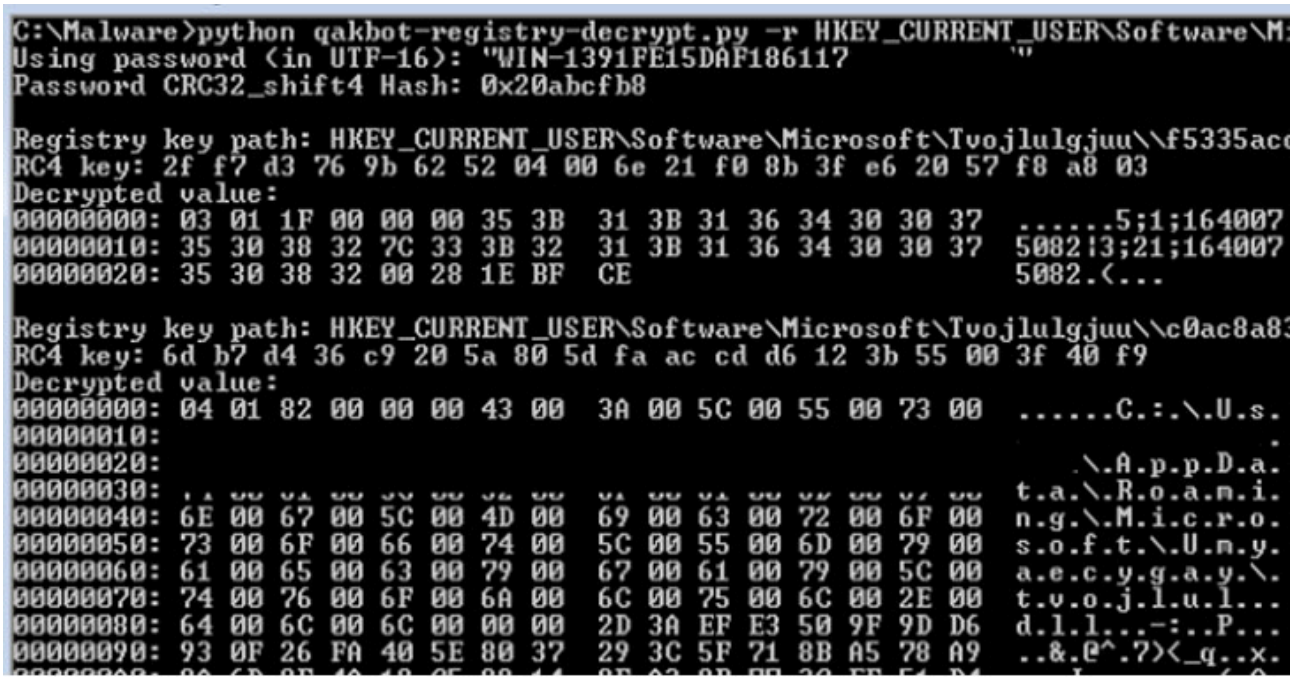
Researchers Decrypted Qakbot Banking Trojan's Encrypted Registry Keys

By The Hacker News

Published: 2022-01-13 · Archived: 2026-04-05 13:00:26 UTC



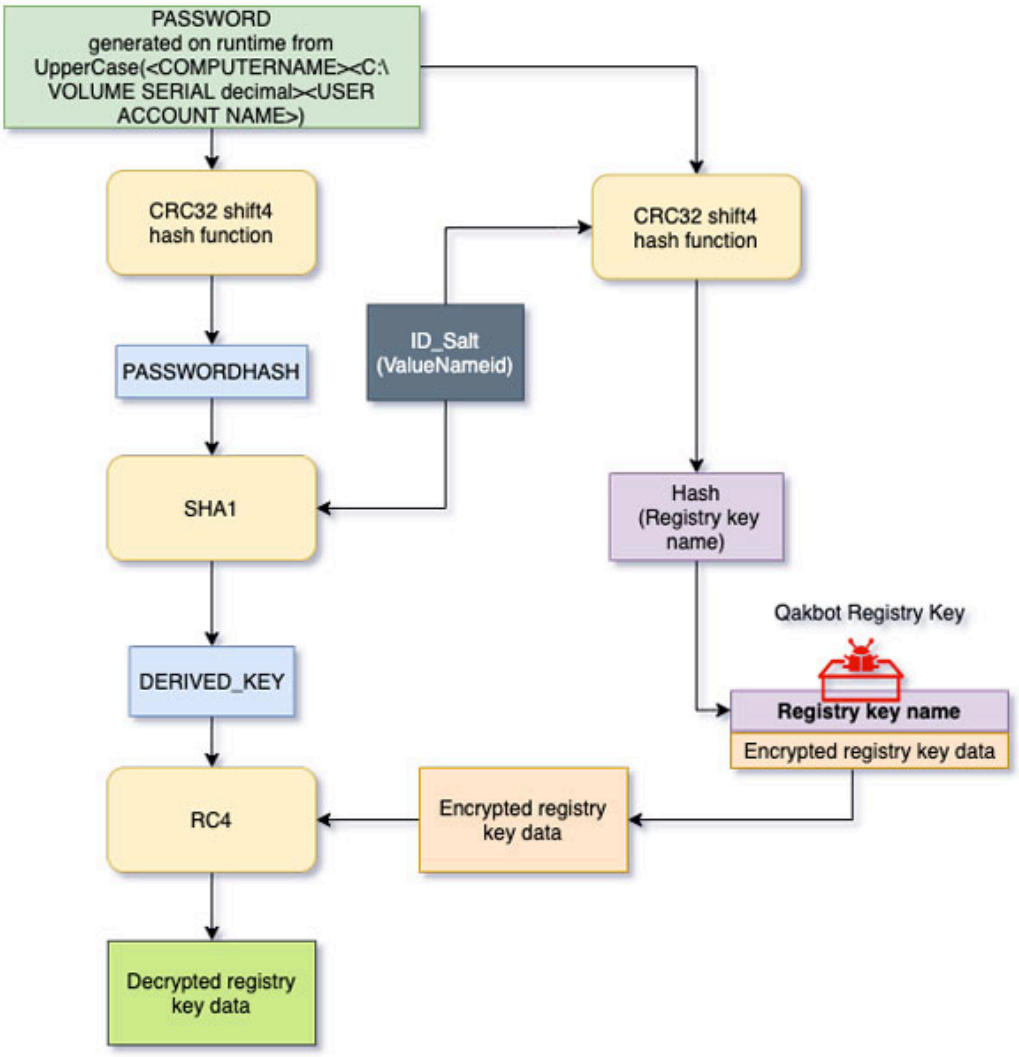
Cybersecurity researchers have decoded the mechanism by which the versatile Qakbot banking trojan handles the insertion of encrypted configuration data into the Windows Registry.

Qakbot, also known as QBot, QuackBot and Pinkslipbot, has been observed in the wild since 2007. Although mainly fashioned as an information-stealing malware, Qakbot has since shifted its goals and acquired new functionality to deliver post-compromise attack platforms such as Cobalt Strike Beacon, with the final objective of loading ransomware on infected machines.

"It has been continually developed, with new capabilities introduced such as lateral movement, the ability to exfiltrate email and browser data, and to install additional malware," Trustwave researchers Lloyd Macrohon and Rodel Mendrez said in a report shared with The Hacker News.

In recent months, phishing campaigns have culminated in the distribution of a new loader called SQUIRRELWAFFLE, which acts as a channel to retrieve final-stage payloads such as Cobalt Strike

and QBot.



Newer versions of Qakbot have also gained the ability to hijack email and browser data as well as insert encrypted configuration information pertaining to the malware into the registry as opposed to writing them to a file on disk as part of its attempts to leave no trace of the infection.

"While QakBot is not going fully fileless, its new tactics will surely lower its detection," Hornetsecurity researchers pointed out in December 2020.

Trustwave's analysis into the malware aims to reverse engineer this process and decrypt the configuration stored in the registry key, with the cybersecurity company noting that the key used to encrypt the registry key value data is derived from a combination of computer name, volume serial number, and the user account name, which is then hashed and salted along with a one-byte identifier (ID).

"The SHA1 hash result will be used as a derived key to decrypt the registry key value data respective to the ID using the RC4 algorithm," the researchers said, in addition to making available a Python-based decryptor utility that can be used to extract the configuration from the registry.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
