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 › Vulnerabilities

Microsoft Patches Office Zero-Day Bug Used by APT Group

By Eduard Kovacs on July 16, 2015

Share Tweet Recommend 22 RSS

Microsoft on Tuesday patched several memory corruption vulnerabilities in Office, including one that had been exploited in the wild by a well known advanced persistent threat (APT) actor.

Trend Micro reported earlier this week that the Russian threat group Pawn Storm (also known as APT28, Sednit, Fancy Bear, Sofacy and Tsar Team) had been leveraging an Oracle Java zero-day vulnerability in attacks against the armed forces of a NATO member country, and defense organizations in the United States and Canada.

According to iSIGHT Partners, this isn't the only zero-day bug used recently by the group. On June 30, the threat intelligence company discovered that Pawn Storm had been exploiting an unpatched vulnerability in Microsoft Office (CVE-2015-2424). iSIGHT Partners immediately notified Microsoft and the flaw was patched when the company released its July 2015 security updates.

“When we found the exploit it appeared to be under development and evidence suggests it was deployed in Georgia,” iSIGHT Partners noted in a blog post.

The Microsoft Office zero-day exploited by the threat actor is a heap corruption vulnerability triggered during processing of a malformed Microsoft Forms Image. The flaw affects Office 2013 SP1 and prior, and it can be exploited to execute arbitrary code via a specially crafted Office document.

In the Pawn Storm attack spotted by iSIGHT, the attackers used a document named “Iran_nuclear_talks.rtf” to hide the exploit. Brian Bartholomew, senior researcher in the Cyber Espionage Threat Intelligence team at iSIGHT Partners, told *SecurityWeek* that the content of the lure document was ripped from a June 28 CNN article on nuclear talks with Iran.

When the document was opened, an embedded OLE object triggered the vulnerability and a dropper payload was written and executed on the targeted system. The dropper then dropped a Sofacy malware payload.

“Based on several artifacts in the exploit document and the unreliability of successful exploitation when running the exploit document, iSIGHT Partners believes the exploit document was potentially hastily thrown together, or the exploit is still being developed to be more reliable,” iSIGHT explained.

The threat group, which the security firm calls Tsar Team, has also leveraged at least one of the zero-day exploits leaked after the Hacking Team breach.

Bartholomew told *SecurityWeek* that iSIGHT has observed Tsar Team using one of the three Adobe Flash Player exploits (CVE-2015-5119) from the Hacking Team leak.

“While this is the only one we have observed in use by this team, it is not out of the realm of possibility that they may have repurposed any of the other five released zero-days from Hacking Team,” said Bartholomew. “5119 was re-written and in use by Tsar Team within 24 hours of the exploit being released on the Internet.

In April, FireEye reported that the threat group had used Flash Player and Windows zero-days in a highly targeted attack aimed at an international government entity.

iSIGHT Partners has been monitoring the APT actor’s activities and the company believes that the group is actually behind the hacktivist group known as Cyber Caliphate, which attacked several companies apparently in support of ISIS.

Share Tweet Recommend 22 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:

- Critical Flaw in VMware Workstation, Fusion Allows Code Execution on Host From Guest
- Currency Data Provider 'Open Exchange Rates' Discloses Breach
- Out-of-Band Windows Updates Patch Wormable SMB Vulnerability
- Several Vulnerabilities Expose Phoenix Contact Industrial 4G Routers to Attacks
- Google Offering Higher Bonuses for Cloud Platform Vulnerabilities

Tags: NEWS & INDUSTRY Vulnerabilities

Google™ Custom Search Search

SUBSCRIBE TO THE DAILY BRIEFING

BRIEFING
Business Email Address SUBSCRIBE

Most Recent Most Read

- How National Security Surveillance Nabs More Than Spies
- European Authorities Dismantle Two SIM Hijacking Gangs
- US Surveillance Powers Set to Temporarily Expire
- Flaws in Popup Builder Plugin Impacted Over 100,000 WordPress Sites
- Microsoft Deprecates Remote Desktop Connection Manager
- Critical Flaw in VMware Workstation, Fusion Allows Code Execution on Host From Guest
- China-linked APT Hackers Launch Coronavirus-Themed Attacks
- U.S. Senators Seek to Ban TikTok on Government Devices
- Trump Signs Bill to Help Telecoms Replace Huawei Equipment
- House Strikes Deal to Extend Surveillance Powers

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