FILTER

Alphabetical

CYBERCRIME

GOLD LAGOON

Objectives

GOLD LAGOON is a financially motivated cybercriminal threat group active since 2007 that operated the Qakbot (aka Qbot) malware. Qakbot is a modular malware framework that supports numerous capabilities such as credential theft, spam delivery, interception and manipulation of web traffic with webinjects, and remote access. At 23:27 UTC on August 25, CTU researchers detected the Qakbot botnet distributing shellcode to infected devices containing code that cleanly terminates the running Qakbot process on the host, and concluded it constituted an attempt to take the botnet offline. On August 29, 2023, U.S. law enforcement announced a takedown of the botnet under international Operation Duck Hunt. Qakbot was frequently distributed through spam campaigns and until February 2020 as a second-stage download from the Emotet botnet. An optional email collection module enables additional infections by replying to a victim's existing email threads with a malicious attachment or link leading to the download of Qakbot. It can also self-spread using an SMB brute force module that contains a list of commonly used passwords. A universal plug-and-play (UPnP) module is able to transform infected hosts without direct Internet connectivity into intermediate command and control (C2) servers used for the botnet. The takedown, let by the U.S. Federal Bureau of Investigation (FBI), represents a significant disruption to the cybercrime ecosystem. The FBI estimates that Qakbot's use in the initial stages of ransomware deployment has resulted in losses to global businesses in the hundreds of millions of dollars. Third-party reports suggest the botnet has facilitated the delivery of Conti, DoppelPaymer, ProLock, Egregor, and MegaCortex. CTU researchers have observed it used to deploy REvil, and, more recently, Black Basta ransomware. It may also have been used for the deployment of Clop. The takedown was comprehensive, and appeared focused on preventing GOLD LAGOON reacquiring infected systems in the current Qakbot botnet. GOLD LAGOON may make an effort to reconstitute the botnet by creating a new one entirely but this will be a challenging and it remains to be seen how effective any attempts to do so might be.

READ LESS