A Zebra in Gopher's Clothing: Russian APT Uses COVID-19 Lures to Deliver Zebrocy

intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy

December 9, 2020

Written by Joakim Kennedy - 9 December 2020

Summary

In November, we uncovered COVID-19 phishing lures that were used to deliver the Go version of Zebrocy. Zebrocy is mainly used against governments and commercial organizations engaged in foreign affairs. The lures consisted of documents about Sinopharm International Corporation—a pharmaceutical company that COVID-19 vaccine is currently going through phase three clinical trials—and an impersonated evacuation letter from Directorate General of Civil Aviation.

The lure was delivered as part of a Virtual Hard Drive (VHD) file that requires victims to use Windows 10 to access the files. While the malware samples were heavily obfuscated, it was possible to attribute them to the Sofacy threat actor since they shared genomes with samples used in previous campaigns.

It appears that the threat actor switched from delivering VHD files with the Delphi version of Zebrocy, to the Go version in the middle of November. Given that many COVID-19 vaccines are about to be approved for clinical use, it's likely that APTs

(Advanced Persistent Threat) and financially motivated threat actors will use this malware in their attacks.

Zebrocy Evolution

Zebrocy is a malware used by the threat group Sofacy, also known as Sednit, APT28, Fancy Bear, and STRONTIUM. Sofacy was one of the groups indicted by the Department of Justice (DOJ) for the compromise of the Democratic National Committee (DNC). The Zebrocy toolset was first reported by Kaspersky Labs as part of theirAPT Trends report in 2017. The malware was first used in2015 and overlapped with known Sofacy infrastructure at the time. Zebrocy operates as a downloader and collects information about the infected host that is uploaded to the command and control (C&C) server before downloading and executing the next stage.

The first version of the downloader was written in Delphi and was based on aprevious malware used by Sofacy. One unique aspect of the operators behind Zebrocy is their choice of evolving the malware. Instead of improving their codebase to add new functionalities and increase their chance of staying undetected, the group has opted to keep the malware simple by implementing new versions in different programming languages. Zebrocy samples written in AutoIT, C++, C#, Delphi, Go, and VB.NET have been discovered by the research community.

While Zebrocy is known to be used by a subset of the Sofacy threat group, Kaspersky Labs reported in January 2019 that they had discovered infrastructure used both by Zebrocy and GreyEnergy. GreyEnergy was discovered by ESET and reported on inOctober 2018. The group is believed to be the successor of BlackEnergy, also known as Sandworm. Sandworm was recently attributed to Russia's GRU by the United States government in an indictment for the NotPetya and Olympic Destroyer campaigns. Generally speaking, Sofacy and BlackEnergy have diverging goals and have been known to go after different targets. In this case, the common infrastructure and targets between the Sofacy subgroup using Zebrocy and GreyEnergy suggests a relationship between the groups.

Zebrocy is mainly used againstgovernments and commercial organizations engaged inforeign affairs. Victims have been locatedin: "Afghanistan, Azerbaijan, Bosnia and Herzegovina, China, Egypt, Georgia, Iran, Japan, Kazakhstan, Korea, Kyrgyzstan, Mongolia, Russia, Saudi Arabia, Serbia, Switzerland, Tajikistan, Turkey, Turkmenistan, Ukraine, Uruguay, and Zimbabwe." The delivery of Zebrocy is usually via a spear-phishingemail. The email has contained Microsoft Office documents or archive files.

Technical Analysis

At the end of November, we discovered a Virtual Hard Drive (VHD) file (a7b446d79d3fc05a7e1881d6d4abaf55) named **30-22-243.vhd** that was uploaded from Azerbaijan to VirusTotal. VHD is the native file format for virtual hard drives used by

Microsoft's hypervisor, Hyper-V. Windows 10 has native support for the file format and allows the user to mount the file and access its content. Figure 1 shows what the user would see if they downloaded the file to their desktop. According to timestamps stored in the file, the disk was created on November 20, 2020, 10 days before it was uploaded to VirusTotal.

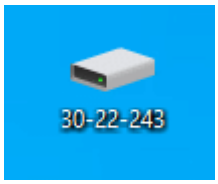

Figure 1: VHD phishing lure.

If the user double-clicks on the file, Windows will mount the drive and it appears as an external hard drive. Figure 2 shows the content of the VHD.

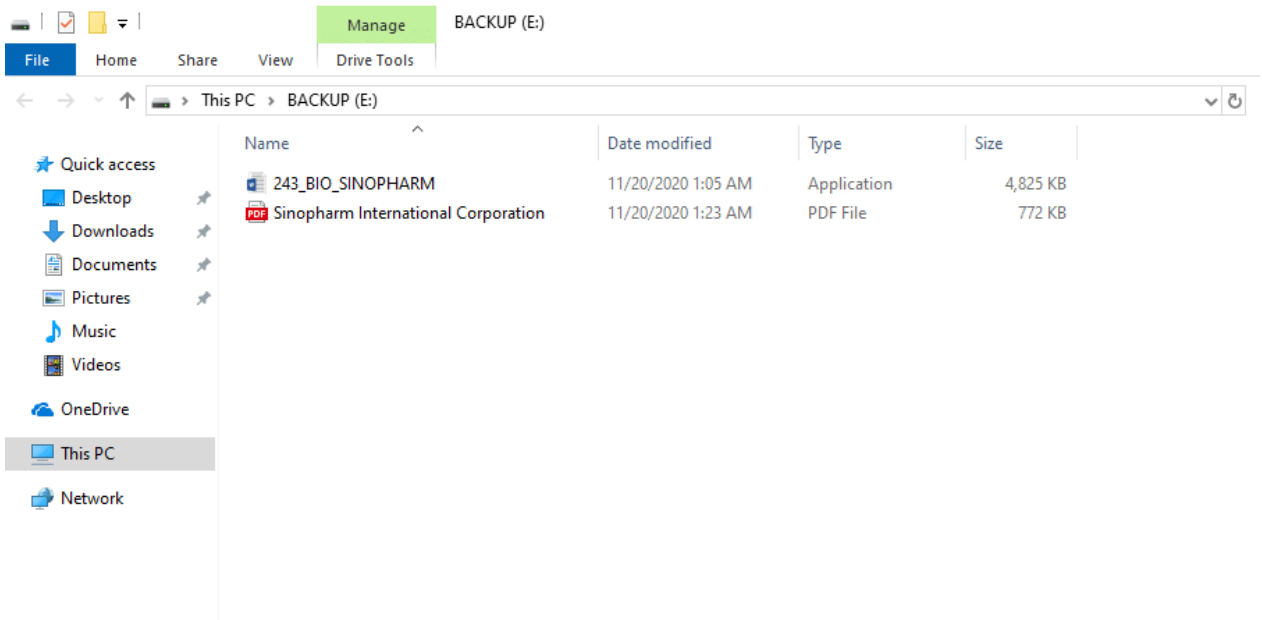

Figure 2: Content of the VHD file. It contains two files: A PDF file and an executable that is masquerading as a Microsoft Word document.

The VHD file includes two files, a PDF document and an executable that is masquerading as a Microsoft Word document. The PDF file consists of presentation slides about *Sinopharm International Corporation*. Figure 3 displays a screenshot of the first slide.

Figure 3: PDF of presentation slides used as part of the lure.

Sinopharm International Corporation is a China-based manufacturer of pharmaceutical products. It is one of the companies in China that is currently working on a vaccine for COVID-19. Their vaccine is currently undergoingphase three clinical trials but it has already beengiven to nearly one million people. It may not come as a surprise that the threat group behind Zebrocy is using COVID-19-themed related lures when many vaccines are about to get approved for use. The group is known to usecurrent events as part of their phishing lures.

The second file is the malware. By default, Windows hides known file extensions and the user can be easily tricked into believing that it's a Word document. The scan results of the executable from VirusTotal is shown in Figure 4 and Intezer Analyze in Figure 5. Only nine of the 70 antivirus engines detected the file as generic malware while Analyze detected the file as malware associated with Sofacy.

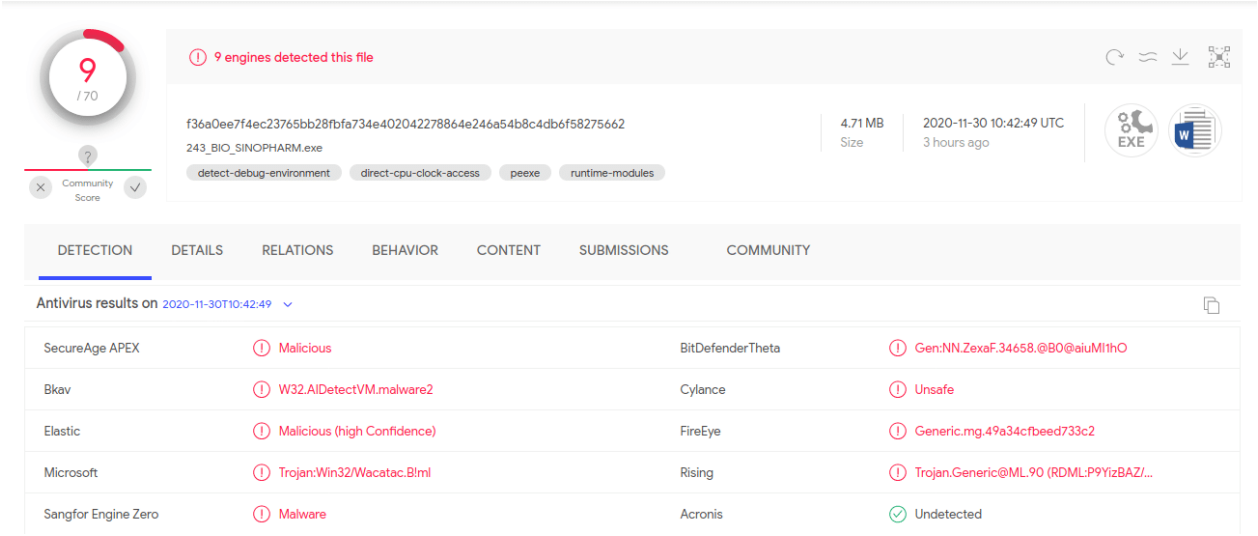

Figure 4: VirusTotal scan results of the binary file with generic detection.

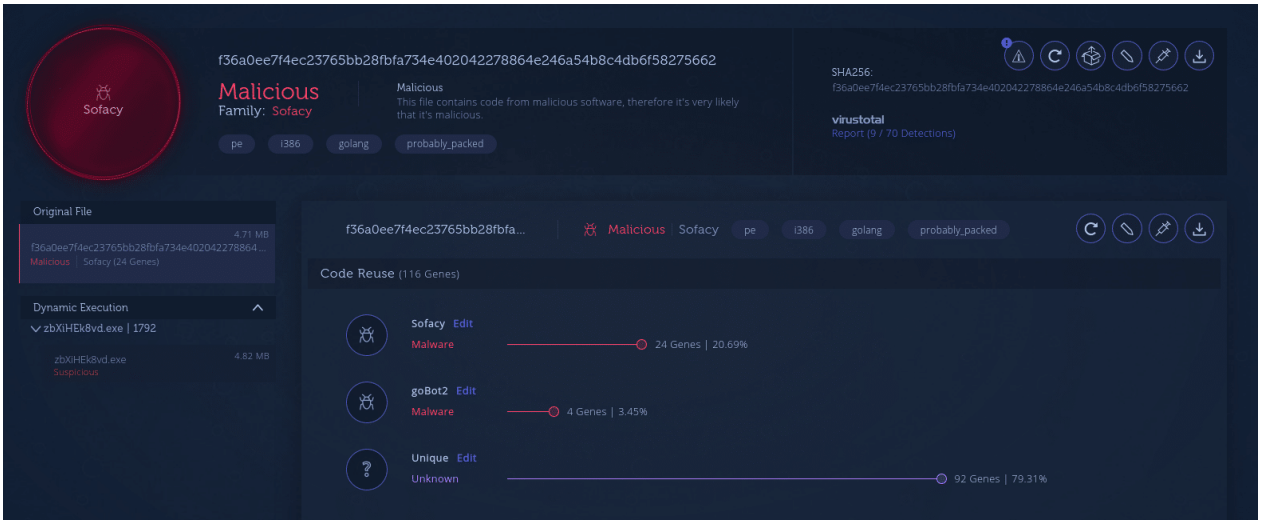

Figure 5: Intezer Analyze detects the file as genetically similar to malware used by Sofacy one year ago.

The malware is a new sample of Zebrocy written in Go. Earlier this year, QuoIntelligence detected an ongoing campaign by Sofacy, assessing with medium-high confidence that the group was targeting Azerbaijan. In that campaign, the Delphi version was used. It appears that the threat group has now switched from delivering the Delphi downloader to the Go downloader.

The downloader is similar to the original downloader reported byPalo Alto Networks Unit 42. The sample has been obfuscated with gobfuscator, the same tool used by the Blackrota malware. The sample doesn't collect the same amount of information about the infected machine (i.e., running processes, local disk information, and system information from "systeminfo") as in previous campaigns. Instead, it collects the hostname and the path to the user's **TEMP** folder. This information is used to generate an identifier by hashing the values with MD5. The screenshot functionality is not performed by an imported third-party library. Rather, the malware author has included the screenshot code from the library directly in the main codebase. The malware has

some anti-debugging checks. In Figure 6, it can be seen how the malware calls the Windows API function **IsDebuggerPresent**. If true is returned, it enters an infinite sleeping loop.

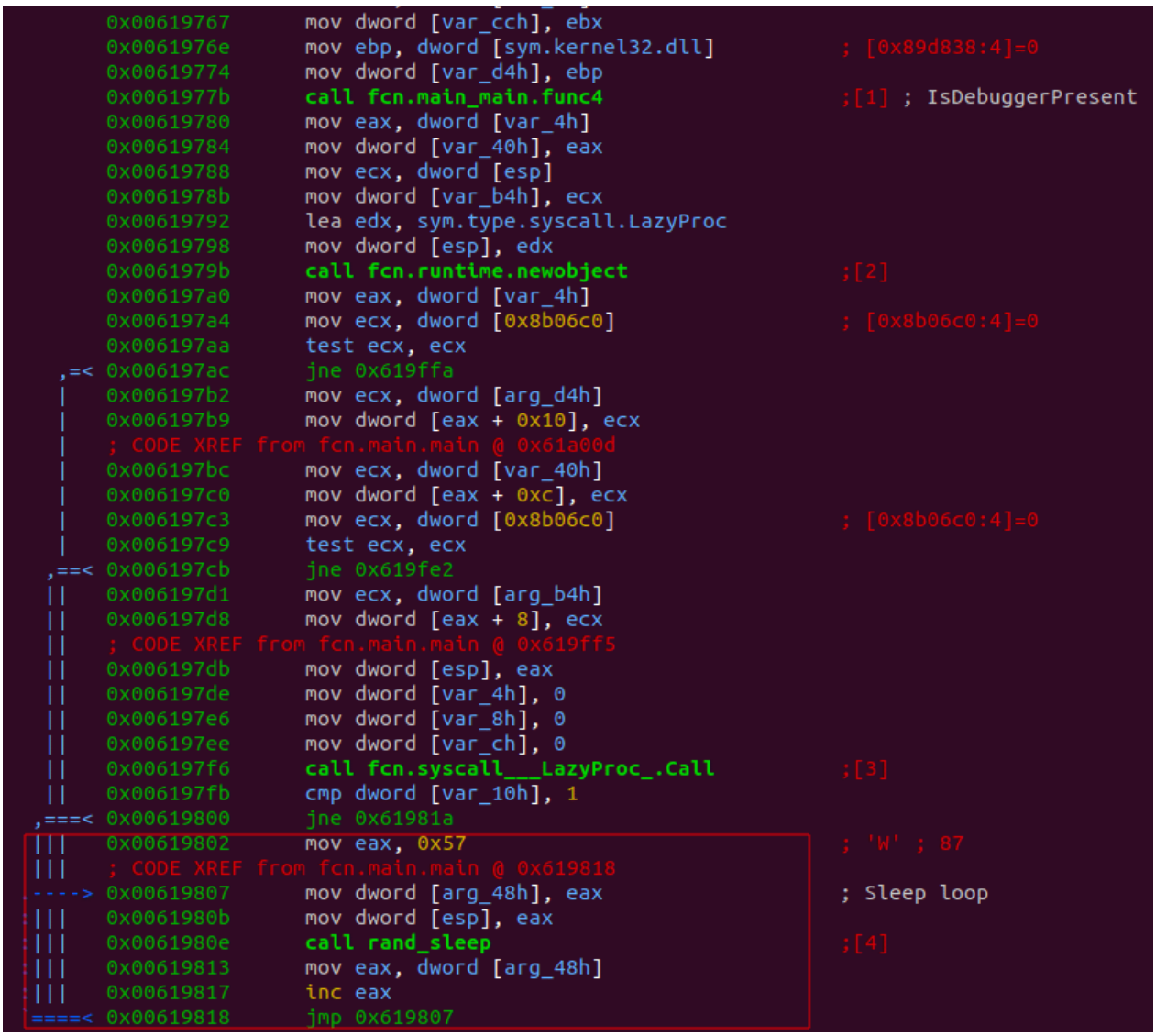

Figure 6: Logic that checks if the process is being debugged. If true, it enters a sleeping loop.

The screenshot is uploaded to the C&C located at the URL: **hxxps://support-cloud[.]life/managment/cb-secure/technology.php**. If the C&C returns a second stage, the file is written to the disk and executed. The URL scheme for the C&C is similar to the URL scheme used in the originalGo version (**hxxp://89.37.226[.]148/technet-support/library/online-service-description.php**). The domain name was registered with NameCheap on October 20, 2020, and uses a certificate issued by Let's Encrypt. The certificate was issued on November 2, 2020. The infrastructure is hosted on **80.90.39.24** which is owned by the Luxembourg-based hosting company, Visual Online. The infrastructure appears to be new.

Earlier Campaigns

Using the icon resource from the original phishing lure, we found another phishing lure (395e166af5197967503f45c3ac134ff7) that was uploaded to VirusTotal from Kazakhstan on November 12. This VHD file was named **No.243.CB3-EVACUATION LETTER.vhd**. The content of the file is shown in Figure 7.

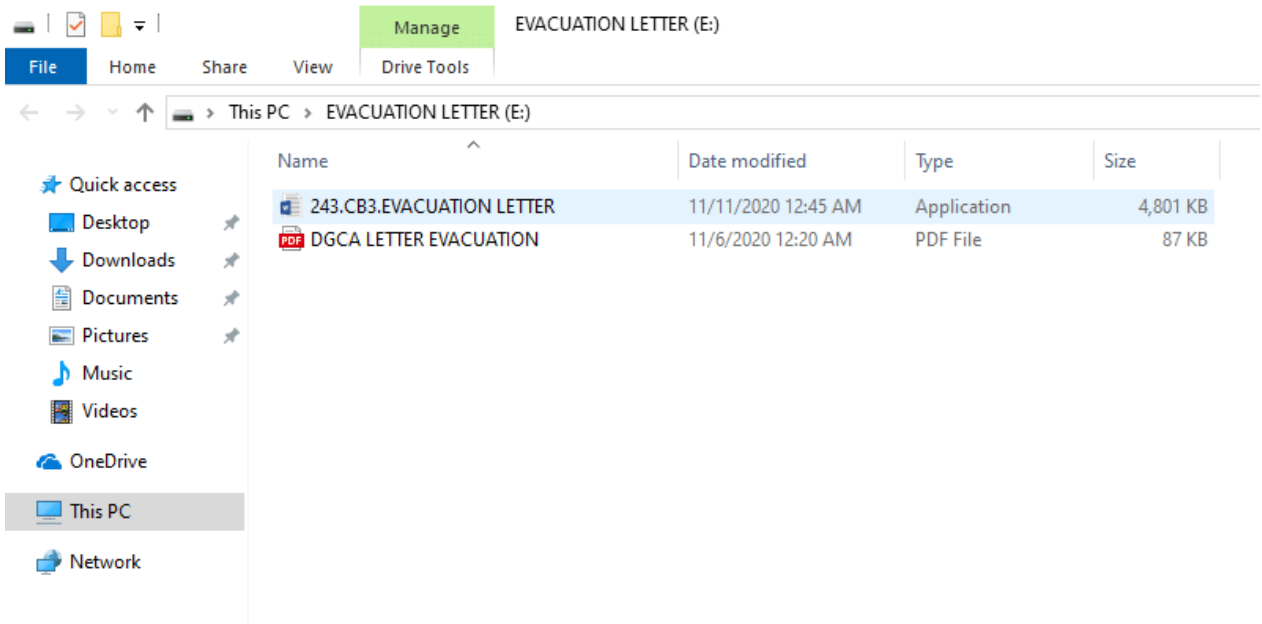

Figure 7: Content of No.243.CB3-EVACUATION LETTER.vhd. The disk file includes an executable file and a PDF file.

The executable is another Go version of Zebrocy. It uses the same C&C URL. The sample is obfuscated using the same technique the group has used for their prior versions. The function names have been mangled and the strings have been obfuscated. In this version, the strings are obfuscated by rotating the characters in the string one step. For example, **A** has been rotated to **B**.

The PDF file is corrupted. This is not the first time the group is usingcorrupt files as part of its lures. CorruptMicrosoft Excel files were used in the campaign uncovered by QuoIntelligence earlier this year. The technique is likely used to trick the user into executing the application rather than just viewing the lure.

Based on the file name, one theory we have is a message from India's Directorate General of Civil Aviation is being impersonated. It was announced in August that a flight network between India, Russia, and other Central Asian countries was being developed. While India has suspended international flights due to the pandemic, some airlines have operated charter flights to "Russia, Uzbekistan, Ukraine, Kazakhstan and Kyrgyzstan."

It turns out the same VHD file was uploaded in October to VirusTotal with different content (855005fee45e71c36a466527c7fad62f); both samples share the same disk ID. The content of this sample is shown in Figure 8. As with the other VHD files, this also

has a PDF file and an executable masquerading as a Microsoft Word Document. Instead of delivering the Go version of Zebrocy, the Delphi loader was used.

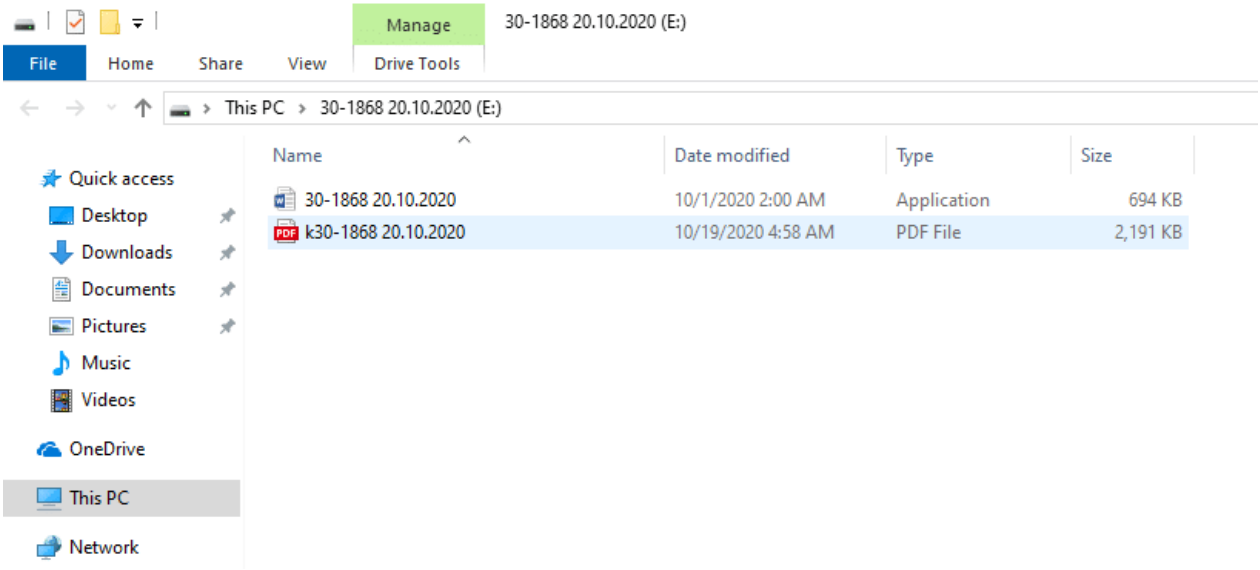

Figure 8: Content of VHD uploaded to VirusTotal in October.

The PDF lure is written in Russian. The title is, according to Google Translate: “NATIONAL LIST INDIVIDUALS AND LEGAL ENTITIES INVOLVED IN TERRORIST AND EXTREMIST ACTIVITIES OR THE DISTRIBUTION OF WEAPONS OF MASS DESTRUCTION.” The content of the first page is shown in Figure 9.

Приложение 1 к приказу ГСФР
от 8 февраля 2017 года № 6/П

НАЦИОНАЛЬНЫЙ ПЕРЕЧЕНЬ
ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ, ПРИЧАСТНЫХ К ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ ИЛИ РАСПРОСТРАНЕНИЮ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ

(в редакции приказов ГСФР от 08.02.2017 года № 6/П, 18.04.2017 года № 25/П, 01.06.2017 года № 32/П, 29.06.2017 года № 41/П, 04.07.2017 года № 45/П, 06.09.2017 года № 66/П, 19.09.2017 года № 69/П, 20.10.2017 года № 84/П, 28.10.2017 года № 85/П, 03.11.2017 года № 88/П, 14.11.2017 года № 89/П, 30.11.2017 года № 99/П, 11.12.2017 года № 102/П, 20.12.2017 года № 103/П, 17.01.2018 года № 2/П, 31.01.2018 года № 6/П, 06.03.2018 года № 20/П, 15.03.2018 года № 25/П, 12.04.2018 года № 34/П, 07.05.2018 года № 44/П, 08.05.2018 года № 45/П)

1. ФИЗИЧЕСКИЕ ЛИЦА:

№	Фамилия	Имя	Отчество	Дата рождения	Место рождения	Основание для включения физического лица в Перечень	Категория физического лица	Дата включения физического лица
1.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1

Figure 9: Redacted screenshot of PDF lure written in Russian.

According to timestamps, the VHD was created on October 21, the day after the domain (support-cloud[.]life) was registered. The domain was used in a spear-phishing attack against a Kazakhstan government ministry the same day. The VHD file was uploaded to VirusTotal the next day. On November 11, the same VHD file was reused but the lure and payload were changed. This version of the VHD was uploaded to VirusTotal the next day. By applying this logic to the VHD file used to deliver the Sinopharm-based lure, we can estimate that it was used around November 20.

Conclusion

Zebrocy is a malware toolset used by the Sofacy threat group. While the group keeps changing obfuscation and delivery techniques, code reuse allowed Intezer to detect and correctly classify this malware. With these recent phishing lures, it's clear that COVID-19 themed attacks are still a threat and we might see more as vaccines become available to the general public.

It's important that companies use defense-in-depth strategies to protect against threats. Employers should also ensure employees are trained on detecting and reacting to phishing attempts. Phishing attempts do not always originate from an external email address; they can also come from a compromised account within the enterprise.

IoCs

Network

hxxps://support-cloud[.]life/managment/cb-secure/technology.php

VHD files

- d5d9210ef49c6780016536b0863cc50f6de03f73e70c2af46cc3cff0e2bf9353 30-1868.vhd
- 43c65d87d690aea7c515fe84317af40b7e64b350304b0fc958a51d62826feade 30-22-243.vhd
- d444fde5885ec1241041d04b3001be17162523d2058ab1a7f88aac50a6059bc0 No.243.CB3-EVACUATION LETTER.vhd

Zebrocy

- f36a0ee7f4ec23765bb28fbfa734e402042278864e246a54b8c4db6f58275662 243_BIO_SINOPHARM.exe
- 61c2e524dcc25a59d7f2fe7eff269865a3ed14d6b40e4fea33b3cd3f58c14f19 243.CB3.EVACUATION LETTER.exe

- 6449d0cb1396d6feba7fb9e25fb20e9a0a5ef3e8623332844458d73057cf04a1 30-1868 20.10.2020.exe

Joakim Kennedy
Dr. Joakim Kennedy is a Security Researcher analyzing malware and tracking threat actors on a daily basis. For the last few years, Joakim has been researching malware written in Go. To make the analysis easier he has written the Go Reverse Engineering Toolkit (github.com/goretk), an open-source toolkit for analysis of Go binaries.