(https://nsfocusglobal.com/under-attack/)

APT LOREC53 GROUP LAUNCHED A SERIES OF CYBER ATTACKS AGAINST UKRAINE

APT Lorec53 group launched a series of cyber attacks against Ukraine

February 21, 2022 | **Jie Ji**

Overview

Recently, NSFOCUS Security Labs captured a large number of phishing files against Ukraine in format of pdf, doc, cpl, lnk and other types. After ana series of phishing activities came from the APT group Lorec53. During the period from the end of 2021 to February 2022, this group used multiple a variety of phishing documents to key state sectors such as the Ministry of Defense, Ministry of Finance, embassies, state-owned enterprises, and pu to collect personnel information of these organizations.

About Lorec53 Group

Lorec53, active in Eastern Europe, is a new type of APT group first identified and named by NSFOCUS Security Labs. The Ukrainian Computer Emerg this group as UAC-0056 in a recent report (https://cert.gov.ua/article/18419). NSFOCUS Security Labs found that the group's captureable spy Trojans began to wage large-scale cyber espionage attacks against Ukraine and Georgia in early 2021.

Lorec53 group exposed lots of Russian-linked characteristics in attack tools, registration information of domain names, asset location, etc., and its a related to national interests of Russia. The study on Lorec53's shows there is a likelihood that this group was hired by other high-level espionage org undertaking state-level espionage attacks or selling confidential government documents.

Lorec53 has strong infiltration ability and flexible attack methods, capable of organizing large-scale and frequent phishing attacks and good at harn technologies and network resource management methods learned from other threat actors.

At present, the victims affected by attacks launched by the Lorec53 group include users of the National Bank of Iran, Georgia's Ministry of Epidemic Ministry of Defense, the Presidential Office, the Ministry of the Interior, and the Border Service.

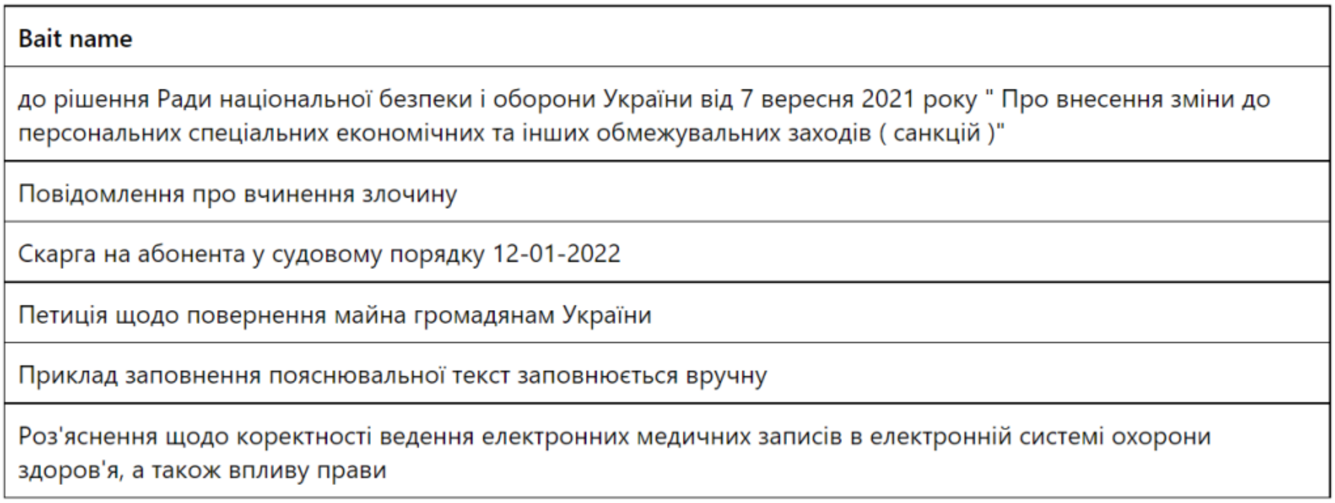
For more reports related to the group, see Analysis Report on Lorec 53 Group (http://(https://nsfocusglobal.com/company-overview/resources/anal

(https://nsfocusglobal.com/under-attack/)

Event overview

This time Lorec53 launched a long wave of attacks aiming at a wide range of targets. similarity of attack methods allowed us to connect these attack

The same as previous methods, Lorec53 used baits such as Ukrainian government documents masked some information, shortcut files with Ukrain extensions, and cpl files with Ukrainian file names, and masqueraded as a member of a credible organization to send these baits.



Bait name
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)"
Повідомлення про вчинення злочину
Скарга на абонента у судовому порядку 12-01-2022
Петиція щодо повернення майна громадянам України
Приклад заповнення пояснювальної текст заповнюється вручну
Роз'яснення щодо коректності ведення електронних медичних записів в електронній системі охорони здоров'я, а також впливу прави

(https://r content/uploads/2022/02/0221f.png)
Some names of phishing files

In this series of phishing attacks, the attack actors mainly used three domain names, namely 3237.site, stun.site , and eumr.site , as download serve domain is one of the commonly used domains of Lorec53 group. As of February 11 , some URLs are still accessible and can deliver payload files, ind is still ongoing .

The Lorec53 group directly wrote the collected mailboxes of key Ukrainian facilities into the decoy text in this series of attacks, which was likely to in Such actions also helped researchers to estimate the attack coverage.

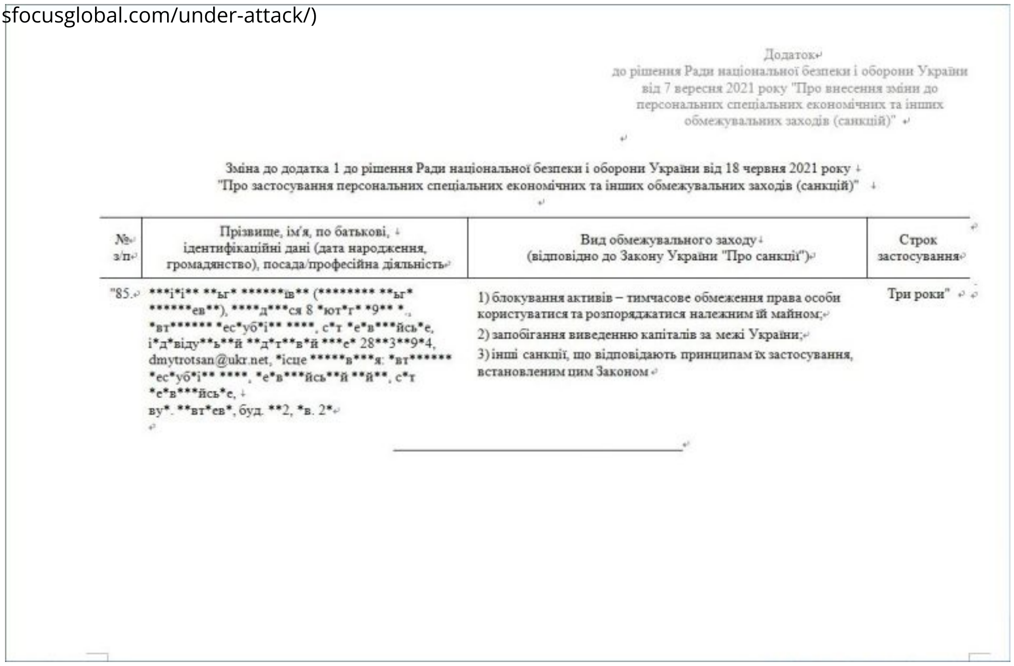
The Lorec53 group still employed known Trojan programs, including LorecDocStealer (also known as OutSteel), LorecCPL , SaintBot , and packaged as possible.

Event analysis

Attack event (1)

The first phishing attack in this wave was spotted at the end of 2021. The Lorec53 group constructed a large number of phishing documents with ” д безпеки і оборони України від 7 вересня 2021 року ” Про внесення зміни до персональних спеціальних економічних та інших обмежувальн content of these phishing documents refers to a presidential decree adopted by the National Security and Defense Council of Ukraine on Septembe asset restrictions and sanctions will be imposed on specific individuals.

(https://nsfocusglobal.com/under-attack/)



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*г* *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"

(https://nsfocusglobal.com/wp-content

Example of the phishing documents

According to the Ukrainian decree, some State departments such as Security Service of Ukraine and Cabinet of Ministers of Ukraine have the rights or delete the individuals for economic sanctions. In the amendment on September 7, an economic sanctions object numbered 85 was added.

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 group made the following changes to the text:

- Obfuscated specific citizen information using asterisks;

This is Lorec53's usual behavior when building phishing documents. It attracts readers to enable the editing function of the document, and then rur

- Added email addresses that did 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 " email had nothing to do with the sanctions, but pointed to the the state treasure service of Ukraine in Volyn region. (ГОЛОВНЕ УПРАВЛІННЯ ДЕРЖ. СЛУЖБИ УКРАЇНИ У ВОЛИНСЬКІЙ ОБЛАСТІ).

The above two changes indicate that the target of this phishing attack is the Ukrainian government, and the email addresses in the phishing email is victim's email addresses. NSFOCUS Security Labs listed these addresses in all captured phishing emails to assess the impact of this Lorec53 phishin

Mail	Corresponding organization
dmytrotsan@ukr.net	The State Treasury Service of Ukraine in Volyn region
emb_sm@mfa.gov.ua	Embassy Of Ukraine In Belgrade, Serbia
kev_dnipro@post.mil.gov.ua	Apartment-operational Department of Dnipro
zorkz@mil.gov.ua	Joint Operational Headquarters of the Armed Forces of Ukraine
office.skdvs@ks.treasury.gov.ua	Department of the State Treasury Service of Ukraine in Skadovsk district of Kherson region
sadovska-ii@utg.ua	Ukrtransgaz Joint Stock Company
ufg.csc@ufg@.com.ua	Ukrainian Financial Group
pokrovske_tckspdp@post.mil.gov.ua	Third Sector Staffing and Social Support Centre, Sinernikivsky District, Dnipropetrovsk Oblast, Ukra
zmievkazna@ukr.net	The State Treasury Service of Ukraine from the Zmiivsky district of the Kharkiv region
kuzmych@naftogaz.com	The Joint Stock Company Naftogaz of Ukraine
zvernmou@ukr.net	Section for Public Appeals Handling and Public Access to Information of the Ministry of Defense of
perevod@pivdenny.ua	Pivdennyi bank
kevzp@post.mil.gov.ua	Press and Information Office of the Ukraine's MoD
i.kozarovska@ukrburgas.com.ua	JSC "Ukrgazvydobuvannya" represented by the branch of the Drilling Department "Ukrburgaz"
kanivkamvo@ukr.net	Department of education of The executive committee of the KANIV city council of cherkasy region
t.litovko@direkcy.atom.gov.ua	VP KB ATOMPRILAD DP NAEK ENERGOATOM
timm93@ukr.net	Department of the State Treasury Service of Ukraine in Vasylivka district of Zaporizhia region
office.cherv@lv.treasury.gov.ua	Department of the State Treasury Service of Ukraine in Chervonohrad, Lviv Region
kevplt_kes@post.mil.gov.ua	
babich-ka@utg.ua	UKRTRANSGAZ Co., LTD
kevplt_zhytlo@post.mil.gov.ua	
corruption@direkcy.atom.gov.ua	State-owned enterprises of Ukraine "NNEGC" Energoatom"
emb_jp@mfa.gov.ua	Embassy of Ukraine in Japan
genotdel@odessa.gov.ua	Odessa Regional State Administration
zoya_skl@ukr.net	The State Treasury Service of Ukraine in the Oleksandrivsky district of the Kirovohrad region
ruslan.marunia@bank.gov.ua	National Bank of Ukraine currency Circulation Department
malyshev.tender@ukroboronprom.com	Malyshev factory
emb_pl@mfa.gov.ua	Embassy of Ukraine in Poland
irudksu@i.ua	The Department of the State Treasury Service of Ukraine in Irshava district of Zakarpattia region
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	Main Department of the State Treasury Service of Ukraine in Kyiv

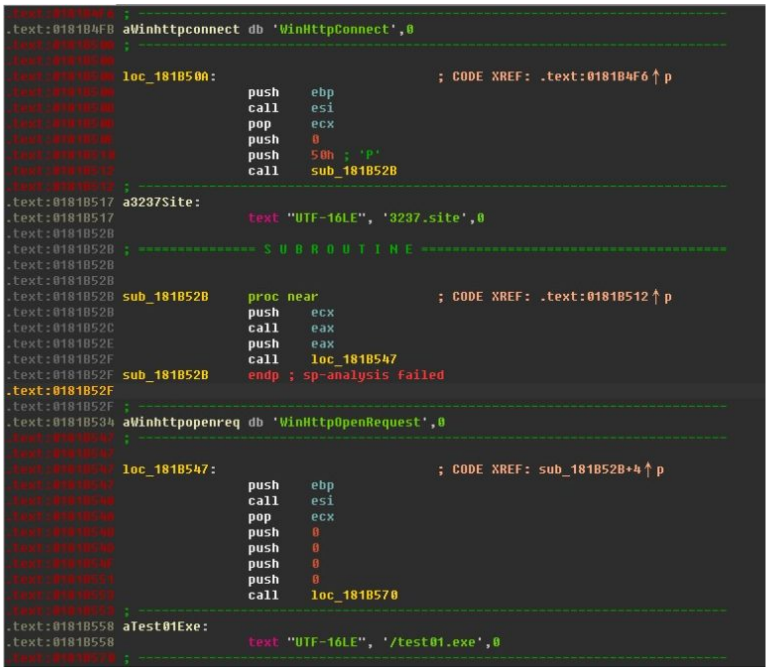
(https://nsfocusglobal.com/under-attack/)

Mail	Corresponding organization
1545@ukc.gov.ua	Government Contact Center Government Hotline 1545
tetiana.rupcheva@bank.gov.ua	Department of Monetary Policy and Market Transactions, National Bank of Ukraine
pr@atom.gov.ua	State-owned enterprises of Ukraine “NNEGC” Energoatom”
1201_buhg@dmsu.gov.ua	ICE of Ukraine in the Dnepropetrovsk region
kherson_kev@post.mil.gov.ua	Housing and Maintenance Department of Kherson
sholyak27@ukr.net	The Statetreasury Service Of Ukraine In Thetranscarpathian Region
office@novator-tm.com	State-owned enterprises of Ukraine “Novator”
mps@industrialbank.ua	AKB Industrialbank PAT
v.harchenko@mil.gov.ua	

Email addresses and corresponding organizations in phishing emails

The associated information of these email addresses shows that the purpose of Lorec53 in this phishing attack is to explore and collect information organization’s previous activities.

The malicious macros in these phishing documents will download and run the Trojan at http [:] //3237 [.] site/test01.exe. Also associated with this документи СБУ .lnk” (a special. lnk file of Security Service of Ukraine), and Lorec53’s known Trojan program LorecCPL (named “08-2021.cpl”), a direc group.

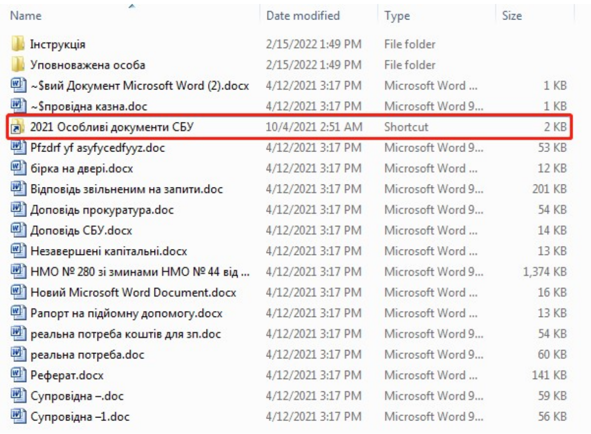


```
.text:0181B4FA ; ---------------------------------------------------------------------------
.text:0181B4FB aWinhttpconnect db 'WinHttpConnect',0
.text:0181B50A ; ---------------------------------------------------------------------------
.text:0181B50A
.text:0181B50A loc_181B50A:                            ; 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 ; ---------------------------------------------------------------------------
```

(https://nsfocusglobal.com/wp-content/uploads/202

Main logic part of the LorecCPL Trojan

The malicious shortcut file named “Особливі документи СБУ.lnk” was also used by the Lorec53 group in several attacks. Lorec53 put the malicious clear files into crafted many compressed files with names including “sadovska-iiutg.ua.zip”, “feukslpost.mil.gov.ua.zip”, “n. lashevychdirekcy.atom.go “feukslpost.mil.gov.ua.zip”, expecting victims run the malicious file while browsing file by file. This decoy method also fits with Lorec53’s historical ta



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

(https://nsfocusglobal.com/wp-content/uploads/2022/02/02

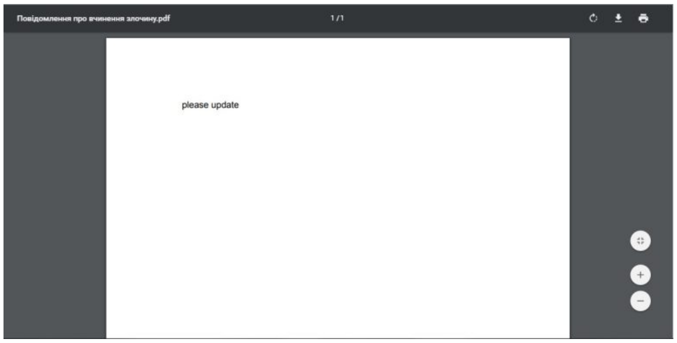
File directory of a crafted compressed package

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 aforementione economic sanctions, which can be speculated to be the same series of attacks.

Attack event (2)

(https://nsfocusglobal.com/under-attack/) This is a phishing attack occured between Decemeber 2021 and February 2022.

In early February, Lorec53 produced a series of phishing documents titled ” Повідомлення про вчинення злочину” (Report of Crime), delivered in vulnerability and DOCX file with malicious macros. The former file displayed “please update” when opened.



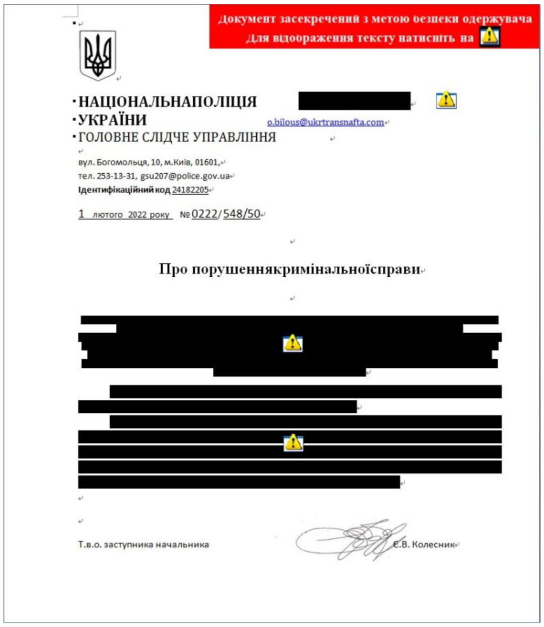
please update

(https://nsfocusglobal.com/wp-content/uploads/2022/02

Phishing document titled “Повідомлення про вчинення злочину”

Crafting PDF phishing documents is a commonly-used method by the Lorec53 group. It is used to download the Trojan programs https[:]//get.adobe.com.uk.reader.updateadobeacrobatreaderdc.stun[.]site/get.adobe.com.uk.reader/get.adobe.com.uk.reader/get.adobe.com.uk.r This Trojan is another form the Trojan LorecDocStealer (also known as OutSteel) and used to steal documents from compromised hosts. The shell Lorec53 group on this Trojan is commonly seen in AgentTesla spyware.

The latter DOCX file ” Повідомлення про вчинення злочину (Білоус Олексій Сергійович) .docx” presented images and textual information with used the by Lorec53 group when it was opened.



Документ засекречений з метою безпеки одержувача
Для відображення тексту натисніть на ⚠

НАЦІОНАЛЬНАПОЛІЦІЯ [redacted] ⚠
УКРАЇНИ o.bilous@ukrtransnafta.com
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Богомольця, 10, м.Київ, 01601,
тел. 253-13-31, gsu207@police.gov.ua
Ідентифікаційний код 24182205

1 лютого 2022 року № 0222/548/50

Про порушеннякримінальноїсправи

[redacted] ⚠

[redacted] ⚠

Т.в.о. заступника начальника Є.В. Колесник

(https://nsfocusglobal.com/wp-content/uploads/2022/02/0221

DOCX phishing document titled ” Повідомлення про вчинення злочину”

The document is disguised as a document from the investigation department of the Ukrainian National Police, and through a piece of red prompt ir tricked readers to click the icon ole object in the document and then execute JavaScript to download and run the Trojan horse in the link https[:]//cc in /attachments/932413459872747544/938291977735266344/putty.exe. The Trojan is also a new look of Trojan LorecDocStealer (or OutSteel).

With reference to the aforementioned attack, the unobfuscated email address o.bilous@ukrtransnafta.com in this document is very likely to belong company of this mailbox is UkrTransNafta in Ukraine .

In addition, this DOCX phishing document was also spotted and published by the Ukrainian Computer Emergency Response Center (CERT-UA), whe Lorec53 group as the UAC-0056 (https://cert.gov.ua/article/18419 (https://cert.gov.ua/article/18419)).

Association analysis to the domain name stun.site appeared in this attack shows NSFOCUS security researchers that a variety of decoy files release December 2021. These files include .lnk, .cpl , .rar and other formats, all of which are known decoy forms of the Lorec53 group. The main purpose o LorecDocStealer (OutSteel) Trojan from stun.site for further attack activities .

Attack event (3)

The is an attack linked to the domain name eumr[.]site.

(https://nsfocusglobal.com/under-attack/)

In the early of February, the Lorec53 group constructed a phishing document named " Роз'яснення " щодо коректності ведення електронних мед системі охорони здоров'я, а також впливу прави" (Clarification on the correctness of electronic medical records in the electronic health care syste and sent out in .zip format. As indicated by the name, it's targeted the Ukrainian medical system, the same target in Lorec53 previous attacks.

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

The latest modified date of this decoy shows on January 31, 2022.

Domain names and C2 server addresses appeared in this attack can be associated with a large number of other malicious programs, all of which ar the LorecDocStealer (OutSteel) Trojan.

Conclusion

The attacks spotted this time are all part of a large-scale cyberattack campaign carried out by the Lorec53 group between the end of 2021 and Febru government departments, the military, and state-owned enterprises. The main purpose of these attacks are still probing and collecting information, Lorec53 groups at each stage.

The phishing lures captured this time show that the Lorec53 group has indeed inherited the group's mercenary hacking characteristics when operat campaign. The Lorec53 group will batch-produce and regularly adjust the content of the phishing bait, with flexible download server addresses and indiscriminately harass and attack the exposed mailboxes of critical facilities of Ukraine. This large-scale attack idea is similar to Lorec53's early oper operator. As the situation in Eastern Europe has changed, the activities of cyber espionage against Ukraine have increased significantly recently. NS continue to pay attention to the Lorec53 group and its attack activities.

PRODUCTS (/PRODUCTS/ANTI-DDOS-SYSTEM-ADS/)

Anti-DDoS Protection (/anti-ddos-system-ads/)

Cloud DDoS Protection (/cloud-ddos-protection-service-cloud-dps/)

Threat Intelligence (/Threat-Intelligence-Ti/)

Application Security (/Threat-Analysis-System/)

Intelligent Security Operation Platform (https://nsfocusglobal.com/products/intelligent-security-operation-platform-isop/)

Unified Threat Sensor (https://nsfocusglobal.com/products/unified-threat-sensor/)

Next-Generation Firewall (https://nsfocusglobal.com/products/next-gen-firewall/)

SOLUTIONS (HTTPS://NSFOCUSGLOBAL.COM/SOLUTIONS-OVERVIEW/)

Overview (https://nsfocusglobal.com/solutions-overview/)

Cloud-in-a-Box (https://nsfocusglobal.com/products/cloud-box-ciab/)

On-Premises DDoS Defenses (https://nsfocusglobal.com/solutions-overview-3/on-premises/)

Hybrid DDoS Defenses (https://nsfocusglobal.com/solutions-overview-3/hybrid-ddos-protection/)

Value-Added Service for ISP/MSP (https://nsfocusglobal.com/solutions-overview-3/value-added-service-solution/)

5G Network Security Solution (https://nsfocusglobal.com/solutions-overview-3/5g-network-security-solution/)

SERVICES (HTTPS://NSFOCUSGLOBAL.COM/SERVICES/)

Services Overview (/services)

NSFOCUS Product Support Services (https://nsfocusglobal.com/services/nsfocus-product-support-services/)

NSFOCUS Professional Services (https://nsfocusglobal.com/services/nsfocus-professional-services/)

NSFOCUS Security Assessment Services (https://nsfocusglobal.com/services/nsfocus-security-assessment-services/)

NSFOCUS Managed Security Services (https://nsfocusglobal.com/services/nsfocus-managed-security-services/)

Training Services (https://nsfocusglobal.com/services/training-services/)

RESOURCES (HTTPS://NSFOCUSGLOBAL.COM/COMPANY-OVERVIEW/RESOURCES/)

Datasheets (https://nsfocusglobal.com/company-overview/resources#datasheets)

Whitepapers (https://nsfocusglobal.com/company-overview/resources#whitepapers)

Reports (https://nsfocusglobal.com/company-overview/resources#reports)

Case Studies (https://nsfocusglobal.com/company-overview/resources#case-studies)

Infographics (https://nsfocusglobal.com/company-overview/resources#info)

Articles (https://nsfocusglobal.com/company-overview/resources#articles)

NEWS AND EVENTS (/CATEGORY/PRESS-RELEASES/)

Press Releases (https://nsfocusglobal.com/categor releases/)

NSFOCUS in the News (https://nsfocusglobal.com/categor

Global Events (https://nsfocusglobal.com/categor

COMPANY (HTTPS://NSFOCUSGLOBAL.C OVERVIEW/ABOUT/)

About (https://nsfocusglobal.com/compar overview/about/)

Management Team (https://nsfocusglobal.com/compar overview/management-team/)

NSFOCUS Security Labs (https://nsfocusglobal.com/compar overview/nsfocus-security-labs/)

Careers (https://nsfocusglobal.com/compar overview/careers/)

Contact Us (https://nsfocusglobal.com/compar overview/contact-us/)

(https://www.facebook.com/nsfocus) (https://www.linkedin.com/company/nsfocus) (https://twitter.com/NSFOCUS_Intl)

(https://nsfocusglobal.com/under-attack/)