Kingdom targeted by new malware

phnompenhpost.com/national/kingdom-targeted-new-malware

By Alessandro Marazzi Sassoon, Rinith Taing

The Kingdom's computer networks, including government servers, are reported to be the targets of a virus unique to Cambodia and deployed through spam emails and phishing campaigns, which lure victims with emails disguised as official communications, though officials yesterday maintained they were unaffected.

First reported by the cybersecurity firm Palo Alto Networks over the weekend, the attacks are a form of Trojan – or malware disguised as legitimate software – known as "KHRAT", which began circulating in late June.

Attackers used a weaponised Word document in an email attachment labelled "MIWRMP phase 3", a reference to the $15 million World Bank-funded Mekong Integrated Water Resources Management Phase 3 Project.

According to the security firm's report, the virus grants hackers "access to the victim system, including keylogging, screenshot capabilities, remote shell access and so on".

“We believe this malware, the infrastructure being used, and the TTPs [tactics, techniques and procedures] highlight a more sophisticated threat actor group, which we will continue to monitor closely and report on as necessary,” Palo Alto’s report notes, adding that the attack compromised Cambodian government servers.

Chea Pov, head of the Interior Ministry’s cybercrime unit, said while he was aware of the type of attack, he had received no indication government officials, websites or servers had been affected. “If this problem happens among our officials or institutions, they will submit the complaint to us, but now I have not seen any. If we receive any complaint, we will work out how to deal with it,” he said.

According to the World Bank website, the Mekong water management project is designed “to establish the foundation for the effective management of water resources and fisheries in the project areas of northeast Cambodia”.

The project also falls within the framework of the Mekong River Commission’s (MRC) work on water management. Inquiries to the MRC and World Bank went unanswered yesterday.

Te Navuth, general secretary of the project’s implementing partner, the Cambodia National Mekong Committee, said he was previously unaware of the cyber threat. “Now that I know about it, I will have to think first about how this issue should be dealt with,” he said.

Cybersecurity expert Niklas Femerstrand in an email yesterday pointed out that while servers in several different countries appear to be the origin the attack, it has been linked to the DragonOK campaign.

“The DragonOK campaign has previously [in 2014] targeted organizations in Taiwan, Japan, Tibet and Russia, and political organizations in Cambodia since at least January, 2017,” he wrote, adding that there are “strong indications” the campaign is “an operation funded by China”.

“They’re looking for any intelligence from anybody, and most probably this is linked to a wider Advanced Persistent Threat operation . . . of which right now we are only seeing the iceberg tip,” he wrote, referring to a continuous covert hacking process used to target a specific entity.

Professor Carlyle Thayer, an Asian security expert at the University of New South Wales, noted Chinese state-sponsored hacking is not necessarily always targeted, but did recall that earlier this year “Chinese directed phishing attacks against Cambodian citizens was reported”, and that some “seemed directed at opposition political parties”.

“While some hacking is specific, other hacking efforts are designed just to gather information to expand files and data bases,” he wrote.

According to Femerstrand, the best protection is to not open unexpected attachments in emails from unverified senders and to be wary of external links in documents, in addition to keeping antivirus software up to date.