

India's largest IT services company is hit by a hacker '

The giant in the field of providing IT services in the world's second most populous country, Wipro Ltd, based in Bengaluru, Karnataka, India, has become the latest name and also the most lucrative. join the list of businesses that are victims of phishing attacks in 2019.

The giant in the field of providing IT services in the world's second most populous country, Wipro Ltd, based in Bengaluru, Karnataka, India, has become the latest name and also the most lucrative. join the list of businesses that are victims of phishing attacks in 2019.

Wipro Limited is a multinational corporation providing information technology services, consulting and business processes. With sales of up to 8.4 billion USD in 2018, this is also one of India's largest IT businesses. According to the initial report from Wipro's own security team, the company's system was compromised and it was the result of a large phishing campaign targeting employees of this famous IT group. .



1. [Infographic] How to recognize and prevent Phishing attacks

It did not stop there, by analyzing some suspicious activities from the accounts of employees, of Wipro's internal IT team also found that attackers could advance. operating small campaigns targeting Wipro's customers in order to discredit and directly damage the company financially. Coincidentally, Wipro had previously scheduled a quarterly review of business results with all stakeholders on the same day when the incident occurred.

"We have discovered some unusual activities that appear in some of the employee accounts on the company's intranet system, which are more likely to originate from a campaign. When the incident was discovered, we quickly began an investigation, pinpointing the affected users and at the same time taking corrective actions to

prevent and In addition, the company's security team has also collected and monitored advanced security intelligence to strengthen the security wall for The whole system ', Vipin Nair, representative of WiPro shared.



1. Malicious ad campaigns abuse Chrome to steal 500 million iOS user sessions

With the cause of the incident being gradually revealed, WiPro announced that the company had decided to completely stop using its current email system and replace it with a filtering email solution as well as discovering fraudulent agents better - a tough and timely decision of India's largest IT business.

The WiPro side suspects that this is a spear phishing campaign, because the analysis shows that phishing messages are customized to make them highly persuasive, leading to WiPro employees being easily fooled. .

'We currently have strong internal processes and an advanced security technology system that can detect fraudulent attempts and protect ourselves from such attacks. WiPro has always kept track of its entire infrastructure at a high level of alert to deal with any potential network threats, 'Nair Vipin added.



1. 25% of "out-of-the-box" phishing emails are the default security of Office 365

Rajan Kohli, chairman of WiPro's Board of Directors, stressed that cyber defense is one of the areas that this group will continue to promote investment as a pillar in the operating structure. In particular, investing in the application of better security technologies and continuously upgrading the network will be the key tasks, by detecting time as well as responding to security incidents sooner or later. or slow will play an extremely important role, which may affect the survival of an entire system.

WiPro said it is contacting customers affected by the security incident, and is also committed to using all the tools and processes in its security control system to identify The object behind behind initiated this prestigious case.

'We are taking advantage of the industry's leading cyber security measures, and collaborating with the ecosystem of our partners to collect and monitor intelligence about the attack, thereby finding a dynamic. the true identity and identity of the person behind this incident. WiPro is partnering with a reputable computer forensic company, working independently to support investigation, as well as continuing to monitor its business organization and infrastructure at a level of vigilance. Highest ', WiPro representative said in a press release.



1. Danger: Hackers can target medical devices, change medical examination and treatment results

About 11 Fortune 500 companies are Wipro customers who have been affected by this security issue. Wipro is a large enterprise operating in the IT services sector with more than 170,000 employees globally, and is an important partner of many companies on the list of the largest US businesses and the largest in the world. .

You finished reading the article "**India's largest IT services company is hit by a hacker** " edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.