INDUSTRY SECURITY BRIEF

Malware in Education

Hunt and respond to malware with Infocyte HUNT.

SANS INSTITUTE SURVEY

Key attack vectors listed in the SANS Institute survey:

- Exploits against internal database systems and servers, malware delivered to staff endpoints
- Exploits against websites or servers, exploits against other critical applications running on endpoints
- DNS server exploits and malware delivered to student endpoints

RECENT MALWARE ATTACKS

- July 2018: Networks at the Australian National University in Canberra, which is home to several defense-focused research units, were breached for months.
- March 2018: Internet service at Mississippi Valley State University's campus temporarily down. Officials confirmed that the school was hit by a SamSam ransomware attack.
- June 2017: University College London suffered a widespread ransomware attack. Staff and students warned of the risk of data loss and substantial disruption as access to networks was restricted.
- April 2017: National University of Singapore and Nanyang Technological University suffered APT attacks. Government and research data targeted.

Educational Institutions at Growing Risk

Schools, colleges, and universities are attractive targets for hackers and cyber attacks are on the rise within higher education. The Wannacry campaign of 2017 struck institutions in Asia, where there were widespread reports of attacks at universities, with students locked out of their theses and final papers as graduation loomed.

Schools and universities are highly connected environments, with lots of file sharing. Every day there are tens of thousands of students, academics, and employees circulating files and using laptops, tablets, and smartphones to access institutional data.

As academia has become the hub and repository of critical applied research in science, business, and technology, the threat to intellectual property is a real and present danger.

The growing number and sophistication of malware attacks has elevated the importance of cyber security and risk management in general, but there is an expectation of care when it comes to protecting our students.

COLLEGES AND UNIVERSITIES ARE HIGH-PROFILE TARGETS

Educational institutions are high-profile targets for cyber espionage and attacks by external nation state actors. The 2018 Verizon Data Breach Investigations Report noted that in the Education sector, cyber espionage accounted for 20% of reported breaches — qualifying as an important pattern. Financial motivation remained the key driver, per the DBIR, for 70% of breaches.

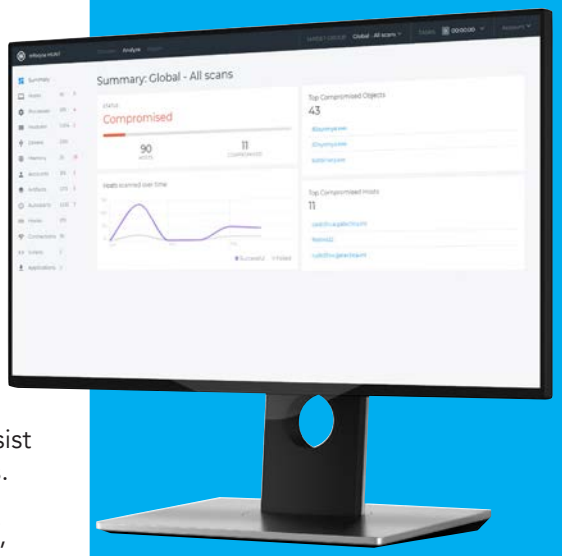
Why are educational institutions such prime targets?

- Complex mix of users, public/private areas, and open networks
- Storage and sharing of valuable research and intellectual property
- High number (sometimes in the millions) of personal records with enough personally identifiable information to create credit files
- High-quality databases containing information for alumni, board members, researchers, and academics
- Access to third-party research, intelligence, or intellectual property (government, private sector, etc.)

Along with being high-priority targets, colleges and universities are also very difficult networks and systems to defend because they often have legacy systems and outdated approaches to cyber security. Schools often operate in highly decentralized IT environments and are slow to adapt to change and new technologies — they are also slow to address security risks.

Cyber Health in Education

Study finds systems and endpoints need triage



The SANS Institute conducted a survey of the current computer security landscape in junior colleges, community colleges, and universities, from nearly 300 IT professionals. The results clearly indicate the primary threats and what assets educational institutions should protect. Primarily, IT professionals are mostly concerned about administrative systems (70%) and the security of faculty and staff endpoints/computers (64%).

Current IT management is concerned about endpoints that could be weak points vulnerable to hacker targeting in order to deliver an attack.

When students experience medical issues, there are institutional resources to assist them – from a primary school nurse to health centers at universities and colleges. Yet, educational institutions have been slow to adapt to the current barrage of malware that is continually putting the private information of their students, staff, faculty, and alumni at risk.

Educational institutions must evolve and adapt to the realities of malware and cyber health. Part of this involves a maturing approach to immediate and long-term security threats. Mounting a comprehensive cyber security effort, including continuous threat hunting, may address many of the challenges malware poses.

HUNT MALWARE AND PROTECT YOUR INSTITUTIONAL ASSETS

Infocyte HUNT offers educational institutions the ability to proactively and continuously hunt malware and other persistent threats that have evaded their defenses — undetected. Ransomware has dominated the security mindset recently, and it's important to note that attackers often seed secondary malware when conducting a ransomware attack. For educational institutions victimized by ransomware, the focus is usually on dealing with the primary breach and ransom. Once the primary breach is addressed, institutions lack any recourse to ensure that additional payloads dropped have been found and addressed.

The Forensic State Analysis (FSA) approach used by Infocyte HUNT enables an organization to schedule regular scans of endpoints to detect any suspicious activity. Once malware is identified – users can then take steps to remediate the security breach. There is no need to wait for a high profile event, such as a data breach, to call attention to the breach and precipitate discovery. In addition, Infocyte HUNT dispels any superficial trust in security vendors, solutions, and even business partners — removing the ability to exploit such trust. The source of a file is irrelevant, Infocyte HUNT finds anything suspicious.

INFOCYTE HUNT

- Definitively and independently determines if your endpoints are compromised
- Performs live volatile memory analysis to establish the compromise state of an endpoint at a given point in time
- Combines advanced detection, forensic automation, and patent-pending memory analysis
- Not reliant on a host OS, which may be itself compromised
- Extremely fast — capable of inspecting upwards of 50,000 endpoints per day
- Easy to use and does not require forensic experts or extensive training
- Delivers a final report with actionable intelligence within minutes

1. SANS Institute, Higher Education: Open and Secure?, 2014

Infocyte

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com

© 2018 Infocyte Inc.

All Rights Reserved. Infocyte and Infocyte HUNT are trademarks of Infocyte, Inc. All other trademarks and servicemarks are the property of their respective owners.

TRY HUNT FOR FREE »

Discover why Infocyte HUNT has been recognized as a top threat hunting solution by industry leaders.

www.infocyte.com