Spearphishing Attack Uses COVID-21 Lure to Target Ukrainian Government

fortinet.com/blog/threat-research/spearphishing-attack-uses-covid-21-lure-to-target-ukrainian-government

May 3, 2021

FortiGuard Labs Threat Research Report

Affected platforms: Microsoft Windows
Impacted parties: Windows Users
Impact: Collection of sensitive information from infected victims
Severity level: High

Introduction

FortiGuard Labs has discovered yet another COVID themed lure designed to compel unsuspecting victims to click on what appears at first be an innocuous link. However, unbeknownst to the target, the link leads to a zip file that contains malicious attachments.

This blog will highlight the steps taken by an unnamed threat actor targeting the security interests of a former Eastern bloc nation.

Key Takeaways of This Blog

- Spearphishing emails were sent to various security arms of the Ukrainian government utilizing social engineering lures containing subjects such as: “New COVID-21 Variant” and “An Urgent Computer Update”.
- Attacker’s goals
  - Steal sensitive documents and files
  - Install Saint Bot Downloader on targets
- Note: The Saint Bot Downloader has been observed downloading infostealers and other downloaders.

Overview

This latest iteration of the COVID-themed lures we have been seeing over the past year is not about COVID-19, but a fictitious COVID-21 (bypassing the equally fictitious COVID-20 entirely!) using a fake World Health Organization (WHO) link. It is likely that the threat actor is hoping that the novelty of a COVID-21 announcement might entice the recipient into following the link, either through misjudgment or sheer curiosity. The following research looks at possible motivations for this particular attack, as well as provides technical analysis of the malware involved and related infrastructure.

In this case, we have observed specific instances of spearphishing emails being sent to various arms of the Ukrainian government and have also identified that the infrastructure used for these attacks originates in Russia. The first instance we detected targeted two separate entities of the Ukrainian government, both dealing with security interests of the Ukrainian state.

Figure 1. Message body of the COVID-21 Lure

The email purports to originate from a “Political Officer” at the United States Embassy. Interestingly, a search engine check revealed that *Political Officer* is indeed an actual title within the US State Department. Further, a review of the email headers highlights that the sender is either a legitimate Gmail account created for such spam purposes, or one that has been compromised, as the email was relayed through Gmail servers. Sending spam email through clean reputable servers as a relay is an ideal tactic for attackers as they are often allowed to bypass spam filtering software since they originate from a reputable IP block.

This email is targeting one of the security arms of the Ukrainian Government. However, a search engine result yielded no results for the email address, which leads us to believe that this is either a targeted or a dictionary/harvest based attack.

Another tactic observed was that the threat actors used masqueraded emails within the message body containing a back and forth conversation between (likely fictitious) personnel at the World Health Organization (WHO) and the United States Department of State (state.gov). We surmise that this email is targeted as it includes government-specific communication and not, for example, a generic purchase order from a random industry vertical, etc.

Technical Details

Instead of using attachments, this lure opted to use a link to deliver its payload, further ensuring that the spearphishing email makes it to the intended victim by bypassing security tools that detect and neutralize malicious attachments. The fake WHO link goes to hxxps://cut[.]ly/LcHx2Ga, which redirects to hxxp://2330[.]site/NewCovid-21[.]zip. The contents of the zip archive are shown below.

Figure 2. Zip file archive

The PDF is legitimate and not malicious. The other files however, are each malicious in their own way. The two shortcut files appear to launch cmd.exe. However, after examining these two files further, we found that the true attack vector actually uses cmd.exe to launch PowerShell in order to download and execute yet another malicious file.

The final file contained in the zip archive is a malicious document that exploits CVE-2017-11882 (Microsoft Office Equation Editor Vulnerability) and acts similarly to the shortcut files. Affecting multiple Microsoft Office versions, up to Word 2016, CVE-2017-11882 allows arbitrary code execution in the context of the current user by failing to properly handle objects in memory. By exploiting this vulnerability, the document is able to download and execute yet another malicious file.

Each of these malicious files will be explored further in the next sections.

Malicious Shortcuts (LNK) Files

The shortcut files at first appear to be benign:

Figure 3. Properties of LNK file

Nothing except cmd.exe and whitespace can be seen. Peering into the .lnk file itself with a hex editor, or even a strings command, however, shows there is a PowerShell command hidden within. The essence of this command is to download a file from hxxp://2330[.]site/soft/08042021[.]exe and saves it as %TEMP%\WindowsUpdate.exe. It then executes the downloaded file.

A cursory review of the 2330.site reveals that the domain has been associated with the following IP addresses in the past:

95.143.218[.]55
31.31.205[.]163
195.128.123[.]215
185.195.27[.]112
176.113.115[.]133

All of these IP addresses resolve back to the Russian Federation.

A quick perusal of the WindowsUpdate.exe files shows that it is packed. Underneath the surface lies an AutoIT file that cannot be decompiled by a standard decompiler. To get around this roadblock, the AutoIT compiled script can be found in memory and dumped into a separate file.

Figure 4. AutoIT compiled script from memory

The bytecode in this file can then be decompiled properly.

Figure 5. Results after decompiling

This AutoIT script is designed to exfiltrate user files. It targets filetypes located in the user's home directory and uploads them to a server.

The targeted filetypes are: .doc, .pdf, .ppt, .dot, .xl, .csv, .rtf, .mdb, .acdb, .pot, .pps, .ppa, .rar, .zip, .tar, .7z.

Figure 6. Filetypes targeted

Given the branches of the government targeted by this phishing attack, the filetypes being captured could potentially vary from benign to sensitive to even classified information.

Files stolen by this script are uploaded to hxxp://name4050[.]com:8080/upld/

Malicious Word Document

The last file in the NewCovid-21.zip archive is a malicious document that exploits CVE-2017-11882 (Microsoft Equation Editor Vulnerability). The exploit forces the user to visit hxxp://bit[.]ly/3rQULnp. The user is then redirected to a predetermined URL, hxxp://name1d[.]site/index.txt. This is not a text file, but a PE file that then gets executed.

Part 1 of Social Engineering Lures

The downloaded PE file is also packed. After some investigation, we determined that its contents are similar to the files downloaded by the LNK files.

Figure 7. Analysis of downloaded PE file from hxxp://name1d[.]site/index.txt

The only significant difference in this sample is that it uploads gathered files to a different C2 server: hxxp://31.42.185[.]63:8080/upld/. The list of filetypes is still the same.

Part 2 - A Saint Amongst Blocs

Sometime later, a different index.txt file was served, possibly for a different campaign. We analyzed this new file as well. It is a PE file that is a variant of the Saint malware recently discovered by security researchers. As it is a downloader, its possible uses are limitless. It has been observed to even download other downloaders as well.

This version turned out to be Saint_v3, which operates similarly to the one analyzed here: (https://blog.malwarebytes.com/threat-analysis/2021/04/a-deep-dive-into-saint-bot-downloader/). However, the C2 server this variant goes to is hxxp://smm2021[.]net/wp-adm/gate.php and it uses compromised WordPress sites to communicate. It may also use 8003659902[.]site as well as 8003659902[.]space as part of its network infrastructure.

Saint_v3 has specific functionality in case it ends up running on a Windows 10 machine. It checks the registry for the ProductName to see if it is Windows 10. If so, it then checks for another registry setting, called ConsentPromptBehaviorAdmin, to see if it has a value of 5.

Microsoft defines this value as: *‘[T]he default. It is used to prompt the administrator in Admin Approval Mode to select either "Permit" or "Deny" for an operation that requires elevation of privilege for any non-Windows binaries. If the Consent Admin selects Permit, the operation will continue with the highest available privilege. This operation will happen on the secure desktop.’*

It then performs a few other actions under a Windows 10 environment.

One unique thing that was observed is that this malware will not run on an infected computer running one of the following locales:

Figure 8. Locales avoided by Saint Malware

Given that the phishing email gathered indicates that it is targeting a victim based in the former Eastern Bloc, and may be using one of the listed locales, one wonders if the attackers have narrowed down their target to the point they know the victim does not use any of these locales? Perhaps as a defensive posture, the victim was using English or another version, and the attacker knew this? In any case, this just adds another layer of mystery to this attack.

Even though there is not much code in the AutoIT samples, the same coding method is seen in the downloaded Saint_v3 files.

Figure 9. Cleaning up all evidence

The cleanup functions are somewhat similar.

Urgent Update Variation

Another sample that we observed appears to be related to this same campaign, and is likewise targeting a security arm of the Ukrainian government. Its email purports to be coming from the main security arm of the Ukrainian government, and the link attempts to convince the target that orders are coming from higher in the chain of command, possibly hoping that the link will be clicked on in a moment of misjudgment. The email address that this spearphishing email is being sent from can actually be found on the main page of the website of this security arm of the Ukrainian government:

Figure 10. Original Urgent Update Email

Figure 11. Urgent Update Email (Translated to English)

The broken text in the subject line that could not be rendered is:

Термінове оновлення !!!

Which translates to English as:

Urgent Update

Clicking on the forged [redacted].gov.ua update link leads to a bit.ly URL shortener link that goes to redirect[.]co.ua, which then redirects to a predetermined download site that contains the following zip file:

hxxp://2215[.]site/soft2/Update-AV[.]zip

This Update-AV file [C33A905E513005CEE9071ED10933B8E6A11BE2335755660E3F7B2ADF554F704A] is also a malicious Saint_v3 file. The icon used by this malware is the country's flag with a shield on it to lend a sense that this is a legitimate protection update, as the email alluded to.

Figure 12: Malicious Update-AV file

Notice the similarity in the nomenclature between both domains (2215[.]site and 2330[.]site). The 2215[.]site domain is registered to fed****kar@rambler[.]ru. As of April 21st, both of these domains share the same IP address, [176[.]113.115.133]. While performing a dig on both domains we discovered the following:

Figure 13. Dig for 2215[.]site

Figure 13b. Dig for 2330[.]site

We can assume that these sites are both under the control of the same attacker or attacking group. Because of the similarity of the attacks to the examples above, we will focus on the shared infrastructure between the 2330[.]site and 2215[.]site that ties both campaigns together.

Connecting the dots

A search on the 2330[.]site domain reveals that the domain is registered to the email contact kun*******1969@rambler[.]ru. Subsequent searches reveal that the registrant owns the following domains:

1017[.]site

1202[.]site

2330[.]site

29572459487545-4543543-543534255-454-35432524-5243523-234543[.]xyz (this had only been registered for three days at the time of writing)

Below is a screenshot tying in the infrastructure below, along with the connection to the IP address 176[.]113.115.133 to the following domains:

2330[.]site

2115[.]site

29572459487545-4543543-543534255-454-35432524-5243523-234543[.]xyz

Figure 14. Shared infrastructure

C2 Infrastructure

This is the 2330[.]site DNS over time:

Date	Class	Type	IP
2021/01/11 04:08:54 PM	IN	A	95[.]143.218.55
2021/04/20 11:27:04 PM	IN	A	185[.]195.27.112
2021/04/21 10:01:25 PM	IN	A	176[.]113.115.133

This is the name4050[.]com DNS Over time

Timestamp	Class	Type	Response
2021/04/03 07:10:58 AM	IN	A	31[.]42.185.63

Conclusion

The spearphishing examples above highlight the ways that attackers leverage simple techniques to coerce and compel a target into following a link. Although, the attacker in this case has spent time crafting the spearphishing email, setting up the fake URLs that lead elsewhere, and using the Saint_v3 malware, this is by no means a sophisticated attack. But planning something like this, including the infrastructure that goes with it, takes time and resources.

One example of the lack of sophistication of this spearphishing email is that it is obvious that the message body appears to be rushed, given the grammar issues, etc. And the strategy used is not unique. It is the same old spearphishing strategy that we’ve seen many times before. However, the Covid-21 lure is unique and preys on the public’s fears of the unknown.

What is most concerning is that such attacks are often successful, and the malware being delivered can just be the beginning of a bigger attack as Saint itself is a downloader. And once a backdoor access is achieved, a multitude of things can occur, such as a ransomware infection, damage to the reputation and bottom line of any organizations, and given the agencies targeted in this campaign, the potential loss of sensitive information and state secrets.

In the grand scheme of things, it doesn’t really matter how ineffective or rushed an attack like this might be, because all it takes is a one mistake by one of the targeted victims. And once this occurs, the attacker has a beachhead within which to establish a foothold. When political tensions are high, gathering intelligence is critical. And it is easy to just send widespread and far flung lures in the hope of getting one person to fall prey as part of a larger strategy. All it takes is one bite and you are in.

Attackers know that there are many layers of security that they have to get through to get the data or resources they are targeting. And although there have been many technological advancements in security over time, the weakest link in any defense is still the human one. Because humans are fallible, organization must take the time to train and emphasize to its employees that such attacks exist—and happen quite often. They need to be the focus of continuous internal security training sessions, as no amount of technology can stop human curiosity, fear, and misjudgment.

Fortinet Protections

Fortinet customers are already protected from this Saint V3 campaign and associated files with FortiGuard’s AntiVirus and WebFiltering services, as follows:

The redirected URLs launched from the Word Document and LNK samples are rated as "Malicious Websites" by the FortiGuard Web Filtering service.

The attached "Covid-21" Word Document file is detected as “RTF/CoinMiner.OIE!exploit” the index.txt [AutoIT exfiltrator] file is detected as "W32/GenKryptik.FDZD!tr," the WindowsUpdate.exe [AutoIT exfiltrator] is detected as "W32/Kryptik.HKKC!tr" and the Saintv3 downloader "W32/Kryptik.HKMB!tr" are blocked by the FortiGuard AntiVirus service.

For FortiEDR protections, all published IOC's were added to our Cloud intelligence and will be blocked if executed on customer systems.

The FortiGuard AntiVirus service is supported by FortiGate, FortiMail, FortiClient, and FortiEDR. The Fortinet AntiVirus engine is a part of each of those solutions as well. As a result, customers who have these products with up-to-date protections are protected.

We also suggest our readers to go through the free NSE training -- NSE 1 – Information Security Awareness, which has a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

Fortinet’s Phishing Simulation Service, FortiPhish, can also be used to proactively test the susceptibility of your organization to these kinds of phishing attacks.

MITRE ATT&CK:

Initial Access

==============

Spearphishing Link - T1566.002

Execution

=========

PowerShell - T1059.001

Windows Command Shell - T1059.003

Execution for Client Execution - T1203

Malicious Link - T1204.001

Defense Evasion

===============

Execution Guardrails - T1480

File Deletion - T1070.004

Discovery

=========

File and Directory Discovery - T1083

Collection

==========

Data from Local System - T1005

Command and Control

===================

Web Protocols - T1071.001

IOCs

File: COVID-21.doc

- Size: 4184194 bytes

- MD5: 44697AAD796C0D82C1ADBEE15FD1266B

- SHA256: 9803E65AFA5B8EEF0B6F7CED42EBD15F979889B791B8EADFC98E7F102853451A

Detected by FortiGuard Anti-Virus as: RTF/CoinMiner.OIE!exploit

File: index.txt

- Size: 744448 bytes

- MD5: D377C71F7DF1C515705EB6B0CC745F7D

- SHA256: 89DA9A4A5C26B7818E5660B33941B45C8838FA7CFA15685ADFE83FF84463799A

- AutoIT file stealer

Detected by FortiGuard Anti-Virus as: W32/GenKryptik.FDZD!tr

File: index.txt/Update-AV.exe

- Size: 229888 bytes

- MD5: 9AE3D8BA1311AF690523AEB2E69BB469

- SHA256: C33A905E513005CEE9071ED10933B8E6A11BE2335755660E3F7B2ADF554F704A

- Saint_v3

Detected by FortiGuard Anti-Virus as: W32/Kryptik.HKMB!tr

File: WindowsUpdate.exe

- Size: 612352 bytes

- MD5: E4855693722DE3856421B1B6920BA54D

- SHA256: 0E1E2F87699A24D1D7B0D984C3622971028A0CAFAF665C791C70215F76C7C8FE

- AutoIT file stealer

Detected by FortiGuard Anti-Virus as: W32/Kryptik.HKKC!tr

The following URLs are blocked by the WebFiltering Client:

31[.]42.185.63

1017[.]site

1202[.]site

2330[.]site

name1d[.]site

name4050[.]com

http://smm2021[.]net/wp-adm/gate.php

29572459487545-4543543-543534255-454-35432524-5243523-234543[.]xyz

Learn more about FortiGuard Labs threat research and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training initiative or about the Fortinet NSE Training program, Security Academy program, and Veterans program.