EXHIBIT 7

An analysis of Dorkbot's infection vectors (part 1)

msft-mmpc | 14 Nov 2012 6:00 AM | 0

Malware nowadays benefits from the complexity of the Internet ecosystem to infect new computers through vectors such as browser plugins, social networks, and instant messaging programs.

In this two-parter series, we'll look at Worm:Win32/Dorkbot, a prevalent worm with the capabilities of an IRC backdoor and a password stealer. Dorkbot relies both on social engineering attacks and on methods that don't require human intervention, such as infected removable drives and drive-by downloads. This versatility has contributed to a spike in Dorkbot detections in the last year and a half: over 28 million detections of Dorkbot have been reported since we saw this malware family in April of 2011, as seen in Figure 1.

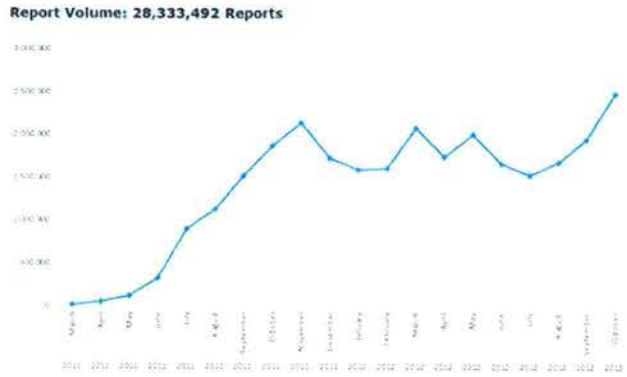

Figure 1: *Number of Worm:Win32/Dorkbot detections since 2011 based on MAPS telemetry*

Dorkbot uses IRC over SSL to communicate with its command-and-control (C&C) server. To find out what it's transmitting to the remote attacker, we intercepted the SSL-encrypted traffic, as shown in Figure 2.

Figure 2: *A machine infected with Dorkbot talking to the C&C server*

Dorkbot hooks several Windows APIs related to network access to steal FTP and website login credentials. The network traffic capture in Figure 2 also shows Dorkbot stealing FTP credentials from Total Commander and login credentials for several websites: facebook.com, gmail.com and mail.yahoo.com. For a full list of the websites that are targeted, please see the Worm:Win32/Dorkbot description.

After it connects to an IRC channel, the worm is instructed to download its spamming component and additional malware, such as Worm:Win32/Gnoewin.A, Worm:Win32/Gnoewin.B, Trojan.Win32.Lethic.F, and Worm:Win32/Pushbot.gen.

This first post is about Dorkbot's spreading vectors that require user interaction.

Spreading vectors requiring user interaction: Social engineering, IM programs, and social networks

Dorkbot relies on simple social engineering attacks to propagate with user interaction. Using its downloaded spamming component, it spams all the contacts on Windows Live Messenger and Skype with an enticing message, designed to trick them into downloading and running a Dorkbot copy.

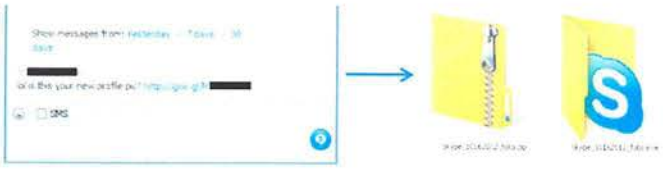

***Figure 3**: Dorkbot posting a goo.gl short URL in a Skype window; the URL leads to a copy of the Dorkbot worm*

The spreading mechanism is as follows: Dorkbot downloads a separate spamming component, which in turn spams the user's contacts with a link to the main Dorkbot executable. If the contact opens the link and executes Dorkbot, the spamming component is downloaded again, and the cycle continues as shown in Figure 4.

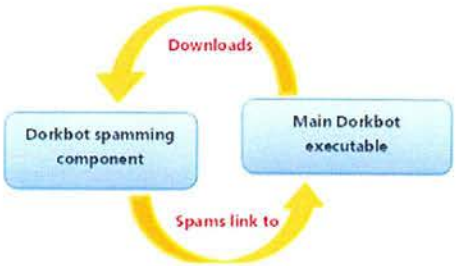

***Figure 4**: The relationship between the spamming component and the main executable*

The attack is made more effective by the localization of the spammed message in over 24 languages (Figure 5). Dorkbot picks up the language depending on your Windows locale from one of: English, French, Portuguese, Spanish, Hungarian, Dutch, German, Swiss German, Albanian, Swedish, Turkish, Serbian, Polish, Italian, Norwegian, Czech, Russian, Slovakian, Danish, Thai, Mandarin, Indonesian, Vietnamese, and Filipino.

***Figure 5**: Localized messages are hardcoded in the resource section of the Dorkbot component*

We checked a goo.gl short URL link out of the hundreds that have been spammed by Dorkbot. As of this writing, it's been clicked about 100,000 times. The access pattern shows a spike for a short period of time, until the link is flagged as malicious by Google.

***Figure 6**: Statistics for a spammed link leading to Dorkbot*

Another way that it spreads using social engineering is by posting arbitrary messages, such as links to malware, on the following social networks: Facebook, Twitter, VKontakte, Friendster and Bebo, whenever it is instructed by its C&C server.

In the case of Firefox, Dorkbot hooks the function *PR_Write* exported by *nspr4.dll*. This function gets called every time the browser writes data to a remote socket. To take the example of Facebook, when a user writes an instant message to another user, an HTTP POST request containing details about the message is sent to facebook.com. The HTTP request triggers a call to the PR_Write hook and Dorkbot has a chance to inject additional content into it, such as malware URLs (see Figure 7).

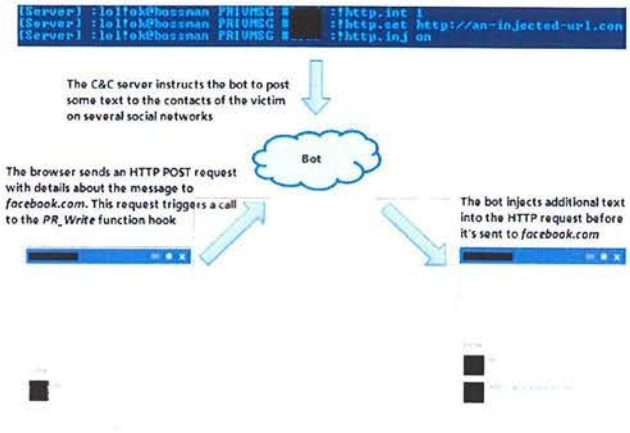

***Figure 7**: Dorkbot hijacking Facebook messages*

To avoid getting infected through Dorkbot's social engineering attacks be careful about the links you click on, even if they're from a trusted source – if possible, verify with your contacts first that they actually did send you the link. If you're using Internet Explorer 8 and newer, SmartScreen checks the URLs that you open to make sure they don't lead to malware.

Next week, spreading vectors not requiring user interaction.

Horea Coroiu, MMPC Munich

1

Comments