Introducing Blue Pill

Jun 22, 2006 by **Joanna Rutkowska**

All the current rootkits and backdoors, which I am aware of, are based on a *concept*. For example: FU was based on an idea of unlinking EPROCESS blocks from the kernel list of active processes, Shadow Walker was based on a concept of hooking the page fault handler and marking some pages as invalid, deepdoor on changing some fields in NDIS data structure, etc... Once you know the concept you can (at least theoretically) detect the given rootkit.

Now, imagine a malware (e.g. a network backdoor, keylogger, etc...) whose capabilities to remain undetectable do not rely on obscurity of the concept. Malware, which could not be detected even though its algorithm (concept) is publicly known. Let's go further and imagine that even its code could be made public, but still there would be no way for detecting that this creature is running on our machines...

Over the past few months I have been working on a technology code-named Blue Pill, which is just about that - creating 100% undetectable malware, which is not based on an obscure concept.

The idea behind Blue Pill is simple: your operating system swallows the Blue Pill and it awakes inside the Matrix controlled by the ultra thin Blue Pill hypervisor. This all happens on-the-fly (i.e. without restarting the system) and there is no performance penalty and all the devices, like graphics card, are fully accessible to the operating system, which is now executing inside virtual machine. This is all possible thanks to the latest virtualization technology from AMD called SVM/Pacifica.

How does the Blue Pill-based malware relates to **SubVirt rootkit (http://research.microsoft.com/csm/CSM_Publications.htm)**, presented a few months ago by Microsoft Research and University of Michigan? Well, there are couple of important differences:

1. SubVirt is a permanent (i.e. restart surviving) rootkit. And it has to be, because the SubVirt's installation process requires that it takes control before the original operating system boots. Consequently, in contrast to Blue Pill, SubVirt can not be installed 'on-the-fly'. It also means that SubVirt must introduce some modifications to hard disk, which allows for the 'off line' detection.

2. SubVirt was implemented on x86 hardware, which doesn't allow to achieve 100% virtualization, because there are number of sensitive instructions, which are not privileged, like the famous SIDT/SGDT/SLDT. This allows for trivial detection of the virtual mode - see e.g. my little **Red Pill (http://invisiblethings.org/papers/redpill.html)** program. This however, doesn't apply to Blue Pill, as it relies on AMD SVM technology.

3. SubVirt is based on one of the commercial VMM: Virtual PC and/or VMWare. Both of these applications create virtual devices to be used by the operating system, which are different from the real underlying hardware (e.g. network cards, graphic cards, etc.), which allows for easy detection of the virtual machine.

I would like to make it clear, that the Blue Pill technology does not rely on any bug of the underlying operating system. I have implemented a working prototype for Vista x64, but I see no reasons why it should not be possible to port it to other operating systems, like Linux or BSD which can be run on x64 platform.

I will be talking about Blue Pill and demonstrating a working prototype for Vista x64 at the end of July at **SyScan Conference (http://syscan.org/)** in Singapore.

Also, I will present a generic method (i.e. not relaying on any implementation bug) of how to insert arbitrary code into the Vista Beta 2 kernel (x64 edition), thus effectively bypassing the (in)famous Vista policy for allowing only digitally singed code to be loaded into kernel. Of course, the presented attack does not require system reboot.

Joanna Rutkowska
Qubes OS (https://qubes-os.org) & Invisible Things Lab (http://invisiblethingslab.com/)