Exposing the Deception: Russian EFF Impersonators Behind Stealc & Pyramid C2

Published: 2025-03-04 · Archived: 2026-04-06 00:54:17 UTC

Open directories often expose more than just files--they provide a window into how malicious campaigns operate. In this case, we identified a **threat actor impersonating the Electronic Frontier Foundation (EFF) to target the online gaming community**. The exposed directory contained decoy documents alongside the malware used in this operation: Steal and Pyramid C2.

Further analysis linked 11 additional servers to the campaign through shared SSH keys, indicating a broad network footprint. Code comments found within malicious Python and PowerShell scripts suggest the work of a Russian-speaking developer. The tactics and malware observed align with financially motivated cybercrime activity. Hunt had already identified both C2 servers weeks earlier as part of routine scanning, but the open directory provided the link between the malware and this operation.

This post examines the role of the decoy documents and phishing attempts in the activity and explores how code analysis revealed additional infrastructure.

Campaign Overview

A threat group impersonating the Electronic Frontier Foundation (EFF) is targeting Albion Online players through decoy documents designed to lend credibility while malware executes in the background.

Albion Online is a multiplayer online role-playing game (MMORPG) with a player-driven economy. While real-money transactions are against the game's terms of service and can result in permanent bans, third-party markets exist where in-game assets are exchanged for money, making player accounts a lucrative target.

Players on the game's forum have reported receiving messages from other members directing them to phishing websites, with the EFF's name used as a pretext to discuss the security of in-game goods tied to their accounts.

Technical Details

Open Directory

On February 27th, Hunt's AttackCapture™ identified an open directory at http[:]//83.217.208[.]90/documents.

AttackCapture™ scans and archives files from exposed servers while categorizing malicious samples based on sandbox analysis, enabling quick reference during threat hunting. This particular server contained detections for PowerShell usage and Stealc, which immediately grabbed our attention.

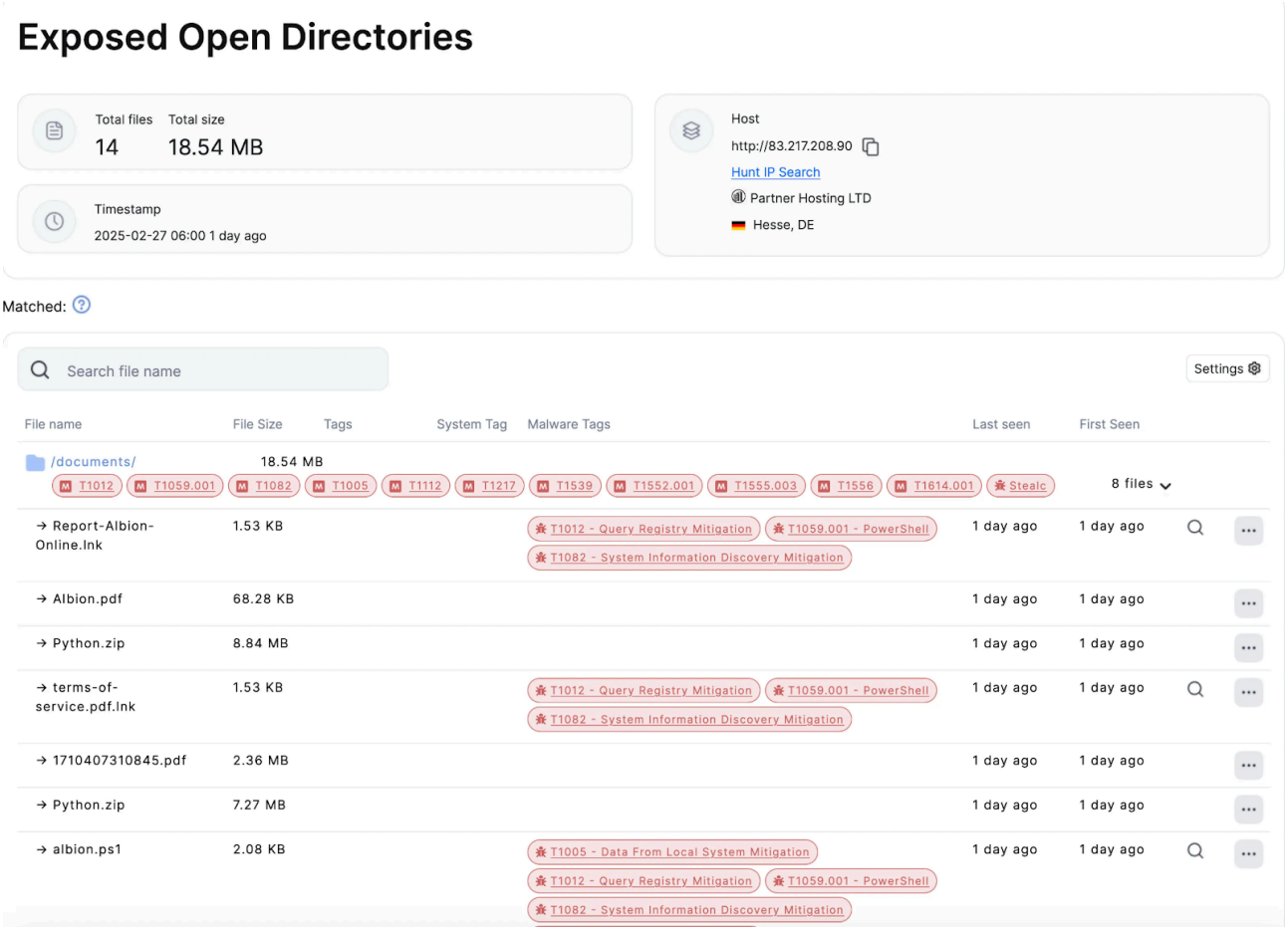

Figure 1: Screenshot of the directory contents hosted at 83.217.208[.]90 in Hunt.

The server hosted a mix of PDFs, ZIP archives, PowerShell scripts, and filenames with double extensions---common indicators of malware staging. While this section provides a brief overview of notable files, a detailed analysis follows in the next section.

Infrastructure & SSH Key Overlaps

Let's first look at the IP address hosting the malware. Clicking on 'Hunt IP Search' in the Host section brings us to the overview page, which quickly shows two areas of interest.

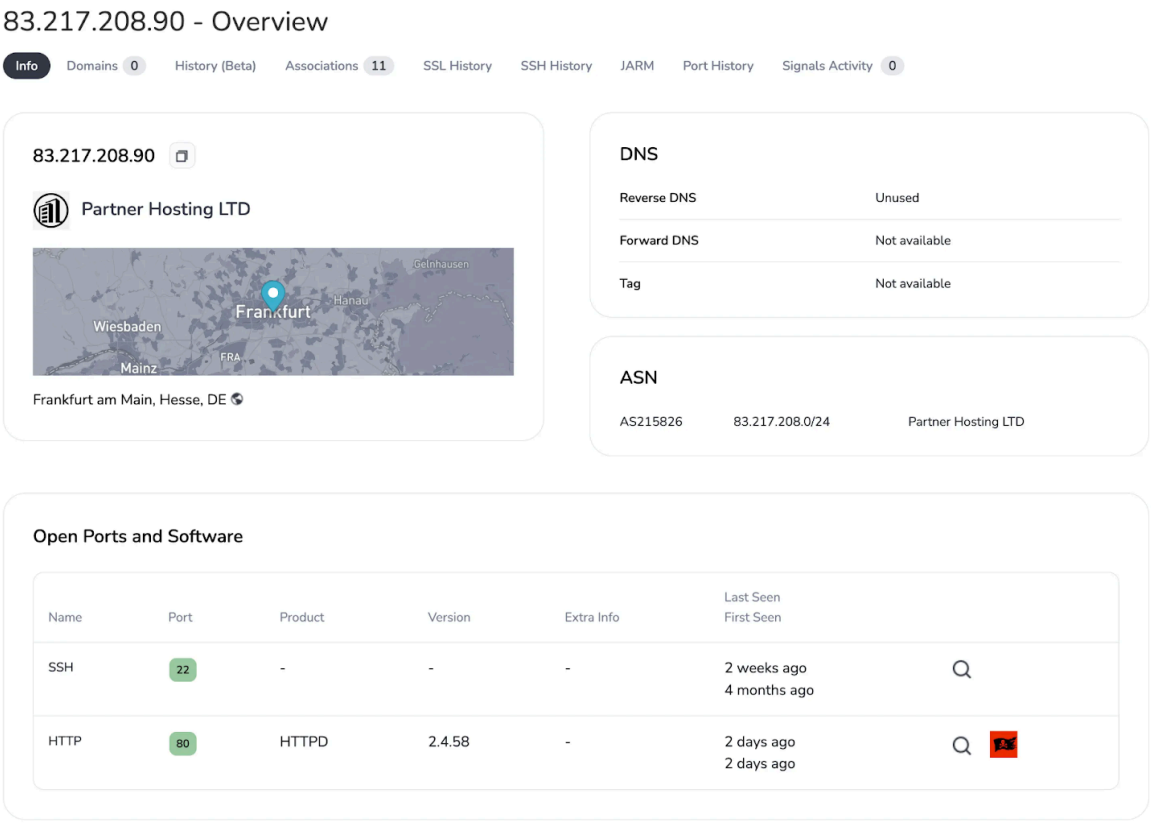

Figure 2: Hunt overview for the suspicious IP.

First, the 'Associations' tab displayed a pivot point revealing additional infrastructure. This IP address shares SSH keys (fingerprint `b48b0e3657560b80ce5e8309e422aa1655e4df2642d4a955b83945bac096b3f`) with 11 other IPs, all hosted on the Partner Hosting LTD network.

While no significant indicators were found linking these servers to other known operations, all remained active between early to mid-January 2025 before ceasing activity around February 21.

More interestingly, the icon next to the magnifying glass for port 80 identifies that Hunt has already detected this IP as hosting a Stealc C2. We currently track 23 unique command-and-control servers associated with the stealer, with detailed information fully accessible to users.

Decoy Documents and Phishing Strategy

Within the `/albion/files` folder is a document titled `'Albion.pdf.'` Upon opening the file, readers are presented with what appears to be a report from the Electronic Frontier Foundation titled:

"Electronic Report on Investigation of Virtual Asset Theft in Albion Online."

Hunt researchers have not been able to verify the document's authenticity as of this article's publication.

*The EFF is a nonprofit that advocates for digital privacy, free expression, and cybersecurity protections while challenging government surveillance and online censorship.

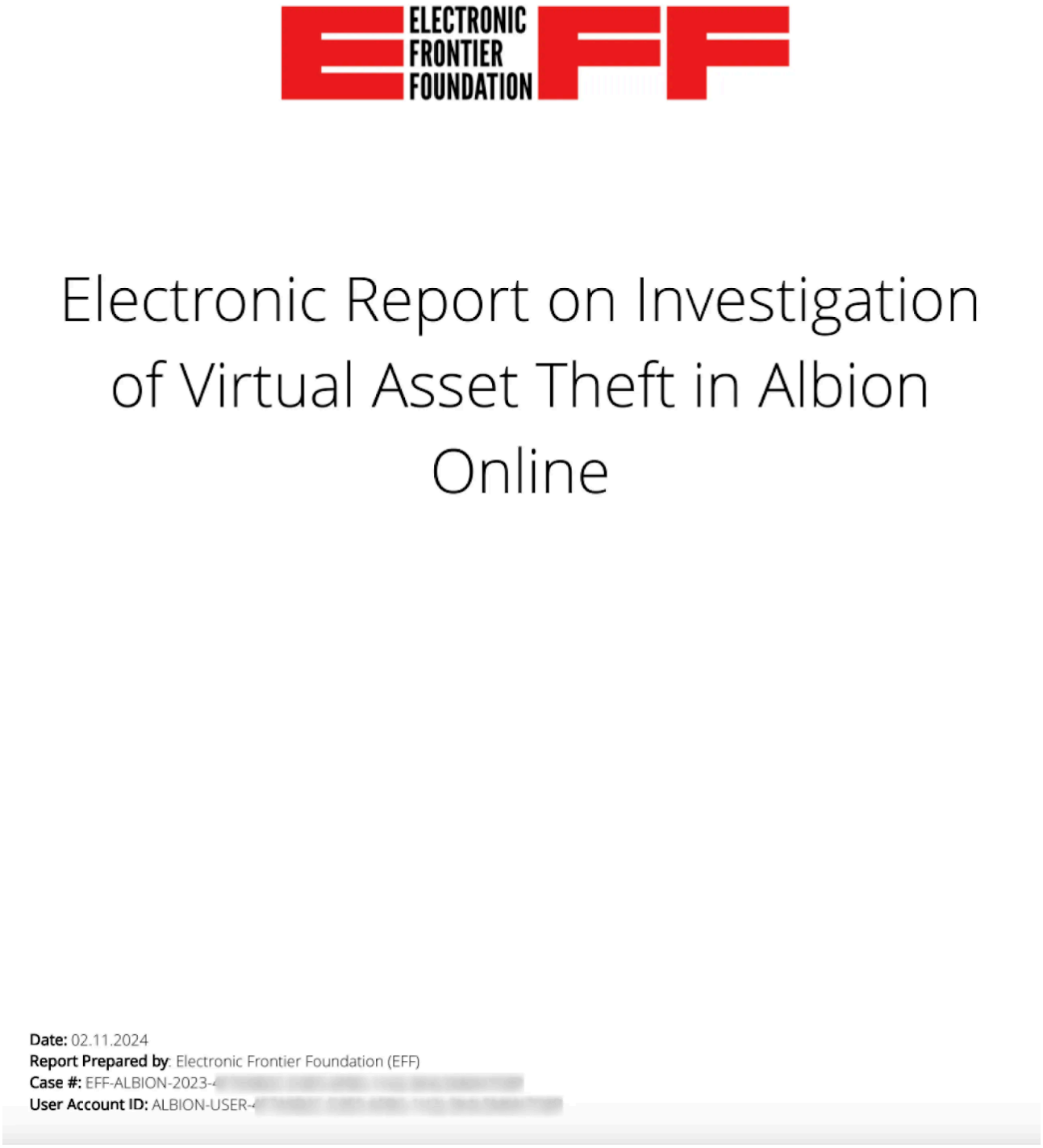

Figure 3: Suspicious PDF targeting users of the Albion online game.

The document is three pages in length, and informs the reader that EFF received a request from the administrators of the online game to analyze transactions on the individuals account.

After listing seemingly random item IDs linked to the potential victim's account, the report leads directly into the investigation results, informing the reader that unauthorized login attempts were detected and that stolen items

were transferred to their account.

The report concludes with recommended steps to further secure the user's account and leaves only the URL for the EFF contact webpage for questions.

Document Analysis

Extracting metadata from the PDF using pdfinfo revealed several notable details:

- Creation Date: Feb 18, 2025
- PDF Library: Skia/PDF m132
- Title: `localhost:36223/webpageToPdf_67b3548070585_14546073906135025492.html`
- Creator: `Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/132.0.0.0 Safari/537.36`

The above suggests the PDF was generated programmatically rather than manually created. The title field indicates it was converted from an HTML page hosted on localhost, reinforcing our belief that this was an automated process to mass-generate lures for phishing campaigns.

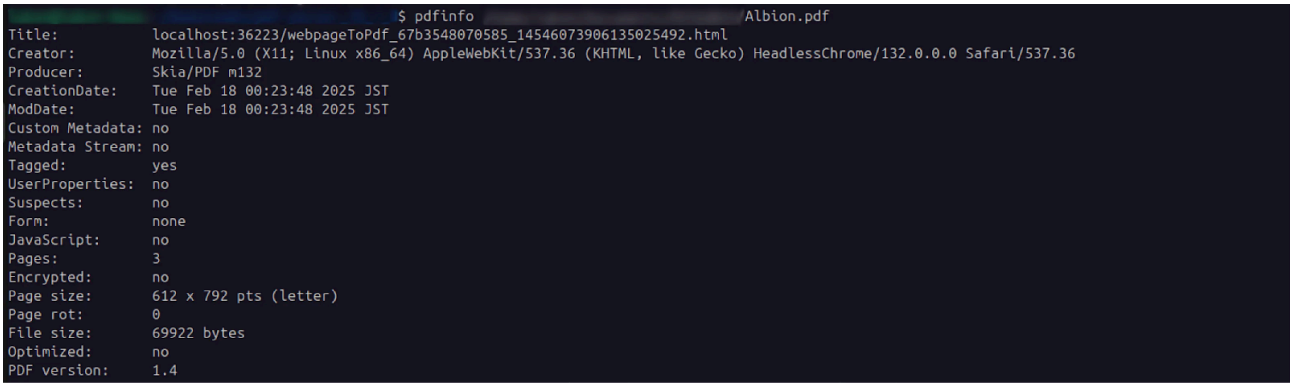

Figure 4: Results of running pdfinfo on Albion.pdf.

We won't discuss in detail the other PDF on the server, '1710407310845,' as we could not find proof of its use in the wild. The document appears to target individuals in India with DCMA takedown notices.

Of note, this document contained the below details, which were a departure from Albion.pdf:

- Title: New Applications_April 2023.xlsx
- Author: shitesh
- Creator: Acrobat PDFMaker 22 для Word ("для" translates to "for" in English)

Phishing Attempts Against Forum Users

On 28 February, a user on the Albion Online forum (forum[.]albiononline[.]com) created a thread detailing phishing messages they had received. The messages, impersonating the EFF, attempted to lure players into

engagement under the pretense of an investigation. Notably, the user ended their post by expressing frustration at the increasing volume of these messages, suggesting the campaign is widespread.

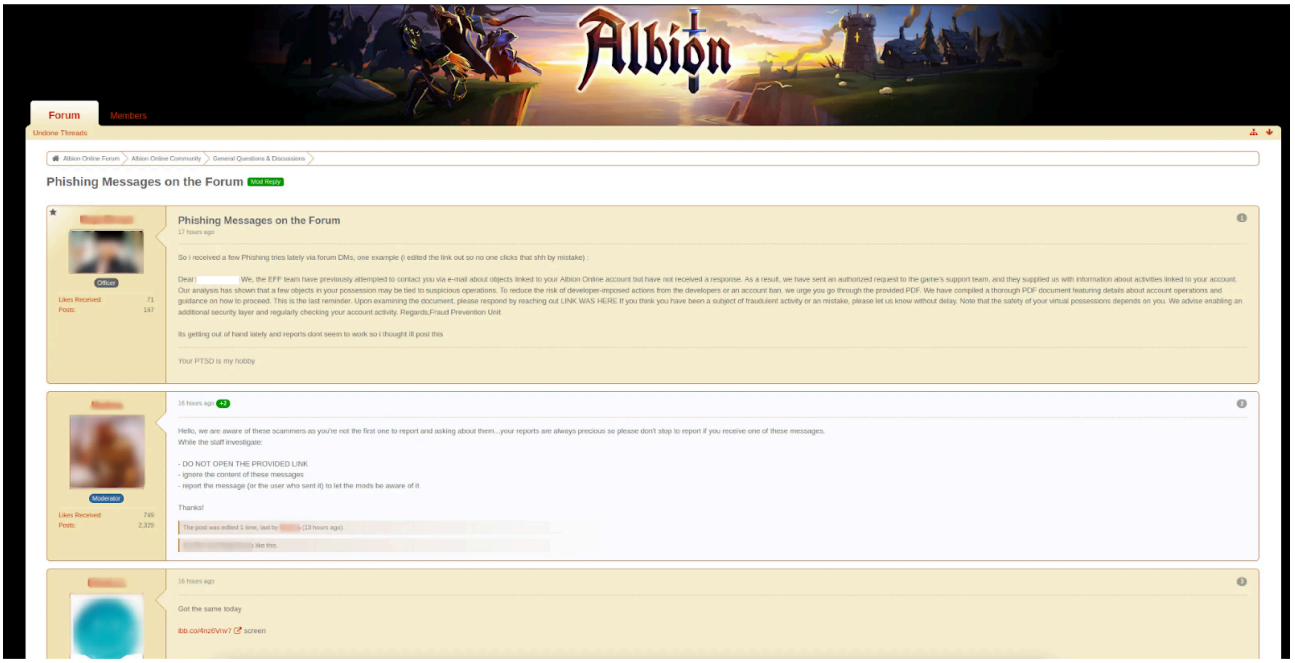

Figure 5: Screenshot of forum posts describing the phishing attempts against users.

The moderator acknowledged the attempts and provided general security recommendations as the discussion continued. An additional user reported receiving the same message and attached a screenshot showing the sender and contents.

The image revealed another piece of attacker-controlled infrastructure hosting a PDF at: `act-7wbq8j3peso0qc1.pages[.]dev/819768.pdf`

Figure 6: User-provided screenshot of the phishing message they received.

We were unable to retrieve the document as requests to the page resulted in a perpetual loading page. The sender of these messages, "reraveca1977," created their forum account the same day, February 28, before likely wiping their activity. There have been no further posts/activity from this account as of this writing.

The forum discussions confirm that phishing messages were actively circulating, aligning with findings from the open directory and leading to additional attacker-controlled infrastructure hosting decoy documents.

Malware Analysis

Looking into the /albion directory revealed a Windows shortcut (LNK) file designed to execute a PowerShell script, which facilitates malware delivery. The directory contains:

- Report-Albion-Online.lnk
- /files/Python.zip
- /files/Albion.pdf

Figure 7: Screenshot of the files contained within the /albion directory.

The LNK file executes PowerShell using an Execution Policy Bypass, running `albion.ps1` -a script located in /documents/pwsh/ on the same server. Once executed, the code retrieves Albion.pdf and Python.zip from the directory depicted in Figure 7.

The PowerShell code contains multiple comments in Russian, further supporting earlier indicators that Russian-speaking developers were involved in this operation. The script performs the following actions:

1. Opens Albion.pdf to distract the user while the malware executes in the background.
2. Extracts Python.zip and sleeps for 30 seconds.

3. Searches for `pythonw.lnk`, a secondary shortcut file.
4. If found, it executes pythonw.lnk and moves it to the Windows Startup folder, ensuring persistence on reboot.
5. Drops `albion.exe` and `12.py` from the zip archive into the TEMP folder.
    - `albion.exe` is a renamed legitimate Python 3.10.8 executable, likely used to execute the accompanying script.
    - `12.py` will be discussed below.

Reviewing the contents of `12.py` in a text editor, we found that the developer commented (in Russian) on every line of roughly 130+ lines of code.

The script includes logging, error checking, and, more importantly, two strings defined, `encoded_script_1` and `encoded_script_2`, obfuscated using zlib compression and base64 encoding. Upon decoding, both scripts are executed in the background while the main program sleeps for 30 minutes and then terminates the two processes at the end of the time.

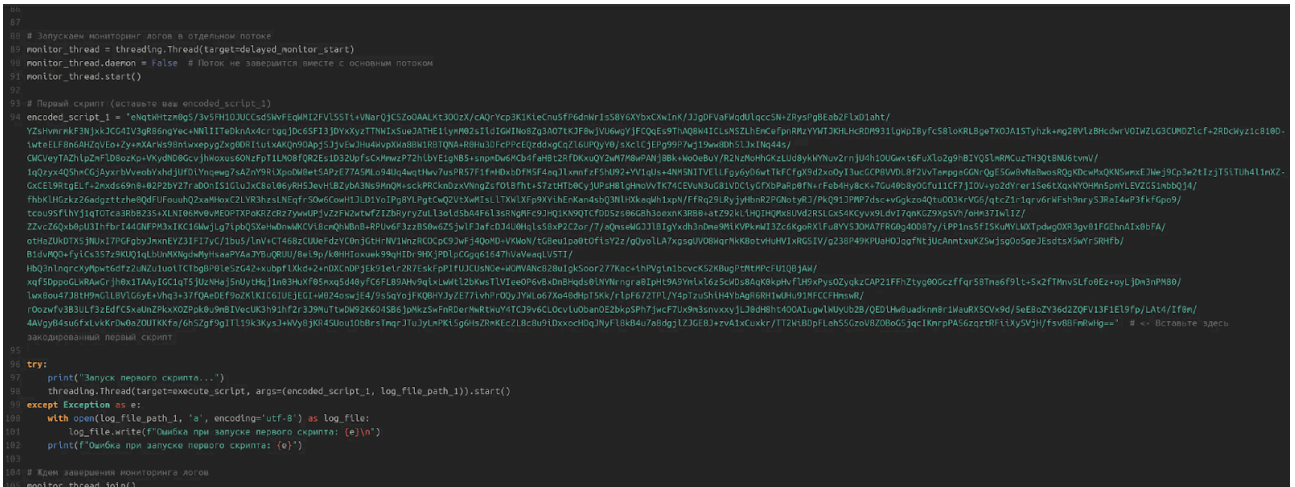

Figure 8: Snippet of 12.py.

Decoding the strings in CyberChef reveals configuration files for [Pyramid C2, an open-source framework we previously wrote about](), including tips on hunting for these servers in the wild.

Extracted C2 Infrastructure

encoded_script_1 contains the C2: 104.245.240[.]19:443

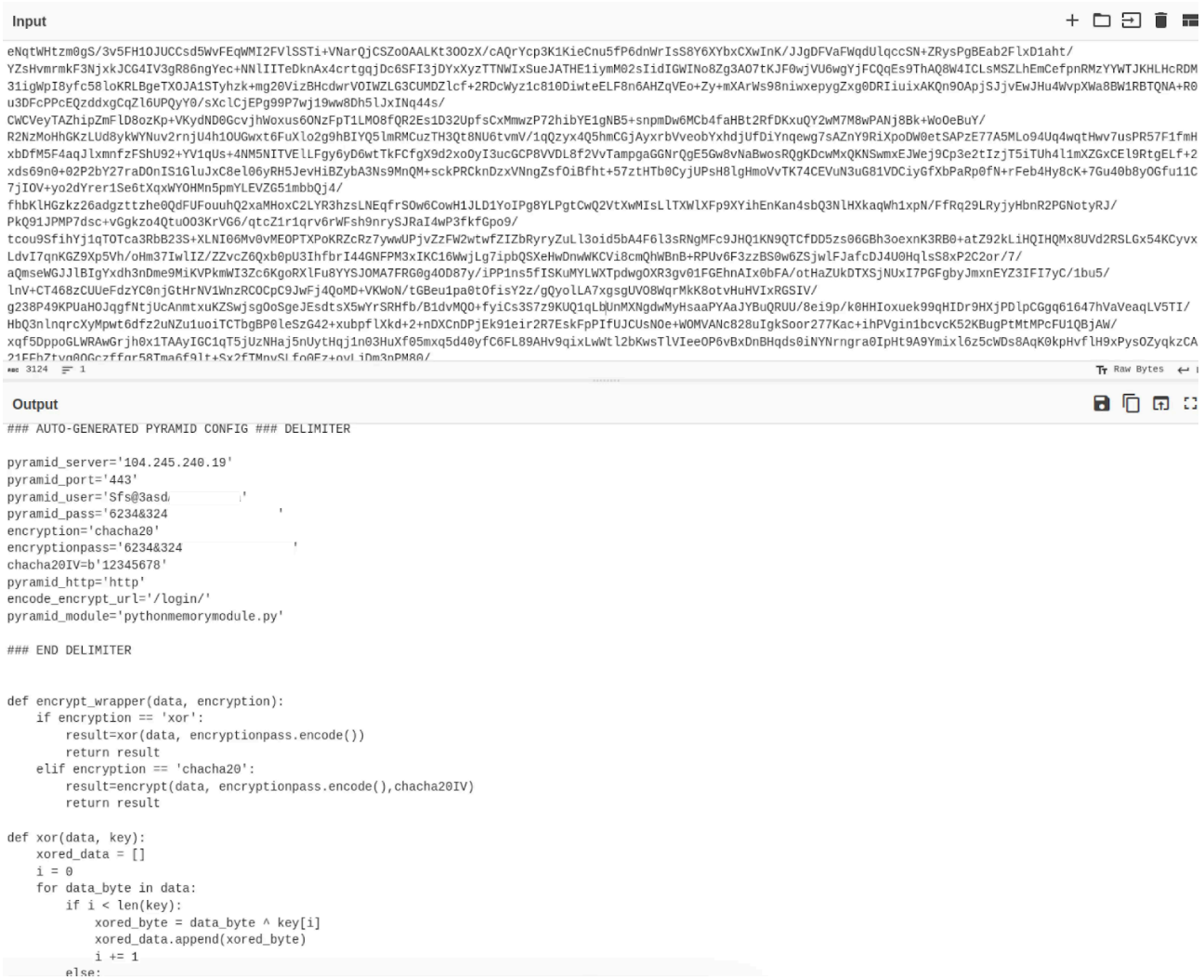

Figure 9: CyberChef decoding results for encoded_script_1.

C2 for encoded_script_2: 212.87.222[.]84:443

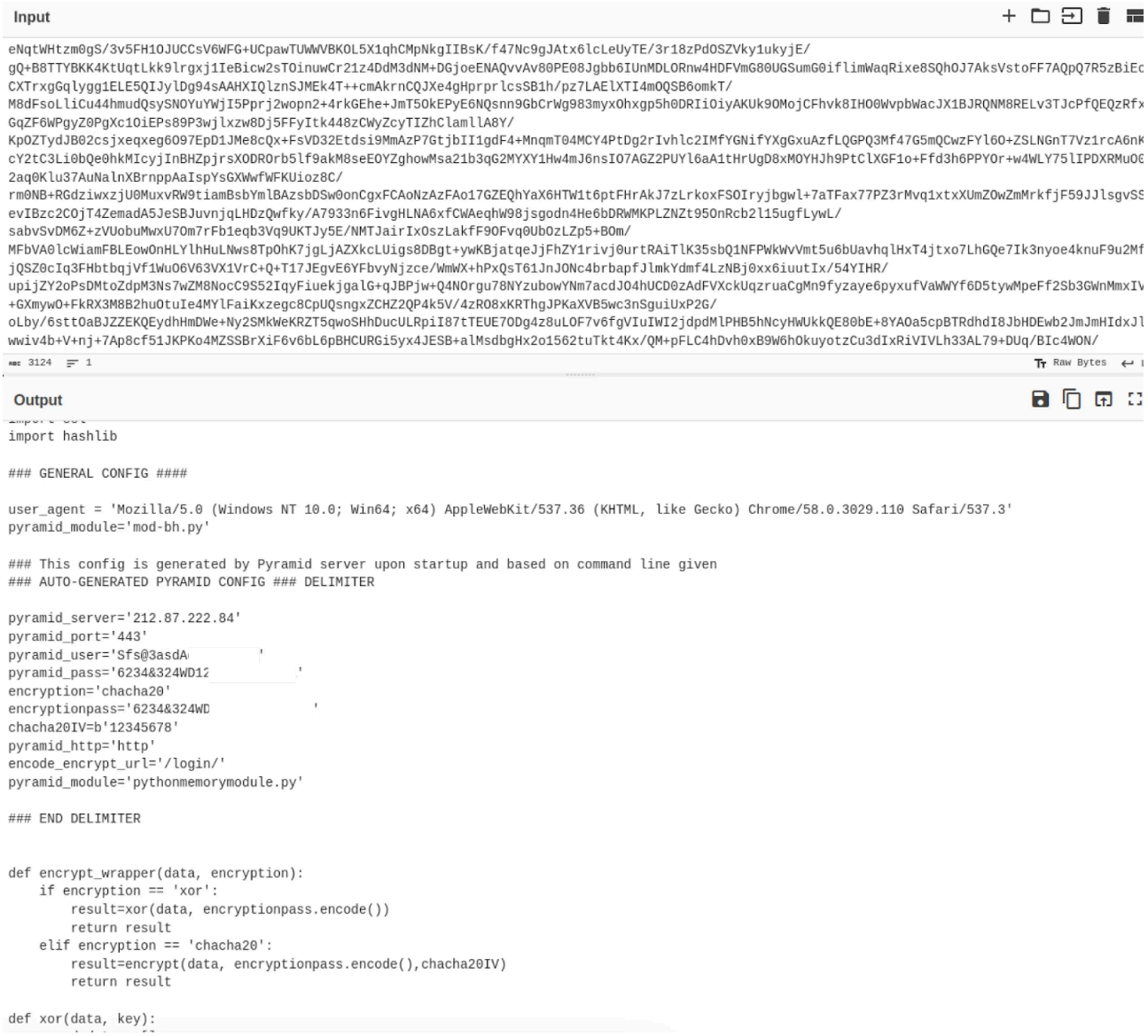

Figure 10: CyberChef decoding results for encoded_script_2.

Checking these IPs in Hunt, we were surprised to find that our scanners detected the second C2 as Pyramid C2 infrastructure roughly two weeks ago.

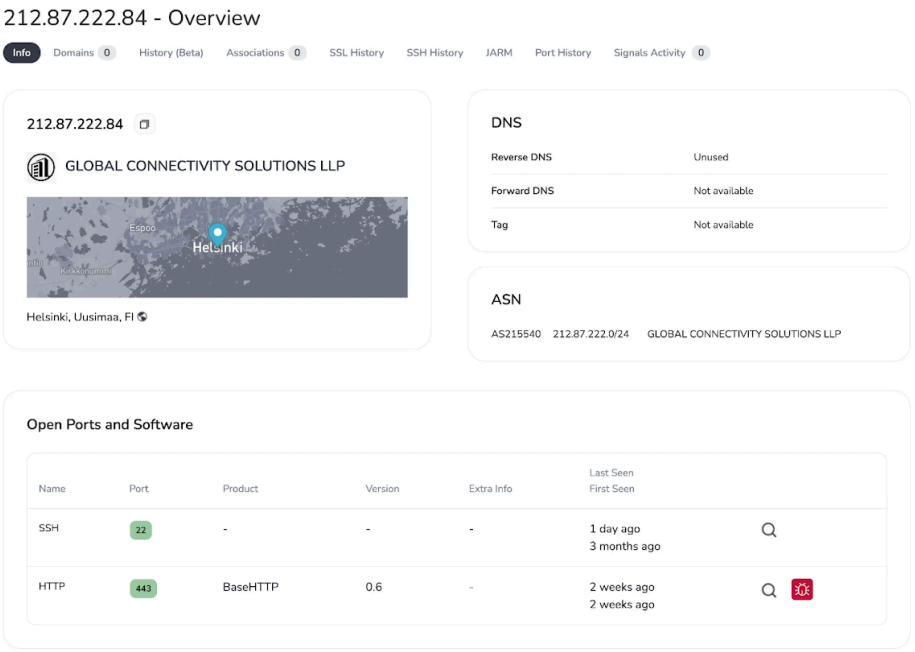

Figure 11: IP overview of 212.87.222[.]8, showing it as a Pyramid C2 in Hunt.

Pyramid C2 Behavior

Pyramid C2 is designed to deliver files encrypted, a technique that may allow it to bypass endpoint detection and response (EDR) solutions. Prior research identified its use of Basic Authentication and a distinct JSON response format, which appeared again in this case. Reviewing the network communications from a malware sandbox analysis displayed an HTTP GET request to `http[:]//104.245.240[.]19:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5`

The response is consistent with previously observed Pyramid C2 research, reinforcing its role in this campaign.

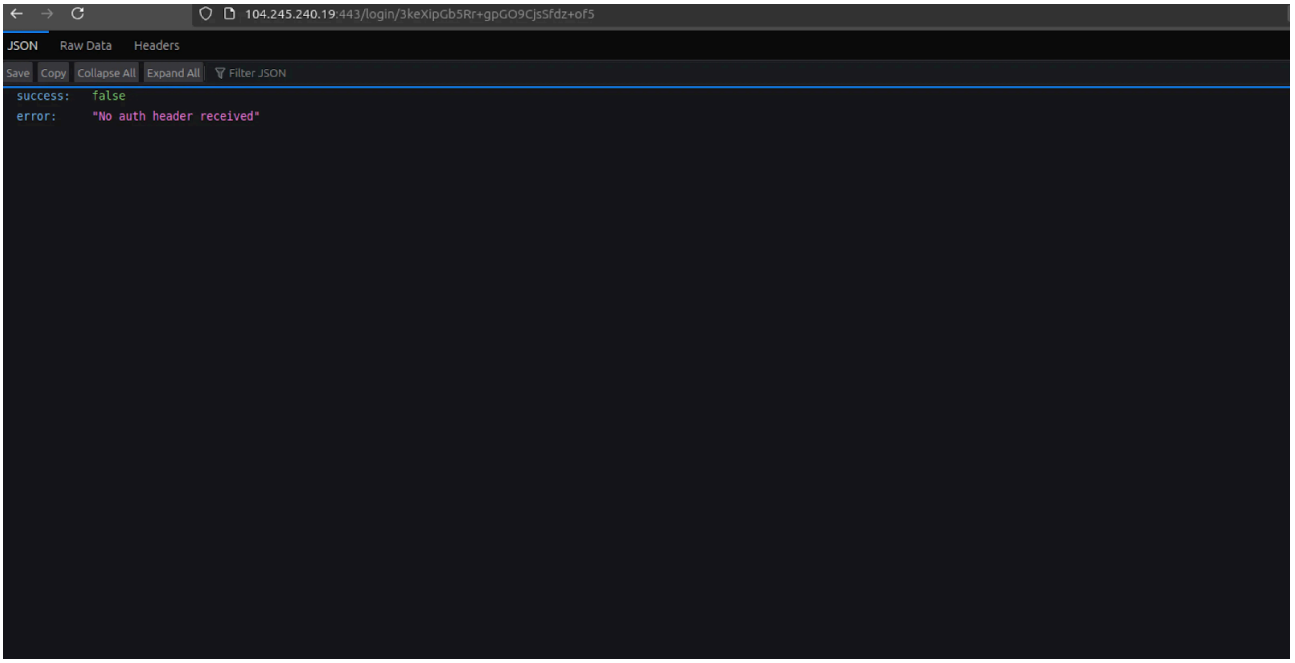

Figure 12: JSON response from the Pyramid C2 server.

Steal Communications

Following the Pyramid C2 check-in, the malware initiates multiple POST requests to `http[:]//104.245.240[.]18/d7f85cd3e24a4757.php`.

These requests, made over port 80, align with Stealc stealer's standard check-in process. The malware proceeds to interact with the Firefox and Chrome browsers, extracting stored credentials before sending them back to the C2 server.

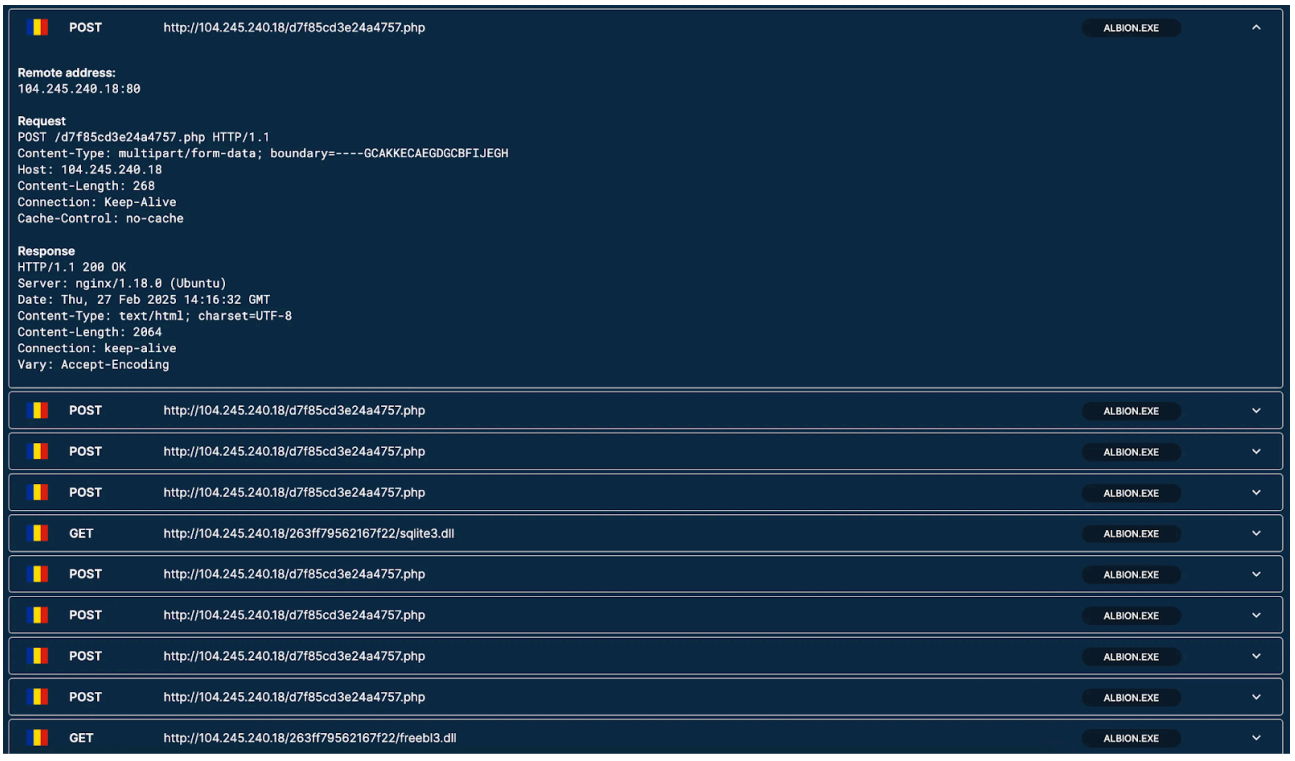

Figure 13: Snippet of the C2 communications as found by Triage.

The remaining PowerShell script, `osnova.ps1`, functions identically to the previously analyzed code and, unfortunately, does not introduce any new tactics.

Conclusion

The recent campaign targeting the Albion Online gaming community underscores the evolving tactics of cyber adversaries. By impersonating reputable organizations like the Electronic Frontier Foundation (EFF), attackers disseminated phishing messages that directed users to malicious infrastructures hosting both decoy documents and malware.

This strategy not only exploits the trust users place in well-known entities but also leverages the immersive nature of gaming environments to increase the likelihood of successful compromises.

Our investigation revealed that the threat actors mistakenly or intentionally left directories exposed where their malicious payloads were stored and distributed, a misstep that can easily go unnoticed without proactive monitoring. By analyzing these open directories, we identified the deployment of tools such as the Stealc stealer and Pyramid C2, highlighting the sophistication and resourcefulness of the adversaries.

Mitigation Strategies

To stay safe against such phishing campaigns, users are advised to:

- **Exercise caution with unsolicited communications**: Be wary of unexpected messages, especially those requesting personal information or urging immediate action.
- **Verify the authenticity of sources**: Cross-check the legitimacy of emails or messages purportedly from reputable organizations by contacting them through official channels.
- **Utilize security tools for link and attachment analysis**: Before interacting with links or downloading attachments, employ sandbox services like **URLScan** or **VirusTotal** to assess potential threats. *Ensure you aren't uploading sensitive information first.

Infrastructure Observables and IOCs

SSH Fingerprint: `b48b0e3657560b80ce5e8309e422aa1655e4df2642d4a955b83945bac096b3fb`

Network Observables and IOCs

IP Address	ASN	Notes
83.217.208[.]90	Partner Hosting LTD	Opendir/Stealc C2 -- Port 80
104.245.240[.]19	Railnet LLC	Pyramid C2
212.87.222[.]84	GLOBAL CONNECTIVITY SOLUTIONS LLP	Pyramid C2 -- Port 443
185.102.115[.]18	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90

IP Address	ASN	Notes
185.102.115[.]16	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]20	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]22	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
83.217.208[.]108	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90 Domain: immediate-zenar[.]net
185.102.115[.]17	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]11	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]14	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]19	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]21	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
185.102.115[.]15	Partner Hosting LTD	Shared SSH keys w/ 83.217.208[.]90
N/A	CloudFlare, Inc.	act-7wbq8j3peso0qc1.pages[.]dev

Host Observables and IOCs

Filename	SHA-256
albion.ps1	a524d1acb0692fc90e20548d4bea29b4996c4113420942e43addd8c5609e29a4
osnova.ps1	4dcca5d3269eb44f3cf7af62c0da3b6acab67eb758c9fb2f5cc5b1d13a7286f7
Report-Albion-Online.lnk	cf8065df8674c2a09b3cb94f308c48f04a8664b066dd5107b117e99062f5621e
terms-of-service.pdf.lnk	cf8065df8674c2a09b3cb94f308c48f04a8664b066dd5107b117e99062f5621e
1710407310845.pdf	a7e617783d7f1b0079c605126fba074ee7ee431077cd97d391e41f364a0afe1b
Albion.pdf	b7612517337a7a3678e7f138dab36cd8a42e843f0536c0ccb74a2b0aa2224505
Python.zip (/albion/files/)	f60c212190a69149480586c9c9e340605dfa4b16a571f34b2ce31db4d0f7659a
12.py	aa89169a746709de1fd18510fc6e8850a863ebcc419ba0ca21fa479e59730c6e
albion.exe	56f1a4d528fdee439b5b747c00d0b4a61b2c0bd8783e0abdb87c6d969a8f1e91
Python.zip (/files/zip/)	3d3559a29f94bb349b928518dcf0c3757813e32195d16880e94169ca9affdede

---

Source: https://hunt.io/blog/russian-speaking-actors-impersonate-etf-distribute-stealc-pyramid-c2