W32.Qakbot | Symantec

W32.Qakbot is a worm that spreads through network shares and removable drives. It downloads additional files, steals information, and opens a back door on the compromised computer. The worm also contains rootkit functionality to allow it to hide its presence.

Infection

W32.Qakbot spreads by exploiting vulnerabilities when a user visits certain Web pages. Exploit code hosted at these remote locations downloads the threat on to the compromised computer. Many of the infections are aided by users unwittingly clicking on malicious links. As more and more threats make use of the Web to spread, the clearer it becomes that Every Click Matters.

The worm also spreads through network shares by copying itself to shared folders when instructed to by a remote attacker. It also copies itself to removable drives.

Functionality

While W32.Qakbot has multiple capabilities, its ultimate goal is clearly theft of information. Identification theft is big business in the underground world of cybercrime and the more data a threat can steal, the bigger the profit that can be made. W32.Qakbot is capable of gathering a number of different kinds of information, including the following confidential information:

- Authentication cookies, including Flash cookies
- DNS, IP, hostname details
- OS and system information
- Geographic and browser version information
- Keystrokes including login information
- Login details for FTP, IRC, POP3 email, and IMAP email
- Outlook account information
- Private keys from system certificates
- Login credentials for certain websites
- URLs visited

Cybercrime is big business, and it is real crime. The U.S. Dept. of Treasury reports that cybercrime has surpassed illegal drug trafficking as a criminal money maker, with one in five people becoming a victim. With the profits often in the millions of dollars, it takes very little effort for a cybercriminal to set up an operation, steal identities and begin selling. Just a

small glimpse of what is possible -- or, say, an Introduction to the Black Market -- can give the average internet user an idea of the insidious nature of cybercrime.

There is a funny credit card television ad that features barbarians running around using the credit card and the tag-line is "What's in your wallet?" You can almost hear the cybercriminals asking themselves, "What's on your computer?" If you have a computer, you're at risk, which means that assessing your level of risk is always a good idea.

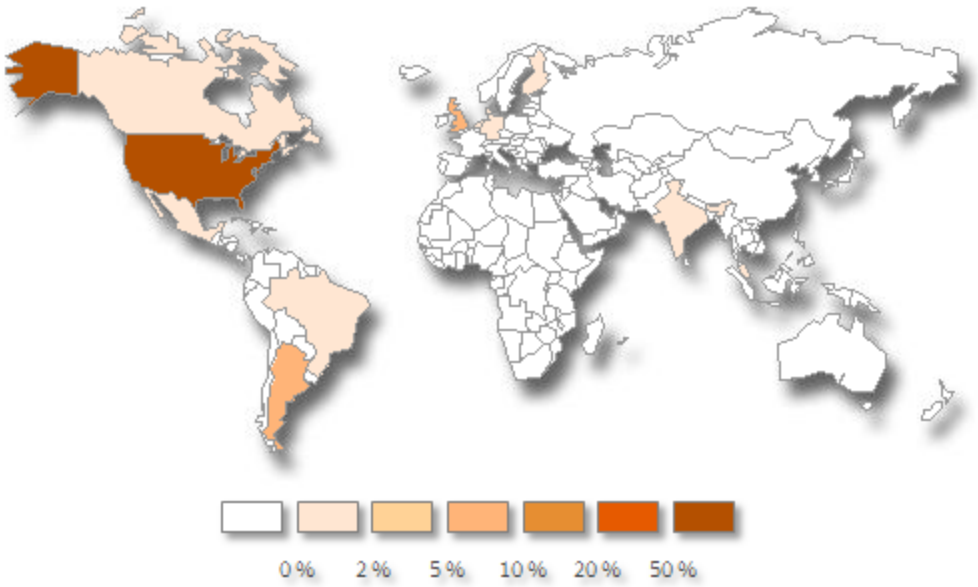
Once stolen, login details, credentials from particular websites, passwords, financial information and other personally identifiable information can be sold on the black market. Ultimately, that ends in identity theft. The most often used technique, keylogging, attempts to provide as much data as possible; the more details about the user that end up in the hands of the remote attacker, the bigger the Black Market Keylogging profit.

White paper: W32.Qakbot in Detail

Symantec have published a white paper probing deeper into the worm to reveal its inner workings. To find out more about this worm, download a copy of the paper: W32.Qakbot in Detail.

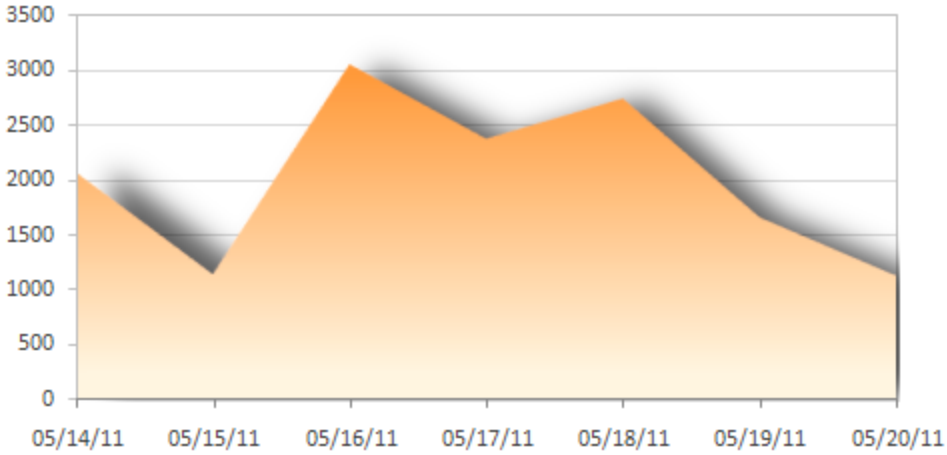
GEOGRAPHICAL DISTRIBUTION

Symantec has observed the following geographic distribution of this threat.



PREVALENCE

Symantec has observed the following infection levels of this threat worldwide.



SYMANTEC PROTECTION SUMMARY

The following content is provided by Symantec to protect against this threat family.

Antivirus signatures

W32.Qakbot

Antivirus (heuristic/generic)

- Packed.Cupx!gen2
- Packed.Cupx!gen3
- Packed.Cupx!gen4
- Packed.Cupx!gen5
- Packed.Generic.276
- Packed.Generic.304
- Packed.Generic.308
- Packed.Generic.368
- SONAR.Qakbot!gen1
- W32.Qakbot!conf
- W32.Qakbot!conf2
- W32.Qakbot!conf3
- W32.Qakbot!gen1
- W32.Qakbot!gen2
- W32.Qakbot!gen3
- W32.Qakbot!gen4
- W32.Qakbot!gen5
- W32.Qakbot!gen6
- W32.Qakbot!gen7
- W32.Qakbot!gen8
- W32.Qakbot!html

- W32.Qakbot!job
- W32.Qakbot!zip

Browser protection
Symantec Browser Protection is known to be effective at preventing some infection attempts made through the Web browser.

Intrusion Prevention System

- MSIE Apple QuickTime RTSP URI Remote BO
- System Infected: W32.Qakbot Activity
- System Infected: W32.Qakbot Activity 2
- System Infected: W32.Qakbot FTP Activity
- System Infected: W32.Qakbot FTP Activity 3
- HTTP W32 QakBot File Download Activity
- MSIE ADODB.Stream Object File Installation Weakness
- HTTP Trojan IRCBot Activity

Symantec Endpoint Protection – Application and Device Control
Symantec Security Response has developed an Application and Device Control (ADC) Policy for Symantec Endpoint Protection to protect against the activities associated with this threat. ADC policies are useful in reducing the risk of a threat infecting a computer, the unintentional removal of data, and to restrict the programs that are run on a computer.

This particular ADC policy can be used to help combat an outbreak of this threat by slowing down or eliminating its ability to spread from one computer to another. If you are experiencing an outbreak of this threat on your network, please download the policy by right-clicking the link, choosing your browser's "save as" option, and saving the file as "W32.Qakbot.dat".

To use the policy, import the .dat file into your Symantec Endpoint Protection Manager. When distributing it to client computers, we recommend using it in **Test (log only)** mode initially in order to determine the possible impacts of the policy on normal network/computer usage. After observing the policy for a period of time, and determining the possible consequences of enabling it in your environment, deploy the policy in **Production** mode to enable active protection.

For more information on ADC and how to manage and deploy them throughout your organization, please refer to the Symantec Endpoint Protection Administration Manual (PDF).

Note: The ADC policies developed by Security Response are recommended for use in outbreak situations. While useful in such situations, due to their restrictive nature they may cause disruptions to normal business activities.

- **Initial Rapid Release version** May 7, 2009 revision 001
- **Latest Rapid Release version** October 26, 2015 revision 035
- **Initial Daily Certified version** May 7, 2009 revision 003
- **Latest Daily Certified version** October 26, 2015 revision 022
- **Initial Weekly Certified release date** May 13, 2009

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.