Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2020-0024

Email extortion scams

Original Issue Date: April 27, 2020

Severity Rating: High

Description

In email extortion campaign, the scammers have sent numerous emails to people stating that their computers were hacked, a video was taken using their webcam, and that they know their passwords.

Understanding extortion email

Firstly, the scammer would try to grab the recipient's attention by writing their old password in the mail, which could look the following:

"I know, xxx, is your password. You don't know me and you're thinking why you received this e mail, right?"

After that, the scammer would craft a story containing computer jargons in order to convince the recipient that the scammeris a very skilled hacker, which could look the following:

"Well, I actually placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account."

This could be the final step before asking for ransom, so here the scammer would claim to have recorded personal video(s)by compromising the recipient's webcam, which could look the following:

"What exactly did I do?

I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam (Yep! It's you doing nasty things!). "

Now, the scammer will ask for the ransom in the form of Bitcoin (BTC), which could look the following:

"What should you do?

Well, I believe, $1900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address:

bc1qzl2qlywq8fzfm49e7mvsuz4yvpdwpzfqs5g85r

(It is cAsE sensitive, so copy and paste it) "

Lastly, the scammer will give the deadline of 24hrs to comply and threaten to send videos to their relatives, coworkers etc..., which could look the following:

"Important:

You have 24 hours in order to make the payment. (I have an unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your 5 friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email. "

Observations

Although, the listed passwords are in many cases actual passwords used by the recipient in the past, but the attacker does not know them by hacking your account, but rather through leaked data breaches shared online. These emails are fake, scams, and nothing to worry about.

Best Practices

- Recipients should not send any payments to the scammers.
- If the passwords listed are in use or familiar, recipients are advised to change the password at any site that they are being used.

References

https://www.bleepingcomputer.com/news/security/large-email-extortion-campaign-underway-dont-panic/

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