'Operation Tropic Trooper' Hits Targets in Taiwan, Philippines: Trend Micro

By Brian Prince on May 14, 2015

A three-year-old cyber operation is using a mix of social engineering, Microsoft Windows vulnerabilities and basic stenography to target government, military and industry officials in Taiwan and the Philippines, according to Trend Micro.

In a new report, the security firm revealed the ongoing attacks - which it dubbed 'Operation Tropic Trooper' - go back to 2012, but the malware the attackers are using shares traits with samples Trend Micro first examined in 2011. Between March and May of this year, 62 percent of the malware infections have targeted Taiwanese organizations, while the remaining 38 percent have hit entities in the Philippines. In Taiwan, the targets have included government ministries and heavy industries, while the targets in the Philippines have been in the military.

While Trend Micro did not identify the actors behind the attacks, researchers were able to pinpoint command and control servers in four countries: Taiwan (home to 43 percent of the servers), Hong Kong (14 percent), U.S. (36 percent) and the United Arab Emirates (seven percent).

"This latest attack relied on two of the most-exploited Windows vulnerabilities to date—CVE-2010-3333 and CVE-2012-0158—to infiltrate the target networks," **blogged** Kervin Alintanahin, threats analyst at Trend Micro. "This suggests that the organizations were running on unpatched, vulnerable systems that made them more susceptible to threats."

"Aside from exploiting those vulnerabilities, the threat actors used basic steganography," the researcher continued. "This means they were able to conceal malicious code in JPEG files popularly used as Windows XP wallpapers. Steganography, although not a new cybercriminal tactic, is not commonly used in targeted attacks."

The attackers may have chosen this approach because of the continued **use of XP systems** in Taiwan and the Philippines despite the operating system having reached its end-of-life, Alintanahin noted. There is also a chance the threat actors have used steganography because they either still use Windows XP themselves or have in-depth knowledge of it, the researchers added.

The attack starts with emails laced with a malicious attachment. Opening the documents leads to the execution of malware that downloads an image file to the system, according to Trend Micro.

"Closer inspection of the downloaded image file reveals that it uses steganography to hide the malicious content," the researcher explained. "It will decrypt executable files in memory and will not save it to the disks. These files are installers and will drop the backdoor BKDR_YAHAMAM. With the backdoor's capabilities of downloading, uploading, and creating a remote shell, it can easily conduct the next phase of its attack which is to find other targets within its reach."

"Operation Tropic Trooper is not highly sophisticated," Alintanahin noted. "But the fact that it has attained some degree of success and has managed to infiltrate crucial organizations in both Taiwan and the Philippines shows the urgent need for targeted entities to rectify their shortcomings in terms of security. Knowing that attackers are still using old techniques and exploiting known vulnerabilities will make it easier for the targeted organizations to pinpoint and fix security gaps in their networks."

The Trend Micro report can be **read here.**

Share | Tweet | Recommend 13 | RSS

Brian Prince is a Contributing Writer for SecurityWeek.

Previous Columns by Brian Prince:

- U.S. Healthcare Companies Hardest Hit by 'Stegoloader' Malware
- CryptoWall Ransomware Cost Victims More Than $18 Million Since April 2014: FBI
- New Adobe Flash Player Flaw Shares Similarities With Previous Vulnerability: Trend Micro
- Visibility Challenges Industrial Control System Security: Survey
- Adobe Flash Player Zero-Day Exploited in Attack Campaign

Tags: NEWS & INDUSTRY Virus & Malware

Most Recent | Most Read

- Cisco Patches Several Vulnerabilities in SD-WAN Solution
- Researchers Track Coronavirus-Themed Cyberattacks
- Analyzing Cyberspace Solarium Commission's Blueprint for a Cybersecure Nation
- Sixgill Introduces Dark Web Data Feed Product
- Adobe Patches Critical Flaws in Reader, ColdFusion, Other Products
- VMware Fixes Privilege Escalation Vulnerability in Fusion for Mac
- The Human Element and Beyond: Why Static Passwords Aren't Enough
- Ransomware Is Mostly Deployed After Hours: Report
- The Other Virus Threat: Surge in COVID-Themed Cyberattacks
- Barr: FBI Probing If Foreign Gov't Behind HHS Cyber Incident