Fake Email Campaign Demanding Ransom in Cryptocurrency

A fake email campaign claims to have recorded personal videos of victims which it threatens to publish if demanded ransom in cryptocurrency not paid.

Internet users have been alerted by national federal cybersecurity agency against a fake email campaign that is going on in the country; the authors behind the campaign are threatening to post a personal video of a victim that they claim to have recorded if the demanded ransom in the form of cryptocurrency is not paid to them.

While assuring users that there's nothing major to worry about these emails as the claims made in it are fake, the Computer Emergency Response Team of India (CERT-In) in a related advisory, suggested users assign new passwords to all their online platforms including their social media handles.

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology security organization. It has been designated as the national agency to respond to computer security incidents. The purpose of CERT-In is to issue guidelines, advisories, and promote effective IT security practices throughout the country.

A number of emails have been sent as a part of the campaign, claiming that the receiver's computer was compromised and a video was recorded via their webcam and that the sender has access to their passwords, as per the CERT-In latest advisory on the

matter. The attacker attempts to convince the user into falling in his trap by mentioning his previous password in the email, then by strategic use of computer jargon, the attacker comes up with a story to appear as a highly-skilled scammer to the recipient. The story tells the victim that while he was surfing a porn website, his display screen and webcam was compromised by a malware placed by the hacker onto the website.

It states that all of the user's contacts from Facebook, email, and messenger have been hacked alongside.

As these emails are scams and claim false information, users are advised to not get tricked into paying the demanded ransom in haste as even if the password mentioned by attackers in the email seems familiar it's because they accessed it via leaked data posted online and not through hacking their account. All you have to do is change or update your password for all the online platforms where it is being used.

https://www.ehackingnews.com/2020/05/fake-email-campaign-demanding-ransom-in.html