Report

Cybersecurity in Higher Education
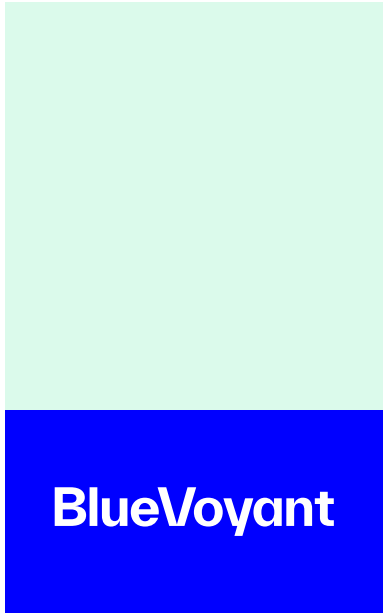## 2022

BlueVoyant
Digital Risk Protection

BlueVoyant

Table of Contents

BlueVoyant

Introduction

The higher education sector is going through an unprecedented period of change. Universities are embracing, or wrestling with, a host of new technologies and teaching methods - including a variety of apps, portals, and remote teaching technologies that support online or blended learning environments. As the nature of classrooms and the student experience changes, universities face new challenges, new demands, and new risks.

The year 2020, and in particular the COVID-19 pandemic, has put many of these changes and challenges in stark relief. Forced to abandon teaching in person, colleges have become more reliant on remote learning technologies. At the same time, financial pressures have skyrocketed as students postpone applications or demand rebates and refunds for classes they take in their bedrooms. Universities are staring down increasingly greater risks and slimmer financial margins.[1,2]

Against this backdrop, cybersecurity is more important than it has ever been. BlueVoyant analysis suggests that ransomware attacks against universities are becoming more frequent and more expensive. Data breaches are increasingly common, driven in part by colossal credential combolists sold and traded in dark web marketplaces, and a proliferation of login services across new technologies like Zoom, Chegg, ProctorU, and other third-party education partners. The attack surface for schools has metastasized, and there is no going back. BlueVoyant has undertaken this report in an effort to shed light on the cybersecurity challenges facing higher education. Online threats and vulnerabilities to education have never represented higher risk. This report uses open source and proprietary tools and datasets to examine that risk.

Using original data and research, this report outlines the higher education threat landscape today, delivering insights into the growing threat of ransomware attacks; the outsized impact of credential breaches; the knock-on consequences for schools in the form of credential stuffing attacks; and the prevalence of high-risk but easily-remediable vulnerabilities.

$447K

was the average cost of a ransomware attack in higher education in 2020
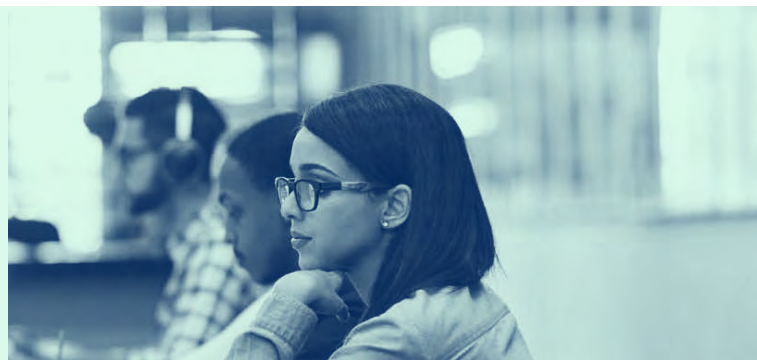
Key findings

Ransomware costs and number of ransomware attacks are both on the rise, stressing organizations already under intense financial pressure.

BlueVoyant analysis of open-source data shows that ransomware attacks against universities increased by 100% between 2019 and 2020. Worse, the pattern of "big game hunting" seen in other sectors - holding organizations to ransom for larger and larger sums of money - has now been observed among universities. The average cost of a ransomware attack in higher education in 2020 was $447,000. These attacks can be traced back to different threat actors using different tactics, techniques, and procedures (TTPs), but they are all disruptive and financially significant

University credential lists are massive and heavily trafficked in dark web markets - underpinning a huge volume of threats targeting accounts and vulnerable websites.

Student account and login data is among the most voluminous and highly trafficked PII data on the web. Not only do students maintain university accounts well past their graduation, but increasingly they use university accounts to log in to a wider range of services: administrative portals, remote video tools, university and student web applications, and remote learning tools. This proliferation of accounts drives a boom in data breaches - and a boom in threats targeting vulnerable websites.

The most common threats target the most common vulnerabilities.

BlueVoyant analyzed two sets of data. One used an automated analysis to search for vulnerabilities and threats observed across thousands of universities globally. The second used more in-depth and curated analysis to examine a smaller number of higher education institutions, broken down into top 10 schools, state schools, and community colleges. Across the field, all universities exhibited unsecured ports related to remote desktop and online databases. Many also showed evidence of poor email security configurations, leaving them exposed to phishing attacks.

Across the field, all universities exhibited unsecured ports related to remote desktop and online databases. Many also showed evidence of poor email security configurations, leaving them exposed to phishing attacks.

Threat Landscape

Historically, higher education institutions operated with a diverse threat profile, tracked closely by opportunistic criminals as well as nation-state actors. Universities have found themselves subject to conventional cyber attacks, such as fraud, cryptojacking, and data breaches, and sophisticated espionage operations sponsored by Iran, Russia, China, and the Democratic People's Republic of Korea (DPRK).[3, 4, 5]

Today, that threat landscape is shifting and being magnified. It's shifting because ransomware has emerged, as it has across all sectors, as a persistent and growing threat. The threat landscape is magnified because an ever-increasing reliance on mobile devices, remote learning, and third-party education partners is multiplying the higher education attack surface. Worse, these developments come during the most financially unstable period in recent higher education history.

The proliferation of devices is well-documented. An October 2019 survey by EDUCAUSE Center for Analysis and Research found 89% of U.S. students used smartphones in at least one course, 99% use laptops and 59% used tablets - 99% reported owning their phones and 97% said they owned their laptops.[6] A similar September 2020 study by Jisc, the UK's expert body for digital technology and digital resources in higher education, echoed high BYOD-usage rates for UK students as well: 93% used their own laptop for courses, 83% used a smartphone, and 29% used a tablet.7
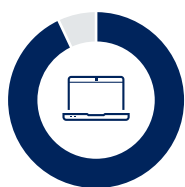
93%   **83%**   **29%**

The proliferation of third-party technologies and services is also well-documented, as blended learning environments - incorporating in-person teaching alongside mobile and online learning tools - have been on the rise for years.[8, 9] However, the COVID-19 pandemic has dramatically accelerated adoption of, and reliance on, these technologies. The risk profile for universities shows a corresponding rise, as more login points and more credentials become necessary for teaching. In the last

two years, breaches have occurred against ProctorU[10], BlackBaud[11], OneClass[12], Zoom[13,14],Handshake[15], Chegg[16, 17], proprietary remote-viewing software[18], administrative web apps[19, 20, 21], and student-designed university apps.[22,23] These breaches contribute to a growing body of stolen university credentials, which leads to increased, aggressive credential stuffing attacks.

There is even some evidence that the pandemic may be increasing the targeting of higher education institutions by nation-state actors - specifically targeting vaccine research. vaccine research. In July 2020, cyber and intelligence agencies from the U.S., U.K., and Canadian security officials issued a joint warning that Russian-linked advanced persistent threat actor APT29 (aka the Dukes, Cozy Bear) was actively targeting their national vaccine research and development organizations. However, traditional espionage against university-level research also persists. In October 2020, security researchers with Malwarebytes Labs revealed that an Iranian-linked APT, Scholar Kitten, was carrying out a wide-scale phishing campaign targeting universities across the globe.[25] In March 2019, the Wall Street Journal reported Chinese state-sponsored hackers targeted 27 institutions in the U.S., Canada and across Southeast Asia looking for naval military technology secrets. Among the U.S. colleges were the Massachusetts Institute of Technology, the University of Hawaii, Pennsylvania State University, Duke University and the University of Washington.[26]

"**Recent studies point to heightened cyber risk in the Higher Education space. According to the 2020 Ponemon study, the cost of a data breach in the education sector is $3,900,000. In a time of shrinking budgets, no school can afford to take a financial hit like this. The most prudent risk managers are responding to this threat by evaluating and deploying cyber risk transfer mechanisms via both contracts and cyber insurance.**"
JOHN FARLEY, CIPP/US, MANAGING DIRECTOR, CYBER PRACTICE, GALLAGHER

These developments all come as universities face severe restrictions on their spending and resources. Not only are universities facing pushbacks from current students, as discussed above, but also face critical revenue losses from the loss of international students, who cannot travel and who make up a non-trivial proportion of university fees.[27] An overwhelming 77% of CIOs and senior campus officials participating in a recent survey indicated "hiring and retaining IT talent" as the top institutional priority and 78% pointed to uncompetitive salaries and benefits as a significant issue to that goal.[28] A full two-thirds (67%) reported their "IT funding has not recovered from the budget cuts" imposed since the recession of 2008.[29]

The arrival of the pandemic after that survey suggests more stringent budget cuts to come: survey results by EDUCAUSE released in May 2020 show respondents are preparing primarily for IT budget cuts between about 5% and 30%.[30] Recent events, including the demands for rebates and refunds by students, indicate that things could get worse.[31, 32]

77%
CIOs indicated hiring & retaining IT talent is the top priority

Timeline

Of course, the rise of ransomware attacks is common across all sectors; but ransomware has fully made its way onto the higher education scene. This trend is global: a Freedom of Information (FOI request in the U.K.) revealed that 25% of all British universities had been victim to a ransomware attack in the last decade.[33]

BlueVoyant undertook an analysis of all open source cyber events affecting higher education institutions globally in the last two years - i.e., from January 2019 to date. The analysis excluded accidents, such as credential lists emailed to unintended recipients by mistake, or exposed databases that were discovered by a cybersecurity researcher.

BlueVoyant researchers constructed a timeline using this analysis, which revealed certain key insights:

First, ransomware is the No. 1 threat facing universities - and ransomware events doubled from 2019 to 2020. Ransomware is expensive: the average cost for ransomware attacks in higher education in 2020 is $447,000.

Second, data breaches were the No. 2 threat facing universities - making up half of all events in 2019. More than one-third of all data breach events were related to remote or blended learning tools - including Zoom, Chegg, and ProctorU. These can include Personally Identifiable Information (PII) as well as login credentials.

Third, data theft by nation states is a real threat - affecting over 200 universities in the past two years. Five separate nation-state campaigns were publicly identified, though the real number is likely to be much, much higher - whether because, when identified, these campaigns are not revealed in the press, or because they are not identified at all.

Ransomware attacks have largely followed patterns seen in other sectors. The major ransomware families are Clop, Ryuk, NetWalker and DoppelPaymer. The attack on Monroe College in July 2019, for 170 Bitcoin (approximately $2 million), appears to be the first of the big game hunting attacks observed in other sectors. And, just as we have seen with ransomware overall, a large number of colleges and universities hit after April 2021 faced the additional ignominy of "name and shame" extortion schemes.

Open source cyber events affecting higher education institutions globally

■ Data breach events ■ Ransomware events
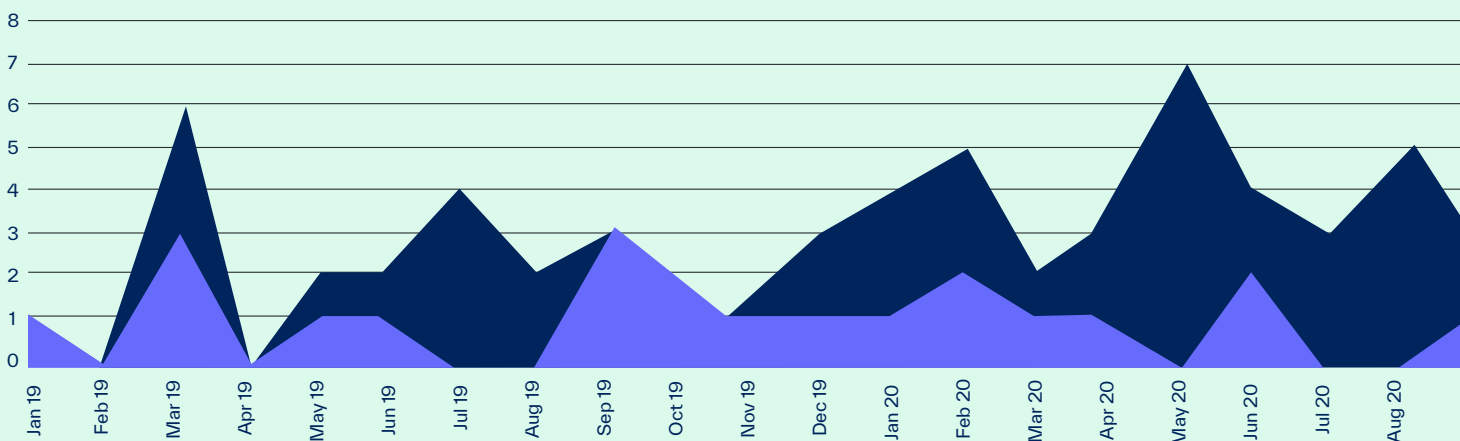
Password Analysis:
Revisiting the ABCs & 123s

The most commonly used passwords are known and available to threat actors. Dark web and underground forums where unspeakably large data sets are bought, sold, traded, and given away for criminal credibility are populated by everyone from small time crooks to global intelligence organizations.34 And, while some custodians of sensitive password information are getting better at protecting this data, malicious actors are also getting better at pilfering it. Data breaches have splashed across news headlines for decades. Most people don't even pay much attention anymore, but as Stuart Panensky, partner at FisherBroyles notes,

"The education and learning sciences sectors face unique privacy and cyber risks due to the combination of sensitive data they traffic in, the nature of how technology is deployed throughout the sector and the myriad of state and federal laws and regulations that govern these issues."

While these headline-grabbing data breaches are tremendously detrimental to personal and organizational privacy and security, for every breach that is made publicly known, there are countless others that go unreported. "Private collections" of sensitive data command sums in the thousands of dollars, while older (but no smaller) breaches are posted for trivial sums or distributed for free.[35]

Many data breaches include payment card information (PCI), protected health information (PHI), or social security numbers, home addresses and other PII. These breaches can be leveraged for tremendous criminal gain in schemes involving account takeover, identity theft, financial fraud, and other online criminal pursuits.

The topic at hand focuses on a different data set: the combolist. Combolists are succinct data sets consisting of only accounts and passwords and take the form:

They are used to achieve unauthorized access into victims' accounts and email inboxes. Unauthorized entry into an online account is considered a felony under the Computer Fraud and Abuse Act (CFAA).

Email address: Password

Account Login: Password

Login

When Bullies Come Knocking

In this report, we will explain various techniques behind account takeover. Here we define the most common, applicable attack methods:

Credential stuffing:

A type of cyber attack where stolen account credentials, typically consisting of lists of usernames and/or email addresses and the corresponding passwords, are used to gain unauthorized access to user accounts through large-scale automated login attempts.

Brute-forcing:

When an attacker systematically submits many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Dehashing/cracking:

The process of recovering passwords from data that has been stored in an unsalted hashed form. Hashes are scrambled versions of passwords that services use to enhance security practices, however, hashing is not cryptography and many hashes can be "cracked" or guessed.

Schoolhouse Rock

In order to access your education email inboxes, software accounts, VPN connections, and other critical systems necessary for higher education, cybercriminals proceed strategically and efficiently.

There is a document, widely available on the open internet, called the RockYou.txt file. RockYou is a list of 14,344,391 of the most commonly-used passwords. This list, among others, exists to aid cybercriminals in credential stuffing, brute-forcing, or dehashing your passwords.

On the internet, RockYou.txt file is a list of

14,344,391

of the most commonly-used passwords

BlueVoyant cross-referenced publicly available combolists, with credential counts in the billions, in order to identify unique credentials related to .edu domains. Using that analysis of education email and password combinations (which includes hashed passwords), 8.945% - a figure in the millions - of those passwords made exact matches with passwords found on the RockYou list. In other words, passwords for education accounts are easily found online - and number in the millions.

Chug, Chug, Chegg!

Chegg is an online textbook rental service that also provides college-level students with homework help and assignment resources. In April 2018, Chegg suffered a data breach that impacted 40 million subscribers.
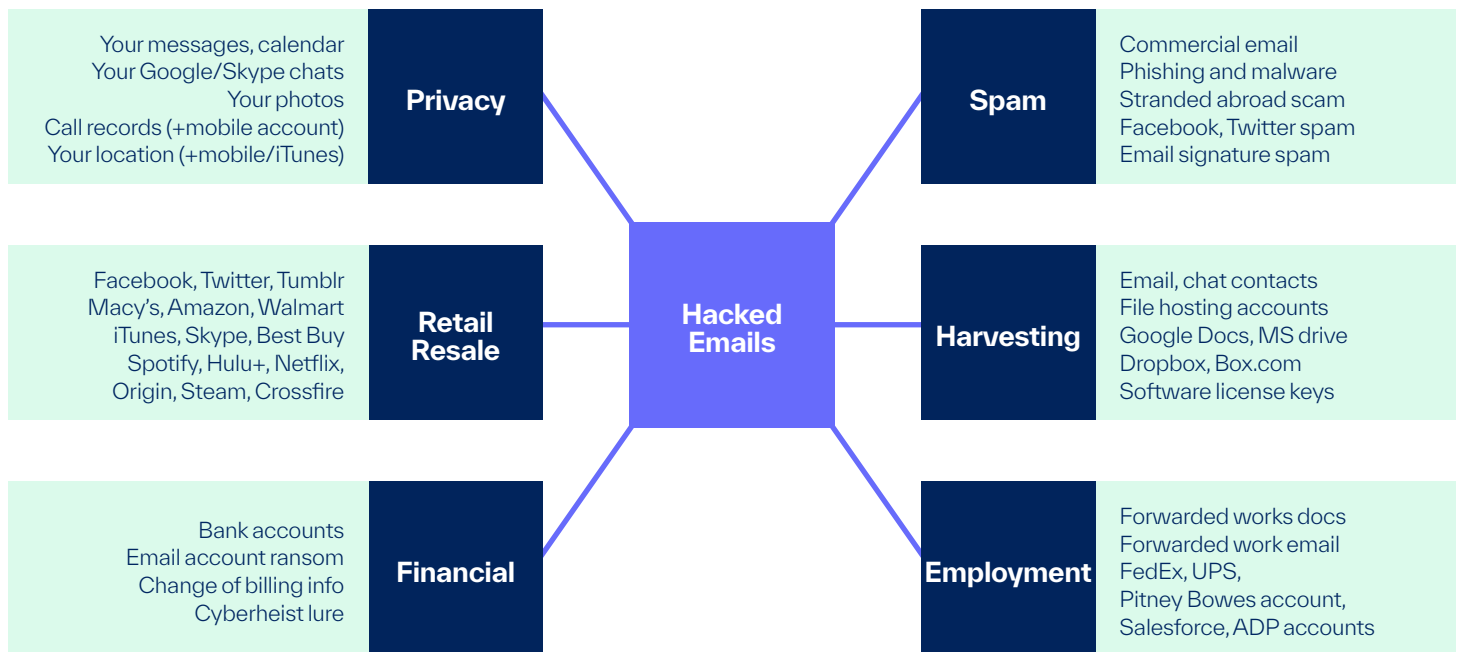
The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes.[36] As might be expected, a textbook rental service, deeply embedded with many universities, included a majority of compromised .edu emails. There are 5,127,069 .edu email addresses exposed in this data set (the others likely comprising personal email addresses).

In late 2020, Boston University had to temporarily disable over 1,000 student email addresses after their email servers were flooded with spam from compromised legitimate student email addresses.[37] Students were forced to reset their passwords, since threat actors had achieved access using the passwords found in the Chegg breach.

BlueVoyant analysts observed 11,442 @bu.edu email addresses in the Chegg breach data. These passwords were stored (and later distributed) in hashed MD5 form. However, MD5 hashes are one of the hashing algorithms that has fallen into the dustbin as cracking practices have advanced.[38] In fact, for more than two years since before the breach, unsalted MD5 hashes were easily crackable: "Less than 10 seconds later, [popular cybercriminal dehashing software] Hashcat cracked that password. On my commodity Windows laptop."

5,127,069.edu
email addresses exposed in Chegg data breach.

Affected students lost access to their email inboxes, teaching resources such as BlackBoard and the BU student portal, and campus Wifi. Their educational experience was halted in its tracks. Perhaps more importantly, it opened the students up to a flood of cybercriminal activity that derives from email account access. Credential re-use could have exposed countless other accounts, including financial, retail, or personal.

Your messages, calendar Your Google/Skype chats Your photos Call records (+mobile account) Your location (+mobile/iTunes)	**Privacy**	
Facebook, Twitter, Tumblr Macy's, Amazon, Walmart iTunes, Skype, Best Buy Spotify, Hulu+, Netflix, Origin, Steam, Crossfire	**Retail Resale**	**Hacked Emails**
Bank accounts Email account ransom Change of billing info Cyberheist lure	**Financial**	

Spam	Commercial email Phishing and malware Stranded abroad scam Facebook, Twitter spam Email signature spam
Harvesting	Email, chat contacts File hosting accounts Google Docs, MS drive Dropbox, Box.com Software license keys
Employment	Forwarded works docs Forwarded work email FedEx, UPS, Pitney Bowes account, Salesforce, ADP accounts

Cybersecurity reporter Brian Krebs created a succinct graphic to demonstrate all of the criminal uses an email account offers - many of which the average user would never have considered.

As Boston University's Executive Director of Information Security wrote at the time:

"Everywhere the individual uses the same password has it protected by the company with the weakest security […] The more places you use it, the more likely it is that it will be compromised, and if it becomes compromised you are giving away access to your email, your student records, and potentially health and financial information."[39]

Psych 101

Passwords, unless they are automatically generated, are a reflection of our routines, lifestyles, preferences, and general psychology generally. Passwords are about the people and animals we call family, they are about our favorite sports teams, and they are sourced from our addresses, birthdays, anniversaries, and our desires. Passwords often derive from the most important people, places, and events of our lives.

If psychology is a science based on patterns of the human mind, passwords are a body of evidence that gives us unseen insights into the way that people think. Across a large body of password data, repeating patterns can be unexpectedly revealing.

Sometimes, the instructor can be distracting to the point that it shows in a student's password:

1hotprof	Columbus State Community College
hotprof2	NYU and Columbia University
sexy!teacher1	Florida State University
sexyteacher03	University of Alabama
hot4teacher1111	Florida Gulf Coast University

Unsurprisingly, many college kids have sex on their mind. The word appears in 13,496 .edu passwords within the Chegg breach data.

But if your teacher isn't so hot, you might find yourself bored in class. The word "bored" appears in 613 of the compromised passwords, "boring" in 126. Here are some examples:

imbored!	University of Virginia
boredsilly	Springfield College
boredatwork	University of Wisconsin - Madison
boredcollegekid1	Appalachian State University
boredguy995	University of Maryland - Baltimore County
imfucknbored	Kent State University
bored2tears	Baylor University
boredtodeath	Temple University
imbored420	Arkansas State University
Schoolisboring09	Middlesex Community College
wellthisisboring	NYU

Other times, a student's ire can be more extreme:

1damnclass	Indiana State University
kill_the_Professor	North Carolina State University

Passwords are a reflection of our routines, lifestyles, preferences, and psychology

Passwords can reveal the overachievers:

aplusgrades	University of Florida
highgrades	University of Minnesota
supergrades	St. Petersburg College
keepgoodgrades	Clarkson University
Goodgrades.	Bowling Green State University

And the slackers...

stupidgrades	Baylor University
lowgrade712	University of Alabama
h8grades	Calvin University
nowfailingoutofschool	Illinois Wesleyan University
striveforfailure	University of Illinois Urbana-Champaign

The slackers should spend more time in the... library. The word "library" appears in 1,185 email passwords. If a student isn't studying in the library, they might be in the "cafe" (714), drinking "coffee" (2,777) or, when really in need of a pickmeup, "redbull" (602).

If an upperclassman puts in their time "study"ing (1,630 counts), then perhaps they've earned a "beer" (3,408) or a trip to the "gym" (4,825). Maybe they're eager to meet their "girlfriend" (128) or "boyfriend" (175) at a nearby "frat" (467) "party" (2,634).

BlueVoyant encourages all "student"s (5,490) to hit the "book"s (20,984) hard and major in "computer" (4,505) "science" (1,607) or a related field. The "smart" (3,139) ones can apply for a "job" (6,800) or a "career" (1,541) at BlueVoyant... just so long as their password isn't simple enough that it is based on the word "password" (65,420).

Top word usage in passwords

Party 2,634	Coffee 2,777	Smart 3,139
Beer 3,408	Computer 4,505	Gym 4,825
Student 5,490	Book 20,984	Password 65,420

Threat intelligence analysis

In the preparation of this piece, BlueVoyant analyzed almost 3,000universities - 2,702 - across 43 different countries to identify the broadest possible patterns of vulnerability and risk.

The returns were exhaustive, but several insights stood out:

More than half of all analyzed universities and colleges lacked all basic email security configurations. DNS-based email security protocols - SPF, DKIM, and DMARC - authenticate emails between users and protect against phishing attacks. 66% of universities had none of these configurations in place.

More than one-fifth of all analyzed universities and colleges had open or unsecured remote desktop ports. Open remote desktop protocol (RDP) ports are the No. 2 threat vector - behind phishing - for ransomware gangs.[40] 22% of all universities had at least one open RDP port.

Almost 40% of all analyzed universities and colleges had open or unsecured database ports.BlueVoyant observed open or unsecured MySQL, Microsoft, and Oracle database ports on 38% of all observed institutions.

BlueVoyant excluded accidental database breach events from the events timeline above, but such breaches make up a non-trivial number of cyber events affecting universities (at least 1/10th of all identified events in open source reports).

Eighty-six percent of all observed universities and colleges showed evidence of inbound botnet targeting. The rise of botnet activity over the past year has been a major feature of cybersecurity news, more so as many active botnet families are in sudden resurgence - including Andromeda and the relatively ancient Conficker worm. Regardless, these botnets can be responsible for significant damage and compromise to targeted networks.

66%
of universities lacked all basic email security configurations

22%
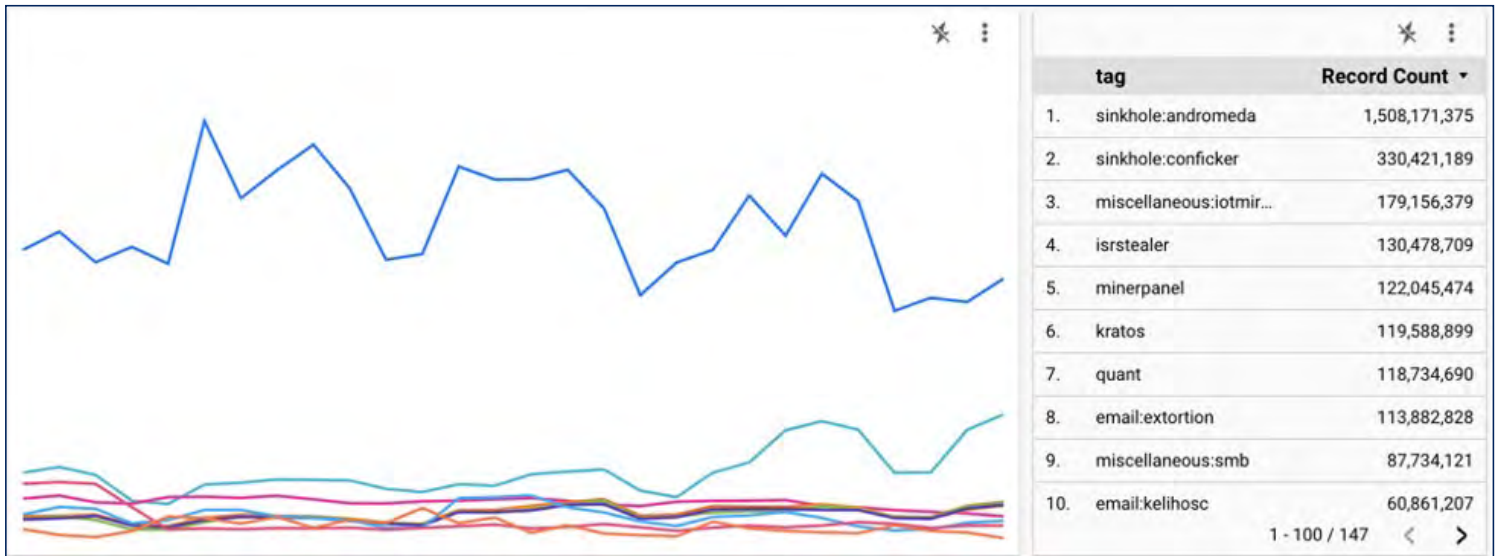of all universities had at least one open RDP port

38%
of all analyzed universities and colleges had open or unsecured database ports
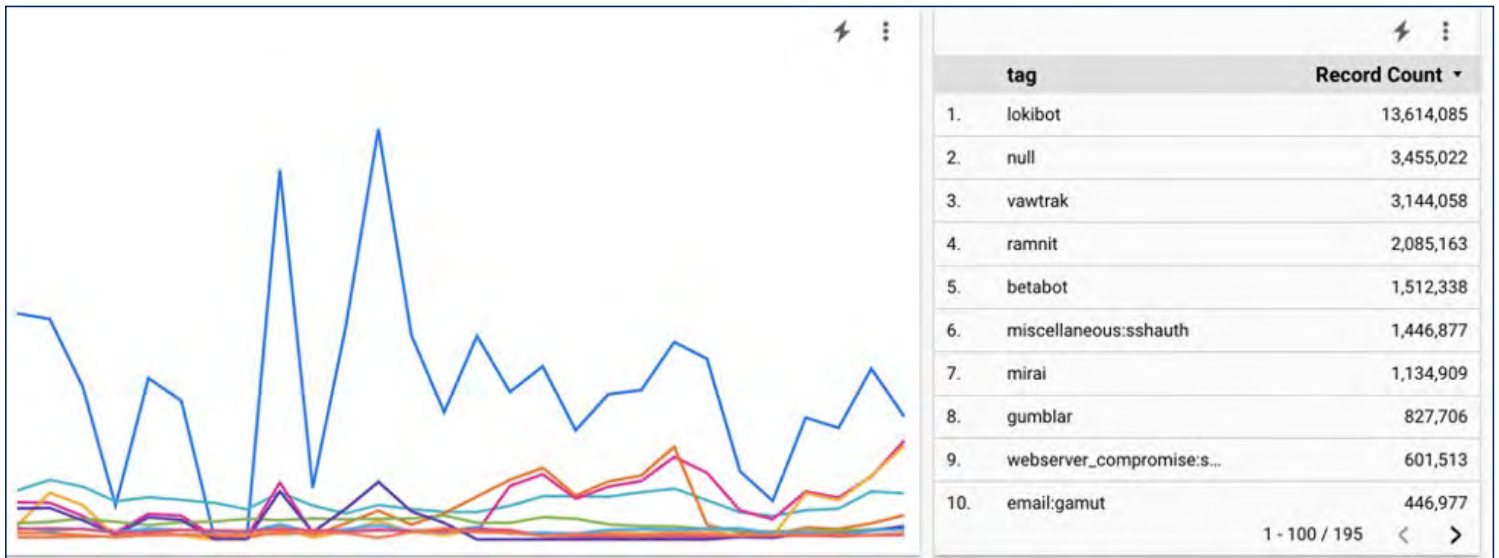
86%
of all observed universities and colleges showed evidence of inbound botnet targeting

The graph showing inbound targeting below simply describes the volume of targeting. Outbound activity, on the other hand, describes the massive (13 million) count for observed compromised devices.

	tag	Record Count ▼
1.	sinkhole:andromeda	1,508,171,375
2.	sinkhole:conficker	330,421,189
3.	miscellaneous:iotmir...	179,156,379
4.	isrstealer	130,478,709
5.	minerpanel	122,045,474
6.	kratos	119,588,899
7.	quant	118,734,690
8.	email:extortion	113,882,828
9.	miscellaneous:smb	87,734,121
10.	email:kelihosc	60,861,207
		1 - 100 / 147 < >

A monthly count of inbound botnet targeting for all observed (2,702) universities.

	tag	Record Count ▼
1.	lokibot	13,614,085
2.	null	3,455,022
3.	vawtrak	3,144,058
4.	ramnit	2,085,163
5.	betabot	1,512,338
6.	miscellaneous:sshauth	1,446,877
7.	mirai	1,134,909
8.	gumblar	827,706
9.	webserver_compromise:s...	601,513
10.	email:gamut	446,977
		1 - 100 / 195 < >

A monthly count of outbound botnet targeting for all observed (2,702) universities.

Deep dive analysis

In addition to the broad scope analysis above, BlueVoyant also produced insights into a smaller pool of universities with more in-depth analysis.

BlueVoyant selected a variety of higher education institutions with widely varied structures, offerings, and online infrastructures. The 30 institutions below reflect the diversity present in the U.S. higher education sector: research institutions with large legacy networks of hundreds of thousands of domains and IPs; state schools with enormous student bodies; and community colleges with more varied and dedicated online programs and services.

BlueVoyant conducted full, passive risk and threat analyses across all 30 schools looking for distinct patterns and trends, but especially looking to identify vulnerabilities that matched the known threat vectors and known risks facing higher education today. The analysis pulled out some interesting insights.

State

Institution	Number of students
Ohio State	66,444
Georgia Tech	36,489
UFlorida	8,231
UMichigan	44,718
UVirginia	25,018
UC Irvine	33,467
UNC	29,469
UCLA	45,742
UC Santa Barbara	26,314
UC San Diego	35,821

Top Ten

Institution	Number of students
UC Berkeley	4,1910
UChicago	14,739
CalTech	2,233
Stanford	17,249
Columbia	33,413
Yale	13,609
MIT	11,520
UPenn	22,432
Harvard	20,970
Princeton	8,623

Community College

Institution	Number of students
New Mexico Military Institute	412
Valencia	4,2631
Western Iowa Tech	5,674
Fox Valley Technical College	10,888
Lake Area Technical College	2,245
Cloud County	1,187
Mitchell Technical Institute	1,839
Indian Capital Technology Center	15,134
University of South Carolina Lancaster	1,588

All 30 universities showed evidence of torrenting on their networks. Torrenting is a popular method of sharing large, distributed files easily online - typically, pirated movies, games, music, and other content. Students love to use torrents, since they provide access to huge libraries of media content for free. Free, that is, except for the large amounts of malware that are often bundled along with the "free" media in the .torrent file.

Speaking of gaming, all 30 universities also had observations of gaming devices on their networks - no surprise, of course, except sometimes for the sheer scale of gaming activity. Georgia Tech had more than 4,400 gaming consoles visible on their networks. Ohio State had more than 8,000. But the laurel goes to the University of Florida, which had just shy of 4,000 consoles - not as much as Ohio or Georgia Tech, maybe, but per capita that amounts to one gaming device for every two students. Kudos, Florida.

All 30 universities had unsecured ports. More concerning, three-quarters of these universities had open remote desktop ports, and over 60% had open database ports - meaning that most universities have glaring weaknesses for the most common threats to higher education (ransomware and data breaches). Sometimes, these vulnerabilities appeared in extremely high numbers. For example, just under .5% of the Ivy League school IPs had an open RDP or open database ports, which amounts to almost 10,000 ports. Similarly, just under 1% of all state school IPs had the same vulnerability: that amounts to over 22,000 ports.
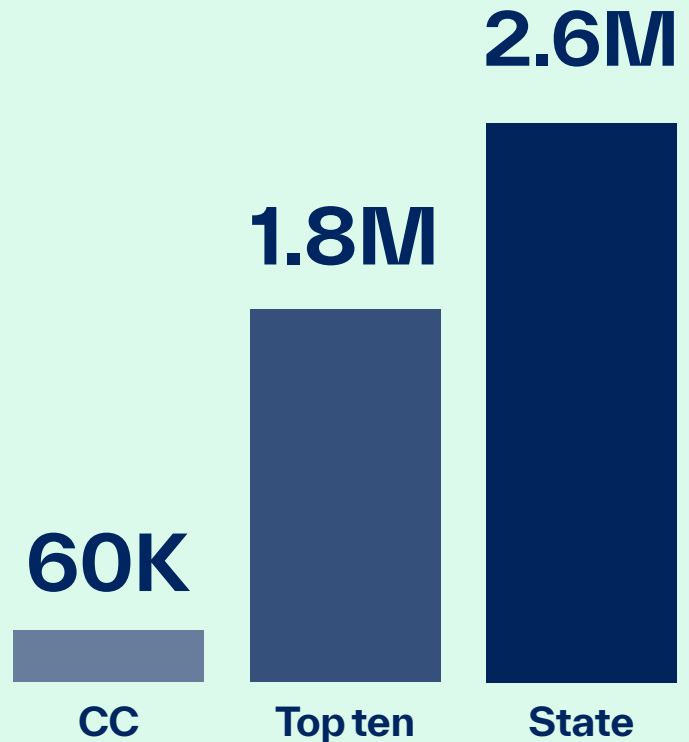
Breached PII data

Unique credential counts observed by BlueVoyant, collated according to higher education category.

All 30 universities had unsecured ports

60%
Had open database ports

meaning that most universities have glaring weaknesses for the most common threats to higher education

While these are interesting data points, the real shock is the scale of credential data available. The 2019 Verizon Data Breach Report indicated that 53% of all observed attacks against colleges and universities involved stolen credentials.[41]

These credential totals are well in excess of numbers found for any other sector. For example, while the current total number of all students in all state schools analyzed by BlueVoyant amounts to roughly 160,000, the number of unique credentials observed is roughly 2,600,000 - more than over six times the total number of students. For comparison, the number of state school credentials available in publicly-exposed combolists is equivalent to the total number of credentials possible for the last 24 years of state school graduates.

For Ivy League schools, the total is even more exaggerated - the amount of unique credentials found was 13 times the total number of current top ten school students.

There are many reasons why this should be the case. Students use their university and college email addresses long after they graduate. The credentials also include faculty and visiting staff. Regardless, the outsized figures are responsible for driving an extraordinary volume of targeted attacks against login and other vulnerable webpages across university online space.

10K
Brute force attacks per institution per week

Number of brute force attempts

143,605 — CC
33,981 — Top ten
159,950 — State
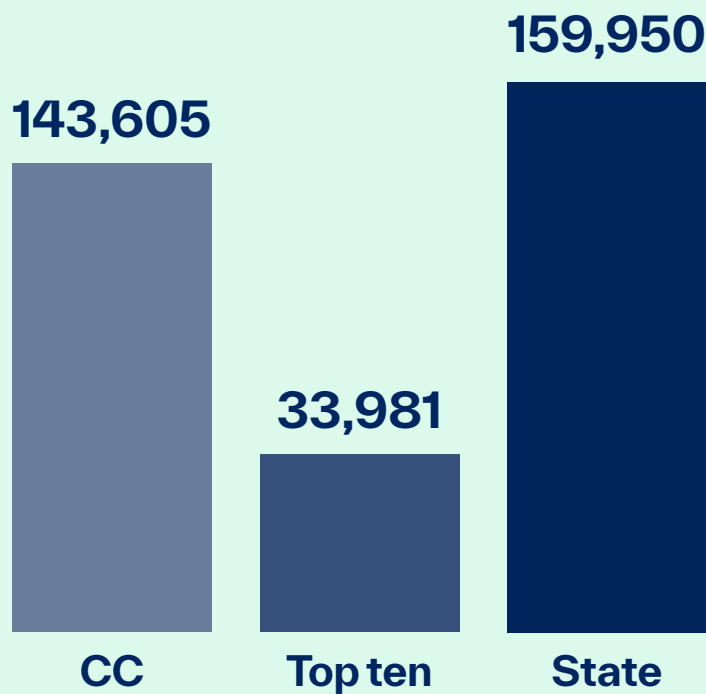
Brute force attempts in one week against state, Ivy, and community colleges.

The table above shows total figures for brute force (or credential stuffing) attacks against identified university login webpages. Inbound scanning and probing events occur daily in high volume against institutions across all sectors. Brute force attacks, however, normally constitute a much smaller proportion of all inbound adversarial activity observed by BlueVoyant analytics.

These high brute force figures are driven by the massive numbers of available university credentials for sale (or available for free) online - an average of 10,000 brute force attacks per institution per week. Such attacks lead directly to compromise of critical networks of critical networks, including email accounts, portals, and third-party services.

Recommendations: Looking Forward

For now, universities need to recognize cybersecurity as a critical factor of their success - and survival - in the years to come.

Higher education is entering a period of profound change. Even after classes resume in full - even after students return to classrooms en masse - the shift toward fully blended learning environments has taken an irrevocable step forward. For now, universities need to recognize cybersecurity as a critical factor of their success - and survival - in the years to come.

Securing learning environments for students, as well as the data and credentials owned and managed by universities, are paramount concerns for any higher education institution.

Thankfully, most of the risks outlined in this report are remediable. Strong cybersecurity requires several layers of defense, which should be systematically implemented over time.

In addition, there are several simple steps that can be taken to reduce the risk, including the four actions listed below:

Ensure multi-factor authentication (MFA) using a cloud-based single sign-on (SSO) solution, such as Azure AD or Okta.

MFA should be implemented across all accounts. This is present in some higher education institutions, but not a sufficient percentage and has far too many exceptions in most organizations. The vast majority of account compromise will be prevented with just this one additional step of authentication. By enabling SSO, you will also streamline your user's logon experiences as well as your ability to detect and respond to any compromises that do successfully manage to defeat MFA.

Develop baselines and anomaly alerting for all logins.

You must understand your users' login patterns, and develop visibility into baseline as well as deviation from normal user activity for authentications events across all systems and services.

Ensure all passwords are screened for compromise and malicious activity.

Even if passwords are secured through MFA, knowing that an account password has been breached and is actively being explored for compromise will help you defend your user accounts from potential takeover, or denial of service by forcing a system lockout.

Deploy layered email security for all email accounts.

Phishing is still the origin for more than 90% of cyber incidents. You must regularly and actively attempt to phish your own users to help improve their awareness. You can also drastically reduce risk of phishing by ensuring you have SPF, DKIM and DMARC records all configured according to best practices for each. In addition to anti-phishing, all attachments and URLs in any email should be scanned and automatically checked against threat and reputational databases to avoid directing users to malicious websites or compromise of their machines or data.

Sources

1. https://www.weforum.org/agenda/2020/11/covid-19-higher-educationand-the-impact-on-society-what-we-know-so-far-and-what-could-happen/

2. https://time.com/5883098/higher-education-broken-pandemic/

3. https://www.insidehighered.com/news/2020/06/11/colleges-faceevolving-cyber-extortion-threat

4. https://www.fireeye.com/blog/executive-perspective/2019/04/highereducation-faces-a-unique-cyber-threat-landscape.html

5. https://www.insidehighered.com/news/2019/03/06/report-topuniversities-us-targeted-chinese-hackers

6. https://library.educause.edu/-/media/files/library/2019/10/2019ssinfograph.pdf?la=en&hash=5E6F-0F5E29347E57526F808D8B10CE79993DCEEF

7. https://www.jisc.ac.uk/sites/default/files/student-dei-he-report-2020.pdf

8. http://www.newschools.org/wp-content/uploads/2019/09/Gallup-Ed-Tech-Use-in-Schools-2.pdf

9. https://www.cnbc.com/2020/06/08/ed-tech-how-schools-educationindustry-is-changing-under-coronavirus.html#:~:text=Even%20before%20the%20outbreak%2C%20education,look%20for%20learning%20resources%20online.

10. https://www.bleepingcomputer.com/news/security/proctoruconfirms-data-breach-after-database-leaked-online/

11. https://www.blackbaud.com/securityincident

12. https://www.forbes.com/sites/leemathews/2020/06/28/oneclassaccidentally-exposed-millions-of-student-records/#730b74dc3f90

13. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

14. https://www.cpomagazine.com/cyber-security/half-a-million-zoomaccounts-compromised-by-credential-stuffing-sold-on-dark-web/

15. http://udreview.com/handshake-security-breach-affects-thousandsof-university-students/

16. https://ndsmcobserver.com/2019/10/saint-marys-email-addressesappear-in-credential-dump-following-chegg-data-breach/

17. https://dailyfreepress.com/2019/10/10/following-flood-of-spamemails-more-than-1000-student-accounts-temporarily-disabled/

18. https://news.sky.com/story/warwick-university-was-hacked-and-keptbreach-secret-from-students-and-staff-11978792

19. https://databreaches.net/hackers-breach-62-us-colleges-by-exploiting-erpvulnerability/

20. https://www.news.gatech.edu/2019/04/02/unauthorized-accessgeorgia-tech-network-exposes-information-13-million-individuals

21. https://www.databreaches.net/ph-san-beda-student-portal-hackedpersonal-data-of-thousands-stolen/

22. https://www.9news.com.au/technology/get-ticketing-data-privacy/f7343ce6-a8ab-4b19-9604-8503b313b204

23. https://mailchi.mp/fountainhopper/foho-89startup-garage-projectqueer-chart-exposes-data-on-200-stanford-students-team-allegedlyknew-about-vulnerability-according-to-tipsters

24. https://www.cnn.com/2020/07/16/politics/russia-cyberattack-covidvaccine-research/index.html

25. https://blog.malwarebytes.com/malware-bytes-news/2020/10/silentlibrarian-apt-phishing-attack/

26. https://www.wsj.com/articles/chinese-hackers-target-universities-inpursuit-of-maritime-military-secrets-11551781800?mod=hp_lead_pos1

27. https://hechingerreport.org/losing-international-students-because-ofthe-pandemic-will-damage-colleges-financially/

28. https://www.campuscomputing.net/content/2019/10/15/the-2019-campus-computing-survey

29. https://static1.squarespace.com/static/5757372f8a65e295305044dc/t/5da60e-02c69e0005bf93690e/1571163656824/Campus+Computing+-+2019+Report.pdf

30. https://er.educause.edu/blogs/2020/5/educause-covid-19-quickpoll-results-itbudgets-2020-2021

31. https://www.chicagomaroon.com/article/2020/4/21/student-petitionhalve-tuition-gains-1700-signatur/

32. https://www.insidehighered.com/news/2020/04/10/students-fileclass-action-seeking-tuition-reimbursement

33. https://www.bleepingcomputer.com/news/security/over-25-percentof-all-uk-universities-were-attacked-by-ransomware/

34. https://www.kaspersky.com/resource-center/threats/deep-web

35. https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

36. https://haveibeenpwned.com/PwnedWebsites#Chegg

37. https://dailyfreepress.com/2019/10/10/following-flood-of-spamemails-more-than-1000-student-accounts-temporarily-disabled/

38. https://medium.com/@svanas/why-an-unsalted-md5-hash-is-badpractice-6a0d7d017856

39. https://dailyfreepress.com/2019/10/10/following-flood-of-spamemails-more-than-1000-student-accounts-temporarily-disabled/

40. https://www.zdnet.com/article/top-exploits-used-by-ransomwaregangs-are-vpn-bugs-but-rdp-still-reigns-supreme/

41. https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbirwidup.pdf

Rock-solid cyber defense you can trust

BlueVoyant

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/digital-risk-protection

to learn more.