EXHIBIT 4

MSRT March 2012: Breaking bad

msft-mmpc | 13 Mar 2012 10:00 AM | 0

This month, the MMPC added Win32/Dorkbot to the Microsoft Malicious Software Removal Tool along with detections for the threats Win32/Hioles, Win32/Pluzoks and Win32/Yeltminky.

Win32/Dorkbot is described as an IRC-based botnet and a worm, a backdoor with rootkit capability and a password stealer. Despite using a very simple IRC protocol to communicate with the command and control (C&C) server, it was able to build a substantial installation base after a couple of years in operation. Some might compare Win32/Dorkbot with the infamous Win32/EyeStye due to some similarities in their behavior and advanced features.

Dorkbot implements an advanced user-level rootkit that is very similar to the hooking technique used by EyeStye. The hooking is used to hide its registry and file components from users that are not using rootkit detection software. Both threats appear to have a dedicated development team and both threats can also steal users credentials, which may include personal and banking information, via a form grabbing technique.

For an attacker, the Dorkbot malware is simpler to configure and control, less aggressive and less expensive to own than EyeStye. It also strictly uses the IRC protocol, while EyeStye is a complex botnet with a changeable communication protocol, from P2P, UDP to a custom protocol.

The following is an example of an underground site promoting the malware (with offensive context edited) :

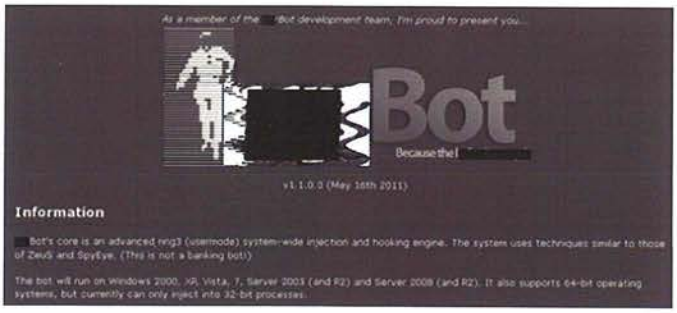

Figure 1 - Dorkbot as seen posted for sale in an underground forum in May 2011

Win32/Dorkbot spreads via the following three vectors:

- USB drives: the worm transfers to inserted USB media. When the infected media is inserted in another computer, the worm spreads to the new host.
- Instant Messaging (IM): the C&C master communicates malicious links to Win32/Dorkbot client that joins a specific IRC channel. The worm then hooks several important APIs to help monitor IM communication, and when the affected user chats with other contacts, the worm intercepts the conversation and injects the malicious link into the chat reply. When the user clicks the link, it will download and execute arbitrary files which could be other malware or an update of the worm.
- Social network sites: similar to the IM spreading mechanism, Dorkbot monitors a large array of popular social networks such as Twitter, Facebook and others. Using the social network chat functionality, the worm may spread by injecting the malicious link into chat conversations.

The popularity of social networks is a contributing factor to success of the Dorkbot propagation and a majority of installations are presumed to be consumers in the private sector, primarily because communication on the IRC protocol is commonly blocked in corporate networks. Dorkbot has a long list of features, such as

- data stealing via form grabbing
- denial of service attacks
- rootkit capability

- modify DNS settings
- and more...

The bot also uses two other features called "Ruskill" and "Pdef" or "Proactive Defense". The Ruskill feature is a mode that can be enabled by the bot master to command the bot to delete the file that Dorkbot downloads, creates or copies itself to, when the system restarts. PDEF mode commands the bot to "stand its ground" by attempting to remove other files that may exhibit behavior that resemble malware, such as an attempt to spread via USB drives, or an unknown IRC communication for example. Being a persistent threat on an installed host adds "value" for bot herders, or attackers that control an installed base of bot malware. The added "value" factors in when the attacker sells the bot on the underground market. Security researchers and aficionados may recall the silent war between released variants of MyDoom, Beagle and Netsky -- one malware would seek and remove another from an infected computer in order to remain installed.

Dorkbot can be a real killjoy by not allowing the infected system to reach security-related websites by hooking "*Dnsapi.dll*" APIs. The domain block list is a plain text file that may be updated by the botmaster by commanding the bot to download from a remote link, for example:

hxxp://<removed>.fuskbugg.se/<removed>/4e28ae2064f07_av.txt

The following is an example of the block list:

Figure 2 - Example domain access block list

The popularity of Dorkbot resulted in the reverse engineering of the bot by hackers. The modified binary has been sold for a mere $100 US, compared to the "official" Dorkbot release code, which sells for three times as much. Some hackers also created their own kit/builders that provides "script kiddies", or hackers that have little coding experience, an opportunity to create more Dorkbot variants, with their own configuration, such as command strings, C&C channel, and the malicious link that they can easily modify:

Figure 3 - Dorkbot builders (with offensive alias edited)

After generating new Dorkbot binaries, hackers stuff them inside VB or .Net crypters to try and avoid AV detection. For more details about this threat, please visit its detailed description here.

There is a slang saying for this time of year and that is "*In like a lion, out like a lamb*". Loosely translated, although the changing of the seasons brings a turbulent wind, it recesses and gives way to a calm. May your digital landscape be calm.

The following are SHA1 examples for malware mentioned in this blog.

Win32/Dorkbot:
f7f77927b000ef74dc244c48f5b550d3eedfca6d
fa7402f86131addbfb1ff4bd3c45b5f7973e602d
950ca89996b6ae85df0ada8a6d44fd948738e7a6
02127b7c97893f9fc76c72a46e5690b259bff7d8

-- Rex Plantado, MMPC

1

Comments