Microsoft Storm-1152 Crackdown: Stopping Threat Actors

securityboulevard.com/2023/12/microsoft-storm-1152-crackdown-stopping-threat-actors/

by Wajahat Raja on December 29, 2023 December 29, 2023

In a significant stride against cybercrime, Microsoft has declared victory in dismantling cybercrime operations of Storm-1152. This group, a major player in the cybercrime-as-a-service (CaaS) ecosystem, was involved in selling access to fraudulent Outlook accounts, impacting Microsoft and its users. This blog explores the details of this Microsoft Storm-1152 Crackdown and the potential implications for the broader cybersecurity landscape.

Microsoft Storm-1152 Crackdown

Microsoft's investigation revealed that Storm-1152, tracked as a key player in the CaaS landscape, operated by creating approximately 750 million fraudulent Microsoft accounts through its *"hotmailbox.me"* service. The illicit earnings amounted to millions of dollars, causing substantial damage to Microsoft.

The group specialized in using Internet 'bots' to deceive Microsoft's security systems, opening Outlook email accounts in fictitious usernames, and then selling these fraudulent accounts to cybercriminals. However, Microsoft has employed advanced strategies for combating cyber threats, leveraging cutting-edge technology to ensure a secure digital environment for users worldwide.

The Role Of CAPTCHA Solvers

Beyond fraudulent accounts, Storm-1152 offered rate solver services for CAPTCHAs, such as *“1stCAPTCHA,” “AnyCAPTCHA,”* and *“NoneCAPTCHA.”* These services were marketed as tools to bypass any type of CAPTCHA, enabling fraudsters to exploit Microsoft’s online environments and those of other enterprises.

Connections To Ransomware And Extortion

Microsoft identified several ransomware and extortion groups leveraging Storm-1152’s services, including the notorious Scattered Spider (Octo Tempest) group. Scattered Spider, previously linked to attacks on Okta and the MGM Resorts breach, was found to be connected to massive ransomware attacks against flagship Microsoft customers. These attacks resulted in service disruptions, inflicting hundreds of millions of dollars in damage.

Microsoft’s Swift Response

On December 7, Microsoft obtained a court order from the Southern District of New York, allowing it to seize Storm-1152’s U.S.-based infrastructure and domains. This included the shutdown of *“hotmailbox.me”* and disruption of services like for CAPTCHAs mentioned before. Additionally, Microsoft targeted social media accounts used by Storm-1152 for promoting its illicit services. The effectiveness of Microsoft’s cyber threat response has no doubt ensured robust security measures against evolving online threats.

Identifying The Culprits

Microsoft, in a decisive move, identified the individuals behind Storm-1152’s operations. Duong Dinh Tu, Linh Van Nguyễn (also known as Nguyễn Van Linh), and Tai Van Nguyen were named as the perpetrators, and they are based in Vietnam. By revealing the faces behind the cybercrime network takedown, Microsoft aims to deter criminal behavior and raise the cost of doing business for cybercriminals.

Microsoft And Law Enforcement Collaboration

Arkose Labs, a San Francisco-based cybersecurity company, played a crucial role in assisting Microsoft during the takedown. Kevin Gosschalk, the founder and CEO of Arkose

Labs, highlighted Storm-1152's unique approach of operating as an internet-going concern, openly providing training and customer support for its tools.

Industry Experts On Microsoft Storm-1152 Crackdown

Craig Jones, Vice President of Security Operations at Ontinue, acknowledges the significance of Microsoft's action against Storm-1152. However, he emphasizes the nuanced nature of its long-term effectiveness. While disrupting current operations is a notable achievement, the adaptability and resilience of cybercrime groups pose ongoing challenges.

Hacking Group Targeted By Microsoft

Jones points out that the fight against cybercrime demands persistent and collaborative efforts across the digital ecosystem. The impact of the Microsoft Storm-1152 crackdown relies on the sharing of information and coordinated efforts among tech companies, law enforcement, and intelligence agencies.

The fight against cybercrime requires continuous vigilance and collaborative efforts to stay ahead of evolving threats. Microsoft's actions serve as a reminder of the ongoing battle to protect customers and online users from the ever-changing global cybersecurity efforts.

Conclusion

Microsoft's successful takedown of Storm-1152 marks a significant victory in the fight against cybercrime. While the impact of legal actions against cybercrime is evident, the long-term effectiveness depends on sustained efforts and collaboration within the cybersecurity community. As we celebrate this win, it serves as a poignant reminder that the battle against cyber threats is ongoing, requiring vigilance and proactive measures, adaptability, and a united front from industry players, law enforcement, and cybersecurity experts.

The sources for this piece include articles in The Hacker News and TechCrunch.

The post Microsoft Storm-1152 Crackdown: Stopping Threat Actors appeared first on TuxCare.

*** This is a Security Bloggers Network syndicated blog from TuxCare authored by Wajahat Raja. Read the original post at: https://tuxcare.com/blog/microsoft-storm-1152-crackdown/