LOGPOINT

An old acquaintance resurfaces with new capabilities

Sep 21, 2022 11:15 CEST

QakBOT: An old acquaintance resurfaces with new capabilities

- **A new Logpoint study reveals that the latest QakBot malware version is heavily used in malspam campaigns by notorious ransomware gangs**
- **The new QakBot emergence uses multiple, simple yet effective defense evasion techniques against static detection methods**

COPENHAGEN, Denmark & BOSTON, September 21, 2022 – Logpoint's Global Services team has analyzed the emergence, attack patterns, and possible detections of the new version of the notorious QakBot malware in 2022. QakBot has evolved multiple times and sees a resurrection every few years

associating itself with new vulnerabilities, actors, and industries.

The ransomware gang Black Basta is the driver behind the current QakBot. Since the group surfaced in April, it has gained attention due to its successful cyberattacks on over 50 organizations worldwide with double extortion methods. According to a Trend Micro report, Black Basta's tactics, techniques, and procedures (TTPs) include QakBot for access, movement, and using the PrintNightmarevulnerability to gain privileged file actions.

"In general, QakBot is an efficient information thief and backdoor, and many ransomware gangs use different variations to access corporate networks before encrypting files. Previous versions of QakBot were distributed via Emotet, but the latest resurgence shows that the attacks are rising through very targeted malspam email campaigns," says Doron Davidson, VP Global Services, Logpoint.

QakBot tactics, techniques, and procedures

The most recent QakBot operations gain initial access through an email thread hijacking and distributing malicious links, attachments, or embedded pictures. Opening the file drops a password-protected ZIP file into the local system with an Office document. The document contains malicious code that kicks off the infection chain, ultimately downloading and running QakBot through the PowerShell exploit Follinaor Living Off the Land Binaries (LOLBins).

QakBot has evasion and persistence mechanisms in place to evade any defenses. The malware creates and copies multiple files, modifies defender registry keys, injects itself into processes, and contains a technique for VM and Debug detections. In addition, the latest versions add a long list of blacklisted analysis programs like SysAnalyzer, Fiddler, and Filemon, enabling the malware to identify detection processes and take actions that evade them.

Mitigating the QakBot threat

As QakBot is modular and evolves with each new threat actor, making use of existing binaries, vulnerabilities, and advanced defense evasion techniques, detecting it is difficult. Organizations need to have solid prevention and

mitigation procedures in place, like setting up suitable detection rules and enabling dynamic detection methods.

An organization impacted by a QBot incident should isolate the infected system and secure backups. Organizations can isolate systems by turning off other computers and devices and segregating any other computers or devices that share a network with the infected computers that have not been fully encrypted by ransomware. They should also ensure that backup data is offline, secure, and malware-free.

You can read Logpoint's blog post about QakBot, here to learn more and get access to Logpoint's Emerging Threats report, What the Qak: Hunt for QBot with Logpoint, containing the analysis, infection chain, detection, and mitigation.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98