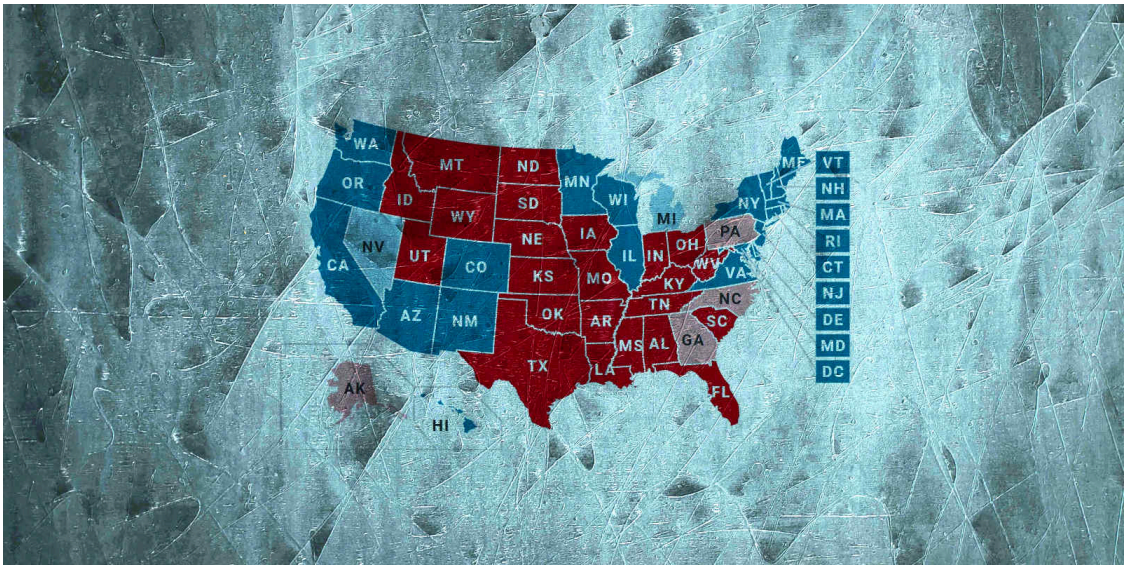
QBot phishing lures victims using US election interference emails

By Sergiu Gatlan

Published: 2020-11-04 · Archived: 2026-04-05 13:30:34 UTC



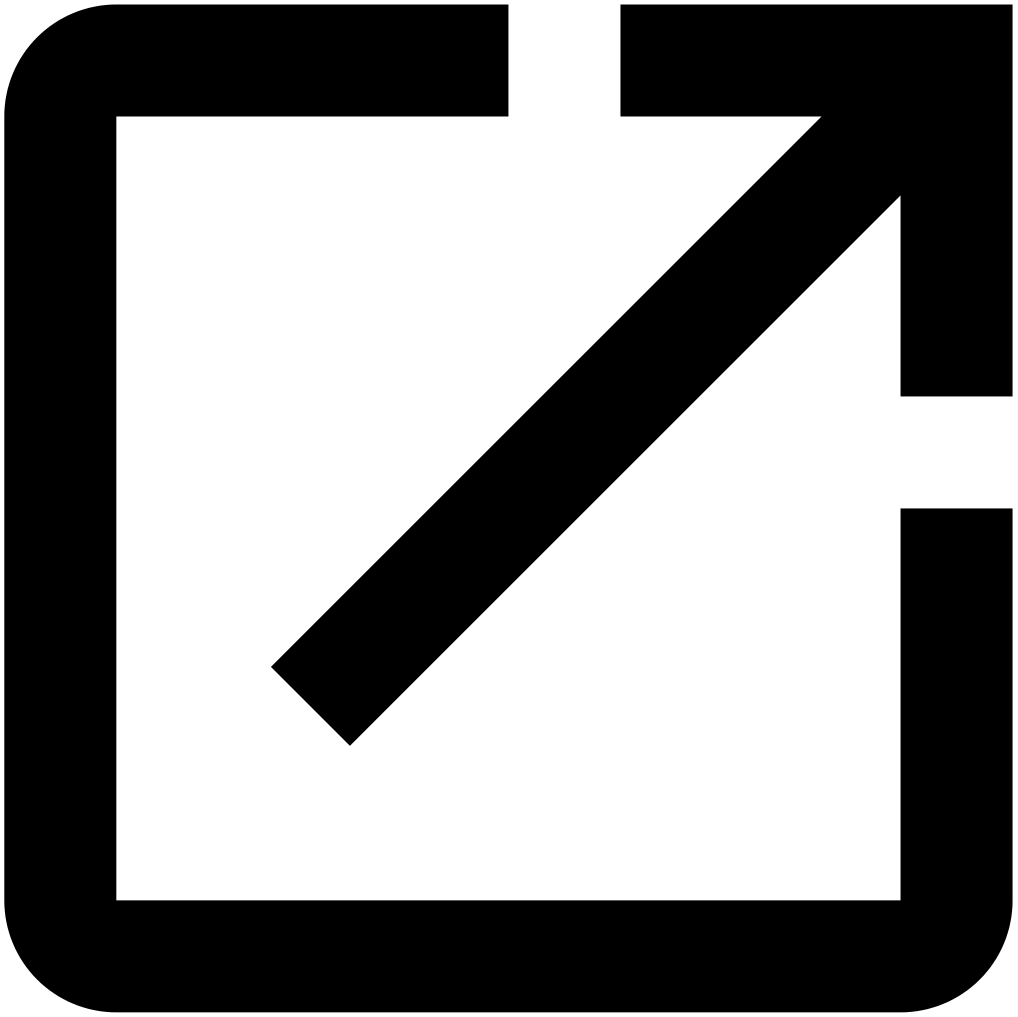
The Qbot botnet is now spewing U.S. election-themed phishing emails used to infect victims with malicious payloads designed to harvest user data and emails for use in future campaigns.

Qbot (aka Qakbot, Pinkslipbot, and Quakbot) is a banking trojan with worm features [1, 2, 3] actively used since at least 2009 to steal financial data and banking credentials, as well as to log user keystrokes, to deploy backdoors, and to drop additional malware.

Election interference baits

The malspam emails recently spotted by Malwarebytes Labs' Threat Intelligence Team are camouflaged as replies in previously stolen email threads, a tactic used to add legitimacy in the targets' eyes.


DIE LINKE.
0:00

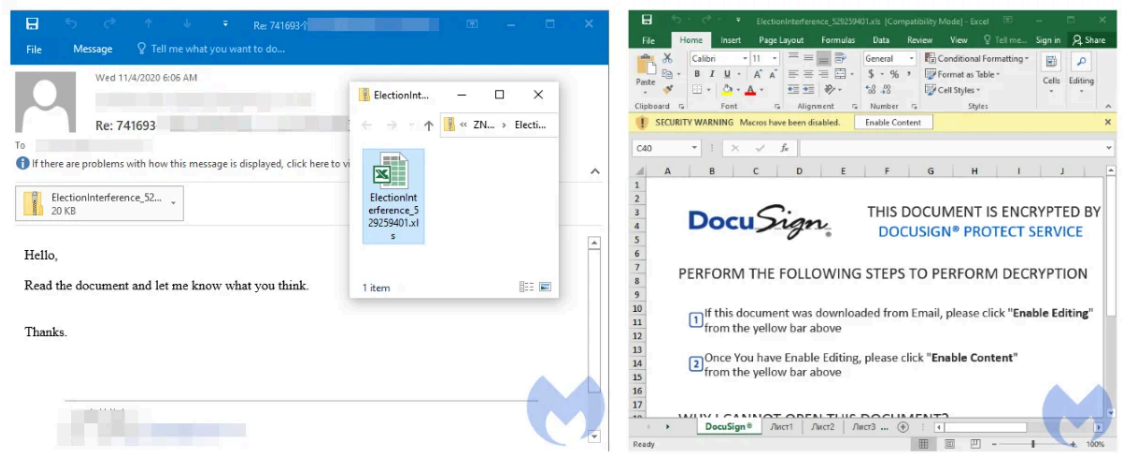


Each of the phishing messages come with malicious Excel spreadsheet attachments disguised as secure DocuSign file allegedly containing information related to election interference.

This new template has been adopted to abuse the public's concerns regarding the 2020 US elections' outcome, and to make it easier for the threat actors to lure potential victims into opening bait documents and enabling macros used to drop malware payloads.

After the Qbot malware is executed and infects the victims' computers, it will reach out to its command and control center to ask for further instructions.

"In addition to stealing and exfiltrating data from its victims, QBot will also start grabbing emails that will later be used as part of the next malspam campaigns," Malwarebytes' Jérôme Segura and Hossein Jazi explain.



Phishing email | Malicious attachment

Aggressive malware used in targeted campaigns

Besides phishing campaigns, attackers are also often using exploit kits to drop Qbot payloads, with the bot subsequently infecting other devices on the victims' network using network share exploits and highly aggressive brute-force attacks that target Active Directory admin accounts.

Even though active for over a decade, the Qbot banking trojan was mostly used in targeted attacks against corporate entities that provide a higher return on investment.

As proof of this, Qbot campaigns have been quite uncommon over time, with researchers detecting one in October 2014, one in April 2016, and another one in May 2017.

Qbot process flow (*Malwarebytes*)

Qbot has also seen a resurgence last year, being dropped as a first stage or as a second stage malware payload by the Emotet gang, as well as part of a context-aware phishing campaign in March 2019 using hijacked email threads.

During 2020, Qbot was used to harvest credentials from customers of dozens of U.S. financial institutions and to deliver ProLock ransomware following Qbot spear-phishing campaigns.

A full list of indicators of compromised (IOCs) including a matrix of MITRE ATT&CK techniques and malware sample hashes used in this Qbot campaign can be found at the end of the Malwarebytes report.

Source: https://www.bleepingcomputer.com/news/security/qbot-phishing-lures-victims-using-us-election-interference-emails/