Only now we known that International Civil Aviation Organization (ICAO) was hacked in 2016

March 1, 2019 By Pierluigi Paganini

Canadian media revealed that in November 2016, the International Civil Aviation Organization (ICAO) was a hit by a large-scale cyberattack.

"The analyst at Lockheed Martin emphasized that this attack could represent a "significant threat to the aviation industry.""

Cyber security experts believe the attack was carried out by the China-linked APT group LuckyMouse (aka Emissary Panda, APT27 and Threat Group 3390, and Bronze Union).

The ICAO organization hired an external analyst to help it to evaluate the extent of the attack. According to an investigation conducted by Secureworks hackers were also able to access the hackers were also able to compromise the mail servers to obtain access to admin accounts.

"Mail server, domain administrator and system administrator accounts were all affected, giving cyberespions access to the past and current passwords of more than 2,000 ICAO system users. Hackers could read, send or delete emails from any user." reports Radio-Canada.

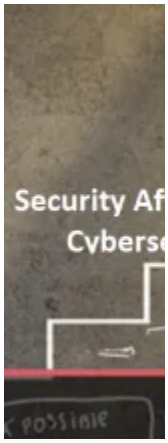
"The spies also had access to the personal records of past and present employees, the medical records of those who had used the ICAO clinic, financial transaction records and personal information of anyone who had visited the ICAO building or was registered on the website."

In the weeks following the attack, the e-mail account of an ICAO delegate was also hacked and used to send out messages, but at the time it is not clear if both incidents are linked.

According to Radio Canada, ICAO tried to hide a cyberattack with important consequences in the incident response.

Documents cited by Radio Canada reveal that four members of the ICAO information and communication technology (ICT) team attempted to conceal evidence of their own incompetence.

SecurityAffa
Cybersecurit
Cybersecurit



Center for C
Relations Stu

Center f
Internati

According to ESET experts Matthieu Faou, the Chinese LuckyMouse APT group specializes in watering hole attacks. The hackers scan the Internet for vulnerable servers that could lead to compromising valuable targets.

"In addition to using generic tools relatively accessible on the Web, the group has developed tools of its own, including a rootkit. Last year, they stole a digital certificate belonging to a legitimate company, used to sign its rootkit." explained Faou.

Why ICAO?

According to José Fernandez, cybersecurity expert and professor at Polytechnique Montréal, "ICAO is a natural choice", for the purpose of cyber-espionage, a type of campaign with which LuckyMouse is often associated. "The agency thus becoming a one-stop shop for the hacking of all other players in the aerospace industry."

Anthony Philbin, ICAO's chief of communications, attempted to reassure the community following the disclosure of the attack that has happened in 2016.

"Decisions made by ICAO regarding the 2016 incident you've referenced were based on forensic evidence provided by two independent expert bodies," Philbin said.

"I'm sure you'll understand that it wouldn't be prudent for me to discuss more specific details with media on matters relating to ICAO security measures, cyber or otherwise."
"ICAO maintains no type of financial or other private information which could possibly pose risks to individual Canadians."

"We are not aware of the serious cyber security consequences for the external partners that would have resulted from this incident …", adding that since the attack, "ICAO has made significant improvements to its cybersecurity framework and approaches to mitigate other incidents."

Pierluigi Paganini

(SecurityAffairs – APT, hacking)

APT | China | cyber espionage | ICAO | LuckyMouse | Pierluigi Paganini

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Analyzing the evolution of MageCart cybercrime groups' TTPs

NEXT ARTICLE

Cybaze-Yoroi ZLab analyze GoBrut: A new GoLang Botnet

YOU MIGHT ALSO LIKE

November 23, 2020 By Pierluigi Paganini