Deepanshu Kasaba Kher **2021**

Crime: Intentional Damage to a Protected Computer
Court: Southern District of California
State: CA
Result: Pled Guilty
Sentence: 24 months
Fine: $567,084
Year of Conviction: 2021
Age at conviction: 32
Employee Type: Industry Employee
Military: n/a
Job: Information Technology Specialist
Country of Concern: n/a
Targeted Technology: Computers

Indicators: Access Attributes, Professional Lifecycle and Performance, Foreign Considerations

Cyber Intrusion / Sabotage

WHAT HAPPENED:
Deepanshu Kher was employed by an information technology consulting firm from 2017 through May 2018. In 2017, the consulting firm was hired by the Carlsbad Company to assist with its migration to a Microsoft Office 365 (MSO365) environment. In response, the consulting firm sent its employee, Kher, to the company's Carlsbad headquarters to assist with the migration.

The company was dissatisfied with Kher's work and relayed their dissatisfaction to the consulting firm soon after Kher's arrival. In January 2018, the consulting firm pulled Kher from the company's headquarters. A few months later, on May 4, 2018, the firm fired Kher, and a month after that, in June 2018, Kher returned to Delhi, India.

On August 8, 2018, two months after his return to India, Kher hacked into the Carlsbad Company's server and deleted over 1,200 of its 1,500 MSO365 user accounts. The attack affected the bulk of the company's employees and completely shut down the company for two days.

Unfortunately, even after those two days, the problems remained. Employees were not receiving meeting invites or

cancellations, employees' contacts lists could not be completely rebuilt, and affected employees could no longer access folders to which they previously had access. The Carlsbad Company repeatedly handled multitudes of IT problems for three months.

Kher was arrested when he flew from India to the United States on January 11, 2021, unaware of the outstanding warrant for his arrest.

Deepanshu Kher pled guilty to Intentional Damage to a Protected Computer and was sentenced to two years in prison.

INDICATORS:
Access Attributes – Kher had privileged access to the Carlsbad Company servers

Professional Lifecycle and Performance – Kher was removed from the MSO365 project due to unsatisfactory performance and was later fired

Foreign Considerations – Kher was an Indian national and therefore possessed an Indian passport. He also had close family members in India

IMPACT:
As the company's Vice President of Information Technology (IT) explained, the impact was felt inside and outside the company. Employee accounts were deleted, and employees could not access their email, contacts lists, meeting calendars, documents, corporate directories, video and audio conferences, and the virtual teams environment necessary for them to perform their jobs. Outside the company, customers, vendors and consumers were unable to reach company employees (and the employees were unable to reach them). No one was able to inform these buyers what was going on or when the company would be operational again.

The Vice President of IT for the Carlsbad Company said, "In my 30-plus years as an IT professional, I have never been a part of a more difficult and trying work situation."

ADDITIONAL INFO:
"The FBI was able to identify, arrest, and prosecute Deepanshu Kher, despite the fact that he committed this harmful hack while outside the United States. This case shows the commitment, expertise, and reach of

the FBI in working cyber intrusion cases," said Suzanne Turner, Special Agent in Charge of the FBI's San Diego Field Office.

In 2019, Kher applied for a visa to visit his brother in the United States. The FBI had obtained a court order for assistance from the travel company Sabre. As a result of that order, Sabre notified the FBI when Kher booked travel to the US. Kher was arrested when he flew from India to the United States on January 11, 2021, unaware of the outstanding warrant for his arrest.

Companies should develop a relationship with the FBI and local law enforcement prior to a cybersecurity incident and incorporate them into incident response plans. In this case, the victim company's swift notification and cooperation with the FBI contributed greatly to the successful outcome. Living in a digital world, it is important to get ahead of the threats, and be proactive and predictive in the way we approach cybersecurity.

If victimized in a cybersecurity incident, the FBI encourages companies to immediately contact the FBI. Specialized cyber agents will work with companies to protect company information and the personal data of its customers.