Homeland Security

INTELLIGENCE ASSESSMENT

(U//FOUO) Malicious Cyber Actors Target US Universities and Colleges

16 January 2015

Office of Intelligence and Analysis
IA-0090-15

Homeland Security
Office of Intelligence and Analysis
INTELLIGENCE ASSESSMENT
16 January 2015

(U//FOUO) Malicious Cyber Actors Target US Universities and Colleges

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

(U) Scope

(U//FOUO) This *Assessment* analyzes cyber threats to networks and systems supporting US higher education institutions and provides mitigation suggestions from REN-ISAC to assist federal, state, local, tribal, territorial, and private sector partners associated with .edu networks in identifying measures to protect against future malicious cyber operations.

(U) Key Judgments

(U//FOUO) **We assess that the primary cyber threat to US university and college networks is cybercrime and unwitting hosting of malicious activity, likely because the regular turnover of student network users and requirements for accessibility to the networks make the networks difficult to monitor and secure.**

(U//FOUO) **We assess malicious cyber actors targeting intellectual property and research are the emerging cyber threat facing university and college networks. Cutting-edge research and sensitive US government and cleared defense contractor projects are appealing targets for cyber actors looking to gain access to sensitive research programs and information.**

(U//FOUO) University Networks Face Common Cyber Threats

(U//FOUO) Malicious cyber actors have targeted US universities and colleges with typical cybercrime activities, such as spear phishing students and faculty with university-themed messages, creating fake university websites, and infecting computers with malicious software, likely in an attempt to gain access to student and faculty e-mail and bank accounts. We have no indication that cybercriminals target university systems and users more than any other cybercrime victims.

» (U//FOUO) According to sensitive DHS reporting, several different types of malware designed to gather personally identifiable information (PII) and exploit computer systems for financial gain—ransomware, clickfraud malware, and credential-harvesting malware—were found on computer systems of an identified US university in late August 2014. We do not know if PII was compromised or exfiltrated as a result of these infections.

» (U//FOUO) In February 2014, unknown cyber actors targeted departments at an identified US university with phishing messages containing malicious links, according to FBI reporting. Computers of recipients that responded were infected with ransomware requiring victims to pay between $50 and $500 to decrypt their computers, according to FBI reporting.

» (U//FOUO) In early 2014, malicious cyber actors successfully executed an e-mail phishing attack against 166 employees at an identified US university. The phishing message was embedded with a malicious link to a fraudulent university website that, when accessed, prompted employees to provide PII associated with their financial accounts. The actors successfully compromised the financial accounts of two employees, changing their direct deposit information so that money was delivered to an unspecified US bank, resulting in financial losses for the employees, according to an FBI contact with excellent access.

(U//FOUO) US universities and colleges have extensive computer networks and infrastructure making them ideal targets for unwitting hosting of malicious cyber operations, including denial-of-service (DoS) attacks and undetected storage of malware. As with cybercrime, we have no indication that malicious cyber actors target university and college networks for these activities any more than other networks.

» (U//FOUO) In early 2014, an unidentified cyber actor leveraged a supercomputer at an identified US university to initiate a DoS attack against the servers

of several identified US businesses that host servers for gaming activities, according to an FBI source with indirect access. The attack used about 98 percent of the university's bandwidth.

» (U//FOUO) Unidentified cyber actors used a named US university's web server as a file repository for distributing malicious tools, according to sensitive DHS reporting. Analysis of the web server confirmed that a number of malicious tools had been uploaded to the system, as of mid-2014.

(U//FOUO) University Networks May Be Target for Cyberespionage

(U//FOUO) While malicious cyber actors looking to exploit university and college networks for PII remain a consistent threat, we assess that the emerging cyber threat facing US university and college networks is cyberespionage actors seeking information and intellectual property. In addition to in-house, cutting-edge research, numerous US universities and colleges are involved in sensitive US government and cleared defense contractor research projects. These associations are very appealing to cyberespionage actors looking to gain access to sensitive research programs to exfiltrate information. University networks, which often have multiple levels of connectivity and accessibility to fuel collaboration, may present an easier target for cyberespionage actors than sensitive government or private industry networks. We have only a few examples of data exfiltration from university networks, but those we have lead us to judge that this activity does target research information and intellectual property.

» (U) According to reporting from a US cybersecurity firm, likely Iranian cyber actors, as part of a global espionage campaign, targeted universities in the United States, India, Israel, and South Korea from 2012 to late 2014. The cyber actors targeted research efforts, student information, student housing, and financial aid systems. According to the security firm, the cyber actors reportedly harvested confidential critical infrastructure documents from major educational institutions around the world.

» (U) A late-2013 review of the infrastructure associated with a probable foreign cyberespionage campaign indicated broad targeting of university computer systems, including those in the United States, the United Kingdom, and Israel, according to DHS reporting. The unknown actors successfully exfiltrated sensitive research information associated with university-affiliated medical organizations, including passwords and passport images.

(U//FOUO) Appendix: Best Practices and Mitigation

(U//FOUO) REN-ISAC provides the following recommendations to help US universities and colleges protect systems and networks against malicious cyber actors.

(U) Prevention

» (U) Educate and reinforce to students, faculty, and staff the threat from phishing attacks.

(U) Protection

» (U) Store data securely, e.g., in protected central storage or on devices with whole-disk encryption.

» (U) Have solid backup procedures to mitigate the risk posed by ransomware and other threats.

» (U) Protect networks where sensitive functions are performed, e.g., using access control lists or firewalls.

» (U) Have policies on secure deployment and maintenance of departmental systems. Include specific recommendations concerning problematic web content-management systems.

» (U) Enforce policies for strong passwords or passphrases, ensure that authentication is protected by encryption, and use multi-factor authentication where appropriate.

» (U) Aggressively patch operating systems and applications, and use inspection tools to identify out-of-date software.

» (U) Employ active protections and detections, such as intrusion detection systems, intrusion prevention systems, and domain name system (DNS) sinkholes.

(U) Monitor

» (U) Collect and store logs (e.g., DNS, network/port address translation, dynamic host configuration protocol, network access control, and authentication) and monitor network flow for incident discovery and response.

(U) Be Aware

» (U) Perform vulnerability scans and penetration testing of systems, applications, and networks.

» (U) Maintain awareness of threats to supervisory control and data acquisition and building control systems, and update and patch these systems regularly.

» (U) Assess the risks of insider threat, and take appropriate action.

» (U) Engage in a community of trusted peers (e.g., the REN-ISAC and the Multi-State Information Sharing and Analysis Center) to share information concerning threats and protection.

(U) Respond

» (U) Document and practice incident response and business continuity processes.

» (U) Have the technical capabilities and delegated authority to quickly block compromised hosts.

» (U) Cope with malware infections, such as through quarantine and remediation.

(U) Be Deliberate

» (U) Have an information security officer and a well-staffed and funded security team with technical expertise, executive support, and operational authority and accountability.

» (U) Train software developers and system administrators concerning secure practices.

(U) Be a Good Citizen

» (U) Conform to best practices, e.g., filter spoofed traffic at your border, eliminate open recursive DNS servers, and control protocols used in DoS amplification attacks to prevent systems on your network from being used against others.

(U) For further information, consult EDUCAUSE's Information Security Guide: "Effective Practices and Solutions for Higher Education."

(U) ***Source Summary Statement***

(U//FOUO) This Assessment is based on DHS and FBI reporting. Information from a private US cybersecurity firm was also used; this information has been shown to be largely accurate. We have ***high confidence*** *in our primary judgment that US university and college networks face a persistent threat as targets of opportunity for unwitting hosting of malicious cyber activity and cybercrime. Credible reporting provides relevant examples, and the prevalence of this activity across the cyber domain corroborates what we see targeting this sector. The absence of a large body of reporting regarding incidents in which cyber actors are observed targeting US universities and colleges to collect sensitive research information causes us to have* ***medium confidence*** *in the assessment that the emerging cyber threat facing university and college networks is malicious cyber actors targeting intellectual property and research.*

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870 or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) **Tracked by:** HSEC-1.1, HSEC-1.2, HSEC-1.8