DarkGate and PikaBot Threat Surge Post-QakBot Takedown

A highly sophisticated phishing campaign, observed since September 2023, has elevated its threat level by incorporating the PikaBot malware alongside DarkGate, becoming one of the most advanced campaigns since the dismantling of the Qakbot (Qbot) operation. Following the FBI's takedown of Qakbot's infrastructure, threat actors behind this campaign have transitioned to newer malware botnets, employing tactics and techniques reminiscent of the Qakbot campaigns. The campaign's significance lies in its high-level threat status, utilizing advanced procedures and demonstrating the capability to deliver potent malware payloads. Given the modular nature of DarkGate and PikaBot, similar to the notorious Qakbot, enterprises face a substantial risk, as these malware loaders can facilitate initial network access, potentially leading to ransomware, espionage, and data theft attacks.

The phishing attack methodology is intricate, leveraging stolen discussion threads to enhance the appearance of trustworthiness in malicious emails. Users who click on embedded URLs undergo a series of validation checks before being prompted to download a ZIP archive containing a malware dropper, fetching the final payload from a remote resource. The threat actors have experimented with various initial malware droppers, including JavaScript droppers, Excel-DNA loaders, VBS downloaders, and LNK downloaders, showcasing a dynamic and adaptive approach. Notably, the DarkGate malware was the primary payload until October 2023, when it was replaced by PikaBot.

DarkGate, documented since 2017 but recently distributed widely, is an advanced modular malware supporting various malicious activities, such as remote access, cryptocurrency mining, keylogging, and information stealing. PikaBot, a newer addition first identified in early 2023, boasts a loader and a core module with robust anti-debugging and anti-emulation mechanisms. The threat actors behind these campaigns exhibit a high level of expertise, surpassing ordinary phishers. It is imperative for enterprises to familiarize themselves with the tactics employed in this campaign to enhance their cybersecurity posture and mitigate potential risks effectively. Regular monitoring, employee training, and updated security measures are essential components of a proactive defense strategy against this evolving and sophisticated threat landscape.

____

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:
https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/?web_view=true