Radware Advisory

Education: A Rough Start To The School Year

October 6, 2022

Persistently Targeted

Educational institutions are no strangers to cyberattacks. Every year they see a segment of their student population turn into threat actors, looking to manipulate the registration processes, delay tests, or target digital learning platforms for several reasons, including just for fun. But more recently, external to the student body, extortion-based threat groups have entered the educational threat landscape with terrorizing attacks, further opening educational institutions up to a wider variety of threats.

Recent Wave of Cyberattacks

Over the last two months, following the return to school, there has been a wave of cyberattacks targeting educational resources worldwide. These attacks have ranged from denial-of-service attacks and defacements to credential stuffing attacks and extortion-based campaigns.

Radware Advisory

Education: A Rough Start To The School Year

October 6, 2022

CREDENTIAL STUFFING

Credential stuffing is a sub-technique of brute force account cracking. The attack consists of threat actors leveraging credentials obtained from a public data dump to access unrelated accounts via credential overlap due to users reusing the same password across personal and business accounts.

In September, threat actors were able to compromise **Seesaw**, an interactive learning platform used by elementary schools. The platform was targeted by a credential stuffing attack (**T1110.004**) that leveraged compromised accounts. The threat actors in this event used their access to send an inappropriate image to users for entertainment purposes.

Seesaw Schools and Districts Curriculum Product Support Get a Quote Log In

A Note from Our Co-Founder/CEO about the Credential Stuffing Incident

Product Updates · September 15, 2022

To the Seesaw Community,

For nearly a decade, you have trusted Seesaw to be at the heart of your classroom. We take that responsibility very seriously and are deeply sorry for the disruption caused by the attack on Seesaw user accounts earlier this week. With this in mind, I wanted to write to you directly about what happened.

Late on September 13, individual Seesaw users were subjected to a coordinated "credential stuffing" attack. Some of the compromised accounts were used to send a message with a link to an inappropriate image. Less than 0.5% of users were affected.

First and foremost, I want to assure our community that Seesaw is safe and the attack has been shut down. Seesaw was not compromised, and we have put a number of additional safety practices in place to ensure that an attack like this doesn't happen again.

We also want to be transparent about what happened, how we dealt with this incident, and what we are doing moving forward.

Figure 1: Seesaw Credential Stuffing incident

DEFACEMENT CAMPAIGN

A defacement attack is a widespread technique often used by threat actors to modify the visual appearance of a website. Typically, threat actors deface websites to spread political or religious propaganda related to a specific event. Defacements may also cause users to distrust and question the system's integrity post-compromise.

In September, Russian threat group **NoName057(16)** compromised and defaced (**T1491.002**) the Kyiv National University of Trade and Economics website. The threat actor launched the attack to spread pro-Russian propaganda in response to the Russo-Ukranian war.

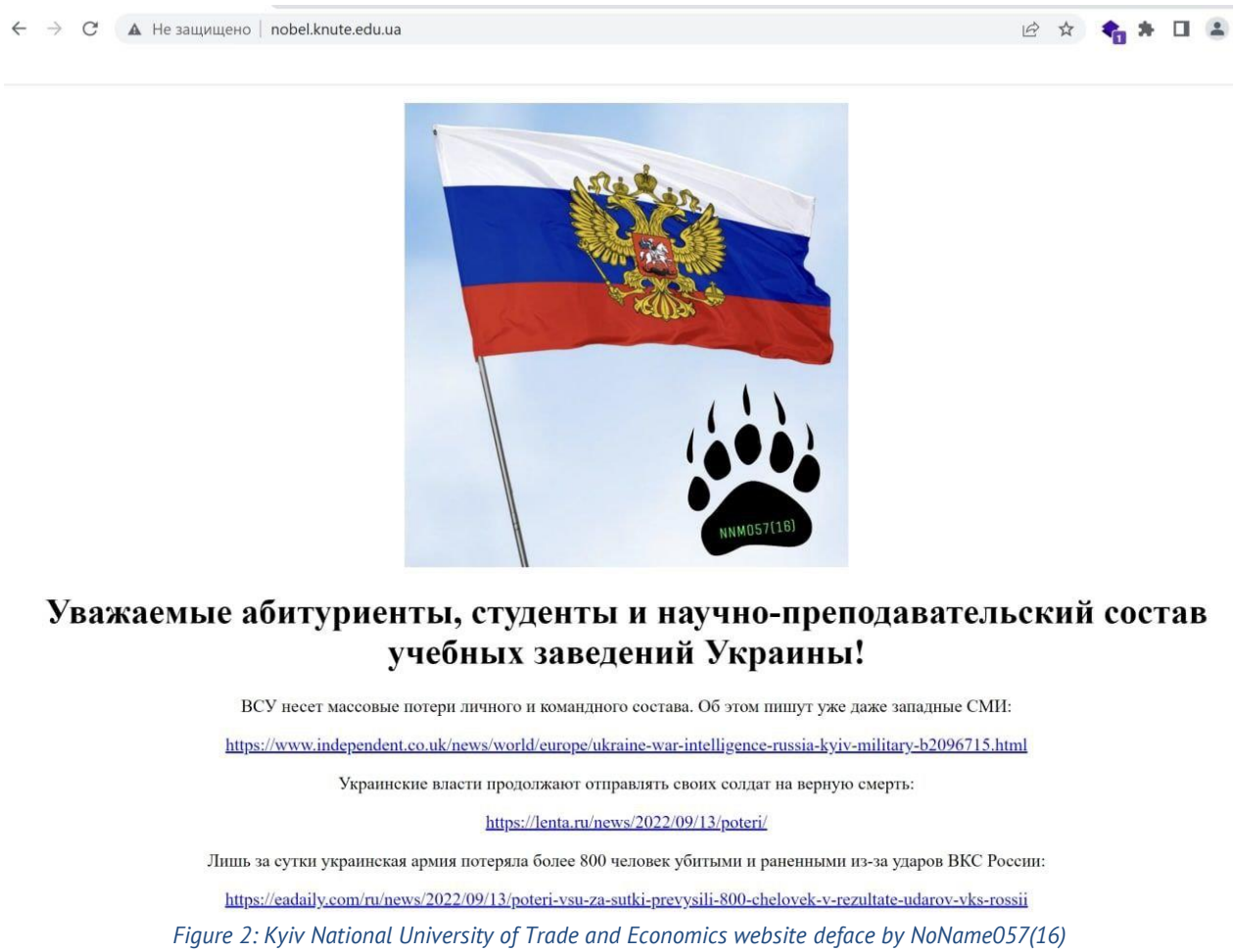

Figure 2: Kyiv National University of Trade and Economics website deface by NoName057(16)

DENIAL-OF-SERVICE

An application exhaustion flood is a form of a denial-of-service attack that targets resource-intensive features of an application to cause service degradation.

In August, threat actors were able to take down **QuickLaunch** on the first day of school via an application exhaustion flood (**T1499.003**). QuickLaunch is an identity-as-a-service platform (IDaaS) that manages educational institutions' and organizations' human and device authentication, authorization, and access control. The threat actors flooded password.quicklaunch.io with repeated requests, causing multiple passwords reset calls to exhaust system resources and deny access to the application. As a result of the outage, students could not log in to their university email or learning management systems.

13:03, Aug 23 EDT

Fixing

What is the this outage, technically ?

Denial of Service on QuickLaunch Password Manager Services. This DOS attack on the public URL - Password.QuickLaunch.io is generating password reset by what seems to be a bot that is using one of the customer domains to make password reset calls. The flood of these password reset calls which started at approximately Tuesday, 8:15 AM ET are creating performance issues on Password Manager services and as the password reset calls pool, the logs show that the Login services become non-performant and unavailable as a result. Due to QuickLaunch' s architecture setup on multi-node and auto-scaling, the Login service will "spin" for end users as Login requests continue to increase and pool.
Snippet of Denial of Service logs:
Aug 23 13:01:36 QL8-PROD-PASSWORDMANAGER1 kernel: [913.933432] TCP: request_sock_TCP: Possible SYN flooding on port 8080. Sending cookies.
Check SNMP counters.

Figure 3: QuickLaunch's notification of the denial-of-service attack

BUSINESS EMAIL COMPROMISE

Compromising email accounts is popular among threat actors. By leveraging validated data leaks, threat actors can use email accounts to conduct further operations, such as phishing attacks. Using an existing persona, a threat actor can leverage a preestablished relationship of trust to target new victims.

In August, the **Pennsylvania Treasurer** and the **District Attorney** announced the results of an investigation into the theft of millions of dollars from the Pennsylvania Department of Education (PDE). Last year, the Treasurer's office was notified by a financial institution that a payment request to Chester Upland School District (CUSD) was flagged for fraudulent activity. The hack was part of a two-part scheme that allowed an international threat group to misdirect funds intended for CUSD. First, the threat group compromised a CUSD email account (**T1586.002**) and requested a bank account change from the PDE. The threat group then used a money mule, extorted via a romance scam, in Florida, to distribute the misdirected fund to members of the group. As a result of the investigation, officials recovered $10.3 million in misdirected funds.

RANSOM DENIAL-OF-SERVICE (RDOS)

A ransom denial-of-service (RDoS) attack is a denial-of-service attack that is motivated by monetary gain. Attacks typically start with a letter or post threatening to launch an attack on a specific day and time unless a ransom payment is made. In some cases, attackers will launch a small attack on a victim's network as proof that the threat is real.

Since the start of the school year, there have been several reported cases of RDoS attacks (T1498) targeting educational institutions. In these cases, threat actors have contacted educational institutions via email or chat service, demanding tens of thousands of dollars to stop the denial-of-service attacks. The criminals appear to be less sophisticated threat actors from Russia who also advertise DDoS services, such as booters and stressers.

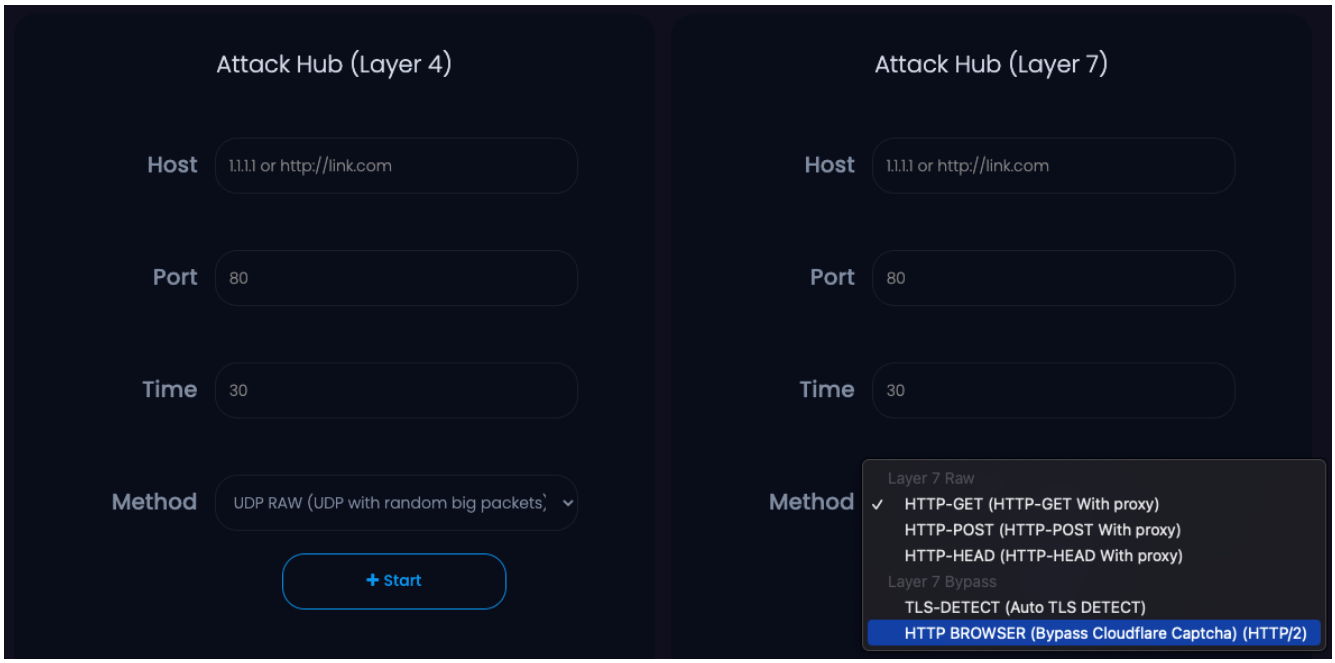

Figure 4: One for the advertised booter/stresser service

RANSOMWARE

A data encryption attack is when a threat actor encrypts data on a targeted system or multiple networked systems in an attempt to disrupt the operations of an organization. A data encryption attack becomes a ransomware attack when the threat actor withholds the decryption key under the demand of monetary compensation from the victim.

In September, over the United States Labor Day weekend, the Los Angeles Unified School District (**LAUSD**), the second largest school district in the United States, was compromised by a ransomware attack (**T1486**) at the hands of Vice Society. While details of the attack are still unclear, days before the attack, **CISA** published an alert about Vice Society excessively targeting educational institutions.

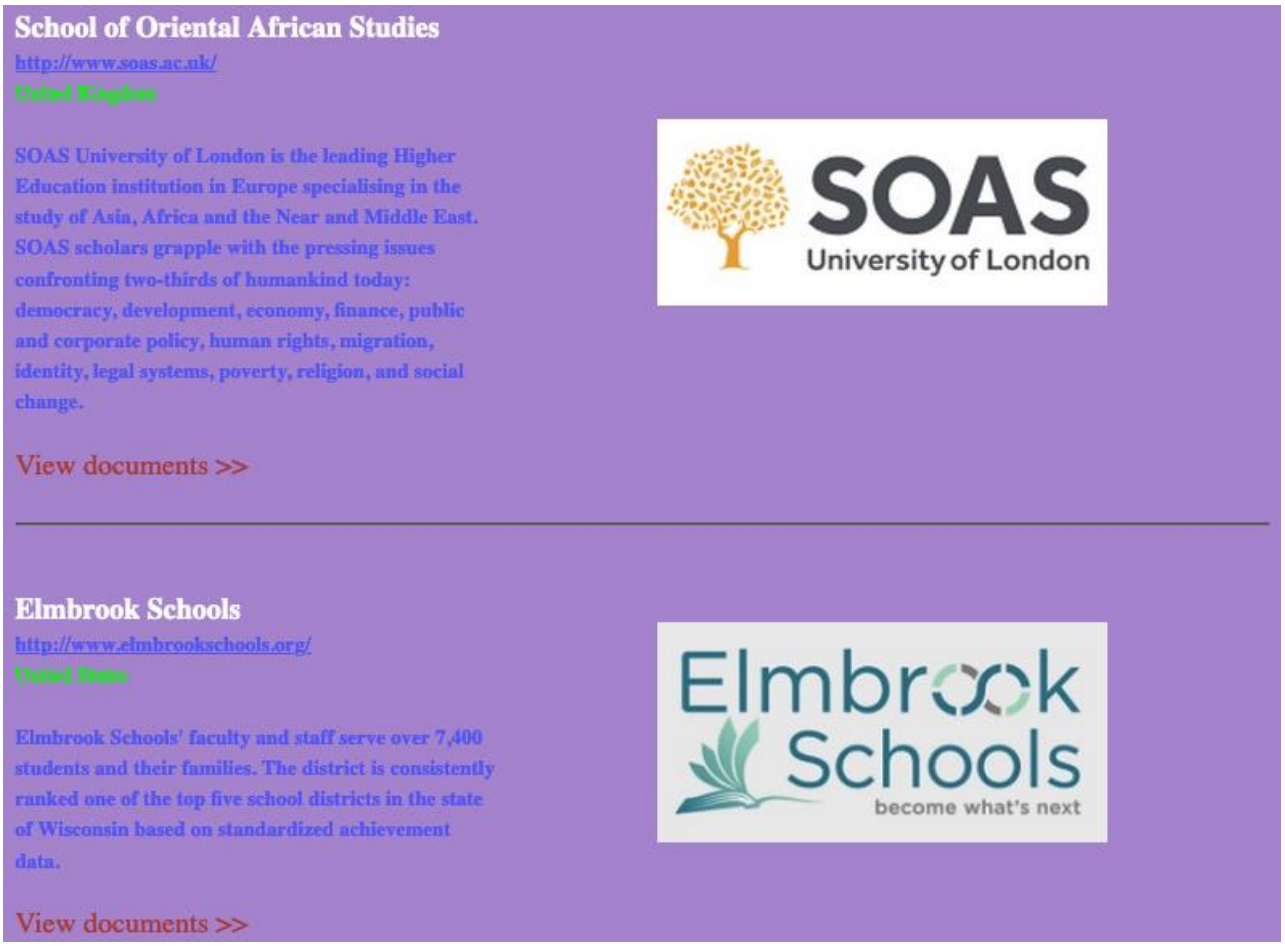

Figure 5: Education victims advertised on Vice Society Darknet site

What to Consider

Maintaining network security while preserving communication and the free exchange of information presents educational institutions with unique obstacles. Meanwhile, challenges such as IT talent shortages and insufficient funding for cybersecurity projects have educational institutions searching for solutions to secure their environments in the face of new risks.

Applications are the textbooks of the 21st century, and educational institutions require applications and networks to provide content, educate students and reduce operational costs. The growth of online services and web-based content introduces new security challenges to districts and universities that must ensure 24x7 access to online services and protect student records.

AVAILABILITY OF ONLINE SERVICES

Schools and universities depend on their websites and online services. Networks and applications must be available 24x7 to allow students and faculty access to resources, especially during admissions, exams, and other time-sensitive periods.

SAFEGUARDING DATA

Schools and universities process and store large volumes of personal information. Based on a recent study by the Consortium for School Networking of U.S. school districts, student-data privacy and security have become a critical priority, and over half of school districts have formal password and security policies that are widely followed.

Transitioning applications and data to the public cloud only exacerbates data security because educational institutions have less control and visibility to manage and secure these applications in cloud environments.

LACK OF RESOURCES

Although keeping websites, data, and networks secure is critical, it is becoming increasingly complex due to the cybersecurity skills shortage and the increasing array of attack vectors. For larger school districts, this presents various resource problems. Still, these resource shortfalls can be catastrophic for smaller school systems with little to no IT staff, according to the Consortium for School Networking.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto-policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible Deployment Options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT THE RADWARE SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit **Radware's Security Research Center**, it is the ultimate resource maintained by our Threat Intelligence team for everything security professionals need to know about DDoS attacks and cyber security. Also visit our quarterly updated **DDoS & Application Threat Analysis Hub** for up to date statistics and analytics on all threats relating to denial-of-service and online application attacks.