Emotet’s Return Foreshadows Surge in Ransomware Attacks

CYBER THREAT ANALYSIS REPORT | JANUARY 2022
After a ten-month hiatus, Emotet returns with multiple spam campaigns delivering malicious documents to mailboxes worldwide. Commonly used by eCrime groups like Wizard Spider, the return of Emotet foreshadows a potential surge in ransomware attacks.

Emotet has been described as one of the world's most dangerous types of malware as it, Emotet ranks high among the most professional and long-lasting cybercrime services. Since it was discovered as a Trojan in 2014, the malware has evolved into the favored solution for cybercriminals. According to Europol, the Emotet infrastructure acts as a primary door opener for computer systems on a global scale. Once access is established, these are sold to other top-level criminal groups to deploy further illicit activities such as data theft and extortion through ransomware.

What makes Emotet so dangerous is that the malware is offered as Malware-as-a-Service (MaaS) for other cybercriminals to use as part of their ongoing operations. Often seen working in conjunction with Trickbot, and Ryuk, eCrime groups such as Wizard Spider have been known to use Emotet to act as a loader for what is known as 'Big Game Hunting'. Usually spread through malspam campaigns, targeted accounts receive phishing emails containing macro-laden Microsoft Word documents frequently masquerading as invoices, package delivery, or even unpaid bills. Once opened, these phishing emails execute Emotet on a victim's system. Emotet then acts as loader for advanced operations due to its ability to spread laterally across networks after gaining initial access. Once access and communication to the command and control server are established, the Trickbot banking trojan gets installed on the victim network. This allows adversaries to steal sensitive data such as bank credentials and other personal identifiable information. Shortly after Trickbot is installed, it is not uncommon for ransomware such as Ryuk to be deployed on a network.

In January of this year, globally coordinated action by law enforcement and judicial authorities successfully disrupted Emotet by taking control of its infrastructure. This operation was a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine, with Europol and Eurojust coordinating international activity. Infected machines of victims were redirected towards law enforcement-controlled infrastructure to effectively disrupt the threat actors’ activities. However, as anticipated, Emotet has resurfaced and is back to infecting networks around the world. More importantly, is that the return of Emotet signals a potential surge of ransomware attacks in the coming months.
Emotet

THREAT ANALYSIS

In November, the Trickbot banking trojan was observed downloading and executing updated Emotet binaries to computers previously infected with Trickbot. Malspam campaigns distributing Emotet resumed as well, with the classic Office document lures containing macros. These macro-laden Microsoft Excel, Microsoft Word, and a password-protected ZIP archive containing a Word document as payloads, mark the resurgence of the highly known, sophisticated threat.

**Figure 1:** This figure shows a phishing webpage using social engineering to get a user to click on the preview button.

**Figure 2:** This figure shows the document that is downloaded once the user clicks on the preview button shown above.
Emotet's downloaders are usually Microsoft Word formats (.DOC, .XML and .DOCX) which use VBA (Visual Basic for Applications) AutoOpen macros to execute code to the initial loader that will call out to one of several compromised websites to retrieve the Emotet payload. AutoOpen macros are a feature of Microsoft Office that enables document creators to automatically run a series of instructions when the document is opened. Recent versions of Microsoft Word are configured to disable running macros automatically by default. To overcome this mitigation, Emotet Word documents contain embedded images (figure 2) advising the user to click the “Enable Editing” button which will disable Microsoft Word’s read-only mode (Protected View), and “Enable Content” which will run the macro.

**Figure 3:** This figure shows a preview of the macro code contained inside of the malicious document.

```
1 Rem Attribute VBA ModuleType=VBA Module
2 Option VBASupport 1
3 Function ModifyVBAStyle()()
4 GoTo FmKBAR
5 Set ui[0]D3 = c3!G
6 Dim wXmHs, rdwZFK, DIM As Long
7 Dim zM43a3JMA As WordParagraph
8 Dim akXYV[] As Byte
9 For Each zM43a3JMA In SkySedbfre3x7q8.Paragraphs
10 akXYV = zM43a3JMA.Range
11 ssc = "^&" & akXYV & "^&" & akXYV.Range
```

Upon execution, the code shown above (figure 3) will assemble itself into a Base64 encoded PowerShell script (figure 4) which will reach out to a compromised website in order to retrieve a follow-on payload. While this action is occurring, the user will receive the error message “Word experienced an error trying to open the file”.

**Figure 4:** This figure shows the Base64 encoded PowerShell script that is assembled after the macros have executed.
**Figure 5:** This figure shows a heavily obfuscated PowerShell script that will be executed on the victim’s system.

This PowerShell script makes heavy use of string manipulation, and junk code in order to prevent analysis or at a minimum delay analysis through frustration. At first glance we can see that line 16 contains the domains this initial payload is looking to communicate with. In order to conduct our analysis we need to identify substitution patterns that will occur at run time.

**Figure 6:** This figure shows the resulting code after it has been decoded.
As we can see in the previous image (figure 6), after we conduct variable replacement and remove several lines of junk code, we can see that the script is only 29 lines long. In those 29 lines, it will look to create three subfolders in the user's home directory and name the next payload ‘E6_R.dll’. From there it will attempt to contact each of the domains listed in lines 10 - 16 one at a time in an effort to download the malicious dynamic-link library (DLL) – most likely Emotet. Afterwards, if the byte size of the downloaded file is greater than or equal to 33,120 bytes (approximately 32.34 kb in size), it will execute the Windows native executable rundll32.exe to load and run the 32-bit DLL.

**CONCLUSIONS**

Even though Emotet has made a resurgence thanks to Trickbot, its current methods of luring unsuspecting users to enable macros and its follow-on execution of obfuscated PowerShell scripts is still similar to its methods of operation prior to the international takedown since overall, Emotet’s code-base is solid. By moving Emotet to the Trickbot multipurpose ‘platform’, the authors now have the ability to take advantage of multiple attack vectors as well as having an additional botnet in their arsenal (along with their own Epoch4 and Epoch5). Emotet authors also improved the overall malware functionality, including: the addition of Elliptic Curve Cryptography (ECC) to better secure C2 channels; conducting processing monitoring on the victim system(s); and building a variant that deploys via Windows application installer package(s) so that it appears to be a legitimate executable.

All of these improvements point to Emotet authors recognizing the need for improved resiliency in the event of additional international action. It would not be a shock if other malware families follow suit and improve their overall ability to withstand the type of takedown that Emotet endured. Furthermore, it is only a matter of time until eCrime groups and other advanced threat actors modify Emotet, yet again, to include new functionality or repurpose it for their own needs. For now, defenders must continue to practice good cyber hygiene, understand our threat landscape, continue to recognize the signs of an attack, and learn how to rapidly report and remediate a perceived threat.
zveloCTI™ SOLUTIONS

zvelo CTI™ delivers meticulously curated, high veracity, actionable data on phishing and malicious domains which Threat Intelligence Teams can ingest for analysis and enrichment.

PHISHBLOCKLIST

zvelo’s AI-powered Phishing Intelligence detects phishing threats within the ActiveWeb traffic and other sensor-based data streams to deliver a richly packaged feed of highly curated and validated phishing threats that are enriched with additional metadata attributes like date detected, targeted brand, and other crucial data points.

MALICIOUS DETAILED DETECTION FEED

zvelo’s Malicious Intelligence identifies, confirms, and enriches malicious URLs for direct action by defenders and analysts. The data feed includes specific malicious URLs, as well as a range of metadata attributes such as date detected, malware family, and other significant intelligence data attributes.

THREAT INTELLIGENCE REPORTING

zvelo delivers meticulously curated, actionable Threat Intelligence data with industry leading accuracy and low false positive rates for maximum precision, efficacy and protection against evolving and emerging threats.

• Malicious Intelligence Reporting
• Phishing Intelligence Reporting
• Brand Threat Intelligence Reporting
• Exposed/Exploited Assets Reporting
• Additional Intelligence Reporting Available

ABOUT ZVELO

zvelo’s passion is to make the internet safer and more secure by providing the industry’s premium Cyber Threat Intelligence and web classification data services.

LEARN MORE

To learn more about zveloCTI or to request an evaluation, please contact us at sales@zvelo.com or visit www.zvelo.com.

www.zvelo.com
cybersecurity@zvelo.com