BIZCOMMUNITY

USBs are back: Kaspersky uncovers a rare threat campaign

Kaspersky has uncovered a rare, wide-scale advanced persistent threat (APT) campaign against users that was first detected in Southeast Asia. Kaspersky identified approximately 1,500 victims, some of which were government entities. Initial infection occurs via spear-phishing emails containing a malicious Word document; once downloaded on one system, the malware can then spread to other hosts through removable USB drives.

Source: Unsplash

"APT campaigns are, by nature, highly targeted. Often, no more than a few dozen users are targeted, often with surgical like precision. However, recently, Kaspersky uncovered a rare, widespread threat campaign with a rarely used, yet still a movie-like attack vector. Once downloaded on a system, the malware attempts to infect other hosts by spreading through removable USB drives. If a drive is found, the malware creates hidden directories on the drive, where it then moves all of the victim's files, along with the malicious executables," Kaspersky said in a statement.

This cluster of activity — dubbed LuminousMoth — has been conducting cyberespionage attacks against government entities since at least October 2020. While initially focusing their attention on Myanmar, the attackers have since shifted their focus to the Philippines. The attackers typically gain an initial foothold in the system through a spear-phishing email with a Dropbox download link. Once clicked, this link downloads a RAR archive disguised as a Word document that contains the malicious payload.

Kaspersky experts attribute LuminousMoth to the HoneyMyte threat group, a well-known, long-standing, Chinese-speaking threat actor, with medium to high confidence. HoneyMyte is primarily interested in gathering geopolitical and economic intelligence in Asia and Africa.

New and unknown malware implants

"This new cluster of activity might once again point to a trend we've been witnessing over the course of this year: Chinese-speaking threat actors re-tooling and producing new and unknown malware implants," comments Mark Lechtik, senior

security researcher with the Global Research and Analysis Team (Great) at Kaspersky.

“The massive scale of the attack is quite rare. It’s also interesting that we’ve seen far more attacks in the Philippines than in Myanmar. This could be due to the use of USB drives as a spreading mechanism or there could be yet another infection vector that we’re not yet aware of being used in the Philippines,” adds Aseel Kayal security researcher with Great at Kaspersky.

“We’re seeing increased activity by Chinese-speaking threat actors this past year, and this most likely won’t be the last of LuminousMoth. In addition, there’s a high chance the group will begin to further sharpen its toolset. We’ll be keeping an eye out for any future developments,” comments Paul Rascagneres, senior security researcher with Great at Kaspersky.

For more, visit: https://www.bizcommunity.com