Middle Eastern hacking group is using FinFisher malware to conduct international espionage

By Chris Bing

Published: 2017-10-16 · Archived: 2026-04-06 00:34:17 UTC

A well-funded, highly active group of Middle Eastern hackers was caught, yet again, using a lucrative zero-day exploit in the wild to break into computers and infect them with powerful spyware developed by an infamous cyberweapons dealer named Gamma Group.

The incident, as described by security researchers with Moscow-based cybersecurity firm Kaspersky Lab, shines a rare light on the opaque although apparently vibrant market for software exploits and spyware, which in this case appears to have been purchased by a nation-state.

The Middle Eastern hacker group in this case is codenamed "BlackOasis." Kaspersky found the group was exploiting a Adobe Flash Player zero-day vulnerability (CVE-2016-4117) to remotely deliver the latest version of "FinSpy" malware, according to a new blog post published Monday. Adobe issued a fix Monday to its users in the form of a software update.

FinSpy, a final-stage payload that allows for an attacker to covertly learn what a target is talking about and who they are communicating with, is associated with Gamma Group — which goes by other names, including FinFisher and Lench IT Solutions.

BlackOasis in recent months sent a wave of phishing emails. These emails contained malicious Microsoft Word documents with the aforementioned Flash Player zero-day hidden inside an embedded ActiveX object. In the past, BlackOasis messages were designed to appear like news articles from 2016 about political relations between Angola and China.

The term zero-day is indicative of a software flaw that remains unknown to the software's creator. Zero-days can be highly disruptive because they provide a window of time for an attacker to breach victims before the vendor is able to apply a software update to address the specific security hole.

U.S. cybersecurity firm FireEye also recently captured BlackOasis activity as part of a similar incident where the group relied on a different zero-day exploit — more specifically, a SOAP WSDL parser code injection vulnerability — to install FinSpy onto a small number of devices. Again, the attacker's intention appeared to be espionage.

"Unlike other FinFisher customers or users who focus mostly on domestic operations, BlackOasis focuses on external operations and go after a wide range of targets around the world," explained Costin Raiu, director of the global research and analysis team at Kaspersky Lab.

Gamma Group has been accused of selling its products to authoritarian regimes that can use the technology to both track dissidents and conduct foreign espionage over the internet.

The discovery by Kaspersky marks at least the fifth zero-day exploit used by BlackOasis and exposed by security researchers since June 2015. It's unclear whether the hackers are purchasing the exploits and spyware together, directly from Gamma Group, or if they were able to acquire some of the tools through other avenues.

"BlackOasis' interests span a wide gamut of figures involved in Middle Eastern politics and verticals disproportionately relevant to the region. This includes prominent figures in the United Nations, opposition bloggers and activists, and regional news correspondents," a blogpost about Kaspersky's findings reads.

The post continues, "during 2016, we observed a heavy interest in Angola, exemplified by lure documents indicating targets with suspected ties to oil, money laundering, and other illicit activities. There is also an interest in international activists and think tanks … Victims of BlackOasis have been observed in the following countries: Russia, Iraq, Afghanistan, Nigeria, Libya, Jordan, Tunisia, Saudi Arabia, Iran, Netherlands, Bahrain, United Kingdom and Angola."

Brian Bartholomew, a senior security researcher with Kaspersky, said on Twitter that BlackOasis' espionage included non-traditional targets — "going outside of that lawful surveillance boundary."

An advanced persistent threat group, previously identified by Microsoft and codenamed Neodymium, is closely associated with BlackOasis' operations.

Last year, Microsoft researchers described Neodymium's behavior as unusual: "unlike many activity groups, which typically gather information for monetary gain or economic espionage, PROMETHIUM and NEODYMIUM appear to launch campaigns simply to gather information about certain individuals. These activity groups are also unusual in that they use the same zero-day exploit to launch attacks at around the same time in the same region. Their targets, however, appear to be individuals that do not share common affiliations."

A cursory review of BlackOasis' espionage campaign suggests there is some overlap between the group's actions and Saudi Arabia's geopolitical interests. For example, the targeting of Angolan organizations in mid-2016 coincidences directly with the rise of Angola's oil business with China, which displaced Saudi Arabia as the number one exporter of crude oil to China at the time.

All 13 countries where Kaspersky reportedly observed BlackOasis activity are connected to Saudi Arabia in one of three ways: economically; from a national security perspective; or due to established policy agreements.

In addition, Saudi Arabia is a known customer of spyware and has used the technology domestically, according to Citizen Lab, a cybersecurity and human-rights focused research laboratory. Kaspersky's research notes that BlackOasis hacked into computers based in Saudi Arabia.

Source: https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/