New EMOTET Hijacks a Windows API, Evades Sandbox

blog.trendmicro.com/trendlabs-security-intelligence/new-emotet-hijacks-windows-api-evades-sandbox-analysis/

November 15, 2017

Malware

We recently discovered that EMOTET has a new iteration with a few changes in its usual behavior and new routines that allow it to elude sandbox and malware analysis.

By: Rubio Wu November 15, 2017 Read time: (words)

We discussed the re-emergence of banking malware EMOTET in September and how it has adopted a wider scope since it wasn't picky about the industries it attacks. We recently discovered that EMOTET has a new iteration (detected as TSPY_EMOTET.SMD10) with a few changes in its usual behavior and new routines that allow it to elude sandbox and malware analysis.

Based on our findings, EMOTET's dropper changed from using RunPE to exploiting CreateTimerQueueTimer. CreateTimerQueueTimer is a Windows application programming interface (API) that creates a queue for timers. These timers are lightweight objects that enable the selection of a callback function at a specified time. The original function of the API is to be part of the process chain by creating a timer routine, but here, the callback function

of the API becomes EMOTET's actual payload. EMOTET seems to have traded RunPE for a Windows API because the exploitation of the former has become popular while the latter is lesser known, theoretically making it more difficult to detect by security scanners.

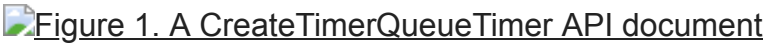
Figure 1. A CreateTimerQueueTimer API document

Figure 1. A CreateTimerQueueTimer API document (from CreateTimerQueueTimer function)


Figure 2. When the EMOTET dropper executes at Stage 4

Figure 2. When the EMOTET dropper executes at Stage 4, the Stage 5 payload at 0x 0x428310 will be injected to CreateTimerQueueTimer.

This is not the first malware we've seen abusing CreateTimerQueueTimer. Hancitor, a banking Trojan that dropped PONY and VAWTRAK, also exploited the API in its dropper, which is a malicious macro document.

Anti-Analysis and Anti-Sandbox Techniques

We also observed a new behavior in this variant, which is its anti-analysis technique. Some malware are designed to sleep for a period of time to avoid detection from malware analysis products. The analysis platform will change its sleep period to a very short time to scan for malicious activities. EMOTET's anti-analysis technique involves checking when the scanner monitors activities to dodge detection. CreateTimerQueueTimer helps EMOTET do the job every 0x3E8 milliseconds.

This variant has the ability to check if it's inside a sandbox environment at the second stage of its payload. The EMOTET loader will not proceed if it sees that it's running inside a sandbox environment.

The dropper will check for the following to discern whether it is running in a sandbox environment:

- When NetBIOS' name is TEQUILABOOMBOOM.
- When UserName is Wilber, NetBIOS' name starts with SC, and NetBIOS name starts with CW.
- When UserName is admin, DnsHostName is SystemIT, and if there's a Debugger symbol file like C:\\Symbols\aagmmc.pdb.
- When Username is admin, and NetBIOS name is KLONE_X64-PC
- When UserName is John Doe.
- When UserName is John and there are two files called C:\\take_screenshot.ps1 and C:\\loaddll.exe.
- When these files are present: C:\\email.doc, C:\\123\\email.doc, and C:\\123\\\email.docx.
- When these files are present: C:\\a\\foobar.bmp, C:\\a\\foobar.doc, and C:\\a\\foobar.gif.


Figure 3. When sample files are named sample., mlwr_smple. or artifact.exe, the malicious payload will also not be launched.

Figure 3. When sample files are named sample., mlwr_smple. or artifact.exe, the malicious payload will also not be launched.

As part of its unpacking technique, this variant will run itself through another process if it does not have admin privilege. If the process has admin privilege, it will proceed with the following:

1. Create new service as an auto start to make malware persistent
2. Change the service description to “Provides support for 3rd party protocol plug-ins for Internet Connection Sharing.”
3. Start the service.
4. Collect system information such as process name and system information
5. Encrypt the collected information via the AES-128 algorithm and SHA1 hash algorithm.
6. Encrypt the information and POST at the C&C server.

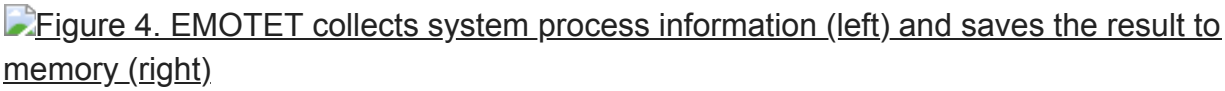
Figure 4. EMOTET collects system process information (left) and saves the result to memory (right)

Figure 4. EMOTET collects system process *information (left) and saves the result to memory (right)*

Figure 5. EMOTET collects information about the system version and current applications running under C:\\WOW64

*Figure 6. EMOTET C2 IP(*RED):PORT*(YELLOW) List*

Infection Chain

Figure 7. The variant’s infection chain

The infection chain of this variant starts with a phishing email. The email contains a malicious URL that will drop a document file containing a malicious macro.


Figure 8. EMOTET phishing email

Figure 8. EMOTET phishing email


Figure 9. Malicious EMOTET document

Figure 9. Malicious EMOTET document

Figure 10. The malicious macro inside the document will prompt cmd.exe and PowerShell to execute an encoded and obfuscated string.

Figure 10. The malicious macro inside the document will prompt cmd.exe and PowerShell to execute an encoded and obfuscated string.

The command downloads EMOTET from hxxp*://bonn-medien[.]de/RfThRpWC/* and will execute the dropper PE payload from the malicious site.

Figure 11. The network traffic of Powershell downloading the dropper

Figure 11. The network traffic of Powershell downloading the dropper from bonn-medien[.]de/RfThRpWC/

Enterprises and end-users can avoid threats like EMOTET by following best practices for defending against phishing attacks. Users should always be cautious of individuals or organizations that ask for personal information. Most companies will not ask for sensitive data from its customers. When in doubt, users should verify with the company to avoid any potential issues. Users should also avoid clicking links or downloading files even if they come from seemingly "trustworthy" sources. In addition, enterprises can stay protected by employing strong security policies to their email gateway and ensuring that their network infrastructure can filter, validate, and block malicious traffic like anomalous data exfiltration.

Trend Micro Solutions

Combating threats against the likes of EMOTET call for a multilayered and proactive approach to security—from the gateway, endpoints, networks, and servers. Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security can protect users and businesses from these threats by detecting malicious files, and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs.

Trend Micro™ Hosted Email Security is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Indicators of Compromise (IoCs)

SHA256

- Malicious document (W2KM_POWLOAD.AUSJTM)
  455be9278594633944bfdada541725a55e5ef3b7189ae13be8b311848d473b53
- Dropper sample (TSPY_EMOTET.SMD10)
  fbff242aeeff98285e000ef03cfa96e87d6d63c41080d531edcb455646b64eec
- Malicious macro (W2KM_EMOTET.DG)
  3f75ee07639bbcebf9b904debae1b40ae1e2f2cbfcef44caeda21a9dae71c982

Malicious C&Cs

- 164[.]208[.]152[.]175:8080
- 66[.]234[.]234[.]36:8080
- 62[.]210[.]86[.]114:8080
- 162[.]243[.]154[.]25:443
- 37[.]187[.]57[.].57:443
- 94[.]199[.]242[.]92:8080
- 178[.]254[.]33[.]12:8080
- 136[.]243[.]202[.]133:8080

C&C public key

-----BEGIN RSA PUBLIC KEY-----
MGcCYDeWo1m4l56rx8uAsn+gsDBAYoJARIdddsLOaiOf4oxe0GGy3IruKSmi
RSMfzj93sIHm88vzhJOeUkLES+RuDXUwSfob8u8bx5TjoSmY2kdmx5rgkp8U
NqD3z+P0m6bAxwIDAQAB -----END RSA PUBLIC KEY-----

Tags

Malware | Endpoints | Research