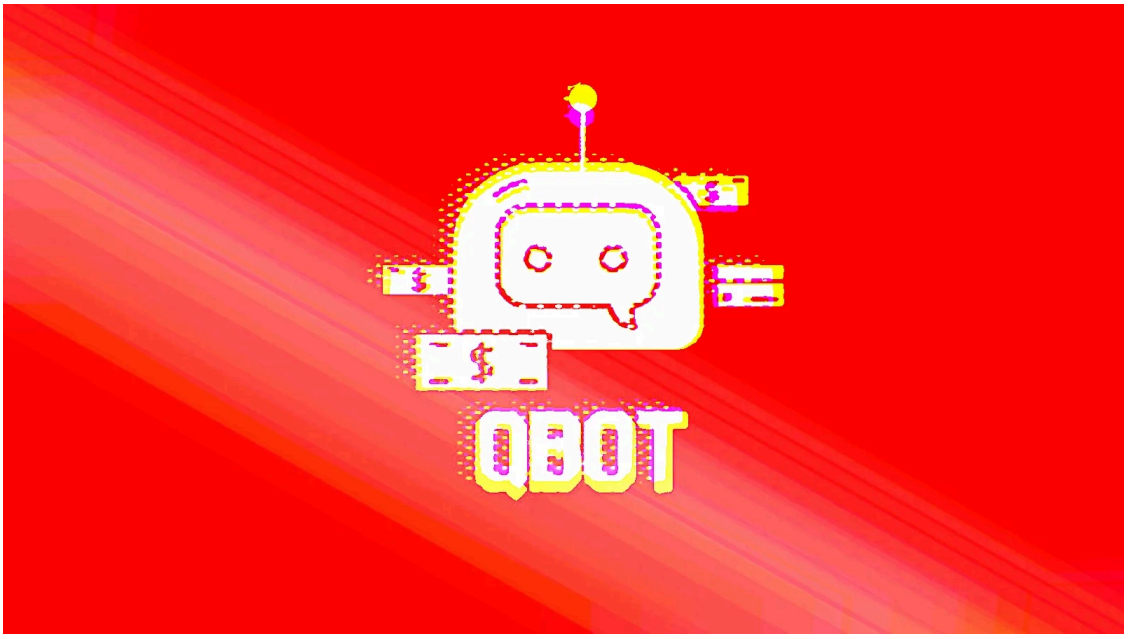
New Qbot malware variant uses fake Adobe installer popup for evasion

By Bill Toulas

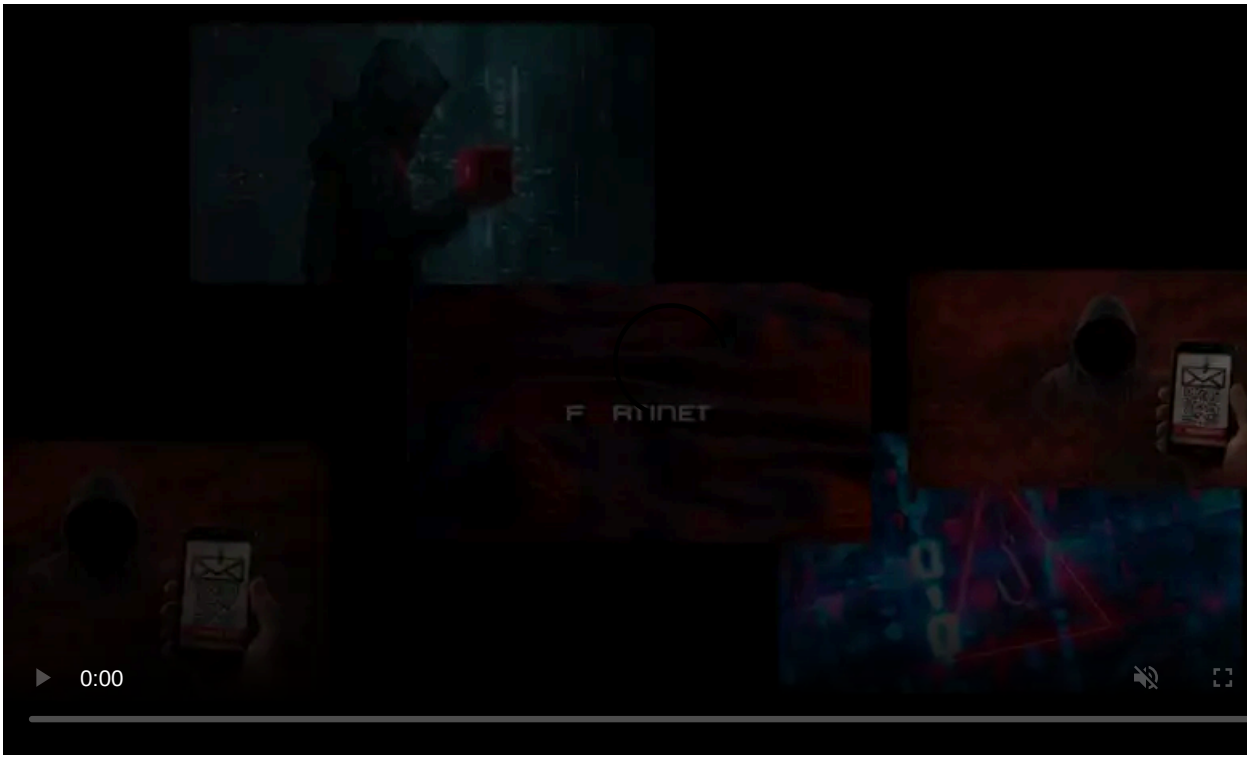
Published: 2024-02-15 · Archived: 2026-04-06 00:39:53 UTC

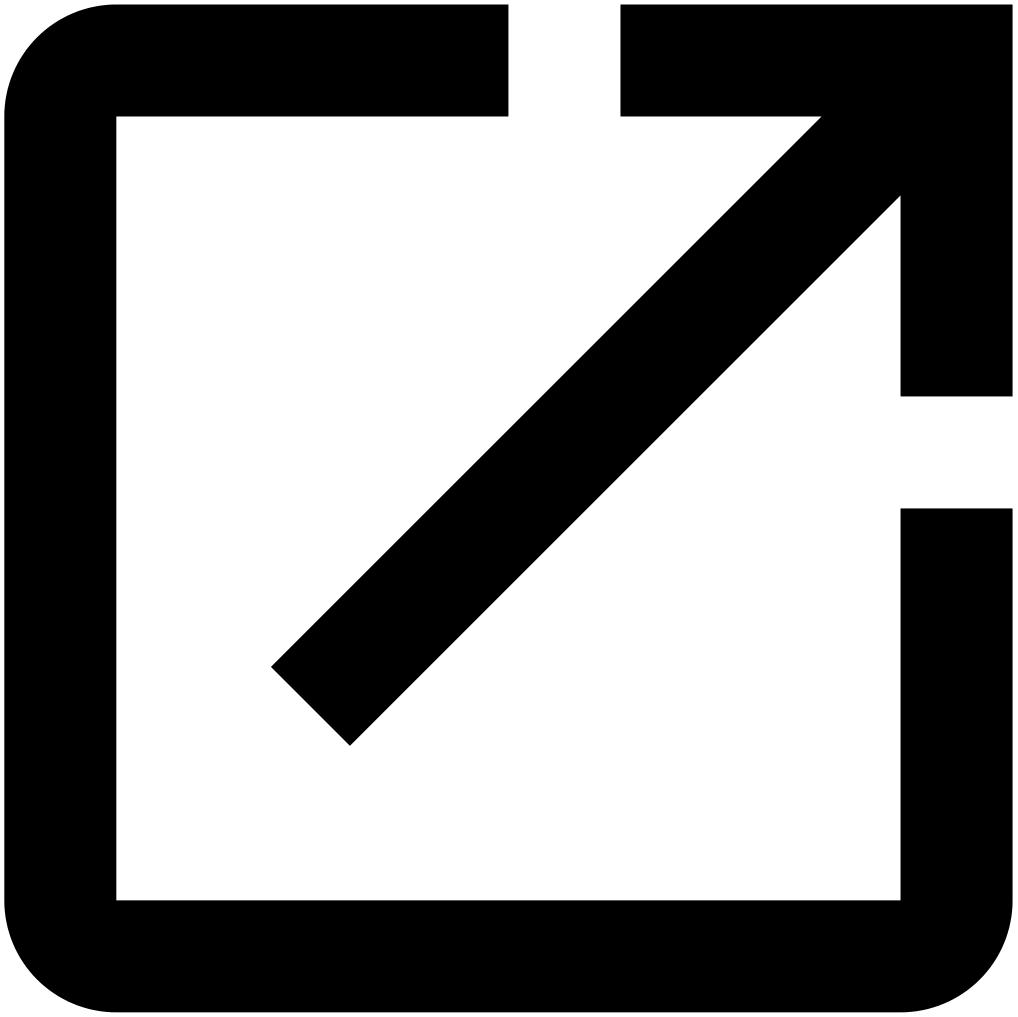


The developer of Qakbot malware, or someone with access to the source code, seems to be experimenting with new builds as fresh samples have been observed in email campaigns since mid-December.

One of the variants observed uses on Windows a fake installer for an Adobe product to trick the user into deploying the malware.

Also named QBot, the malware has served for many years as a loader for various malicious payloads, including ransowmare, delivered to victims mainly over email.


0:00



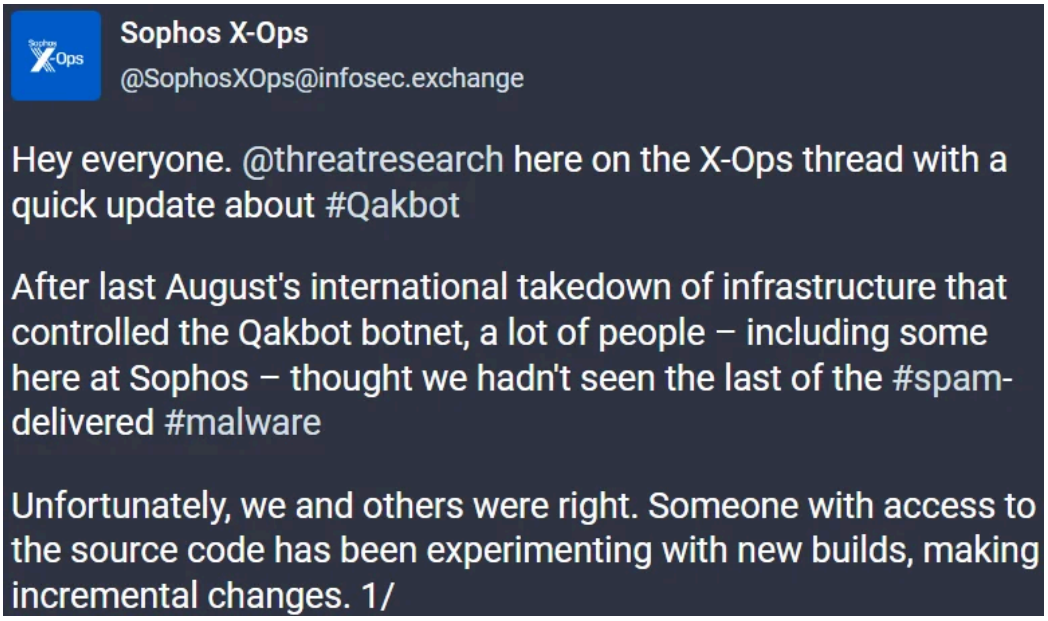
Until its takedown last August, QBot had infected over 700,000 systems and in just 18 months it caused financial damages estimated to more than $58 million.

Codenamed Duck Hunt, the operation didn't involve any arrests, and many security researchers believed that Qakbot developers would rebuild their infrastructure and restart the distribution campaigns.

Last year, Cisco Talos reported on a Qakbot campaign that had started before the takedown and was still active in early October. The researchers believe this was possible because law enforcement disrupted only the malware's command and control servers, not the spam delivery infrastructure.

In December 2023, Microsoft observed a QBot phishing campaign impersonating the IRS, confirming fears about the malware's return.

Sophos' advanced threat response joint task force, Sophos X-Ops, noticed fresh Qbot activity recently, with up to 10 new malware builds emerging since mid-December.



The new developments regarding Qbot have also been noticed by researchers at cloud security company Zscaler, who published in late January a technical report about the malware and its evolution since 2008.

New QBot variants

Sophos X-Ops analysts reverse-engineered new Qbot samples, noting small increments in the build number, which indicates that the developers are testing and refining the binaries.

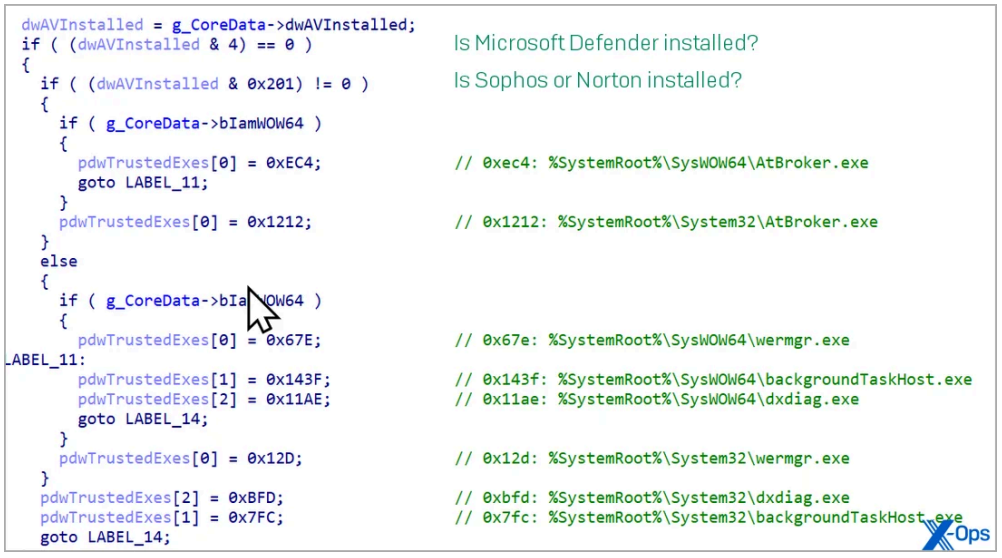
Samples from December and January came as a Microsoft Software Installer (.MSI) executable that dropped a DLL binary using a .CAB (Windows Cabinet) archive.

This method differs from previous versions that injected code into benign Windows processes (*AtBroker.exe*, *backgroundTaskHost.exe*, *dxdiag.exe*) to evade detection.

The new Qakbot variants use enhanced obfuscation techniques, including advanced encryption to hide strings and command-and-control (C2) communication.

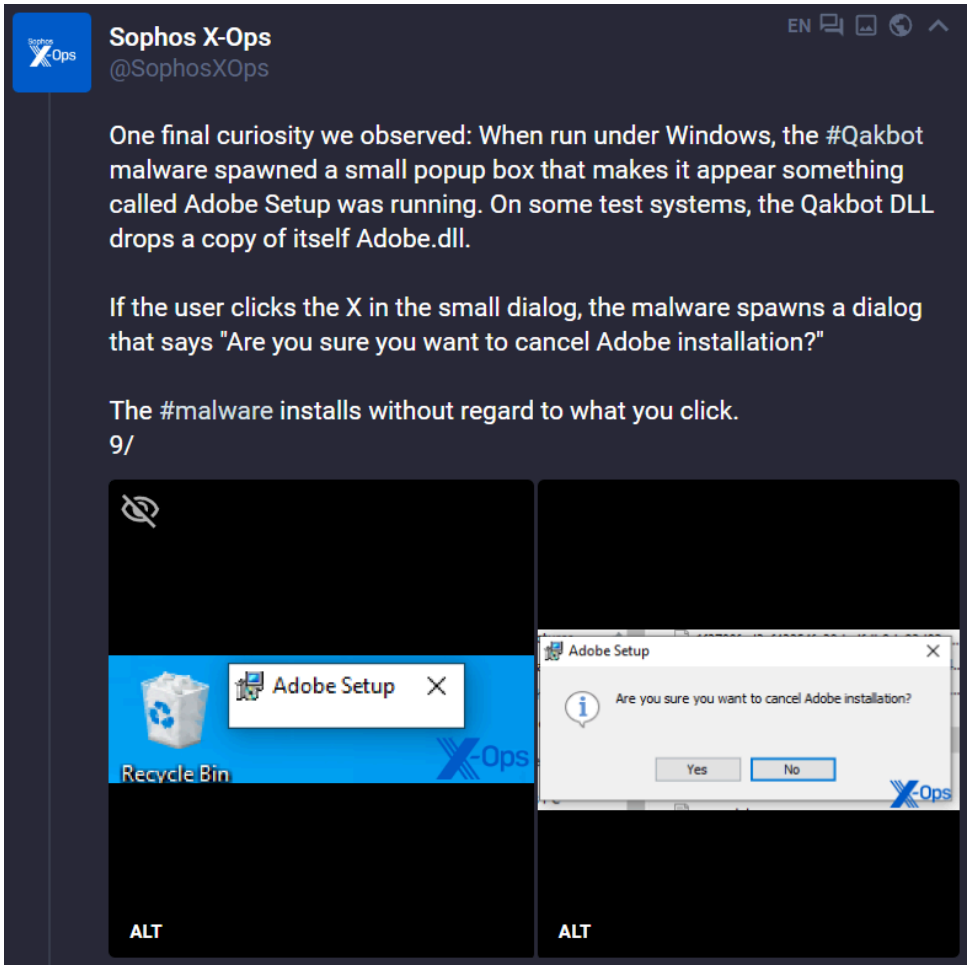
Specifically, the malware uses AES-256 encryption on top of the XOR method seen in older samples.

The malware checks for endpoint protection software and reintroduced checks for virtualized environments, attempting to evade detection by entering an infinite loop if it finds itself on a virtual machine.



AV checks performed by QBot *(Sophos)*

Additionally, Qakbot presents a misleading popup suggesting Adobe Setup is running on the system, to trick users with bogus installation prompts that launch the malware regardless of what is clicked.



Bogus Adobe installation prompt *(Sophos)*

Sophos researchers say that by monitoring QBot's development closely, they can update their detection rules and share crucial info with other security vendors.

Although a small number of samples have surfaced after Qbot's C2 infrastructure was taken down last year, researchers believe "that any activity by threat actors to bring it back deserves surveillance and scrutiny."

Source: https://www.bleepingcomputer.com/news/security/new-qbot-malware-variant-uses-fake-adobe-installer-popup-for-evasion/