SUCCESS STORY

KELAGROUP

KELA GROUP'S PROACTIVE DEFENSE TECHNOLOGY SUCCESSFULLY SHIELDS LARGE U.S. SCHOOL DISTRICT FROM CYBERSECURITY ATTACK

The school district, situated in the southeastern United States, oversees 140+ school buildings and educates over 180,000 students.

Automated Intelligence and Analysis for Proactive Protection Against Cyber Threats

KELA Group's Cyber Intelligence Platform swiftly identified and secured the education institute's internet assets. The company's analysis technology automatically detected and alerted on threats, ensuring rapid response and ransomware protection.

Education Institutions - Targets for Cyber Attacks

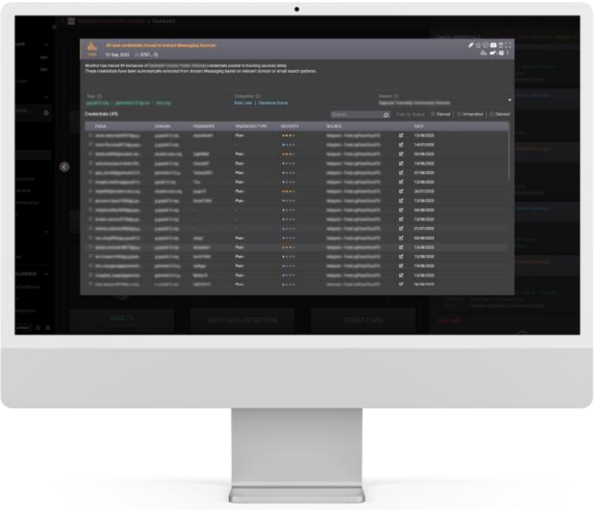
In the 2022-2023 academic year, eight prominent school districts experienced substantial cyberattacks, as reported by both the White House and GAO. These attacks led to the cancellation of classes and school closures in at least four instances, with financial losses exceeding $1 million. K-12 school districts are particularly appealing targets due to their extensive attack surface, limited IT and cybersecurity resources, and the expectation that they may comply with ransom demands.

GAO has pinpointed the following cyberattack techniques as the ones with the highest likelihood of being employed against schools: phishing, ransomware, Distributed Denial of Service (DDoS), and video conferencing disruption. In response, federal, state, and local governments are bolstering the resources allocated to school districts, enabling them to acquire the necessary personnel, procedures, and tools for robust defense against such attacks.

KELA Group's Cyber Intelligence Technology adopts a perspective from the attacker's standpoint, leveraging validated intelligence to gain insights into and assist in mitigating the potential risks associated with a ransomware or network attack on the target.

Keeping the School District Safe:

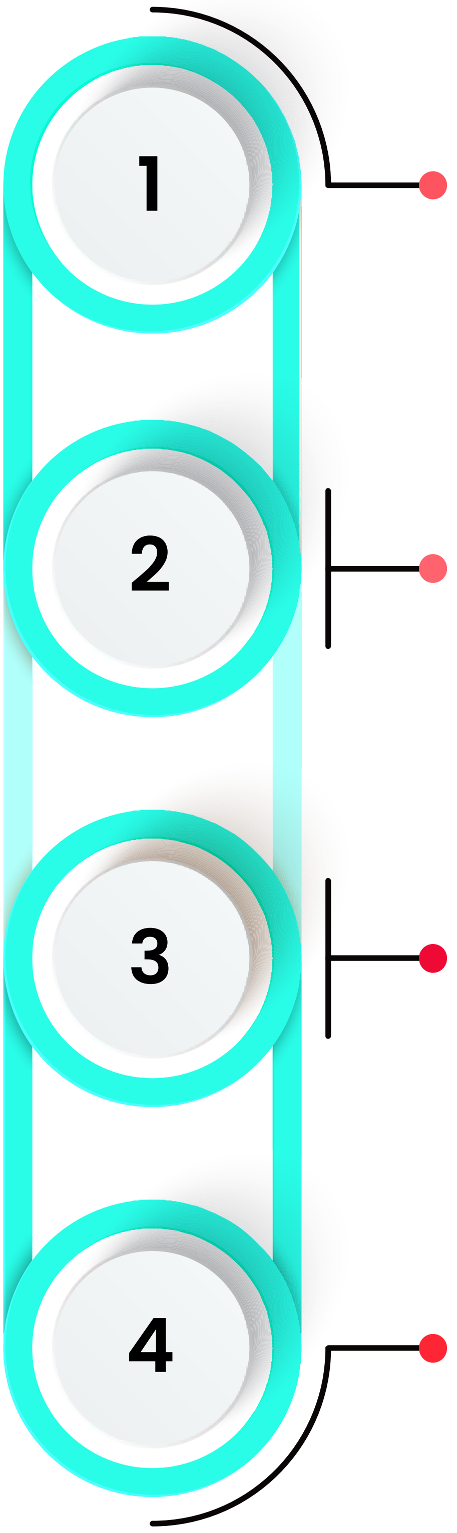
- Continuously discover and manage the true attack surface at scale, safeguarding against potential exploitation by attackers.
- Automatically identify bots (infected computers) associated with specific school subdomains and services, enabling the security team to swiftly address credential and risk issues at a subdomain level.
- Conduct robust and timed scans to assess both known and unknown vulnerabilities, extending beyond CVEs and misconfigurations, and deliver validated endpoint vulnerabilities.
- Rapidly disseminate findings and take proactive measures upon detecting school assets (such as credentials and open ports) on the cybercrime underground.
- Leverage the group's managed services for effective triage and proactive threat hunting, optimizing staff time and resources by targeting the most critical threats.



Protect Against Data Theft, Data Encryption and DDoS Attacks

While prioritizing the seamless facilitation of learning and the flexibility of device usage both within the institute and remotely, several paramount concerns encompass data security. These concerns include guarding against data theft, ensuring robust data encryption, and fortifying defenses against DDoS attacks.

Securing Success: From Threat Detection to Data Protection



Identification of Threats

Automated monitoring by KELA Group's Cyber Intelligence technology detected compromised accounts for sale

The risk

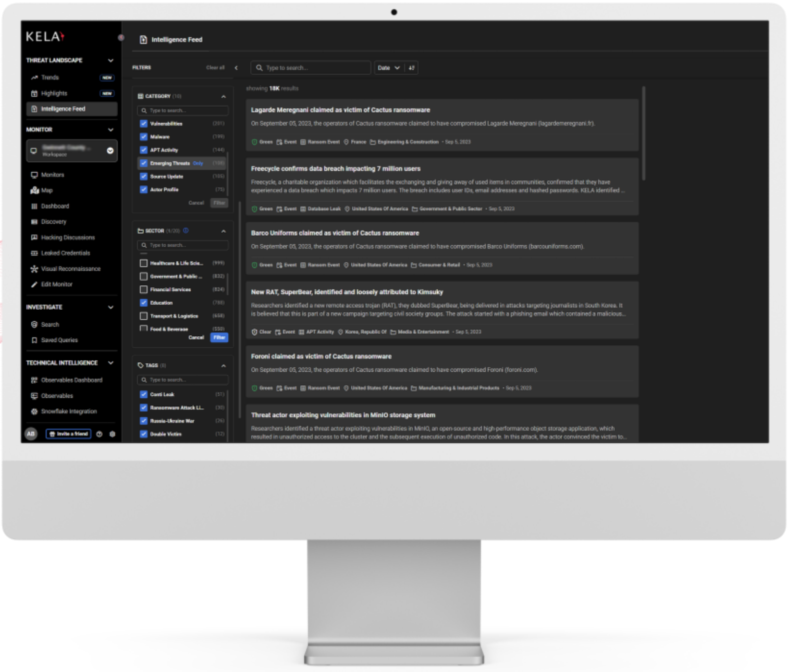
The compromised accounts would have provided an attacker access to the school district’s internal system

Mitigation

The school district requested to purchase the bot files and collaborated with KELA Group's Cyber intelligence Center to remove them from the Cybercrime underground

Outcome

KELA Group’s proactive approach secured the school district’s network, preventing a large-scale data leak and potential ransomware attack



showing 18K results

Lagarde Meregnani claimed as victim of Cactus ransomware

On September 05, 2023, the operators of Cactus ransomware claimed to have compromised Lagarde Meregnani (lagardemeregnani.fr).

Green · Event · Ransom Event · France · Engineering & Construction · Sep 5, 2023

Freecycle confirms data breach impacting 7 million users

Freecycle, a charitable organization which facilitates the exchanging and giving away of used items in communities, confirmed that they have experienced a data breach which impacts 7 million users. The breach includes user IDs, email addresses and hashed passwords. KELA identified ...

Green · Event · Database Leak · United States Of America · Government & Public Sector · Sep 5, 2023

Barco Uniforms claimed as victim of Cactus ransomware

On September 05, 2023, the operators of Cactus ransomware claimed to have compromised Barco Uniforms (barcouniforms.com).

Green · Event · Ransom Event · United States Of America · Consumer & Retail · Sep 5, 2023

New RAT, SuperBear, identified and loosely attributed to Kimsuky

Researchers identified a new remote access trojan (RAT), they dubbed SuperBear, being delivered in attacks targeting journalists in South Korea. It is believed that this is part of a new campaign targeting civil society groups. The attack started with a phishing email which contained a malicious...

Clear · Event · APT Activity · Korea, Republic Of · Media & Entertainment · Sep 5, 2023

Foroni claimed as victim of Cactus ransomware

On September 05, 2023, the operators of Cactus ransomware claimed to have compromised Foroni (foroni.com).

Green · Event · Ransom Event · United States Of America · Manufacturing & Industrial Products · Sep 5, 2023

Threat actor exploiting vulnerabilities in MinIO storage system

Researchers identified a threat actor exploiting vulnerabilities in MinIO, an open-source and high-performance object storage application, which resulted in unauthorized access to the cluster and the subsequent execution of unauthorized code. In this attack, the actor convinced the victim to...