Russian tourist offered employee $1 million to cripple Tesla with malware

reader comments

70 with 54 posters participating

Share this story

Tesla’s Nevada Gigafactory was the target of a concerted plot to cripple the company’s network with malware, CEO Elon Musk confirmed on Thursday afternoon.

The plan’s outline was divulged on Tuesday in a criminal complaint that accused a Russian man of offering $1 million to the employee of a Nevada company, identified only as “Company A,” in exchange for the employee infecting the company’s network. The employee reported the offer to Tesla and later worked with the FBI in a sting that involved him covertly recording face-to-face meetings discussing the proposal.

“The purpose of the conspiracy was to recruit an employee of a company to surreptitiously transmit malware provided by the coconspirators into the company’s computer system, exfiltrate data from the company’s network, and threaten to disclose the data online unless the company paid the coconspirators’ ransom demand,” prosecutors wrote in the complaint.

Musk: “This was a serious attack”

Until Thursday afternoon, the identity of Company A was

uncertain, although there was plenty of Twitter speculation—and several sourceless blog reports—that Tesla's site in Nevada was the target. In a Tweet responding to one of the unconfirmed reports, Musk wrote: "Much appreciated. This was a serious attack."

> *Much appreciated. This was a serious attack.*
>
> *— Elon Musk (@elonmusk)* ***August 27, 2020***

Tuesday's charging document, which was filed in federal court in Nevada, detailed an extensive and determined attempt to infect Company A's network. Defendant Egor Igorevich Kriuchkov, 27, allegedly traveled from Russia to Nevada and then met with the unnamed employee on multiple occasions. When Kriuchkov's initial $500,000 bid failed to clinch the deal, the defendant doubled the offer, prosecutors said.

Wining, dining, and boozing

According to the complaint, Kriuchkov wined, dined, and boozed the employee, and when discussing especially sensitive details, conducted conversations in cars. When FBI agents couldn't conduct physical surveillance in restaurants or bars, the employee recorded them.

One alleged meeting occurred on August 7 in a car Kriuchkov rented. Referring to the employee as CHS1—short for confidential human source No. 1—prosecutors described it this way:

> *During this meeting, which the FBI had consensually recorded, KRIUCHKOV reiterated some of the details of the criminal activity previously proposed to CHS1. KRIUCHKOV described the malware attack as he did before, adding that the first part of the attack (DDoS attack) would be successful for the "group" but the Victim Company's security officers would think the attack had failed. KRIUCHKOV again listed prior*

companies the "group" had targeted. KRIUCHKOV stated each of these targeted companies had a person working at those companies who installed malware on behalf of the "group." To ease CHS1's concerns about getting caught, KRIUCHKOV claimed the oldest "project" the "group" had worked on took place three and a half years ago and the "group's" co-optee still worked for the company. KRIUCHKOV also told CHS1 the "group" had technical staff who would ensure the malware could not be traced back to CHS1. In fact, KRIUCHKOV claimed the group could attribute the attack to another person at Victim Company A, should there be "someone in mind CHS1 wants to teach a lesson."

During the meeting, CHS1 expressed how concerned and stressed CHS1 had been over the request. CHS1 stated if CHS1 were to agree to install the malware, CHS1 would need more money. KRIUCHKOV asked how much, and CHS1 responded US $1,000,000. KRIUCHKOV was sympathetic to the request and said he understood, but would have to contact the "group" before agreeing to the request. KRIUCHKOV confided that the "group" was paying KRIUCHKOV US $500,000 for his participation in getting CHS1 to install the malware, and he was willing to give a significant portion of the payment (US $300,000 to US $450,000) to CHS1 to entice his involvement.

CHS1 said CHS1 would need money upfront to ensure KRIUCHKOV would not have him install the software and then not pay him. Again, KRIUCHKOV asked how much, and CHS1 responded US $50,000. KRIUCHKOV said this was an acceptable amount and a reasonable request but he would have to work on this because he only had US $10,000 with him due to U.S. Customs restrictions on the amount of money he could bring into the country. KRIUCHKOV also questioned what would prevent CHS1 from taking the up-front money and then not following through on installing the malware. CHS1 stated CHS1 was sure KRIUCHKOV or the "group" would figure a way to apply leverage against CHS1 to ensure CHS1 held up his end of the

> *arrangement. CHS1 and KRIUCHKOV discussed the timing of the next meeting, and KRIUCHKOV said he would return to Reno on or around August 17, 2020.*

Absolutely insane

Besides targeting an iconic car maker, the plot is notable for other reasons. One is its sheer audacity and recklessness. As security researcher and reformed teenage cybercrime hacker Marcus Hutchins noted on Twitter: "One of the benefit of cybercrime is criminals don't have to expose themselves to unnecessary risk by conducting business in person. Flying into US jurisdiction to have malware manually installed on a company's network is absolutely insane."

> *One of the benefit of cybercrime is criminals don't have to expose themselves to unnecessary risk by conducting business in person. Flying into US jurisdiction to have malware manually installed on a company's network is absolutely insane.*
>
> *— MalwareTech (@MalwareTechBlog)* ***August 27, 2020***

A chilling observation, from Craig Williams, director of outreach as Cisco's security arm Talos Labs, was what might have happened had the plot succeeded.

"This does bring into question the risk added if the system responsible for your self driving car comes under attacker control—due to malicious insider or otherwise," he wrote. "The entire thing is extremely exciting and concerning."

> *So I suppose this means my guess was correct. This does bring into question the risk added if the system responsible for your self driving car comes under attacker control — due to malicious insider or otherwise. The entire thing is extremely exciting and concerning.* ***https://t.co/oYKnDWKem1***

— *Craig Williams (@security_craig)* ***August 28, 2020***

Musk didn’t elaborate on his two-sentence Twitter confirmation, and Tesla representatives didn’t respond to an email seeking comment for this post.

The plot and its cast of characters—replete with villains, heroes and whatever Musk is—make for an interesting backstory and possibly a dramatic TV reenactment. For now, readers will have to content themselves with additional reading in Wednesday’s coverage of the complaint.

https://arstechnica.com/?p=1701893