How to avoid hacking? Read this story, then turn off your computer

August 8 2016, by Tim Johnson, Mcclatchy Washington Bureau

Here's some advice for newbies to the largest cybersecurity and hacking conferences in the world, taking place in Las Vegas this week: Hackers are going to hack, so do everything you can to get out of their way.

Disable Wi-Fi and Bluetooth on your cellphone. Turn off your computer. Do not use ATMs near the convention site this week. Pay for everything with cash.

Sound extreme? Not to experts at the Black Hat and DefCon 24 conventions, which have drawn about 16,000 people from 108 countries, many of them trained to snoop on other people's digital devices.

In fact, some of the sessions at the three-day Black Hat convention, which started small in 1997 but now has corporate sponsors and plenty of law enforcement attendees, offered training on how to break into networks or how to attack them surreptitiously. Information security officers find the sessions helpful in understanding the evolving coding of malware, the software tools through which hackers break into systems.

In the unseen air around the Mandalay Bay Convention Center, it's mano a mano among digital combatants, hackers and security specialists.

"We're not stopping attacks. We're just observing them," said Neil R. Wyler, speaking at a network monitoring facility with multiple large screens at the convention center.

Wyler goes by the user name of "Grifter" and his day job is with RSA, a network security company based in Bedford, Mass. His business cards describe him as "hacker-in-residence" and "threat hunting & incident response specialist." As a security expert, he usually spots network intrusions and goes after them. But at Black Hat, he's had to take his hand off the holster even while observing that "there's a significant amount of malware flying around."

"We have full visibility. Every packet that flies across the network, we see it," he said.

Some of the harmful coding Wyler detects is instructional, coming from the laptops of experts in various conference rooms offering demonstrations.

"They are teaching them the latest hacking methods, how to stay stealthy," Wyler said, and if he and other monitors tried to stop the attacks, "you could screw up someone's demo in front of 4,000 people."

"Black Hat attracts the most talented hackers around the world in the private and public sector," said Vitali Kremez, a cybercrime intelligence analyst at Flashpoint, a cybersecurity company based in New York. "It's the Wild West. Some people are going to get hurt."

He looked at a hapless visitor and warned: "Don't connect."

The DefCon 24 Hacking Conference, which began Thursday and ends Sunday at the nearby Bally's Las Vegas Hotel & Casino, is a little grittier. Sessions include one on how to use digital tools to overthrow a government.

"DefCon is where you really don't want to leave your cellphone turned on at the show," said Tim Erlin, security and IT risk strategist at

Tripwire, a Portland, Ore.-based security software company. Some attendees take "burners," cheap disposable phones that they can throw in the trash afterward, he said.

If someone takes a smartphone, pranksters at DefCon "might 'brick' your device, make it inoperable," Erlin said.

It's not entirely diabolical. Those employing such mischief aren't out to make money but to prove a point. Hackers and digital renegades want to show security specialists that they remain one step ahead of them.

"If you're going after the guys who defend the network, it's like 'Ha! Ha! Ha!'" said Wyler, noting the satisfaction that hackers feel at one-upping those who should know better.

In an article on "How to stay safe at Black Hat," which was offered to attendees, Wyler emphasized the extent to which hackers might go to infect computers at the conference.

"Every year, we have people dropping random USB drives around the conference floor," Wyler wrote, referring to portable flash drives. "At Black Hat 2015 someone was literally throwing USB drives into open classroom doors. It's not just a story, it happens. So if you see a drive on the ground, pick it up and put it in the nearest trash can."

The flash drives invariably contain malicious coding, he said.

Underlying many of the talks at the Black Hat convention is concern about an explosion in cybercrime, ranging from the Bitcoin-hungry individual who encrypts a victim's computer and then demands a ransom payment in order to restore access to the major cyber gang that steals credit card information in order to commit massive fraud.

"To become a cybercriminal today, you don't have to have any skills. You don't have to be a hacker," said Eyal Benishti, founder and chief executive of Ironscales, an Israeli security company. With barely $300, one can buy software to launch a phishing scam, luring unsuspecting email recipients into clicking on links to open doors into their hard drives, potentially revealing banking information. "If you send enough phishing attempts, someone will click."

Despite recent attention to the hacking of the Democratic National Committee, which saw the theft of more than 19,000 emails, the public is hardly conscious of the extent of malware floating around the internet.

"I would say the public is aware of 5 percent," said Christopher Pogue, chief information security officer at Nuix, an Australian software company that's involved in cybersecurity and digital investigation.

"Ninety-five percent is either unreported, underreported or part of a criminal investigation, so it can't be disclosed," Pogue said. "Lots of people are hacked and have no idea."

Digital breaches at companies are on average not detected for 200 to 300 days, Pogue said, giving cyber criminals plenty of time to search for proprietary information. Whoever hacked into the DNC is thought to have had access to the system for nearly a year.

In a keynote speech at Black Hat, renowned security expert Dan Kaminsky warned that the internet could become overwhelmed by viruses and malicious software unless a major global effort is made to increase security.

"We're risking losing this engine of beauty," Kaminsky said. "We could lose the internet, you know? ... It's not a rule of the universe that we get to have all this fun."

Citation: How to avoid hacking? Read this story, then turn off your computer (2016, August 8) retrieved 26 June 2024 from https://phys.org/news/2016-08-hacking-story.html