PHYS.ORG

IT firm baits hackers with online model train set

March 17 2015, by Frank Zeller

Internet security experts have set up Project Honey Train with an online railway control system as bait, hoping to get inside the heads of cyber criminals

Somewhere on Earth a computer hacker types a malicious command and hits enter. Half a world away, an urban commuter train speeds out of control, derails and crashes into a building.

Happily the kind of scenario that makes for Hollywood blockbusters and keeps public security officials awake at night would, in this case, only damage a model train set at a German IT industry fair.

Internet security experts have set up "Project Honey Train" with an online railway control system as bait, hoping to "get inside the heads of cyber criminals"—but without the real-life casualties.

"The goal is to provide an environment where we can study how people may try to attack public infrastructure projects where they could put public safety at risk," said Chester Wisniewski of security company Sophos.

"I suspect that this is a pretty good copy of some of the worst of public security that we see in real life... systems that were designed in a simpler time when people weren't trying to attack them, which is what makes them vulnerable."

Their miniature rail system at the CeBIT IT business fair in Hanover is built on a scale of 1:87 and set in a fictitious German city, with street names chosen from the board game Monopoly.

To an online attacker it's all meant to look real, with original software components and inbuilt vulnerabilities which are advertised in known hackers' chatrooms.

Critical infrastructure

Online users have long been exposed to risks from ID theft, "phishing" and scams by mafia groups, to mass data collection by social media giants and snooping by secret services.

But some fear we haven't seen the worst of it yet, in an age when urban transport systems, chemical plants and power stations are considered potentially vulnerable to digital sabotage.

"I'm surprised that not more has happened already," said Christoph Meinel, head of German IT university the Hasso Plattner Institute.

"It's urgently necessary to do something about this. Some say 'don't worry, it won't happen', but that's the wrong approach. Once someone has done it successfully, you can quickly expect to see copycats."

Security experts have warned of vulnerabilities in the systems that run, for example, factories, oil pipelines and water networks—the so-called supervisory control and data acquisition or SCADA systems.

A real-life example is the computer worm Stuxnet, which was used to clandestinely attack Iran's nuclear programme in 2010 by ordering centrifuges to speed up and spin out of control until they ripped apart.

In his 2012 best-selling novel "Blackout", journalist Mark Elsberg describes how hackers attack European power grids, sparking the collapse of transport, communication and food distribution and even triggering a nuclear reactor meltdown.

Marco di Filippo of Sophos said he considers the book's premise and technical explanations "very valid".

"The greatest vulnerability is that automation now speaks TCP/IP and has ended up online, unprotected," he said, referring to the communication standard Transmission Control Protocol/Internet Protocol.

"This includes everything, be it power grids, power stations, wind farms, dams but also traffic management systems."

'Bad guys'

Andrey Nikishin, head of future technologies at Moscow-based software security group Kaspersky Lab, agreed there were theoretical risks but said a successful attack was difficult.

"If something is connected to the Internet it is theoretically possible to hack it," he said.

But he stressed that governments are aware of risks to critical national infrastructure, take steps to protect it and that many systems have a manual backup.

"And you can't hack the manual switch, fortunately," he said.

Kaspersky Lab has identified four main types of attackers—teenager hackers showing off, cyber criminals out for money, extremists seeking to sabotage, and state actors whose main goal is espionage.

While operating on the same technical basis, the big difference is the resources they have to hand, Nikishin said.

He added that potential threats would multiply in the era of the "Internet of Things", when not just PCs, laptops and phones but also houses, cars and appliances have IP addresses.

"The world is changing," he said, predicting however that one thing would stay the same—"The actor, the bad guy... they have existed, they do exist, and they will exist."

Citation: IT firm baits hackers with online model train set (2015, March 17) retrieved 28 April 2024 from https://phys.org/news/2015-03-firm-baits-hackers-online.html