Wilton-Lyndeborough Cooperative School District-SAU #63
Technology Director

192 Forest Road Lyndeborough, NH 03082
603-654-8088

Kevin P. Verratti, Director of Technology

Technology School Board Report
11/20/2017

- Storm damage on 10/29 and 10/30 caused a loss of power, loss of phone service and network/internet service. All systems came back online and recovered properly once power was restored.
- Replacement of the camera backend at WLCS was completed 11/1 along with the addition of two cameras to cover blind spots. The replacement of two low-resolution cameras with high-resolution cameras has been budgeted for in FY19.
- An issue with the Auto-Attendant that stopped parents from reporting their children absent if they called before 6am has been resolved.
- A total of 13 Para-Educators joined me on 10/31 for google training. The topics revolved around advanced use of chromebooks with students and other google tools.
- Several high profile data breaches have been in the news lately regarding school districts and student information. While there is no immediate threat specifically to our systems, the board should be aware that we do utilize several third-party systems that could be potential targets. Every effort is made to minimize exposure and maximize the security of our systems.

Respectfully,

Kevin P. Verratti
Director of Technology
SAU #63

The Washington Post

Answer Sheet • Analysis

Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts

By Valerie Strauss and Moriah Balingit October 26

A group calling itself the "Dark Overlord" says it hacked into school districts in several states, released student data and threatened violence in recent weeks, and the Education Department — in an apparent reference to the hackers — issued a warning of a "new threat" from criminals who vowed to release sensitive records unless extortion demands were met.

The department did not name the Dark Overlord in its warning (see text below) but the group took credit on Twitter for releasing information on students in a few school districts — which temporarily closed schools — and issuing threats of violence against children if demands were not met. No violence has been reported.

The Dark Overlord said on Twitter it hacked the Johnston Community School District in Iowa this month and released personal information on students, making it easy for "any child predator" to "easily acquire new targets." A statement on the district's website said on the night of Oct. 2, some students and parents in the Johnston School District received anonymous messages threatening the students' safety, leading to the closure of schools Oct. 3 and a delayed start Oct. 4.

The anonymous messages lit up the phones of parents in Johnston, a well-to-do suburb of Des Moines.

"Your child still looks so innocent," one message read, according to an image shared by a parent with the Des Moines Register and authenticated by a school official. "Don't let your child go outside."

Laura Sprague, a spokeswoman for the Johnston Community School District, said the messages got more specific and more frightening. The messages cited children by name and by school, threatening to bring harm to both.

"The texts were very malicious in nature, and for anyone who may read those or who have received those, it's chilling," Sprague said.

Out of caution, officials shut down eight schools the following day while law enforcement conducted sweeps with bomb-sniffing dogs. They reopened the schools the following day with additional security, Sprague said.

Sprague said police and the FBI, which are investigating the matter, determined the hackers got student information and parent phone numbers from a server kept by a third-party vendor, but she said she was not at liberty to identify the vendor.

School districts outsource tasks to private companies and sometimes hand over student information as part of the contracts. Sprague said her district contracts for everything from grass-cutting to messaging services that help schools connect with parents quickly and efficiently through mass text messages. School districts use those services to notify parents about snow days and school events.

Sprague said the malicious activity went beyond tweets: The group that claimed responsibility for the hack then posted phone numbers and names of students online, encouraging predators to target them.

The Dark Overlord also took credit for a "vivacious" attack on the Splendora Independent School District in Texas, and authorities in Montana said the group was responsible for the hacking of student information from the Columbia Falls School District.

The group has previously claimed credit for hacking into Netflix — releasing new episodes of "Orange Is the New Black" — after the company refused to pay a ransom. It also has said it obtained thousands of patient records by hacking into the computers of medical centers and health organizations, and claimed credit for other cyber attacks as well. The sheriff's office in Flathead County, Mont., said authorities had determined that the group operated from overseas.

According to the Flathead Beacon, a seven-page ransom letter was sent to officials in Columbia Falls in September demanding $75,000 in bitcoin in exchange for the group refraining from releasing student data it said it obtained through hacking the district's computer system. Several dozen schools closed for three days in the district, though the Flathead sheriff's office said in a Sept. 18 Facebook post:

> We fully understand the concern and fear that has resulted from this cyberattack, and want the community to know that all the valley law enforcement agency heads feel there is no threat to the physical safety of our children.
>
> As previously stated, the safety of our children has always, throughout this investigation, remained our paramount concern. We will continue to work around the clock to bring those responsible to justice, and remain fully committed to this investigation, even though we now know the physical threat to our children does not exist.

Here is the recent warning released by the Education Department:

> Posted Date: October 16, 2017

Author: Tiina Rodrigue, Senior Advisor for Cybersecurity, Federal Student Aid

Subject: ALERT! — CyberAdvisory — New Type of Cyber Extortion/Threat

Summary

Schools have long been targets for cyber thieves and criminals. We are writing to let you know of a new threat, where the criminals are seeking to extort money from school districts and other educational institutions on the threat of releasing sensitive data from student records. In some cases, this has included threats of violence, shaming, or bullying the children unless payment is received.

These attacks are being actively investigated by the FBI, and it is important to note that none of the threats of violence have thus far been judged to be credible. At least three states have been affected.

How to Protect Yourself

The attackers are likely targeting districts with weak data security, or well-known vulnerabilities that enable the attackers to gain access to sensitive data. This may be in the form of electronic attacks against school/district computers or applications, malicious software, or even through phishing attacks against staff or employees.

IT Staff at Schools / Districts are encouraged to protect your organizations by
##conducting security audits to identify weaknesses and update/patch vulnerable systems;
##ensuring proper audit logs are created and reviewed routinely for suspicious activity;
##training staff and students on data security best practices and phishing/social engineering awareness; and
##reviewing all sensitive data to verify that outside access is appropriately limited.

What to Do if This Happens to You

If your organization is affected by this type of attack, it is important to contact local law enforcement immediately. It’s not mandatory, but if you are an affected K12 school, please contact us at privacyTA@ed.gov so that we can monitor the spread of this threat. Additionally, the PTAC website contains a wealth of information that may be helpful in responding to and recovering from cyber attacks.

While this new threat has thus far been directed only to K12, institutions of higher education should know that they are required to notify the Office of Federal Student Aid (FSA) of data breaches via email pursuant to the GLBA Act, and your Title IV participation and SAIG agreements. Additional proactive tools for institutions of higher education are available at our Cybersecurity page on ifap.ed.gov.

5 Comments

Valerie Strauss covers education and runs The Answer Sheet blog. Follow @valeriestrauss

Moriah Balingit writes about education for the Post. Follow @ByMoriah