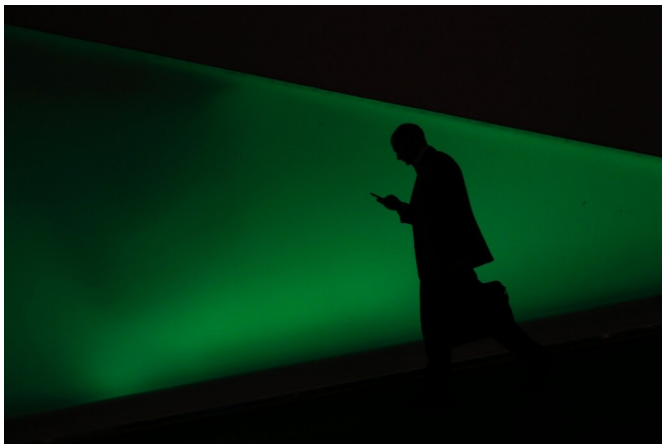
Hackers target UN humanitarian organizations: Lookout

24 October 2019



Security researchers say UN and other humanitarian workers are being targeted by phony emails by hackers looking for passwords

Hackers are targeting United Nations and humanitarian aid workers with a scheme designed to trick members into revealing passwords, security researchers said Thursday.

A report released by cybersecurity firm Lookout said the campaign aimed at UN-connected relief organizations has been active since early this year, and is crafted to lure workers to fake websites where their credentials may be stolen.

Lookout principal security intelligence engineer Jeremy Richards told AFP groups targeted included the UN World Food Program, UNICEF and the International Federation of the Red Cross and Red Crescent Societies.

The attacks use spoofed emails in a tactic known as "phishing" to hook victims.

The spoofed messages are designed to appear like legitimate ones but often will have booby-trapped link or files included or lead to malicious websites.

"We come across a lot of phishing," Richards said.

"But it is not very often that we see NGOs attacked at this scale."

Lures sent to potential victims appeared to include texted or emailed invitations to take surveys or access online documents, with links to "landing pages" that mirror legitimate organization log-in pages but which capture information for hackers, according to Lookout.

Hacker software used in the ploy is tailored to capture whatever is typed into password fields even if it is quickly deleted, and to recognize when people are connecting from mobile devices.

"If a target doesn't complete the log-in activity or if they enter another, unintended, password by mistake this information is still sent back to the malicious actor," Richards said.

Taking the bait for a promised PDF file, in this attack, led to a document addressed to the "Pyong Yang international community," according to Lookout. Pyongyang is the capital of North Korea.

Once a hacker has an email password, they could obtain a password reset link to a victim's other online accounts, or dupe contacts with rigged responses to legitimate email exchanges.

It remained unclear who was behind the attack or how successful it has been.

Lookout has warned targeted organizations and shared its discovery with law enforcement, according to the mobile cybersecurity firm.

Phishing campaigns crafted to dupe users of smartphones or tablets have become a heightened risk for businesses, Lookout said.

Websites used in the phishing attack on UN groups were evidently being run from a "bulletproof hosting service" in Malaysia that promises anonymous computing services insulated from investigators or governments, according to Richards.