Qakbot Steals 2GB of Confidential Data per Week

Archived: 2026-04-05 21:50:57 UTC

Our previous blog entries about W32.Qakbot gave details about how the threat works, how it spreads, and its capabilities for stealing information. This entry focuses on the scale and type of data Qakbot has been successful in acquiring.

Stealing data

Qakbot monitors compromised computers for sensitive information and uploads the stolen data to an FTP server. The FTP server information is downloaded from the botnet and can change over time. Here is an example of a recent FTP configuration:

exec=!var ftphost_1=ftp.df[REMOVED]
exec=!var ftphost_2=web1[REMOVED]
exec=!var ftphost_3=ftp.su[REMOVED]
exec=!var ftphost_4=ftp.ab[REMOVED]
exec=!var ftphost_5=ftp.51[REMOVED]
exec=!var ftphost_6=ftp.fan[REMOVED]

While analyzing this threat we gained access to and closely monitored two of these FTP servers. The results are quite startling. Although Qakbot is a smaller botnet, over the course of two weeks we observed roughly four gigabytes of stolen information that was uploaded to these FTP servers. The data uploaded includes:

- Online banking information
- Credit card information
- Social network credentials: Facebook, Twitter, Orkut, Bebo, Adult FriendFinder, and more.
- Internet mail credentials: Hotmail, Gmail, Yahoo!, and more.
- Internet search histories

Qakbot records the contents of information that is stored and used by the AutoComplete feature. In a nutshell, if your computer is compromised, every bit of information you type into your browser will be stolen.

The following image shows some stolen AutoComplete data:

Qakbot also steals detailed information about the computer on which it’s running:

Indiscriminate targeting

One unusual aspect of Qakbot is that even though its purpose is to steal information associated with home users, it has also been successful at compromising computers in corporate environments as well as government departments. For instance, there are over 100 compromised computers on a Brazilian regional government network. More alarmingly, the logs show that there is a significant Qakbot infection on a major national health organization network in the UK. This threat has managed to infect over 1,100 separate computers that are spread across multiple subnets within their network. We have attempted to contact the affected parties and have no evidence to show that any customer or patient data has been stolen. Given that these figures are based on the evidence from logs obtained from only two servers over two weeks, the actual numbers may be higher.

This map shows the distribution of the infected hosts represented only by the information in FTP data. As you can see, this botnet has coverage on a global scale:

Consequences

The stolen data gives a snapshot of user activity at a given time, but because login credentials are also stolen, anyone in possession of this information can gain a far more complete view of a user's life. For example, one woman, after chatting on Facebook, bought some items online at the retailers Argos and WHSmith. She then posted updates about her activities on that day. If required, the attacker can then log in to the above sites and can gain access to the orders, which gives access to the home address where the items will be ultimately delivered. Personal information including name, address, age, shopping habits, interests, friend lists, and photographs for this and other users has been compromised by Qakbot.

Also, whoever is behind Qakbot has not put much effort into securing the stolen information. Anyone with a sample of this threat who knows what they are doing will be able to access this data quite easily. At the time of this writing we have only observed Qakbot stealing consumer-based information, but since Qakbot also functions as a downloader, corporate environments compromised by Qakbot could find themselves defending a more serious attack if appropriate action is not taken now.

How do I protect myself?

Symantec users are protected from this threat by both our antivirus and IPS engines. The malicious binaries will be detected as W32.Qakbot, while the IPS engine will detect malicious **Qakbot** downloads as HTTP W32 Qakbot File Download Activity. More importantly, the IPS engine also detects and blocks attempts to upload stolen data to the FTP servers as FTP W32.Qakbot Activity. This will help to prevent stolen data from reaching the attackers. Education is always a powerful tool in the fight against any malware; our W32.Qakbot writeup on this threat gives a great deal of information about it.

If you are reading this and are worried about malicious third parties gaining access to your online accounts, now would be a good time to ensure that you change all of your passwords related to your online presence. What's clear from the data we have analyzed is that people use bad habits for creating their passwords. Use hard-to-guess passwords and please don't use the same password across many online services.

Security Response is attempting to shut down the dump sites and command-and-control servers in order to neuter current versions of **Qakbot**.

Thanks to Nicolas Falliere for his work in reversing the format of the Qakbot log files.
