The Latest Fortinet Threat Report for Educational Institutions

Education continues to be one of the most targeted industries by cybercriminals, primarily due to the data that is stored in most school data centers. This information ranges from the PII of students, to stored payment information related to fees and tuitions, to original research being conducted by faculty and graduate students.

FortiGuard Labs collects data from globally placed devices, such as antivirus and IPS sensors, that are triggered when attacks are detected. Over the 2018 school year, hundreds of billions of these data points were collected and correlated by FortiGuard Labs. This has resulted in unique insights that can be used to protect and educate customers and improve product development efforts. This blog combines general threat and attack trends with critical intelligence related to the Education sector gathered from our global threat intelligence database.

In this blog, we will look at two areas targeting Educational institutions – viruses and malware – as well as take a quick look at the security implications of the top application traffic crossing the networks of many educational institutions.

Viruses

For 2018, the top two industries targeted by viruses were Environmental and Education sectors. The environmental industry consists of organizations that address environmental issues related to water, air, soil, and complex ecosystems (such as wetlands or marine biospheres), as well as problems such as pollution, waste, erosion, and noise. The Educational sector includes all academic institutions, public and private, ranging from elementary and secondary schools to universities and academic research facilities.

The dominant threat families targeting Education were Riskware and Adware. These are usually programs disguised as legitimate applications, but instead end up doing things such as displaying more popup ads when browsing the Internet.

For example, AirPush designed for Android devices is used by developers to monetize their applications by displaying advertisements. While this may not seem like anything more than a nuisance, it is actually a severe issue because malicious actors regularly inject malware into these ads. While some of these ads require the user to click on a link to download malware or land on an infected website, advertisement popups can also drop malware onto the end user device through a technique called malvertising.

The most common exploit detected was CVE-2017-1182, which is a 17-year old memory corruption issue found in Microsoft Office (including Office 360). It is often exploited using a phishing campaign that includes a malicious attachment. Once the malicious document is opened, it allows attackers to execute remote code on a vulnerable machine.

The flaw resides within the Microsoft Equation Editor, which is used to insert and edit complex equations such as Object Linking and Embedding (OLE) items in Microsoft Word documents. It has been installed by default with every version of the Office suite since Office 2000. While this vulnerability was fixed during Microsoft's Patch Tuesday last November, publicly released proof-of-concept exploits continue to have success using this CVE for their initial attack vector. This is due, in part, to a general decline in rigorous patching and updating across all industries.

Malware

Overall, Education ranks third in terms of detected malware attacks, after Telco/Carrier and Technology verticals. While there are millions of malware families in the wild, the ones targeting Education can be broken down into three categories: IoT, cryptojacking, and targeted attacks.

IoT - In 2018 Educational institutions saw hits on router vendors, such as Linksys, Dlink, Avtech, MVPower, Vacron, and Zyxel, as well as closed-circuit cameras. This increased trend of attacking cameras was documented in the Threat Landscape Report for Q4 of 2018.

Cryptojacking – Cryptojacking especially targeted the Education sector in 2018. Cryptojacking hijacks the unused cycles of a compromised (usually IoT) device to mine for cryptocurrencies. While many may see cryptojacking as a benign activity since it only steals unused CPU resources to mine for cryptocurrencies, many variants also include other malicious activities, such as turning off anti-malware controls or opening ports on the firewall, allowing malicious software to be dropped. As a result, the detection of crypto-jacking malware should be seen as a precursor to other threats, such as ransomware being loaded onto your cyber assets.

Targeted attacks – We also detected attack campaigns aimed at university professors to steal data and intellectual property. Since 2013, threat actors have managed to break into the accounts of nearly 8,000 professors at hundreds of universities across the world. These attacks were highly targeted, requiring an enormous amount of upfront reconnaissance to understand each professor to ensure their phishing email had the

right content to render interest, and included links to malicious websites imitating the login page of another professor who expressed interest in the targeted professor's research. Once visited, these customized sites would steal login credentials which were then used to break into the victim's own devices.

One such campaign involved the use of sixteen domains that contained more than 300 spoofed websites and login pages for 76 universities in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States. According to the U.S. Department of Justice, the hackers managed to compromise the accounts of around 8,000 university professors and then steal 31 terabytes of academic data and intellectual property.

Critical Application Traffic Analysis

According to FortiGuard Labs data, Facebook is the most-used application at schools. While this may seem like trivial information, this information can have a profound impact on security if used correctly by cybercriminals.

For example, Facebook user credentials have been breached multiple times over the last few years. In September of 2008, the accounts of nearly 50 million Facebook users accounts were breached. In April of this year, 1.5 million Facebook users had their email contacts harvested due to a privacy breach. An app called At the Pool also exposed Facebook databases as well as the unprotected Facebook passwords of over 22,000 users. This was in addition to the more than 540 million Facebook records that were publicly exposed earlier that same month.

Because people tend to use the same username and password for their social sites as they do for their work systems, network access, and VPN connections. This creates a potentially significant attack vector for gaining access to the educational networks that teachers, faculty, and students use daily.

In addition, information posted on social media sites is regularly farmed to create personalized phishing attacks that increase the likelihood of someone opening a file or clicking on a link that then becomes the entry point for a successful system breach. It's worth noting that we see a trend where criminals send these phishing emails during lunch as they know faculty and students are more likely to be viewing their email on their phone – where it's a bit harder to determine whether or not an email is a phishing attack, thereby increasing the chances of someone falling for the scam.

With that information in hand, IT teams should ensure that users never use their social media password for access into their work environment. This can be done through user awareness training program, or requiring two-factor authentication can help to minimize this risk.

Leverage Threat Intelligence to Protect Students and Faculty

Threat intelligence focused on the Education sector is a valuable tool for IT teams charged with protecting the systems and data of school districts, private schools, colleges and universities, and academic research facilities. Leveraging live threat intelligence streams, in-depth data analysis, and practical tips from a variety of sources will help reduce the likelihood that your institution will be part of the growing trend of cybercriminals successfully targeting educational institutions.