State-backed players join pandemic cyber crime attacks

March 30 2020

Sophisticated state-supported actors are following cybercriminals in exploiting the coronavirous pandemic and posing an "advanced persistent threat" (APT), French defence technology giant Thales warned Monday.

Hades, linked to the APT28 which is believed to be of Russian origin and behind an attack on the US Democrat party in 2016, was the first state-backed group to use the epidemic as bait, Thales' cyber intelligence service reported.

"According to the cyber security company QiAnXin, Hades hackers waged a campaign in mid-February by hiding a Trojan horse in bait documents (...) disguised as e-mail from the Ukrainian health ministry's public health centre," Thales said.

"These targeted emails seem to have been part of an even bigger disinformation campaign that affected the entire country on different fronts," with the aim of creating panic in Ukraine, it added.

Vicious Panda, a group believed to be of Chinese origin, was behind "a new campaign against the Mongolian public sector", Thales said, quoting the US-Israeli firm Checkpoint.

Mustang Panda, also believed to be Chinese in origin, "managed to target Taiwan using new lures," linked to the coronavirus, while Kimsuky, suspected to be of North Korean origin, continues to attack targets in

South Korea, and APT36, a group said to have Pakistani origins, has gone after Indian targets.

Thales also warned of a proliferation of fake virus information applications for Android that exploit public demand.

The company said several sources confirmed that half of the domain names set up since December linked to COVID-19 themes are exposed to malware.

"It seems that the cyber threat ecosystem is following the geographical spread of COVID-19 with attacks first in Asia, then eastern Europe and now in western Europe," Thales noted.