SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

China Cybergang Using Hacking Team Exploits Against Financial Firm

By Eduard Kovacs on August 19, 2015

Share Tweet Recommend 15 RSS

Emissary Panda Using Hacking Team Exploits to Deliver RAT

The Chinese advanced persistent threat (APT) group known as Emissary Panda and Threat Group 3390 has been using Hacking Team's Flash Player exploits in its operations.

According to Zscaler, the group leveraged the CVE-2015-5119 vulnerability to target a major financial services firm. While it has not been named, Zscaler told *SecurityWeek* that the targeted organization is a multi-national financial services firm with locations across Europe, Middle East and Asia.

"The main motive of this group is to monitor and exfiltrate intellectual property data from the target organization," Zscaler researchers explained in a blog post.

The attack targeting the financial services firm started with a spear phishing message containing a malicious URL. The link pointed to a server in Hong Kong set up to host the Hacking Team Flash Player exploit. The attackers attempted to use the exploit to install a variant of the HttpBrowser remote access Trojan (RAT) hosted on the same Hong Kong-based server, which has also been used for command and control (C&C).

HttpBrowser RAT, a piece of malware that is highly popular among APT groups, leverages a legitimate digitally signed executable from Symantec to decrypt and run the RAT payload without being detected.

The financial services firm targeted by the cyber espionage group is a Zscaler customer and the security company said it blocked the attack before any damage was caused.

Zscaler told *SecurityWeek* that Emissary Panda has also leveraged another Hacking Team Flash Player exploit (CVE-2015-5123) in its operations. According to the company, the attack on the financial services firm was not an isolated incident -- Zscaler plans on releasing additional research in the upcoming days.

Several exploits were leaked online after the Italian surveillance software company Hacking Team suffered a data breach, and Emissary Panda is not the only APT actor to use the spyware maker's exploits.

The Chinese group known as Wekby (APT 18) has also used at least one of the exploits to deliver Gh0st RAT. Cyber espionage groups such as Pawn Storm, APT3 and Darkhotel have also leveraged Hacking Team's exploits in their campaigns.

A report published earlier this month by Dell's SecureWorks Counter Threat Unit revealed that Emissary Panda has become more selective when it comes to data exfiltration.

The group has targeted a wide range of companies over the past years, including automobile, electronics, aircraft, pharmaceutical, and oil and gas manufacturers. Up until recently, the threat actor stole all the information it could find on compromised networks, but now it has changed its tactics and only takes what it believes to be more valuable.

Share Tweet Recommend 15 RSS

Eduard Kovacs (**@EduardKovacs**) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

- » Cisco Patches Several Vulnerabilities in SD-WAN Solution
- » VMware Fixes Privilege Escalation Vulnerability in Fusion for Mac
- » Trend Micro Patches Two Vulnerabilities Exploited in the Wild
- » Financial Services Firms Exposed 500,000 Sensitive Documents
- » Private Application Access Firm Axis Security Emerges From Stealth

Tags: NEWS & INDUSTRY Virus & Threats

Google™ Custom Search Search

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

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- ICS Cyber Security Conference
- CISO Forum, Presented by Intel
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media