DANGER USB! COULD A FLASH DRIVE'S FIRMWARE BE HIDING UNDETECTABLE MALWARE?

GRAHAM CLULEY

AUG 1, 2014

You see that USB stick in your hand?

The one that has been wiped and contains no files, that your anti-virus software claims is squeaky-clean and free of any malicious code?

Well, maybe it's not quite as simple as that.

Because a pair of security researchers are planning to demonstrate next week how they managed to reprogram the firmware on removable USB drives to contain malware capable of compromising computer systems.

And, because the malware never touches the flash memory of the USB device (where you files would normally reside) but in the firmware that controls the stick's basic functions instead, the malicious code is entirely invisible to conventional security tools and your computer's operating system.

Once reprogrammed, claim the researchers, there are a number of ways in which the once harmless USB drive can act maliciously:

- A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.

- The device can also spoof a network card and change the computer's DNS setting to redirect traffic.
- A modified thumb drive or external hard disk can – when it detects that the computer is starting up – boot a small virus, which infects the computer's operating system prior to boot.

To prove the concept, security researchers Karsten Nohl and Jakob Lell have created some code that they have dubbed "BadUSB", which they claim can turn a benign device "evil".

BadUSB tricks the targeted computer into believing that it is not a USB flash drive, but a USB keyboard instead. When you plug in the USB stick, it rapidly sends a string of characters which look to the computer just as though they have been typed at the keyboard by the user.

In short, it's as though you have logged into your computer, and allowed a complete stranger to push you out of your chair and start typing commands on your PC.

And if those commands, say, opened a browser window which surfed to a webpage containing a zero-day exploit you might find that your computer has been badly compromised within a blink of the eye. Alternatively, the keyboard commands sent by the malicious firmware could attempt to execute dangerous code on the USB stick's flash drive itself.

Keystroke injection via USB devices isn't an entirely new concept, and there have been tools available for penetration testers and hackers to buy online for years which have

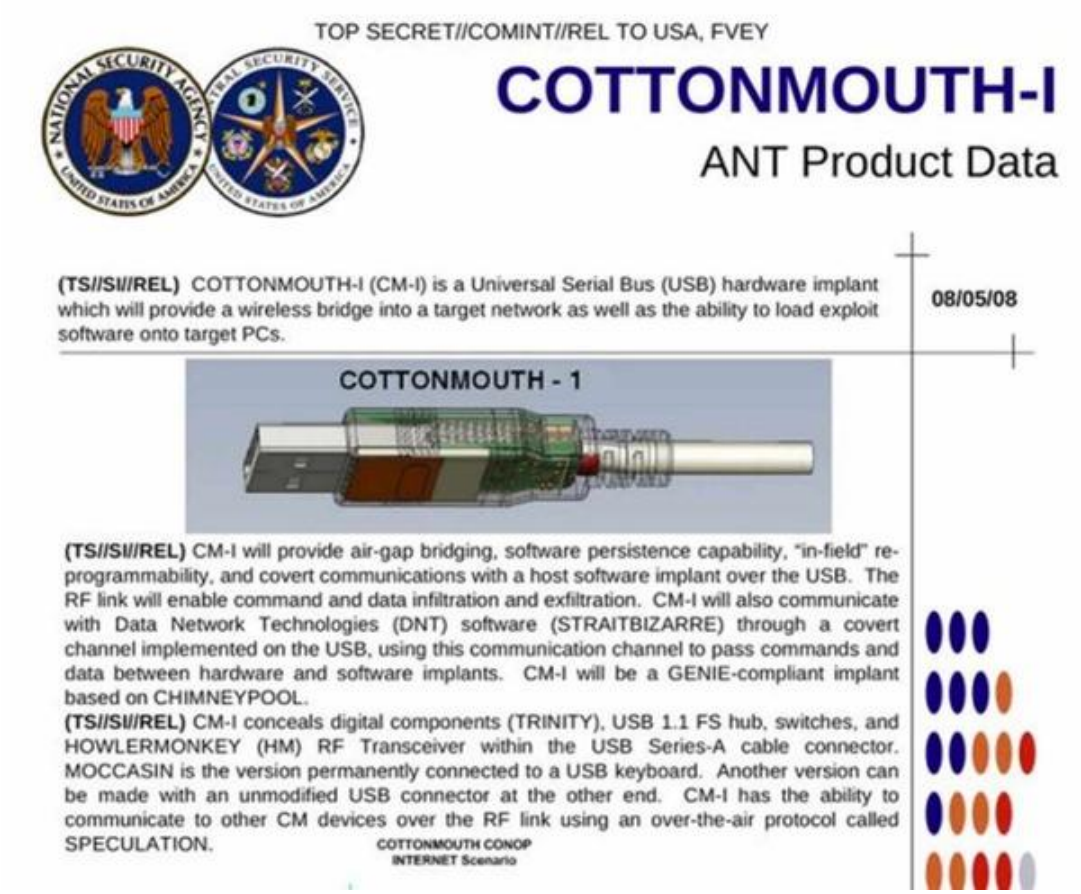
exploited this issue, and allowed them to take advantage of a few seconds' physical access to a target PC.

But what makes BadUSB different is that they appear to have shown how the firmware of a regular USB stick can be subverted in this fashion, making a breach much less likely to be spotted. Nohl and Lell spent months researching and reverse engineering the controller chip firmware on USB devices, and working out how malware on an already infected PC could make a clean USB stick malicious, greatly increasing the chances of an infection spreading.

Such a method of spreading would be tremendously handy, of course, to hackers targeting organizations running an air-gapped environment, where computers had no internet access, and were not networked together for security reasons. What sorts of organizations would be likely to air-gapping its computers? Well, critical infrastructure would be one obvious example.

Remember Stuxnet? That malware, which targeted critical infrastructure at a uranium enrichment facility at Natanz, Iran, spread via USB sticks – exploiting a zero-day Windows vulnerability.

And then there is Cottonmouth, the top-secret spying device used by the NSA which – according to documents leaked by Edward Snowden – could silently install malware onto a targeted computer while disguised as a USB plug.



There's no evidence that Cottonmouth involved firmware-exploitation like BadUSB, but it's clearly a possibility.

It's worth bearing in mind, that threats like BadUSB aren't just a potential problem for traditional computers and laptops.

There are many electronic devices these days which connect via a USB, or use a USB connection to charge their batteries. In theory, a carefully-crafted attack could attempt to meddle with these types of devices also.

It's easy to imagine, for instance, that smartphones could be targeted as they are often plugged into USB connections for charging or to sync files with desktop computers.

Nohl and Lell claim that the ubiquity of USB is its "Achilles heel":

"Since different device classes can plug into the same connectors, one type of device can turn into a more capable or malicious type without the user noticing."

"To turn one device type into another, USB controller chips in peripherals need to be reprogrammed. Very widely spread USB controller chips, including those in thumb drives, have no protection from such reprogramming."

So, what can you do about the threat of malicious flash drive firmware?

Well, firstly, don't panic.

These are sophisticated attacks which require considerable research and effort to pull off successfully. And, as Iain Thomson at The Register points out, attacks are vendor-specific as every vendor creates their controllers differently.

Secondly, the BadUSB scenario described above details how a sequence of keystrokes could take your browser to a website hosting a malicious exploit, or run malicious code elsewhere on the flash drive.

If you have followed best practices then you will have hopefully been keeping your computer systems updated with the latest security patches, web filtering, access control and anti-virus software to reduce the opportunities for such an attack to succeed – even if you cannot stop the malicious code in a USB stick's firmware from executing, make sure that it fails in its next objective.

Thirdly, moan at the USB vendors. They should be building security into their devices to prevent unauthorised parties from updating USB drive firmware, and only allow updates that have been cryptographically verified for their legitimacy.

Finally, always be careful about what devices you plug into your computer. If you have ever shared a USB device with someone else it *could* have been compromised, and *might* no longer be trustworthy. The golden rule is never plug anything into your computer that you do not 100% trust.

Maybe it's looking more attractive all the time to share files via the internet (although that brings its own issues) rather than USB sticks, and we'll begin to see the USB drive go the way of the floppy disk…