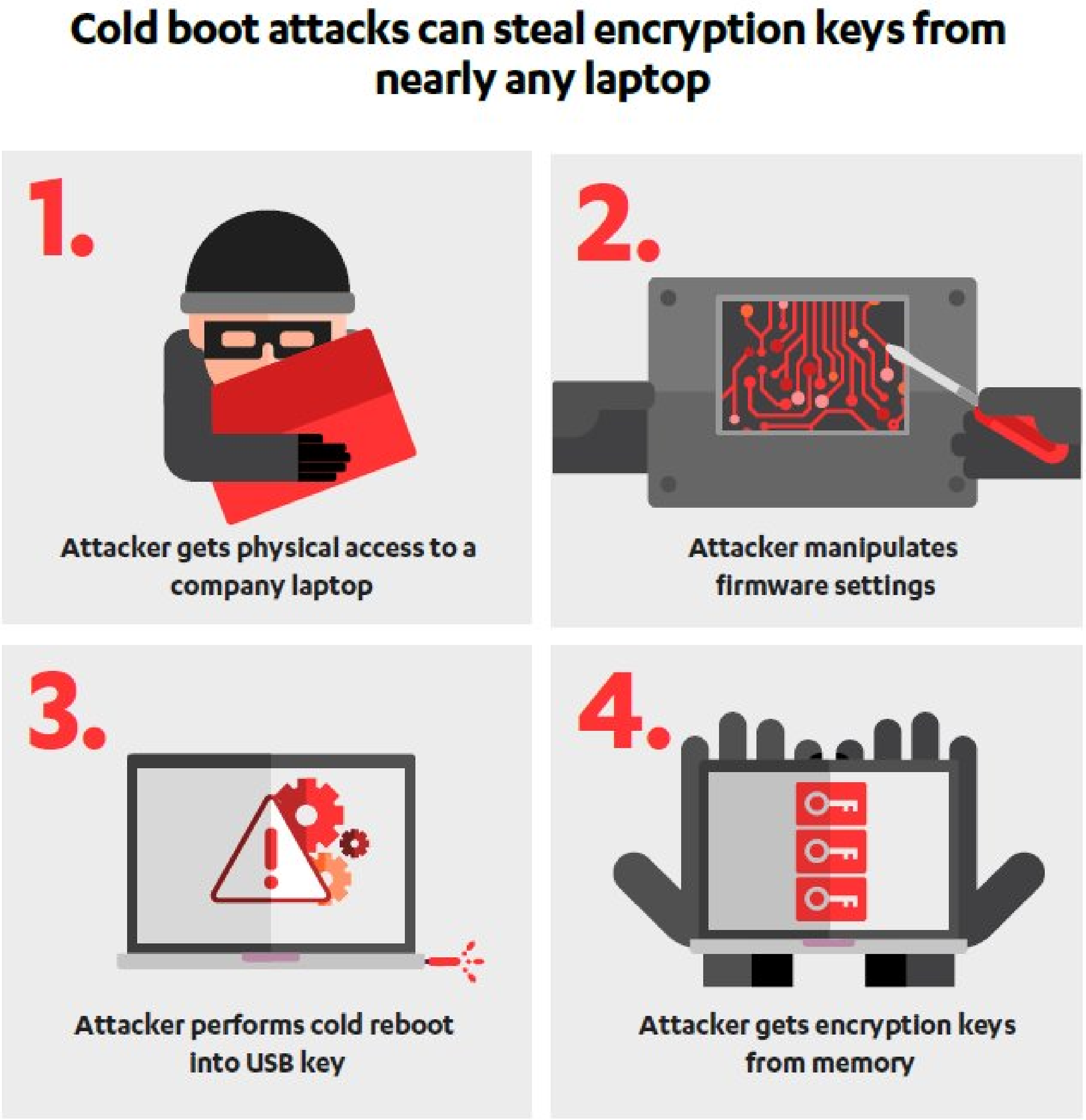
Firmware weakness extends red carpet for cold boot attacks

September 16 2018, by Nancy Owano


Cold boot attacks can steal encryption keys from nearly any laptop
1.
Attacker gets physical access to a company laptop
2.
Attacker manipulates firmware settings
3.
Attacker performs cold reboot into USB key
4.
Attacker gets encryption keys from memory

Credit: F-Secure

"The chilling reality of cold boot attacks" is the title of a video posted by F-Secure on Thursday. The chilling reality is that savvy security mischief-makers can still perform the attacks, as two researchers learned recently.

Here is a show of industry effort in the past, though. Computer firmware has carried measures to guard against cold boot attacks that essentially are seeking to grab sensitive data from high value computers.

Here is some good news: Cold boot attacks are not trivial types of exploit; they require physical access and special hardware tooling to perform, said Catalin Cimpanu in *ZDNet*.

One argument might then be, well it's not such a big deal in terms of ease of exploit; not every computer user can get physical, so to speak, with anything more complex than changing batteries and plugging in new peripherals.

In turn, these are not the kinds of attacks can say is a threat vector for normal users, "but only for computers storing highly-sensitive information, or for high-value individuals such as government officials or businessmen."

Well, on the other hand, if you are in IT management of a business, the boot attack the researchers describe is not that comforting as hackers would get the keys to people's computers. The duo found a way to bypass protection and exploit a weakness in the computer firmware to steal encryption keys and other data, in a successful cold boot attack.

Who spotted this?

Olle Segerdahl, principal security researcher with F-Secure, along with fellow security consultant Pasi Saarinen, found that a third-party protection could be broken if they manipulated the firmware.

What does "cold boot attack" mean?

Cimpanu: It's when an attacker forces a computer reset/reboot and then steals any data left over in the RAM.

Actually, the researchers said they discovered the weakness "in nearly all modern laptops."

Over to their F-Secure blog where Adam Pilkey spelled out what all the fuss was about—fuss would not be a careless word choice considering the ploy could get credentials to corporate networks, leave alone passwords.

"Using a simple tool, Olle and Pasi learned how to rewrite the non-volatile memory chip that contains these settings, disable memory overwriting, and enable booting from external devices. Cold boot attacks can then be carried out by booting a special program off a USB stick."

Translation: They got physical with the hardware. Point is, wrote Pilkey, "it's a known technique among hackers." Olle further commented that it is the kind of exploit attackers looking for bigger fish, such as corporate or bank group, would be likely to try.

Several types of data could potentially be at risk, said Segerdahl. "Our primary target was hard drive encryption keys stored in memory," he explains, but attackers could also access passwords, network credentials, and any information on the machine that its user can access.

The two were sharing their findings with companies like Microsoft, Intel and Apple—and with the public via a presentation at a conference in Sweden and at Microsoft's BlueHat v18 in the US on September 27. Pilkey noted some companies exploring mitigation strategies.

Long and short, there is a weakness in how computers protect firmware. Once they gain access to a computer they can scoff up encryption keys and other information.

If the very phrase cold boot attack sounds all too familiar it should be; cold boot attacks have for some time been a known way of getting encryption keys from devices. So, what do the F-Secure team recommend? After all, Pilkey said that "companies can configure laptops so that an attacker using a cold boot attack won't find anything to steal."

The potential value of having a Bitlocker PIN in the mix of safeguards was mentioned, whereby IT departments configure all company computers to either shut down or hibernate—not sleep mode. Then users would enter their Bitlocker PIN when they power up or restore their computers.

More information: blog.f-secure.com/cold-boot-attacks/

Citation: Firmware weakness extends red carpet for cold boot attacks (2018, September 16) retrieved 20 March 2024 from https://techxplore.com/news/2018-09-firmware-weakness-red-carpet-cold.html