Detroit Free Press

MSU: We won't pay hacker demanding ransom, threatening university over records

Samuel Zwickel, Detroit Free Press

Published 12:01 p.m. ET June 3, 2020 | **Updated 12:45 p.m. ET June 3, 2020**

Michigan State University said it doesn't plan to give into a hacker threatening to publish students' personal records and university financial documents if the university fails to pay an unspecified bounty this week.

MSU spokesperson Dan Olsen — citing the ongoing nature of the investigation — declined to answer questions about the amount of ransom money requested or the associated deadline.

University officials believe the latest breach occurred on Memorial Day and took relevant computer systems offline within hours of the intrusion, according to a news release. It compromised data associated with the Department of Physics and Astronomy, and information technology teams are coordinating with law enforcement to understand the scope of the breach. Investigators are notifying and providing support to affected MSU affiliates as they are identified.

The cybersecurity breach, known as a ransomware attack, first became public May 27 when a hacker-affiliated blog posted screenshots of files allegedly belonging to MSU affiliates. Images circulating on social media include a redacted passport and a list of transactions related to physics and astronomy projects. They also show a countdown clock that warns of "secret data publication" less than one week from when the screenshots were taken.

Although the hacker demands a ransom, administrators will not be paying it, MSU Police Chief Kelly Roudebush said in a statement.

"Paying cyber-intrusion ransoms perpetuates these crimes and provides an opportunity for the group to live another day and prey upon another victim," she said.

Michigan State Police are providing technical assistance with the investigation and sharing information with federal officials, according to department spokesperson Shanon Banner.

The present incident follows a 2016 data breach at MSU in which hackers accessed 400,000 records — including names, social security numbers, and university identification numbers — from a database of sensitive personal information. Following that incident, administrators offered to purchase identity protection services for affected parties.

Olsen wrote in an emailed statement that MSU is "continually updating" information security protections as technology evolves and educating employees on best practices in order to prevent such crises.

"Following the 2016 breach, a number of added measures were put in place to prevent similar future attacks. One of the key improvements was centralizing our IT infrastructure and enhancing our security programs and software," Olsen wrote. "Those were critical improvements to our systems and are, in part, why this was such an isolated incident."

More: Richmond school district shuts down in ransomware cyberattack

More: Latest tax scam holds your info for ransom. Here's how to spot it and other fraud

Hackers are known to target schools, hospitals, private businesses, and governments agencies with ransomware. Between 2013 and April 2019, American city and state governments suffered more than 169 such attacks, according to cybersecurity company Recorded Future.

In a traditional ransomware intrusion, hackers freeze the contents of an individual or network computer system and demand payment in order to regain access to compromised files. The variety plaguing MSU, which threatens the public release of sensitive data, is much less common, according to information technology experts.

Stanford researcher Gregory Falco, who specializes in cyber risk management, said there are three kinds of actors who tend to instigate such attacks: petty criminals who buy ransomware kits on the dark web, state-sponsored entities that often target critical infrastructure in order to sow chaos and organized crime rings aiming for a handsome profit. Despite an often-dire impact, they are “not super sophisticated” from a technical standpoint and can be triggered by as little as a negligent click, according to Falco.

“It’s really just often a matter of an employee or someone at the university clicking on a phishing email with a bad link,” he said. “And then it is able to kind of propagate throughout the network, and then you have a whole bunch of systems that are now shut down and compromised.”

It can be exceedingly difficult to determine the source of this kind of cyberattack. Hackers demand difficult-to-trace cryptocurrency payments — often worth tens to hundreds of thousands of United States dollars — and carefully cover their tracks. The most sophisticated efforts deliberately mislead law enforcement, according to Massachusetts Institute of Technology engineering professor and cybersecurity researcher Stuart Madnick.

“A really highly talented cyber hacker of this kind will lead so many wrong trails, cover their trail so well, that it is extremely hard to talk about suspicions,” Madnick said.

Lawrence Susskind — an MIT professor who studies negotiation — said there is a growing market for commercial “cyber insurance” policies that provide emergency consulting and cover ransom payments in the event of a breach. Because a third party technically pays off the demand, he explained, organizations often claim success without the stigma of capitulating to the criminals.

“The insurance company takes over, and it negotiates to try to get the amount down. And there’s a fixed amount that’s a cap on what they’ll pay,” Susskind said. “The [institution] stands up to say, ‘We refused to negotiate with those terrorists, but we managed with the help of outside assistance to get our data back.’ And they didn’t pay the ransom; the insurance company did.”

Several experts agreed that negotiating with hackers and ultimately proffering some form of bounty tends to be in victims’ best interest. In most cases, they explain, instigators follow through with their promise to resolve the problem upon receiving payment. In some cases, the consequences of refusing can be vastly more costly for victims.

“You should always consider how much you’re going to be ending up paying to consulting services, and in breach of contracts and lawsuits and all the things that you’ll end up dealing with,” Falco said.

Falco, Madnick, and Susskind referred to a particularly severe incident last May in which the City of Baltimore refused to pay about $76,000 to free locked files. That devastated city computer systems, and the Baltimore budget office projected that restoring the network could cost taxpayers more than $18 million.

However, Banner noted that the Michigan State Police do not condone providing a ransom to criminal groups.

“In all instances, we advise organizations against paying a ransom, as it only encourages and supports continued nefarious activities,” she said.

A ransomware attack is one of university administrators’ “greatest nightmares” and motivates extensive precautions, according to Jason Williams, who oversees information security at the University of Notre Dame. Williams said Notre Dame invests in “cyber hygiene” training for affiliates, has a cyber insurance plan and even runs simulations to test decision-making protocols for a hacking emergency. He added that leadership lacks consensus as to whether it would disburse a bounty.

“Do we pay the ransom or not — very interesting conversation. It’s split within the organization,” Williams said. “I’ve never actually had to put this into practice. And I would like not to have to do this.”

Samuel Zwickel is a news intern with the Detroit Free Press. Follow him on Twitter @samuel_zwickel.