How Emotet Stole Christmas

Author: James Barnett

Overview

Leading up to 25 December, Infoblox observed an email campaign themed around both Christmas and Swedish environmental activist Greta Thunberg to lure recipients into opening Microsoft Word documents with malicious macros that infected victims with the Emotet information stealer.

Customer Impact

Emotet is an information stealer and trojan downloader that targets businesses and individuals around the world. It is distributed through malicious spam emails sent by compromised servers in many countries worldwide. The emails use a variety of schemes to entice users to open a weaponized Microsoft Word document.

Once Emotet infects a victim's device, it steals various sensitive credentials and communicates with its command and control (C2) server to receive further instructions. In many cases these instructions include downloading and installing additional malware.

Campaign Analysis

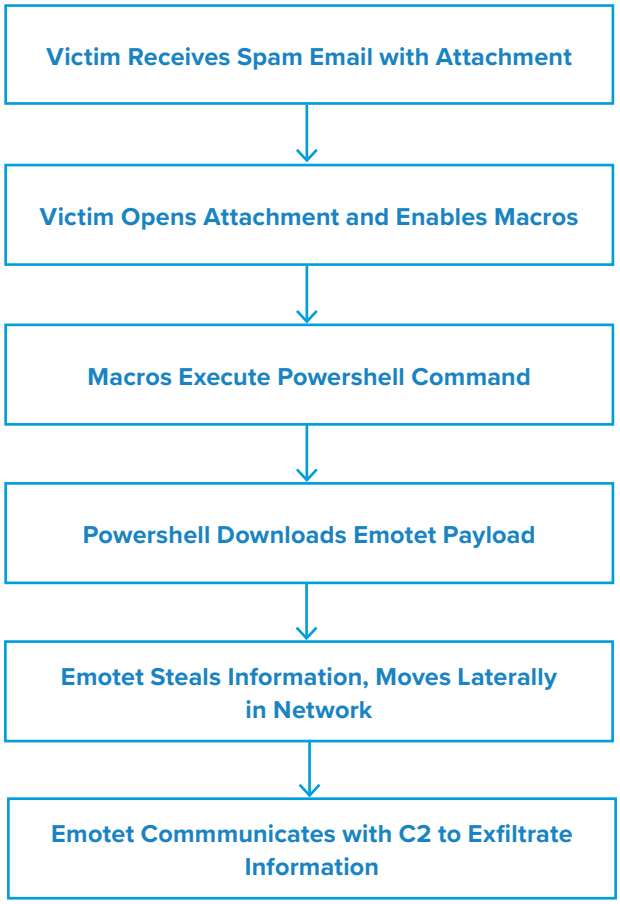
The campaign that Infoblox observed used emails whose subject lines often varied but always included Greta Thunberg's name. A majority of these subject lines also included the phrase "Time Person of the Year 2019."

The bodies of these emails were Christmas-themed messages that invited the recipient to participate in a protest related to climate change and instructed them to open an attached Word document for details. The emails we observed were composed in one of five different languages: English, French, German, Italian, and Polish.

Another notable aspect of this campaign was that the message concluded by requesting the recipient to forward the email to their friends, family, and colleagues. This is a relatively unusual approach for malicious spam campaigns, and while its purpose is unclear it may have been intended as a method of covertly infecting a relatively large number of systems.

Attack Chain

When the recipient opens the malicious Word document and enables macros, the macros decode and execute a Powershell command that downloads the Emotet payload from a compromised website, and then executes it.



Upon execution, Emotet attempts to spread laterally across the victim's network to infect additional devices while stealing sensitive information from all infected devices. Throughout the infection process Emotet routinely contacts its C2 servers to transmit stolen credentials, receive further instructions, and potentially retrieve additional malware payloads.

At the time we observed the malware no additional payloads were being delivered, which may be related to the campaign's unusual request for victims to forward the email to their contacts. Refraining from delivering additional payloads would increase the chances that victims might forward the email, thus increasing the spread of the Emotet infection and maximizing the effect of any additional payloads the threat actor may eventually deliver.

Vulnerabilities & Mitigation

Emotet uses several advanced countermeasures to bypass antivirus and firewall-based security, and its ability to move laterally through networks poses an additional risk for organizations. The best way for organizations to protect themselves is to ensure that users exercise proper caution when handling email attachments.

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Users should know that seeing their name in the subject line or body of the email 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 your 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 your system's file sharing capabilities are closed or protected with a strong password.

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