APT group Lorec53 (Lori Bear) recently launched a large-scale cyber attack on Ukraine

blog.nsfocus.net/apt-lorec53-20220216

Fuying Lab

1. Summary of the event

Recently, NSFOCUS Fuying Lab has captured a large number of phishing file attacks against Ukraine, and the associated malicious files include pdf, doc, cpl, lnk and other types. After analysis, we confirmed that this series of fishing activities came from the APT organization Lorec53 (Chinese name: Lori Xiong). During the period from the end of 2021 to February 2022, the organization used a variety of attack methods to deliver a variety of phishing documents to key state institutions such as the Ministry of Defense, Ministry of Finance, embassies, state-owned enterprises, and public medical facilities of Ukraine to collect organizational Personnel information-based network attack activities.

2. Organizational Background

Lorec53 (Chinese name: Lori Xiong) is a new type of APT organization first identified and named by NSFOCUS Fuying Laboratory, active in Eastern Europe. The Ukrainian Computer Emergency Response Center identified the organization as UAC-0056 in a recent report (https://cert.gov.ua/article/18419). Fuying Lab found that the group's captureable spy Trojans first appeared in 2020, and began to organize large-scale cyber espionage attacks against Ukraine and Georgia in early 2021.

Lorec53 exposed a large number of Russian hacker characteristics in terms of attack tools, domain name registration information, asset location, etc., and its attack targets are also closely related to Russia's national interests. A study of Lorec53's development trajectory found that the organization was suspected of being employed by other high-level espionage organizations to gain revenue by undertaking state-level espionage attacks or selling confidential government documents.

Lorec53 has strong infiltration ability and changeable attack methods. It can organize large-scale and high-density phishing attacks. It is also good at learning from other organizations' social engineering technology and network resource management methods.

At present, the victims affected by the Lorec53 attack include users of the National Bank of Iran, Georgia's Epidemic Prevention and Health Department, Ukraine's Ministry of Defense, the Presidential Office, the Ministry of the Interior, and the Border Guard.

For more reports related to the organization, please refer to the analysis report of Fuying Lab on the organization (http://blog.nsfocus.net/lorec-53/, http://blog.nsfocus.net/lorec53-nsfocus/ , http://blog.nsfocus.net/apt-lorec/)

3. Overview of events

Lorec53's current round of attacks lasted for a long time, with a wide range of targets, and the attack methods had obvious organizational characteristics.

Lorec53 continued the previous decoy design methods in this round of attacks, constructing phishing including Ukrainian government documents that mask some information, shortcut files with Ukrainian titles and camouflaged extensions, and cpl files with Ukrainian file names. bait, and distribute these bait masquerading as a member of a credible organization.

bait name	translate
до рішення Ради національної безпеки і оборони України від 7 вересня 2021 року "Про внесення зміни до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"	According to the decision of the National Security and Defense Council of Ukraine of September 7, 2021 "On the modification of special economic and other restrictions on individuals (sanctions)"
Повідомлення про вчинення злочину	crime report
Скарга на абонента у судовому порядку 12-01-2022	Complain to the court orderer 12-01-2022
Петиція щодо повернення майна громадянам України	Petition to return property to Ukrainian citizen
Приклад заповнення пояснювальної текст заповнюється вручну	The example of filling in the description text is filled in manually
Роз'яснення щодо коректності ведення електронних медичних записів в електронній системі охорони здоров'я , а пророж	Clarify the correctness of electronic medical records in the electronic health system, and the impact of the law

Table 3.1 Some fishing lures names and translations

In this series of phishing attacks, Lorec53 attackers mainly used three domain names, 3237.site, stun.site, and eumr.site, as download servers for various phishing files. The site domain is one of the commonly used domains of Lorec53. As of February 11, some URLs are still accessible and can deliver payload files, indicating that this round of attacks is still ongoing.

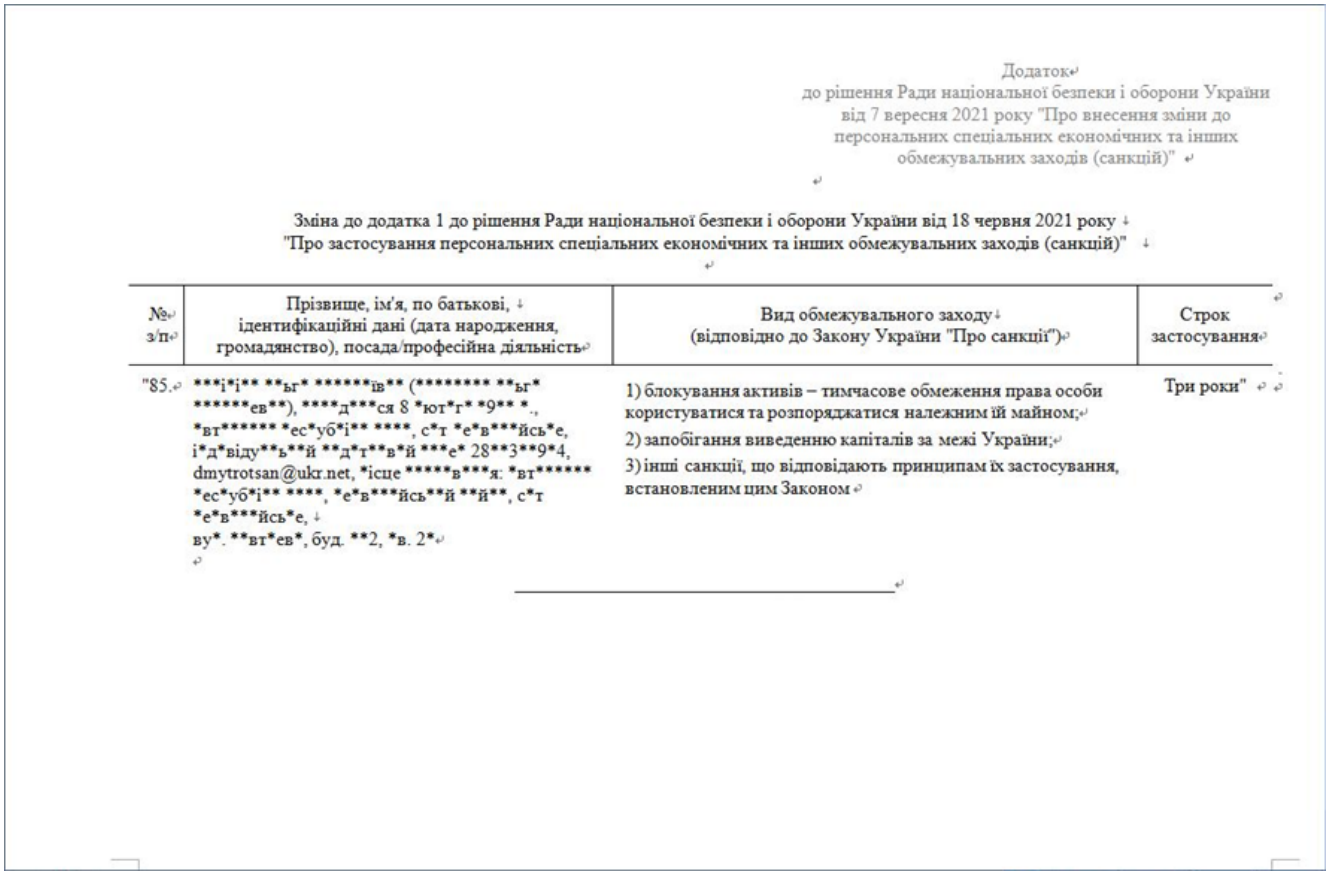
In this series of attacks, Lorec53 directly wrote the collected mailboxes of key Ukrainian facilities into the decoy text. Judging from Lorec53's past behavior, such an operation may be used to increase the credibility of the bait. This feature also provides a basis for investigators to confirm the attack coverage.

This time, Lorec53 still uses known Trojan programs, including LorecDocStealer (also known as OutSteel), LorecCPL, SaintBot, and packaged these Trojan programs as much as possible.

4. Event Analysis

4.1 Attack event one

First from phishing attacks occurred in late 2021, Lorec53 constructed a lot to "до рішення Ради національної безпеки і оборони України від 7 вересня 2021 року" Про внесення зміни до персональних спеціальних економічних та інших обмежувальних заходів (санкцій) "" the title of the fishing documentation. The contents of these phishing documents refer to a presidential decree adopted by the National Security and Defense Council of Ukraine on September 7, 2021, claiming that special asset restrictions and sanctions will be imposed on a specific person.



Додаток
до рішення Ради національної безпеки і оборони України
від 7 вересня 2021 року "Про внесення зміни до
персональних спеціальних економічних та інших
обмежувальних заходів (санкцій)"

Зміна до додатка 1 до рішення Ради національної безпеки і оборони України від 18 червня 2021 року
"Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"

№ з/п	Прізвище, ім'я, по батькові, ідентифікаційні дані (дата народження, громадянство), посада/професійна діяльність	Вид обмежувального заходу (відповідно до Закону України "Про санкції")	Строк застосування
"85.	***і*і** **ьг* ******ів** (******** **ьг* ******ев**), ****д***ся 8 *ют*т* *9** *., *вт****** *ес*уб*і** ****, с*т *е*в***йсь*е, і*д*віду**ь**й **д*т**в*й ***е* 28**3**9*4, dmytrotsan@ukr.net, *ісце *****в***я: *вт****** *ес*уб*і** ****, *е*в***йсь**й **й**, с*т *е*в***йсь*е, ву*. **вт*ев*, буд. **2, *в. 2*	1) блокування активів – тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном; 2) запобігання виведенню капіталів за межі України; 3) інші санкції, що відповідають принципам їх застосування, встановленим цим Законом	Три роки"

Figure 4.1 Phishing document titled “Restrictions (sanctions) on modification of personal special economics”

According to the relevant decrees of Ukraine, the Ukrainian Security Service, the Cabinet and other state departments can modify the document "Restriction Measures (Sanctions) for Individual Special Economics and Others" to add or delete specific economic sanctions. In the amendment on September 7, the economic sanctions object numbered 85 was added.

It should be noted that the content of the phishing file is roughly the same as the content of the attachment in the presidential decree published by the Ukrainian government (https://zakon.rada.gov.ua/laws/show/n0062525-21#Text), but the Lorec53 attacker The following changes have been made to the text:

1. The use of asterisks obscures specific citizen information;

This is Lorec53's usual practice when building phishing documents, in this way to lure victims to enable the editing function of the document, and then run the macro code in the document

2. Added email addresses that do not exist in the original text;

The Lorec53 attacker added government email addresses to the original citizen information without fuzzing. After query, the "DMYTROTSAN@ukr.net" address in the sample fishing email does not matter, but point to the Ukrainian Wolin Treasury (головне управління державної клужбееіккїї у уобииііііни у іііі їїїїл іі).

The above two changes indicate that the target of Lorec53's phishing operation is the Ukrainian government, and the email address in the phishing email is likely to be the same as the victim's email address. Fuying Lab counted the mailbox information in all captured phishing emails to evaluate the impact of this Lorec53 phishing attack.

Mail	Corresponding institution or enterprise
dmytrotsan@ukr.net	Ministry of Finance of Volin Oblast, Ukraine
emb_sm@mfa.gov.ua	Embassy of Ukraine in Serbia
kev_dnipro@post.mil.gov.ua	Ministry of Housing and Operations of Dnipro Oblast, Ukraine
zorkz@mil.gov.ua	Joint Operations Command of the Armed Forces of Ukraine
office.skdvs@ks.treasury.gov.ua	Ministry of Finance, Skadovsk District, Kherson Oblast, Ukraine
sadovska-ii@utg.ua	UKRTRANSGAZ AG
ufg.csc@ufg@.com.ua	Ukrainian Financial Group
pokrovske_tckspdp@post.mil.gov.ua	Staffing and Social Support Center of the Third Sector, Sinernikivsky District, Dnipropetrovsk Oblast, Ukraine
zmievkazna@ukr.net	Ministry of Finance, Zmiv District, Kharkiv Region, Ukraine
kuzmych@naftogaz.com	Ukrainian Naftogaz Joint Stock Company
zvernmou@ukr.net	Department of Civil Work and Access to Public Information of the Ministry of Defense of Ukraine
perevod@pivdenny.ua	Pivdennyi Bank
kevzp@post.mil.gov.ua	Press and Information Department of the Ministry of Defense of Ukraine
i.kozarovska@ukrburgas.com.ua	UkrGasVydobuvannya JSC Branch Ukrburgaz
kanivkamvo@ukr.net	Department of Education, Executive Committee, Kanif City Council, Cherkassy Region
t.litovko@direkcy.atom.gov.ua	VP KB ATOMPRILAD DP NAEK ENERGOATOM
timm93@ukr.net	Ministry of Finance of Vasilevka, Zaporozhye Oblast, Ukraine
office.cherv@lv.treasury.gov.ua	Ministry of Finance of Chervonohrad, Lviv Oblast, Ukraine
kevplt_kes@post.mil.gov.ua	
babich-ka@utg.ua	UKRTRANSGAZ AG
kevplt_zhytlo@post.mil.gov.ua	

corruption@direkcy.atom.gov.ua	Ukrainian state-owned enterprise "NNEGC" Energoatom"
emb_jp@mfa.gov.ua	Embassy of Ukraine in Japan
genotdel@odessa.gov.ua	Odessa Oblast Administration of Ukraine
zoya_skl@ukr.net	Ministry of Finance, Oleshandrivka District, Kirovolad Oblast, Ukraine
ruslan.marunia@bank.gov.ua	Department of Currency Circulation, National Bank of Ukraine
malyshev.tender@ukroboronprom.com	Maleshev Plant
emb_pl@mfa.gov.ua	Embassy of Ukraine in Poland
irudksu@i.ua	Ministry of Finance, Irshava District, Zakarpatia Region, Ukraine
emb_lt@mfa.gov.ua	Embassy of Ukraine in Lithuania
emb_fi@mfa.gov.ua	Embassy of Ukraine in Finland
abashinao@kv.treasury.gov.ua	Ministry of Finance of Kiev, Ukraine
1545@ukc.gov.ua	Ukrainian Government Hotline 1545
tetiana.rupcheva@bank.gov.ua	Monetary Policy and Market Operations Department of the National Bank of Ukraine
pr@atom.gov.ua	Ukrainian state-owned enterprise "NNEGC" Energoatom"
1201_buhg@dmsu.gov.ua	Dnipropetrovsk Oblast Immigration Office of Ukraine
kherson_kev@post.mil.gov.ua	Ministry of Housing and Operations of Kherson Oblast, Ukraine
sholyak27@ukr.net	Ministry of Finance of the Transcarpathian State of Ukraine
office@novator-tm.com	Ukrainian state-owned enterprise "Novator"
mps@industrialbank.ua	AKB Industrialbank PAT
v.harchenko@mil.gov.ua	

Table 4.1 Email addresses and corresponding organizations in phishing emails

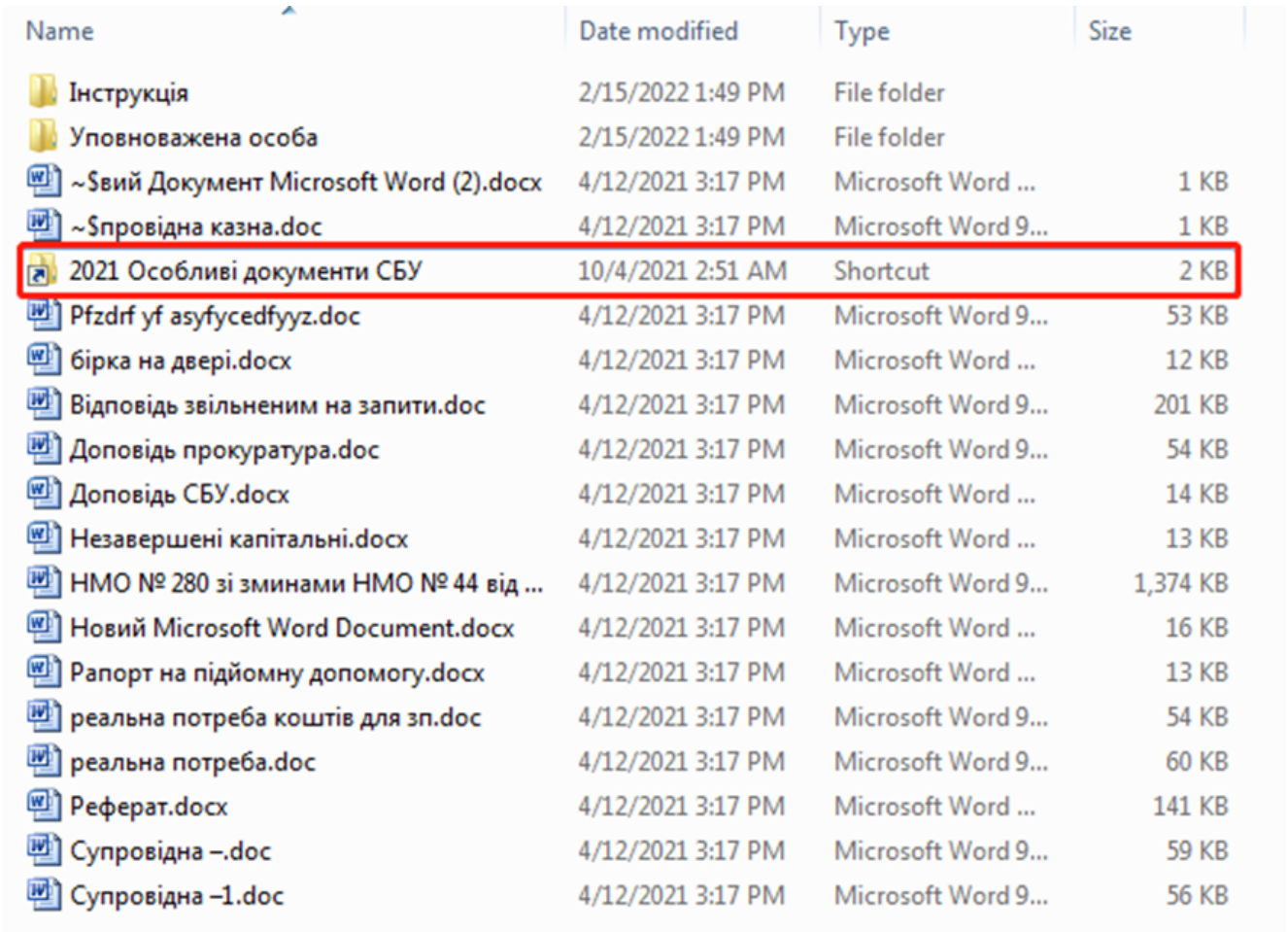
The associated information of these email addresses shows that the main goal of Lorec53 in this phishing attack is early detection and information collection, which is the same as the organization's previous activities.

The malicious macro in these phishing documents will download and run the Trojan at http[:]//3237[.]site/test01.exe. Also associated with this domain is a phishing shortcut file named "Особливі документи СБУ.lnk" (a special file of the Ukrainian Security Service.lnk), and a known Lorec53 Trojan named "08-2021.cpl" LorecCPL, so The direct correlation of this domain name to Lorec53 can be confirmed.

```
.text:0181B4F6 ; ---------------------------------------------------------------------------
.text:0181B4FB aWinhttpconnect db 'WinHttpConnect',0
.text:0181B50A ; ---------------------------------------------------------------------------
.text:0181B50A
.text:0181B50A loc_181B50A:                            ; CODE XREF: .text:0181B4F6↑p
.text:0181B50A                 push    ebp
.text:0181B50B                 call    esi
.text:0181B50D                 pop     ecx
.text:0181B50E                 push    0
.text:0181B510                 push    50h ; 'P'
.text:0181B512                 call    sub_181B52B
.text:0181B512 ; ---------------------------------------------------------------------------
.text:0181B517 a3237Site:
.text:0181B517                 text "UTF-16LE", '3237.site',0
.text:0181B52B
.text:0181B52B ; =============== S U B R O U T I N E =======================================
.text:0181B52B
.text:0181B52B
.text:0181B52B sub_181B52B     proc near               ; CODE XREF: .text:0181B512↑p
.text:0181B52B                 push    ecx
.text:0181B52C                 call    eax
.text:0181B52E                 push    eax
.text:0181B52F                 call    loc_181B547
.text:0181B52F sub_181B52B     endp ; sp-analysis failed
.text:0181B52F
.text:0181B52F ; ---------------------------------------------------------------------------
.text:0181B534 aWinhttpopenreq db 'WinHttpOpenRequest',0
.text:0181B547 ; ---------------------------------------------------------------------------
.text:0181B547
.text:0181B547 loc_181B547:                            ; CODE XREF: sub_181B52B+4↑p
.text:0181B547                 push    ebp
.text:0181B548                 call    esi
.text:0181B54A                 pop     ecx
.text:0181B54B                 push    0
.text:0181B54D                 push    0
.text:0181B54F                 push    0
.text:0181B551                 push    0
.text:0181B553                 call    loc_181B570
.text:0181B553 ; ---------------------------------------------------------------------------
.text:0181B558 aTest01Exe:
.text:0181B558                 text "UTF-16LE", '/test01.exe',0
.text:0181B570 ; ---------------------------------------------------------------------------
```

Figure 4.2 The main logic part of the LorecCPL Trojan

A malicious shortcut file named "Особливі документи СБУ.lnk" was also used by Lorec53 in several attacks. Lorec53 constructs named "sadovska-iiutg.ua.zip", "feukslpost.mil.gov.ua.zip", "n.lashevychdirekcy.atom.gov.ua.zip", "feukslpost.mil.gov.ua. zip", etc., and put this malicious shortcut file in the same folder as a large number of non-toxic decoy files, expecting the victim to run the malicious file while browsing file by file. This baiting method also fits with Lorec53's historical approach.



Name	Date modified	Type	Size
Інструкція	2/15/2022 1:49 PM	File folder	
Уповноважена особа	2/15/2022 1:49 PM	File folder	
~$вий Документ Microsoft Word (2).docx	4/12/2021 3:17 PM	Microsoft Word ...	1 KB
~$провідна казна.doc	4/12/2021 3:17 PM	Microsoft Word 9...	1 KB
2021 Особливі документи СБУ	10/4/2021 2:51 AM	Shortcut	2 KB
Pfzdrf yf asyfycedfyyz.doc	4/12/2021 3:17 PM	Microsoft Word 9...	53 KB
бірка на двері.docx	4/12/2021 3:17 PM	Microsoft Word ...	12 KB
Відповідь звільненим на запити.doc	4/12/2021 3:17 PM	Microsoft Word 9...	201 KB
Доповідь прокуратура.doc	4/12/2021 3:17 PM	Microsoft Word 9...	54 KB
Доповідь СБУ.docx	4/12/2021 3:17 PM	Microsoft Word ...	14 KB
Незавершені капітальні.docx	4/12/2021 3:17 PM	Microsoft Word ...	13 KB
НМО № 280 зі змінами НМО № 44 від ...	4/12/2021 3:17 PM	Microsoft Word 9...	1,374 KB
Новий Microsoft Word Document.docx	4/12/2021 3:17 PM	Microsoft Word ...	16 KB
Рапорт на підйомну допомогу.docx	4/12/2021 3:17 PM	Microsoft Word ...	13 KB
реальна потреба коштів для зп.doc	4/12/2021 3:17 PM	Microsoft Word 9...	54 KB
реальна потреба.doc	4/12/2021 3:17 PM	Microsoft Word 9...	60 KB
Реферат.docx	4/12/2021 3:17 PM	Microsoft Word ...	141 KB
Супровідна –.doc	4/12/2021 3:17 PM	Microsoft Word 9...	59 KB
Супровідна –1.doc	4/12/2021 3:17 PM	Microsoft Word 9...	56 KB

Figure 4.3 Decoy zip file directory, red is the malicious shortcut file

From the name of the compressed package, it can be seen that the target of this attack is similar to and partially overlapped with the aforementioned personal economic sanctions phishing document, which can be speculated to be the same series of attacks.

4.2 Attack event 2

Another phishing attack occurred between December 2021 and February 2022.

In early February, Lorec53 produced a series of phishing documents with the theme of "Повідомлення про вчинення злочину" (criminal report), which were delivered in the form of pdf vulnerability files and docx malicious macro files.

The phishing document named "Повідомлення про вчинення злочину.pdf" (criminal report.pdf) displayed the words "please update" when opened.

Figure 4.4 Phishing document titled "Crime Report"

This is the commonly used pdf decoy construction method for Lorec53, the file is used to download the link https[:]//get.adobe.com.uk.reader.updateadobeacrobatreaderdc.stun[.]site/get.adobe.com.uk.reader/ Trojan programs corresponding to get.adobe.com.uk.reader/get.adobe.com.uk.reader/AdobeAcrobatUpdate.exe. The trojan is a packaged LorecDocStealer (also known as OutSteel) trojan, which is used to steal various document files on the victim's host. The shell wrapping technique used by Lorec53 on this Trojan is very common in AgentTesla spyware.

A similar phishing document "Повідомлення про вчинення злочину (Білоус Олексій Сергійович).docx" was opened to display images and textual information with obvious Lorec53 lure build characteristics.

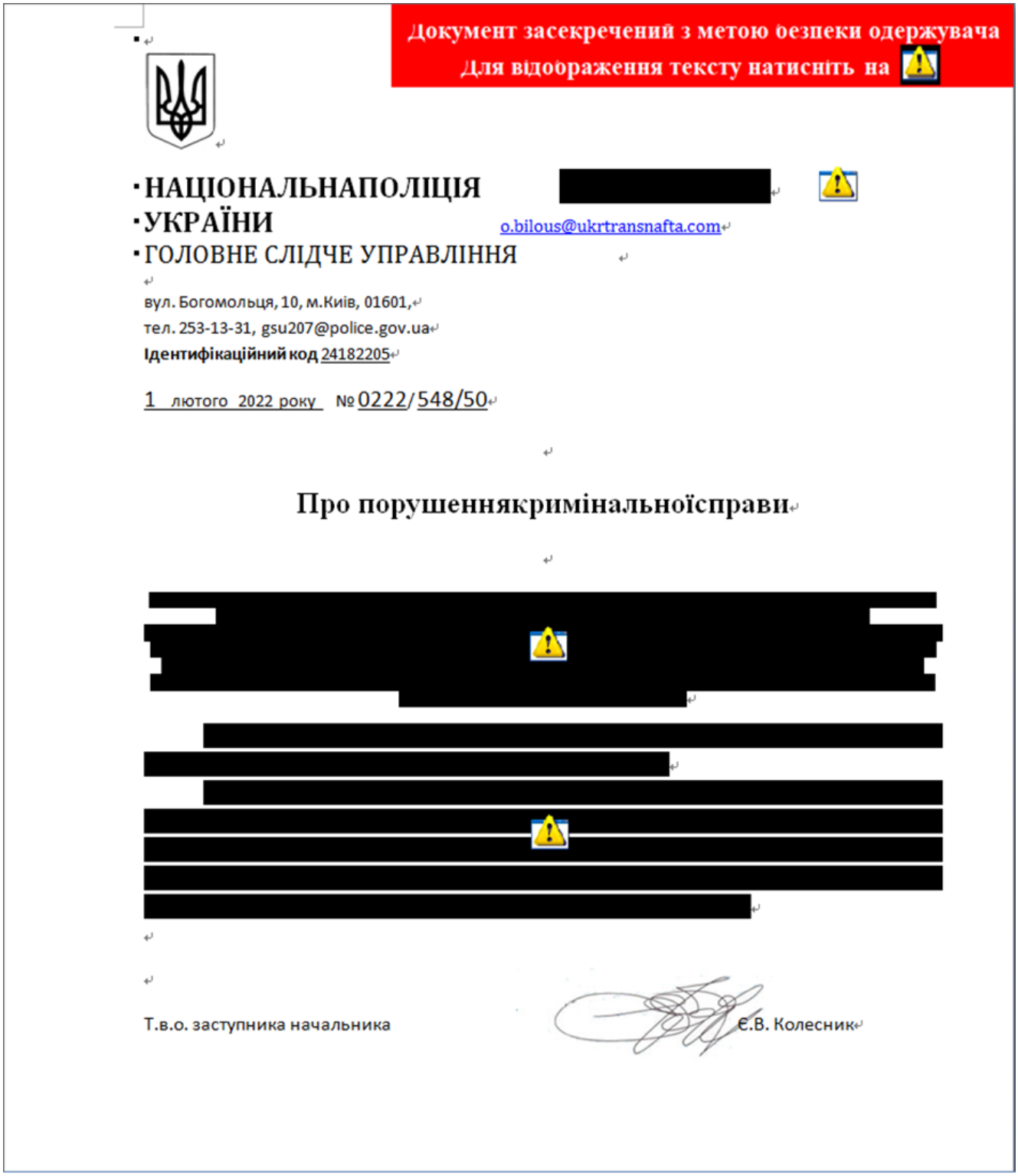


Figure 4.5 Phishing document titled “Crime Report (Belous Alexei Sergeevich)”

The document is disguised as a document of the investigation department of the Ukrainian National Police. By blocking the image and red prompt information, it induces the victim to click the icon ole object in the document, and then execute the js script, download and run https[:]//cdn.discordapp[.] Trojan in com/attachments/932413459872747544/938291977735266344/putty.exe. The Trojan is also the packaged LorecDocStealer (OutSteel) Trojan.

With reference to the aforementioned attack incident, the unobfuscated email address o.bilous@ukrtransnafta.com in this document may be the email address of the direct victims of this incident. The affiliate company of this mailbox is UKRTRANSNAFT Joint Stock Company of Ukraine.

In addition, the docx phishing document was also captured and published by the Ukrainian Computer Emergency Response Center (CERT-UA). In related reports (https://cert.gov.ua/article/18419), CERT-UA referred to the Lorec53 organization as the UAC-0056.

Through correlation analysis of the stun.site domain name that appeared in this attack, Fuying Lab confirmed a variety of decoy files released by Lorec53 from December 2021. These files include .lnk, .cpl, .rar and other formats, all of which are known decoy forms of Lorec53. The main function is to obtain and run the subsequent LorecDocStealer (OutSteel) Trojan from stun.site.

4.3 Attack event 3

The third attack incident mainly revolved around the domain name eumr[.]site.

In early 2, Lorec53 structure called "Роз'яснення щодо коректності ведення електронних медичних записів в електронній системі охорони здоров'я, а також впливу прави" (electronic medical system to clarify the validity of electronic medical records, as well as the impact of the law) bait , delivered in the form of a zip archive. Based on the name of the decoy, it can be speculated that the file comes from an attack campaign against the Ukrainian medical system, which overlaps with previous Lorec53 targets.

The malicious shortcut file in the compressed package is a typical Lorec53 phishing lure, used to download and run the Trojan program located at http[:]//eumr[.]site/up74987340.exe, which is the LorecDocStealer (OutSteel) spy Trojan.

The file properties show that these decoy files were modified on January 31, 2022.

The domain names and CnC communication addresses that appeared in this incident can be linked to a number of other malicious programs, which are various forms of wrappers for the LorecDocStealer (OutSteel) spyware.

V. Summary

The multiple attacks discovered this time are all part of the large-scale cyber attack activities carried out by Lorec53 (Lori Bear) in different time periods from the end of 2021 to February 2022 against Ukrainian government departments, the military, and state-owned enterprises. The main targets of these attacks are still early detection and information collection, and they show the distinctive characteristics of Lorec53 at various stages.

The phishing lures captured this time show that Lorec53 has indeed inherited the organization's mercenary hacking characteristics when operating a national-level cyber attack campaign. Lorec53 will batch-produce and regularly adjust the content of phishing bait, with flexible download server

addresses and CnC addresses, to indiscriminately harass and attack the exposed mailboxes of key Ukrainian institutions. This large-scale attack idea is similar to Lorec53's early operation idea as an email botnet operator.

With the changes in the situation in Eastern Europe, the activity of cyber espionage activities against Ukraine has increased significantly recently, and Fuying Lab will continue to pay attention to the progress of the activities of the Lorec53 organization.

Copyright Notice