October 16, 2017

Kaspersky Lab discovers Adobe Flash Zero Day used in the wild by a threat actor to deliver spyware

Woburn, MA – October 16, 2017 – The Kaspersky Lab advanced exploit prevention system has identified a new Adobe Flash zero day exploit, used in an attack on October 10, 2017 by a threat actor known as BlackOasis.

Woburn, MA – October 16, 2017 – The Kaspersky Lab advanced exploit prevention system has identified a new Adobe Flash zero day exploit, used in an attack on October 10, 2017 by a threat actor known as BlackOasis. The exploit is delivered through a Microsoft Word document and deploys the FinSpy commercial malware. Kaspersky Lab has reported the vulnerability to Adobe, which has issued an advisory.

According to Kaspersky Lab researchers, the zero day, CVE-2017-11292, has been spotted in a live attack, and they advise businesses and government organizations to install the update from Adobe immediately.

The researchers believe that the group behind the attack was also responsible for CVE-2017-8759, another zero day, reported in September – and they are confident that the threat actor involved is BlackOasis, which the Kaspersky Lab Global Research and Analysis Team began tracking in 2016.

Analysis reveals that, upon successful exploitation of the vulnerability, the FinSpy malware (also known as FinFisher) is installed on the target computer. FinSpy is a commercial malware, typically sold to nation states and law enforcement agencies to conduct surveillance. In the past, use of the malware was mostly domestic, with law enforcement agencies deploying it for surveillance on local targets. BlackOasis is a significant exception to this – using it against a wide range of targets across the world. This appears to suggest that FinSpy is now fuelling global intelligence operations, with one country using it against another. Companies developing surveillance software such as FinSpy make this arms race possible.

The malware used in the attack is the most recent version of FinSpy, equipped with multiple anti-analysis techniques to make forensic analysis more difficult.

After installation, the malware establishes a foothold on the attacked computer and connects to its command and control servers located in Switzerland, Bulgaria and the Netherlands, to await further instructions and exfiltrate data.

Based on Kaspersky Lab's assessment, the interests of BlackOasis span a whole gamut of figures involved in Middle Eastern politics, including prominent figures in the United Nations, opposition bloggers and activists, as well as regional news correspondents. They also appear to have an interest in verticals of particular relevance to the region. During 2016, the company's researchers observed a heavy interest in Angola, exemplified by lure documents indicating targets with suspected ties to oil, money laundering and other activities. There is also an interest in international activists and think tanks.

So far, victims of BlackOasis have been observed in the following countries: Russia, Iraq, Afghanistan, Nigeria, Libya, Jordan, Tunisia, Saudi Arabia, Iran, the Netherlands, Bahrain, United Kingdom and Angola.

"The attack using the recently discovered zero-day exploit is the third time this year we have seen FinSpy distribution through exploits to zero-day vulnerabilities," said Anton Ivanov, lead malware analyst at Kaspersky Lab. "Previously, actors deploying this malware abused critical issues in Microsoft Word and Adobe products. We believe the number of attacks relying on FinSpy software, supported by zero day exploits such as the one described here, will continue to grow."

Kaspersky Lab security solutions successfully detect and block exploits utilizing the newly discovered vulnerability.

Kaspersky Lab experts advise organizations to take the following actions to protect their systems and data against this threat:

- If not already implemented, use the killbit feature for Flash software and, wherever possible, disable it completely.
- Implement an advanced, multi-layered security solution that covers all networks, systems and endpoints.
- Educate and train personnel on social engineering tactics as this method is often used to make a victim open a malicious document or click on an infected link.
- Conduct regular security assessments of the organization's IT infrastructure.
- Use Kaspersky Lab's Threat Intelligence, which tracks cyberattacks, incident or threats and provides customers with up-to-date relevant information that they are unaware of. Find out more at intelreports@kaspersky.com.

For technical details, including indicators of compromise and YARA rules, please read the blogpost on Securelist.com.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company celebrating its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

For the latest in-depth information on security threat issues and trends, please visit:

Securelist | Information about Viruses, Hackers and Spam

Follow @Securelist on Twitter

Threatpost | The First Stop for Security News
Follow @Threatpost on Twitter

Media Contact
Sarah Kitsos
781.503.2615
sarah.kitsos@kaspersky.com

Related Articles Virus News

Kaspersky Lab GReAT Releases Targeted Threat Predictions for 2019

Researchers predict that in the coming year, threat actors will go to new lengths to carry out devastating attacks

Read More >

Kaspersky Lab Finds 2018's Malicious Crypto-Mining Fever Powered by Pirated Software and Content

Cryptocurrency mining malware wreaks havoc in 2018, infecting more than five million people in the first three quarters of the year

Read More >

Remote Access Nightmare: Amount of Malware Found to be Backdoors Increases by 44% in 2018

New report shows Kaspersky Lab technologies detected 346,000 new malicious files every day in the first ten months of the year

Read More >