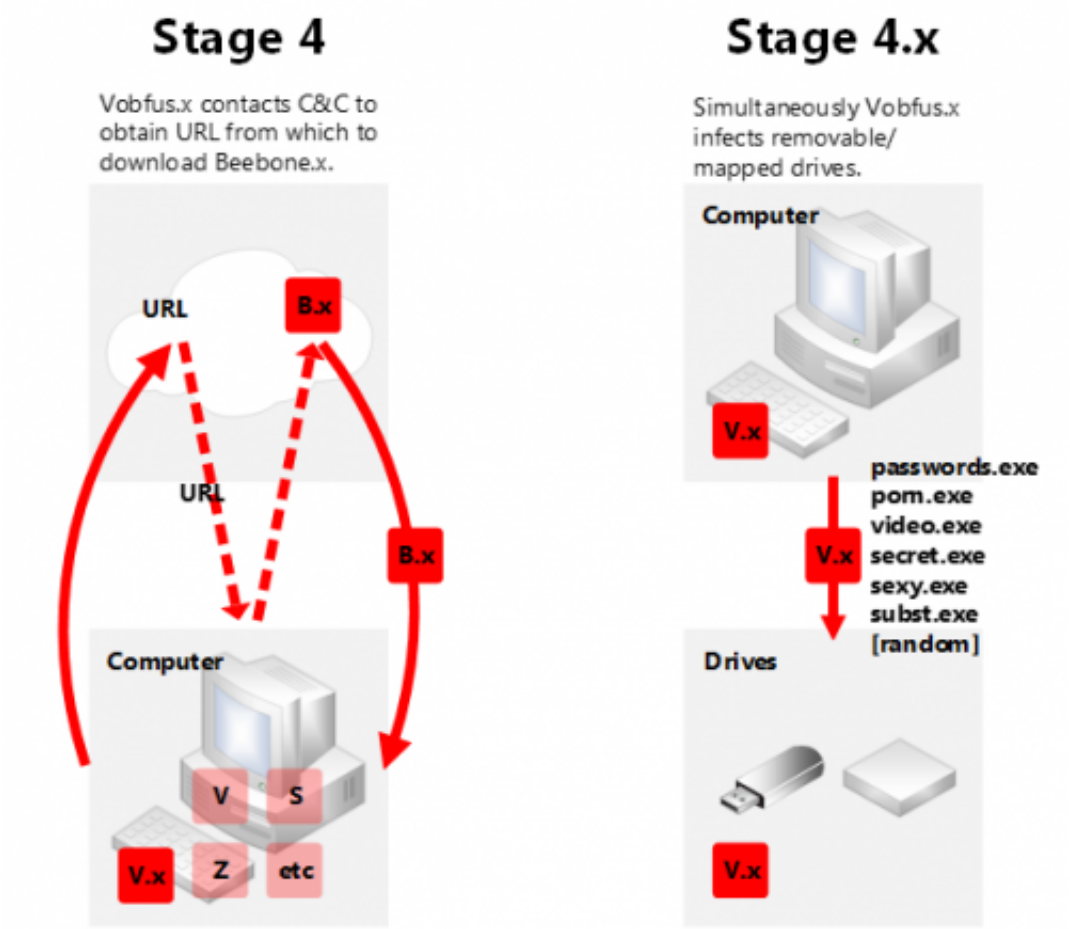
Malware: Vobfus and Beebone infections are double-trouble

July 2 2013, by Nancy Owano



Credit: Microsoft

(Phys.org) —Vobfus and Beebone sound like two lovable crayon-colored goldfish still on the Pixar drawing boards: Wouldn't that be nice.

Microsoft's security team would much prefer they be animated box-office hits but they are a pair of malicious software programs that work in concert with one another. A recent blog posting at Microsoft made it known that they are quite a headache. Hyun Choi of the Microsoft Malware Protection Center said that the two programs are regularly found together. They operate collaboratively. They are "downloaders" and they work by alternatively downloading different variations of one another. The problem, aside from their computer invasion, is that they are hard to clean and can elude antivirus software.

The first malware player, Vobfus, is named after its characteristics. Think "Visual Basic." Think "obfuscated." Vobfus, detected in September 2009, is known as a downloader and it is compiled in p-code (pseudo code) or native code. A computer user might, for example, pick up Vobfus by way of a booby-trapped link. Once Vobfus gets into the system, it downloads the Beebone program, another downloader, ready for action to install other malicious software. Beebone has been downloading Trojans such as Zbot, Sirefef, Fareit, Nedsym and Cutwall.

In his blog posting, Choi talked about how this works. "Vobfus copies itself to the %userprofile% folder with a random name, or a not-so-random name…It also creates a runkey to ensure it runs every time Windows starts. Finally, Vobfus contacts a C&C server to obtain encrypted instructions on where to download Beebone; Beebone subsequently downloads Vobfus, and a number of other threats."

Choi also commented on the downsides of the pair's cyclical nature:

"Where Vobfus is detected, we often findWin32/Beebone too; thus exists the cyclical relationship between Vobfus and Beebone, the two threat families that are intrinsically related. This cyclical relationship between Beebone and Vobfus downloading each other is the reason why Vobfus may seem so resilient to antivirus products. Vobfus and Beebone

can constantly update each other with new variants."

Among his guidelines for helping to prevent Vobfus and Beebone infections, he noted that "one infection vector is drive-by download, so use caution when clicking external links, and keep your browser and all other installed software up to date to help prevent software exploits." Also, as Vobfus is primarily downloaded by Beebone or spread via removable drives, "a possible method of prevention is disabling autorun functionality."

The Microsoft Malware Protection Center gathers and analyzes data, working with organizations inside and outside Microsoft, and staying "agile to combat evolving threats." The Center seeks to respond to malware outbreaks and advise customers.

More information: blogs.technet.com/b/mmpc/archi … ions-from-above.aspx

Citation: Malware: Vobfus and Beebone infections are double-trouble (2013, July 2) retrieved 23 June 2024 from https://phys.org/news/2013-07-malware-vobfus-beebone-infections-double-trouble.html