School Safety Newsletter

Volume 6, Issue 12 July 2019

Louisiana Governor Declares Statewide Cybersecurity Emergency: Ongoing Malware Attack Impacting Three North Louisiana School Districts

KSLA, July 24, 2019

https://www.ksla.com/2019/07/24/la-governor-declares-statewide-cybersecurity-emergency/

BATON ROUGE, La. (KSLA) — Louisiana Gov. John Bel Edwards has declared a statewide cybersecurity emergency.

There's an ongoing malware attack impacting three public school districts in North Louisiana — Sabine, Morehouse and Ouachita, the governor's office reports.

In response, the Governor's Office of Homeland Security and Emergency Preparedness has activated its crisis action team and the Emergency Services Function-17.

State officials were notified Wednesday and have been providing technical support ever since, said Christina Stephens, a spokeswoman for the governor's office.

"There have been some discussions with the school systems about what to look for and how to protect themselves. In addition, the Fusion Center at Louisiana State Police has provided some guidance to law enforcement and others about the threat. "

Louisiana State Police, the Louisiana National Guard, the state Office of Technology Services and other agencies are coordinating the response and determining future actions.

Sabine School District says the telephones at its Central Office also are being impacted. Staffers can call out but cannot receive calls. Parents are being advised to contact their children's schools if they need assistance.

The School District released the following statement Wednesday evening:

"The Sabine Parish School System was hit with an electronic virus early Sunday morning. This virus has disabled some of our technology systems and our central office phone system. The district staff reported this electronic viral attack to local law enforcement, state officials and the FBI. All available resources are being utilized to get the district systems back online. An investigation involving local, state and federal law enforcement is ongoing at this time. The school phone systems were not affected by this attack. The central office phone system is being repaired and service will be restored as soon as possible. According to the Louisiana Department of Education, several other school districts were attacked by the same virus this week."

— Sabine Parish School District

Eddie Jones, principal of Florien High School in Sabine Parish, said his technology supervisor got an alert on his phone about 4 a.m. Sunday about unusually high bandwidth usage, particularly considering the time of day and the summer break.

They were told a ransomeware virus was discovered installed on their system, he said.

Jones doesn't think any sensitive information was lost. What is lost, he said, is anything and everything housed solely on the School District's servers.

Protecting our future through information sharing

In This Issue

Louisiana Governor Declares Statewide Cybersecurity Emergency: Ongoing Malware Attack Impacting Three North Louisiana School Districts (Continued)

For Jones, he said that means 17 years of documents he created — speeches, test schedules, master schedules, etc.

This is the first time Louisiana has activated its emergency support function relating to cybersecurity.

So far, the state is coordinating with the FBI, state agencies and higher education partners.

N.Y. School District, Library Hit with Ransomware Attack

MeriTalk, July 22, 2019

https://meritalkslg.com/articles/n-y-school-district-library-hit-with-ransomware-attack/

The Syracuse City School District (SCSD) and Onondaga County Libraries, both in New York, were hit with a Ryuk ransomware earlier this month.

On July 9, SCSD was hit by an attack that rendered its computer files and systems inoperable. On July 12, district officials announced that they had restored "some" back-end systems, including HR, payroll, and student management, but that it was still working on public-facing systems such as email.

SCSD also said that it had "no indication that any data was compromised but rather the attack froze the district from accessing our own systems." The district also noted it has been working with both cybersecurity experts and law enforcement to restore systems that were still inoperable. WSYR, a local news outlet, reported that the "district has been unwilling to answer questions about how it is handling the attack" and will not confirm or deny whether it will pay a ransom to regain access to its systems.

Libraries across Onondaga County discovered July 12 that library systems were being held hostage by cybercriminals. Luckily for library users, Past Library Chair Ginny Biesiada said library officials do not believe that any library cards or other personal information are at risk. However, the Onondaga County Public Libraries' website notes that "many library services continue to be unavailable."

While it is unlikely any library card or other personal information is at risk, Biesiada said the ransomware attack continues to hold the library system hostage.

Unlike SCSD, an Onondaga County spokesperson said definitively that the county would not be paying a ransom should one be demanded. The spokesperson also said that the county doesn't anticipate purchasing any new hardware or software as part of its recovery.

Ryuk should be a familiar name to anyone in the cybersecurity field. This specific strain of ransomware has already left a string of high-profile victims in its wake, including Albany, N.Y., Jackson County, Ga., and Tribune Publishing. According to McAfee, Ryuk appears to have been developed from a toolkit by a Russian operator. The ransomware strain hits high-value targets who can't afford to be taken offline for large chunks of time. The name 'Ryuk' is fitting because it is taken from the Japanese manga character that "drops a death note" and the targets of the ransomware are dropped ransom notes for hefty Bitcoin sums.

For additional background and resources on RYUK ransomware, visit:

- FBI Flash RYUK Notice (May 2019): https://content.govdelivery.com/attachments/USDHSFACIR/2019/05/08/file_attachments/1207473/FLASH-MC-000103-MW-Ryuk.pdf
- National Cyber Security Centre RYUK Advisory (June 2019): https://s3.eu-west-1.amazonaws.com/ncsc-content/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf

Monthly Webinars!

First Wednesday of Every Month

at 10 am

(Except January, July, and August).

Next Webinars

Wednesday, September 4, 2019

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email

isp.schoolsafety@illinois.edu

Superintendent Calls For 'Thoughtful' Discussion Over Proposal to Demolish Columbine

NPR, July 7, 2019

https://www.npr.org/2019/07/07/739357969/superintendent-calls-for-discussion-over-proposal-to-shutter-columbine-high-scho

Twenty years after two gunmen attacked Columbine High School, the community of Littleton, Colo. remains divided over whether it's time to tear down the site of one of the worst school shootings in U.S. history.

Among those in the community calling for the school to be demolished is Jason Glass, the superintendent of Jeffco Public Schools, the school district where Columbine is located. In a recent op-ed for The Washington Post, Glass said the school has become a tourist destination, and while most visitors are harmless, some may be potential copycat shooters. He says the school should be torn down and rebuilt nearby.

In his op-ed, Glass writes that from June 2018 to May 2019, some 2,400 people were stopped or arrested for intruding on the grounds of Columbine.

"There are intractable challenges in operating a comprehensive high school for roughly 1,700 students in a building that seems to serve as a macabre inspiration for the contagion of school shootings in the United States over the past two decades," Glass wrote.

Speaking to NPR, Glass said, "It's the constant management of that and the pressure that any one of those unauthorized individuals who comes onto the site may be there to do harm — that is the concern."

Residents who want the building to stay have valid reasons rooted in emotion, economics and tradition, Glass told NPR.

The very fact that the building is still standing represents resilience, for many in the community, Glass said, who feel that "the building stands as sort of a symbol against what shooters were trying to accomplish in 1999, and it needs to continue to do that."

Ultimately, the community will make the final decision, Glass said. If Columbine is demolished, taxpayers would have to pay as much as $70 million for the construction of a new high school.

Glass said he hopes that no matter the building's fate, the emotional debate might serve as a crucial chance for Columbine to distinguish itself, above all, as a community that accomplishes a difficult decision with love and respect.

"Right now our responsibility is to inform the community of the question and help them navigate through it," Glass said. "I think it's just really important, especially on an issue that relates to the community's children, that we show that we can come together and have a thoughtful conversation."

Columbine is far from the only community that has been forced to grapple with what to do with the physical site of a mass shooting. As NPR's Bobby Allyn recently reported:

- "In Newtown, Conn., Sandy Hook Elementary School, where a gunman killed 20 students and six adults in 2012, was demolished in 2013 and a whole new building was built on the property.
- Officials in Parkland, Fla., are moving toward replacing the three-story Marjory Stoneman Douglas building that was the site of the killing of 17 students and staff."

To Combat Vaping, Nebraska School District Will Randomly Test Students for Nicotine

NPR, July 7, 2019

https://www.nbcnews.com/health/kids-health/combat-vaping-nebraska-school-district-will-randomly-test-students-nicotine-n1018886

At Fairbury Junior-Senior High School in southeast Nebraska, school administrators have noticed an alarming increase in students sneaking puffs of e-cigarettes: in locker rooms, restrooms and elsewhere on school grounds.

In an effort to reverse the vaping trend, the school district is taking a drastic step. Starting in the fall, all students who participate in extracurricular activities will be subject to random nicotine testing.

"It's a huge problem, and right now, I think it's new enough that we're being very naive to think that more kids aren't doing it," the Fairbury public schools superintendent, Stephen Grizzle, said of vaping. "We want to provide a safe, substance-free school as best we can, and we're just hoping that through the implementation of the policy, that we're helping students make the best decision."

The uptick in e-cigarette use in Fairbury echoes a national epidemic of teen vaping, according to public health experts. A 2018 Centers for

To Combat Vaping, Nebraska School District Will Randomly Test Students for Nicotine (Continued)

Disease Control and Prevention survey found that 3.05 million high school students and 570,000 middle school students had used e-cigarettes within 30 days. The authors attributed the popularity to "e-cigarettes shaped like a USB flash drive, such as JUUL; these products can be used discreetly, have a high nicotine content, and come in flavors that appeal to youths."

Once a month, 20 to 25 kids at Fairbury will be randomly selected to be tested for nicotine through a urine test, Grizzle said. If they are found to have nicotine in their system, the student must sit out for 10 participation days of their extracurricular activity. If there is a second offense, they have to sit out for 45 days, and see a certified substance abuse counselor or licensed mental health provider for an evaluation or treatment at their own expense, he said. Third-time offenders cannot partake in their extracurricular for 12 months.

"Our main concern is that No, 1, it's unhealthy. No. 2, it's against the law: They are not supposed to be able to purchase cigarettes and vaping and all that," Grizzle said. Plus, he added, "I think it would stand to reason that it would get in the way of opportunities and educational experiences if they're focused more on when they can vape as opposed to what's going on in the classroom."

The rural school district of Fairbury has about 900 students, 383 of whom are enrolled at the junior-senior high school. In the 2017 to 2018 school year, there were seven disciplinary incidents involving vaping at the high school; in the 2018 to 2019 school year, that number jumped to 30, Grizzle said.

Many states have moved to tamper teen vaping, with at least a dozen raising the tobacco and vaping device purchase age to 21. In Nebraska, e-cigarettes are legal for users 18 and up, but lawmakers are trying to raise the age to 19.

Dr. Sharon Levy, a pediatrician and director of the Adolescent Substance Use and Addiction Program at Boston Children's Hospital, said most teenagers have no idea how dangerous vaping can be.

"The active ingredient in vapes is nicotine, but they're really different than cigarettes in the way that they deliver nicotine. They can deliver a much higher dose much faster," she said. "The worst part is, we really don't know what the long-term effects of such high doses of nicotine on the teenage brain are."

Smoking of any sort is prohibited on school grounds in Fairbury. Grizzle said he believed his school district will be the first in Nebraska to test for nicotine. The district already does random drug tests for students involved in extracurriculars, which encompasses somewhere to 60 to 65 percent of the student body: For the past two years, it has tested them for illegal or performing-enhancing drugs.

Adding nicotine to the existing drug tests will cost $5 per test, at an estimated cost of $900 per year, Grizzle said.

The test will be quantitative, not qualitative, meaning those who inhale secondhand smoke will not have high enough levels of nicotine to register as positive, he said.

The testing is done by Sport Safe Testing Service, a Powell, Ohio-based student drug testing company that works with more than 100 school districts around the country. Grizzle said the company does not collect students' names, and instead assigns them a random identification number. The test results will only affect extracurriculars, which range from sports to speech clubs, and will not go on students' records, he said.

The policy was approved by the local board of education last month. Grizzle said the reaction from the community has been "predominantly" positive.

"Obviously you're going to have some that are against it, and think it's an intrusion, but overall, it's been positively received," he said. "We're focused on trying to be proactive the best we can."

FBI Releases Warning on Sextortion Scams Targeting Teenagers

Bleeping Computer, July 4, 2019

https://www.bleepingcomputer.com/news/security/fbi-releases-warning-on-sextortion-scams-targeting-teenagers/

The U.S. Federal Bureau of Investigation (FBI) issued a warning on Twitter regarding sextortion campaigns used by scammers to target young people from all over the United States.

"The internet connects you with the world. Do you know who in the world is connecting with you? Sending one explicit image can start a scary cycle," says the FBI in a tweet shared on July 3.

The agency also added to their alert the fact that sextortion scams usually rely on photos sent by potential victims to people they don't know in real life.

FBI Releases Warning on Sextortion Scams Targeting Teenagers (Continued)

In a story published on FBI's official website at the end of May, the agency states that it is currently "seeing a significant increase in activity involving sextortion—a federal crime that happens when an adult coerces a child to produce sexually explicit photographs or video of themselves and then send it to them over the Internet."

The scammers who operate sextortion campaigns that impact kids usually make use of a variety of channels to contact their young targets from social media and gaming platforms to video and dating chat apps.

FBI Special Agent Brian Herrick stated that "the FBI is seeing an increasing number of cases start on connected gaming systems, where the competition is intense and the offer of game credits or codes is enough to convince a child to create an explicit image."

Extortionists also employ several methods to coerce the kids to send them explicit content in the form of images or videos, from flattery and attention to involving romantic interest in their online relationship, and even offering money and various other valuable items, with threats also being involved in many cases if no other measures are successful.

"The second the criminal gets a picture, that child's life is going to be turned upside down," said Special Agent Ryan Barrett, who worked on the Finkbiner's sextortion case from April 2012."These people are relentless. They don't care."

Scammers increasingly using sextortion

As Kaspersky Principal Security Researcher Ido Naor told BleepingComputer in an email exchange, their "research suggests that many sextortion attacks appear to originate in Africa. Further, our latest spam and phishing analysis noted a rise towards the end of 2018 in the volume of sextortion-based email spam. These can use personal data harvested from earlier data breaches to tailor and lend authenticity to the threatening emails."

The researchers also added that, while extortionists who used spam campaigns to reach their victims — kids and adults alike — mainly focused on English-speaking targets, new campaigns were seen sending emails in other languages by the end of 2018, including German, Italian, Arabic, and Japanese.

"We are aware of dozens of sextortion cases over the last year, often using popular online video platforms to post alleged victim content, or contacting victims over social media accounts. Such attacks are not only illegal and malicious, but deeply distressing for the individuals involved," also added Naor.

In one of the sextortion incidents described by Naor, "the attacker had uploaded videos claiming to belong to the victim onto an account the hacker had set up on the online video platform, XVideos, using the alias: 'Ahmed2130'."

Subsequently, the Kaspersky Lab team "reported the videos as malicious content to XVideos, which promptly took them down and deleted the account. The hacker appears to have disappeared."

When asked by BleepingComputer about how often take downs due to sextortion appear to be occurring, an XVideos spokesperson said that they are "manually deleting something like 1 account per week on average. And most of the time we notice them before they start accumulating strikes - often people are afraid to fill out the take-down form, so they contact us by mail."

Ido Naor also shared these steps to be taken by anyone targeted by a sextortion scam to control the potential damage:

• First of all: seek help. Tell someone what is happening so the damage can be contained.

• Don't respond to any communications from the attacker – but do not delete the messages as they could help investigators.

• Remember that it doesn't benefit the attacker to release the content they claim to hold, as that makes it useless for extorting money.

• As soon as there is proof of intent to blackmail: for example, the attacker shares a link to a video and makes a demand for payment – share that with a security professional who can submit a report to the relevant video platform and get the file taken down.

• Let the police know – they may not be able to assist in your particular case, but it may help to protect others by allowing law enforcement to build up a body of evidence.

Preventing and reporting sextortion scams

As FBI Special Agent Damon Bateson added, these are the most relevant messages parents and caretakers have to convey to young kids so that they can better defend from scammers:

• Many people online are not who they say they are.

FBI Releases Warning on Sextortion Scams Targeting Teenagers (Continued)

• Don't talk to people you don't know online.

• Understand that any content produced on a web-enabled device can be made public.

• If you are being threatened or coerced online, tell someone. There is help and there is hope.

The agency provides potential victims with the following contact methods to report sextortion scams:

• To report suspected sextortion, call the nearest FBI field office or 1-800-CALL-FBI (225-5324).

• To make a CyberTipline Report with the National Center for Missing & Exploited Children (NCMEC), visit report.cybertip.org.

Herrick explains what sextortion is and how kids are being coerced to send explicit content to extortionists in a video that can be viewed at: https://youtu.be/KkCrtqr2h-g

Automatic Wifi Login Helped Police ID Teens Who Vandalized School

Gizmodo, July 10, 2019

https://gizmodo.com/automatic-wifi-login-helped-police-id-teens-who-vandali-1836249333

Four Maryland students charged with hate crimes for plastering their school in racist, homophobic, and anti-Semitic words and imagery just days before their high school graduation last year were identified by school administrators because their phones had automatically connected to the campus' wifi network, according to reports.

As part of its series exploring hate crimes, the Washington Post on Tuesday published a feature on the vandalism, evidently intended to be a senior prank, that included details specific to how the four Glenelg High School students—Joshua Shaffer, Seth Taylor, Matthew Lipp, and Tyler Curtiss—were caught.

In order to connect to the school's wifi network, students must log in from their phones with unique IDs that continue thereafter to "automatically connect whenever they are on campus," according to the Post. The Howard County Times previously reported that wifi had a hand in helping identify the involved students.

Despite masking their faces with t-shirts to shield themselves from security cameras, the four teens were automatically registered as being on campus at 11:35pm on May 23, 2018, the night the crimes occurred. Surveillance footage captured the four using spray paint to graffiti penises, swastikas, racist and homophobic slurs, and other images across the school's property.

The Post reported that all told, the teens left more than 100 graffiti marks on the campus, though the Howard County Times reported the number of graffiti drawings and epithets as being more than 50, a figure also cited by the Howard County State's Attorney's Office.

The teens were charged with a hate crime and sentenced earlier this year to probation, community service, and consecutive weekends in jail ranging from nine to 18 weeks. According to the post, the teens were only required to serve part of their respective sentences.

All of the students reportedly spray-painted some form of hateful graffiti, whether it be homophobic, racist, or anti-Semitic. The graffiti also targeted Glenelg High Principal David Burton, who is black, with a racial slur.

"This was something that was 50 separate acts of hate, you have anti-Semitic graffiti, you have racist graffiti, racist graffiti that targeted Principal Burton by name, you have homophobic references that were made," State's Attorney Rich Gibson said during an April press conference, per the Howard County Times. "This is an act of violence that rips the fabric of our community."

School Safety Newsletter

Statewide Terrorism &
Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail:
Isp.schoolsafety@illinois.com

Mia A. Ray
School Intelligence
Officer