THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

December 2024

From the Desk of Denise Spiller, Director

Office of Research Security

Anyone can buy data tracking US soldiers and spies to nuclear vaults and Brothels in Germany

Dhruv Mehrotra and Dell Cameron, November 19, 2024

More than 3 billion phone coordinates collected by a US data broker expose the detailed movements of US military and intelligence workers in Germany and the Pentagon is powerless to stop it.

Nearly every weekday morning, a device leaves a two-story home near Wiesbaden, Germany, and makes a 15-minute commute along a major autobahn. By around 7 am, it arrives at Lucius D. Clay Kaserne—the US Army's European headquarters and a key hub for US intelligence operations.

The device stops near a restaurant before heading to an office near the base that belongs to a major government contractor responsible for outfitting and securing some of the nation's most sensitive facilities.

To read the full article, use the link below: https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/

End of the year reminders:

ALL Annual Security training requirements must be completed by Thursday, December 19, 2024. Annual Security Trainings include CITI Export Control, Controlled Unclassified Information (CUI), Insider Threat and the 2024 Annual Security Refresher trainings.

The 2024 Annual Security Refresher training is currently on-line for the remainder of the year.

Hackers can access laptop webcams without activating the LED, researcher finds

Ernestas Naprys, Senior Journalist, November 28, 2024

Taping the webcam on your laptop isn't a dumb idea. A security engineer has discovered a way to reflash the webcam firmware on a Lenovo ThinkPad X230 laptop and arbitrarily control its LED independently if the webcam itself is activated. Malware could effectively turn on the camera without an LED.

Andrey Konovalov, a Linux kernel security engineer who goes by the moniker xairy on GitHub, posted a tool to get software control of a webcam's LED on the business laptop ThinkPad X230.

While the laptop model is already more than a decade old, the code sparked a heated discussion on Hacker News. Why isn't the webcam LED hardwired?

The whitehat discovered that the X230's camera is plugged in over a USB connector and is based on the Ricoh R5U8710 USB camera controller. Some other laptops from 2012 also use this controller.

It stores part of the firmware, and the LED is connected to one of the pins. Therefore, the controller can enable or disable the LED independently.

After bricking a few laptops, xairy was able to develop and flash a custom firmware. To achieve that, the engineer had to dump and analyze the controller's SROM (read-only memory) in hexadecimal and disassemble the code without any documentation to find locations responsible for streaming video and enabling the LED pin.

Xairy demonstrated that USB device firmware can be overwritten using software and then controlled by corrupted code.

To read the full article, use the link below: https://cybernews.com/security/hackers-can-access-laptop-webcams-without-activating-the-led/

Novel phishing campaign uses corrupted Word documents to evade security

Lawrence Abrams

A novel phishing attack abuses Microsoft's Word file recovery feature by sending corrupted Word documents as email attachments, allowing them to bypass security software due to their damaged state but still be recoverable by the application.

Threat actors constantly look for new ways to bypass email security software and land their phishing emails in targets' inboxes.

A new phishing campaign discovered by malware hunting firm Any.Run utilizes intentionally corrupted Word documents as attachments in emails that pretend to be from payroll and human resources departments.

To read the full article, use the link below:

https://www.bleepingcomputer.com/news/security/novel-phishing-campaign-uses-corrupted-word-documents-to-evade-security/

OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER
Director
824-6444, denise.spiller@uah.edu

JANINE WILSON
Assistant Director
824-3025, janine.wilson@uah.edu

JOSEPH DORROH
Special Security Officer (SSO)
824-6034, joseph.dorroh@uah.edu

APRIL MCMEANS
Security Specialist
824-6048, april.mcmeans@uah.edu

RILEY STARK
Student Specialist
824-6035, riley.stark@uah.edu