Homeland Security

24 April 2020

(U) Cyber Mission Center

(U//FOUO) COVID-19: Cybercriminals Likely to See Opportunity to Exploit Academic Entities' Online Distance Learning Platforms and Users

(U//FOUO) Scope. This *Article* warns federal, state, and local departments of education and school administrators, information technology staff, network defenders, and law enforcement personnel of financially motivated cyber threats facing academic institutions, faculty, and students during the COVID-19 pandemic. For the purposes of this assessment, we define academic institutions as private and public pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. This *Article* considers cybercriminals to include actors seeking to profit from as well as save money through illicit cyber activity. This *Article i*s the latest in a series of assessments on COVID-19 cyber threats, including those associated with telework.[a,b,c] While this *Article* similarly addresses cyber threats associated with conducting legitimate activities remotely, it focuses on unique threats to educational institutions vis-à-vis schools that rely on distance learning alternatives. The information cutoff date for this *Article* is 8 April 2020.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC) and Counterintelligence Mission Center (CIMC). Coordinated with CBP, CISA, CWMD, FEMA, ICE, S&T, TSA, USCG, USSS, CIA, DIA, Department of Energy, Department of State, Department of the Treasury, FBI, NASIC, NGA, NIC, and NSA.

(U) Key Assumption

(U) Most US school districts as of 23 March 2020 are and will remain closed until the end of the academic school year or "until further notice" because of COVID-19, according to data provided by a Maryland-based online publication that provides scholastic news and analysis. This *Article* assumes that while pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools are closed, many are relying on internet-enabled distance learning (eLearning) alternatives in place of traditional classroom instruction.

(U//FOUO) We assess cybercriminals likely view schools' greater reliance on eLearning tools due to the pandemic as an opportunity to conduct a range of criminal activity against educational institutions, faculty, and students who use these tools. We base this judgment on examples of credential theft, advertisements of remote access, and cyber-enabled extortion against students, faculty, staff, alumni, and educational institutions.

(U) **Credential theft** is a cybercrime involving the unlawful attainment of an organizations' or individual's password(s) with the intent to access and abuse or exfiltrate critical data and information, according to a US network traffic analysis company.[1] Cybercriminals often work to identify users and devices that will provide access to sensitive data. Credential-based attacks open the door for more repeatable attacks, as they allow threat actors to assume the identity of users who are authorized to access targeted data, according to the same report.

[a] (U//FOUO) *Homeland Intelligence Article*, "Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear-Phishing Against Homeland Targets," published on 27 March 2020, serial number IA-43452-20.
[b] (U//FOUO) *Homeland Intelligence Article*, "Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic as an Opportunity to Exploit Enterprise Networks," published on 30 March 2020, serial number IA-43325-20.
[c] (U//FOUO) *Homeland Intelligence Article*, "Malicious Cyber Actors Likely See Opportunity to Target Virtual Private Network Vulnerabilities as More People Telework Due to COVID-19," published on 8 April 2020, serial number IA-43472-20.

» (U) **For cost savings:** Iranian Government-affiliated cyber actors from late 2019 to early 2020 were ordered to steal students' login credentials from universities throughout Europe, Australia, and the United States, according to a Dutch online press report citing a US consultancy firm claiming to have discovered the campaign.[2,d] The actors posted the credentials on a forum (that also hosts login data for approximately 5,000 educational institutions, including high schools) for Iranian students to access libraries and other resources to which they would not normally have access, according to the same report.

» (U) **For profit:** Cybersecurity researchers in March 2017 identified 13,930,176 e-mail addresses and passwords belonging to faculty, staff, students, and alumni at US higher education institutions (some freely available and others listed for between $3.50 and $10) on dark web sites—79 percent of which were uploaded within the previous 12 months—according to a US advocacy group's report on cybercriminal activity affecting US universities.[3] The report notes school credentials are attractive to buyers for three reasons: higher education servers are designed for many users, they are almost always on, thus giving malicious cyber actors confidence that compromised infrastructure will remain available for use; cyber actors are attracted to the vast amounts of innovative intellectual property at universities; and buyers can use university credentials to get discounts on popular goods and services normally reserved for students, faculty, and staff, according to the same report.

(U) **Identity theft:** Personally identifiable information (PII) can be any piece of information meant to identify a specific individual, which presents opportunities for financial gain to criminal entities who can open lines of credit or take out mortgages, according to an Irish multinational consumer credit reporting company's website.[4,e] The value of PII listed in underground forums ranges from $1 - $2,000, depending on the specific information, according to a second article from the same company.[5] We assume that actors steal PII from academic entities for financial gain. We also assume that eLearning necessitates additional use of file-sharing, collaboration, and communication platforms to which users must register with PII.

» (U) **PII for sale**: A Russian-speaking actor in 2016 advertised 4,000 datasets of compromised PII purportedly belonging to students at a US-based college, according to a US cybersecurity firm.[6] Five sample records that the actor provided indicated each dataset contained full names, dates of birth, home addresses, student e-mail addresses, and social security numbers, according to the same source.

» (U) **PII theft:** A cyber actor between January and November 2018 accessed a San Diego Unified School District student database and stole PII from over 500,000 staff members and students dating back to the 2008-2009 school year, according to a statement from the school district. The actor gained access by sending phishing e-mails that gathered login information belonging to approximately 50 staff members, according to the same source.[7]

(U) **Sale of remote access to compromised machines:** A US cybersecurity company in 2018 examined remote desktop protocol (RDP) shops on underground forums and found that cyber actors sold remote access to compromised computers for as little as three dollars.[8,f] RDP access to compromised computers is attractive to cyber actors because the computers serve as a proxy from which to conduct other illicit activities while it hides the attackers' true origin, allows attackers to access almost all information stored on the system, and enables attackers to install ransomware or cryptocurrency miners, according to the same source. A second US cybersecurity company in 2017 found an underground marketplace selling RDP access to over 85,000 compromised computers—approximately 75 percent of which were in the education sector—according to a blog

[d] (U) The US consultancy firm's public-facing website did not provide any information regarding this incident.
[e] (U) PII includes social security number, driver's license number, financial accounts, e-mail addresses, login credentials and passwords, addresses, phone numbers, and date of birth.
[f] (U) RDP is a proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet. This protocol provides complete control over the desktop of a remote machine by transmitting input such as mouse movements and keystrokes and sending back a graphical user interface. Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system. Attacks using the RDP protocol do not require user input, making intrusions difficult to detect.

post on the company's website.[9] A US information technology company detected the number of internet-exposed RDP endpoints grew from approximately 3.5 million on 20 January 2020 to 4.7 million on 20 March 2020.[10] The vast majority of the endpoints belong to organizations where remote access to a Windows computer is a frequent necessity, according to the same source.

» (U) Russian-speaking actors between 4 and 23 March 2020 advertised access to UK secondary school and French education center networks, according to three reports from a US cybersecurity firm.[11,12,13] The first report indicates that the actor was selling access for $900. The second report indicates that the actor gained remote access through RDP bruteforcing.[g] The third report indicates that the actor has RDP access to a host in the victim network that can access network drives, which contain files related to the European Union student exchange program.

(U) Extortion: Cyber extortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack, according to a US marketing firm.[14] A US cybersecurity firm assessed financially motivated extortionists' targeting calculus likely is influenced by the perceived net worth of the targeted organization, perceived value of sensitive information, perceived security posture, and the actors' assessment of the likelihood that a targeted organization will agree to extortion demands.[15] Cyber extortionists have sought monetary compensation in exchange for not disclosing student, parent, and school staff members' private information; or for unlocking encrypted data on educational institutions' networks.

(U) Extortion Through Disruptive Attacks

(U//FOUO) We did not identify an example of an actor leveraging denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks to extort or attempt to extort an educational institution; however, actors have demanded compensation from entities in non-educational sectors in exchange for not launching an attack or stopping an attack already in progress.[h,i]

» (U) Cyber actors as of February 2020 threatened Australian financial services sector entities with a sustained DoS attack unless a sum of cryptocurrency was paid, according to the Australian Cyber Security Centre.[16]

» (U) Cyber actors in March 2018 launched a DDoS attack against a network provider and demanded the victim pay extortion fees in exchange for stopping the attack, according to a US online publication.[17]

» (U) Cyber actors in 2017 compromised a Montana-based school district's network where they obtained information about past and present students, parents, and staff members including PII, private health information, personal information from counselors and social workers, and academic records, according to a Montana-based media report and the actors' ransom note.[18,19] The actors' ransom note also hinted that that students' private lives had been recorded through webcams on school-issued laptops. The actors demanded $150,000 in bitcoin in exchange for not publicizing the information, according to the same report.

» (U) Throughout 2019, 89 US universities, colleges, and school districts were victims of ransomware, potentially affecting operations at up to 1,233 individual schools, according to a New Zealand anti-malware

[g] (U) A brute-force attack consists of an attacker submitting every possible combination of characters that could exist in a password until the correct password is guessed. Passphrases are far more secure (and easier to remember) than complex passwords. For more information, please see https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords.

[h] (U) A DoS attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include e-mail, websites, online accounts, or other services that rely on the affected computer or network. A DoS condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.

[i] (U) A DDoS attack occurs when multiple machines operate together to attack one target. Attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large-scale attacks. DDoS attacks are normally more consequential than DoS attacks.

company.[20] Some ransomware groups since late 2019 have increased pressure on victims by threatening to disclose proprietary or potentially embarrassing information to competitors or the public under the assumption that such a release could be more costly than the ransom demand, according to a FBI private industry notification.[21]

(U) Mitigation

(U) **Credential Theft**: CISA notes that cyber actors can use legitimate credentials to expand unauthorized access, maintain persistence, exfiltrate data, and conduct other operations, while appearing to be authorized users. Leveraging legitimate credentials to exploit trusted network relationships also allows advanced persistent threat actors to access other devices and other trusted networks, which affords intrusions a high level of persistence and stealth. CISA recommended best practices for mitigating this threat include rigorous credential and privileged-access management, as well as remote-access control and audits of legitimate remote-access logs. For more information, please see https://www.us-cert.gov/ncas/alerts/TA18-276A.

(U) **RDP Exposure**: The Internet Crime Complaint Center (IC3) recommends auditing networks for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts. For more information, please see https://www.ic3.gov/media/2019/191002.aspx.

(U) **DoS and DDoS Attacks**: CISA notes that while there is no way to completely avoid becoming a target of a DoS or DDoS attack, there are proactive steps administrators can take to reduce the effects of an attack on their network, including enrollment in a DoS protection service, creation of a disaster recovery plan. CISA also recommends installing and maintaining antivirus software, configuring firewalls to restrict inbound and outbound traffic, and to evaluate security settings. For more information, please see https://www.us-cert.gov/ncas/tips/ST04-015.

(U) **Ransomware**: FBI recommends that users and administrators take preventative measures to protect their computer networks from ransomware infections. FBI also offers business continuity considerations and remediation measures in the event of a successful infection. For more information, please see https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

(U) **Identity Theft**: The National Security Agency (NSA) notes that identity thieves' goals may include (but are not limited to) character degradation, altering financial status, and/or creating legal problems. NSA recommends securing systems, limiting exposure (electronic and physical), applying application controls, and service partitioning (e.g. using different devices/OSes/browsers for activities of differing sensitivities) to safeguard against identity theft. NSA also provides recommendations for identity theft victims. For more information, please see https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-indentity-theft-threat-and-mitigations.pdf

(U) Reporting Computer Security Incidents
(U) **To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. 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) **To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every U.S. state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

(U) **Tracked by:** HSEC-1.2, HSEC-1.5, HSEC-1.8

(U) Source Summary Statement

(U//FOUO) This *Article* is based on an article from a Netherlands-based media outlet, a report from a US non-profit advocacy group, four reports from a US cybersecurity firm, one report from a New Zealand cybersecurity firm, a Montana-based weekly news outlet, a cyber actor group's ransom note, a statement from a US school district, and a private industry notification from the FBI.

(U//FOUO) Cybercriminals likely view schools' greater reliance on eLearning tools due to the pandemic as an opportunity to conduct a range of criminal activity against educational institutions, faculty, and students who use these tools. We have **moderate confidence** in this assessment based on the assumption that many US schools are relying on eLearning alternatives to traditional classroom environments and reporting that describes actors who have stolen login credentials for use and profit, actors who have stolen student PII, actors who advertise RDP access to schools, and extortion activities. We would have greater confidence in this assessment with information describing criminal actors' intent to exploit remote learning environments or the students and teachers participating in those environments. We would also have greater confidence in our assessment with more reputable sources describing the activities within this *Article*.

(U//FOUO) Our judgment that actors could steal login credentials to educational institutions is informed by a Netherlands-based media outlet of unknown reliability describing Iranian actors who provided stolen student credentials to Iranian students for use and a reliable US non-profit advocacy organization describes actors' sales of student credentials.

(U//FOUO) Our judgment that actors could profit from stolen PII is informed by a US cybersecurity firm's report on student PII advertised on an underground forum and a reliable US school district's official statement that describes a cyber-enabled theft of PII belonging to staff and students.

(U//FOUO) Our judgment that actors could sell access to educational institutions' vulnerable RDP endpoints is informed by three reports from a reliable US cybersecurity company describing advertisements of remote access to UK and French secondary schools.

(U//FOUO) Our judgment that actors could seek monetary compensation in exchange for not disclosing student, parent, and school staff members' private information is informed by a Montana-based media report of unknown reliability and a credible ransom note that describes the actors' attempt to extort $150,000 in Bitcoin in exchange for not publicly releasing the information. This judgment is also informed by a New Zealand-based anti-malware company that describes ransomware infections in US universities, colleges, and school districts in 2019 and a reliable FBI report that describes a new technique cyber actors employ to increase pressure on ransomware victims to acquiesce to ransom demands.

[1] (U); Awake Security; "Credential Theft"; https://awakesecurity.com/glossary/credential-theft/; accessed on 02 April 2020; Source is a reliable California-based network traffic analysis company.

[2] (U); Netherland Times; "Iranian hackers targeting Dutch universities: report"; 14 February 2020; https://nltimes.nl/2020/02/14/iranian-hackers-targeting-dutch-universities-report; accessed on 26 March 2020; Source is a Netherlands-based media outlet of unknown reliability or credibility that cites a credible US consultancy firm. Information directly from the US consultancy firm is unavailable.

[3] (U); Digital Citizens Alliance; "Cyber Criminals, College Credentials, and the Dark Web: A Security Challenge Facing U.S. University Communities"; March 2017; Source is a reliable US non-profit advocacy organization provides research and analysis on internet threats to consumers.

[4] (U); Experian; "What Is Personally Identifiable Information?"; 31 May 2018; https://www.experian.com/blogs/ask-experian/what-is-personally-identifiable-information/; accessed on 04 April 2020; Source is a reliable Irish-domiciled multinational consumer credit reporting company that collects and aggregates information consumers and businesses.

[5] (U); Experian; "Here's How Much Your Personal Information Is Selling for on the Dark Web"; 06 December 2017; https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; accessed on 04 April 2020; Source is a reliable Irish-domiciled multinational consumer credit reporting company that collects and aggregates information consumers and businesses.

[6] (U); FireEye; 16-00014834; "Actor Sells US College Student and Unnamed Bank Customer Data, Most Likely for Identity Theft Operations"; 29 September 2016; Source is a reliable cybersecurity firm that produces cyber threat, vulnerability, and risk assessments.
[7] (U); San Diego Unified School District; "Data Safety"; https://www.sandiegounified.org/datasafety; accessed on 26 March 2020; Source is a public school district based in San Diego, California whose reporting on this incident is credible.
[8] (U); McAfee; Organizations Leave Backdoors Open to Cheap Remote Desktop Protocol Attacks"; 11 July 2018; https://www.mcafee.com/blogs/other-blogs/mcafee-labs/organizations-leave-backdoors-open-to-cheap-remote-desktop-protocol-attacks/; accessed on 04 April 2020; Source is a US global computer security software company that has a history of credible threat reporting.
[9] (U); Flashpoint; "Dataset from "xDedic" Marketplace Suggests Government, Corporate RDP Servers Targeted"; 25 April 2017; https://www.flashpoint-intel.com/blog/cybercrime/xdedic-rdp-targets/; accessed on 06 April 2020; Source is a credible US cyber risk intelligence firm.
[10] (U); Reposify; "127% increase in exposed RDPs due to surge in remote work"; 30 March 2020; https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work; accessed on 08 April 2020; Source is a US information technology company of unknown reliability or credibility that maps the internet on a daily basis to help clients limit exposure.
[11] (U); FireEye; 20-00004926; "Threat Activity Alert: Russian-Speaking Actor 'Lannister' Advertises Access to Network of French Education Center"; 23 March 2020; Source is a reliable cybersecurity firm that produces cyber threat, vulnerability, and risk assessments.
[12] (U); FireEye; 20-00003801; "Threat Activity Alert: Russian-Speaking Actor Advertises RDP Access to UK Secondary School"; 4 March 2020; Source is a reliable cybersecurity firm that produces cyber threat, vulnerability, and risk assessments.
[13] (U); FireEye; 20-00005181; "Threat Activity Alert: Russian-Speaking Actor 'TrueFighter' Advertised Access to UK Secondary School"; 25 March 2020; Source is a reliable cybersecurity firm that produces cyber threat, vulnerability, and risk assessments.
[14] (U); TechTarget; "cyberextortion"; April 2018; https://searchsecurity.techtarget.com/definition/cyberextortion; accessed on 05 April 2020; Source is a US marketing firm of unknown reliability or credibility that delivers marketing services to business-to-business technology vendors.
[15] (U); FireEye; 17-00008613; "Mass Appeal of Cyber Extortion Continues to Influence Threat Actors' Strategies for Monetizing Compromised Networks"; 16 August 2017; Source is a reliable cybersecurity firm that produces cyber threat, vulnerability, and risk assessments.
[16] (U); ACSC; "ACSC aware of DDoS threats being made against Australian organisations"; 25 February 2020; https://www.cyber.gov.au/threats/acsc-aware-ddos-threats-being-made-against-australian-organisations; accessed on 06 April 2020; Source is a reliable Australian Government agency for cybersecurity.
[17] (U); TechCrunch; "New DDoS extortions hit the Internet"; 08 March 2020; https://techcrunch.com/2018/03/08/new-ddos-extortions-hit-the-internet/2018/03/08/new-ddos-extortions-hit-the-internet/; accessed on 06 April 2020; Source is a US online publication with a history or credible reporting on technology issues.
[18] (U); Flathead Beacon; "Authorities: Overseas Hackers Seeking to Extort Community with Cyber Threats"; 18 September 2017; https://flatheadbeacon.com/2017/09/18/authorities-overseas-hackers-seeking-extort-community-cyber-threats/; accessed on 06 April 2020; Source is a weekly news outlet of unknown reliability or credibility that serves the northwestern Montana area.
[19] (U); XXX; "Title"; http://1qb1ow3qfudf14kwjzalxq61.wpengine.netdna-cdn.com/wp-content/uploads/2017/09/Letter-with-redaction.pdf; 2020; accessed on 06 APR 2020; Source is a credible ransom note from TheDarkOverlord cyber actors.
[20] (U); Emsisoft; "The State of Ransomware in the US: Report and Statistics 2019"; 12 December 2019; https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/; accessed on 07 April 2020; Source is a New Zealand-based anti-malware company of unknown reliability or credibility.
[21] (U); FBI; Private Industry Notification 20200401-001; "Sodinokibi Ransomware Actors Adopt New Tactics"; 1 April 2020; TLP: White; Source is a reliable federal law-enforcement agency.