Published on *Tux Machines* (http://www.tuxmachines.org)

Home > content > Security: Scare, Onion and Listening Devices

Security: Scare, Onion and Listening Devices

By *Roy Schestowitz*

Created *13/11/2019 - 8:23pm*

Submitted by Roy Schestowitz on Wednesday 13th of November 2019 08:23:37 PM Filed under Security [1]

- **Yes, if you install malicious programs, then they will likely do malicious things [2] [Ed: Yes, if you install malicious programs, then they will likely do malicious things]**

> The researchers determined that parts of a specific component used by Cobalt in the third stage of an attack are present in PureLocker. It is the JScript loader for the "more_eggs" backdoor, described by security researchers at Morphisec.
>
> In previous research, IBM X-Force revealed that FIN6, another cybercriminal group targeting financial organizations, also used the "more_eggs" malware kit.
>
> Most of the code in PureLocker is unique, though. This suggests that the malware is either a new one or an existent threat that has been heavily modified.

- **What is Security Onion? And is it better than a commercial IDS? [3]**

> Back in the early oughts, a common complaint about Linux was that while it was free/libre, it came with no support and you had to pay expensive senior sysadmins to run Linux systems. Fast forward to today, and Linux has conquered basically every field except for the desktop market.
>
> [...]
>
> Security Onion is looking more and more polished with every year that passes, and it may be worth considering if you've got a deep enough security bench to customize, deploy and maintain Security Onion for your enterprise.

- **Fooling Voice Assistants with Lasers** [4]

    Siri, Alexa, and Google Assistant are vulnerable to attacks that use lasers to inject inaudible?and sometimes invisible?commands into the devices and surreptitiously cause them to unlock doors, visit websites, and locate, unlock, and start vehicles, researchers report in a research paper published on Monday. Dubbed Light Commands, the attack works against Facebook Portal and a variety of phones.

    Shining a low-powered laser into these voice-activated systems allows attackers to inject commands of their choice from as far away as 360 feet (110m). Because voice-controlled systems often don?t require users to authenticate themselves, the attack can frequently be carried out without the need of a password or PIN. Even when the systems require authentication for certain actions, it may be feasible to brute force the PIN, since many devices don?t limit the number of guesses a user can make. Among other things, light-based commands can be sent from one building to another and penetrate glass when a vulnerable device is kept near a closed window.

    The attack exploits a vulnerability in microphones that use micro-electro-mechanical systems, or MEMS. The microscopic MEMS components of these microphones unintentionally respond to light as if it were sound. While the researchers tested only Siri, Alexa, Google Assistant, Facebook Portal, and a small number of tablets and phones, the researchers believe all devices that use MEMS microphones are susceptible to Light Commands attacks.

Security

Source URL: http://www.tuxmachines.org/node/130456

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.bleepingcomputer.com/news/security/purelocker-ransomware-can-lock-files-on-windows-linux-and-macos/
[3] https://www.csoonline.com/article/3453199/what-is-security-onion-and-is-it-better-than-a-commercial-ids.html
[4] https://arstechnica.com/information-technology/2019/11/researchers-hack-siri-alexa-and-google-home-by-shining-lasers-at-them/