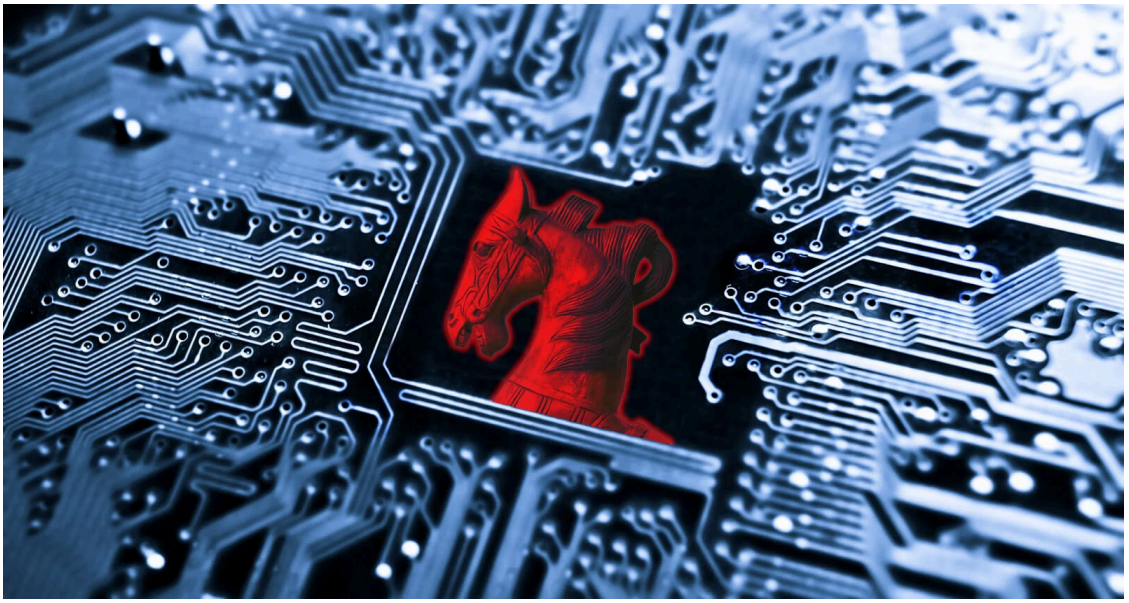
QBot malware is back replacing IcedID in malspam campaigns

By Ionut Ilascu

Published: 2021-04-13 · Archived: 2026-04-05 19:25:49 UTC

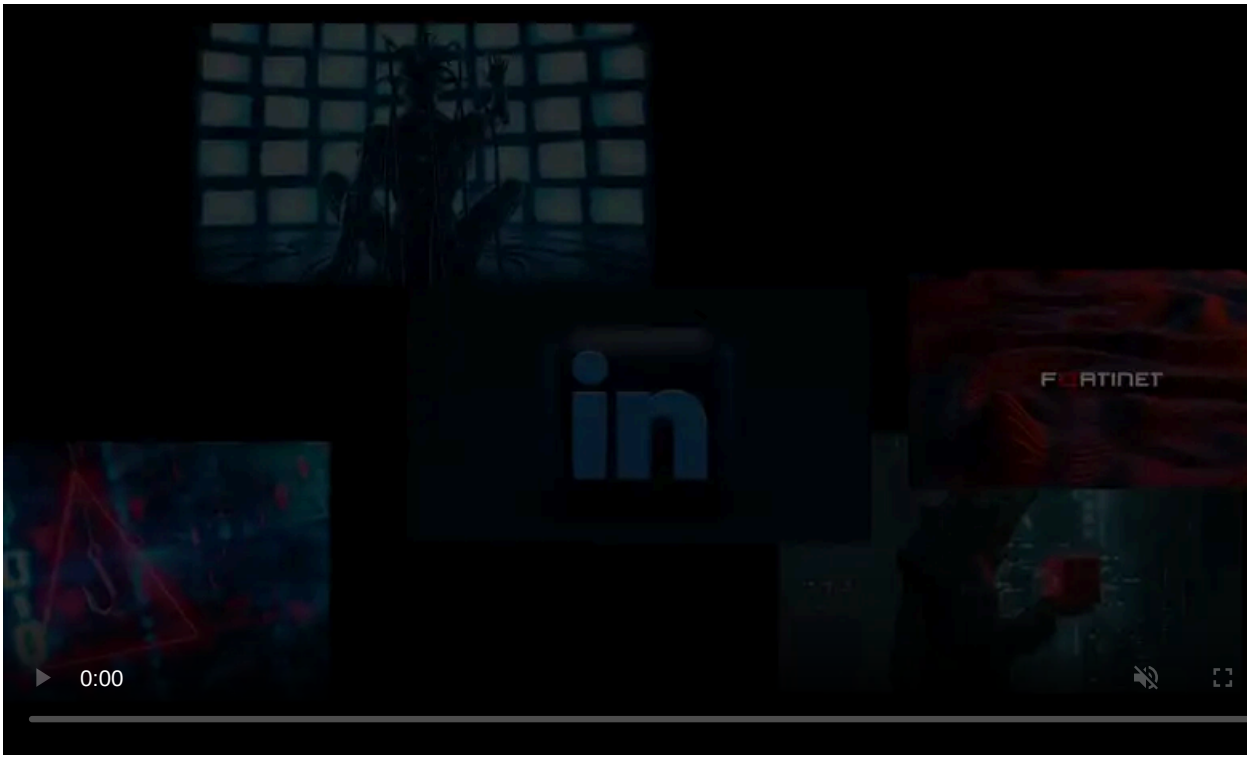


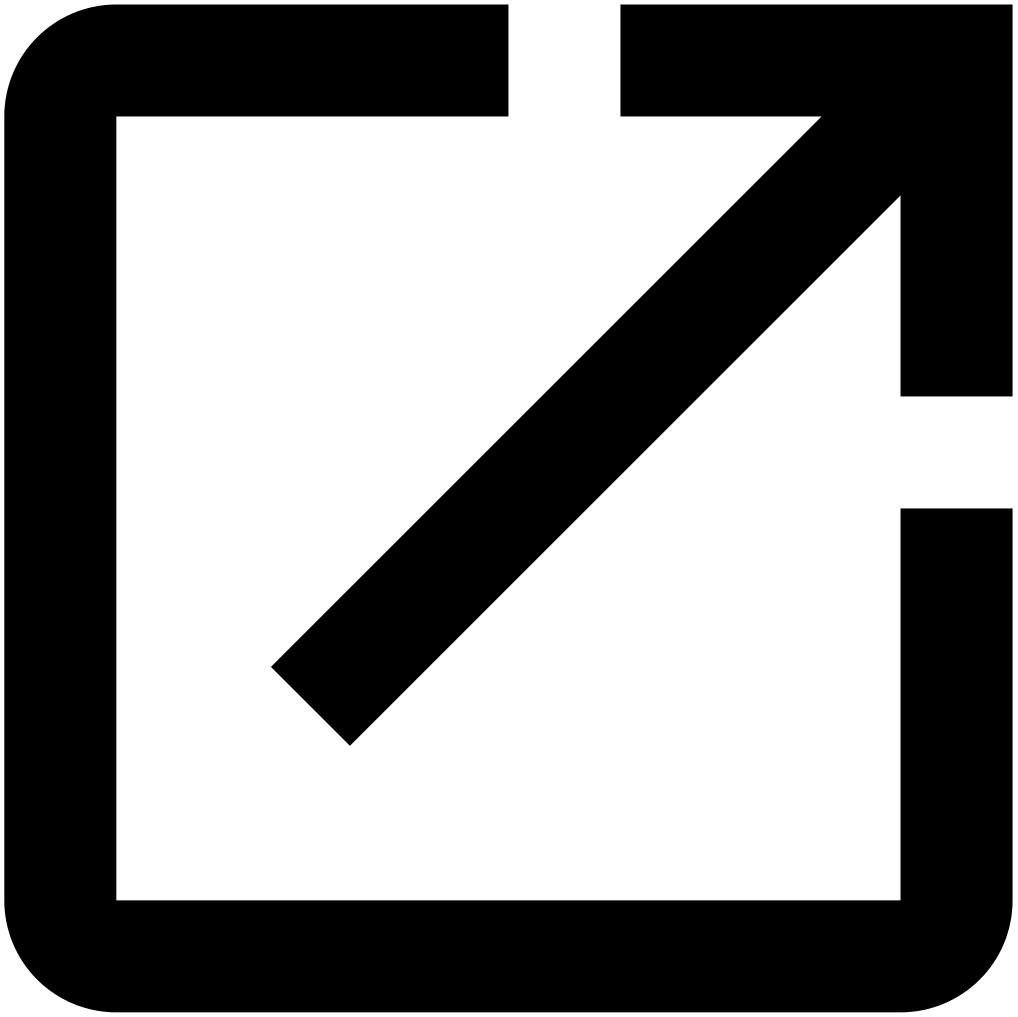
Malware distributors are rotating payloads once again, switching between trojans that are many times an intermediary stage in a longer infection chain.

In one case, the tango seems to be with QBot and IcedID, two banking trojans that are often seen delivering various ransomware strains as the final payload in the attack.

Return to initial payload

Earlier this year, researchers observed a malicious email campaign spreading weaponized Office documents that delivered QBot trojan, only to change the payload after a short while.


0:00



In February, IcedID was the new malware coming from the URLs that used to serve QBot. Brad Duncan of Palo Alto Networks caught the change and notes in his analysis at the time:

“HTTPS URL generated by the Excel macro ends with /ds/2202.gif which normally would deliver Qakbot, but today it delivered IcedID” - Brad Duncan

Threat researcher James Quinn of Binary Defense makes the same observation in a blog post in March, as the company discovered a new IcedID/BokBot variant while tracking a malicious spam campaign from a QakBot distributor.

IcedID started as a banking trojan in 2017 and adjusted its functionality for malware delivery. It has been seen distributing RansomExx, Maze, and Egregor ransomware in the past.

After about a gap of a month and a half, the malware distributor switched the payload back to QBot (a.k.a. QakBot), which has been seen delivering ProLock, Egregor, and DoppelPaymer ransomware in the past.

Malware researcher and reverse engineer reecDeep spotted the switch on Monday, saying that the campaign relies on updated XLM macros.

As seen in the screenshot above, the malicious Office file poses as a DocuSign document to trick users into enabling macro support that fetches the payload on the system.

The same trick is seen in the analysis from both Binary Defense and Brad Duncan on the malware distributor’s switch to delivering IcedID in February 2021.

Recently, security researchers at threat intelligence firm Intel 471 published details about EtterSilent, a malicious document builder that’s been gaining in popularity due to its constant development and ability to bypass several security mechanisms (Windows Defender, AMSI, email services).

One feature of the tool is that it can create malicious documents that look like DocuSign or DigiCert-protected files that require user interaction for decryption.

According to Intel 471, multiple cybercriminal groups started to use EtterSilent services, including IcedID, QakBot, Ursnif, and Trickbot.

Contacted by BleepingComputer about the recent switch to QakBot, James Quinn confirmed the campaigns, saying that all evidence points to "a fairly large update to QakBot" that comes with changed decryption algorithms for the internal configuration.

Quinn notes that this breaks the configuration extraction on many samples.

Source: https://www.bleepingcomputer.com/news/security/qbot-malware-is-back-replacing-icedid-in-malspam-campaigns/