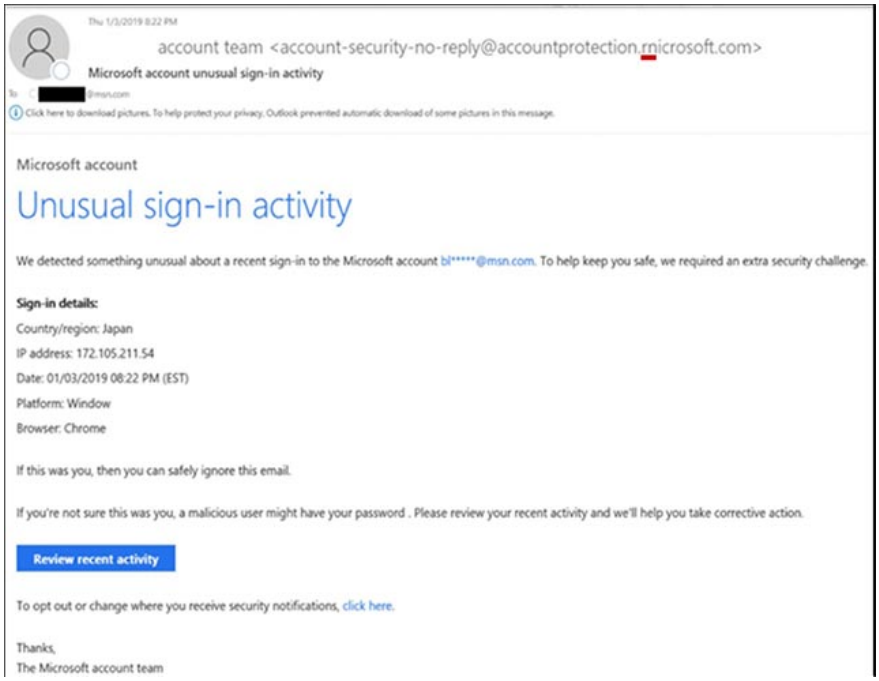
Microsoft successfully rescued 50 domain names from the notorious hacker group

Another great victory for Microsoft against state-sponsored hackers.

Add a resounding victory for Microsoft against the sponsored hacker groups. The East Virginia District Court recently issued a decision agreeing to allow Microsoft to confiscate 50 domain names from the notorious Thallium hacker group.

Thallium is a large hacker organization with strong ties to the Korean government. The group designed many malicious networks, which are used to target identified victims and then compromise online accounts, infect malware on computer systems, compromise network security. and stealing sensitive information from victims. The Thallium targets are primarily government officials, university staff, academics, members of world peace and human rights organizations, and working individuals. in the nuclear field. Most targets are in the United States, Japan and South Korea.

Thallium often tries to trick the victim through a technique called spear phishing. By collecting targeted personal information through social media accounts, in networks from relevant organizations and other public sources, Thallium can create an extremely specialized phishing email. You can now deceive a victim to deceive the victim in response to the request outlined in the email. The email content may look legitimate at first glance, but a closer review shows that Thallium has faked Microsoft by combining the letters' r 'and' n 'so that when placed next to each other will look like the letter' m ', such as' rnicrosoft.com'.



The link in the fake email of Thallium will redirect the user to a website that requires credentials for authentication, then they will use this information to log in to the victim account. After successfully penetrating the victim's account, Thallium can review emails, contacts, calendar appointments and anything else they are interested in. In addition, they often create a new mail forwarding rule in the victim account settings. This mail forwarding rule will forward all new emails the victim receives to Thallium-controlled accounts. By using forwarding rules, Thallium can continue to access any email the victim receives, even after this account password is updated.

In addition to hijacking unauthorized login credentials, Thallium also uses malware to infect systems and steal data. The two types of malware commonly used by this group are called 'BabyShark' and 'KimJongRAT.'

To protect against these threats, Microsoft recommends users enable two-factor authentication on all personal and business email accounts they hold. Second, users need to learn how to detect phishing scams and protect themselves from them. Finally, turn on security alerts for links, files from suspicious websites and carefully check email forwarding rules on your account.