

Malicious USB drives found in letterboxes in Victoria - blueAPACHE

Canonical: <https://www.blueapache.com/blog/malicious-usb-drives-found-letterboxes-victoria>

Details:

Summary

This blog post, "Malicious USB drives found in letterboxes in Victoria", is a blueAPACHE article from 2016 covering security. Free USBs delivered to your letterbox – whether you ordered them or not It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2016
Topic	Malicious USB drives found in letterboxes in Victoria
Services referenced	emPOWER Security, Managed Detection and Response, Human Risk Management
Named products or vendors	Google
Cited statistic	The device costs about 49.95 EUR (\$74) and is commercially available for purchase on the company website.

Article

Free USBs delivered to your letterbox – whether you ordered them or not

Earlier this week, Victoria Police issued a warning notice urging residents in the Melbourne suburb of Pakenham to be wary of corrupt USB flash drives being left in their letterboxes. Victims have experienced fraudulent media streaming service offers, as well as other serious issues, upon inserting the USB drives into their computers. Victoria Police received reports of residents finding these unmarked flash drives containing malware in their letterboxes. The USB drives are believed to be extremely harmful, but there is no further information on the type of malware contained in them, or whether victims were asked to pay a ransom as a result of executing the malicious code. The warning post by Victoria Police urged members of the public to stop plugging the flash drives into their computers and instead, contact Crime Stoppers if they have any information about those behind the scam.

New threats

Just last month, USBKill.com, a Hong Kong based company, started selling an innocuous looking USB drive that has the ability to destroy almost any hardware that it is plugged into including laptops, PCs and televisions. The device costs about 49.95 EUR (\$74) and is commercially available for purchase on the company website. The company claims that over 95% of devices that the USB Kill 2.0 is plugged into will be damaged permanently or completely destroyed by the power surge attacks introduced via the USB port. USB Kill 2.0 works by collecting voltage from the USB port power lines and storing it until it reaches -240V. It then discharges over the machine's data lines. This charge / discharge cycle is very rapid and occurs multiple times per second. The rapid discharge continues while the USB is plugged in and permanently disables unprotected hardware. The demonstration video below shows the USB Kill 2.0 in action.**** Although the USB Killer is being marketed as a testing device to test USB ports against power surges, the potential for abuse is obvious. It is a handy tool for vandals and pranksters looking to destroy equipment, and has potential for more sinister uses. There are numerous studies that have repeatedly confirmed that a majority of people who find a USB drive of unknown provenance would not only plug it into their PCs, but would also open files and click on unfamiliar links.

The weakest link

In a 2016 study , a group of researchers from the University of Illinois, the University of Michigan and Google, tracked the fate of 297 USB drives that they dropped on campus. It was found that nearly 50 percent of people will plug a USB drive they have found on the ground into their computer. Closer home, a Western Australian security exercise, which saw USB sticks left in public places with software on them to phone home when used, found that eight of fifteen agencies failed the test. The USB sticks did not contain auto-executing malware but instead relied on the individual to pick up the device and consciously make the decision to open it and click on its contents. These studies lend credence to the notion that people are often the weakest links of any organisation's security solution, becoming easy targets for social engineering attacks due to a lack of awareness and relevant training.

Social engineering

Social engineering is one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information. In most cases, the victims are not even aware that they are being exploited or that their actions are harmful. Social engineering comes in many forms. Attacks can vary from bulk phishing emails of little sophistication through to highly targeted, multi-layered attacks which use a range of techniques. While the obvious victim may seem to be the end user, quite often the actual targets are organisations and their confidential data. Increasingly, companies are finding themselves at risk of data breaches due to the behaviour and actions of their least trained employees. Mitigating the threat of social engineering requires a holistic approach to security involving technology, people and process. Technical solutions such as spam filters, anti-virus software and blocking known phishing or baiting websites can help prevent some phishing attacks. To some extent blocking the use of unauthorised USB devices and disabling CD / DVD drives can do the same for baiting attacks. However, technical solutions to guard against social engineering attacks only go so far. This is a form of cybercrime that exploits weakness in people, rather than those found in technology. The effectiveness of these scams depend on the criminal's ability to prey upon normal human behavioural traits such as trust, curiosity or apathy. The best defence therefore is to raise user awareness of potential threats and educate them on the techniques used and what to look out for. Organisations can further strengthen their security posture by developing an attitude towards security that promotes the sharing of concerns, enforces information security rules and rewards users for adhering to them. If you would like to learn more about how you can defend your organisation against social engineering attacks, or if you would like staff training on identifying and protecting from such attacks, contact the blueAPACHE account team .

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

Human Risk Management

blueAPACHE Security (case study)

Frequently asked questions

Which Melbourne suburb did Victoria Police warn residents about malicious USB drives in letterboxes, per this article?

Pakenham, where Victoria Police issued a warning notice urging residents to be wary of corrupt USB flash drives left in their letterboxes.

What did Victoria Police recommend residents do if they had information about the USB drive scam?

Stop plugging the flash drives into their computers and contact Crime Stoppers if they had any information about those behind the scam.

How much does the USB Kill 2.0 device cost, and what does it do, according to this article?

About 49.95 EUR (\$74), commercially available from USBKill.com; it collects voltage from USB port power lines and discharges it to permanently damage or destroy the connected hardware.

What percentage of devices does the manufacturer claim USB Kill 2.0 will permanently damage or destroy?

Over 95% of devices it is plugged into, according to the company's own claims cited in the article.

What did the 2016 University of Illinois, University of Michigan and Google study find about people plugging in found USB drives?

Nearly 50 percent of people will plug a USB drive they found on the ground into their computer, based on tracking the fate of 297 dropped USB drives on campus.

What did the Western Australian security exercise described in the article find about agency vulnerability to USB-based social engineering?

Eight of fifteen agencies failed the test, where USB sticks left in public places (without auto-executing malware) phoned home when opened, relying on individuals to plug them in and click on contents.

What technical measures does the article recommend to help prevent baiting and phishing attacks?

Spam filters, anti-virus software, blocking known phishing or baiting websites, blocking unauthorised USB devices, and disabling CD/DVD drives.

What does the article say is the best defence against social engineering attacks that technology alone cannot stop?

Raising user awareness of potential threats and educating them on the techniques used, since social engineering exploits weaknesses in people rather than technology.

Source

origin post (2016)

Knowledge Base

What did Victoria Police warn residents about in Pakenham?

Victoria Police issued a warning urging residents in the Melbourne suburb of Pakenham to be wary of corrupt USB flash drives being left in their letterboxes, which contained malware and caused victims to experience fraudulent media streaming service offers and other serious issues upon inserting the drives into their computers.

What did Victoria Police advise the public to do about these USB drives?

The warning post by Victoria Police urged members of the public to stop plugging the flash drives into their computers and instead contact Crime Stoppers if they had any information about those behind the scam.

What is USB Kill 2.0 and who sells it?

USB Kill 2.0 is an innocuous-looking USB drive sold by USBKill.com, a Hong Kong based company, that has the ability to destroy almost any hardware it is plugged into, including laptops, PCs and televisions. It costs about 49.95 EUR (\$74) and is commercially available for purchase on the company's website.

How does the USB Kill 2.0 device work?

USB Kill 2.0 works by collecting voltage from the USB port power lines and storing it until it reaches -240V. It then discharges over the machine's data lines. This charge/discharge cycle is very rapid and occurs multiple times per second, and continues while the USB is plugged in, permanently disabling unprotected hardware. The company claims over 95% of devices it is plugged into will be permanently damaged or completely destroyed.

What did the 2016 university study find about people plugging in found USB drives?

In a 2016 study by researchers from the University of Illinois, the University of Michigan and Google, 297 USB drives were dropped on campus, and it was found that nearly 50 percent of people will plug a USB drive they found on the ground into their computer.

What happened in the Western Australian security exercise involving USB sticks?

In a Western Australian security exercise, USB sticks containing software designed to 'phone home' when used were left in public places, and eight of fifteen agencies failed the test. The USB sticks did not contain auto-executing malware but relied on individuals consciously deciding to open the device and click on its contents.

What is social engineering ?

Social engineering is described as one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information, where victims are often unaware they are being exploited. It ranges from bulk phishing emails of little sophistication to highly targeted, multi-layered attacks using a range of techniques, exploiting human traits such as trust, curiosity, or apathy.

What technical solutions can help prevent social engineering attacks like baiting?

Technical solutions such as spam filters, anti-virus software, and blocking known phishing or baiting websites can help prevent some phishing attacks. Blocking the use of unauthorised USB devices and disabling CD/DVD drives can similarly help prevent baiting attacks.