Hand-delivered hacking: malicious USBs left in mailboxes

September 22 2016, by Raphael Satter

This photo taken July 9, 2016 shows a thumb drive delivered to the home of French software engineer Julien Ascoet outside the French port city of Nantes. Although the memory stick is branded, Ascoet says he doesn't believe the brand is in any way linked to the mysterious delivery. And Ascoet is not alone; there are signs that cybercriminals are experimenting with hand-delivery of malware to people's homes. Australian police have drawn international attention by announcing that "extremely harmful" memory sticks have been left in mailboxes across the suburban town of Pakenham, about 60 kilometers (37 miles) southeast of Melbourne. (Julien Ascoet via AP)

Julien Ascoet was already suspicious when he pulled the plain white

envelope from his mailbox this past July.

The letter had no stamp and was completely unmarked. Someone must have delivered it in person to Ascoet's home outside the French port city of Nantes.

"I opened it gingerly," the software engineer said in an online chat Thursday. "You never know what's inside. I was remembering an episode of (police procedural drama) 'NCIS' where they found a similar envelope with anthrax."

What Ascoet found was a memory stick with no note or explanation. It wasn't anthrax, but it could still be dangerous.

Memory sticks, also called thumb drives or USBs, are sometimes used to spread malicious software from computer to computer. This USB was branded, but Ascoet said the device appeared used and that he doubted there was any connection between the brand and the mysterious delivery.

Ascoet, who also works as a security researcher, eventually threw the device out—although not before photographing it and posting the picture to Twitter .

"Never EVER plug in such present," he said by way of caption.

Stories like Ascoet's are anecdotal, but as web users get wise to rogue links and booby-trapped attachments, there are signs that cybercriminals are experimenting with hand-delivery of malware to people's homes.

On Wednesday, Australian police drew international attention when they announced that "extremely harmful" memory sticks had been left in mailboxes across the suburban town of Pakenham, about 60 kilometers (37 miles) southeast of Melbourne. Pakenham Police Sgt. Guy Matheson

said in a telephone interview Thursday that the unmarked thumb drives started showing up several days ago.

Disguised as offers for Netflix or a similar service, Matheson said rogue programs lurking on the drives instead held victims' computers hostage, demanding a hefty payment in the electronic currency Bitcoin as ransom.

Matheson said two or three people had fallen for the ruse.

The technique of dropping a malicious USB somewhere and hoping someone will pick it up and plug it in has long been favored by spies to hack into hard-to-reach computers, said University of Manchester doctoral student Nikola Milosevic, who has studied the history of malware. The New York Times reported that the infrastructure-wrecking Stuxnet worm spread to Iran's nuclear facilities using a thumb drive placed in the hands of an unwitting employee, for example. And despite the risks inherent in walking up to someone's house and dropping malicious software through their mail slot, leveraging people's inherent curiosity can mean a bigger potential payoff.

"People are more likely to put USB stick into their computer than click a link or open file sent by the unknown person," Milosevic said in an email. "This type of attack has the potential to have a high success rate."