Businesses Beware: Qakbot Spreads like a Worm, Stings like a Trojan

Subscribe Here

Subscribe to the RSA blogs and podcasts for the latest posts and security updates!

Written on October 25, 2010 by RSA FraudAction Research Labs

Comments

While the name Qakbot may sound funny, the Trojan is targeting business and corporate accounts—and no one is laughing. Named after its main executable file, **_qakbot.dll**, the Qakbot Trojan is not new; however the RSA FraudAction Research Lab has uncovered some unique attributes of Qakbot rarely seen before in other financial crimeware.

Our recent research into Qakbot shows that its trigger list is almost completely comprised of large US-based financial institutions, with a few instances of Non-US institutions. Furthermore, Qakbot is the first Trojan seen to be exclusively targeting business/corporate accounts at these financial institutions. Why is Qakbot limiting itself? Why not expand beyond corporate accounts and victimize the ordinary consumer? The answer is economics – the goal for Qakbot is to siphon out larger sums of money, much more than would generally be available in private online accounts. While Qakbot is *not* the first and only Trojan to target such accounts, it is the only one that shows this type of strict “preference” by design, and with no exceptions.

How the Qakbot Trojan actually gets money out of corporate bank accounts is still being investigated. Surprisingly, we did not trace HTML or JavaScript code injections, nor Man-In-The-Browser attacks that are typically used to circumvent the two-factor authentication mechanisms that normally protect these high-asset accounts. Still, we suspect that Qakbot *does* have some sort of module for completing real time attacks, since it would otherwise not target business accounts to begin with.

Another unique attribute to the Qakbot Trojan is its makeup. Qakbot is the ultimate multi-tasker, designed to spread like a worm—infecting multiple machines at a time—while also stealing data like an ordinary banker Trojan. Qakbot targets shared networks, copying its executable file into shared directories; a technique that enables it to propagate on corporate networks, rendering every computer connected to such networks vulnerable. While not completely original, the worm/Trojan combination is rare and extremely effective.

Finally, Qakbot is an organization dynamo. It is the first Trojan to separate out targeted credentials, from other stolen information on the client side rather than in a drop zone. After the distinction between targeted credentials and other information is made on the victim's computer, targeted credentials are sent to the Qakbot's drop server while credentials stolen from entities that are not specifically targeted by Qakbot are uploaded to hijacked FTP accounts, located on legitimate FTP servers.

The sheer volume and detail of information stolen by Qakbot is astounding. Every time an infected user accesses an entity's website, the Trojan organizes data transmitted from the victim's machine into 3 separate files: **System Information** (IP address, DNS server, country, state, city, software applications installed, etc.) (see Figure 1), **Seclog** (HTTP/S POST requests) (see Figure 2), and **Protected Storage** (information saved in the Internet Explorer Protected Storage and auto complete credentials including usernames, passwords, and browser history) (see Figure 3). These files are organized per user and are complete with comprehensive system and user-account information. Why bother aggregating such extensive system data on each user account defined on every infected computer? All this information is likely aggregated by Qakbot's authors to research future possible exploits.

The Qakbot Trojan's most famous victim to date, was the National Health Service (NHS), the UK's publically funded healthcare system. Qakbot infected over 1,100 computers and while there was no evidence that patient data was compromised, 4 GB of credentials from Facebook, Twitter, Hotmail, Gmail and Yahoo, were seen being funneled through NHS monitored servers.

Qakbot's Other Idiosyncrasies

Two of Qakbot's extensive stealth functionalities stand out as being particularly unusual: The first is Qakbot's extensive lab-evasion procedures, designed to ensure that the Trojan does not run in a security company's research lab. Qakbot's developers are definitely not the first

crimeware authors to design lab-evading tests in an effort to avoid having their crimeware studied by researchers in a lab environment. However, unlike some other Trojans, which simply check whether they are being run on a virtual machine to determine whether to continue their self-installation, Qakbot's authors have taken pains to set up a series of seven (7) tests in an attempt to ensure that their Trojan will not be reverse engineered and scrutinized by security researchers.

In addition, and this is the more unusual part, if Qakbot identifies that it is being run in a lab setting, it goes to the trouble of reporting the relevant IP address to the Trojan's drop zone: The Trojan sends the system's IP address and bot ID to Qakbot's drop zone (via the internal command **getip**). This kind of notification is likely performed to blacklist the IP address, so that the Trojan never again attempts to infect the same research lab.

The second unusual stealth functionality traced by the lab is the unique, self-developed compression format created by Qakbot's authors to compress credentials stolen by the Trojan—the first programming feat of its kind witnessed by the Lab, as most banking Trojans simply use popular compression formats such as ZIP, RAR, and TARGZ. The Qakbot authors' proprietary archive format forces professional security researchers to dedicate a considerable amount of time and effort to write an appropriate decompressor.

*****

It is important to note that the Qakbot Trojan's distribution is quite limited so it is likely privately owned and operated by a single cybercriminal or gang, as opposed to being commercially available in the underground. However, despite the Trojan's low prevalence in the wild, its unique functionalities all make Qakbot a highly-targeted virtual burglar.

Figure 1: SI – System Information File sent from Bot to Qakbot C&C Server

Figure 2: Seclog – File sent from Bot to Qakbot C&C Server

Figure 3: PS – Protected Storage File sent from Bot to Qakbot's C&C Server

Leave a Reply

© Copyright 2011 EMC Corporation. All Rights Reserved.
The opinions expressed here may be personal. Content published here is not read or approved in advance by EMC
and does not necessarily reflect the views and opinions of EMC.