THE STATE SPONSORED THREAT

THE INTERNATIONAL SCIENTIST TURNED CORPORATE SPY

When a foreign national working as a scientist for a Fortune Global 200 Company ($54 billion in annual revenue) asked his employer's IT department to "wipe the drive" on his laptop after a trip to China, company officials became suspicious and contacted SpearTip.

Our operatives quickly sprang into action, interviewing the scientist and analyzing his laptop. While the scientist claimed to be virtually computer illiterate, his laptop told a vastly different story.

After a thorough and detailed investigation, our cyber counterintelligence team revealed a calculated and carefully crafted case of international corporate espionage. Embedded within the laptop was sophisticated malware, created by the Chinese government, which had been used to breach secure company networks and systems, then extract valuable IP, trade secrets, and pre-patent data.

Even more concerning was the fact that the scientist lacked the necessary security clearance to obtain much of the compromised data.

Once the company's most sensitive secrets had been transferred to the scientist's laptop, the stolen research data, formulas and product information were rapidly uploaded to foreign agents, using highly sophisticated programs, again attributed to the government of China.

SpearTip immediately ended the threat, mitigating all malware and extracting it from the company's systems.

We then turned our attention to the scientist. During a series of interviews, the scientist revealed that he had been personally compromised through threats and intimidation. With the source of the espionage attack now in-hand, SpearTip provided the company with the necessary information to seek justice and re-gain control of their IP and formulas.

(As a matter of privacy and confidentiality, SpearTip never names clients when providing case studies.)