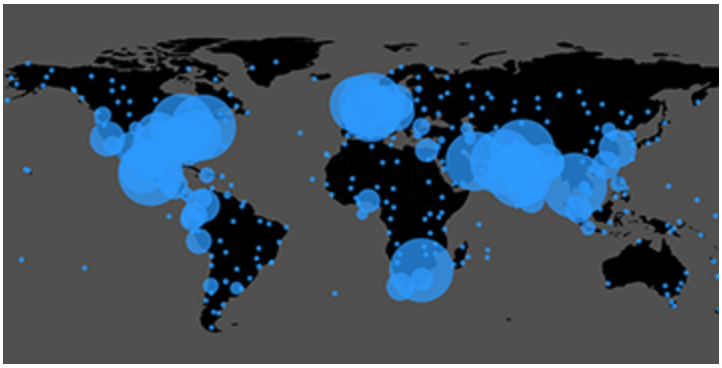
# Emotet Awakens With New Campaign of Mass Email Exfiltration

blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html



Authored by: Kryptos Logic Vantage Team on Wednesday, October 31, 2018
Tags: emotet

The Emotet malware family just raised the stakes by adding email exfiltration to its arsenal, thereby escalating its capabilities to cyber espionage. While it has recently made headlines for delivering ransomware payloads to United States infrastructure such as Water Utilities, Emotet has laid mostly dormant for the past month. In the past days, however, the mummy has returned just in time for Halloween as we observed a new module capable of exfiltrating email content back to the botnet's operators.

This new capability is effectively taking all existing Emotet infections with emails and sending them back to the attacker going back 180 days in mail history.

This post will examine the new threat payload enabling Emotet mass email capture, examine the exfiltration process, and observe its global distribution.

Even protected systems can be infected by this advanced malware. Be sure to check out Telltale, our free victim notification service if you wish to check if your organization has been infected.

## A Brief Overview of Emotet's Email Harvesting Module

Previous Emotet modules already used the Outlook Messaging API to steal contact lists. This API is, essentially, an interface that allows an application to become email-ready. The most common cases of MAPI usage are Simple MAPI, included in Windows as part of the default Windows Live email client, or the full MAPI as used by Outlook and Exchange. In other words, this API gives an application access to email, if Windows is adequately configured.

This configuration is the first thing checked by this module. In particular, the registry key `HKLM\Software\Clients\Mail\Microsoft Outlook` is accessed, and the value `DllPathEx` —the path to the `mapi32.dll` module—is expected to be defined. If it is not, the module does not proceed. Note that the registry key is pretty specific—there are other plausible keys, such as `HKLM\Software\Clients\Mail\Windows Mail`, that this module simply does not care about.

More specifically, for each email, the previous module queried

- Sender name and email;
- Destination name and email.

The new module ( `6cd44f2d00b43d80c08922d99d51cce804a59a54` ), however, is more thorough, and also includes email subjects and bodies. It will crawl every email of every subfolder in the interpersonal message (IPM) root folder, and

- Verify whether the email has been sent/received ( `PR_MESSAGE_DELIVERY_TIME` ) in the last 100e-9 * 15552000000 * 10000 / 3600 / 24 = 180 days;
- If so, obtain its sender ( `PR_SENDER_NAME_W` , `PR_SENDER_EMAIL_ADDRESS_W` ), destination ( `PR_RECEIVED_BY_NAME_W` , `PR_RECEIVED_BY_EMAIL_ADDRESS_W` ), subject ( `PR_SUBJECT_W` ) and body ( `PR_BODY_W` ).
- If the body is longer than 16384 characters, it is truncated to this size plus the string `...`.

A structure containing the above email information is then added to a global linked list which, upon termination, is written in Base64 encoding to a temporary file.

## How Emotet Actors Are Harvesting Your Emails

### Steps (click to expand)

It is important to emphasize that this module can be deployed in any existing Emotet infected systems (See Telltale global threat tracking below) and begin to harvest emails and send them back to the actor. In other words, Emotet will likely, over the next few days, harvest countless emails across tens of thousands of actively infected systems.

Here is how the process works (see also picture above):

1. An infected Emotet loads the module DLL from the command and control (C2) server, and this DLL injects the payload binary into a new Emotet process;
2. As described above, the new process scans all the emails, and saves results to a temporary file;

3. Original module DLL waits for this payload to finish (or kills it after 300 seconds), then reads the temporary file in its entirety;
4. Original DLL issues an HTTP request using the WinINet API, which will send the temporary file, if it is bigger than 116 bytes, to the C2 server.

## Telltale global threat tracking of Emotet (interactive)

**Tracking of Emotet Infections Worldwide. Even the whales appear infected.**

## Conclusion

Emotet was already a serious threat, incurring costs of up to 1 million dollars for a single incident, and recently unleashing ransomware on Onslow Water and Sewer Authority and other U.S. cities. The United States is by a wide margin the most affected country, which is consistent with our earlier report on Emotet. While Emotet's operators may have simply moved to server-side extraction, harvesting data in mass provides a weaponized data-driven analytical capability which should not be underestimated, given how effective surgical email leaks have been in the recent past.

Protecting against this actor is non-trivial. Emotet is arguably one of the most advanced botnets ever created. These actors appear to be aware of maintaining and designing very resilient and efficient distribution systems. Enterprises should be thinking about how to immediately reduce their risk exposure and act on this actionable intelligence. We'd like to thank our information sharing friends and intelligence partners, including Tim Davies.