Microsoft takes court action against fourth nation-state cybercrime group - Microsoft On the Issues

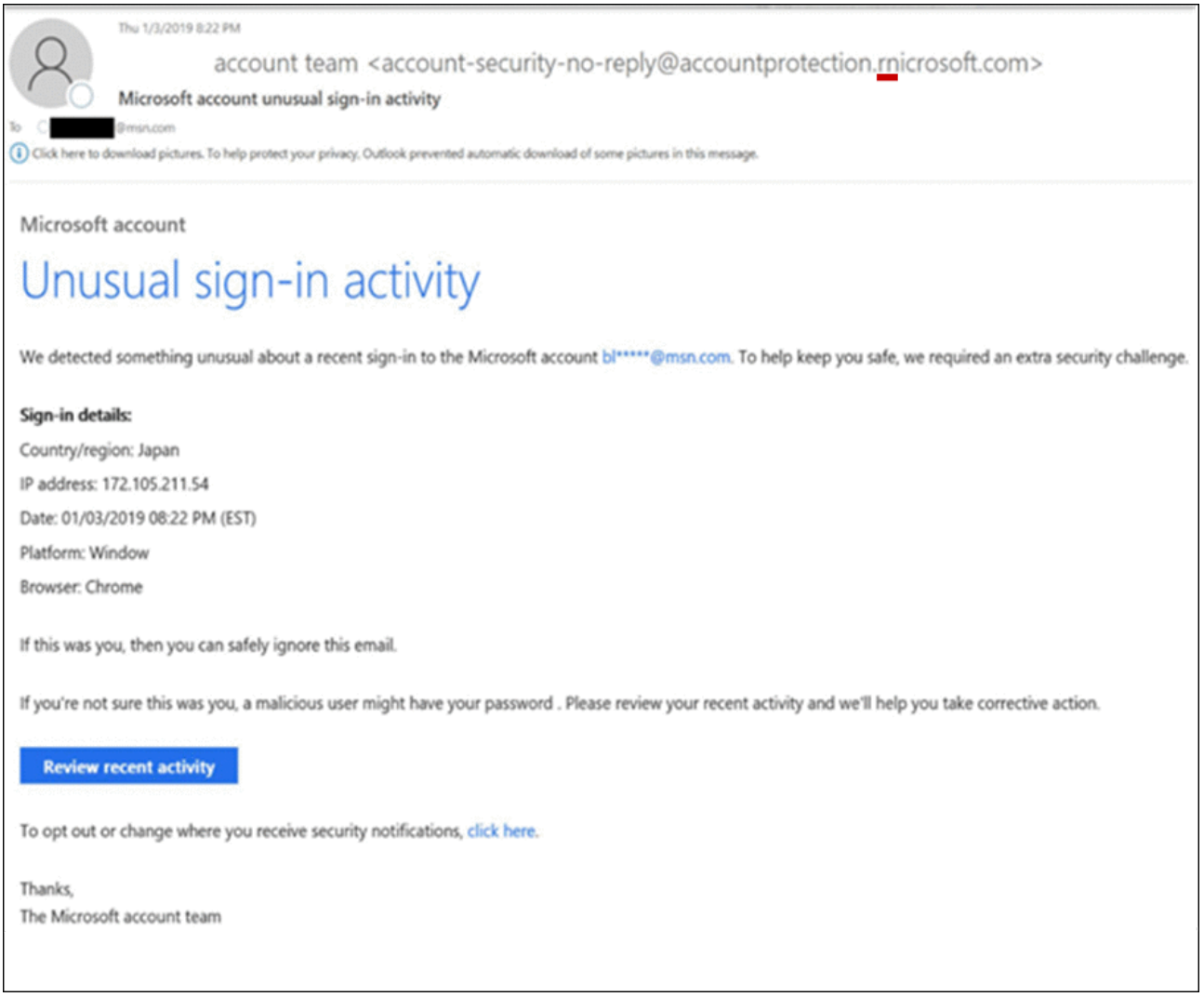
By Tom Burt

Published: 2019-12-30 · Archived: 2026-04-05 18:49:49 UTC

On December 27, a U.S. district court unsealed documents detailing work Microsoft has performed to disrupt cyberattacks from a threat group we call Thallium, which is believed to operate from North Korea. Our court case against Thallium, filed in the U.S. District Court for the Eastern District of Virginia, resulted in a court order enabling Microsoft to take control of 50 domains that the group uses to conduct its operations. With this action, the sites can no longer be used to execute attacks.

Microsoft's Digital Crimes Unit (DCU) and the Microsoft Threat Intelligence Center (MSTIC) have been tracking and gathering information on Thallium, monitoring the group's activities to establish and operate a network of websites, domains and internet-connected computers. This network was used to target victims and then compromise their online accounts, infect their computers, compromise the security of their networks and steal sensitive information. Based on victim information, the targets included government employees, think tanks, university staff members, members of organizations focused on world peace and human rights, and individuals that work on nuclear proliferation issues. Most targets were based in the U.S., as well as Japan and South Korea.

Like many cybercriminals and threat actors, Thallium typically attempts to trick victims through a technique known as spear phishing. By gathering information about the targeted individuals from social media, public personnel directories from organizations the individual is involved with and other public sources, Thallium is able to craft a personalized spear-phishing email in a way that gives the email credibility to the target. As seen in the sample spear-phishing email below, the content is designed to appear legitimate, but closer review shows that Thallium has spoofed the sender by combining the letters "r" and "n" to appear as the first letter "m" in "microsoft.com."



The link in the email redirects the user to a website requesting the user's account credentials. By tricking victims into clicking on the fraudulent links and providing their credentials, Thallium is then able to log into the victim's account. Upon successful compromise of a victim account, Thallium can review emails, contact lists, calendar appointments and anything else of interest in the compromised account. Thallium often also creates a new mail forwarding rule in the victim's account settings. This mail forwarding rule will forward all new emails received by the victim to Thallium-controlled accounts. By using forwarding rules, Thallium can continue to see email received by the victim, even after the victim's account password is updated.

In addition to targeting user credentials, Thallium also utilizes malware to compromise systems and steal data. Once installed on a victim's computer, this malware exfiltrates information from it, maintains a persistent presence and waits for further instructions. The Thallium threat actors have utilized known malware named "BabyShark" and "KimJongRAT."

This is the fourth nation-state activity group against which Microsoft has filed similar legal actions to take down malicious domain infrastructure. Previous disruptions have targeted Barium, operating from China, Strontium, operating from Russia, and Phosphorus, operating from Iran. These actions have resulted in the takedown of hundreds of domains, the protection of thousands of victims and improved the security of the ecosystem.

As we've said in the past, we believe it's important to share significant threat activity like that we're announcing today. We think it's critical that governments and the private sector are increasingly transparent about nation-state activity so we can all continue the global dialogue about protecting the internet. We also hope publishing this information helps raise awareness among organizations and individuals about steps they can take to protect themselves.

Microsoft applies the knowledge we have collected from tracking Thallium activity to add protections for our customers in all of our security products. You can protect yourself from these types of attacks in at least three ways. We recommend, first, that you enable two-factor authentication on all business and personal email accounts. Second, learn how to spot phishing schemes and protect yourself from them. Third, enable security alerts about links and files from suspicious websites and carefully check your email forwarding rules for any suspicious activity.

Tags: cyberattacks, DCU, MSTIC, Thallium, The Digital Crimes Unit

---