QBot Malware Spotted Using Windows Defender Antivirus Lure

securityintelligence.com/news/qbot-malware-using-windows-defender-antivirus-lure/

News April 28, 2021

By David Bisson 2 min read

Attackers are using fake Windows Defender Antivirus emails to distribute QBot malware.

The QBot Attack Campaign

In late August 2020, Bleeping Computer revealed that QBot had begun using a new template in its email attacks.

This template also used stolen branding. It displayed a fake security warning from Windows Defender Antivirus within a Microsoft Word document. The fake alert also copied logos stolen from three other real firms.

According to the template, the sender supposedly encrypted the Word document with 'corporative firewall.'

It then instructed the user to decrypt the document's contents by clicking 'Enable Content' and enabling macros.

Compliance with that request caused the document's malicious macros to execute and to install Emotet malware on the victim's computer.

What Is Emotet?

Emotet is a complex trojan that commonly operates as a downloader of other malware samples. In the attack described above, Emotet downloaded QBot onto the victim's computer when installed.

During the summer of 2020, both Malwarebytes and Check Point observed a resurgence of Emotet activity after those responsible for the trojan had seemingly gone quiet for five months.

Emotet's handlers didn't hold back in the months that followed. At the beginning of October 2020, for instance, the U.S. Cybersecurity & Infrastructure Security Agency revealed in an advisory that it had detected 16,000 alerts pertaining to Emotet since July of that year.

The warning arrived just days after Bleeping Computer spotted an attack campaign in which Emotet capitalized on the interest surrounding the 2020 U.S. presidential election by sending out emails that referenced a legitimate Democratic National Convention initiative.

QBot Malware's Busy Year

QBot also had its fair share of fun last year.

Back in June, for instance, F5 Labs spotted a dedicated campaign in which digital attackers used a browser hijack or redirection to target banks in the United States with the information-stealing trojan.

Things ramped up in August when QBot entered Check Point's monthly top 10 malware index for the first time at 10th place. That same month, researchers at the security firm revealed that they had witnessed the malware using a new "email collector module" to extract email threads from a victim's Outlook client and to upload that data to a remote server under its attackers' control.

By the following month, this new trick had helped QBot to climb to sixth place on Check Point's malware list.

In November, QBot followed the example of Emotet by wading into the 2020 presidential election. In this case, email attackers used claims of election tampering to trick people into opening corrupted Excel files.

How to Defend Against QBot Malware

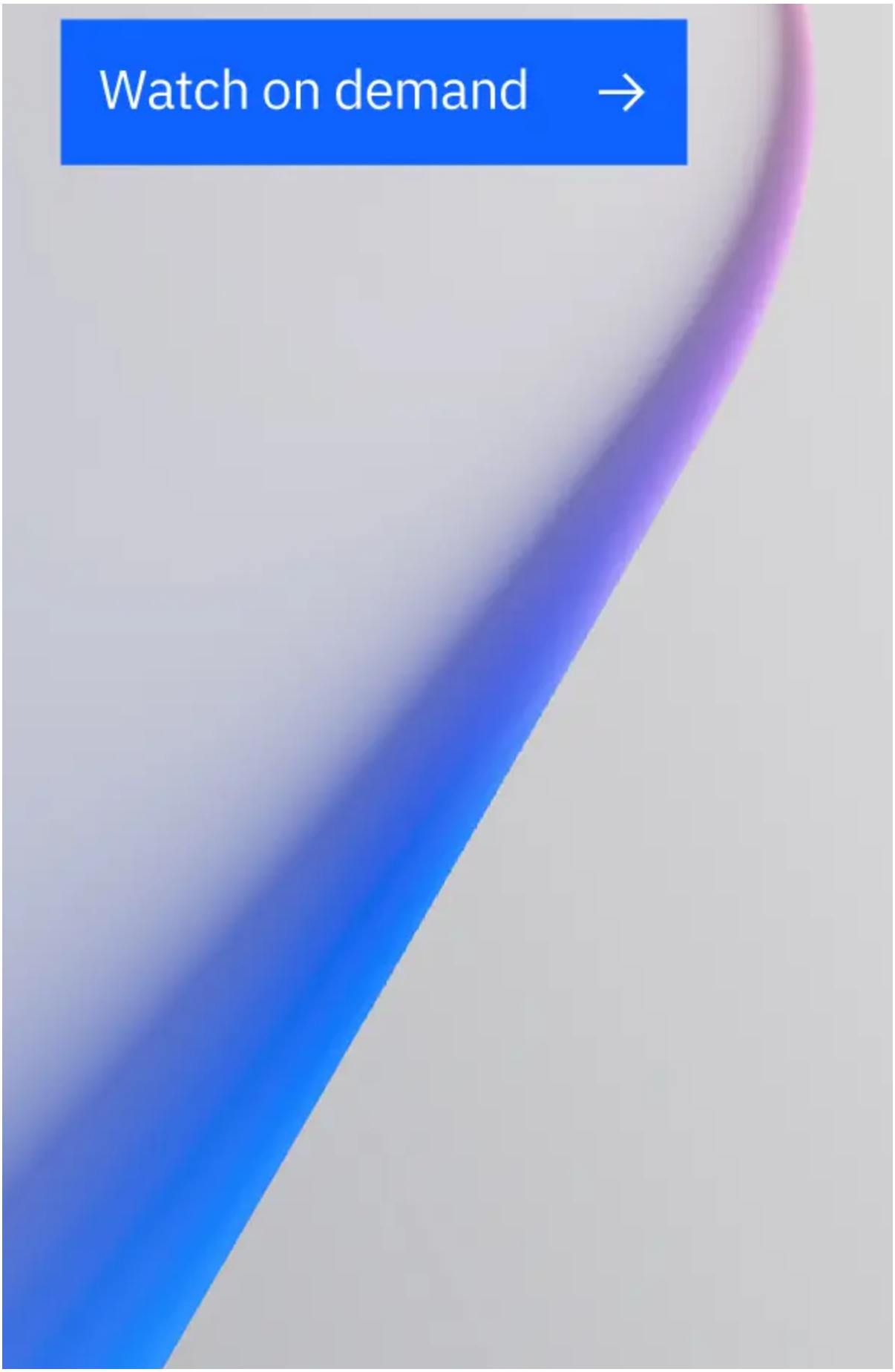
The persistence of threats such as QBot and Emotet highlights the need for defenses against email-borne malware. They can do this by regularly testing their employees' awareness with phishing attacks and by using role-based employee education to instruct the entire workforce about the types of threats that might enter their inboxes.

At the same time, consider developing dedicated incident response plans, processes and teams. These could help reduce the harm of a successful email attack that might be carrying a malware payload. To make sure they're protected, you should test those processes and plans on a regular basis.

Antivirus | Malware | Windows

David Bisson
Contributing Editor

David Bisson is an infosec news junkie and security journalist. He works as Contributing Editor for Graham Cluley Security News and Associate Editor for Trip...


Watch on demand