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

Russian Hackers Favor Windows, Office Exploits: Report

By SecurityWeek News on August 05, 2016

Share Tweet Recommend 20 RSS

Adobe's Flash Player might be the most targeted product when criminal exploit kits are involved, but Microsoft products such as Office, Windows and Internet Explorer take center stage when Russian advanced persistent threat (APT) groups are involved.

According to a new report from Recorded Future, 55% of vulnerabilities exploited by these groups are targeting versions of Office, Windows and Internet Explorer. State-sponsored actors have been focusing on widely adopted software, and only 46% of the known Russian APT exploited vulnerabilities can be also found in exploit kits used by cyber criminals.

Dubbed "*Running for Office: Russian APT Toolkits Revealed*," Recorded Future's report also reveals that there might be no connection between APT28 and APT29, two of the most active actors. The former, which is also known as Fancy Bear, Operation Pawn Storm, Sednit, and Sofacy, is associated by many with Russian military intelligence (GRU), while the latter, also called Cozy Bear, The Dukes, and Office Monkeys, is possibly associated with the Russian Federal Security Service (FSB).

Of the 33 known exploited product vulnerabilities that various Russian APTs use to steal information, 27 are tied to APT28 (22) and APT29 (5), but they don't overlap, although both were found to have compromised the Democratic National Committee (DNC) network. APT29 managed to infiltrate the network last year, while APT28 compromised it in April this year.

Alongside these two groups, the alleged Russian state-sponsored groups Energetic Bear (also known as Dragonfly, Group 24, Koala Team) and Turla (aka Snake, Ouroboros, Carbon) also regularly target Microsoft products, the report claims. The massive user bases these products enjoy make them targets of choice: Windows has over 1.5 billion users, while Office has over 1.2 billion.

In addition to Microsoft products, these groups also focus on exploiting vulnerable Adobe software, including Flash Player and Acrobat, Oracle products, such as Java, Mozilla applications, and community software. According to Recorded Future's report, only 73% of vulnerabilities targeted by Russian APTs have public exploits available on portals such as Metasploit, Exploit Database and Github.

Some of these vulnerabilities include CVE-2015-1701 and CVE-2015-3043, both associated with APT28 last year, CVE-2015-7645, patched in October by Adobe, and CVE-2015-1641, currently one of the most popular Office flaws, alongside CVE-2015-2545. CVE-2012-0158, another highly abused vulnerability in Office, is also targeted by these groups.

Although these groups are still targeting vulnerabilities discovered seven or six years ago (such as CVE-2009-1123, CVE-2010-3333, and CVE-2010-4398) in Microsoft products, they don't use flaws that have been reported this year. The only new exploit is CVE-2016-0728, used by APT28 to target Linux machines.

The attack tactics employed by these groups are similar to those used by other threat actors, such as spear-phishing, spoofed domains supporting credential phishing, social engineering and watering hole attacks. The security researchers claim that Office and Acrobat are popular targets among them because of attacks that use attachments in spear-phishing emails. Of the 33 analyzed vulnerabilities, 8 impact Office/Acrobat.

"Heavy Russian APT use of Office and Adobe PDF exploits may be in line with the more targeted nature of state-sponsored attacks. Criminal campaigns such as ransomware play a numbers game, while state-sponsored attacks focus on specific organizations and information," the report reveals.

When looking at the 22 exploits used by APT28 and the 5 employed by APT29, researchers discovered that they are different, meaning that the two groups are not connected. Previous reports also suggested that the two groups do not coordinate or share resources and infrastructure. Although both actors infiltrated DNC, they did so by unwittingly stealing the same set of credentials, researchers say.

Related: XTunnel Malware Specifically Built for DNC Hack

Related: Hacking of DNC Raises Fears of Cyber Attack on U.S. Election

Share Tweet Recommend 20 RSS

Previous Columns by SecurityWeek News:

- RSA Conference 2020: Product Announcement Summary (Day 3)
- RSA Conference 2020: Product Announcement Summary (Day 2)
- SECURITI.ai Wins RSA Conference 2020 Innovation Sandbox Contest
- RSA Conference 2020: Product Announcement Summary (Day 1)
- Encryption Firm With NSA Roots Raises $10 Million

Tags: NEWS & INDUSTRY Vulnerabilities

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