The Return of Emotet

Author: Eric Patterson

Overview

On 17 July, Proofpoint's threat research team observed a malicious spam (malspam) campaign featuring the return of the Emotet malware after a five-month hiatus. This was a sizable campaign that included nearly a quarter million malspam messages.[1] While the scope of this campaign differs from our previous report on Emotet,[2] the tactics and techniques it uses are largely the same.

Customer Impact

Threat actors use Emotet to steal stored passwords, sensitive banking data, and browser histories from victims' computers.

The threat actors behind Emotet have repeatedly evolved the malware over time, including supplementing its native banking trojan functionality with third party tools that help to increase the malware's capabilities, such as Qakbot,[3] Trickbot,[4] or IcedID.[5]

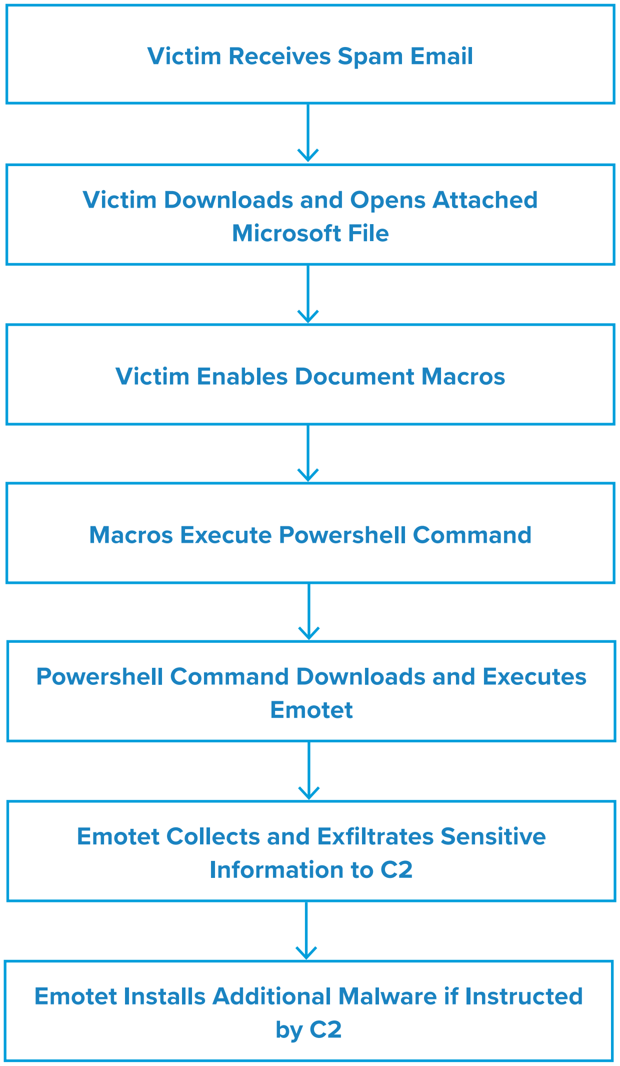
Emotet's capabilities may vary depending on the additional malware that the threat actor chooses to deliver, but they typically involve some form of credential stealer along with modules that allow the threat actor to expand the scope of their attack. These modules may include network exploits that allow the threat to move laterally within an organization's network, as well as address book harvesters that can be used to identify targets for future malspam campaigns.

Campaign Analysis

The email lures observed in this campaign are simple in nature and are similar to lures that Emotet has previously used. The subject lines are largely generic terms like "Re:" or "Invoice#" followed by a series of numbers, but some also include the names of targeted organizations. Message bodies are generic and reference an attachment that the user must open. The attachments are Microsoft Office documents (e.g. Word or Excel) with filenames themed after common business documents like payroll and resumes.

Attack Chain

When the user opens the attached document, they are directed to enable macros. Once the user enables macros, the macros execute a Powershell (*powershell.exe*) command that attempts to download the Emotet payload (*WFSR.exe*) from one of five Base64-encoded domain names embedded in the command. If this download is successful then the Powershell command proceeds to execute the Emotet payload.


Victim Receives Spam Email
Victim Downloads and Opens Attached Microsoft File
Victim Enables Document Macros
Macros Execute Powershell Command
Powershell Command Downloads and Executes Emotet
Emotet Collects and Exfiltrates Sensitive Information to C2
Emotet Installs Additional Malware if Instructed by C2

Upon execution, Emotet attempts to steal sensitive information from the victim and exfiltrate this data to one of its command and control (C2) servers. After stealing the victim's information Emotet will typically attempt to install additional malware, but it is currently unclear what additional payloads this particular campaign may be delivering.

Vulnerabilities & Mitigation

Emotet is distributed via spam emails, so many of the generic precautions regarding malspam apply. Infoblox recommends the following actions to reduce the risk of this type of infection:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- A subject line or email body with the user's name does not increase the validity of the message. Likewise, just because an email appears to be part of an existing thread does not mean it is; if it does not seem to fit the context of the discussion, treat the message as a potential phish.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Never enable macros and do not configure settings to enable macros by default. They are a common infection vector that many families of malware use.
- Never click on URLs in emails from unknown sources.
- Ensure the system's file sharing capability is closed and protected with a strong password.

Endnotes

1. https://www.proofpoint.com/us/blog/security-briefs/emotet-returns-after-five-month-hiatus
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--53
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--68
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--77
5. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--78

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com