TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

U.S. indicts 'prolific Swiss hacker' of government and corporate computers

A grand jury in Washington state's Western District has indicted an alleged Swiss hacker for conspiracy, wire fraud, and aggravated identity theft. The alleged cybercriminal is a 21-year-old "prolific hacker" Till Kottmann (aka "deletescape" and "tillie crimew"), who calls Lucerne his home.

The indictment alleges that Kottmann, along with a network of conspirators, hacked over 100 entities in governmental and corporate sectors. The indictment says that once Kottmann gained access, he and co-conspirators posted a treasure trove of private data on the Internet.

Continued on next page...

April 2021

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

"In February 2020, KOTTMANN illegally accessed computers belonging to a security device manufacturer located in the Western District of Washington and stole proprietary data. Likewise, in April 2020, KOTTMANN victimized the manufacturer of tactical equipment. In the latter instance, KOTTMANN improperly used the credentials of an employee to access illegally the manufacturer's source code databases. In August, KOTTMANN hacked a Washington state agency and a U.S. government contractor and stole source code related to various web applications. And, more recently, in January 2021, KOTTMANN similarly conducted cyberattacks on an automobile manufacturer and a financial investment company. KOTTMANN published data stolen through these hacks, among many others, on KOTTMANN's website and used social media to promote the hacking activity and the theft and release of proprietary information."

Swiss police executed search warrants in mid-March once enough probable cause was given that Kottman was the hacker. Following the evidence found in these searches, the indictment occurred soon after.

The case is being primarily prosecuted by Assistant United States Attorneys Steven Masada and Jehiel Baer with additional aid from Swiss legal experts (in particular Canton of Luzerne Police, the Canton of Luzerne Prosecutor's Office, and the Swiss Federal Office of Justice). Investigations are being carried out by the Seattle division of the FBI's Cyber Task Force. Assuming that the maximum sentence is carried out on each separate charge, the time that the Swiss national could face in prison is 27 years.—*Peter King for Techgenix*

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

PHISHING EMAIL LEADS TO DATA BREACH AT CALIF. STATE CONTROLLER'S OFFICE

The California State Controller's Office experienced a data breach on March 20. This was made public via a news alert shared by the office. According to the alert, the breach was caused by an employee responding to a phishing email. The employee in question was a part of the California State Controller's Office (SCO) Unclaimed Property Division and clicked a malicious link within the phishing email, subsequently entering their ID and password. As one might guess, threat actors were able to gain privileged access to the State Controller's network and subsequent databases as a result.

The hacker had access to the system from March 18 to March 19. According to the news update, the attacker gained access to "personal identifying information contained in Unclaimed Property Holder Reports" and also "sent potentially malicious emails to some of the SCO employee's contacts."

Continued on next page...

Following the breach, the access was removed and an investigation was launched. The State Controller's Office immediately sent out messages to any potential targets instructing them to delete any suspicious emails and monitor accounts. In the news alert, links to the three credit bureaus (Experian, TransUnion, and Equifax) were given. The SCO states that all affected by the breach should contact the agencies in question and place fraud alerts on accounts.

While this breach could have been worse considering the data handled by the SCO (such as payroll and state accounting), it is a lesson in basic security protocols. Every governmental agency, corporation, and any other potential target should invest in training employees on how to be defensive against cyberattacks. Time and time again, we hear of data breaches and other incidents caused by lapses in judgment. This is what cybercriminals count on, and until everyone is properly informed on how to recognize their tactics, these incidents will continue to occur.

You can have the best physical and network defenses money can buy, yet human error can render all of it useless. Education on information security is a vital component of any cyber-defense strategy.—*Derek Kortepeter for Techgenix*

Client Spotlight

Since establishing in 1985, South Australian owned Antelco has leapt ahead with its continuing focus on providing high quality, low volume, micro irrigation products to meet the global need for efficient water distribution.

To keep up with growing demand, Antelco Corporation was established in 1989 in Florida USA and serves the North American, Canadian and Mexican markets. More recently, Antelco UK Limited was established in Bedfordshire UK, to better meet the needs of the UK and European markets.

The success of Antelco is due to the experienced, dedicated staff that includes the Research and Development team. Experienced engineers and product developers, with a wealth of knowledge on plastics materials and the tooling and manufacturing process, create quality and cost effective micro irrigation products. The products undergo rigorous field testing so that any faults or imperfections can be designed out, resulting in a fault-free, quality product worthy of the Antelco name.

SIERRA WIRELESS HIT BY RANSOMWARE ATTACK, OPERATIONS DISRUPTED

A major multinational IoT communication services company has suffered a major ransomware attack. British Columbia-based Sierra Wireless, known for products that span over 550 patents, announced the attack via Berkshire Hathaway's Business Wire as the incident took down their website.

According to Sierra Wireless's press release, the ransomware infected its internal IT systems on March 20. Once the attack was discovered, the company immediately began implementing countermeasures in accordance with its cybersecurity policy. They also brought in third-party experts, and according to them, the attack has been successfully stopped.

Continued on next page...

The aftershocks of the ransomware attack can be found as described in the following press release excerpt from Sierra Wireless:

"*At this time, Sierra Wireless believes the impact of the attack was limited to Sierra Wireless systems, as the company maintains a clear separation between its internal IT systems and customer-facing products and services. As a result of the ransomware attack, Sierra Wireless halted production at its manufacturing sites. The company's website and other internal operations have also been disrupted by the attack. The company believes it will restart production at these facilities and resume normal operations soon. In the meantime, Sierra Wireless asks its customers and partners for their patience as it seeks to remediate the situation.*"

At the time of this article's publishing, it is not known publicly who the attackers were or what they wanted. It is also unknown, likely due to the ongoing investigation, what strain of ransomware was responsible for the infection and how the ransomware found a point of infection. Sierra Wireless is staying tight-lipped outside of the press release when it comes to media inquiries. It appears this ransomware attack will exact a significant monetary toll on Sierra Wireless's bottom line.

As part of the press release, Sierra said, "Due to these disruptions, Sierra Wireless is at this time withdrawing the First Quarter 2021 guidance it provided on February 23, 2021." When Threatpost's Lindsey O'Donnell contacted the company for further comment for her report on the ransomware incident, Sierra Wireless declined to elaborate beyond what was already shared.

Updates on this story will be shared if and when they are available.—*Derek Kortepeter for Techgenix*