CYBER THREATS TO THE EDUCATION INDUSTRY

THE EDUCATION INDUSTRY FACES CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced Persistent Threat (APT)[1] groups attempting to gain access to sensitive intellectual property, such as from university research centers, for economic or political espionage.
- APT groups aiming to use an educational institution's network infrastructure as a staging ground from which to target victims in other industries, on the assumption that their activity will appear less suspicious originating from a reputable institution's network.
- Enterprise-like cybercriminals seeking to steal and profit from sensitive personal and financial information from students, faculty, and staff
- Hacktivists trying to deface and disrupt websites as a method of protest or way to call attention to a certain cause.

CASE STUDY: CHINA-BASED THREAT ACTORS TARGET UNIVERSITY RESEARCHERS

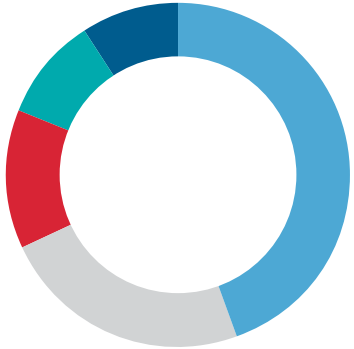
FireEye investigated two intrusions involving a China-based threat group that had compromised two U.S. universities. The threat group gained initial access to one of the schools by uploading malicious webshells to an unauthenticated upload page on one of the university's web servers. Once inside the school's network, the threat actors expanded their access and obtained credentials for a webserver shared between the universities. The threat actors then leveraged their access to the webserver to compromise the network of the second university. The threat actors appeared interested in the universities' China-focused academic programs and research institutions.

WE HAVE OBSERVED AT LEAST 8 ADVANCED THREAT GROUPS COMPROMISE ENTITIES IN THESE SUBSECTORS:

- Colleges & Universities
- Education & Training Software
- Research Laboratories

1 Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

FireEye



TOP 5
MALWARE DETECTIONS

- **45%** SOGU (aka Kaba)
- **24%** WITCHCOVEN
- **13%** Gh0stRAT
- **10%** SpyNet
- **9%** Pandora

TOP 5
CRIMEWARE DETECTIONS

- **40%** Fareit
- **25%** Zeus
- **14%** Cryptowall
- **14%** Simda
- **8%** Treemz

THREAT HORIZON & INDUSTRY OUTLOOK

Education institutions will likely continue to face cyber threats due to the valuable information stored on school networks and the ability for threat actors to use network infrastructure to launch operations against other targets. University networks in particular are difficult for administrators to effectively secure, given the network's size and number of users, as well as the need for internal and external users to access and share information. We anticipate that the following factors will also influence threat activity towards the sector:

- Involvement in research programs that may have a potentially high economic payoff or support sensitive government research contracts would probably lead to increased targeting from APT groups in search of related intelligence to benefit their sponsoring government or associated state-owned companies.
- Association with high profile or influential academics or dissidents would likely also result in greater threat activity from APT groups seeking to gather information that would allow their sponsoring government to monitor that individual's activity, and gain insight into policy discussions.
- Perceived role as a highly visible or symbolic target may lead to threat activity from hacktivists or APT groups seeking to disrupt website or network operations for political purposes.
- Involvement in controversy may lead to threat activity from hacktivists seeking to protest and embarrass the victim organization through disrupting website access, defacing webpages, or stealing and exposing the organization's sensitive information.

DATA STOLEN FROM EDUCATIONAL INSTITUTIONS

- Business Communication
- Business Documents
- Employee Evaluations
- Finance Documents
- Grant/Scholarship Documents
- Industry Research & News
- Invoices
- Marketing Materials
- Meeting Records
- Personally Identifiable Information
- Programs & Initiatives
- Public Newsletters

TOP MALWARE DETECTIONS

FireEye detected and alerted education industry customers to threat actors using the following types of malware most often:

SOGU	(aka Kaba, PlugX), a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control (C2) server with graphical access to the desktop.
WITCHCOVEN	is a profiling script design to learn information about the operating systems, browsers, and applications of site visitors. We suspect APT actors are using these scripts to engage in footprinting, an information gathering technique used to profile computer systems and the organizations to which they belong.
GH0STRAT	is a remote access tool derived from publicly available source code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.
SPYNET	is a publicly available RAT that allows threat actors to interact with a compromised system via a remote shell, upload and download files, interact with the registry, and start and stop processes and services. It can capture images of the desktop, record from webcam and audio inputs, extract saved passwords, and turn a compromised system into a proxy server. There is also keylogging functionality, as well as anti-debugging/virtual machine defensive mechanisms.
PANDORA	is a backdoor that is multi-threaded, implements multiple anti-analysis techniques, and is able to communicate via both UDP and TCP. It achieves persistence by generating multiple copies of itself and replacing any executables listed in the system registry's 'Run' key. This backdoor is capable of keylogging, screen captures, file manipulation and infection, self-updating, downloading and executing other files, and can provide a threat actor remote control of the system, but will not run on systems with popular Chinese anti-virus programs installed.

TOP CRIMEWARE DETECTIONS

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the education industry:

FAREIT	(aka Pony Loader, InfoStealer) is an information stealing Trojan that can also force infected systems to engage in distributed denial of service (DDoS) attacks and download additional types of malware.
Zeus	(aka Zbot, Citadel, Gameover) is a family of Trojans primarily designed to engage in banking credential theft. It is capable of a wide variety of function, including the ability to remotely execute shell commands.
Cryptowall	(aka Crowti) is ransomware that encrypts files on victim's endpoint and uses the onion router (TOR) for C2 communication.
Simda	is a multipurpose Trojan capable of credential theft, infecting additional files, downloading malware, and opening a backdoor on infected systems.
TREEMZ	is a Trojan capable of logging keystrokes. It may be disguised as an update to a popular online game.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye