Moroccan hacker Dr HeX arrested for phishing attacks, malware distribution

therecord.media/moroccan-hacker-dr-hex-arrested-for-phishing-attacks-malware-distribution/

July 6, 2021

Image: The Record

Moroccan authorities arrested a suspect known in underground hacking circles as "**Dr HeX**" on accusations of orchestrating a 12-year-old cybercrime spree that included website defacements, phishing attacks, and malware distribution, Interpol announced today.

- The arrest took place in May this year and was announced today as part of Interpol's Operation Lyrebird.
- In a blog post today, cyber-security firm Group-IB said its analysts were the ones to track down the hacker's location.
- Group-IB said it managed to link an email address used in one of Dr HeX's phishing kits to the suspect's real-world identity.
- Per the company's researchers, the email address was used to register a public YouTube channel, and the description of one of the videos hosted on this profile linked to an Arabic crowd-funding platform.
- In total, Group-IB said its investigation unearthed five email addresses and six public nicknames used by the hacker, including accounts on Skype, Facebook, Instagram, and YouTube.
- These emails and public nicknames helped researchers track the suspect's activities back to 2009, when the threat actor began defacing public websites.
- Subsequent sleuthing linked Dr HeX to phishing campaigns and intrusions at a French corporation, from where Group-IB said the suspect tried to steal banking card data.

- Other phishing and malware attacks also targeted French telecommunications companies, major French banks, and several multinational corporations.

> We have seen direct links between this actor #DrHeX in numerous credential phishing kits and also using the ZombiBot SMTP Cracker.
>
> The actor is also seen to be using code from other phishing kits in their own code which we usually associate with less skilled actors.#Phishing https://t.co/BLjmZPLBPb pic.twitter.com/DiRxtZmB85
>
> — Jake – JCyberSec_ (@JCyberSec_) July 6, 2021

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.