SECURITYWEEK NETWORK: Information Security News | Infosec Island | CISO Forum Security Experts: WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2019 CISO Forum, Presented by Intel | ICS Cyber Security Conference | Contact

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security Strategy SCADA / ICS IoT Security

Home › Cyberwarfare

China-Linked Spies Use Recent Zero-Day to Target Financial Firms

By Eduard Kovacs on May 02, 2017

Share Tweet Recommend 16 RSS

A cyber espionage group has targeted analysts working at major financial firms using a recently patched Microsoft Office vulnerability, Proofpoint reported last week.

The threat actor, tracked by the security firm as TA459, has been active since at least 2013 and it's believed to be operating out of China. The cyberspies have been known for using malware such as NetTraveler (aka TravNet), PlugX, Saker, Netbot, DarkStRat, and ZeroT in attacks aimed at organizations in Russia and neighboring countries.

Proofpoint recently detailed a series of attacks launched by the group against military and aerospace organizations in Russia and Belarus.

On April 20, researchers spotted a campaign aimed at global financial firms operating in Russia and neighboring countries. Given that the attacks were apparently aimed at analysts covering the telecommunications industry, experts believe this latest operation is likely a continuation of a similar campaign first analyzed in the summer of 2015.

In the recent attacks, TA459 sent out spear-phishing emails containing a Word document set up to exploit a recently patched remote code execution vulnerability tracked as CVE-2017-0199. The attackers started leveraging this flaw just days after Microsoft released a fix.

When the malicious document is opened, an HTML application (HTA) file disguised as an RTF document is downloaded. PowerShell is then used to download and execute a script that fetches and runs the ZeroT downloader.

ZeroT was analyzed by Proofpoint when it investigated the recent attacks aimed at military and aerospace organizations, but some changes and improvements have been made in the latest version. One of the changes is the use of a legitimate McAfee utility for sideloading instead of a Norman Safeground utility.

While ZeroT is the threat actor's most common first stage payload, the second payload includes various pieces of malware. In recent attacks, Proofpoint noticed both PlugX and a Trojan tracked as PCrat/Gh0st, which is used less often by the group.

"Multinational organizations like the financial services firms targeted here must be acutely aware of the threats from state-sponsored actors working with sophisticated malware to compromise users and networks," Proofpoint researchers explained. "Ongoing activity from attack groups like TA459 who consistently target individuals specializing in particular areas of research and expertise further complicate an already difficult security situation for organizations dealing with more traditional malware threats, phishing campaigns, and socially engineered threats every day."

The fact that the threat actor has used CVE-2017-0199 in its operation is not surprising. The flaw had been exploited by several groups before Microsoft released a patch for it, and others, including Iranian hackers, started using it shortly after its existence came to light.

Related: China-Linked "DragonOK" Group Expands Operations

Related: Chinese Hacking Group Linked to NetTraveler Espionage Campaign

Share Tweet Recommend 16 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 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
- Users Complain About Windows Update That Patches SMBGhost Vulnerability

- 2020 Singapore ICS Cyber Security Conference | June 16-18 2020]
- 2019 CISO Forum, Presented by Intel (Ritz-Carlton, Half Moon Bay CA)
- 2020 ICS Cyber Security Conference | USA [Oct. 19-22]

sponsored links

Tags: Cyberwarfare NEWS & INDUSTRY Virus & Threats Virus & Malware

Search

SUBSCRIBE TO THE DAILY BRIEFING

BRIEFING

Business Email Address SUBSCRIBE

Most Recent Most Read

- 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
- Trend Micro Patches Two Vulnerabilities Exploited in the Wild

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

Copyright © 2020 Wired Business Media. All Rights Reserved. Privacy Policy