Researcher at London event focuses on e-cig used for computer exploit

June 19 2017, by Nancy Owano

Credit: CC0 Public Domain

(Tech Xplore)—E-cigarettes could be used to hack computers. They could not only serve as your stop-smoking tool but there is a possibility they could serve as an exploit platform as well.

But how? "With only minor modifications, the vape pen can be used by attackers to compromise the computers they are connected to - even if it seems just like they are charging," said Alexander Martin, technology reporter, with *Sky News*.

That's the word that caught the eye of several news sites recently, including *Geek.com* and *Infosecurity Magazine*, with Tara Seals reporting.

Martin said that security researcher Ross Bevington was at the BSides London gathering, where he talked about how an e-cigarette could be used to attack a computer.

The program notes said the title of his presentation was "Holy smokes, how to vape yourself to root." Bevington is a security researcher and consultant.

Launched in mid-2009, Security B-Sides is a community-driven event built for and by info security community members.

"The volunteers for Security B-Sides London were inspired by the framework of the original Security B-Sides event in the USA, and have worked together to bring this to the UK."

Bevington, said Martin, showed how an e-cigarette could be used to attack a computer by fooling the computer to believe it was a keyboard or by tampering with its network traffic.

"Many e-cigarettes can be charged over USB," said Seals, "and Bevington said that takes just a few simple tweaks to the vaporizer to turn it into a weapon that can download malicious payloads from the web."

She quoted Adam Brown, manager of security solutions at Synopsys. "As Bevington's recent research shows, a vape pipe could easily be modified to work as any kind of peripheral device when plugged in, and so could be used in a similar way to either deliver a payload or perform some other malicious activity while plugged in," he said.

Stephanie Mlot in *Geek.com* said, "Most e-cigs include a rechargeable lithium-ion battery, which plugs into a cable or connects directly to the computer's USB port. And that's when they get you."

In the bigger picture, getting us is a security weapon that goes beyond vape pens to a range of devices in this ever-connected world. Cesare Garlarti, chief security strategist at prpl Foundation, said in *Infosecurity Magazine* that this is yet another piece of proof that "a connected-everything world presents staggering cybersecurity ramifications."

Over email, he told them that "Developers and manufacturers understandably are eager to get their new high-tech devices to market, and unfortunately often overlook security."

There is some good news about the e-cigarette situation. First, e-cigs don't have that much memory, so complex code is a no-go, said Seals. An e-cigarette can only hold so much code. Also, many enterprises today block the use of USB ports, which would prevent an attack such as this.

The *Sky News* article, meanwhile, carried some advice from Bevington. Make sure the machine has updated its security patches. Have a good password. Lock your machine when you leave it. If running a business, obtain some kind of monitoring solution that can alert your security team if something like this attack occurs. Be wary if someone wants to plug something into your machine.