Adobe Patches Zero-day Vulnerability Used in Cyberespionage

October 17, 2017

Adobe has released an emergency/out-of-band security update (APSB17-32, for versions 27.0.0.159 and 27.0.0.130) for Adobe Flash Player for Windows, Macintosh, Linux, and Chrome OS. The update addresses a zero-day vulnerability (CVE-2017-11292) that researchers found actively exploited by a group of threat actors known as BlackOasis.

According to researchers, BlackOasis exploits CVE-2017-11292 to distribute the information-stealing malware FinSpy, also known as FinFisher(detected by Trend Micro as BKDR_FINSPY.A, TROJ_FRS.0NA003JC17, and WORM.Win32.TRX.XXPE002FF019). Last September, the group used a separate remote code execution (RCE) vulnerability (CVE-2017-8759) to deliver a variant of the spyware, which is reportedly being sold by its developers and operators as a suite of surveillance software. Researchers note that the attacks they've observed in the wild are targeting Windows machines.

BlackOasis's attack involves the use of spear-phishing emails sent to targets of interest. These malicious emails are attached with a Flash exploit within an ActiveX object embedded in a Word document. The infection chain is multi-stage, using several scripts to retrieve, decrypt, and execute the payload.

CVE-2017-11292 is a memory corruption flaw that can let an attacker execute arbitrary code on a vulnerable system when successfully exploited. Attackers can lure victims with specially crafted Flash content. While it's currently reported to be used in targeted attacks, its public disclosure is likely to make others employ it for their own cybercriminal activities. In fact, some of the other vulnerabilities that BlackOasis use in their campaigns have been employed by other cyberespionage and cybercriminal groups:

- CVE-2015-5119 (also used by a separate cyberespionage group BlackTech)
- CVE-2016-0984 (also used by the Magnitude exploit kit)
- CVE-2016-4117 (also used by Astrum exploit kit and watering hole attacks on financial institutions using the RATANKBA malware)

BlackOasis uses sociopolitical themes as social engineering lures. Like other cyberespionage groups such as BlackTech, ChessMaster, and Pawn Storm, BlackOasis employs decoy documents to divert the would-be victim's attention away from their ulterior motive: steal confidential, mission-critical information. The researchers that monitored BlackOasis note that it is currently targeting Middle Eastern politicians and United Nations officers, as well as journalists and activists. BlackOassis's activities and FinSpy were also observed in Russia, the U.K., Afghanistan, Iraq, Iran, and African countries.

Indeed, vulnerabilities are the bread and butter for many targeted attacks, and patching plays a crucial role in defending against them. In the first half of 2017, 382 new vulnerabilities were reported and disclosed via Trend Micro's Zero Day Initiative, 92 of which were from Adobe—a number that's markedly higher than that of the second half of 2016. Enterprises need to balance their need for maintaining the infrastructure that drives their organizational operations, and the significance of securing them. Defense in depth provides layers of protection against threats that take advantage of security gaps. Some of the best practices to defend against these types of threats include:

- Keep the system and its application updated, or consider virtual patching for legacy systems
- Implement URL categorization, network segmentation, and data categorization
- Enable and deploy firewalls as well as intrusion detection and prevention systems
- Regularly back up data and ensure its integrity
- Enforce the principle of least privilege
- Secure the gateways, especially your email
- Safeguard the tools used by your organization's system administrators to deter hackers from misusing them
- Create stronger patch management policies

Trend Micro Solutions

Trend Micro™ Deep Discovery™ provides detection, in-depth analysis, and proactive response to today's stealthy malware, and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats like the above mentioned zero-day attacks even without any engine or pattern update. Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities.

Given how BlackOasis uses email as an entry point, organizations need to further secure the email gateway to mitigate threats delivered by BlackOasis. Trend Micro™ Hosted Email Security is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevent ransomware from ever reaching end users. At the endpoint level, Trend Micro™ Smart Protection Suites, powered by XGen™ security, deliver several capabilities like high-fidelity machine learning, behavior monitoring and application control, and vulnerability shielding that minimize the threat's impact.

Related Posts
- Operation DRBControl: Uncovering a Cyberespionage Campaign Targeting Gambling Companies in Southeast Asia
- Winnti Group Resurfaces with PortReuse Backdoor, Now Engages in Illicit Cryptocurrency Mining
- Three Recommendations for Securing the Network From Targeted Attacks
- Recognizing Enterprise Mission-Critical Assets
- Trend Micro Security Predictions for 2019: Mapping the Future

Recent Posts
- New Ursnif Campaign Targets Users in Japan
- Developing Story: Coronavirus Used in Malicious Campaigns
- Trickbot Spreads as DLL, Comes with Upgrades Targeting Windows 10
- Analysis: Abuse of .NET features for compiling malicious programs
- WordPress GDPR Plugin Vulnerable to Cross-Site Scripting Attacks

Trend Micro™ Deep Security and Vulnerability Protection protect user systems from any threats that may leverage CVE-2017-11292 via this following DPI rule:

- 1008667 - Adobe Flash Player Type Confusion Vulnerability (CVE-2017-11292)

Trend Micro™ TippingPoint™ customers are protected from threats that may exploit CVE-2017-11292 via this MainlineDV filter:

- 29771: HTTP: Adobe Flash BufferControlParameters Type Confusion Vulnerability

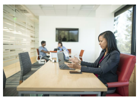
Trend Micro Smart Home Network Security protects customers from threats related to CVE-2017-11292 via this detection rule:

- 1134104: FILE Adobe Flash Player BufferControlParameters Memory Corruption (CVE-2017-11292)

Posted in Vulnerabilities & Exploits, Targeted Attacks

We Recommend

Vulnerabilities & Exploits



WordPress GDPR Plugin Vulnerable to Cross-Site Scripting Attacks

Plugin Leaves Nearly 100,000 WordPress Sites Vulnerable to Compromise

Blocking A CurveBall: PoCs Out for Critical Microsoft-NSA Bug CVE-2020-0601

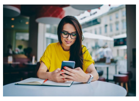
Business Email Compromise

Trend Micro Cloud App Security Report 2019

The Sprawling Reach of Complex Threats

Cybercrime Group Uses G Suite, Physical Checks in BEC Scam

Mobile

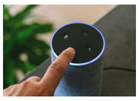


Mobile Banking Trojan FakeToken Resurfaces, Sends Offensive Messages Overseas from Victims' Accounts

Christmas-Themed Shopping, Game and Chat Apps Found Malicious, Lure Users with Deals

Mobile Security: 80% of Android Apps Now Encrypt Network Traffic by Default

Securing Home Routers



Alexa and Google Home Devices can be Abused to Phish and Eavesdrop on Users, Research Finds

Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers

A Look Into the Most Noteworthy Home Network Security Threats of 2017