informa

InformationWeek IT NETWORK | Dark Reading | Network Computing | About Us | Advertise | Register | Login to your account | Welcome Guest

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Authors | Slideshows | Video | Tech Library | University | Radio | Calendar | Black Hat News | Follow DR:

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

tenable
STOP WASTING TIME ON VULNS THAT DON'T POSE RISK.

tenable
FIX THE REAL THREATS TO THE BUSINESS.
GET EBOOK

THREAT INTELLIGENCE

5/11/2017
01:00 PM

Jai Vijayan
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like | Tweet | Share

APT28, Turla Nation-State Groups Deployed Multiple 0Days in Recent Attacks

Attack campaigns by APT28, Turla, and an unidentified group showcase easy availability of zero-days.

Threat actors rarely ever need zero-day flaws to breach enterprise networks. But there appears to be a plentiful supply of such vulnerabilities for those who do.

A flurry of recent exploit activity targeting government, military, and banking entities mostly in Europe and the Middle East is one example.

Security vendors ESET and FireEye this week issued separate advisories on cyberattacks involving the use of three Microsoft zero-day flaws. Two of them involved the Encapsulated PostScript (EPS) function in Microsoft Office, while the third was a privilege escalation flaw in Windows.

Microsoft addressed all three issues in its monthly security update for May this week.

In its advisory, FireEye said it had seen the three flaws being exploited in attacks by an unidentified group and also by APT28 and Turla, two previously known Russian cyber espionage groups. The unknown group appeared to be motivated by financial gain and was focused mainly on regional and global banks operating in the Middle East. The APT28 and Turla attacks were likely targeted at extracting geopolitical intelligence from targets in Europe.

ADVERTISEMENT. CLICK FOR SOUND.

The attacks by Turla and the unknown group involved the use of CVE-2017-0261, a remote code execution flaw that allowed attackers to gain administrative access on vulnerable systems. The EPS vulnerability, according to Microsoft, could be exploited by getting users to open an Office file with a malformed image or by getting them to insert a malformed image into an Office file.

The APT28 group's attacks meanwhile exploited two zero-day flaws; CVE-2017-0262, a remote code execution vulnerability in EPS handling that was nearly identical to the other EPS zero-day; and CVE-2017-0263, an escalation of privilege flaw in Windows.

APT28's objective in using the two zero-day flaws was to drop Seduploader, a reconnaissance tool that the group is well known for using to steal confidential information from targets, ESET said in its blog.

"These vulnerabilities show that financially motivated actors have access to some of the most sophisticated tools that are sometimes thought to be the sole purview of nation states," says Benjamin Read, a security analyst at FireEye. "The use of multiple zero-days by Russian actors underscores the technically sophisticated threat from cyber espionage groups in that country," he says.

Marc-Etienne Leveille, malware researcher at ESET, says that since 2015, the company has observed the APT28 group use at least 12 different zero-days exploits—six in 2015, four in 2016, and two so far in 2017.

The group, which is also known as Sofacy, Fancy Bear, and Sednit, has been active for more than 10 years, so the actual number of zero-days it has used in that period is likely to be much higher. APT28 is believed to have been involved in the attacks on the Democratic National Committee (DNC) and has been cited as proof of Russian involvement in the attack. Most recently, the threat group is believed to have been behind an attempt to gain access to the email accounts of those involved in just elected French President Emmanuel Macron's campaign.

"Because of the amount of zero-days they've used in the past few years, we can assume that they either have very skilled people or enough financial resources to maintain this trend," Leveille says.

ESET does not have information on pricing in the Dark Market for zero-day flaws such as the two used by APT28 in its most recently observed campaigns. But based on prices from zero-day acquisition platform Zerodium, it is likely that the two exploits combined could cost up to $70,000. "Finding or writing new reliable zero-day exploits is not an easy task," he says.

AXONIUS
Sponsored Content
Asset Management Trends: As IT Complexity Increases, Visibility Plummets
This eBook highlights the current asset visibility challenges that IT and security teams are facing as the IT landscape becomes more complex.
Brought to you by Axonius

Related Content:

- 30% of Q4 Malware was New or Zero-Day
- 10 Free or Low-Cost Security Tools
- Dark Reading Radio: 'Bug Bounties & The Zero-Day Trade'
- What To Do When All Malware Is Zero-Day

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

INSIGHTS SPONSORED CONTENT

New 'Perimeter' Requires Fresh Security Approach, Onapsis Say
The advent of mobility, cloud, and different ways of securing business-critical apps has given rise to the idea that "The perimeter is where the data is," posits Jason Fruge, VP of business application cybersecurity for Onapsis. As a former CISO himself, he describes how this new reality impacts customers' security planning and execution.
LEARN MORE

MORE INSIGHTS

Webcasts
- Security Alert Fatigue: Tips for Taking Control
- The ROI Story: Identifying & Justifying Disruptive Technology

MORE WEBCASTS

White Papers
- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data

MORE WHITE PAPERS

Reports
- 2020 IT Salary Survey Results Revealed
- [Report] DevSecOps & Secure App Delivery: What's Working & What's Not

MORE REPORTS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

HOT TOPICS | EDITORS' CHOICE

Many Ransomware Attacks Can be Stopped Before They Begin 3
Jai Vijayan, Contributing Writer, 3/17/2020

This Tax Season, Save the Scorn and Protect Customers from Phishing Scams 2
Dr. Salvatore Stolfo, Founder & CTO, Allure Security, 3/17/2020

Fewer Vulnerabilities in Web Frameworks, but Exploits Remain Steady 1
Robert Lemos, Contributing Writer, 3/16/2020

SUBSCRIBE TO NEWSLETTERS

WEBINARS

- Building an Enterprise Strategy for Detection and Response (XDR)
- Chatbots for the Enterprise
- Security Alert Fatigue: Tips for Taking Control

WEBINAR ARCHIVES

WHITE PAPERS

- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data
- Application Security in the Cloud
- Hacker's Almanac
- Maximize the ROI of Detection and Response

MORE WHITE PAPERS

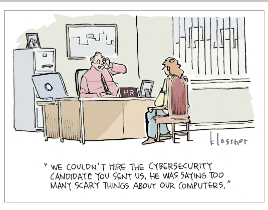
VIDEO

Ransomware Trains Its Sights on Cloud ...
6 COMMENTS

Qualys Launches Free App for IT Asset ...
1 COMMENTS

ALL VIDEOS

CARTOON



"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Latest Comment: Unfortunately nobody wants to spend money on security. Usually they change their mind but often it is too late

CARTOON ARCHIVE

CURRENT ISSUE

6 Emerging Cyber Threats That Enterprises Face in 2020

This Tech Digest gives an in-depth look at six emerging cyber threats that enterprises could face in 2020. Download your copy today!

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes

○ No

○ No but we are considering it

○ Still waiting for cybersecurity guidance from Trump admin EO

○ Don't know

○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

State of Cybersecurity Incident Response

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents. Read this report to find out more.

DOWNLOAD NOW!

- How Enterprises Are Developing and Maintaining Secure Applications — 0 COMMENTS
- How Enterprises are Attacking the Cybersecurity Problem — 0 COMMENTS
- How Data Breaches affect the Enterprise — 0 COMMENTS

MORE REPORTS

TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

CVE-2019-14872
PUBLISHED: 2020-03-19
The _dtoa_r function of the newlib libc library, prior to version 3.3.0, performs multiple memory allocations without checking their return value. This could result in NULL pointer dereference.

CVE-2019-20485
PUBLISHED: 2020-03-19
qemu/qemu_driver.c in libvirt before 6.0.0 mishandles the holding of a monitor job during a query to a guest agent, which allows attackers to cause a denial of service (API blockage).

CVE-2019-19677
PUBLISHED: 2020-03-18
arxes-tolina 3.0.0 allows User Enumeration.

CVE-2019-19676
PUBLISHED: 2020-03-18
A CSV injection in arxes-tolina 3.0.0 allows malicious users to gain remote control of other computers. By entering formula code in the following columns: Kundennummer, Firma, Street, PLZ, Ort, Zahlziel, and Bemerkung, an attacker can create a user with a name that contains malicious code. Other use...

CVE-2020-10365
PUBLISHED: 2020-03-18
LogicalDoc before 8.3.3 allows SQL Injection. LogicalDoc populates the list of available documents by querying the database. This list could be filtered by modifying some of the parameters. Some of them are not properly sanitized which could allow an authenticated attacker to perform arbitrary queri...

This site uses cookies to provide you with the best user experience possible. By using Dark Reading, you accept our use of cookies.

England and Wales with
, London, SW1P 1WG.