



School Safety Newsletter

Volume 7, Issue 3

October 2019

Over 500 US Schools Were Hit By Ransomware in 2019

October 1, 2019, ZDNet

<https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/>

In the first nine months of the year, ransomware infections have hit over 500 US schools, according to a report published last week by cyber-security firm Armor.

In total, the company said it found and tracked ransomware infections at 54 educational organizations like school districts and colleges, accounting for disruptions at over 500 schools.

To make matters worse, the attacks seem to have picked up in the last two weeks, with 15 school districts (accounting for over 100 K-12 schools) getting hit at the worst time possible -- in the first weeks of the new school year.

Of these 15 ransomware incidents, Armos said that five were caused by the Ryuk ransomware, one of today's most active ransomware strains/gangs.

Overall, Connecticut saw ransomware infections hit seven school districts throughout 2019, making them the state whose educational institutions were compromised the most by ransomware attacks this year.

But while Connecticut saw the most ransomware infections targeting school districts, it was Louisiana who handled the attacks the best when, in July, Governor John Bel Edwards declared a state of emergency in response to a wave of ransomware infections that hit three school districts. The governor's actions rallied multiple state and private incident response teams together and helped impacted school districts recover before the new school year, without paying the hackers' ransom demand.

Unfortunately, the Armor report doesn't go into details of what districts paid the ransom demand and which did not, since not all this information is currently available.

However, based on currently available information we know that Crowder College of Neosho, Missouri, reported receiving the highest ransom demand among all school districts, with hackers requesting a whopping \$1.6 million to provide the district with means to decrypt its systems.

DIFFERENT REPORT, DIFFERENT NUMBERS, STILL HUGE

But the number of impacted educational institutions could be even much higher. A different report from antivirus maker Emsisoft, released today, claims to have identified 62 ransomware incidents that impacted US schools in 2019.

Name	City	State
Ava R-I School District	Ava	MO
Wallenpaupack Area School District	Hawley	PA
Mad River Local Schools	Riverside	OH
Papillion-La Vista Comm. Schools	Papillion	NE
Rockford Public Schools	Rockford	IL
Souderton Area School District	Lansdale	PA
Wakulla County School District	Crawfordville	FL
Jackson County School District	Marianna	FL
Wyoming Area School District	Exeter	PA
Mobile County School District	Mobile	AL
Houston County Board of Education	Perry	GA
Guthrie Public Schools	Guthrie	OK
Smyth County Public Schools	Saint MARion	VA
Northshore School District	Bothell	WA

*Protecting our
future through
information
sharing*

In This Issue

- Over 500 US Schools Were Hit By Ransomware in 2019
- Mom Turns in Son After Finding School Shooting Plot in Journal
- Next Monthly Webinar - November 6, 2019
- The Role of Districts in Developing High-Quality School Emergency Operations Plans (2019)
- Boy Brings Gun Into Skokie Library Inside Violin Case, Police Say
- Students Overdose On Prescription Meds At Bowen High School
- Teens Find Circumventing Apple's Parental Controls is Child's Play
- A Montana Elementary School's Playground was Evacuated After Officials thought They Found a Bomb

Over 500 US Schools Were Hit By Ransomware in 2019 (Continued)

These 62 incidents took place at school districts and other educational establishments, and Emsisoft claims they impacted the operations of 1,051 individual schools, colleges, and universities, more than double the number reported by Armor.

But despite a difference in the number of impacted schools in the Armor and Emsisoft reports, both show a sudden spike in the targeting of US educational institutions with ransomware.

According to a report from the K-12 Cybersecurity Resource Center, of the 119 cyber-security incidents US K-12 schools experienced in 2018, only 11 were attributed to ransomware, just a fraction of the 54 and 62 ransomware incidents reported this year along by Armor and Emsisoft respectively.

The only government sector targeted by ransomware more than schools and colleges were local municipalities, which saw 68 ransomware incidents in the first nine months of 2019, according to Emsisoft.

The Emsisoft report includes additional statistics about ransomware attacks in 2019. The Armor report lists all the 54 educational institutions impacted by ransomware this year. Readers who'd like to keep track of recent ransomware attacks in the US can follow the Ransomware War interactive map for new infections.

Last week, the US Senate passed a bill named the DHS Cyber Hunt and Incident Response Teams Act, which would create incident response teams to help private and public entities defend against cyber-attacks, such as ransomware attacks. The bill previously passed the House floor and is expected to be signed into law by the President in the coming months.

Mom Turns in Son After Finding School Shooting Plot in Journal

October 7, 2019, WFMY News 2

<https://www.wfmynews2.com/article/news/nation-world/mom-turns-in-son-for-school-shooting-plot-in-journal-columbine-anniversary/83-ed0a16a8-2299-4ba4-b960-44fcbdc38f92>

COLLEGE PLACE, Wash. — Police in College Place, Washington believe they've stopped what could have been another school massacre. Under arrest - a 17-year-old boy - turned in by his mom. "I know I did all I can do and that I made the right choice," said Nichole, who only wanted to use her first name.

That choice was calling police after finding and reading her son's journal. He wrote about attacking his school on a specific date: April 20, 2020. "The anniversary of Columbine, which is freaky and kind of scary. Very scary," said Nichole. The journal went into chilling detail. He would detonate pipe bombs, and use multiple firearms to "blast anyone in sight" and "execute survivors."

Nichole told CBS News' Jamie Yuccas she feels like she's done something wrong as a mother. Police say she did everything right. "She's very courageous. It's clearly very emotional for her. She loves her son," said College Place Police Chief Troy Tomaras.

"You really wrestled with making the call to police," said Yuccas to Nichole. "Yeah," said Nichole. "My son told them that it was only creative writing. It was just a story."

Chief Tomaras says the journal went too far. "Well, he's plotting to attack. And kill people. That's beyond creative writing. That's beyond normal," said Tomaras.

Nichole says her son had been battling depression. "I'm worried about his mental health, and he needs help." Nichole says she believes her son is safer in jail and so is she.

When asked if she still loves her son, Nichole replied, "Of course I do. It takes a lot to do what I did. It wasn't easy."

Chief Tomaras says Nichole's decision "absolutely" saved people's lives. "She's parenting. That's what we need parents to do," he said. "Very courageous. Very grateful." So are all the other students, teachers and staff - saved by possibly the toughest choice a mother can make.

Monthly Webinars!

First Wednesday of Every Month

at 10 am

(Except January, July, and August).

Next Webinars

Wednesday,
November 6,
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

The Role of Districts in Developing High-Quality School Emergency Operations Plans (2019)

The Readiness and Emergency Management for Schools Technical Assistance Center recently published the Role of Districts in Developing High-Quality School Emergency Operations Plans. This guide was developed collaboratively by Department of Education (ED), Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Department of Justice (DOJ), Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS).

The guide can be found at: https://rems.ed.gov/docs/District_Guide_508C.pdf

It is a companion to the Guide for Developing High-Quality School Emergency Operation Plans (2013): https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf

THE ROLE OF DISTRICTS IN DEVELOPING HIGH-QUALITY SCHOOL EMERGENCY OPERATIONS PLANS

A COMPANION TO THE *SCHOOL GUIDE*



Boy Brings Gun Into Skokie Library Inside Violin Case, Police Say

October 2, 2019, CBS Chicago

<https://chicago.cbslocal.com/2019/10/02/skokie-library-gun-violin-case/>

SKOKIE, Ill. (CBS) — Police say a boy brought gun into a public library in Skokie – hidden in a violin case. As CBS 2 Investigator Megan Hickey reported, the whole conceit sounds like something out of an old gangster movie – but this was not a piece of fiction. Sources said the weapon was rifle hidden inside the violin case, and the person toting it around was a kid.

It happened on Saturday, Skokie police said. They were called to the Skokie Library shortly before 6 p.m. for a report of a minor with a firearm. Sources said the boy brought the rifle inside the library in the violin case, and then opened the case and started showing other people. No one was threatened with gun, Hickey has learned. When police arrived, they took the juvenile into custody.

On Tuesday, staff members at the library said they were well aware of the incident, but were not permitted to speak on camera. You don't have to turn much farther than YouTube to answer the question of how a firearm like that could fit in an instrument case. There are plenty of step-by-step tutorials online, and even popular video games that offer up a similarly shrouded hiding place for a gun.

Skokie Police said they are still working to determine where the gun came from this weekend, and how the boy got his hands on it. Skokie Library director Richard Kong confirmed staff acted quickly to notify police after learning about the gun, and were cooperating with the police investigation.

Boy Brings Gun Into Skokie Library Inside Violin Case, Police Say (Continued)

“We’ve been told by the police that this individual did not intend to use the weapon and that there is no ongoing threat to the library,” Kong said in a statement. “The safety of our staff and patrons is of the utmost importance at Skokie Public Library. We have procedures in place to address emergency situations, which were followed effectively and led to a peaceful resolution of this incident. I will continue to work with our safety staff and the police to ensure the security of our facility. Skokie Public Library is a place where everyone is welcome and we look forward to seeing you here.” Hickey confirmed that there is surveillance video of the whole incident, but her request for that video was denied by the Village of Skokie, citing an on-going investigation.

Students Overdose On Prescription Meds At Bowen High School

October 8, 2019, Patch

<https://patch.com/illinois/southside/students-overdose-prescription-meds-bowen-high-school>

CHICAGO — At least four students at a school on Chicago's Southeast Side were hospitalized October 8, 2019 morning in what has been reported as overdoses on prescription medications. Chicago police confirmed four boys were found unresponsive at Bowen High School in the South Chicago neighborhood around 10:30 a.m.

First responders came to the school, 2710 E. 89th St., after the principal called the nurse's office about a male student who passed out after ingesting something, the Chicago Sun-Times reported. All of the students involved passed out under similar circumstances and were between 15 and 17 years old, the report states.

The Sun-Times reports there were six students who overdosed, while police confirmed only four. A Chicago Fire Department spokesman told the newspaper everyone is expected to make a full recovery.

Four of the boys were taken to Trinity Hospital in stable condition, police said. A couple of weeks ago, multiple deaths were reported from overdoses in Joliet.

Teens Find Circumventing Apple’s Parental Controls is Child’s Play

October 15, 2019, The Washington Post

<https://www.washingtonpost.com/technology/2019/10/15/teens-find-circumventing-apples-parental-controls-is-childs-play/>

Helen Glaze didn’t think anything of it when her two sons told her they were looking for ways to get around Screen Time, Apple’s built-in tool that gives parents control of their kids’ phones. Then she discovered her 9- and 12-year-olds watching “Minecraft” videos at 2 a.m. during their annual trip to Chautauqua, N.Y., this past August.

“I was horrified and really felt betrayed,” she said. And she realized she can’t count on Screen Time to keep her kids off their phones. “It really doesn’t work, and that’s really frustrating.”

Kids are outsmarting an army of engineers from Cupertino, Calif., home to Apple’s headquarters in Silicon Valley. And Apple, which introduced Screen Time a year ago in response to pressure to address phone overuse by kids, has been slow to make fixes to its software that would close these loopholes. It’s causing some parents to raise questions about Apple’s commitment to safeguarding children from harmful content and smartphone addiction.

When Screen Time blocks an app from working, it becomes grayed out, and clicking on it does nothing unless parents approve a request for more time. Or, at least, it’s supposed to work that way.

On Reddit and YouTube, kids are sharing tips and tricks that allow them to circumvent Screen Time. They download special software that can exploit Apple security flaws, disabling Screen Time or cracking their parents’ passwords. They search for bugs that make it easy to keep using their phones, unbeknown to parents, such as changing the time to trick the system or using iMessage to watch YouTube videos.

“These are not rocket science, backdoor, dark Web sort of hacks,” said Chris McKenna, founder of the Internet safety group Protect Young Eyes. “It blows me away that Apple hasn’t thought through the fact that a persistent middle school boy or girl can bang around and find them.”

McKenna said he is miffed that Apple doesn’t fix the loopholes faster, despite its size, its massive hoard of cash and its copious profits. “In one day, I’m confident Apple could clean up all these loopholes,” he said.

Teens Find Circumventing Apple's Parental Controls is Child's Play (Continued)

He recently posted a list of loopholes, which he informed Apple of when Screen Time first launched and which he has been compiling in an effort to warn parents and help them close the loopholes when possible.

Apple spokeswoman Michele Wyman, in a statement, said the company is “committed to providing our users with powerful tools to manage their iOS devices and are always working to make them even better.” Wyman did not comment on specific bugs and workarounds in Screen Time or the speed with which Apple addresses them.

The problem has bedeviled parents who have struggled to strike a balance between allowing smartphone access for school work and basic social interactions and protecting their children from the pitfalls of the mobile world.

“I think there will always be ways that really innovative, critical-thinking children get around the controls,” said Christine Elgersma, senior editor of parent education for Common Sense Media, a nonprofit focused on how children use media and technology. “They’re usually ahead of us technologically.”

Companies with wildly popular and profitable consumer products don’t usually offer tools to help people use them less.

But in early 2018, a pair of major shareholders urged Apple’s board of directors to do something about youth screen addiction, arguing that addressing the issue would be good for Apple’s bottom line in the long run.

Nine months later, Apple launched Screen Time as part of iOS 12. It gave parents the ability to lock down their kids’ iPhones and iPads, limiting the amount of time kids could spend using the devices overall, as well as individual apps. Google offers a suite of similar Digital Wellbeing tools, and Amazon has a kids-only subscription service called FreeTime that comes pre-installed on its kids-edition tablets. (Amazon chief executive Jeff Bezos owns The Washington Post.)

Almost immediately, kids started finding ways to get around the controls, the same way they might look for a way to sneak out of the house while the parents are sleeping.

And parents started reporting that their kids were circumventing the newly added Screen Time restrictions. A widely publicized Reddit post, “My kid managed to pass Screen time limit,” accumulated more than 400 comments. On that post, parents reported their kids deleting and reinstalling apps and changing the clock to avoid time restrictions and using the iMessage app to watch prohibited YouTube videos. On Apple’s discussion board, there were titles such as “

But more than six months later, some parents were still reporting their kids using the same bugs, such as the time-change workaround. Some weren’t fixed until the new operating system, iOS 13, was launched a year later. Others, like the ability to watch YouTube videos inside iMessage, still work on the latest Apple phones and the most recent updates.

On forums hosted on Apple’s website, parents can be seen complaining for months about the same issues and the lack of response from Apple. After the community was unable to help them with their Screen Time glitches, at least two parents were offered a nontechnical solution: punishing their kids for exploiting the bugs.

“I understand that there are ways, such as enforcing consequences, to manage my children’s usage without software help,” one commenter wrote. “However I am not seeking parenting advice, but reporting a limitation of the software which claims to perform a function that it does not.”

Some parents struggle because the Screen Time controls aren’t intuitive, tucked several layers deep into menus under Apple’s settings. And the default settings are often permissive, such as allowing adult websites unless a parent specifically blocks them.

The problem has turned Brian Walker, a 41-year-old sales engineer for an automotive supplier in Michigan, into a part-time detective. Walker has seven kids, three of whom have cellphones. To keep track of what they’re up to, he and his wife use myriad tools to monitor them. But despite his vigilance, the recidivism in his household is high.

A few weeks ago, Walker noticed his 13-year-old son sitting quietly on the couch in the basement for hours, a long time for a kid who is “kind of X-Gamish” and likes to be outside. “I was suspicious because there’s a handful of apps where he will literally just melt his brain,” Walker said. When he walked over to check, he saw his son using TikTok, an app he thought was blocked.

It turns out that because the phone was a hand-me-down from an older sister who was allowed to use that app, the 13-year-old was also able to download it and use it, despite the Screen Time restrictions. “Even with an electrical engineering background, there are still things I don’t understand about how the software works,” Walker said.

Adam Pletter, a child psychologist who founded iParent 101 to help parents with screen-time addiction issues, said the danger for parents who use Apple’s service is that it can lull them into a false sense of security.

Teens Find Circumventing Apple's Parental Controls is Child's Play (Continued)

Parents can use alternative apps to control their kids' smartphone usage, but those services don't have the same access to Apple's operating system that Screen Time enjoys, and Apple has been criticized for limiting their functionality.

Apple's treatment of third-party screen-time apps has come under scrutiny from congressional antitrust investigators, who last month requested information from Apple on the subject.

When Helen Glaze, vacationing with her kids in New York, discovered they had hacked their phone, she confiscated it, and they confessed to their methods: While Screen Time blocked YouTube videos in Safari, the kids found that if they expanded the video to full screen before the Screen Time limit kicked in, they could watch videos continuously.

She eventually gave them back their phone, and Glaze is still using Screen Time. But she has stopped thinking she has any way to truly control her kids' smartphone usage. "I'm not going to engage in the cat-and-mouse game," she said. "I'm going to have to trust them to use their best judgment to know what we expect from them as kids and as people."

Rebecca Shelp, a stay-at-home mom in Littleton, Colo., bought her 14-year-old son a used iPhone 7 in April and set up Screen Time to limit his use of social media and other apps. But her son figured out workarounds almost immediately. By Memorial Day, he simply reset the phone, set up a new Apple ID and used whatever he wanted for as long as he wanted.

Shelp found out when she inspected his phone. She hadn't realized that Screen Time didn't block kids from simply resetting the phone.

But the subterfuge didn't end there. She says her son figured out how to make Screen Time glitch out by turning the phone off and on constantly until it stopped working properly. Her son even coined a term for this: "colliding the system."

Last month, while her son was at a sleepover, Shelp was monitoring his usage on her phone. The timer kept jumping wildly, from two hours to seven hours and back. Her conclusion: He must be "colliding the system" again.

"I can't even tell you how many hours I spend trying to figure out what he did," she said. After a long back-and-forth with Apple customer support, she was finally told that her son had found a known bug. Apple wouldn't tell her whether it planned to fix it.

A Montana Elementary School's Playground was Evacuated After Officials thought They Found a Bomb

October 15, 2019, CNN

<https://www.cnn.com/2019/10/15/us/bomb-exploded-montana-elementary-school-trnd/index.html>

Students at a Montana elementary school were evacuated on October 15, 2019 when someone found what was initially thought to be a homemade bomb on a playground. Officials later said the suspicious object at Rossiter Elementary School was not an improvised explosive device, or IED, and didn't explode, as was initially reported. The object was actually a bottle filled with nuts and bolts from a construction site, Lewis and Clark County Sheriff Leo Dutton told CNN.

"The plastic bottle found this morning at Rossiter Elementary did not explode. It was left there by a transient with mental health issues who thought he was picking up litter," the department said.

Classes at Rossiter were canceled while authorities started an investigation, but the school will now be open Wednesday. All Helena and East Helena schools were swept and cleared after initial lockdowns. The sheriff's office said even though the suspicious object wasn't malicious, the schools' careful response was the correct way to handle the situation.

The FBI, Montana Highway Patrol, Helena Police Department and Bureau of Alcohol, Tobacco, Firearms and Explosives assisted the sheriff's office in the investigation, CNN affiliate KTVH reported.

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

