From: Joichi Ito <[redacted]>
To: Jeffrey Epstein <jeevacation@gmail.com>
Subject: Fwd: [IP] How Splitting a Computer Into Multiple Realities Can Protect You From Hackers
Date: Thu, 20 Nov 2014 20:25:48 +0000

Cool

Sent from my iPhone

Begin forwarded message:

From: "Dave Farber via ip" <[redacted]>
Date: November 20, 2014 at 15:14:19 EST
To: "ip" <[redacted]>
Subject: [IP] How Splitting a Computer Into Multiple Realities Can Protect You From Hackers
Reply-To: dave@farber.net

---------- Forwarded message ----------
From: "Dewayne Hendricks" <[redacted]>
Date: Nov 20, 2014 3:06 PM
Subject: [Dewayne-Net] How Splitting a Computer Into Multiple Realities Can Protect You From Hackers
To: "Multiple recipients of Dewayne-Net" <[redacted]>
Cc:

HOW SPLITTING A COMPUTER INTO MULTIPLE REALITIES CAN PROTECT YOU FROM HACKERS
By ANDY GREENBERG
Nov 20 2014
<[redacted]>

Eight years ago, polish hacker Joanna Rutkowska was experimenting with rootkits—tough-to-detect spyware that infects the deepest level of a computer's operating system—when she came up with a devious notion: What if, instead of putting spyware inside a victim's computer, you put the victim's computer inside the spyware?

At the time, a technology known as virtualization was becoming easier to implement on PCs, allowing anyone to create a miniature operating system, known as a virtual machine, inside their main operating system. Rutkowska manipulated virtualization into a mind-contorting weapon called a Blue Pill attack. Without them knowing, her rootkit moved the victim's entire OS into a virtual machine controlled by the hacker, allowing everything the target did to be watched. The victim's digital world would suddenly exist inside an alternate reality, and no amount of antivirus or antirootkit scanning could break the system out of that aquarium. "Your operating system swallows the Blue Pill and it awakes inside the Matrix," Rutkowska wrote in a blog post explaining the trick. Eventually she honed the maneuver so that not even launching another virtual machine inside the Blue Pilled system would glitch the illusion—her attack supported a dream within a dream.

But as years passed, no real-world instances of Blue Pill attacks were discovered, even after other researchers developed tests capable of detecting the technique. Rutkowska's explanation? For normal spies and cybercriminals, ordinary rootkits work just fine. "There are still so many places in a Windows kernel to hide traditional malware," she says. "I was as vulnerable as any other user. This was annoying."

So Rutkowska flipped the game, this time in favor of the defenders. Four years ago her Warsaw-based firm, Invisible Things Lab, started developing its own operating system known as Qubes. The free open source OS lets users set up a collection of virtual machines on their PC, with a simple central interface to manage each quarantined system. Careful users can keep their personal online activities isolated in one virtual machine, for instance, while they do their work in another, and their banking in a third. (Rutkowska typically runs about 15.) Open a malicious email attachment or click on an infected website and the malware can't break out of that one contaminated container.

If it works as promised, even NSA-level exploits would be contained to a single compartment in Qubes' architecture, one that could be evaporated and re-created at will. Recovering from even the nastiest hacker attack, in other words, could soon be as easy as waking from a bad dream.

Dewayne-Net RSS Feed: <[redacted]>

Archives | Modify Your Subscription | Unsubscribe Now

Powered by Listbox