

Tracing the 2026 World Cup Infostealer Pipeline

✦ flare.io/learn/resources/blog/2026-world-cup-infostealer-pipeline

Flare Research

April 29, 2026

From Pirated Software to Full Access to FIFA: Tracing the 2026 World Cup Infostealer Pipeline



By Assaf Morag, Cybersecurity Researcher

Imagine that someone searches for a free PDF editor. They click a link on a website that seems legitimate, get bounced through a chain of disposable redirect domains, and download what looks like legitimate software. Buried inside the ZIP file is a hijacked Steam binary that silently loads an infostealer. Within minutes, every credential saved in every browser on that machine, including their FIFA account login, is packaged into a stealer log and traded on [Telegram](#).

Multiply that by 130,000 logs containing FIFA-related credentials that Flare identified over a period of one year (April 2025-April 2026), and the scale of the exposure becomes clear. This is the collateral damage of industrialized credential theft, and it creates a growing attack surface as the 2026 World Cup approaches.

About this World Cup Series

The United States, Canada, and Mexico have been selected to host the 2026 FIFA World Cup. As of early April, the lineup of all 48 teams set to compete in the final stage is now complete.

How are threat actors responding? What's already emerging across deep and dark web communities?

This blog is part of Flare's *World Cup 2026 Cybercrime Series*, a collection of focused research pieces examining the evolving threat landscape surrounding the tournament. The series explores key areas including [phishing infrastructure](#), [fraud and scams](#), illegal streaming services, illicit betting platforms, insider threats, and other cybercriminal activities targeting the 2026 World Cup.

Key Findings About FIFA-Related Credential Exposures

- **Nearly 130,000 infostealer logs containing FIFA-related credentials were identified by Flare, with over 2,500 exposed email/password pairs across the fifa.com and fifa.org domains.** This exposure is driven by broad, indiscriminate infostealer infections rather than a targeted campaign against FIFA, meaning the credentials are collateral damage from industrial-scale credential theft that sweeps up everything on an infected machine.
- **Infostealer-driven cybercrime is largely opportunistic.** However, the sheer volume of accumulated credentials creates a growing risk as the tournament approaches, giving threat actors a large pool of accounts to sort through for high-value targets such as staff, partners, or vendors with access to internal systems.
- **Flare researchers traced a complete infection chain of a victim with an email with a FIFA domain from a piracy search to credential theft in detail.** A victim searching for a free PDF editor was led through a multi-stage redirect chain using disposable .cfd domains, landed on a fake download page impersonating Google Drive, and downloaded a ZIP file containing a HijackLoader (Rugmi) infection delivered via DLL side-loading of a legitimate Steam binary, with the final payload almost certainly being Lumma Stealer.
- **Compromised FIFA credentials carry risk well beyond individual account takeover.** Attackers with access to staff or partner credentials can potentially reach internal systems, CRM platforms, or ticketing backends, enabling manipulation of ticket inventories, phishing campaigns targeting fans, or lateral movement into cloud platforms and operational infrastructure tied to the tournament. A single compromised endpoint becomes a scalable attack surface with both financial and operational impact.

Credential & Infostealer Monitoring

Detect Exposed Credentials Before They're Weaponized

Flare continuously scans underground forums, marketplaces, Telegram channels, and combolists to identify compromised accounts tied to your corporate domains, enabling immediate remediation before credentials are traded, reused, or leveraged for lateral movement.

- ✓ Real-time stealer log and credential exposure alerts
- ✓ Context on how credentials are traded and weaponized

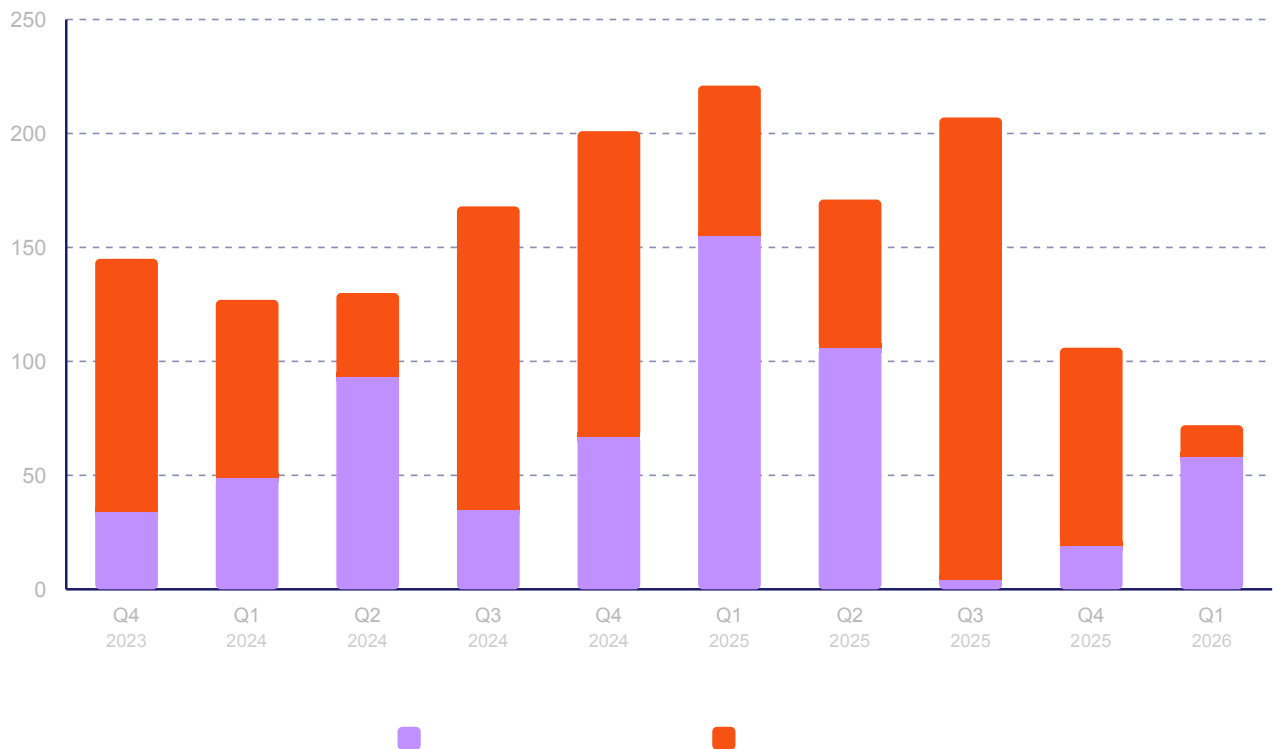
[Start Free Trial](#)

Organizational Credential Exposure

Whether conducting a threat intelligence review or a penetration test, the first step is discovery. We scoped our analysis to two domains owned and controlled by FIFA since 1995: “@fifa.com” and “@fifa.org”. These domains are owned and controlled by FIFA since 1995 and registered via CSC Corporate Domains, Inc. FIFA uses these domains internally to host the official website and to create email accounts for employees, contractors, and partners.

We utilized Flare’s Credential Browser feature to discover exposed assets (primarily email addresses and associated passwords) linked to these domains.

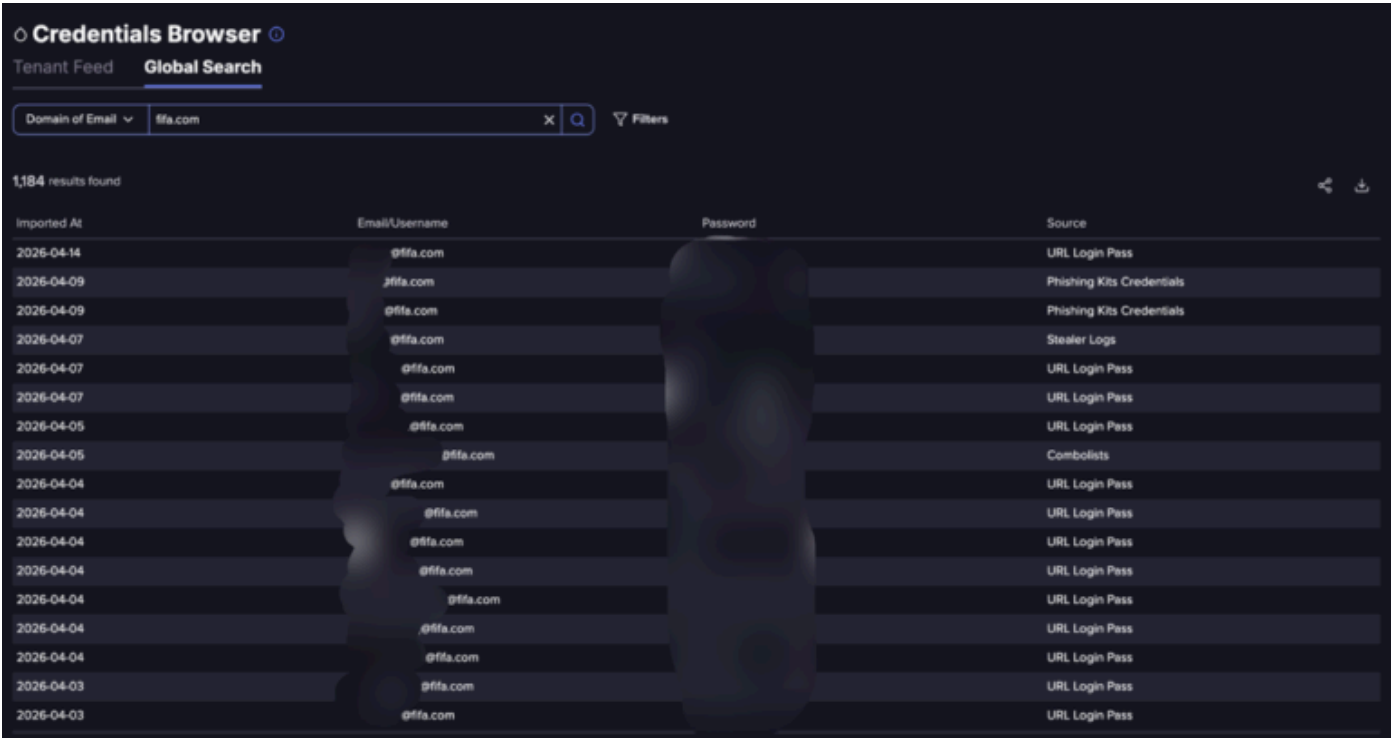
Compromised FIFA Credentials Since the 2022 World Cup



The sources of these credentials are primarily third-party breaches and combolists. These are uploaded to various underground forums and messaging groups, where they are shared or traded to facilitate cybercrime.

Exposure Summary

For [fifa.com](#), we found a total of 1,184 sets of email/username and password in Flare.

The screenshot shows the 'Credentials Browser' interface with a search bar set to 'fifa.com'. It displays a table of 1,184 results. The table has four columns: 'Imported At', 'Email/Username', 'Password', and 'Source'. The 'Email/Username' column contains various email addresses ending in '@fifa.com'. The 'Password' column shows a large number of redacted passwords. The 'Source' column lists various origins like 'URL Login Pass', 'Phishing Kits Credentials', 'Stealer Logs', and 'Combolists'.

Imported At	Email/Username	Password	Source
2026-04-14	@fifa.com	[REDACTED]	URL Login Pass
2026-04-09	@fifa.com	[REDACTED]	Phishing Kits Credentials
2026-04-09	@fifa.com	[REDACTED]	Phishing Kits Credentials
2026-04-07	@fifa.com	[REDACTED]	Stealer Logs
2026-04-07	@fifa.com	[REDACTED]	URL Login Pass
2026-04-07	@fifa.com	[REDACTED]	URL Login Pass
2026-04-05	@fifa.com	[REDACTED]	URL Login Pass
2026-04-05	@fifa.com	[REDACTED]	URL Login Pass
2026-04-05	@fifa.com	[REDACTED]	Combolists
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-04	@fifa.com	[REDACTED]	URL Login Pass
2026-04-03	@fifa.com	[REDACTED]	URL Login Pass
2026-04-03	@fifa.com	[REDACTED]	URL Login Pass

Flare’s Credential Browser search feature showing exposed credentials

For [fifa.org](#), we found a total of 1,329 sets of email/username and password in Flare.

Credentials Browser

Tenant Feed **Global Search**

Domain of Email: fifa.org

1,329 results found

Imported At	Email/Username	Password	Source
2026-04-14	@fifa.org	[REDACTED]	URL Login Pass
2026-04-08	@fifa.org	[REDACTED]	URL Login Pass
2026-04-04	@fifa.org	[REDACTED]	URL Login Pass
2026-03-25	@fifa.org	[REDACTED]	Stealer Logs
2026-03-23	@fifa.org	[REDACTED]	URL Login Pass
2026-03-23	@fifa.org	[REDACTED]	URL Login Pass
2026-03-22	@fifa.org	[REDACTED]	URL Login Pass
2026-03-21	@fifa.org	[REDACTED]	URL Login Pass
2026-03-21	@fifa.org	[REDACTED]	URL Login Pass
2026-03-21	@fifa.org	[REDACTED]	URL Login Pass
2026-03-20	@fifa.org	[REDACTED]	Combolists
2026-03-20	@fifa.org	[REDACTED]	URL Login Pass
2026-03-20	@fifa.org	[REDACTED]	URL Login Pass
2026-03-19	@fifa.org	[REDACTED]	URL Login Pass
2026-03-17	@fifa.org	[REDACTED]	URL Login Pass
2026-03-16	@fifa.org	[REDACTED]	URL Login Pass
2026-03-13	@fifa.org	[REDACTED]	URL Login Pass

Flare’s Credential Browser search feature showing exposed credentials

What Can Attackers Do With FIFA-Related Stealer Logs?

[Stealer logs](#) containing credentials and session data from users of FIFA-related platforms (such as fifa.com or fifa.org) can be extremely valuable to attackers.

This risk escalates across several dimensions:

- **Direct account access:** With access to authenticated sessions, attackers can bypass login protections and directly access user accounts, enabling activities like ticket theft or resale fraud ahead of high-demand events like the World Cup.
- **Internal system compromise:** If any compromised credentials belong to staff, partners, or vendors, attackers may gain access to internal systems, CRM platforms, or ticketing backends. This opens the door to broader data exposure, manipulation of ticket inventories, or unauthorized access to operational systems. Thus, identifying “higher tier” FIFA credentials is a key priority for threat actors ahead of major events.
- **Lateral movement:** Attackers can reuse credentials across services (SSO, email, cloud platforms) to pivot deeper into organizational environments, potentially reaching sensitive data such as financial records, event logistics, or security plans. In the context of a global event, this could escalate into targeted disruption, tampering with ticket distribution, launching phishing campaigns against fans, or even interfering with event infrastructure.

Ultimately, infostealer data turns a single compromised endpoint into a scalable attack surface with both financial and operational impact.

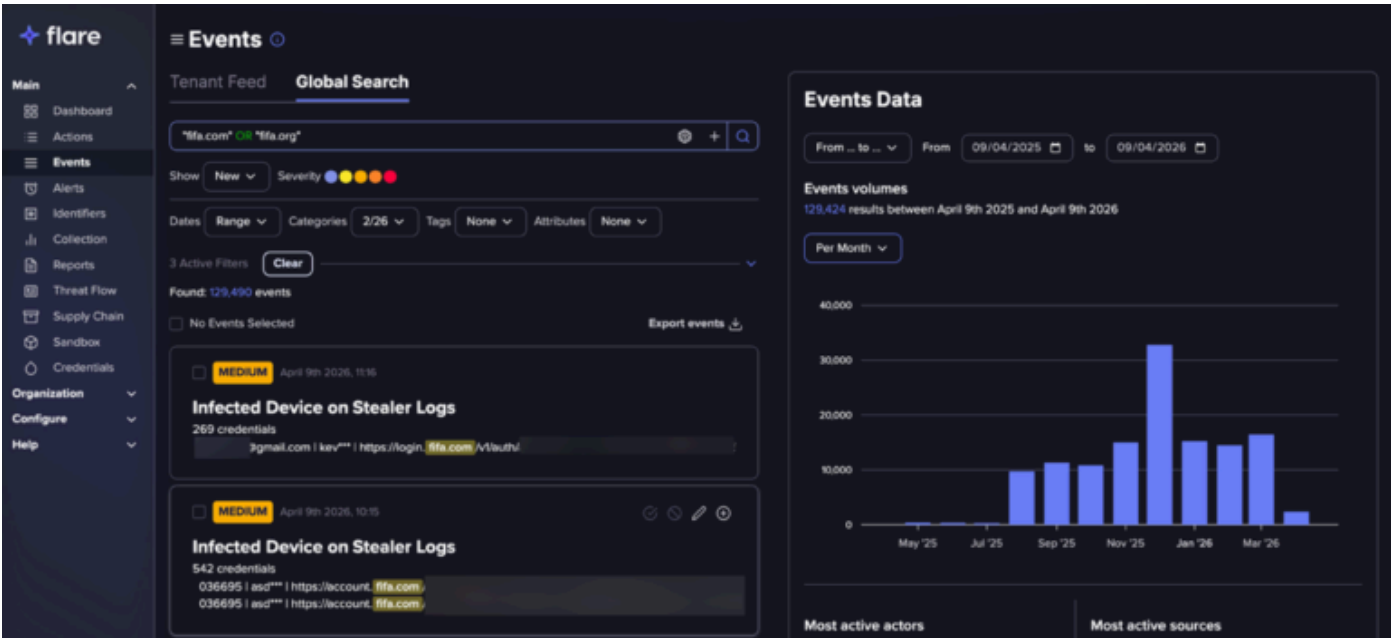
Analyzing the Infostealer Data

Infostealers have become one of the most dominant and scalable threats in modern cybercrime. Malware families like RedLine Stealer, LummaC2, and Vidar quietly harvest credentials, session cookies, autofill data, crypto wallets, and system fingerprints from infected machines, then exfiltrate them into structured logs that are traded across underground marketplaces and Telegram channels.

A single infection can expose dozens of corporate and personal accounts, while millions of such logs are continuously recycled, resold, and weaponized by [initial access brokers](#) and threat actors. Infostealers effectively collapse the boundary between home and enterprise environments, turning compromised endpoints into entry points for ransomware and data breaches.

When leveraging Flare to analyze infostealer activity over the past year, we identified nearly 130,000 logs containing at least one record associated with the domains fifa.com or fifa.org.

The infection trend remains relatively consistent over time, reinforcing a key insight: infostealer-driven cybercrime is largely opportunistic rather than campaign-specific. In other words, despite the heightened global attention surrounding FIFA and the 2026 World Cup, there is no clear indication of a targeted or coordinated campaign specifically aimed at FIFA users. Rather, these credentials are swept up as part of broad, indiscriminate infections at scale.



Searching for FIFA related stealer logs with Flare

Infostealer Family Distribution

We extracted a convenience sample via Flare’s API: the past 10 days for the fifa.com domain (727 distinct users) and a 60-day query for the fifa.org domain (10 distinct users). As expected, Lumma and Vidar infostealers dominate the dataset, consistent with their current market position.

Infostealer Families Distribution of FIFA Credentials

Vidar 67%

Lumma 24%

StealC 5%

RedLine 3%

Nexus 1%

Aurora 1%

Infostealer families distribution in our dataset

What Infostealers Collect

The infostealer data indexed on Flare contains detailed information about each infected machine.



Infected Device on Stealer Logs

Actions 

Summary

Content

Severity

AI Assist

Advanced

Severity **MEDIUM** Tags *none* Notes *none*

Metadata

Source

Stealer Logs

Creation Date

April 21st 2026, 16:10

First Seen

April 21st 2026, 16:11

Last Seen

April 21st 2026, 16:11

Seen In

Stealer Logs Live from Telegram

User Information

Username

HWID

Location

AR, UTC-3

Malware Information

Malware Family

unknown

Build ID

-

Estimated Infected At

2026-04-21T20:10:45+00:00

File Location

C:\WINDOWS\SysWOW64\rundll32.exe

Data about an infostealer infected machine ([Flare](#) link to post, sign up for the [free trial](#) to access if you aren't already a customer)



Files

Expand all

> Autofill

> Cookies

> GoogleAccounts

> History

> Soft

domain detect.txt

Information.txt

passwords.txt

unique_passwords.txt

ViewDownload

ViewDownload

ViewDownload

ViewDownload

Infostealer infected machine files

8/21

- **Autofill data:** Everything from the browser's autofill database, including credit cards, emails, passwords, logins, and other form data the browser automatically completes.
- **Cookies:** Session data stored by websites to enable persistent access. Whoever holds this data can access the websites the victim is currently logged into.
- **Google Accounts:** Account information associated with the victim's Google profile.
- **Browsing history:** Full history, including URLs that may contain login details (e.g., `https://user:password@website.com`).
- **Software tokens:** Authentication and password information for desktop applications such as WhatsApp, Discord, and Telegram.
- **Parsed aggregated lists:** Extracted domains, credentials, and unique passwords organized for easy consumption by other threat actors.

Tracing a Real Victim's Infection Sequence

The data Flare collects includes information about the malicious file's execution path, which reveals how the victim was infected. Therefore, we can further learn about the malware. We analyzed our dataset and found that the majority of samples ran on Windows machines. We selected a recent, illustrative example to retrace the infection sequence:

`C:\Users\<<Reducted>>\Downloads\pdf-xchange_editor_plus_(2026)_full_espa√±ol_[mega].exe`

Step 1: The Search

The victim searched for a free version of PDF-XChange Editor Plus.

descargar pdf-xchange editor plus (2026) full espanol gratis



AI Mode **All** Videos Images Short videos Books Web More ▾ Tools ▾



artistapirata.me

<https://artistapirata.me/pdf-xchan...> · [Translate this page](#) · [⋮](#)

Descargar PDF-XChange Editor Plus v10.8.2.407 Full [Mega ...

10 Jan 2026 — PDF-XChange Editor Plus descargar full 2026 es un editor y visualizador de PDF ligero, rápido y robusto que incluye varios complementos. PDF- ... [Read more](#)



artistapirata.fit

<https://artistapirata.fit/pdf-xchan...> · [Translate this page](#) · [⋮](#)

Descargar PDF-XChange Editor Plus 2026 Full Español Gratis

25 Feb 2026 — Obtenga la versión completa en español de PDF-XChange Editor Plus 10.7.6. Puede crear, examinar, editar, añadir comentarios, aplicar OCR y ... [Read more](#)



ZDescargas

<https://www.zdescargas.org/pdf-...> · [Translate this page](#) · [⋮](#)

PDF-XChange Editor Plus (2026) Full Español [Mega]

18 Dec 2025 — PDF-XChange Editor Plus es un software emocionante que le permite leer archivos PDF. · El editor de PDF viene con muchas funciones y los usuarios ... [Read more](#)



artistapirata.fit

<https://artistapirata.fit/descargar-...> · [Translate this page](#) · [⋮](#)

PDF-XChange Pro 2026 Full Portable con Español Gratis

Diseñador de nuevos formularios PDF rellenables. Creación de sellos y modificación sobre la marcha. El editor PDF-XChange funciona con Google ... [Read more](#)

All of the top results led to malicious downloads. Each linked to a stolen or cracked software sharing website. Most of these sites are not legal, as they offer paid software like PDF-XChange Editor Plus for free (indicating cracked or modified versions). Site names like “artistapirata” openly advertise piracy.

JAN
10

Descargar PDF-XChange Editor Plus v10.8.2.407 Full [Mega] 2026

Filed under [Oficina y PDF](#), [ArtistaPirata Programas](#), [Programa](#), [Software para Mac](#)



DIRECT
Download



Artistapirata PDF-XChange Editor Full Español Mega

The page of an illegal download link for the cracked software

Clicking the download link triggered a chain of intermediate redirects:

The first redirect was: [https://href.li/?https://wikifilhost78.it\[.\]com/?data=...](https://href.li/?https://wikifilhost78.it[.]com/?data=...)

This URL uses a public redirector (href.li) combined with a fake file-hosting domain and includes embedded PHP code that generates random values per request, likely to evade detection and complicate tracking.

This was the second redirect: [https://getcdn82\[.\]host93s\[.\]cfd/?tag=u7tY5vH4](https://getcdn82[.]host93s[.]cfd/?tag=u7tY5vH4)

This page acts as a disposable “Downloading...” redirector, using multiple forced redirection methods to immediately forward users to another dynamically generated .cfd domain. This type of behavior is commonly observed in staged malware or phishing delivery chains.

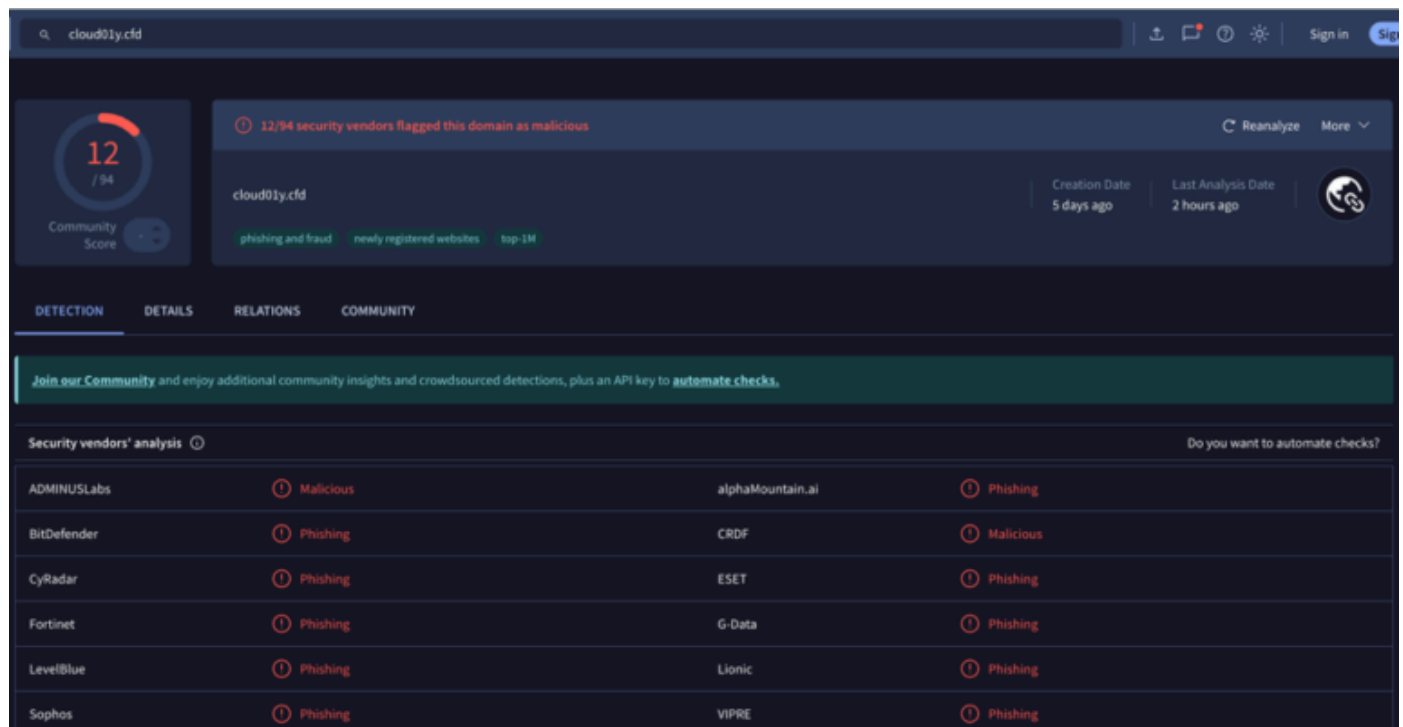
The third redirect was: [https://generate907a38\[.\]host93s\[.\]cfd/?data=...](https://generate907a38[.]host93s[.]cfd/?data=...)

Another lightweight redirector forcing navigation to a dynamically generated domain with encoded parameters, reinforcing the pattern of multi-stage obfuscation used to conceal the true payload.

Both domains on this redirection chain were recently registered, indicating that the infrastructure is highly maintained and volatile.

The operational cycle works as follows: piracy advertisements point to a highly configurable redirect link. As URLs are flagged as malicious over time, newly registered domains replace the burned ones. New victims click the piracy ads, get redirected and infected, the links are eventually reported, and the cycle repeats.

Below you can see that even though this domain is fairly new, it’s already flagged in VirusTotal as malicious with a phishing related connection.



The screenshot shows the VirusTotal interface for the domain **cloud01y.cfd**. At the top, a circular gauge indicates a **Community Score** of 12/94. A notification states that **12/94 security vendors** flagged this domain as malicious. The domain is categorized as **phishing and fraud**, **newly registered websites**, and **top-1M**. It was created **5 days ago** and last analyzed **2 hours ago**. Below this, a table titled "Security vendors' analysis" lists 12 vendors and their detection results:

Vendor	Detection	Vendor	Detection
ADMINUSLabs	Malicious	alphaMountain.ai	Phishing
BitDefender	Phishing	CRDF	Malicious
CyRadar	Phishing	ESET	Phishing
Fortinet	Phishing	G-Data	Phishing
LevelBlue	Phishing	Lionic	Phishing
Sophos	Phishing	VIPRE	Phishing

VirusTotal detections for the domain cloud01y.cfd

The backend dynamically generates a new random subdomain for each request to serve the malware.

Subdomains (811) ⓘ			
file676207.cloud01y.cfd	7 / 94	104.21.31.19	172.67.174.166
file531277.cloud01y.cfd	8 / 94	172.67.174.166	104.21.31.19
file902842.cloud01y.cfd	3 / 94	104.21.31.19	172.67.174.166
file971882.cloud01y.cfd	3 / 94	172.67.174.166	104.21.31.19
file280015.cloud01y.cfd	3 / 94	172.67.174.166	104.21.31.19
file756674.cloud01y.cfd	3 / 94	104.21.31.19	172.67.174.166
file704231.cloud01y.cfd	3 / 94	172.67.174.166	104.21.31.19
file647140.cloud01y.cfd	3 / 94	104.21.31.19	172.67.174.166
file296034.cloud01y.cfd	6 / 94	172.67.174.166	104.21.31.19
file443745.cloud01y.cfd	6 / 94	172.67.174.166	104.21.31.19
file212037.cloud01y.cfd	8 / 94	172.67.174.166	104.21.31.19
file915079.cloud01y.cfd	4 / 94	104.21.31.19	172.67.174.166
file641671.cloud01y.cfd	8 / 94	104.21.31.19	172.67.174.166
file953173.cloud01y.cfd	4 / 94	172.67.174.166	104.21.31.19
file563744.cloud01y.cfd	4 / 94	172.67.174.166	104.21.31.19
file574059.cloud01y.cfd	4 / 94	104.21.31.19	172.67.174.166
file316516.cloud01y.cfd	0 / 94	172.67.174.166	104.21.31.19
file725080.cloud01y.cfd	4 / 94	104.21.31.19	172.67.174.166
file453564.cloud01y.cfd	7 / 94	104.21.31.19	172.67.174.166
file928727.cloud01y.cfd	10 / 94	104.21.31.19	172.67.174.166
file453564.cloud01y.cfd	7 / 94	104.21.31.19	172.67.174.166
file928727.cloud01y.cfd	10 / 94	104.21.31.19	172.67.174.166
file177430.cloud01y.cfd	6 / 94	172.67.174.166	104.21.31.19
file452248.cloud01y.cfd	0 / 94	172.67.174.166	104.21.31.19
file775438.cloud01y.cfd	8 / 94	172.67.174.166	104.21.31.19
file878462.cloud01y.cfd	4 / 94	104.21.31.19	172.67.174.166

VirusTotal's (partial) list of sub-domains for our domain

The newly registered domains were:

host93s.cfd

Updated 1 second ago 



Domain Information

Domain:	host93s.cfd
Registered On:	2026-04-02
Expires On:	2027-04-02
Status:	server transfer prohibited client transfer prohibited
Name Servers:	thea.ns.cloudflare.com vicente.ns.cloudflare.com

Whois host93s.cfd registration details

cloud01y.cfd

Updated 2 days ago 



Domain Information

Domain:	cloud01y.cfd
Registered On:	2026-04-15
Expires On:	2027-04-15
Status:	server transfer prohibited client transfer prohibited add period
Name Servers:	edna.ns.cloudflare.com mark.ns.cloudflare.com

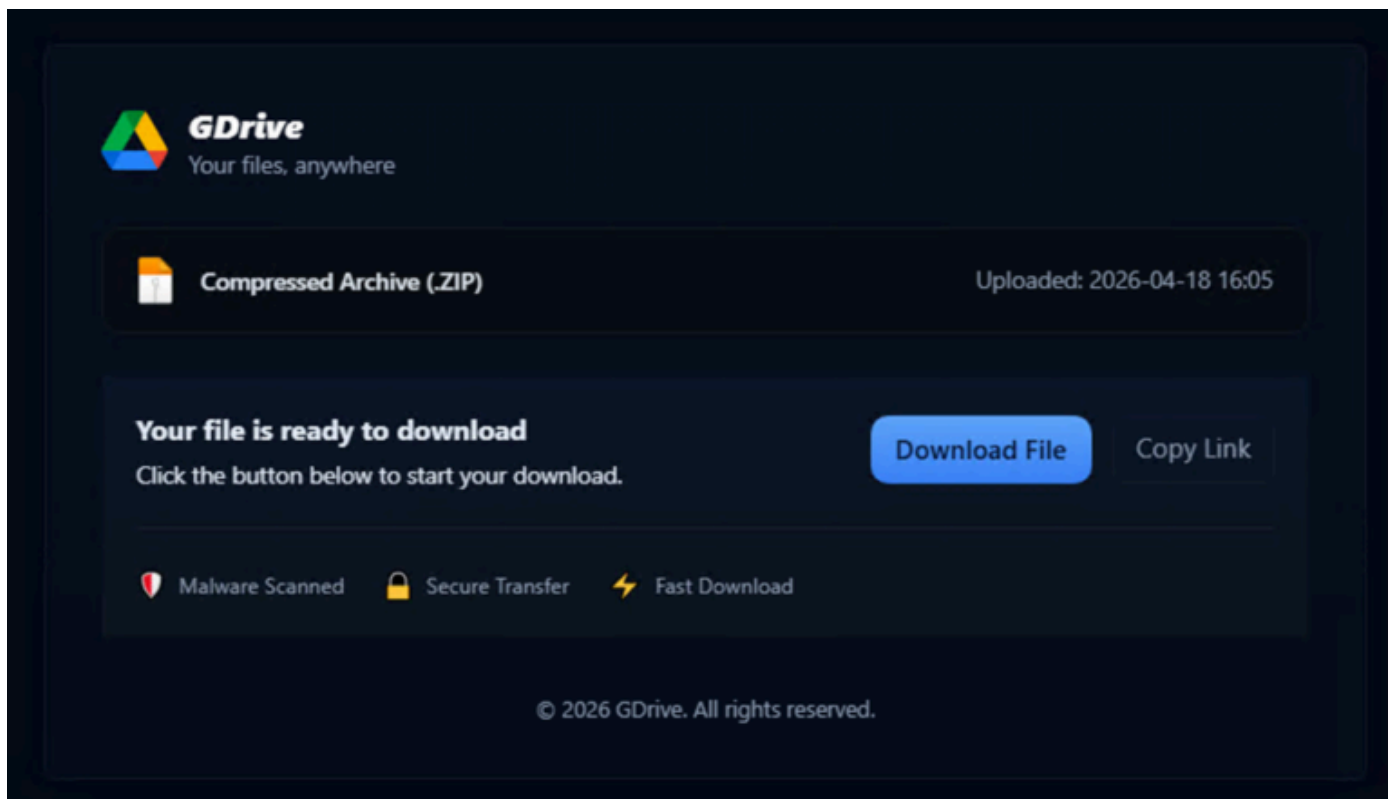
Whois cloud01y.cfd registration details

The .cfd domain is cheap and relatively new, with no established trust. Because it is easy to register and disposable, it is frequently used for short-lived or low-reputation websites. While not all .cfd sites are malicious, they generally carry higher risk compared to established domains.

It is possible that the domain cloud01y is a domain lookalike of the name Cloudly, which bundles several legitimate software companies and an open source project.

Step 3: The Fake Download Page

Below is the final page in the redirect page, which leads to a file download.



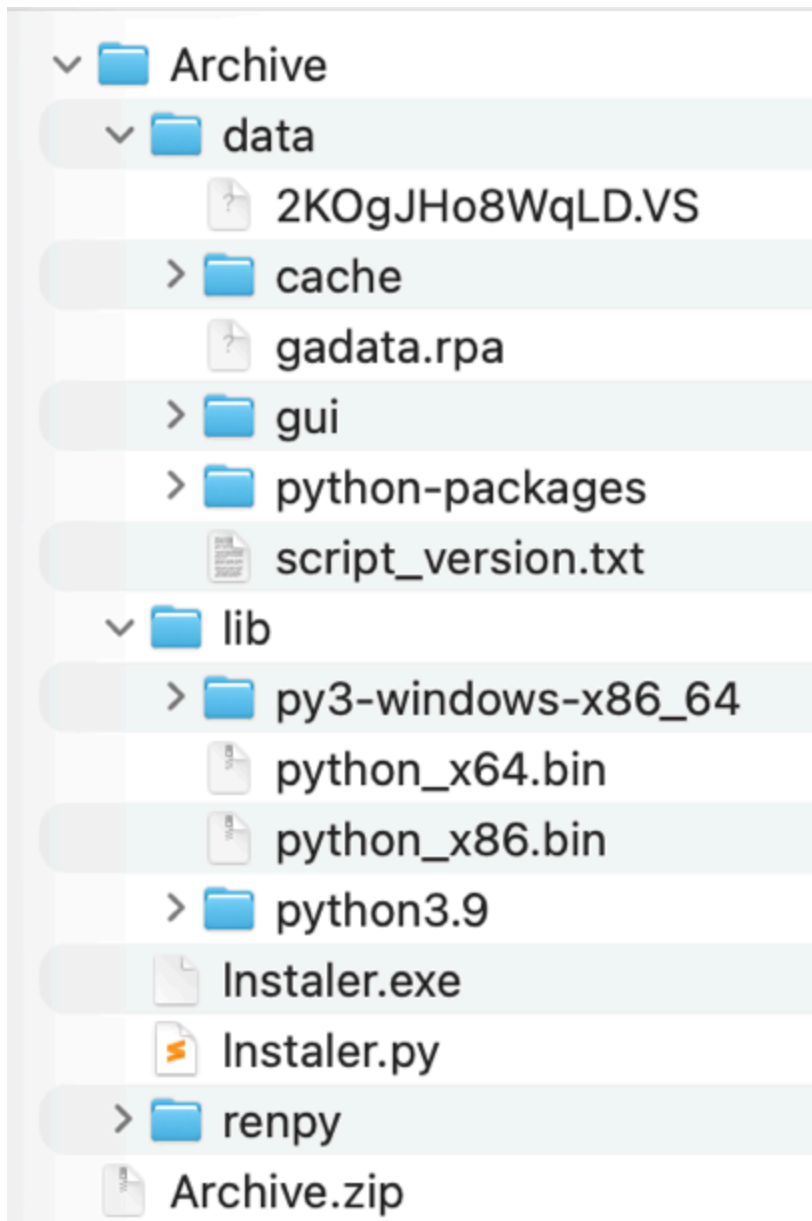
The download site

The final page in the redirect chain presents a fake download interface designed to look like a legitimate cloud storage service (“GDrive”). The actual download link is hidden in the code (`data-url="https[:]//edge2[.]filehost74[.]sbs/..."`), while the visible page shows generic trust signals like “Malware Scanned” and “Secure Transfer” that are not backed by any real functionality. The “Copy Link” button is misleading, as it triggers the same download flow instead of copying anything. These pages rotate logos and names of popular file-sharing services such as Google Drive and Dropbox.

The page also includes basic anti-analysis behavior. A script continuously checks whether developer tools are open and, if detected, clears the page content (`document.documentElement.innerHTML = ""`), which explains why everything disappears during inspection. Additional protections (disabling right-click and text selection) further suggest the page is designed to prevent analysis rather than improve the user experience.

Step 4: The Payload

We downloaded and extracted the compressed .zip file.



The .zip file inflated directory tree

We analyzed all the files in the inflated directory. Most of them were benign. But, we did find a HijackLoader (also known as Rugmi or IDAT Loader) infection chain delivered via the fake pirated software lure.

The attack uses DLL search-order hijacking: a legitimate, code-signed Valve Steam binary is renamed and bundled alongside a trojanized SDL3.dll that implements the HijackLoader malware.

When the victim executes the fake Steam binary, Windows automatically loads the malicious SDL3.dll from the same directory. The loader reads an encrypted PE payload from a disguised configuration file (mesh.conf) using a 1,002-byte key from asset32.tmp, decrypts it in memory, and

reflectively executes the second stage. Based on the delivery context and behavioral indicators, the final payload is most likely Lumma Stealer.

Two of the five files received AV detections on VirusTotal (Rising AV):

File	MD5	Detection
SDL3.dll	9af16f9fc35ce00688c20318e868664a	Downloader.Rugmi/x64!1.134BF
mesh.conf	9eecf800853672a56fc46d26b6fa5bb1	Trojan.HijackLoader!1.12810

The same loader is tracked in the media under 3 different names: IDAT Loader, HijackLoader, and Rugmi. It is a private loader sold on underground cybercrime forums. Different threat actors purchase access and configure their own payload and C2.

Blog Post on OsintCorp

Actions

SummaryContentSeverityAI AssistAdvanced

SeverityLOWTags noneNotes none

Metadata

Source

OsintCorp

Creation Date

December 28th 2023, 1:00

First Seen

July 31st 2024, 23:44

Last Seen

August 25th 2025, 18:48

URL

https://osintcorp.net/new-rugmi-malware-loader-surges-with-hundreds-of-dail...

Classifiers

-

Category Name

-

Content Preview

New Rugmi Malware Loader Surges with Hundreds of Daily Detections

loader that runs the payload from internal resources, and another loader that runs the payload from an external file on the disk," the company said in its Threat Report H2 2023. Telemetry data gathered by the company shows that detections for the Rugmi loader spiked in October and November 2023, surging from single digit daily numbers to hundreds per day. UPCOMING WEBINAR

Related Articles

Intelligence on Rugmi loader from Flare ([Flare](#) link to post, sign up for the free trial to access if you aren't already a customer)

In this case, the distribution vector was a fake pirated software forum. Other common distribution methods for this loader include:

- Fake pirated software / game cracks on torrent sites and warez forums
- Malvertising via Google or Bing ads for cracked software
- Fake YouTube tutorials with malicious download links in descriptions
- Telegram channels distributing “free” game cheats and mods
- ClickFix attacks, a social engineering attack where a fake error or CAPTCHA tricks users into running commands on their own device, effectively executing malware themselves (it bypasses traditional defenses by relying on user actions instead of exploiting software vulnerabilities)

Below is the infection chain:



The infostealer's infection chain

MITRE ATT&CK Mapping

Technique	ID	Description
Supply Chain Compromise: Compromise Software Supply Chain	T1195.002	There is correlation to Phishing, Drive-by-Compromise, and SSC. This is a website that offers cracked software, and introduces malware in the cracked illegal software.

Technique	ID	Description
User Execution: Malicious File	T1204.002	Victim runs <code>GgPIgyXGx.exe</code>
DLL Side-Loading	T1574.002	<code>SDL3.dll</code> loaded by legitimate Steam binary from same directory
Obfuscated Files: Steganography	T1027.003	Second-stage PE hidden inside PNG IDAT chunks in <code>mesh.conf</code>
Obfuscated Files: Encoding	T1027	Text-scrambled key (<code>asset32.tmp</code>) and C2 config (<code>mesh.conf</code> header)
Reflective Code Loading	T1620	In-memory PE loading — no disk write of decrypted payload
Masquerading	T1036	<code>steam.exe</code> renamed to random filename <code>GgPIgyXGx.exe</code>
Indicator Removal	T1070	No registry persistence; payload never written to disk
Obfuscated Files: API Hashing	T1027.007	GetProcAddress-by-hash, custom seed <code>0x0BB7A699</code>
Credentials from Web Browsers	T1555.003	Expected Lumma Stealer target (browser password stores)
Clipboard Data	T1115	Typical Lumma Stealer collection target
Exfiltration over C2 Channel	T1041	Stealer exfiltrates via C2 encoded in <code>mesh.conf</code> config header

Taking the Infostealer Malware Seriously with Proactive Visibility

Flare’s analysis reveals consistent and largely opportunistic exposure of credentials linked to FIFA domains, driven primarily by widespread infostealer infections rather than a coordinated, targeted campaign. However, this should not be mistaken for low risk.

The aggregation of hundreds of credentials and nearly 130,000 infostealer logs (from a period of 10 days) creates a fertile ground for threat actors to identify high-value accounts, reuse access across services, and potentially pivot into sensitive environments.

As the World Cup approaches, the risk is not just in an isolated account compromise but in the compounding effect of scale, where stolen credentials, session tokens, and device data can be weaponized for fraud, phishing, lateral movement, and even disruption of event-related operations.

In a landscape where personal and organizational identities are deeply intertwined, infostealers transform everyday infections into strategic footholds. For organizations involved in global events like FIFA, proactive visibility into exposed assets is no longer optional. It is a critical layer of defense.

Credential & Infostealer Monitoring

Detect Exposed Credentials Before They're Weaponized

Flare continuously scans underground forums, marketplaces, Telegram channels, and combolists to identify compromised accounts tied to your corporate domains, enabling immediate remediation before credentials are traded, reused, or leveraged for lateral movement.

- ✓ Real-time stealer log and credential exposure alerts
- ✓ Context on how credentials are traded and weaponized

[Start Free Trial](#)