CERT-In Advisory CIAD-2020-0040

COVID 19-related Phishing Attack Campaign by Malicious Actors

Original Issue Date: June 19, 2020

Description

It has been reported that malicious actors are planning a large-scale phishing attack campaign against Indian individuals and businesses (small, medium, and large enterprises).

The phishing campaign is expected to use malicious emails under the pretext of local authorities in charge of dispensing government-funded Covid-19 support initiatives. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information.

The phishing campaign is expected to be designed to impersonate government agencies, departments, and trade associations who have been tasked to oversee the disbursement of the government fiscal aid. The malicious actors are claiming to have 2 million individual / citizen email IDs and are planning to send emails with the subject: free COVID-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad, inciting them to provide personal information.

It has been reported that these malicious actors are planning to spoof or create fake email IDs impersonating various authorities. The email id expected to be used for the phishing campaign towards Indian individuals and businesses is expected to be from email such as "ncov2019@gov.in" and the attack campaign is expected to start on 21st June 2020.The email may look as follows:

Best Practices

- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Leverage Pretty Good Privacy in mail communications. Additionally, advise the users to encrypt / protect the sensitive documents stored in the internet facing machines to avoid potential leakage
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header). Block the attachments of file types, "exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"
- Beware about phishing domain, spelling errors in emails, websites and unfamiliar email senders
- Check the integrity of URLs before providing login credentials or clicking a link.
- Do not submit personal information to unknown and unfamiliar websites.
- Beware of clicking form phishing URLs providing special offers like winning prize, rewards, cashback offers.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Update spam filters with latest spam mail contents
- Any unusual activity or attack should be reported immediately at incident@cert-in.org.in. with the relevant logs, email headers for the analysis of the attacks and taking further appropriate actions.

References

https://zeenews.india.com/india/north-koreas-lazarus-hackers-plan-phishing-attack-in-india-to-steal-covid-aid-2290701.html
https://www.cyfirma.com/early-warning/global-covid-19-related-phishing-campaign-by-north-korean-operatives-lazarus-group-exposed-by-cyfirma-researchers/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India