# Emotet Gets Political

*Author: Nick Sundvall*

## Overview

From October 16 to 19, we observed a malspam campaign that referenced political themes in the subject lines of the emails and in the attached file name. The campaign distributed the Emotet banking trojan. The threat actors spreading Emotet have previously used popular topics such as COVID-19 as lures.[1]

## Customer Impact

Emotet is a notorious banking trojan and infostealer that was first observed in 2014.[2] Emotet can steal banking data and passwords from a victim's computer, as well as download and install additional malware such as Trickbot or Qakbot.[3] Once it downloads additional malware, it can then spread laterally across a network by sending malicious emails to contacts of the infected victim, carrying out brute force attacks and using Trickbot to launch exploits such as EternalBlue.[4]

## Campaign Analysis

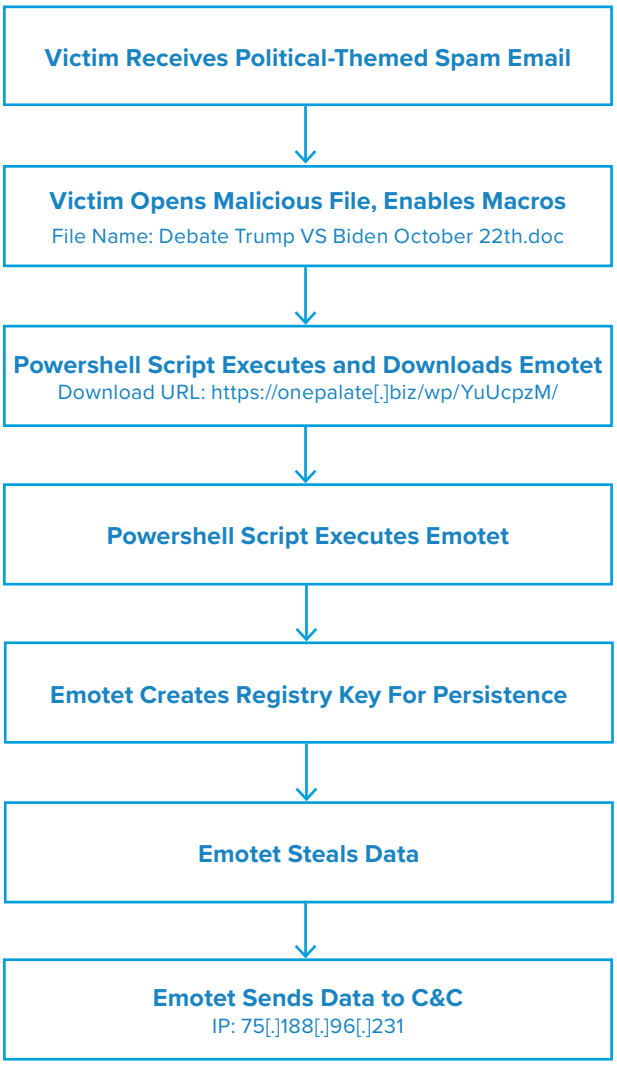
In this campaign, the threat actor used the upcoming presidential election as a lure by sending politically themed emails. Subjects of the emails included *Re: Trump-Ends Another Obama-Era Program and Marc*, *Save up to 30% on health insurance w/ TrumpCare*. Each of the emails had an attached file named *Debate Trump VS Biden October 22th.doc*, referencing the upcoming final presidential debate.

## Attack Chain

Upon opening the attached file, the victim will see a document prompting them to upgrade Microsoft Word by clicking "Enable Editing and then click Enable Content." Following these instructions enables macros and allows the malicious Visual Basic for Applications (VBA) code to run.

Once the victim enables the macros, the VBA code executes a Powershell script containing several URLs. It attempts to reach out to each until it successfully downloads the malicious Emotet payload.

After downloading the payload, the script uses Windows Management Instrumentation (WMI) to execute the payload as *Yzsk_77.exe*. To maintain persistence, the executable then copies itself to a folder in the *%AppData%* directory, as well as creates a new registry key to run the Emotet executable anytime the user logs onto their computer. From here, Emotet connects to its command and control (C&C) server at *75[.]188[.]96[.]231* and sends the stolen data.




## Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for Emotet. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

- Never configure Microsoft Office to enable macros by default. Many malware families use macros as an infection vector.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.
- Do not open attachments that are unexpected or from unfamiliar senders.

## Appendix

| Representative Indicators of Compromise | Description |
|---|---|
| Marc, Save up to 30% on health insurance w/ TrumpCare<br>See Your 2019 TrumpCare Eligibility Review, Marc.<br>Re: Trump-Ends Another Obama-Era Program | Email subject |
| Debate Trump VS Biden October 22th.doc | File attachment name |
| 3bae78182dad47ac43920171f44e275863e25a8cbdd07ac0b0279edb751dd12a<br>d684ed61705b1b1454f593263d3af902f854f6f32c217838fab990f4ad9d1a46<br>cfb29199ec6bb6dd95821e0506b52df13f7ac0f2a4579534454d7d6b025cdbc5<br>4f1b55b5cbbaa28b0d87b93dd256cebd16df18a51e081378940ad152fd24da8e | File attachment SHA256 |
| https://onepalate[.]biz/wp/YuUcpzM/<br>https://webdachieu[.]com/wp-admin/J/<br>http://smallbatchliving[.]com/wp-admin/uccE/<br>http://richellemarie[.]com/wp-admin/xlTWW/<br>http://richelleshadoan[.]com/wp-admin/Ucrkcvp/<br>http://holonchile[.]cl/purelove/Y4/<br>http://a2zarchitect[.]com/wp-admin/LAs0P/<br>https://raumfuerneues[.]eu/error/AuTiH/ | Download URLs |
| 75[.]188[.]96[.]231 | C&C server |

### Endnotes


1. https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/
2. https://www.malwarebytes.com/emotet/
3. https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service
4. https://securityboulevard.com/2019/10/a-closer-look-at-the-emotet-banking-trojan/