RELENTLESS CAMPAIGN

The international phishing expedition looking to hook India’s big fish

A single phishing attack by Pakistani hackers in February compromised hundreds of armed forces personnel—both serving and former. Even troop movement information was breached. The incident isn’t a one-off and India’s lax cybersecurity hygiene is to blame

Pratap Vikram Singh, 24 May 2021

India's government email systems are perennially under attack as state-sponsored actors constantly run phishing campaigns for espionage

In February, Pakistani hackers compromised the Android phones of hundreds of military personnel, managing to access and steal sensitive information

It is hardly an isolated event. Just in the last 12 months, several such attempts with cross-border origins have rattled existing controls

MeitY and NIC, in charge of mail and IT infra and enforcement, reel under staff and funding shortages. Meanwhile, most ministries and agencies absolve themselves of responsibility

Read a 200 word free summary.
SHOW SUMMARY

On the afternoon of 18 February, a retired army officer received a seemingly innocuous mail. Sent by a serving and senior member of the army, and coming from a respectable 'gov.in' address, it was an invitation to a lunch in Delhi. The message was brief, even by military standards, with the details enclosed in an attachment linked within the email.

Unbeknownst to the retired officer, the link was a veritable Pandora's box. When clicked, it downloaded an app containing an assortment of circulars and news related to the Indian army. That, however, was just an eyewash. Its true purpose was to unleash malware, which would course through the victim's computer or phone, stealing everything from WhatsApp chats to SMSes and media files. This malware, if left unchecked, could stay on a target's system indefinitely, constantly pilfering sensitive data.

According to multiple sources working closely with one of the cyber incident response teams attached to the Ministry of Defence, the data was being transmitted to a command and control centre in the Netherlands—the source of the phishing attack. They told *The Ken* that hackers made use of the country's many 'bulletproof hosting' services, which essentially allow hackers to securely host malicious content which can be used to carry out cyber attacks. These servers, which were paid for in Bitcoin, were accessed from Karachi, Pakistan.

While media reports have emerged, claiming that only a few dozen retired army personnel were targeted, *The Ken* has learnt that hundreds of Indian army personnel—both serving and former—fell prey to the email. "The data copied included personal images, audio and call recordings, and PDF documents pertaining to troop movements," say the sources quoted above. If the claim about leaked troop movement documents is true, it indicates that serving personnel were indeed targeted. *The Ken* put this claim to the Ministry of Defence, but received no response.

Phishing attacks—using fraudulent or manipulated messages to steal information—are nothing new. These attacks have found increased utility in espionage, with a number of countries using hackers to ferret out sensitive information from both rivals and allies.

In this case, hackers first compromised the email credentials of a serving officer and used it to send malware-laden emails to others. Coming from a high-ranked official and from an official ID, few suspected anything was amiss.

Guess who

According to a response in the Lok Sabha from the Ministry of Electronics and Information Technology (MeitY), cyber intrusions in the country could have links with Pakistan, China, North Korea, Russia, and the US, among others.

While phishing and spear, or targeted, phishing attacks have been around for well over a decade, both attacks have become far more elaborate. On the other hand, India's cyber defences remain porous.

As of 2014, MeitY had already introduced a stringent email policy, which mandated that all official communications only be carried out through email services provided by the National Informatics Centre (NIC). The policy also prescribed various guidelines for account management and security. In addition, MeitY implemented two-factor authentication (2FA) for checking emails.

Seven years on, however, official email addresses are still vulnerable to bad actors, both foreign and domestic. Compliance with the email policy has been left to the discretion of bureaucratic leadership in the government's various ministries and organisations. The policy is also outdated and must be revised to keep up with the evolving nature of cyber threats.

Adoption of 2FA protocols was even more lax. Never mind civilian ministries, even India's defence ministry did not enforce 2FA until earlier this year. Even this happened after the phishing attacks in February, according to an executive working closely with a defence ministry-linked cyber incident response team.

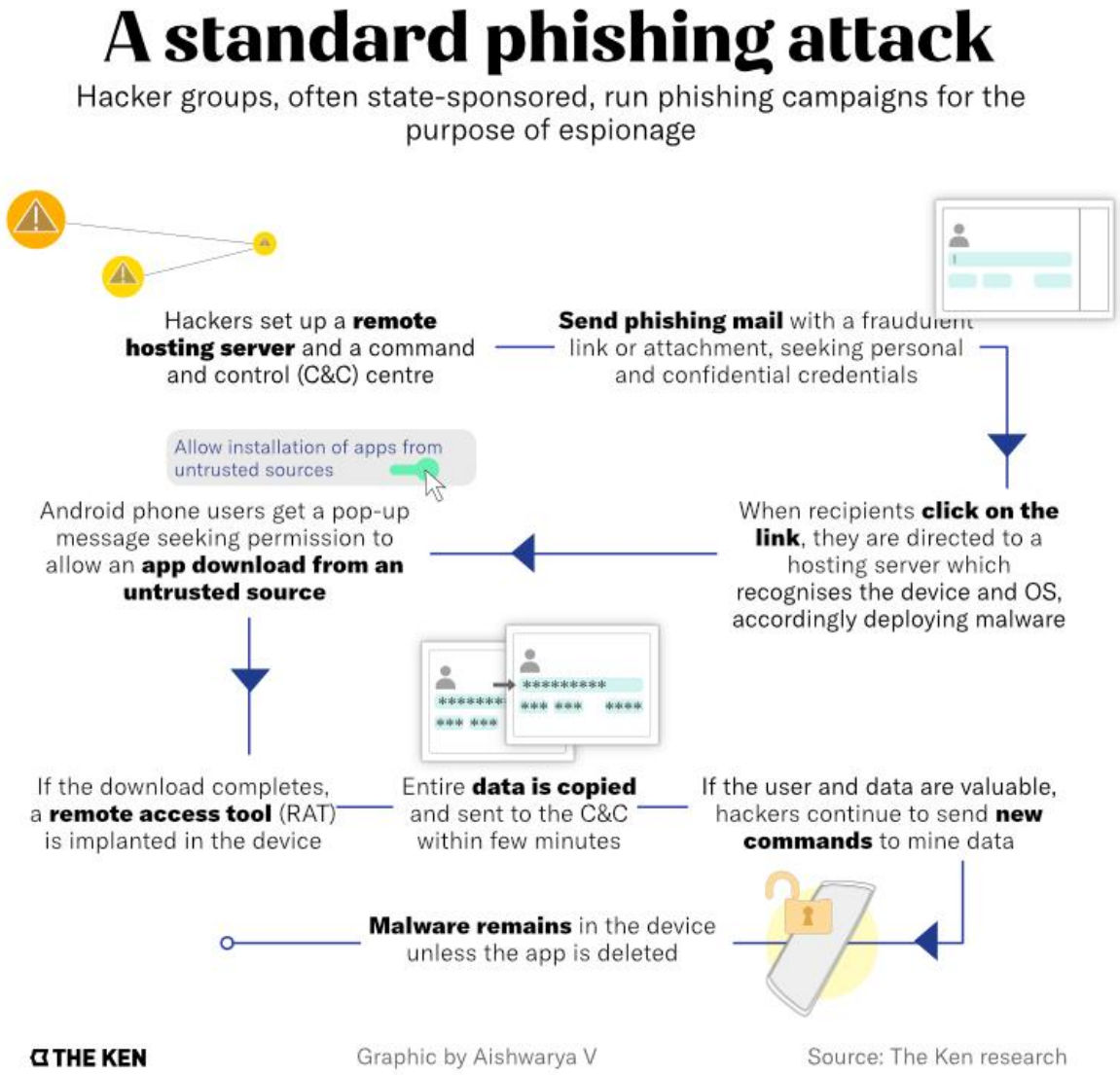
To make matters worse, critical agencies such as the NIC—which manages the entire network and IT infrastructure of the government—remain understaffed and often underfunded, says a former senior official who worked closely with the National Security Council Secretariat (NSCS). All told, there are barely 50 executives in the Computer Emergency Response Team (CERT) at NIC. Almost all of them are contractual staff from advisory firms such as PricewaterhouseCoopers and Deloitte. These workers barely get the industry average in terms of remuneration, multiple sources told *The Ken*.

The art of breaching

According to a senior official with the Delhi Police, NIC witnessed a massive breach in September 2020 after a computer belonging to a MeitY official was compromised. The login credentials were then used to send malware through NIC's email service to over 1,000 email accounts of government officials.

The Ken was unable to determine how many of the targeted officials fell victim to the attack. Questions sent to NIC about this attack went unanswered. According to reports, computers containing information related to Indian Prime Minister Narendra Modi as well as National Security Advisor Ajit Doval were compromised.

The attack was orchestrated by a known hacker group with Advanced Persistent Threat, or APT, capabilities. This category of hackers is usually state-sponsored and capable of infiltrating systems without being detected. The group that carried out the September attacks wasn't particularly elite, though. Their malware was sophisticated yet detectable as it was sent through email, said sources working closely with MeitY.



Over the years, these attacks have become more common as hackers have gotten more sophisticated in their phishing and spoofing attempts, says an official who works closely with MeitY.

Depending on the nature of the attack, a lot of effort goes into targeting individuals. Hackers monitor the social media and web presence of government and armed forces officials. They are profiled, tracked, and accordingly targeted based on their perceived susceptibility.

In some cases, hackers employ social engineering—befriending an employee of the targeted organisation and passing on a pen drive or file that could compromise her login credentials. At other times, hackers will simply compromise devices such as WiFi routers, CCTV cameras, etc. Once the breach is successful, hackers silently carry out surveillance until the time comes for them to use the compromised systems for their own ends.

Even if one government user is compromised, that's a significant win for hackers. The compromised user's credentials are used to send out emails with malware attachments or links to other official accounts. Since the sender is a trusted government email account holder, other recipients are likely to be ensnared. Around February, when defence personnel were being targeted by hackers, sources close to the defence ministry told *The Ken* that close to 50 military personnel were falling prey to phishing emails every day.

According to the executive working closely with the defence incident response team, military personnel have long been targets for bad actors. "When they (incident response team) were informed [about the February attacks], they didn't look surprised," says the executive. He says the unit is exhausted from dealing with these kinds of phishing attempts. Every time agencies identify these breaches and resolve them, the next wave of attacks begin.

The lack of basic cybersecurity hygiene only makes things easier for hackers. "They don't have to go to such levels of sophistication. People fall prey to simple phishing and spoofing," said the official working closely with MeitY.

Locks and keys

Despite MeitY issuing an email policy prohibiting official communications via private email services such as Gmail or Rediff, these rules are often flouted. Several officials weigh the convenience of these feature-rich services over the safety and security of government email networks.

Senior home and defence ministry officials also use WhatsApp to discuss official matters, according to multiple executives within the government and cybersecurity organisations. Even when it comes to classified information, which, according to the government's own guidelines, is not supposed to be sent out via email, rules are often ignored. "Documents as sensitive as Cabinet notes are exchanged over mail, and for all we know, on WhatsApp too," said the former official who worked closely with NSCS quoted earlier.

To put in place basic controls, the NIC introduced a 2FA system called *Kavach* (Hindi for 'shield'), which was procured from Delhi-based IT services firm Innefu Labs. Under this system, once a government official enters her email password, a one-time password (OTP) is sent to her mobile device. This OTP is ultimately what grants her access to her official email account.

Reality check

According to sources close to NIC, the organisation has procured less than 7 lakh user licences for Kavach. According to Google Playstore, however, there are just over 1 lakh downloads of Kavach.

In January, the Indian CERT, or CERT-In, issued another circular reiterating the importance of 2FA protocols. However, while this provides an additional layer of security, it only goes so far. "What if the system or the device has already been compromised? What if the hackers have already deployed a remote access tool? It won't matter what lock you put in if thieves are already in," says the former official.

NIC has also introduced geo-fencing, which ensures that users outside India are not able to access government email services managed by the agency. In cases where such access is required, prior approval from officials is mandated.

Geo-fencing, however, is a hollow measure in today's world. Bypassing it has become child's play thanks to cloud computing. An individual can buy web servers from a cloud provider with data centres in India and use these to access NIC's email services, multiple cybersecurity researchers told *The Ken*. In November last year, this is exactly what happened when NIC's email network was breached yet again. The incident went unreported. Hackers used a Noida-based

cloud company server to bypass geo-fencing, according to an executive at a Delhi-based cyber security firm. The server was paid for in Bitcoin, ensuring there was no trail back to the buyer. NIC didn't respond to queries from *The Ken.*

Plugging the holes

Email is hardly the only way in for hackers. However, it is one of the easiest avenues to protect. This makes the constant breaches a needless occurrence, eating into the time and energy of those staffing India's cyber defences.

While NIC's security controls have improved over the years, there is much more that needs doing. Sources close to MeitY believe the ministry and CERT-In can do more to enforce existing controls and add new ones. When a malware attachment is received in an NIC inbox, it should generate an alert. In addition, there's a need for protection on each user's devices, and while MeitY's guidelines previously prescribed antivirus software, there is now a need to upgrade to malware detection systems.

Ultimately, though, there's only so much MeitY and NIC can do. There's also a need for buy-in from ministries and agencies. This, after all, is why MeitY's 2FA and email guidelines ultimately amounted to little. The solution to this problem already exists. Under the Information Technology Rules, 2018, MeitY mandated that every single organisation and ministry must have a chief information security officer (CISO). The CISO is expected to create awareness and ensure that basic hygiene and standard operating procedures are followed in cybersecurity.

However, even after several years, there is no official document or notification that lays out the eligibility for the position. At present, anyone can be designated as a CISO, and it is often an additional responsibility. "Several ministries have appointed CISOs, but these officials have no clue about their mandate or roles and responsibilities," said the official working closely with MeitY.

There is also the larger problem of a lack of resources for the fight at hand. "Cyber defence is a costly affair. The right agencies should be provided with greater funding. And once funds are there, it should be used judiciously. Right now both are lacking," the former official who worked closely with NSCS said. The manpower shortage is also a major issue. With such a limited roster, senior officials in NIC's CERT handle multiple responsibilities, with little accountability in the system as a result.

Already, hacker groups are selling the login credentials of compromised users on dark web forums. *The Ken* has seen screenshots showing the email credentials of thousands of government officials, which are up for sale on these forums for just a few dollars. These could easily be purchased by bad actors and used to launch the next wave of attacks. If India doesn't want to relive the February hacks, it would do well to at least shore up its cyber defences.