‘Pentagon cyber-espionage op’: US reportedly behind Slingshot malware targeting Mid East & Africa

22/03/2018

Cybersecurity firm Kaspersky Lab reportedly busted a major US military asset when it exposed a sophisticated cyber-espionage operation that targeted computer networks in the Middle East.

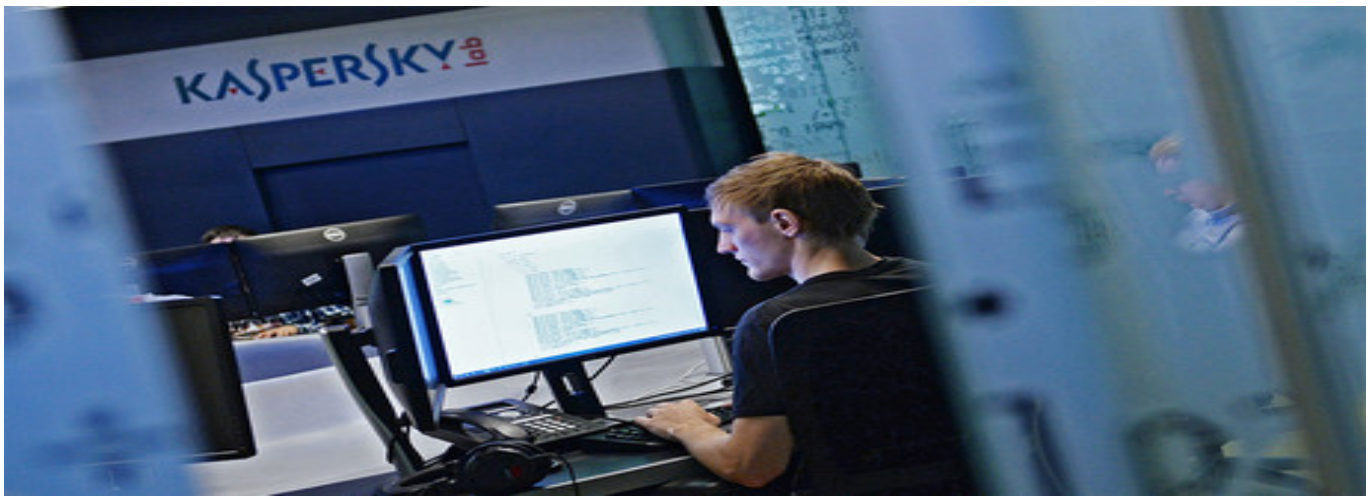
On March 9, the leading Russia-based cybersecurity company reported their research on a program it called Slingshot, which used a highly sophisticated approach to infect computers with malware through infected routers. The operation had targeted computers throughout the Middle East and some parts of Africa since at least 2012, and required a lot of money and expertise from its creators. A report by an industry news publication, CyberScoop, claims Slingshot was run by the Special Operations Command (SOCOM).

@kaspersky #ICYMI: @Securityblvd provides details on sophisticated #Slingshot #malware that uses compromised #routers to penetrate networks #spyware #netsec #cybersecurity #IoT https://kas.pr/889v

The report about the program was the biggest part of the Kaspersky Security Analyst Summit (SAS) this month. The firm’s researchers identified an advanced persistent threat (APT) – a term that usually describes a well-organized and

trained group of hackers operating on a regular basis and possibly on behalf of a state government – that found a way to compromise various devises through routers. The attack was described as *“remarkable and, to the best of our knowledge, unique”* by Kaspersky researchers.

Read more [Kaspersky Lab under attack as it found something the US didn't like – company head]



The company failed to identify how the routers themselves were infected. But they were used to inject malware into computers. The attack replaced one of the Windows libraries with a malicious one, and then used it to download and install two distinct pieces of malware called Cahnadr and GollumApp, which Kaspersky described as *“masterpieces of cyberespionage art.”* Combined, the two gave virtually unrestricted access to an attacked computer, harvesting screenshots, key strokes, network traffic, USB connections, clipboard content, and many other things.

The people behind Slingshot also took serious measures to protect their malware from being detected. For example, it can shut down its own components before being exposed by anti-viral software. It also runs its own file system to remain hidden from the computer-operating system, and blocks disc defragmentation to avoid being damaged by the process.

Kaspersky Lab said it has found around 100 victims of Slingshot and its related modules in Kenya, Yemen, Afghanistan, Libya, Congo, Jordan, Turkey, Iraq, Sudan, Somalia and Tanzania. Kenya and Yemen accounted for the majority of the cases. Most of the victims were individuals rather than organizations.

The company said they could not attribute the threat to a particular actor, but believed the people behind it to be *“highly organized and professional and probably state-sponsored.”* Text clues in the code suggested they were *“English-speaking”*.

The news report quotes unnamed former and current US intelligence officials, who said that Slingshot was an operation of the Joint Special Operations Command (JSOC), a component of SOCOM. Kaspersky Lab “burned” the program, which is believed to have been an anti-terrorist operation, leaving the American military without a valuable tool and potentially putting American lives at risk, the officials claimed.

Read more Kaspersky Lab sues Trump administration over software ban

“SOP [standard operating procedure] is to kill it all with fire once you get caught,” CyberScoop quoted a former intelligence official as saying. *“It happens sometimes and we’re accustomed to dealing with it. But it still sucks… I can tell you this didn’t help anyone.”*

CyberScoop says that Cahnadr and GollumApp are associated with hacker groups widely believed to be the NSA and the CIA respectively in the cybersecurity community. The report implies that Kaspersky Lab should have expected Slingshot to be a US operation.

“It’s clear by the way they wrote about this that they knew what it was being used for,” a senior official told the news service. *“GReAT [Kaspersky’s Global Research & Analysis Team] is extremely adept at understanding the information needs of different actors out there on the internet. They take into considering the geopolitical circumstances, they’ve shown that time and time again. It would be a stretch for me to believe they didn’t know what they’re dealing with here.”*

When asked about the claim that it damaged a US military operation, Kaspersky Lab denied knowing who the Slingshot APT was.

“As a result of anonymized data, it's impossible for us to tell who the specific targets are. All the company can state is that our users are protected against

malicious software that can spy, steal or sabotage data from their computers,” they told RT in a statement.

Kaspersky Lab added that their software does not differentiate between malware based on who created it and for what purpose, as any malware is potentially dangerous, even if created by state actors, because it can always fall into the wrong hands.

Kaspersky Lab is currently in the middle of court battle with the US government over the company’s expulsion from part of the American market. US government entities were banned from purchasing services from Kaspersky after the US intelligence accused the company of providing a backdoor for their Russian counterparts through its anti-virus software. Kaspersky denies the allegations and claimed in its lawsuit that the government’s decision was based largely on uncorroborated news media reports as evidence.