On 13 April, the Free Software Movement of India, a coalition of organisations promoting the adoption of free software, was allowed access to its Twitter account, almost 17 days after the social-media platform locked it out. Twitter had locked the account of FSMI on 27 March, for a tweet that referred to a data breach of customers' details at Big Basket, an online grocery store. On 30 March, Robert Baptiste, a France-based cyber-security expert, who goes by the name Elliot Alderson on Twitter, too, was locked out of his account for a tweet referring to a data breach at Mobikwik, a digital payments platform. The next day, another cyber-security researcher Rajshekhar Rajaharia faced similar action by Twitter for a tweet regarding the MobiKwik breach, which affected the personal data of almost ten crore users. This was the second time in a month that Rajaharia had been locked out of his account for tweets on MobiKwik. In each instance, Twitter told the accounts that their tweets violated its rules against posting private information.

Baptiste and Rajaharia's accounts were restored in less than 12 hours?both of them deleted their respective tweets. Rajaharia shared a screenshot which showed that his account was locked for 12 hours for violating Twitter's private-information policy, but he told me his account was reinstated after about four hours. FSMI, which was locked out of its account for a tweet dated 12 December 2020, chose not to delete the post and Twitter later took down the tweet. Strangely, another tweet by FSMI, from 11 November, which refers to the same content, remained visible on the account.

In each case, it was unclear how the tweets on data breaches violated the rules against posting private information, and if Twitter took action on its own, or whether some other individual or organisation reported these accounts. In an email response to The Caravan on 31 March, Twitter did not answer specific questions on who reported FSMI's account and only said, ?The referenced account was correctly actioned for violating the Private information policy.? However, on 13 April, Twitter sent an email to FSMI, informing them that their account had
been restored and admitted that "After reviewing your account, it looks like we made an error."

- **Cybereason Discovers Global Botnet Campaign Leveraging Microsoft Exchange Vulnerabilities**[3]

  Cybereason, the leader in future-ready attack protection, today announced the discovery of a widespread, global campaign seeking to propagate the stealthy Prometei Botnet, by targeting organizations with a multi-stage attack to steal processing power to mine bitcoin. The threat actors, who appear to be Russian speakers, are taking advantage of previously disclosed Microsoft Exchange vulnerabilities leveraged in the Hafnium attacks to penetrate networks.

  Prometei has a complex infrastructure designed to ensure persistence on infected machines. While Prometei was first reported on in July 2020, Cybereason assesses that the botnet actually dates back to at least 2016, a year before the now infamous WannaCry and NotPetya malware attacks that affected more than 200 countries and caused billions in damages.

  Prometei continues to evolve with new features and tools regularly observed.

- **Prometei Botnet Exploiting Microsoft Exchange Vulnerabilities**[4]

  Recently, the Cybereason Nocturnus Team responded to several incident response (IR) cases involving infections of the Prometei Botnet against companies in North America, observing that the attackers exploited recently published Microsoft Exchange vulnerabilities (CVE-2021-27065 and CVE-2021-26858) in order to penetrate the network and install malware.

  Prometei is a modular and multi-stage cryptocurrency botnet that was first discovered in July 2020 which has both Windows and Linux versions. To achieve their goal of mining Monero coins, Prometei uses different techniques and tools, ranging from Mimikatz to SMB and RDP exploits and other tools that all work together to propagate across the network.

  Although Prometei was officially discovered in mid-2020, the Cybereason Nocturnus Team found evidence that Prometei might date back as far as 2016 and has been evolving ever since, adding new modules and techniques to its capabilities. The latest versions of Prometei now provide the attackers with a sophisticated and stealthy backdoor that supports a wide range of tasks that make mining Monero coins the least of the victims' concerns.

**Security**

Source URL: [http://www.tuxmachines.org/node/150333](http://www.tuxmachines.org/node/150333)

Links:

[1] [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)