



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Higher Education: An Attractive Target for Range of Malicious Actors

September 23, 2015

TLP: **WHITE** | *The NJCCIC assesses New Jersey's higher education institutions are increasingly attractive targets for a range of cyber threat actors due to breadth and value of data available on their largely accessible and often vulnerable networks.* One of the key cybersecurity challenges facing universities stems from their reliance on federated information technology systems, which allow for interoperability and information sharing between many decentralized components. Institutions involved with research and development in collaboration with the private sector, Federal government, or Department of Defense are at a high risk of network exploitation and intellectual property theft on behalf of sophisticated state-sponsored espionage groups, often referred to as advanced persistent threats (APTs). Furthermore, universities are soft targets for cybercriminals seeking to steal sensitive personal and financial data maintained by registrars and other administrative offices, as well as various criminal tactics such as [ransomware](#) or [point-of-sale malware](#). Universities are also frequently victims of website defacements and distributed denial of service (DDoS) attacks conducted by hacktivists and other malicious hacking groups.

- In May, Penn State University [announced two cyberattacks](#) against their College of Engineering which the FBI first brought to their attention in November of 2014. The subsequent investigation revealed the presence of two sophisticated threat actors on the college's network since at least September 2012; one of which was attributed to a China-based actor. While it was unclear whether any data was exfiltrated, the incident raised concerns due to Penn State's involvement in [developing sensitive technology](#) for the US Navy. A number of other US institutions have been targeted in 2015, including the [University of Connecticut](#), [University of Virginia](#), and [Harvard University](#).
- Beginning with an [attack during class registration](#) in November 2014, Rutgers University suffered a series of increasingly powerful DDoS attacks that ultimately resulted in [widespread disruptions](#) of the University's network in late April 2015. While the motive of the attack remains unclear, this incident underscores the challenges in attributing cybercrimes, particularly DDoS attacks that involve millions of IP addresses unrelated to the perpetrator. Moreover, it demonstrated the challenges organizations face in defending against DDoS attacks. Given the variety of attack methods, openly available DDoS tools, and consistent increases in malicious traffic volume, it is now incumbent upon organizations to implement a multi-faceted DDoS defense strategy.
- Universities are also prone to data breaches that can result in significant losses associated with regulatory fines and obligatory identity theft protection for victims, as well as class action lawsuits. In July, the University of California, Los Angeles announced a [breach of their healthcare system](#) which compromised 4.5 million patients' information, including unencrypted Social Security numbers and protected health information (PHI).

Recommendations

The NJCCIC advises higher education institutions to take proactive steps to reduce their cyber risk, beginning with comprehensive audits of their networks to identify and patch existing vulnerabilities in outdated operating systems, applications, servers, and websites. Colleges and universities should limit user privileges to only those systems and files required by one's position, and implement strict authentication policies incorporating mandatory password resets, minimum character requirements, and two factor authentication (2FA) for email, web services, and remote access tools. Additionally, encrypting systems and databases that contain sensitive personal information, user credentials, or intellectual property can mitigate the impacts of data breaches and render stolen data useless. In order to mitigate persistent DDoS threats, educational institutions are urged to consider establishing support relationships with their Internet Service Provider as well as a third-party DDoS mitigation service.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.