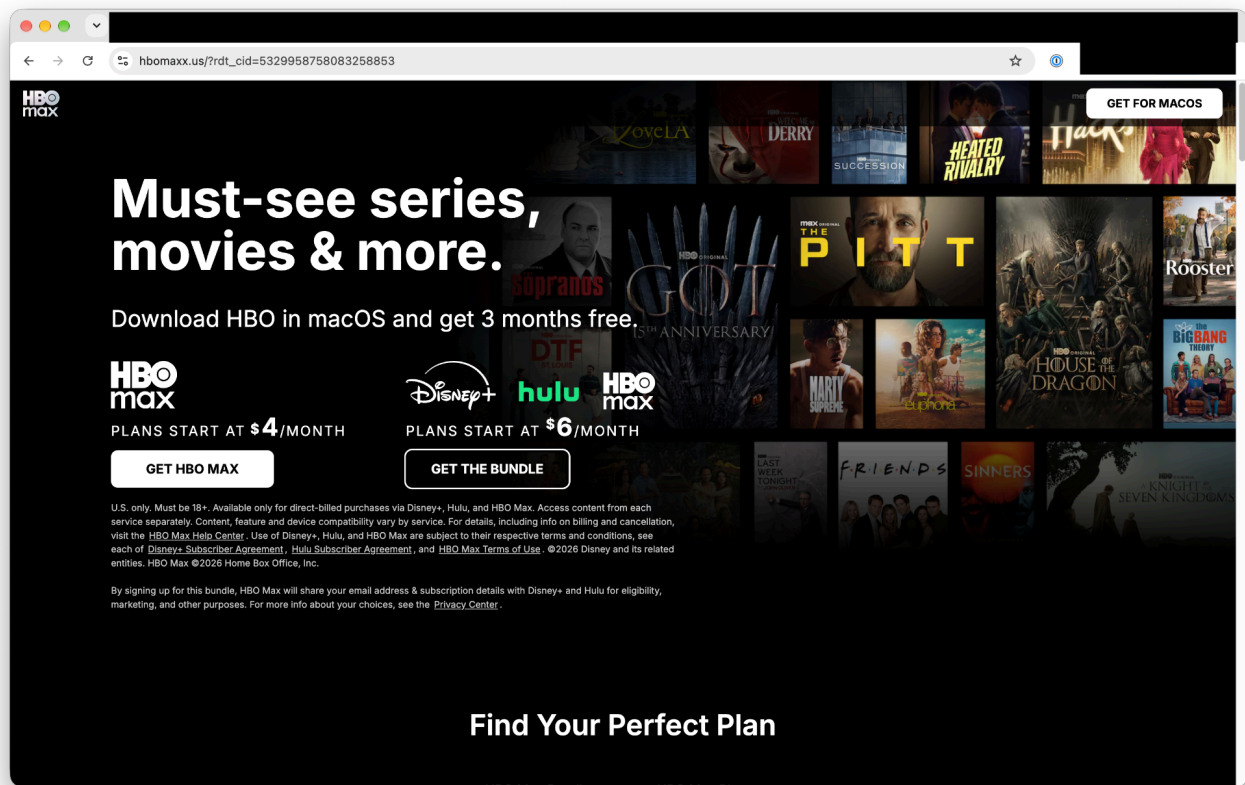
The Lure: Exploiting Trust and ClickFix Mechanics

The threat actors utilized highly polished assets to establish trust before delivering the malicious payload. By hijacking a verified corporate account, they bypassed the initial

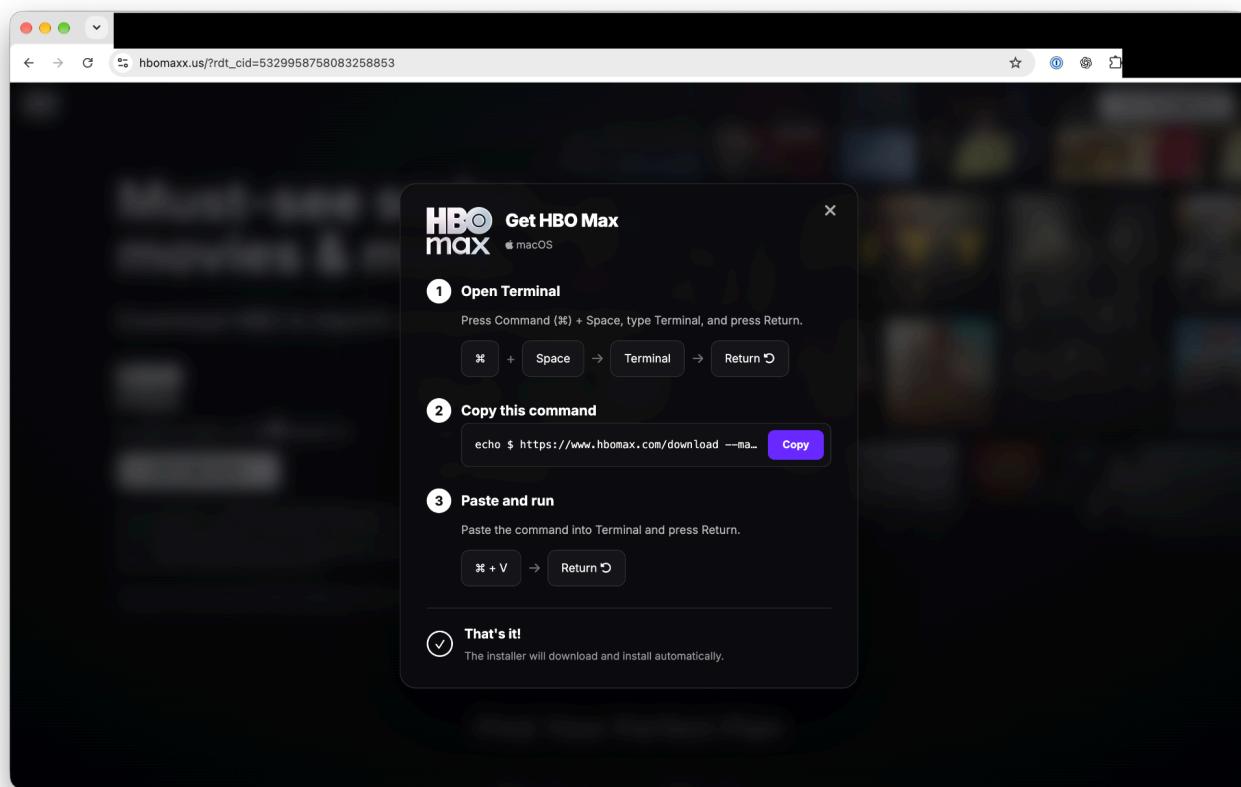
skepticism many users apply to internet advertisements.



A screenshot of the fraudulent advertisement natively displayed on Reddit, posted by the verified HBO Max account. (source: Alex Cutts)



The fraudulent landing page hosted at hbomaxx[.]us, designed to perfectly mimic the official HBO Max branding.



The ClickFix prompt shown by the HBO Max lure, instructing users to run malicious code in their Terminal.

Once the victim engaged with the download button, the site deployed the PasteSwitch ClickFix overlay. This tactic relies entirely on tricking the user into executing code themselves via the terminal or run dialog, successfully bypassing many standard browser-based download protections.

A Broader 48-Hour Malvertising Blitz

Further investigation utilizing OSINT tools revealed that the u/hbomax hijacking was not an isolated test run, but a massive 48-hour malvertising blitz. The threat actors squeezed as much value as possible out of the verified account's status, pivoting quickly when domains were burned.

In total, the attackers pushed **108 distinct ads** spanning multiple software lures. Beyond HBO Max, they targeted developers and power users seeking AI tools and disk cleaners.

u/ hbomax

Results for **u/hbomax** · Arctic Shift + PullPush
Filters

9.2k archived posts 266 comments 65.4k karma active since May 2020

Posts **200+** Comments 200+

^
1

u/hbomax · 4d ago
Use code REDDIT26 and get 6 months of Codex free. Download now.
show 0 comments open in reddit [codex-craft.com](#)

^
1

u/hbomax · 4d ago
Unlock 6 months of Codex at no cost. Enter REDDIT26 when you download.
show 0 comments open in reddit [codex-craft.com](#)

^
1

u/hbomax · 4d ago
Build with OpenAI Codex for 6 months — free with code REDDIT26.
show 0 comments open in reddit [codex-craft.com](#)

^
1

u/hbomax · 4d ago
Use code REDDIT26 and get 6 months of Codex free. Download now.
show 0 comments open in reddit [codex-craft.com](#)

The archived account activity using PullPush to count the 108 advertisements pushed by the hijacked u/hbomax account.

Lure Destination	Target Theme	
hbomaxx[.]app	40 ads	Streaming / Entertainment
codex-craft[.]com	36 ads	AI Tools / Developers
apple.clean-disk-guide[.]com	15 ads	macOS System Utilities
code-desktop[.]com	11 ads	AI Tools / Developers
hbomax-macos[.]com	6 ads	Streaming / Entertainment

The Windows Branch: InstallFix and Amatera

If the PasteSwitch gate detected a Windows user, it dynamically delivered a different payload path utilizing `mshta` and PowerShell. Examples included:

- **InstallFix via mshta:** Victims were prompted to run commands downloading an MP3/HTA polyglot. The HTA created a scheduled task, launched 32-bit PowerShell, disabled AMSI, and calculated a victim-specific subdomain based on the computer name and username.
- **In-Memory Loading:** The subsequent stages used arithmetic fog, opaque predicates, and shellcode to inject the Amatera Stealer PE directly into memory without touching the disk.
- **Deceptive TLS SNI Spoofing:** Once running, Amatera connected directly to an attacker IP (77.91.65.13:443) but presented `facebook.com` through TLS SNI and HTTP authority. By configuring Schannel for manual credential validation (`SCH_CRED_MANUAL_CRED_VALIDATION`), the malware bypasses certificate chain checks. Basic network telemetry mistakenly logs a connection to Facebook rather than the malicious C2, completely evading standard SNI-based filtering.

The Cryptocurrency Clipper Branch: Smart Contract C2 Rotation

For persistent clipboard replacement (swapping crypto addresses when victims try to copy or paste), PasteSwitch delivered `AnimateClipper` and `ZigClipper`.

These clippers utilized **Binance Smart Chain (BSC) contracts** as mutable C2 dead drops. The malware queries specific smart contracts (e.g., calling `getData()` or `balanceOf(address)`) to fetch the current active Command and Control domain (like `lb.propertyfind.cc`).

Between March and July 2026, researchers observed 36 mainnet changes executed by the same attacker controller address. Because the C2 domain is hosted directly on the blockchain, the infrastructure demonstrates dynamic resilience, allowing the threat actors to easily rotate burned domains.

Read the Full Technical Breakdown

For an exhaustive deep dive into the malware staging, network infrastructure, and a complete technical teardown of the PasteSwitch operation, please read the companion report by Kirk from ADAMnetworks: [HBO Max Ads Exposed: The PasteSwitch ClickFix Operation](#).

Reddit's Intervention

Following community reports and an escalating volume of malicious ads, Reddit administrators successfully intervened. They paused the affected ads and launched an internal investigation alongside their Security and Safety teams to secure the verified account.



redtaboo **ADMIN** • 3d



Hey everyone, thanks so much for bringing this to our attention! We've paused the affected ads and are looking into what happened with our Security and Safety teams.

... [← Reply](#)   +1 



PappaFrost • 2d

Does this mean that an official [u/hbomax](#) reddit account was compromised?

A Reddit administrator confirming the malicious ads have been paused pending a security investigation.

Conclusion

The HBO Max account provided PasteSwitch with a trusted advertising identity for 48 hours. The copied command exposed a delivery system that had already operated across software brands, operating systems, malware families, and infrastructure generations.

PasteSwitch kept its visible lures disposable while preserving operational structure. The same route grammar, API keys, helper identifiers, telemetry endpoints, staging conventions, task protocol, persistence paths, and registration patterns appeared after individual domains changed. On Windows, the operation combined InstallFix with layered in-memory loading and an Amatera client that presented facebook.com over a direct socket to 77.91.65.13. In the clipper branch, one controller synchronized C2 changes across testnet and mainnet contracts while two related binaries retained the same 21-address fallback configuration.

Those recurring controls provide the durable detection surface. Process ancestry exposes copied-command execution. Route tokens and API keys connect rotating macOS hosts.

Destination, SNI, certificate, and DNS correlation expose deceptive TLS identity. Contract setter monitoring reveals new clipper C2 domains as they are published. Brand names and lure domains change; the systems behind them retain the signals needed to follow PasteSwitch.

Indicators of Compromise (IOCs)

The inventory below covers the directly observed routes, recovered artifacts, infrastructure, and contract state described in this article. Published MacSync and gated-ClickFix domain sets remain available through the inline Microsoft, Zscaler, RST Cloud, Cato, and lostsh references.

Addresses

Address	Branch	Role	Source
45.94.47.204:80	AMOS helper	Enrollment, task polling, and acknowledgement	April PCAP and helper analysis
77.91.65.13:443	Amatera	Direct-to-IP TLS C2 using facebook.com SNI	Exact PE execution
165.22.199.85	September macOS	Telemetry and /contact exfiltration	September macOS execution
164.90.161.147:80	September macOS	Post-execution HTTP contact	September macOS execution
92.246.136.14	AMOS helper	Fallback /contact exfiltration	Helper configuration and published AMOS reporting
62.60.226.69	Shared provisioning	Nova and macOS-tool cluster	DNS, registration, and infrastructure records
176.53.159.66	Shared delivery	Teardown, TLS, and Windows executable cluster	DNS, TLS, certificate, and execution records

Address	Branch	Role	Source
172.236.51.169	Gated lure	Observed storageprofiler[.]com origin	Page capture and certificate records
138.124.93.32	AMOS helper	/contact exfiltration	Microsoft helper- campaign IOC list
168.100.9.122	AMOS helper	/contact exfiltration	Microsoft helper- campaign IOC list
199.217.98.33	AMOS helper	/contact exfiltration	Microsoft helper- campaign IOC list
38.244.158.103	AMOS helper	/contact exfiltration	Microsoft helper- campaign IOC list
38.244.158.56	AMOS helper	/contact exfiltration	Microsoft helper- campaign IOC list

Core Domains

Function	Indicators
Copied- command lures	filequanticore[.]com, filesiriuscore[.]com, alfredaps[.]com, hbomaxx[.]us, hbomax-macos[.]com, bright-links[.]com, codex- notes[.]com, storageprofiler[.]com, cladesktop[.]gitlab[.]io, cli-desktop[.]com, cli-stack[.]com, homebrwmac-hub[.]com, clean- disk-guide[.]com
Click tracking	flutelikelurkerunsinewy[.]com, camaligsalvatrefoils[.]com
macOS loader delivery	press29[.]com, leaf68[.]com, basequill9[.]com, perchframe15[.]com, canvas-35[.]com, pine63[.]com, trekmesh15[.]com
September telemetry and delivery	weaveridge7[.]com, ember-bridge[.]com, rudder-moss[.]com, wuess[.]com

Function	Indicators
MacSync delivery and control	houstongaragedoorinstallers[.]com, pressureulcerlawyer[.]com, lalandscape-lighting[.]com, aidevmaster[.]com, pinescope11[.]com, dogtrainersgeorgia[.]com, denverplumbingandwaterheater[.]com, restoremental[.]com, glowmedaesthetics[.]com, marbellaresales[.]com, gatemaden[.]space, beaocnagent[.]com, hbubagent[.]com
AMOS helper and tasking	arkypc[.]com, harbor-29[.]com, fern-plume[.]com, node-slate[.]com, grove-12[.]com, verse-18[.]com, lakhov[.]com, mpasvw[.]com, ouilov[.]com, aforvm[.]com
Fake wallet delivery	loop-lumen[.]com, umapla[.]com, glrack[.]com
Windows staging	desktop-version[.]com, oakenfjrod[.]ru
SIC Windows route	sic180[.]com, habar55[.]namebright[.]bike
Provisioning-linked lures	crisp-paths[.]com, cli-guides[.]com, macdeveloperhub[.]com, macfixguide[.]com, claud-tips[.]com, codex-paths[.]com, cmux-lab[.]com, rectangleap[.]com, muse-code-ide[.]com, hbomaxx[.]app, codex-craft[.]com, code-desktop[.]com, claude-tools[.]com, clean-disk-tools[.]com, opendisplay[.]us
Provisioning neighborhood	appldiag[.]com, getnova[.]top, nova-desk[.]top, nova-fix[.]top, nova-hub[.]top, nova-labs[.]top, nova-tools[.]top, novastacktips[.]com, remotion-skills[.]com, macstoragetips[.]com
Teardown and delivery neighborhood	chatgpt-safepage[.]com, thepullmanfolkestone[.]com, gigappyworld[.]com, microsoftupdater[.]info, gogolfonline[.]com, heroestales[.]com, wantsellonline[.]com, papartybus[.]com, clveeragent[.]com, congiagent[.]com, sgaaagent[.]com, sprieagent[.]com, cosimcagent[.]com, cehamilton[.]com, broadwalkindia[.]com, cim-kolea[.]com, hindustanagency[.]com
Address reuse	euquiz[.]space

Function	Indicators
Contract C2	lb[.]propertyfind[.]cc

Smart contracts

AnimateClipper: 0x6936edc505501EBB2F202C985a021a06f1c10C9E
 ZigClipper: 0x7CC3cFC1Ac007B8c6566fD2C7419b15a75473468
 Controller: 0x3a35b409af86e79e8945d6a7ffb1dc59b8dbdf46
 getData(): 0x3bc5de30
 balanceOf(): 0x70a08231
 setData(): 0x47064d6a

Key hashes

eec09815c3664aa6b3cd370a8b8f566be3b804949cfc514f145262136898b009	September macOS payload
d4150c1c97f047c6edb14767bf1efa8f9e37d63b124f38f27da4ef52d570aac2	AccountsHelper service component
f71d72711fe132f00d1a10d6f8c0f26c1544b41f57ca9262668dd2c771cc31f7	metadata mdworker component
a90a93e9776852dac869d4097dba2a4741ef5d316a1ae8631329349287e6a411	metadata mdworker_shared component
93d986f39599df747e4f65484a41d5e5ae7ece345924ea36e4f4ee623ce2f0ae	Arkypc loader
e6e54a8e8f30cedd8492f515ab95e005478bafb41998c43341fcf3a494573d6c	Arkypc helper
f8d09bb7ef38015342fb8ae11c489fcl1a3f01e743123e4222e9291cb474fb75e	fake Ledger archive
131a071301006dbed8dbf4d2e08b2914407b7693ab23566bdfef9f39f157aab4	fake Trezor archive
ecbbf5c7f1fac026dbaa74e8dac630730b4a49fbbb9fd59c333c48c28768ebfb	fake Exodus archive
5e8ad983129f6771d186f60379dca30d208374cac45bac75d5459aaf0fabcb8ad	InstallFix MP3/HTA carrier
480c65e5bb793da2d5ddfdcf00dd37bd4c7176ea0fb58d4e6bd5c891795dc2f5	InstallFix /claude carrier
3276414afb3c7ce7aa19db5401051ce4ad6968a7cc6bf8384cd6470c92541a24	recovered InstallFix PowerShell
ec9111b13bb21c1ce757db666b6df329724ec2ec493bcae1ba64b4ec2e93a331	recovered x86 shellcode
d4eb6e4cec1e69f3bc94bbe2d743e982863fc8549e49f832846c218e1aba3fcb	Amatera PE
6759c72365d0c690db613ff30635970668f5699b65c3842ecdc4f1b695ed13a7	SIC MP3/HTA payload
279d04c0cfd700c8bcb9acbed528131d3ffef8e25d12713e8649772739aecb92	Talos clipper

archive; extracted payload classified as AnimateClipper

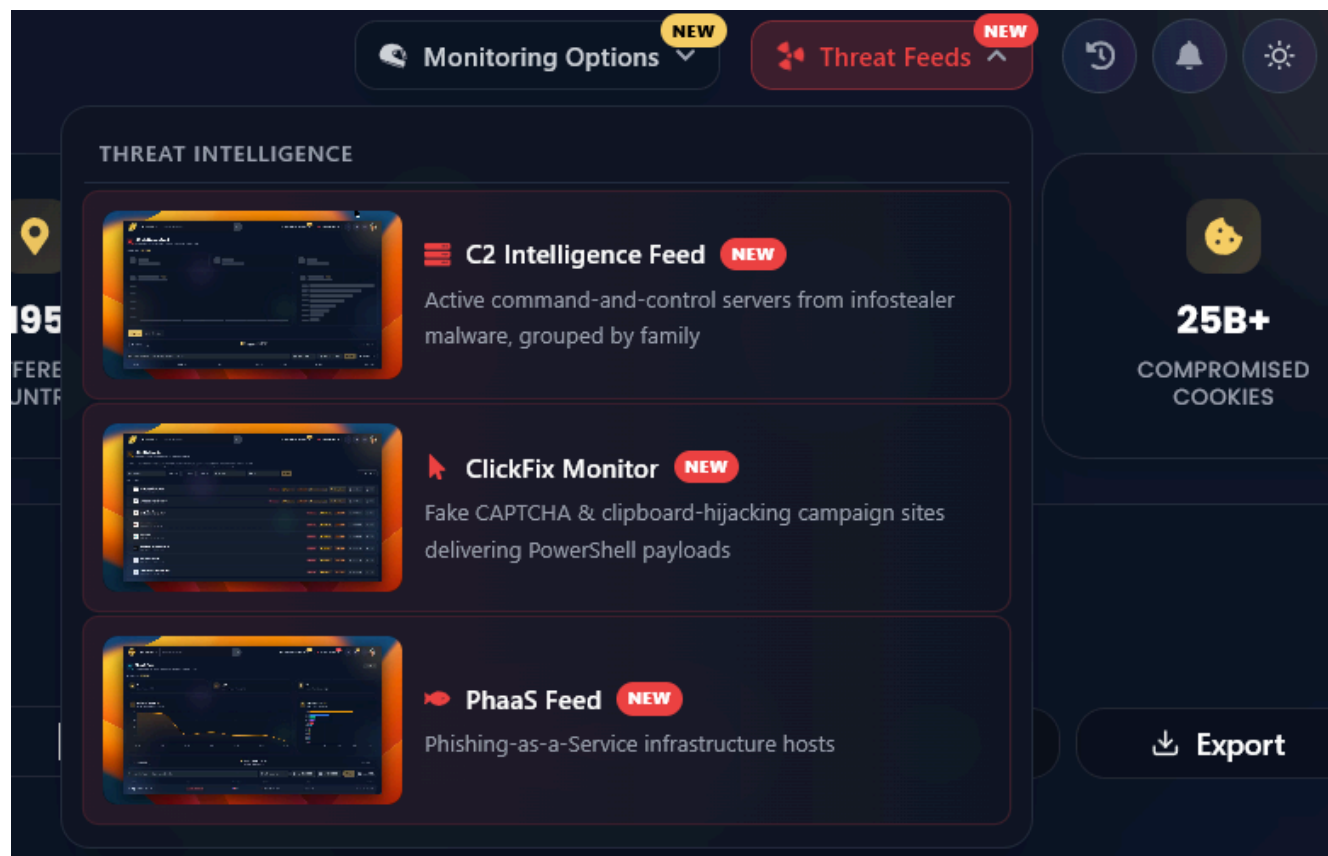
Additional recovered hashes

Contract-resolved C2 history

The following domains were decoded from successful setData(string) transactions against the Animate and Zig contracts. Repeated values are deduplicated.

Animate and Zig replacement addresses

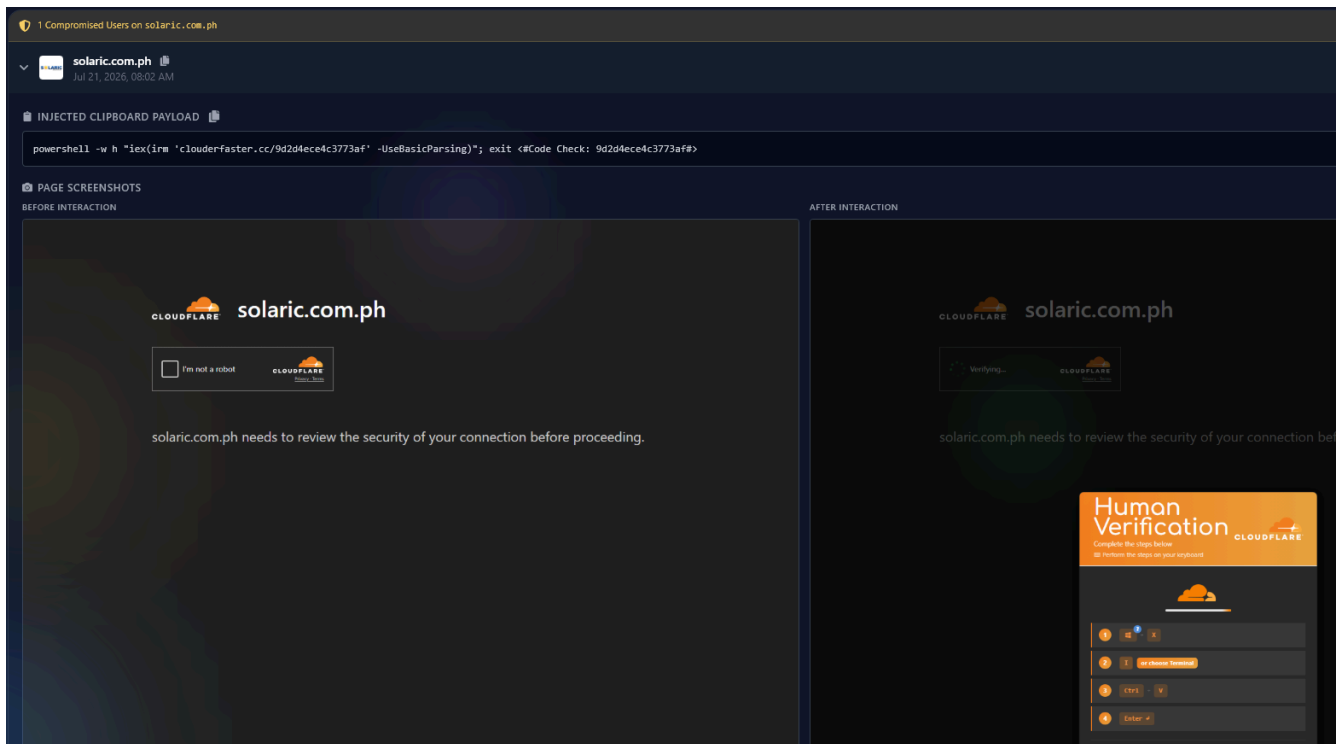
Wuess replacement addresses



Overview of the new Threat Feeds monitoring options available inside Cavalier, including C2 Intelligence, ClickFix Monitor, and PhaaS Feed.

With PasteSwitch and related ClickFix lures becoming increasingly sophisticated, it is vital to understand the exact mechanisms threat actors are using to deceive employees. Hudson Rock's new ClickFix module in Cavalier provides critical visibility into malicious websites that use fake verification pages, CAPTCHA prompts, and clipboard injection techniques to trick users into executing malicious commands.

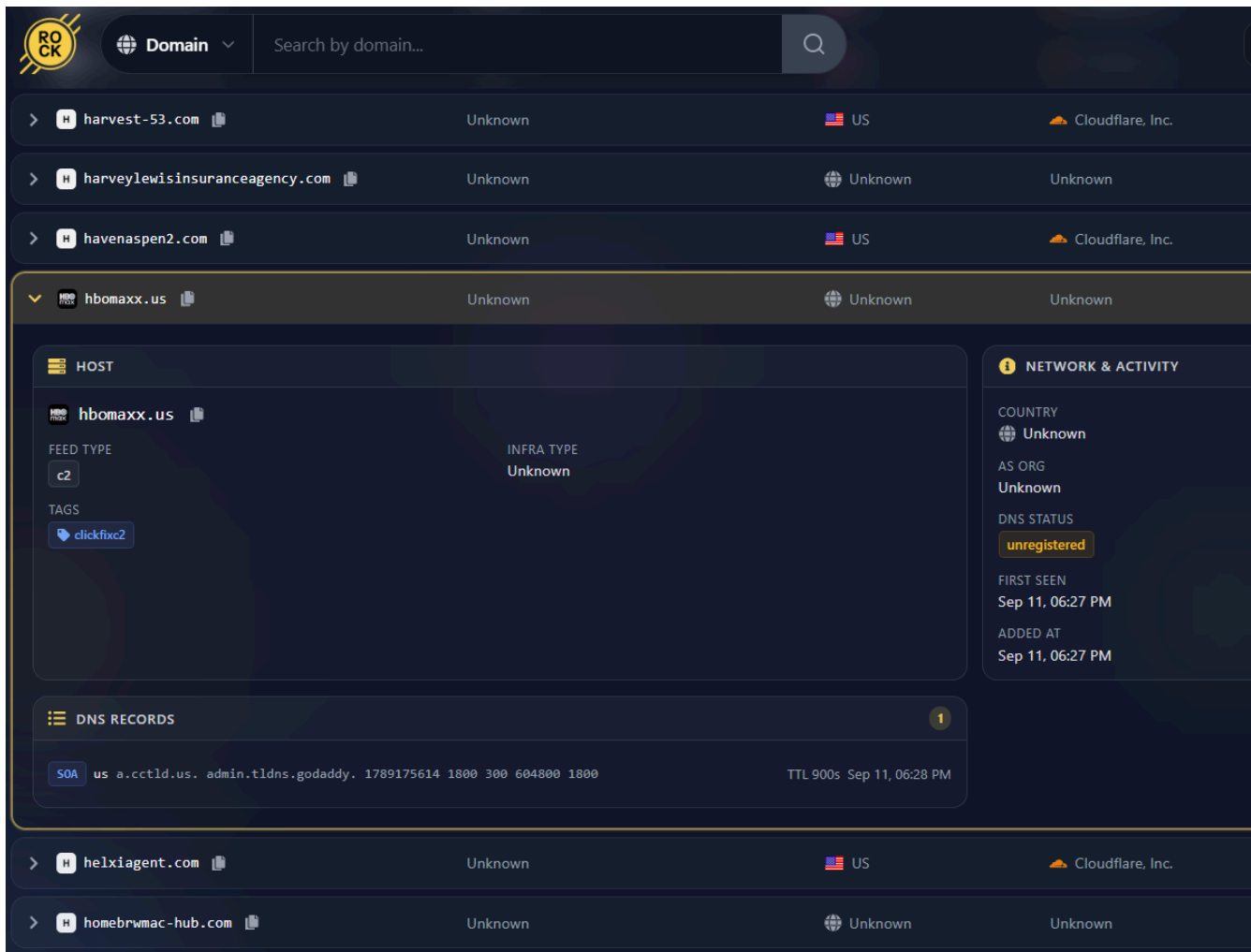
Inside Cavalier, security teams can seamlessly review detected ClickFix sites, clipboard injection and CAPTCHA indicators, injected command payloads, before and after interaction screenshots, and domain records.



Detailed analysis showing a malicious clipboard payload alongside a before and after comparison of a fake CAPTCHA interaction.

Perhaps the most powerful capability of the ClickFix monitor is its integration with Infostealer credential telemetry linked to the hosting platform. By combining insights from our C2 monitoring, which now includes all data surfaced from this cross-platform PasteSwitch campaign, Cavalier pinpoints compromised employee or user credentials that enabled attackers to gain initial access to servers, explaining how legitimate domains become hosts for malware.

Crucially, all of the C2 data surfaced in this research has been added to Hudson Rock's C2 monitoring where we track C2 data from infostealers, clickfix, and PhaaS (phishing as a service).



PasteSwitch C2 infrastructure, including hbomaxx[.]us, actively tracked within Hudson Rock's Cavalier platform.

Protect Your Organization from Imminent Intrusions

With our new Threat Feeds, cybersecurity teams can monitor live C2 infrastructure from infostealer campaigns, ClickFix networks, and PhaaS operations to proactively block malicious communications before they cause damage.

To learn more about how Hudson Rock protects companies from intrusions caused by info-stealer infections of employees, partners, and users, and how we enrich existing cybersecurity solutions with our cybercrime intelligence API, please schedule a call with us today.

[Schedule a Demo](#)