India Telecom News

News and Information on Telecom and wireless in India

http://indiatelecomnews.com/can-ai-solve-the-internet-cybersecurity-epidemic/

Can AI Solve The Internet Cybersecurity Epidemic?

01/06/18

June 1, 2018

Robert Kierstead, Special Agent In Charge , Seattle Field District, U.S. Secret Service

Robert Kierstead, Special Agent In Charge, Seattle Field District, US Secret Service discussed about the Secret Service's mission – who it protects, and today's focus on cybersecurity.

This helped find credit card hacker Roman Seleznev, who was responsible for $170m worth of losses. He was caught in the Maldives even though there wasn't an extradition treaty, and was sentenced to 27 years' imprisonment.

Robert said: "We have an electronic crimes special agent program, or ECSAP. We have a network intrusion program, and we also have a critical systems protection program which is part of our protective suite of services. So, when we conduct an advance for a VIP, for the President, the Vice President, we will actually go and look at HVAC, IT and other types of information technology assets in a site, and so we provide protection for not only the physical protection of those – of our protectees, as we call them, but we will also secure the IT space in which they operate."

"Just a quick overview of our Roman Seleznev Track 2 case. Roman was a Russian national. He was a prolific credit card hacker. He would typically install malware on retailers such as pizza parlours and different types of restaurants and retailers, he'd exfiltrate that information, the Track 2 information off a credit card, he'd put it on a carding website and usually the US consumer, the US criminal or US criminal enterprises would purchase it. Roman actually had a testing service so you could see if the card was still vulnerable or not, and his crimes were responsible for actual losses of $170 million."

Greg Martin, CEO and Co-Founder, JASK said that there were not enough security people in the enterprise to protect against hackers, which is why we need AI to fill the gap – it can help them do 10 times more.

He said: " if we do not develop artificial intelligence to start to accelerate identifying, automating, helping the analysts that we do have to deal with these cyberthreats, we're going to continually fall behind. We're going to have bigger breaches, more destructive breaches, and events like we saw here in the US with companies like Equifax which was simply a matter of not having the appropriate amount of resources to be able to keep up with the threats that they see."

Slavik Markovich, Chief Executive Officer, Demisto said that there was a need to automate and standardise security alerts and responses.

Following a question about how AI helps with security Markovich said that AI doesn't solve everything but we help security analysts be more productive. Kumud Kalia said that the aim of using AI is attack prevention not response. Greg FitzGerald said that his company automates the human tasks to help them find the bad needle in a stack of needles.

Markovich warned that hackers will start using AI to invade enterprises, and Martin said that we are in a cyber-weapon arms race, although some government energies are being used to develop these, an example of which is Stuxnet.

He said that all-day low-and-slow attacks are very hard to detect and then a lot of them are detected almost by chance due to a mistake of the attacker that happens.

Kumud Kalia, Chief Information Officer, Cylance said: "I think what we're seeing is maybe a little bit more sophistication, but the attack vectors are primarily the same ones that have been exploited for a long time. So, I think for companies that have their defences in good shape, they're not really susceptible to these attacks. Now, of course, the attack surface in a company just continues to expand and so it becomes ever more difficult to be that organised and disciplined to keep everything up to date and keep all the doors locked that should be."

He added: "It's relatively easy now for the bad guys to find out, even in companies that should be impregnable, to find the weak link in their armour. I think those are the things that then get exploited and not get noticed using low-and-slow kind of techniques. Sometimes, it's multiple exploits put together and so even if you detect one, you might not think to look in the other place. Sometimes, one attack will be used to overwhelm some resources to hide another stealthier attack underneath. So, I think those are just more sophisticated tactics that are being used by more intelligent attackers, but the techniques themselves are actually well known and documented and exploited for years."
(NetEvents)

This entry was posted on June 1, 2018 at 9:00 pm and is filed under Government, Security. You can follow any responses to this entry through the RSS 2.0 feed.