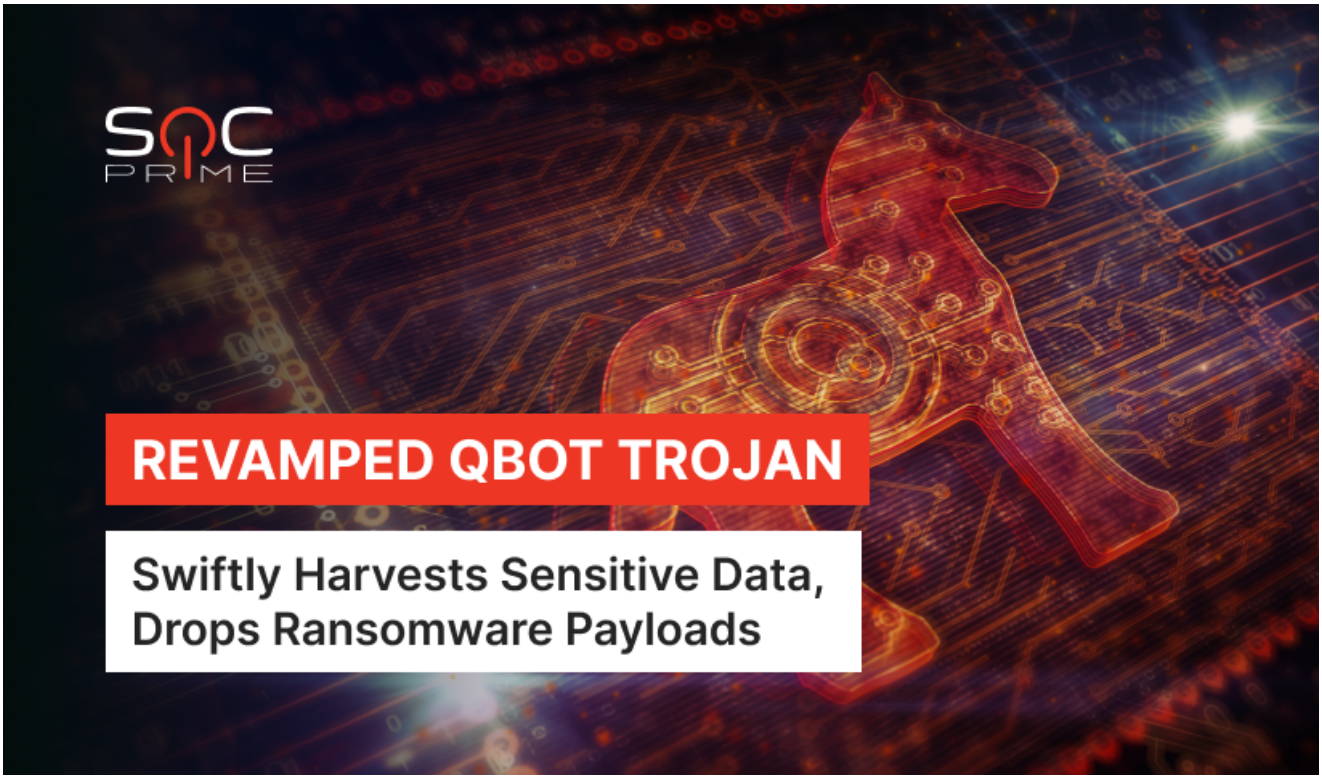
QBot Malware Detection: Old Dog New Tricks

socprime.com/blog/qbot-malware-detection-old-dog-new-tricks/

Alla Yurchenko



You can't teach an old dog new tricks. Yet, cybercriminals ignore common stereotypes, updating QBot with new nefarious tricks to attack victims globally. This malware "veteran" emerged back in 2007, yet security researchers observe QBot being constantly updated to ride the wave of malicious trends.

For instance, security researchers observe QBot maintainers increasingly abusing the LOLBin (Living Off the Land Binaries). Particularly, a common LOLBin is known as Regsvr32.exe: threat actors utilize this command-line utility to plant trojans like Lokibot and QBot in a victim's system. This approach creates a lucrative environment for the operation's success, given that Regsvr32.exe is a tool used within multiple routine processes.

QBot Attacks

QBot (QakBot, QuakBot, also Pinkslipbot) first surfaced in the late 2000s. For about 15 years, the trojan has been causing headaches, with the cybercrooks behind it faithfully coming up with innovative ways of carrying out their malicious activity.

Over the last few years, the QBot malware has grown into a wide-ranging Windows malware family, mostly utilized in phishing campaigns. It enables hackers to steal bank and Windows domain credentials, infect other machines, and provide ransomware groups with remote

access. According to current data, QBot was employed as a delivery agent for ransomware to acquire initial access to corporate networks by such notorious gangs as REvil, PwndLocker, Egregor, ProLock, and MegaCortex.

QBot Infection Chain

Typically, QBot infections stem from another malware infestation or, most commonly, a phishing attack. QBot targets devices running Windows, employing phishing emails as an initial point of access and exploits vulnerabilities in a system's default applications like Microsoft's email client, Outlook. Today, equipped with a module that reads email threads, hackers behind QBot have reached new heights in making bogus emails seem more legitimate to their victims. QBot phishing attacks rely on a vast repertoire of lures, such as sham invoices, payment reminders, banking information, job offers, scanned documents, virus detection warnings, and disturbing COVID-19 alerts, pushing a recipient to open the infected file, enabling embedded macro code.

In the current campaigns, QBot operators deliver malicious Word, Excel, RTF, and composite documents. When a victim opens a document, it fuels the QBot infections' spread. The initial QBot DLL loader is downloaded and the QBot process uses a Windows schedule task to elevate its level of access to the system. In as little as 30 minutes, the entire victim's system is raided.

Preventing the QBot

QBot has been on the cybersecurity radar for more than 15 years now, earning itself a notorious rank of a seasoned malware old-timer, distributed via email. In the light of a growing number of email phishing campaigns, Microsoft announced a default change for five Office applications that run macros, i.e., to block internet-obtained VBA macros, effective April 2022.

The above solution will hopefully become a giant security leap for Windows-operated devices. In the meantime, detection rules by Nattatorn Chuensangarun help security professionals to expose the latest QBot attacks against the organization's network:

Qbot Malware collects browser information (via process_creation)

Qbot Malware use REG Process to Defense Evasion (via process_creation)

Qbot Malware use msra Process to Privilege Escalation (via process_creation)

The full list of detections in the Threat Detection Marketplace repository of the SOC Prime platform is available here.

Sign up for free at SOC Prime’s Detection as Code platform to make threat detection easier, faster, and more efficient with industry’s best practices and shared expertise. The platform also enables SOC professionals to share detection content of their creation, participate in top-tier initiatives, and monetize the input.

Go to Platform Join Threat Bounty

Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

Join for Free Book a Meeting