Hacking attacks plague Massachusetts schools

Remote learning has been disrupted in multiple districts, forcing schools to pay thousands of dollars in cyber-protection.

By **Hiawatha Bray** Globe Staff, Updated February 10, 2021, 2 hours ago

A relentless series of hacking attacks have crippled remote learning efforts at several Massachusetts school districts. ADAM GLANZMAN/BLOOMBERG

It's difficult enough to teach schoolchildren online during the COVID-19 pandemic, but a relentless series of hacking attacks have crippled remote learning efforts at several Massachusetts school districts, forcing them to spend thousands on security systems to fend off the vandals.

“It’s beyond frustrating for our students and our teachers and our parents,” said Jeff Marsden, superintendent of the Medfield school system, which has seen its network disrupted by intermittent attacks that began about two weeks ago.

Similar incidents have plagued Massachusetts school districts since the beginning of the academic year. Schools in Tyngsboro and Sandwich were stricken with network attacks last October; the Norton public school network came under fire in late January and administrators have only recently regained control.

And in Winthrop last Thursday, an attack disrupted town and school computer services. Officials said the attackers did not gain access to student, employee or financial data.

In Duxbury, school superintendent John Antonucci its systems has suffered “intermittent Internet outages” since late December. But in a rare success, the school tracked down the culprits.

“We identified them as members or our school community,” Antonucci said. He declined to name the hackers, but said Duxbury would not bring criminal charges. In a letter to parents, Antonucci said the district has “initiated a disciplinary process for all involved.”

In most cases, it’s likely the perpetrators will never be caught. “I think what we’re seeing is a lot of free time by some people who try to figure out how to create havoc,” said Norton public school system superintendent Joseph Baeta, “and it wouldn’t shock me if it was a student.”

A December report from the Federal Bureau of Investigation cited increases in attacks on school computer networks during the pandemic. These include “distributed denial-of-service” or DDoS attacks, the kind being launched against so many local school networks.

In a DDoS attack, hundreds or thousands of computers fire a massive stream of Internet data at a targeted network, overwhelming the network so that legitimate data traffic can’t get through. It’s a crude way to shut down a network, requiring little technical

get through. It's a crude way to shut down a network, requiring little technical

sophistication. There are even companies that hire out attacks, or sell software for DIYers.

As a result, "the ability to launch attacks has been democratized," said Patrick Sullivan, chief technology officer for security strategies at AkamaiTechnologies in Cambridge, which provides services that block DDoS attacks.

Mark Ostrowski, East Coast engineering chief for data security firm Check Point Software, said some cybercriminals launch DDoS attacks to distract network operators away from more harmful invasions. "The DDoS is what everybody's focusing on," said Ostrowski, "but they're really doing something else."

One common scheme is installing "ransomware" programs that lock up vital school files and can only be unlocked if the school pays a ransom.

Attacks can also be launched by disgruntled students looking to get out of class. "It's kind of the equivalent of pulling the fire alarm," Sullivan said.

In Duxbury, school officials found suspicious online searches performed on a laptop that had been issued by the school system. "They were search terms like 'can you go to jail for a DDoS attack?'" said Antonucci. Investigators found that the attack had been carried out by a DDoS-for-hire service that charged just $25.

DDoS attacks are also expensive to deter. When the Norton school network was first hit during the last week of January, the district's Internet provider Comcast assigned a team to thwart the attack, at an initial cost of $13,000. Then came three more days of additional work, at around $2,000 per day. Finally, the school signed up for Comcast's full-time anti-DDoS service, priced at an annual rate of $32,000 a year.

Comcast later agreed to waive its initial fees and charge only for the annual subscription service. A Comcast spokesman also said that the company offers 90 days of DDoS protection to schools at no charge before the annual rate kicks in. Duxbury's Antonucci

protection to schools at no charge before the annual rate kicks in. Dunbar's office

said his school system is being billed $2,500 a month or $30,000 a year for Comcast's DDoS defense service.

Hiawatha Bray can be reached at hiawatha.bray@globe.com. Follow him on Twitter @GlobeTechLab.

Show comments