Researchers claim China trying to hack South Korea missile defense efforts

arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/

Sean Gallagher

Enlarge / South Korea is deploying Lockheed Martin's THAAD missile defense system, and that's sparked the ire of the Chinese government, as well as military and "hacktivist" hacking groups, according to FireEye.

US Army

Chinese government officials have been very vocal in their opposition to the deployment of the Terminal High-Altitude Air Defense (THAAD) system in South Korea, raising concerns that the anti-ballistic missile system's sensitive radar sensors could be used for espionage. And according to researchers at the information security firm FireEye, Chinese hackers have transformed objection to action by targeting South Korean military, government, and defense industry networks with an increasing number of cyberattacks. Those attacks included a denial of service attack against the website of South Korea's Ministry of Foreign Affairs, which the South Korean government says originated from China.

FireEye's director of cyber-espionage analysis John Hultquist told the *Wall Street Journal* that FireEye had detected a surge in attacks against South Korean targets from China since February, when South Korea announced it would deploy THAAD in response to North Korean missile tests. The espionage attempts have focused on organizations associated with the THAAD deployment. They have included "spear-phishing" e-mails

carrying attachments loaded with malware along with "watering hole" attacks that put exploit code to download malware onto websites frequented by military, government, and defense industry officials.

FireEye claims to have found evidence that the attacks were staged by two groups connected to the Chinese military. One, dubbed Tonto Team by FireEye, operates from the same region of China as previous North Korean hacking operations. The other is known among threat researchers as APT10, or "Stone Panda"—the same group believed to be behind recent espionage efforts against US companies lobbying the Trump administration on global trade. These groups have also been joined in attacks by two "patriotic hacking" groups not directly tied to the Chinese government, Hultquist told the *Journal*—including one calling itself "Denounce Lotte Group" targeting the South Korean conglomerate Lotte. Lotte made the THAAD deployment possible through a land swap with the South Korean government.