QBot uses Windows Defender Antivirus phishing bait to infect PCs

By Lawrence Abrams

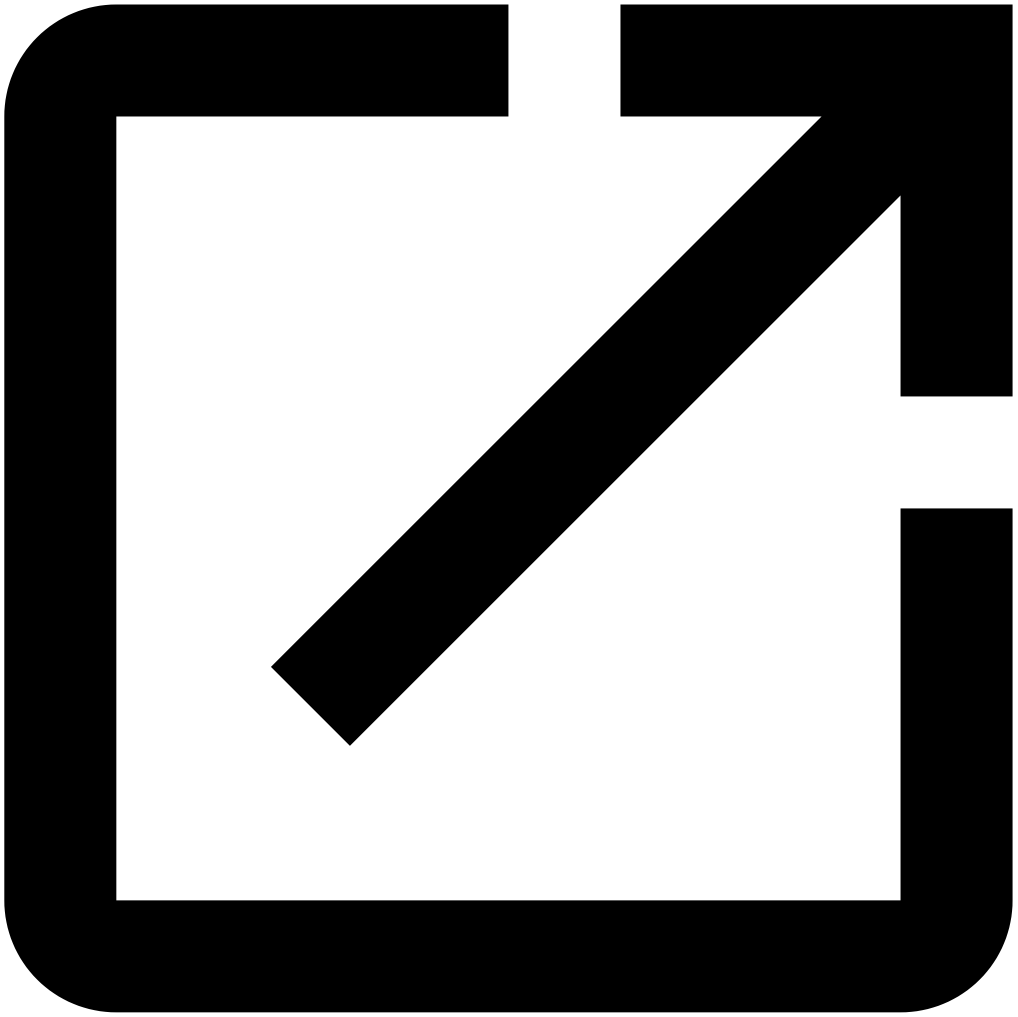
Published: 2020-10-12 · Archived: 2026-04-05 12:36:25 UTC

The Qbot botnet uses a new template for the distribution of their malware that uses a fake Windows Defender Antivirus theme to trick you into enabling Excel macros.

Qbot, otherwise known as QakBot or QuakBot, is Windows malware that steals bank credentials, Windows domain credentials, and provides remote access to threat actors who install ransomware.

Victims usually become infected with Qbot through another malware infection or via phishing campaigns using various lures, including fake invoices, payment and banking information, scanned documents, or invoices.


DIE LINKE.
0:00

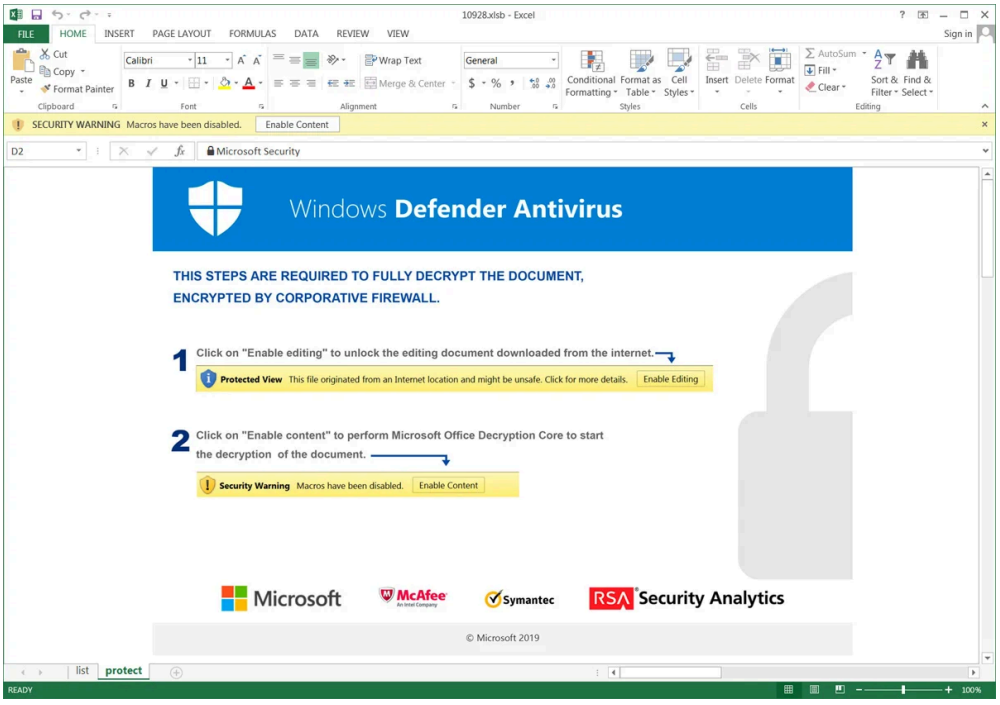


Attached to these spam emails are malicious Excel (.xls) attachments. When opened, these attachments will prompt a user to 'Enable Content' so that malicious macros will run to install the Qbot malware on a victim's computer.

To trick a user into clicking the 'Enable Content button, and thus enabling macros, threat actors use stylized document templates that pretend to be from a trustworthy organization or from your operating system.

On August 25th, the Qbot switched to a new template that pretends to be an alert from Windows Defender Antivirus, claiming that the document is encrypted.

To decrypt the document, users need to click on 'Enable Editing' or 'Enable Content' to decrypt it using the 'Microsoft Office Decryption Core.'



New 'Windows Defender Antivirus' Qbot attachment

Once enable content is clicked, malicious macros will be executed that download and install the Emotet malware on a victim's computer.

To people who work in cybersecurity, are IT admins, or Windows enthusiasts, the above message appears silly and made up. To casual users, though, it is convincing enough that many would follow the instructions and become infected with Qbot.

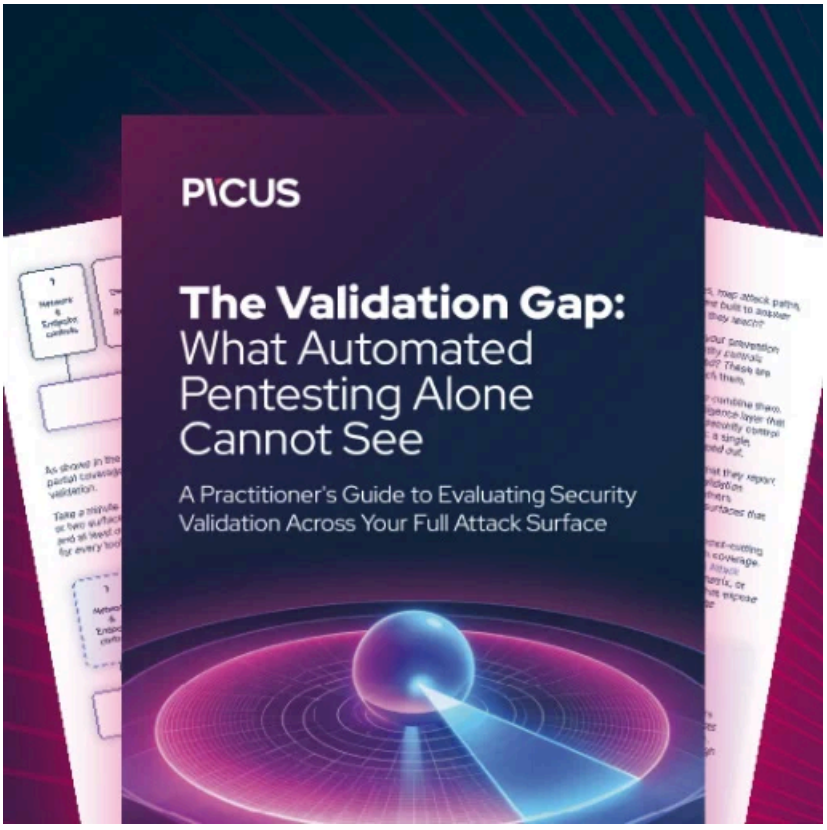
Why it's essential to recognize Qbot attachments?

Over the past couple of months, Qbot has seen increased distribution, especially after being delivered in spam spewed forth by the Emotet botnet.

When infected, Qbot performs various malicious activities that allow threat actors to gain access to your bank accounts and your network.

Once they gain access to a network, they install ransomware such as ProLock throughout the system.

Due to this, it is vital to recognize the malicious document templates used by Qbot so that you do not accidentally become infected.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
