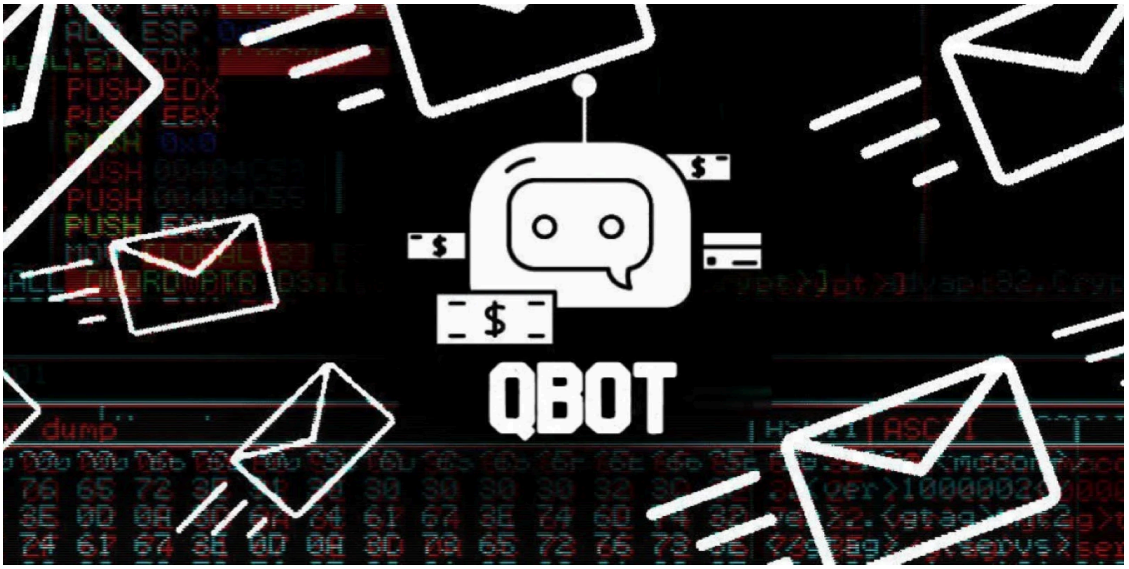
QBot partners with Egregor ransomware in bot-fueled attacks

By Lawrence Abrams

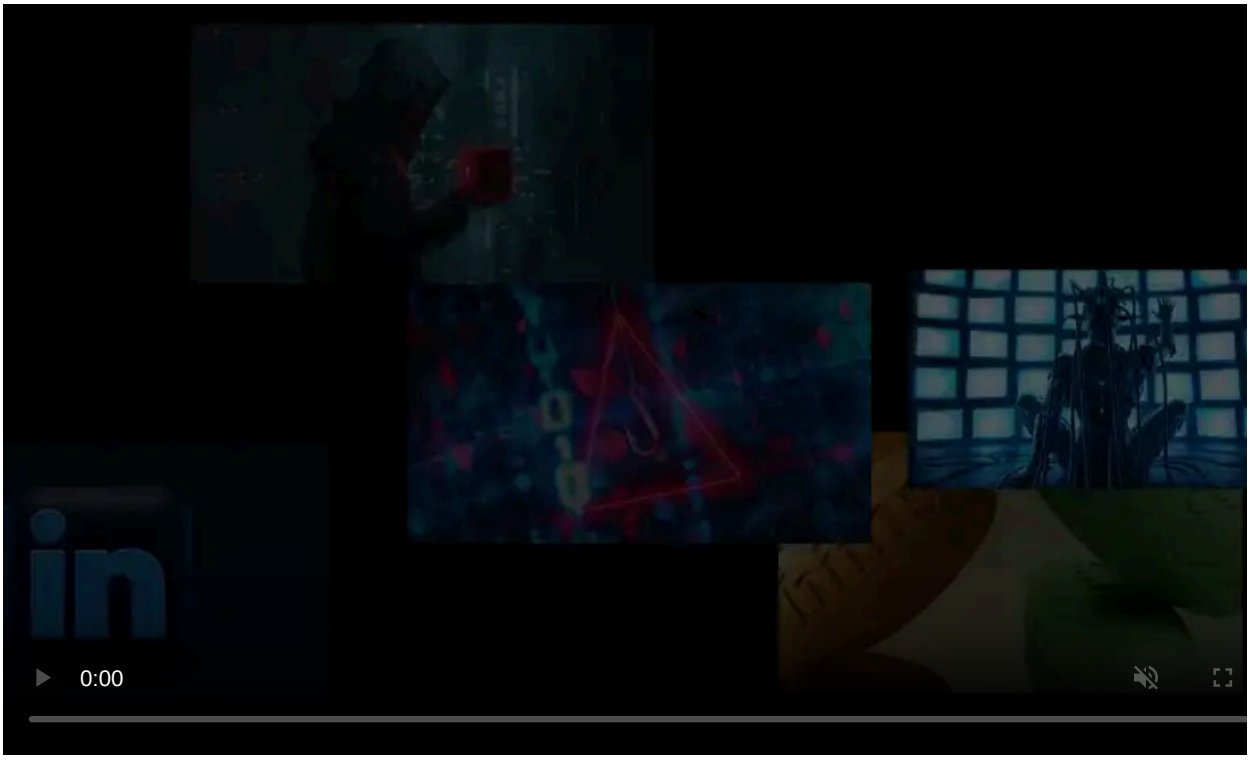
Published: 2020-11-20 · Archived: 2026-04-05 17:12:59 UTC

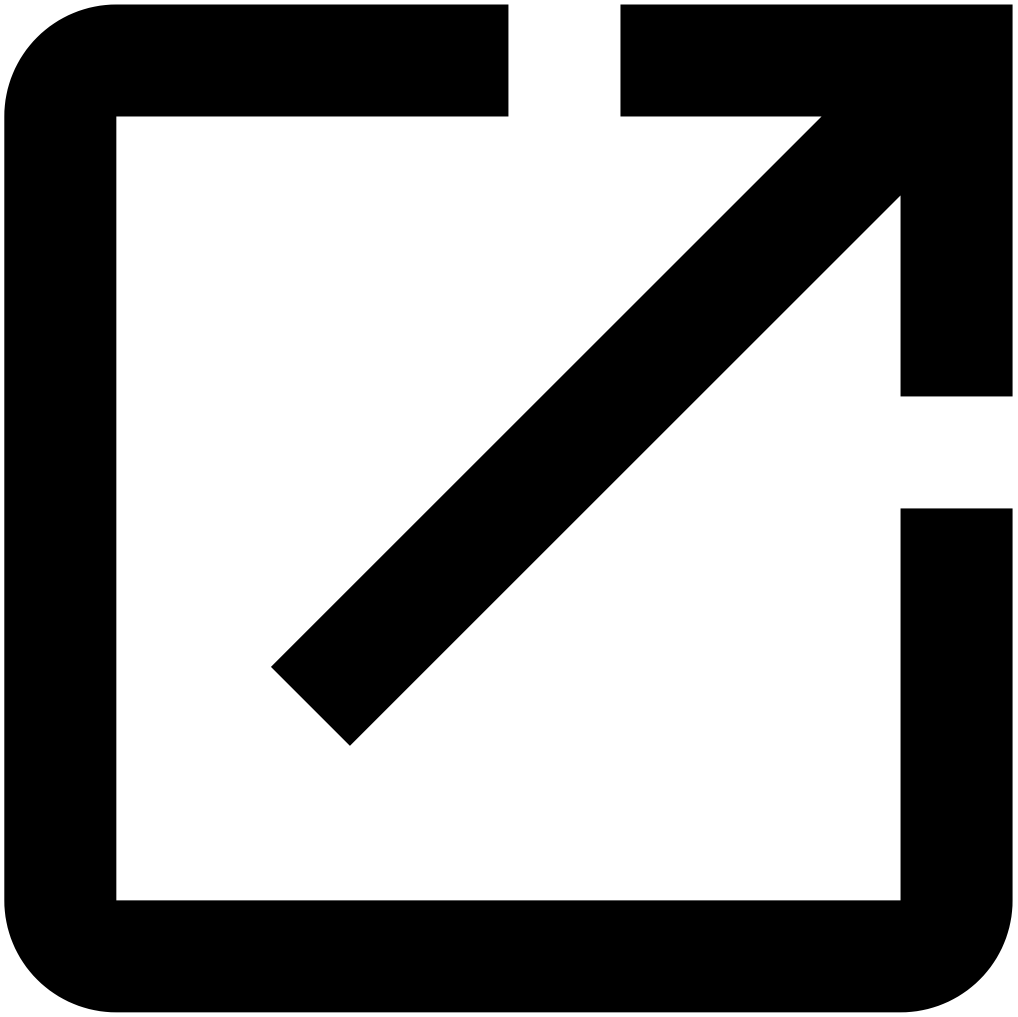


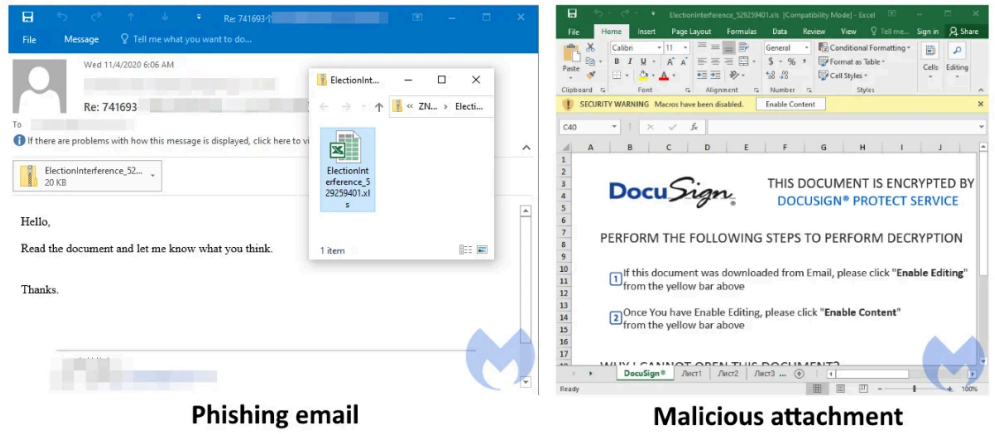
The Qbot banking trojan has dropped the ProLock ransomware in favor of the Egregor ransomware who burst into activity in September.

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 phishing emails utilizing Excel documents that pretend to be DocSign documents, as shown below.


0:00





Qbot Docusign phishing email

Similar to how Ryuk works with TrickBot and DoppelPaymer/BitPaymer work with Dridex for access to networks, the ProLock ransomware has historically worked with Qbot to gain access to compromised networks.

When the ransomware gang is given access to a network, they use the Cobalt Strike pentesting tool to remotely spread laterally through the network while stealing unencrypted files and gathering admin credentials.

Once the attackers gain access to a domain admin account, they use it to deploy the ransomware throughout the Windows domain.

Qbot dumps ProLock for Egregor ransomware

In a new report by Oleg Skulkin, Senior Digital Forensics Analyst at Group-IB. a Singapore-based cybersecurity company, has found that Qbot is has stopped distributing ProLock and is now working with Egregor.

Since their launch in September 2020, Egregor has been one of the most active big game hunting ransomware operations currently active.

After the notorious Maze ransomware gang began shutting down their operation in September, many of their affiliates moved to the new Egregor operation.

Fueled by experienced ex-Maze affiliates and hackers, Egregor quickly started amassing a huge amount of victims worldwide.

"In less than 3 months Egregor operators have managed to successfully hit 69 companies around the world with 32 targets in the US, 7 victims in France and Italy each, 6 in Germany, and 4 in the UK. Other victims happened to be from the APAC, Middle East, and Latin America. Egregor's favorite sectors are Manufacturing (28.9% of victims) and Retail (14.5%)," Skulkin explained.

Egregor activity since September 2020
Source: Group-IB

While the ransomware has changed, Skulkin states that the tactics, techniques, and procedures (TTPs) currently used by Egregor are similar to the previous attacks with ProLock.

'Tactics, techniques and procedures observed are very similar to those seen in the past Qakbot's Big Game Hunting operations," Skulkin stated in a report shared with BleepingComputer.

As more Maze affiliates become involved in the Egregor operation, Skulkin expects the TTPs to eventually align to those seen historically in Maze attacks.

As the ransomware landscape continually evolves, threat actors switch to different operations, and partnerships are made, it is important for security professionals to keep track of the TTPs used by each operation to defend against them.

"The use of CobaltStike and QakBot are to watch when hunting for Egregor. More threat hunting and detection tips from Group-IB DFIR team as well as a detailed technical analysis of Egregor operations are available in Group-IB's blog," Skulkin offers as advice when defending against Egregor.

Since its launch, Egregor has been responsible for other high profile attacks on Crytek, Ubisoft, Cencosud, and Barnes and Noble.
