Tesla targeted in failed ransomware extortion scheme

29 August 2020, by Frank Bajak

In this Oct. 13, 2018 file photo, a sign marks the entrance to the Tesla Gigafactory in Sparks, Nev. Tesla CEO Elon Musk solved a mystery involving a 27-year-old Russian who prosecutors say flew to the United States to offer a major-company insider $1 million to assist in a ransomware extortion attack on the firm. According to the billionaire, the scheme took aim at the electric car company's 1.9 million-square-foot factory in Sparks, Nevada, which makes batteries for Tesla vehicles and energy storage units. (AP Photo/John Locher, File)

In a tweet, Tesla CEO Elon Musk solved a mystery involving a 27-year-old Russian, an insider at an unnamed corporation and an alleged million-dollar payment offered to help trigger a ransomware extortion attack on the firm.

Prosecutors declined to name the target, but Musk was happy to oblige. According to the billionaire, the scheme took aim at the electric car company's 1.9 million-square-foot factory in Sparks, Nevada, which makes batteries for Tesla vehicles and energy storage units.

"This was a serious attack," Musk tweeted Thursday night, responding to a Tesla blog post that detailed the brazen scheme.

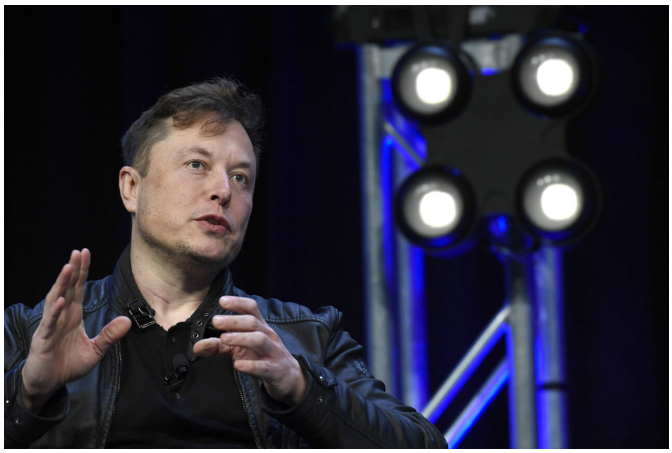
Defendant Egor Igorevich Kriuchkov tried to recruit a fellow Russian speaker who worked at the plant, according to a criminal complaint filed in U.S. District Court in Nevada.

Reaching out to the unnamed worker via WhatsApp in July, Kriuchkov allegedly flew to the United States with a Russian passport on a tourist visa and sought to entice the worker to betray Tesla. Kriuchkov allegedly took the worker, who he'd he'd first met in 2016, on a road trip to Lake Tahoe before offering the person $1 million to plant malware on computer systems at "Victim Company A." Kriuchkov floated the scheme at a Reno area bar on Aug. 3 after the two drank heavily until last call, the complaint says.

But the plant worker informed Tesla, which contacted the FBI and won the employee's cooperation. In subsequent meetings monitored and recorded by federal agents, Kriuchkov laid out a scheme to have the worker infect Tesla computers with a program that would steal valuable data before scrambling plant systems with ransomware, according to the complaint.

Kriuchkov was quoted as saying the inside job would be camouflaged with a distributed denial of service attack on plant computers from outside. Such attacks overwhelm servers with junk traffic. If Tesla didn't pay, the purloined data would be dumped on the open internet.

The complaint says Kriuchkov told the Tesla worker that his organization had executed similar "special projects" on other companies on multiple occasions, with one victim supposedly surrendering a $4 million ransom payment. According to the complaint, Kriuchkov added that his organization employed sophisticated encryption that would mask the Tesla worker's participation and mentioned that one hacker in his group was a high-level employee of a government bank in Russia.



In this March 9, 2020, file photo, Tesla and SpaceX Chief Executive Officer Elon Musk speaks at the SATELLITE Conference and Exhibition in Washington. In a tweet on Thursday, Aug. 27, Musk solved a mystery involving a 27-year-old Russian who prosecutors say flew to the United States to offer a major-company insider $1 million to assist in a ransomware extortion attack on the firm. According to the billionaire, the scheme took aim at the electric car company's 1.9 million-square-foot factory in Sparks, Nevada, which makes batteries for Tesla vehicles and energy storage units. (AP Photo/Susan Walsh, File)

The U.S. Attorney's office for Nevada would not comment on whether Kriuchkov or any of his associates may have had ties to the Russian government. Nothing in the criminal complaint suggested their motives were anything but financial.

Tesla is a lucrative target. It leads the U.S. in electric vehicle sales and the hackers could have obtained valuable information from battery chemistry to manufacturing techniques and costs. Tesla has said the factory has cut battery cell costs through innovative manufacturing.

Kriuchkov was arrested Aug. 22 after driving from Reno to Los Angeles, where the FBI said he planned to fly out of the country, He appeared in federal court there Monday and was charged with conspiracy to intentionally cause damage to a protected computer, said Nevada U.S. Attorney Nicholas Trutanich. A conviction could result in a sentence of five years in prison and a $250,000 fine. Court records did not immediately reflect the name of an attorney who could speak on Kriuchkov's behalf.

It is not clear in the documents if money changed hands. The criminal complaint and a supporting affidavit by investigating FBI Special Agent Michael Hughes describe a considerable amount of haggling over whether the unnamed Tesla worker would get some portion of his promised cut of the ransom in advance.

Tesla did not immediately respond to an email seeking comment.

Other suspected co-conspirators are identified in the complaint by nicknames including Kisa and Pasha; a person is identified as Sasha Skarobogatov.