Covid-19 Relief: North Korea Hackers Lazarus Planning Massive Attack on US, UK, Japan, Singapore, India, South Korea?

By Bhaswati Guha Majumder

Published: 2020-06-18 · Archived: 2026-04-05 23:35:08 UTC

Video Player is loading.

Current TimeÂ 0:00

DurationÂ -:-

Loaded: 0%

Remaining TimeÂ -:-

Â

Hacking activity increased during Coronavirus pandemic

Close

Hacking activity increased during Coronavirus pandemic

North Korea-based hacking group Lazarus is planning to launch broader phishing attacks designed as COVID-19 relief efforts against six countries including Singapore, targeting more than five million individuals and businesses (small, medium, and large enterprises), warned a security firm.

Travel Guides & Travelogues

CYFIRMA, a threat intelligence and cybersecurity platform company, has exposed the malicious plans of North Korean hackers. They revealed that the campaign was planned to launch on Saturday, June 20. The hackers, who

claimed to have 8,000 business contact details, made plans to send phishing emails from a spoofed Ministry of Manpower email account offering additional payment of S$750 for all employees of these companies.

Hacing activitis (Representational picture) Pixabay

If You Receive an Email Like This, Do Not Trust

The phishing emails reads like this:

> ***Member of Singapore Business Federation,***
>
> ⚡Travel Guides & Travelogues
>
> ***Thank you for your long-term support during the COVID19 circuit breaker. We understand the pain and torture you have suffered in the past two months, which has prevented you from conducting business.***
>
> Discover more
>
> Travel Guides & Travelogues
>
> Geographic Reference
>
> Tourist Destinations
>
> ***In the past few months, we have announced many business-friendly programs supported by the Singapore government. In addition, the Ministry of Manpower (MOM) of Singapore today announced a new financial plan that provides a one-time subsidy of S$750 per employee under the Work Support Plan (JSS).***

> ***Please register your company and don't forget to provide your company bank information so that we can transfer funds automatically.***
>
> ***Claim your financial support immediately***
>
> ***Thank you,***
>
> ***Ministry of Manpower [MOM] Singapore***
>
> ***MOM Service Center***
>
> ***1500 Bendemeer Road, Singapore 339946***
>
> ***Employment Pass Service Center***
>
> ***Binhe Road, 20 Upper Ring Road, #04-01/02, Singapore 058416***

The researchers at CYFIRMA, who have been tracking the Lazarus Group for many years, . said their investigation into the Group's activities has revealed detailed plans indicating an upcoming global phishing campaign this weekend.

As in many countries government organizations announced significant financial support to individuals and businesses in their effort to stabilize their pandemic-ravaged economies, the phishing campaign is designed to impersonate government agencies, departments, and trade associations who are tasked to oversee the disbursement of the financial aid.

North Korea Hackers

In a news release, CYFIRMA said they first picked up the lead on June 1. After the analysis, evidence showed that hackers planning to launch attacks in six countries across multiple continents over a two-day period. Further research uncovered seven different email templates impersonating government departments and business associations.

As of Thursday, the researchers have not seen the phishing or impersonated sites defined in the email templates. But the research showed that the North Korean hackers were planning to set that up in the next 24 hours.

They also found that North Korean cyber criminals are planning to spoof or create fake email IDs impersonating various authorities. These are some of the emails discussed in their phishing campaign plan:

A cybersecurity expert *Jeffrey Kok*, who is the Vice President Solution Engineers for Asia Pacific and Japan for CyberArk told IBTimes Singapore:

> ***Phishing remains probably the malicious attacker's number one way of potentially accessing confidential information. For the individual, this can mean compromised personal details, which is damaging but usually limited in scale.***
>
> ***However, for attacks that target businesses, the effects can be much more wide-ranging. Once a foothold in business is established through a successful phish, critical data and assets within the***

> ***business are all at risk if the attack is not contained. This could include customer data files, financial information, or even result in the IT infrastructure being taken down.***
>
> ***To meet this challenge, businesses should consider adopting privileged access management to prevent the lateral spread of an attack. By proactively managing and rotating high-value 'privileged' credentials and limiting user access to only the information and tools needed to perform their immediate role, an attacker's route to critical data and assets can be contained, reducing their ability to exfiltrate information or disrupt operations.***

1 of 5

Country Name	Campaign Launch Date	Target
USA	20 June 2020	Individuals
UK	20 June 2020	Businesses
Japan	20 June 2020	Individuals
India	21 June 2020	Individuals
Singapore	21 June 2020	Businesses
South Korea	21 June 2020	Individuals

Recent analysts also claimed that North Korea will most likely attack the U.S. presidential election in November after Kim Jong Un's regime explicitly threatened that possibility recently. Sung-Yoon Lee, the Kim Koo-Korea Foundation professor in Korean Studies at the Fletcher School of Law and Diplomacy at Tufts University said that North Korea will be able to test how far and to what extent it can damage the U.S. election system. Lee said, "I fully expect North Korea to test its own capabilities to see what it can get away with by hacking into the U.S. election system."

Source: https://www.ibtimes.sg/covid-19-relief-north-korea-hackers-lazarus-planning-massive-attack-us-uk-japan-singapore-47072