Why Ransomware in Education on the Rise and What That Means for 2023

thehackernews.com/2022/10/why-ransomware-in-education-on-rise-and.html

The breach of LA Unified School District (LAUSD) highlights the prevalence of password vulnerabilities, as criminal hackers continue to use breached credentials in increasingly frequent ransomware attacks on education.

The Labor Day weekend breach of LAUSD brought significant districtwide disruptions to access to email, computers, and applications. It's unclear what student or employee data the attackers exfiltrated.

There is a significant trend in ransomware breaches in education, a highly vulnerable sector. The transitory nature of students leaves accounts and passwords vulnerable. The open environments schools create to foster student exploration and the relative naivete in the sector regarding cybersecurity invite attacks.

The breach at LAUSD and what happened afterward#

Four days post-breach, reports came that criminals had offered credentials for accounts inside the school district's network for sale on the dark web months before the attack. The stolen credentials included email addresses with the suffix @lausd.net as the usernames and breached passwords.

LAUSD responded in its update that "compromised email credentials reportedly found on nefarious websites were unrelated to this attack, as attested by federal investigative agencies." The LAUSD breach report confirmed the FBI and CISA as investigators.

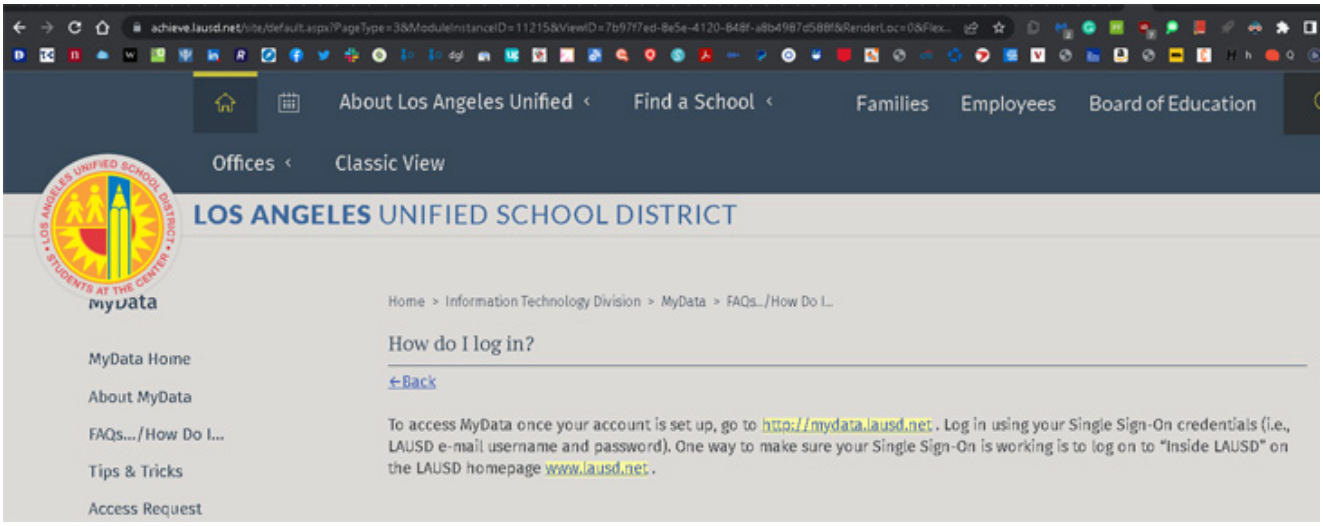
The FBI and CISA and facts surrounding the breach confirm that the threat actors likely used compromised credentials to gain initial access to the LAUSD network to assert control over increasingly privileged passwords.

The FBI and CISA had observed the Vice Society ransomware group, which took credit for the attack, using TTPs including "escalating privileges, then gaining access to domain administrator accounts." The ransomware group used scripts to change network account passwords to prevent the victim organization from remediating the breach.

Escalating privileges assumes attackers had privileges to escalate, meaning they already had access and compromised passwords at the outset of the attack.

As the FBI and CISA advisory explained, "Vice Society actors likely obtain initial network access through compromised credentials by exploiting internet-facing applications."

The LAUSD website advises account holders to access its MyData application at https://mydata.lausd.net, using their "Single Sign-On credentials (i.e., LAUSD email username and password). One way to make sure your Single Sign-On is working is to log on to "Inside LAUSD" on the LAUSD homepage www.lausd.net."



LAUSD website: How do I log in? page

The homepage, email, and SSO are exploitable internet-facing applications. Hackers accessing email via compromised passwords could use SSO to access data throughout the MyData application and any application that allows access via the SSO.

After the breach, LAUSD required employees and students to reset their passwords in person on the district website at a school district location for the @LAUSD.net email suffix before they could log on to its systems. It's something they would do in case of compromised email passwords to prevent further compromise.

The rise of ransomware attacks on education this year#

Ransomware groups often target education, with effects including unauthorized access and theft of staff and student PII. The uptake of teachers, staff, and students working and learning online has expanded the threat landscape, with ransomware attacks on education trending upward since 2019. .

The FBI confirmed compromised education passwords for sale, including a dark web ad for 2,000 US university usernames and passwords on the .edu domain suffix, in 2020. In 2021, the FBI identified 36,000 email and password combinations for accounts on .edu domains on a publicly available instant messaging platform.

This year, the FBI found multiple Russian cybercriminal forums selling or revealing network credentials and VPN access to "a multitude of identified US-based universities and colleges, some including screenshots as proof of access."

Beefing up security for 2023

Attackers buy and sell breached passwords on the dark web by the millions, knowing that, due to password reuse, the average credential grants access to many accounts. Criminal hackers count on it so they can stuff breached passwords into login pages to gain unauthorized access. That illicit access to accounts allows hackers to gain access to sensitive data, exploit an open network, and even inject ransomware.

Specops Password Policy with Breached Password Protection compares passwords in your Active Directory with over 2 billion breached passwords. Specops just added over 13 million newly breached passwords to the list in its latest update. Specops Breached Password Protection compares Active Directory passwords with a continuously updated list of compromised credentials.

For each Active Directory password change or reset, Breached Password Protection blocks the use of any compromised password with dynamic feedback on why it was blocked. If you're looking to secure your educational organization, or any business for that matter, you can test Specops Breached Password Protection for free.