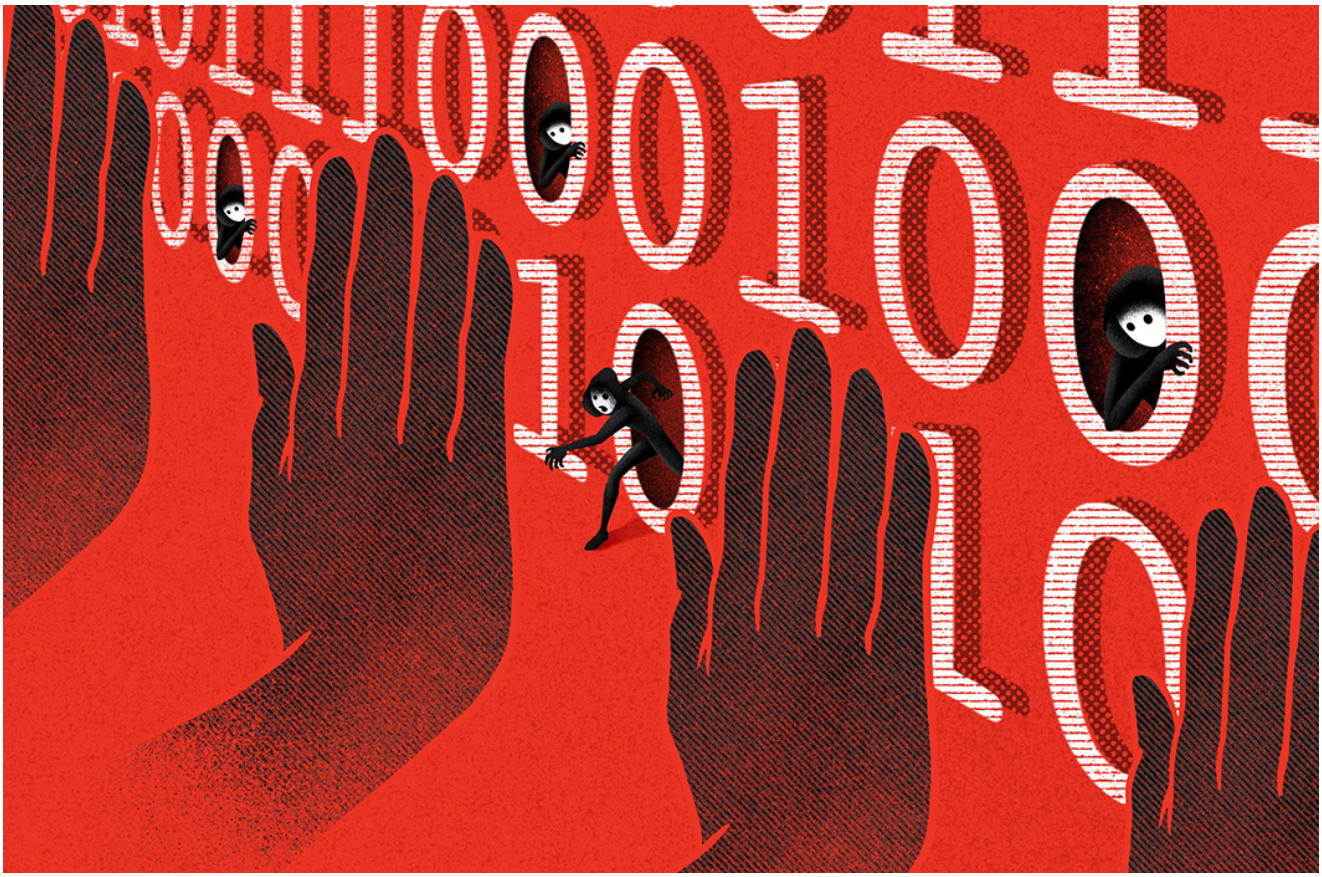
Academia Threat Landscape: 2020 Analysis

crowdstrike.com/blog/academia-threat-landscape-2020-analysis/

Strategic Threat Advisory Group and Falcon OverWatch Team February 17, 2021



The academic and education industry is large and complex. It comprises a diverse range of institutions, from elementary schools through to research organizations, and spans both the public and private sectors. The industry has two critically important roles. The first is providing education as a service, and in this role, the sector needs to be vigilant in the face of the ever-growing threat of eCrime. The second is in driving research and development, and the cultivation of new ideas — and in this role, the education industry has the potential to shape national economies and policy priorities, and ultimately support the power of the state. This positions the academic industry as a priority target for state-sponsored — and to a lesser extent, hacktivist — threat actors.

The primary motivations for threat adversaries to target each of the sub-sectors of academia are outlined in the table below.

	Nation-State	eCrime	Hacktivist

			
Primary & Secondary Education		**X**	
Vocational & Higher-Level Education	**X**	**X**	**X**
Research Entities	**X**	**X**	**X**
Motivations	**Espionage.** Academic institutions hold valuable intellectual property, making them a target for nation-state espionage operations supporting national research and development objectives. Academic institutions also play a pivotal role in policy development, and count many influential people among their staff and alumni. This makes them valuable sources for intelligence collection objectives. **Network Access.** Nation-state adversaries have leveraged compromised academic networks for operational infrastructure, and for gaining additional access to associated parties and networks, due to the culture of open connectivity often observed within academic environments.	**Financial.** The academic attack surface is broad and complex, due to the nature of its users and operations. Criminals exploit the sector's reliance on information systems, using ransomware and data extortion to extract payments.	**Ideology.** Hacktivists may conduct Distributed Denial of Service (DDoS) campaigns, data leaks, or web defacements, or may compromise social media accounts to disrupt academic services and/or publicly embarrass an entity.

What Did the Threat to Academia Look Like in 2020?

Activity observed by CrowdStrike throughout 2020 reinforces that the academic industry faces a serious and present threat from criminal and nation-state adversaries. Falcon OverWatch™ observed a more than fourfold increase in intrusions against the academic and education industries compared to 2019. This increase is driven in large part by eCrime activity, which has accounted for 82% of activity uncovered by Falcon OverWatch in the education and academic industries this year.

Since mid-August 2020, there has been a notable increase in adversaries targeting academia, primarily pursuing big game hunting (BGH) operations against these institutions. BGH adversaries are deploying enterprise-wide ransomware, using both data encryption and extortion to coerce victims into paying large ransoms. A similar period of ransomware activity targeting academic entities was witnessed a year earlier in September 2019. The timing of the new operations coincided with the start of the new academic year for many education institutions in the U.S. and U.K. This year, the threat of disruptions looms larger, as the COVID-19 pandemic has forced many organizations to move lessons online. With eLearning becoming the new normal, disruptions could have a significant impact on the ability to provide learning, making the opportunity that much more tantalizing for eCrime adversaries.

Through 2020, both CrowdStrike Intelligence and Falcon OverWatch also observed nation-state activity targeting schools and universities. Nation-state actors are often highly skilled, well-resourced and have the luxury of time to conduct exhaustive reconnaissance against their intended victims. This allows the adversary to collect sensitive information about their victim to help craft more genuine social engineering campaigns with a greater chance of eliciting a victim response.

A particularly pertinent example of nation-state activity against the academic industry has been the ongoing targeting of universities and research institutions involved in COVID-19 research. Since April 2020, intrusion activity targeting coronavirus research has been reported against U.S., U.K, Spanish, South Korean, Japanese and Australian laboratories; this activity was conducted on the part of Russian, Iranian, Chinese and North Korean actors.

In one such example from the second half of 2020, Falcon OverWatch uncovered a targeted intrusion against an academic institution known to be involved in the development of COVID-19 testing capabilities. The malicious activity in question was attributed to a China-nexus actor, which gained initial access by way of a successful SQL injection attack against a vulnerable web server. Once inside the victim environment, the actor compiled and launched a web shell that was used to perform various malicious activities largely focused on information gathering and collection. Notably, the actor's activities included the enumeration of a particular directory housing health-related files and data, suggesting the actor likely knew what they were looking for. With the extensive research and development that continues to surround the COVID-19 pandemic, Falcon OverWatch continues to observe state-sponsored actors displaying a keen interest in academic institutions.

Interestingly, even when academia is not the ultimate target for nation-state actors, it can still be a valuable intermediate target to support broader intelligence objectives — including political, national security and economic espionage. For reasons explored next, nation-state adversaries may view the academic sector as a soft target for initial access for future operations against other associated sectors.

Although large-scale hacktivism efforts have decreased over the past couple of years, hacktivist groups are assessed to present a low to moderate threat to the academic sector. A historic look at hacktivism targeting academia suggests these actors are opportunistically and intermittently targeting educational institutions in line with certain nationalist and ideological dogmas.

The Who's Who of the Academia Threat Landscape

As of this writing, CrowdStrike is tracking 150 threat actors across nation-state, eCrime and hacktivist motivations, 40 of which have a history of attacking academic institutions.

- 25 of these adversaries are nation-state threat actors
- 11 are sophisticated criminal syndicates
- 4 are hacktivists

Criminal activity accounts for the vast majority of intrusion activity, with groups such as DOPPEL SPIDER, RIDDLE SPIDER, CIRCUS SPIDER, TWISTED SPIDER, PINCHY SPIDER, WIZARD SPIDER and INDRIK SPIDER being most active. Criminal activity across the globe is up 330% in 2020 compared to 2019, while nation-state attacks remain steady. Adversaries such as VELVET CHOLLIMA, LABYRINTH CHOLLIMA, BERSERK BEAR, STATIC KITTEN, WICKED PANDA and KRYPTONITE PANDA account for multiple operations throughout the year.

What Are the Risks for the Academic Industry?

1. The Tyranny of Many Endpoints

Many academic institutions have a wide attack surface relative to other organizations. In the early days of the internet, academic-sector networks were specifically designed to foster collaboration between globally separated research teams. This focus on accessibility means that many organizations still feature "bring your own device" (BYOD) policies to cater to students and independently operated enclaves. An example of this could be a research lab maintaining their own servers outside the administration of an IT department for the sake of sensitive analysis. BYOD setups have also been a key feature of eLearning for schools and universities during the COVID-19 pandemic.

Defenders should be aware that Falcon OverWatch regularly observes adversaries leveraging malware-free or fileless techniques. Accordingly, academic institutions are in the precarious position of having to defend against ever-increasing threats deliberately hidden amongst the benign. State-sponsored and criminal actors continue to live off the land, using compromised credentials in conjunction with trusted utilities often natively available on the host operating system to conduct their actions on objectives. A deterioration in basic security hygiene practices including unpatched external resources and exposed services is often the catalyst for actors gaining initial access, and in many cases a malicious payload or the absence of obvious malware proves challenging for those institutions reliant on traditional AV or technology-based controls. The continued proliferation of malicious activity that blends in as legitimate administrative behavior warrants institutions to adopt a mix of technology and human-led hunting services to counter the ever-increasing threat.

2. Higher-risk Users Present Challenges

Academic institutions are more likely than organizations in any other industry to have a broad cross-section of users accessing their networks. With staff and students accessing academic networks, there is a wide range of ages, skills levels and online behavior to contend with. Further, rolling out regular security awareness training, and ensuring compliance across such a wide user base, is uniquely challenging. Adversaries are well aware that users can be the weak point in an academic institution’s defenses, making them an attractive target for both criminal and state-sponsored intrusions.

3. Dispersed Networks Constrain Effective Oversight

Due to nature in which academic institutions share information, there is a general culture of open connectivity with few security controls deployed at these interconnection points. The academic sector operates as a nexus of information and access for numerous additional sectors, creating a tantalizing prospect for threat adversaries. If a compromise occurs, it may cause ripple effects across multiple other verticals within a targeted region or country.

After finding their way into academic networks, actors turn their attention to discovery, often conducting extensive reconnaissance to identify additional resources within their reach. It is also common to see adversaries leveraging collections of compromised credentials in conjunction with RDP, various native and readily available file retrieval and transfer utilities, and network shares to move laterally between hosts in search of valuable information to support their objectives.

The aforementioned credentials are also combined with the use of various common command-line remote access tools including SSH and telnet to establish persistent access. In recent activity, Falcon OverWatch has also noted the use of alternate methods for preserving remote access such as the deployment and subsequent use of VPN clients, as well as legitimate remote administration utilities.

4. Widely Available Open Source Information Feeds Social Engineering Campaigns

Students, research fellows and professors eager to share their own research may also have their own websites outside of university networks. Although they may not be directly linked with the university, the association still exists. Often, these sites are mined for details supporting threat actor reconnaissance, later used for social engineering and phishing campaigns.

Recommendations

Although these threat adversaries are often highly sophisticated and can leverage complex tooling in their operations, defending against these attacks is not a lost cause. There are many security and intelligence solutions available to assist organizations in better understanding the threat adversaries, their TTPs and the tradecraft they regularly employ. In many cases, it is more important to have visibility as opposed to assuming security technologies alone will be capable of preventing attacks. Here is a list of some high-level recommendations:

- **Sensor Coverage.** You can't stop what you don't see. Organizations should deploy capabilities that provide their defenders with full visibility across their environment, to avoid blind spots that can become a safe haven for adversaries.
- **Technical Intelligence.** Leverage technical intelligence, such as indicators of compromise (IOCs), and consume them into a security information and event manager (SIEM) for data enrichment purposes. This allows for added intelligence when conducting event correlation, potentially highlighting events on the network that may have otherwise gone undetected. Implementing high-fidelity IOCs across multiple security technologies increases much-needed situational awareness.
- **Threat Intelligence.** Consuming narrative threat intelligence reports is a sure-fire method for painting a very vivid picture of threat actor behavior, the tools they leverage and the tradecraft they employ. Threat intelligence assists with threat actor profiling, campaign tracking and malware family tracking. These days, it is more important to understand the context of an attack rather than just knowing an attack itself happened, and this is where threat intelligence plays a vital role.
- **Threat Hunting.** Understanding technology will only get organizations so far is more important now than ever before. Security technologies are not 100%, and understanding technology is not infallible is the first step in coming to grips with the need for 24/7, managed, human-based threat hunting.
- **Service Provider.** Partnering with a best-of-breed service provider is a necessity. Should the unthinkable happen, organizations may require assistance responding to sophisticated threats.

Adopting even just one of these recommendations will go a long way in assisting organizations in strengthening the security strategy. The combination of all — or at least many — of these recommendations greatly enhances an organization's ability to defend and detect these threats with the goal of stopping a breach from occurring.

Conclusion

Due to the current environment, specifically as it relates to COVID-19, there is no expectation of threat activity slowing down in the nearterm. COVID-19 has introduced additional complexity into academia with remote schooling. The various vaccine research and development projects underway at academic institutions across the globe also make for attractive targeting. Criminals will continue to leverage ransomware as a means to disrupt academic networks, pressuring schools and universities into paying in order to restore operations as soon as possible. Additionally, nation-state actors will continue to target academia as a means of supplementing various intelligence-collection objectives primarily centered around political and economic espionage.

Additional Resources

- *Learn about recent intrusion trends, adversary tactics and highlights of notable intrusions identified by the CrowdStrike Falcon OverWatch team in our 2020 Threat Hunting Report.*
- *Read more about threat hunting in this blog, "Successful Threat Hunting Starts with a SEARCH."*
- *Read this analysis about a recent supply chain attack, "SUNSPOT: An Implant in the Build Process."*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent.*