Vietnamese Spies Rival Notorious Russian Group in Sophistication

By Eduard Kovacs on November 07, 2017

Share Tweet RSS

The campaigns of a cyber espionage group believed to be operating out of Vietnam have become increasingly sophisticated, up to the point where they rival operations launched by the notorious Russia-linked advanced persistent threat (APT) actor known as Turla, incident response firm Volexity said on Monday.

The group, tracked as OceanLotus and APT32, has been around since at least 2012, targeting various types of organizations in Southeast Asian countries such as Vietnam, Philippines and China, with some campaigns extending to Europe and the United States. The list of targeted entities includes governments, journalists, activists, tech firms, consumer product manufacturers, banks, and organizations in the hospitality sector.

OceanLotus has used both Windows and Mac malware in its operations, along with some clever techniques that have allowed the group to evade detection.

Volexity has been tracking the threat actor since May 2017, specifically attacks aimed at the Association of Southeast Asian Nations (ASEAN), and media, human rights, and civil society organizations. The security firm agrees with FireEye's previous assessment that OceanLotus is likely based in Vietnam.

"Volexity believes the size and scale of this attack campaign have only previously been rivaled by a Russian APT group commonly referred to as Turla," the security firm said in a blog post.

Volexity's analysis showed that OceanLotus's watering hole attacks involved more than 100 compromised websites belonging to government, military, media, civil society, human rights and oil exploitation entities.

Researchers determined that the group's attacks are highly targeted; the compromised sites served malicious code only to visitors who were on a whitelist. Targeted users are shown a fake screen designed to trick them into authorizing a malicious Google app that could access the victim's emails and contacts. Some of the compromised websites were also set up to deliver backdoors and other types of tools, including legitimate software (e.g. Cobalt Strike) and custom malware.

Researchers also noticed that the attackers created many fake domains designed to mimic legitimate services such as AddThis, Akamai, Baidu, Cloudflare, Disqus, Facebook and Google. Many of these websites leveraged SSL certificates provided by Let's Encrypt, whose services have been increasingly abused by cybercriminals.

"Volexity believes the OceanLotus threat group has rapidly advanced its capabilities and is now one of the more sophisticated APT actors currently in operation," the company concluded.

OceanLotus' sophistication was also described recently in a report from Cybereason, which detailed the group's cat-and-mouse games within the systems of a global company operating in Asia.

Related: Vietnam's Tien Phong Bank Victim of SWIFT-based Attack

Related: Second SWIFT Attack Hits Vietnam Bank Showing Links to Sony Hack

Share Tweet 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:
» VMware Patches Vulnerabilities Reported by Researchers to Chinese Government
» Moxa MXview Vulnerabilities Expose Industrial Networks to Attacks
» Over 28,000 Vulnerabilities Disclosed in 2021: Report
» Sophisticated FritzFrog P2P Botnet Returns After Long Break
» Adobe Releases Emergency Patch for Exploited Commerce Zero-Day

Tags: Cyberwarfare NEWS & INDUSTRY Virus & Threats Malware

Google™ Custom Search Search

GET THE DAILY BRIEFING
BRIEFING
Business Email Address SUBSCRIBE

Most Recent Most Read
» Researchers Dissect Activity of Cybercrime Group Targeting Aviation, Other Sectors
» VMware Patches Vulnerabilities Reported by Researchers to Chinese Government
» QNAP Extends Security Updates for Some EOL Devices
» FBI Warns of BlackByte Ransomware Attacks on Critical Infrastructure
» Moxa MXview Vulnerabilities Expose Industrial Networks to Attacks
» Google Discovers Attack Exploiting Chrome Zero-Day Vulnerability
» 'Don't Be Google': The Rise of Privacy Focused Startups
» Webinar Today: Meet the Inventors of Onion Routing
» Legit Security Raises $30M to Tackle Supply Chain Security
» Over 28,000 Vulnerabilities Disclosed in 2021: Report

Popular Topics
» Cybersecurity News
» IT Security News
» Risk Management
» Cybercrime
» Cloud Security
» Application Security
» Smart Device Security

Security Community
» Virtual Cybersecurity Events
» Webcast Library
» CISO Forum
» ICS Cyber Security Conference
» IT Security Newsletters
» InfosecIsland.Com

Stay Intouch
» Twitter
» Facebook
» LinkedIn Group
» Cyber Weapon Discussion Group
» RSS Feed
» Submit Tip
» Security Intelligence Group

About SecurityWeek
» Team
» Advertising
» Event Sponsorships
» Writing Opportunities
» Feedback
» Contact Us

Wired Business Media