US Arrests Chinese Man Involved With Sakula Malware Used in OPM and Anthem Hacks

bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/

Catalin Cimpanu

By
Catalin Cimpanu

- August 26, 2017
- 01:00 AM
- 0

The FBI has arrested a Chinese national on accusations of distributing and infecting US companies with the Sakula malware, the same malware used in the OPM and Anthem hacks.

The suspect's name is Yu Pingan, 26, of Shanghai. US authorities arrested Yu on Monday, August 21, at the Los Angeles airport, as the suspect entered the US to attend a security conference.

Yu alleged criminal past tied to Sakula trojan

According to an official indictment, authorities accused Yu and two other unnamed co-conspirators of infecting four US companies with Sakula, a backdoor trojan.

The US Department of Justice described Yu as a "malware broker" and charged him with the tool's distribution and four hacking charges. US authorities did not accuse Yu of creating Sakula, nor hacking OPM or Anthem.

Between 2014 and 2015, hackers stole the personal records of over 21 million government employees from the US Office of Personnel Management (OPM), and over 80 million medical records from Anthem Inc., a US company that provides health insurance, including for several government agencies.

Yu accused of using three zero-days, knowing of a fourth

US cyber-security firms have accused Chinese state hackers of carrying out the OPM and Anthem breaches. They blamed a cyber-espionage unit named Deep Panda — also known as APT19.

US authorities did not elaborate on Yu's connection to Deep Panda. Nonetheless, the indictment mentioned that Yu and his co-conspirators were in the possession of at least four zero-days — CVE-2014-0322 (affecting IE10), CVE-2012-4969 (affecting IE6), CVE-2012-4792 (affecting IE6), and an unidentified Flash Player zero-day that Yu mentioned in chat transcripts.

The hacks for which Yu stands accused all took place before the OPM and Anthem breaches. Historically, security firms have observed the Sakula trojan used in nation-state cyber-espionage campaigns exclusively.

Yu will be arraigned in court next week.

On a side note, the video below gives a basic introduction into nation-state cyber-espionage campaigns. At 27:55, security expert The Grugq provides a very simple explanation of why Chinese hackers targeted OPM and Anthem. The rest of the video also explains how the Chinese cyber apparatus works, along with similar infrastructures in Russia and the US.

Watch Video At:

https://youtu.be/wP2J9aYM6Oo

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Chinese ‘Space Pirates’ are hacking Russian aerospace firms

Google: Chinese state hackers keep targeting Russian govt agencies

Cyberspies use IP cameras to deploy backdoors, steal Exchange emails

US and allies warn of Russian hacking threat to critical infrastructure

- APT
- Arrest
- China
- Cyber-espionage
- Data Breach
- Hack
- USA

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: