APT: IN ACTION FOR SIX YEARS

AUG 5, 2014 | RESEARCH

The "Pitty Tiger" advanced persistent threat (APT) group may have been active for over six years, researchers said.

The activities of the Pitty Tiger group first came to light in mid-July by the cybersecurity unit at Airbus Defense & Space. Airbus researchers determined the attackers, which they believe operate out of China have been active since at least 2011. However, researchers at FireEye found more evidence suggesting they have been targeting organizations for much longer.

RELATED STORIES
IoT Devices Vulnerable to Attacks: Report
Spam Indicates Security Vulnerabilities
Organizations 'More Vulnerable Than They Think'
Endpoints Need More Security: Report

FireEye said the group uses spear phishing emails, social engineering, email phishing pages, malware and other tools to accomplish their goals. The spear phishing emails analyzed by FireEye were in French, English and Chinese.

In one attack against a French company, the attackers sent out emails written in English and French that appeared to come from someone within the targeted organization. The malicious messages carried harmless-looking Microsoft Word documents that were set up to drop a first-stage payload, Backdoor.APT.Pgift (Troj/ReRol.A), by exploiting both old (CVE-2012-0158) and new (CVE-2014-1761) vulnerabilities affecting the Microsoft Office suite.

Once it infects a computer, the Trojan sends some information on the compromised device back to its command and control (C&C) server, after which it downloads the second-stage malware.

This wasn't the first time researchers identified an attack using Backdoor.APT.Pgift. They found the same threat at the beginning of this year in a campaign targeting an organization in Taiwan. This and the idea quite a few of the C&C servers used by the cybercriminals are on .tw domains, indicates the attackers have an interest in Taiwan, FireEye researchers said.

The threat group has been using several pieces of malware over the past years. Based on samples that connected to the domain names used in their operations, FireEye said the attackers relied on PoisonIvy during 2008 and 2009.

Backdoor.APT.PittyTiger1.3 (CT RAT) has also seen use, most likely as a second-stage malware since it provides attackers with a remote shell on the compromised system.

Backdoor.APT.PittyTiger is a piece of malware leveraged by the group in 2012 and 2013. The threat is capable of capturing screenshots, uploading and downloading files, and providing a remote shell. Backdoor.APT.Lurid, and variants of Gh0st RAT, including Paladin RAT and Leo RAT, have also seen action by the Pitty Tiger group, FireEye researchers said.

Click here for more information on the APT.

Submit a Comment

Your email address will not be published. Required fields are marked *

SUBMIT COMMENT