

CYBER CRIMINALS, COLLEGE CREDENTIALS, AND THE DARK WEB

A SECURITY CHALLENGE FACING U.S. UNIVERSITY COMMUNITIES



MARCH 2017

digitalcitizens
alliance 

TABLE OF CONTENTS

CONTENTS	i
IMAGES	ii
CHARTS	iii
WHY YOU SHOULD READ THIS REPORT	iv
WANT A COLLEGE EMAIL WITHOUT HAVING TO GO TO CLASS? IT'S ALL TOO EASY	vi
KEY DATA FROM DARK WEB RESEARCH	ix
THE RISK—THE THREATS, VULNERABILITIES, AND ASSETS THAT MAKE ACADEMIC COMMUNITIES A TARGET	1
WHICH SCHOOLS' .EDUs ARE THE MOST DESIRABLE FOR DARK WEB BUYERS?	5
WHY THE MIDWEST? WHY THESE SCHOOLS? NO EASY ANSWERS	7
WHO IS (AND WHO IS NOT) SHARING THESE CREDENTIALS?	10
CREDENTIALS FOR SALE ON THE DARK WEB?	11
HOW CAN COLLEGES AND UNIVERSITIES PROVIDE MORE PROTECTION FOR FACULTY, STAFF, AND STUDENTS	13
ENDGAME	15
METHODOLOGY	16
APPENDIX A	17
APPENDIX B	19
APPENDIX C	21
ENDNOTES	22



TABLE OF IMAGES

IMAGE 01: FROM OWNEDCORE (CAPTURED MARCH 13, 2017)vi

IMAGE 02: FROM EPICNPC (CAPTURED MARCH 13, 2017).....vi

IMAGE 03: FROM MC-MARKET.ORG (CAPTURED MARCH 21, 2017)vii

IMAGE 04: FROM SUBLIMESHOP (CAPTURED MARCH 13, 2017)vii

IMAGE 05: FROM THEBOT.NET (CAPTURED MARCH 13, 2017).....vii

IMAGE 06: FROM THEBOT.NET (CAPTURED MARCH 13, 2017)..... viii

IMAGE 07: FROM OWNEDCORE (CAPTURED MARCH 13, 2017) viii

IMAGE 08: TERRORIST SYMPATHIZER OFFERING STOLEN
CREDENTIALS ON DARK WEB..... 10

IMAGE 09: EXAMPLE OF DARK WEB SITE SELLING .EDUs
(ARTIST'S RE-CREATION)..... 11

IMAGE 10: EXAMPLE OF DARK WEB SITE SELLING .EDUs
(ARTIST'S RE-CREATION)..... 11

IMAGE 11: VENDOR OFFERING .EDUs ON ALPHABAY 12

TABLE OF CHARTS

CHART 01: DETECTED BREACHES OF EDUCATIONAL ORGANIZATIONS 2005-2016	1
CHART 02: THE TEN HIGHER EDUCATION INSTITUTIONS WITH THE MOST CREDENTIALS ON THE DARK WEB	5
CHART 03: TOP TEN HIGHER EDUCATION INSTITUTIONS BY PERCENTAGE OF CREDENTIALS ON THE DARK WEB COMPARED TO FACULTY, STAFF & STUDENT POPULATION	5
CHART 04: TOP TEN HIGHER EDUCATION INSTITUTIONS WITH THE FASTEST GROWING NUMBER OF CREDENTIALS ON THE DARK WEB.....	6
CHART 05: TOTAL CREDENTIALS FROM 300 LARGEST HIGHER EDUCATION INSTITUTIONS BY STATE	7
CHART 06: THE TEN LARGEST HEIs BREACHES RECORDED.....	8
CHART 07: LOS ANGELES VALLEY COLLEGE CREDENTIALS ON DARK WEB SHOOT UP AFTER RANSOMWARE ATTACK, BUT RATE OF INCREASE IS ONLY SLIGHTLY HIGHER THAN THAT OF THE TOP 300 SCHOOLS	8
CHART 08: RANKINGS OF HEIs WITH HIGHEST R&D EXPENDITURE RATE VS. RANK OF SCHOOLS WITH CREDENTIALS ON THE DARK WEB	9



WHY YOU SHOULD READ THIS REPORT

A cabal of criminal entrepreneurs, mischief makers, and loyalists to extremists have found a hideout for their headquarters in the digital space—it is known as the Dark Web. The name and the stories of shadowy figures engaged in nefarious activity leads one to imagine some kind of Tolkienesque, charred hellscape of badlands ruled by those who co-mingle coding and creativity with criminality. In reality, it's a highly-decentralized, unregulated platform where goods, services, and information are marketed, managed, and moved quickly. The Dark Web is inhabited by a variety of disruptors—including entrepreneurs, soldiers of cyberwar, reformers, and whistleblowers—with different motives, tactics, and goals.

Digital Citizens Alliance researchers have spent years exploring the Dark Web. We've seen the Dark Web marketplaces where thieves sell their illicit, often stolen, goods. We've found drugs, weapons, medical information, malware, movies, music, counterfeits—on the online bazaars where there are ever more listings, more vendors, and more customers coming to check out the goods. The increasing opportunities for business draws profiteers, vengeance seekers, and everyday criminals—all of whom are willing to profit from cybercrime.

We've seen sites start from scratch and quickly become power players on the Dark Web—like Evolution (now closed) and AlphaBay (now the leading Dark Web Black Market). We watched Silk Road get taken down by the FBI, but in just months rise from the ashes to become bigger than it was before the takedown. We've seen criminal networks formed to sell malware, using the Dark Web as a place to market and communicate, then spread their product onto the Clear Web, the part of the internet where most of us go to find news, communicate with friends, and shop for our favorite products.

While we've explored the broad range of illicit goods available for sale on the Dark Web, in this report we'll look at another much coveted item found in the internet's darkest corners—you.

Many threat actors^a covet the inherent value of identities and personal information as much as any commodity available in this shadowy marketplace. Working with researchers from leading cybersecurity research organizations, we found millions of credentials (e-mail accounts/IDs and passwords) available on the Dark Web, we visited the sites where they are distributed, and we talked with leaders in academia who work every day to protect the faculty, staff, and students that make up the university community.

You have already seen the vendors we found selling credentials marketed to those wanting student discounts on popular products. In the pages ahead, we'll discuss how criminals can run scams with fake e-mails that inflict considerably more harm on members of the university community. Stolen credentials can be the first step down the path to more sensitive personal information, access to valuable intellectual property, and potentially identity theft. In other cases, individuals have no profit motive at all. Threat actors can be driven by revenge or just mayhem and destruction. The result—millions of e-mails just discarded along the Dark Web for

^a We're using "threat actors" as a catch-all term for hackers, Dark Web vendors, or any individuals facilitating illegal/illicit activity on the Dark Web.

anyone who wants them. That isn't to say they are not valuable. Each address and corresponding password should be thought of as a sort of informational gold mine. For their possessor they offer an immense amount of opportunity to glean the types of personally identifiable information that can be packaged together and sold on the Dark Web. Additionally, the credentials are the gateway to the valuable research and Intellectual Property which is often targeted for corporate and governmental espionage.

But we also found these records from the lives of our young people, our top thinkers and researchers, and the office workers who make universities great places to live, work, and prosper just dumped like trash on the side of road. In this report, we'll explain how something so valued as credentials from the university community can be so easily acquired, utilized, and discarded by criminals of all kinds.

Our objective in this report is not to blame the security professionals who work at universities and colleges. In fact, many (or even most) of the .edu credentials we found on the dark web may have ended up there as a result of one or more breaches in non-academic settings where .edu credential-holders used .edu user names, or the credentials could have been fraudulently created in the first place, not stolen. Rather, we salute the security teams in academia for their efforts to manage a population growing by the hundreds or thousands every year and protecting them from new threats and increasingly brazen threat actors. Our issue is not with the security, the school administrators, or university community population. Our hope is to shed light on how the activities of criminals who steal credentials and/or create fake credentials are putting innocents at risk. We want to show how bad guys profit, why they target academia, and how they use the clear web and Dark Web to share their merchandise. We've shared this publicly so everyone—the schools, the faculty, the staff, and the students—can all take extra measures to protect themselves.

Please see page 15 for a more detailed explanation of the methodologies used in connection with this study. We do not share the names of any victims in this paper.

OUR PARTNERS FOR CYBERSECURITY RESEARCH

For this project, we worked with researchers at ID Agent and their cyber intelligence tool Dark Web ID. Headquartered in Washington, DC, the team at ID Agent monitors more than 2,000 distinct Internet Relay Chat forums and 650,000 private websites, that are only accessible using The Onion Router (TOR), the free software that enables users to browse the Dark Web while encrypting their traffic and IP address.

GroupSense is a Virginia-based cybersecurity reconnaissance company that alerts clients to attacks, fraud, and breaches from across the surface, deep and dark web in real-time. The early warnings, analysis and recommendations that GroupSense provides help business and technology leaders protect their organizations and maximize the value of their security technology investments.

Terbium Labs is a dark web data intelligence company based in Baltimore, Maryland. Terbium runs Matchlight, the world's first fully private, fully automated dark web monitoring system for sensitive data.



WANT A COLLEGE EMAIL WITHOUT HAVING TO GO TO CLASS? IT'S ALL TOO EASY

There's no better way to tell you the marketplace for stolen and/or fake .edus than to simply show it. With the help of a hacktivist who once dumped tens of thousands of emails and passwords belonging to faculty, staff, and students at U.S. colleges and universities onto the internet for anyone to take, Digital Citizens Alliance researchers visited saw more a dozen listings than offering .edus^b for sale.

b.edu is a commonly used term used to describe college or university emails. It comes from the .edu suffix at the end of emails generated and managed by US-based colleges and universities. According to the nonprofit Educause, the .edu domain is one of the seven original top-level subdivisions of the Internet Domain Name System (DNS). The .edu domain is intended for accredited post-secondary educational U.S. institutions. It is managed under the authority of the United States Department of Commerce.

"THIS EMAIL ADDRESS MIGHT NOT LOOK VERY INTERESTING TO YOU, BUT IT IS ... IT'S BECAUSE IT IS A EDU EMAIL ADDRESS."

—tutorial on TheBot.net

IMAGE 01

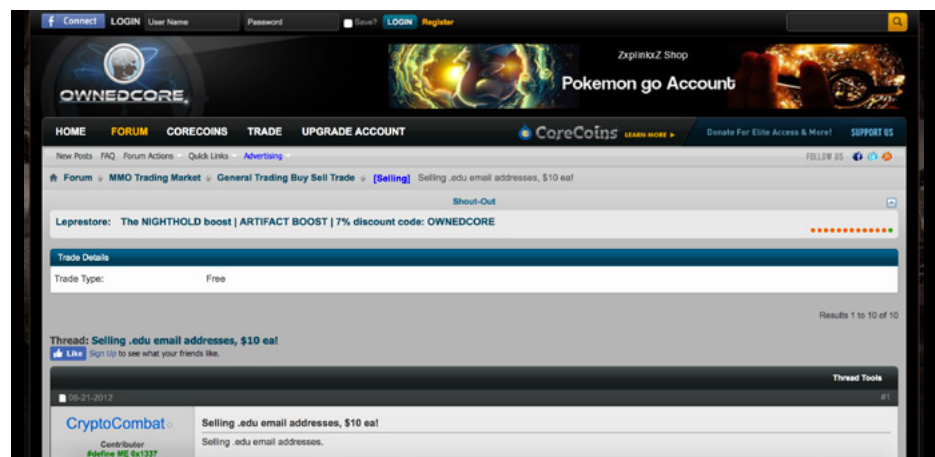


IMAGE 02

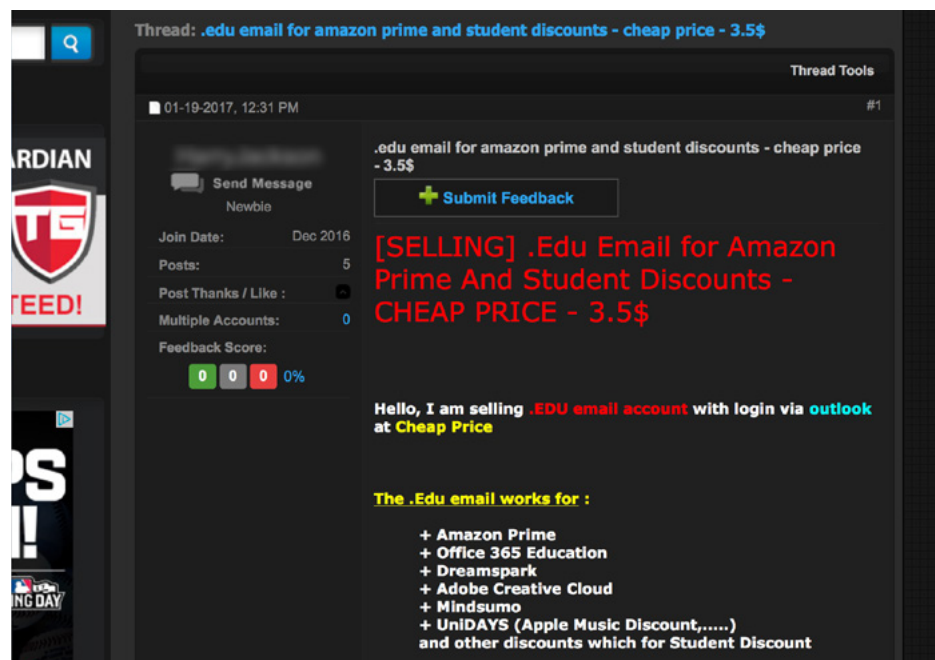
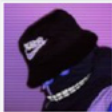


IMAGE 03

Selling [CHEAP] .EDU EMAIL ACCOUNTS! \$2.5 BTC [CHEAP]

Discussion in 'Social Media Accounts' started by Lemzey, Sep 26, 2016.

Sep 26, 2016
#1



Lemzey
bye

Premium

Messages: 1,216
Reactions: +424

Buy now! EDU Email accounts. \$2.5 BTC!

Can be used on any of these sites:
 Microsoft DreamSpark
 Amazon Prime 6 month
 GitHub
 AutoDesk Software
 RipTiger
 JetBrains
 And a shit more.

If you need emails for the student site, PM me. I got stock reserved (all these are used on it)


3 months warranty.

These sites are on the clear web—the internet that we use every day. We also saw tutorials from threat actors offering tips on how others could get e-mails, could make their own credentials and school IDs.


They also share the benefits to buying or creating .edus, which include being able to buy software and other products reserved for members of the university community.

IMAGE 04


- SublimeShop -
#1 shop for instant edu access



◦ Emails




High quality c ◦




EDU Email

With an EDU email you can get great exclusive deals from different companies. You can buy one below!



Combollists

With our HQ and private combollists you dont only get GUARANTEED hits but also HQ accounts



Github student pack

Always wanted the cool perks of the education pack but never had an EDU email. Well now you can!

IMAGE 05

thebot.net

[FREE] Get A Free .edu Email A... [SELLING] .Edu Email Account... Selling .edu email for amazon... [SOLD] [SELLING] .Edu email f...

- Purchase a free .edu email address for as little as \$5.50
- 1. Go to [Fiverr.com](https://www.fiverr.com)
- 2. Search for free.edu email id
- 3. Pay \$5.50 for the administration
- 4. Give wanted username and a photo of your picture ID
- 5. It takes under 24 hours to get it
- 6. You are ready to use your email address for a hosts of discounts and freebies



Image 07 (on bottom) shows a threat actor exploiting benefits extended to faculty, staff, and students. According to our hacktivist tour guide, "These loopholes have been known for years and abused to no end."

We saw multiple listings offering .edus for sale for between \$3.50 to \$10 each. The .edus are popular because buyers can use them to get discounts normally reserved for faculty, students, and staff on popular products including software and Amazon Prime memberships. Again, all the screenshots above are of clear web sites. Cybersecurity researchers helped us find millions of stolen and/or fake credentials offered to anyone on the Dark Web.

IMAGE 06

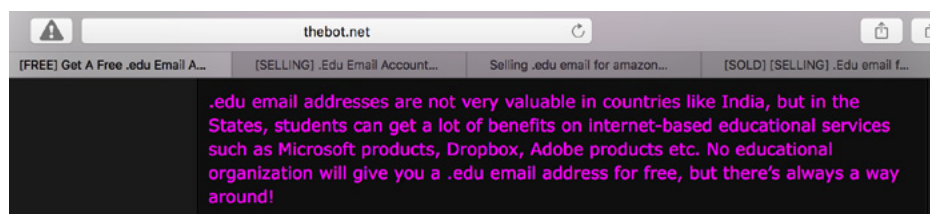
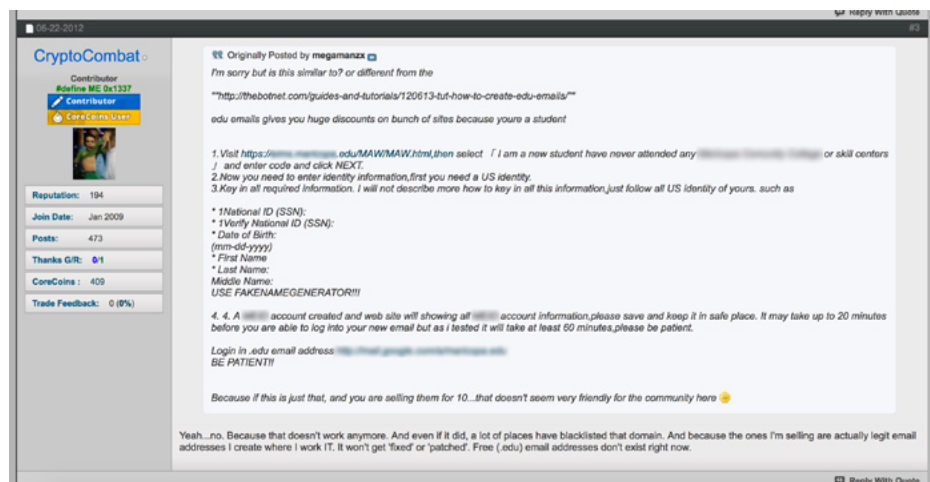


IMAGE 07



KEY DATA FROM DARK WEB RESEARCH

Researchers from the Digital Citizens Alliance worked with two companies that specialize in deep dives into the Dark Web.

This report looked at the availability of credentials from the largest 300 Higher Education Institutions (or HEIs) in the United States. During the eight years of searches, with the most recent scan done on March 2, 2017, researchers from ID Agent discovered:

→ A total of 13,930,176 e-mail addresses and passwords belonging to faculty, staff, students, and alumni at U.S. HEIs available to cyber criminals on Dark Web sites. 79 percent of the 14 million credentials were discovered by ID Agent researchers over the last year.^c The numbers are staggering and rising quickly. More than 10,984,000 credentials with login IDs that had the .edu suffix (presumably from the HEI community) have been discovered within the last 12 months.

→ ID Agent search results showed the University of Michigan had the most credentials offered on the Dark Web with a total of 122,556. Michigan was followed by five other large schools in the middle of America—Penn State, Minnesota, Michigan State, Ohio State, and Illinois.

→ The Massachusetts Institute of Technology (MIT) had the highest ratio of total stolen e-mail

accounts to total current users, followed by Baylor, Cornell, Carnegie Mellon, and Virginia Tech. Each with more than two e-mail accounts per user. This data point highlights intentional action by cybercriminals to attack users from some of the most technical schools in the U.S.

→ When broken down by state, the largest number of e-mails available came from schools in California, followed by New York, Michigan, Texas, and Pennsylvania.

For a look at some specific sites popular with those trafficking credentials on the Dark Web, Digital Citizens worked with GroupSense to monitor non-indexed and/or members only sites. In their research, GroupSense researchers found:

→ Vendors claiming to be affiliated with terrorist organizations offering stolen credentials from HEIs on Dark Web sites;

→ HEI credentials (including .edu e-mails and passwords) offered for free on many "free" Dark Web^d sites to anyone who wants them.

→ Private marketplaces or members only sites offering HEI credentials (along with information grabbed from those e-mail accounts like Social Security Numbers, bank account information, credit card data, and personal identity information (PII)) for sale.

^c Research included e-mail domains that matched ID Agent's search parameters. We are certain that some e-mails are from e-mail domains not managed by the HEI. Fake e-mails designed to resemble a school's actual e-mail also pose threats to those inside the HEI community and the public. Also, ID Agent does not confirm that account passwords are valid, i.e., provide access to the e-mail account. Attempting to gain unauthorized access to a privileged account or network is illegal.

^d Examples of free (no subscription required) Dark Web sites include AlphaBay, Dream Market, Valhalla (Silkittie), and Outlaw Market to name a few. These sites, descendants of Ross Ulbricht's infamous Silk Road, were once predominantly focused on the sale of illicit drugs. Sites like Evolution before it went offline, and now AlphaBay, combined the sale of personally identifiable information and other illicit activities with those selling drugs to give us the free Dark Web sites that we know today.

THE RISK—THE THREATS, VULNERABILITIES, AND ASSETS THAT MAKE ACADEMIC COMMUNITIES A TARGET

THE THREATS

No one person has brought more attention to the theft of .edu credentials than the hacktivist known as “DeadMellox”. He is the leader of a hacktivist organization called “Team GhostShell” and has been called one of the most talented hackers in the world.¹ News reports indicate, DeadMellox has posted tens of thousands of college credentials. Many of the e-mail addresses and passwords he obtained himself. One of Team GhostShell’s best known dumps made headlines around the world in 2012 when the organization published on Pastebin 36,000 e-mails addresses—as well as thousands of names, usernames, passwords, addresses, phone numbers, and (in some cases) payroll information and dates of birth—of faculty, staff, and students at 53 of the world’s most well-known universities.² GhostShell called his 2012 attack “Project West Wind”.

The U.S.-based schools caught in GhostShell’s storm included Harvard, Stanford, Cornell, Johns Hopkins, Carnegie Mellon, and the University of Michigan.

DeadMellox outed (or “doxed”) himself last year. He is Razvan Eugen Gheorghe, a 25-year-old living in Bucharest, Romania. Digital Citizens reached out to Team GhostShell via twitter and got a response from a person who said he was Razvan. Over months of direct messages and e-mails, Razvan shared information about his work and his thoughts on the state of HEIs cybersecurity. He is quick to say that he does not destroy data, deface websites, or spy on other people. Razvan says he has never made any money from his attacks.

So why does he do it? He says his actions were “mostly about sparking a worldwide conversation about today’s education.” More specifically, Razvan is concerned about what he says is the school’s lack of cybersecurity.

Accompanying the massive 2012 dump was a dialogue in which others could comment on the challenges and issues in protecting the privacy of educational resources. He hacks to provoke his “targets” to take new steps that will keep people like him off their networks where he could, if he choose to, do real harm.

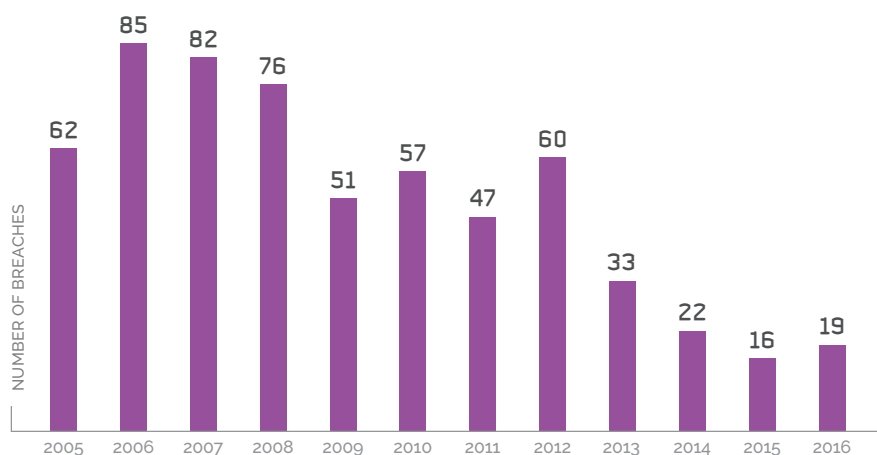
Razvan says he could have released many more credentials, but held back. “.edu’s are literally the most vulnerable domains on the internet. I’ve hacked and leaked hundreds more since (2012) in hopes of raising awareness to this issue. People think

WHEN DID THREAT ACTORS START GOING AFTER HEIs? A BRIEF HISTORY LESSON

The Privacy Rights Clearinghouse has tracked known breaches of educational institutions^e since 2005. In the chart below, you can see how breaches have tapered off since 2013 and 2014.

^e PRC’s education list includes colleges, universities, school systems, and some companies working in the education space.

CHART 01 DETECTED BREACHES OF EDUCATIONAL ORGANIZATIONS 2005-2016



Source: Privacy Rights Clearinghouse Chronology of Data Breaches

that I'm the bad guy here but they don't realize that these places have already been breached long before me and their private data is being used maliciously all the time.

"They're all vulnerable, even after all these years, I can breach them all over again."

Hackers like Razvan are not the only threat out there. The people/organizations behind the vast majority of cyberattacks in the world can be broken into six identifiable classifications:

- State-backed hackers (many of the world's elite hackers work for nation-state organizations like T.A.O (United States), Unit 8200 (Israel), Unit 61398 (China), Deep Panda (China), APT 28 & APT 29 (Russia), and Bureau 121 (North Korea);
- Organized crime (not necessarily the mafia in the traditional sense, but organizations profiting from selling or using stolen digital materials illegally);
- Disorganized crime (could be petty criminals or nuisance hacks just trying to show what they can do);
- Terrorists (hackers with an agenda wanting to inflict damage);
- Inside threats (an employee who goes rogue or assists a bad actor);
- Hacktivists (hackers with a cause).³

Kim Milford is the Executive Director of the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). She has worked at some of America's largest Universities including Indiana University, the University of Rochester, and the University of Wisconsin. We shared Razvan's comments with her and she didn't disagree. "Even if he can't use the same attack on the same server he used in 2012, there are always new exploits."

ASSETS

Some HEIs have more data than leading commercial businesses or government entities, but they face multiple, unique challenges as they have fewer resources (technology, staff, advisors) to deploy to protect their users, equipment, and intellectual property. As with the commercial sector, HEIs utilize enterprise risk assessments to determine priorities for limited resources. Protecting the missions of teaching, learning, and community service takes precedence over protecting online credentials. This is especially true of

"THEY'RE ALL
VULNERABLE, EVEN
AFTER ALL THESE
YEARS, I CAN BREACH
THEM ALL OVER AGAIN."

student accounts that have limited access to institutional resources and data.

HEIs also have physical assets that draw threat actors' interest. "Because (HEIs) have large capacity Internet connection links that serve all the students, and large capacity servers that are designed for many users, they are almost always on, and attackers never have to worry if a part of their infrastructure will be available for use," said Will Glass, Senior Analyst at the intelligence-led security company, FireEye. "We see more advanced groups compromising infrastructure belonging to other institutions, and then using it as a jump point toward their target. That's smart for two reasons, 1) it's free for them, 2) it makes the job of attribution for defenders, like us, much more difficult. You'll see malicious activity coming from an IP address that belongs to a university, but the likelihood that the university is conducting cyber espionage is very low. That just means that there's another step we have to take further back in the chain to figure out what is going on. So in terms of stealing credentials, it may not only be to steal passwords and then break into accounts, but it is also valuable to be able to tap into those university's resources for ill-gain."

But HEIs offer much bigger prizes beyond just the chance to rage against the machines. Pillaging the people of the HEI communities—that's where threat actors find a nirvana rich with opportunities for nefarious activity. Professors and students may have intellectual property and research for everything from Department of Defense contracts to medical breakthroughs to chemical compounds to future literary masterpieces stored away on computers. Even if they do so on their own time and personal devices, the HEI account could provide an attacker the path to the vault.

In 2014, The FBI's Internet Crime Complaint Center (IC3) sent out a warning titled "Cyber-Related Scams Targeting Universities, Employees, and Students." One of the crimes IC3 warned of: criminals taking professors' Personally Identifiable Information (PII) to file fraudulent income tax returns.⁴

And then, there are the students.

Emily Wilson, the Director of Analysis at Terbium Labs, has done extensive research on HEI communities. She told us the student population is unique with economic characteristics unlike others in our society. "Colleges are a built-in population of people who are constantly inundated with information, particularly when you consider the freshmen moving in and the seniors preparing to move out. You're dealing with a population that is unavoidably on content overload, a population less likely to think critically about the information they share or the e-mails they open."

The IC3 issued a warning of such a scam this January. Students were receiving e-mails to their student accounts about job opportunities. Students who applied were given a check for an advance, part of which should be used to buy equipment, materials, or software needed for the job from a "vendor." But those vendors would take the students' information and clear out a student's checking account. In the end, students were left with an empty bank account, a damaged credit rating, and their personal information 'in the wild' where other scammers could steal their identities and commit more crimes.⁵

Wilson added that HEI students "also have an unusual transaction history, particularly around the start of a new semester. Going to a store five or six times in one day, or making an unusually large electronics

purchase might raise red flags, unless it's late August and it would make sense that someone purchased a new laptop."

To a threat actor, students are both valuable and vulnerable.

VULNERABILITIES

The password management and digital vault software company Keeper Security recently reported that 87 percent of people between the ages of 18-30 reuse passwords.⁶ So if a threat actor can get that password for a student's HEI account, they can likely get into another account too. As one researcher told us during this project, "the college password is not just a key, it is the keychain."

Many security experts feel there is little protecting the university community from the threat actors. ID Agent's Brian Dunn says threat actors are aware that some academic institutions are below the "Cyber Poverty Line", which refers to the amount of continued investment needed for strong, effective, cybersecurity protection. "Cyber criminals are motivated to be successful. They understand that some higher ed schools cannot afford the cybersecurity resources that larger, more equipped, commercial and government organizations maintain."

Kim Milford acknowledged that budgets are a challenge for HEIs. "CIOs and CISOs must adopt a risk management approach. They assess the risks of a certain threat or event and put their limited resources to protecting against that. There are always more threats that may occur, and the threats are evolving faster than the safeguards."

While smaller budgets certainly don't help, the HEIs have partially mitigated that problem by pooling together resources and aggressively sharing information, especially in times of crisis. "We don't have the competitive pressures that Fortune 500 companies do," Milford said. "We don't worry about stock prices or competitive advantages. We can share information, such as threat intelligence and specifics about defenses, freely and liberally amongst ourselves in real time." Milford said that HEI cybersecurity professionals and Privacy Officers correspond daily about possible breaches and threats.

Put all of this together, HEI credentials are a lure that is hard for threat actors to resist. In 2015, Royht Belani, CEO of the password protection company PhishMe,

**AS ONE RESEARCHER
TOLD US DURING THIS
PROJECT, "THE COLLEGE
PASSWORD IS NOT
JUST A KEY, IT IS
THE KEYCHAIN."**

told the International Business Times: "We're finding that universities are the test bed for hackers." The IBT story said Belani added that "academia has become a soft target because of the number of accessible student accounts."⁷ Between the attacks targeting HEIs and the attacks on other companies (LinkedIn, DropBox, and Yahoo just to name a few)⁸ in which .edus were stolen, the number of accessible e-mails of faculty, staff, and students continues to grow at an astonishing rate. ID Agent researchers say the number of credentials they've discovered on the Dark Web is up more than 547 percent since 2013.

THREATS + ASSETS + VULNERABILITIES = RISK

Risk is "the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability."⁹ The aforementioned IC3 warnings show what threat actors are capable of doing with the credentials of faculty, students, and staff. The success of such scams emboldens criminals.

Academic communities face new risks coming from both direct attacks on the school's networks, but also as collateral damage as a result of attacks on other high-profile, highly used online services companies. In just the first few months of 2017, we've seen attacks that show what threat actors can do with the right tools to come after university communities.

In February, we learned of damage done by the Russian hacker Rasputin. The security threat intel-

ligence company Recorded Future reported that Rasputin stole data from more than 60 U.S. organizations, including federal, state, local government agencies and 25 U.S.-based colleges (that we know of). According to Computerworld's coverage of the Recorded Future report, Rasputin has built an SQLi tool he uses to "locate and exploit vulnerable web apps" and steal data to sell on the Dark Web.¹⁰ Recorded Future calls Rasputin a "notorious financially-motivated cyber criminal."¹¹

Just this month, HEI security teams took action to patch an exploit in the Web server framework Apache Struts 2. According to ars technica's coverage of the attack, the Apache vulnerability allows threat actors "to take almost complete control of Web servers used by banks, government agencies, and large Internet companies."¹² As exploits of Apache Struts 2 multiplied, many HEIs issued warnings. HEIs have a high number of publicly-facing websites and the threat to unpatched Apache servers can put private information at risk.

Between direct attacks on HEIs and those on companies in which university community members become collateral damage, one can understand why the number of credentials posted is growing, but it is growing so fast it's hard to see how organizations facing even a hint of staffing or funding challenges can keep up.

WHICH SCHOOLS' .EDUS ARE THE MOST DESIRABLE FOR DARK WEB BUYERS?

Digital Citizens wanted to see which HEIs had the most credentials posted on the Dark Web. According to The National Center for Education Statistics (NCES), there are 4,627 post-secondary schools awarding degrees in the United States, with 3,011 of those being four-year institutions. To sift through such a large pool, we worked with researchers at ID Agent using their Dark Web ID technology and focused on the the 300 largest HEIs in the United States compared to the stolen credentials available on the Dark Web. ID Agent researchers found 13,930,176 credentials stolen from current or former faculty, staff, and students at U.S. HEIs. Cyber criminals are getting even more aggressive in their work. About 10,984,000 credentials with login IDs that had the .edu suffix (presumably from the HEI community) have been discovered within the last 12 months.

The ten most commonly found .edus being published on the Dark Web by threat actors include some of the most respected institutions in America.

It is clear that the larger HEIs are more likely to show up at the top of the list, but how do we know if these schools are on top simply because of the number of available e-mail addresses? To get a better sense for the demand in the Dark Web marketplaces and to compare large and small universities on a more

level playing field, Dark Web ID divided the number of stolen e-mail accounts by the number of total users in the current university population (faculty, staff, and students) at a HEI. Using this approach shows the number of stolen e-mail accounts per user. Dark Web ID then sorts the data to show relationships between the organizations.

CHART 02 THE TEN HIGHER EDUCATION INSTITUTIONS WITH THE MOST CREDENTIALS ON THE DARK WEB

INSTITUTION	NUMBER OF E-MAIL ACCOUNTS ON DARK WEB (MARCH 2017)
University of Michigan-Ann Arbor	122,556
Pennsylvania State University-Main Campus	119,350
University of Minnesota-Twin Cities	117,604
Michigan State University	115,973
Ohio State University-Main Campus	114,032
University of Illinois at Urbana-Champaign	99,375
New York University	91,372
University of Florida	87,310
Virginia Polytechnic Institute and State University	82,359
Harvard University	80,100

Source: Dark Web ID. For a full list of the total number of stolen e-mails available from the 300 schools tracked in this report, see [Appendix A](#).

CHART 03 TOP TEN HIGHER EDUCATION INSTITUTIONS BY PERCENTAGE OF AVAILABLE CREDENTIALS COMPARED TO FACULTY, STAFF & STUDENT POPULATION

INSTITUTION	RATIO OF CREDENTIALS ON DARK WEB TO TOTAL ENROLLED AND STAFF
Massachusetts Institute of Technology	2.81 : 1
Carnegie Mellon University	2.4 : 1
Cornell University	2.39 : 1
Baylor University	2.27 : 1
Virginia Polytechnic Institute and State University	2.1 : 1
Pennsylvania State University-Main Campus	1.94 : 1
University of Michigan-Ann Arbor	1.87 : 1
Michigan State University	1.87 : 1
Kent State University at Kent	1.87 : 1
Bowling Green State University-Main Campus	1.87 : 1

Source: Dark Web ID. For a comparison of the ratios of stolen e-mail accounts to number of total users at each of the 300 schools tracked in this report, see [Appendix B](#).

Comparing Chart 02 and Chart 03 on the previous page, we see that some large schools remained high in the rankings, some smaller—and very prestigious—schools shot up the rankings.

It is particularly interesting to see both MIT and Carnegie Mellon at the top of Chart 03. They include in their populations some of the most respected faculty and coveted young minds in the cybersecurity community.

Dark Web ID also showed which schools have had the largest numbers of credentials added to the Dark Web in the last year as shown in Chart 04 below.

There are few important caveats to give these numbers some additional perspective:

→ Our research did not confirm that the log-ins and password were working (i.e., provided access to the e-mail account and institutional resources at the HEI).

→ Not every breach results in a large public dump. It's likely that some of the credentials were lifted from the mega-breaches of popular online services like DropBox and LinkedIn. In these cases, only the individual user knows if

the same password they use for accessing their higher educational resources is the same one they use to access online services.

→ In other cases, local system administrators may have forced a password reset when they were notified about the breach. This is standard practice when breached credentials are discovered.

→ In 2016, REN-ISAC notified HEIs of over 2,197,000 compromised credentials. When an institution receives a notification, standard practice is to either block the account or force a password reset. Either activity greatly mitigates risk to the credential at the institution.

→ However, that will only shut down the HEI e-mail account, not another account in which the user used the e-mail as a user ID or password. REN-ISAC notification does not directly reduce risks if the account and password are reused on other sites, e.g., Facebook. The longer credentials remain publicly posted, the more likely the institution finds out about it and takes steps to mitigate.

CHART 04 TOP TEN HIGHER EDUCATION INSTITUTIONS WITH THE FASTEST GROWING NUMBER OF CREDENTIALS ON THE DARK WEB

INSTITUTION	E-MAIL ACCOUNTS ON DARK WEB (MARCH 2016)	E-MAIL ACCOUNTS ON DARK WEB (MARCH 2017)	PERCENT INCREASE 2016 TO 2017
University of Wisconsin-Madison	4,751	66,809	1306%
University of California-Los Angeles	5,356	72,622	1256%
CUNY Borough of Manhattan Community College	124	1,542	1144%
University of Illinois at Urbana-Champaign	12,344	99,375	705%
Community College of Rhode Island	894	6,997	683%
CUNY New York City College of Technology	179	1,386	674%
Baylor University	5,850	43,309	640%
CUNY LaGuardia Community College	201	1,467	630%
CUNY Queensborough Community College	137	988	621%
El Paso Community College	364	2,614	618%

Source: Dark Web ID.

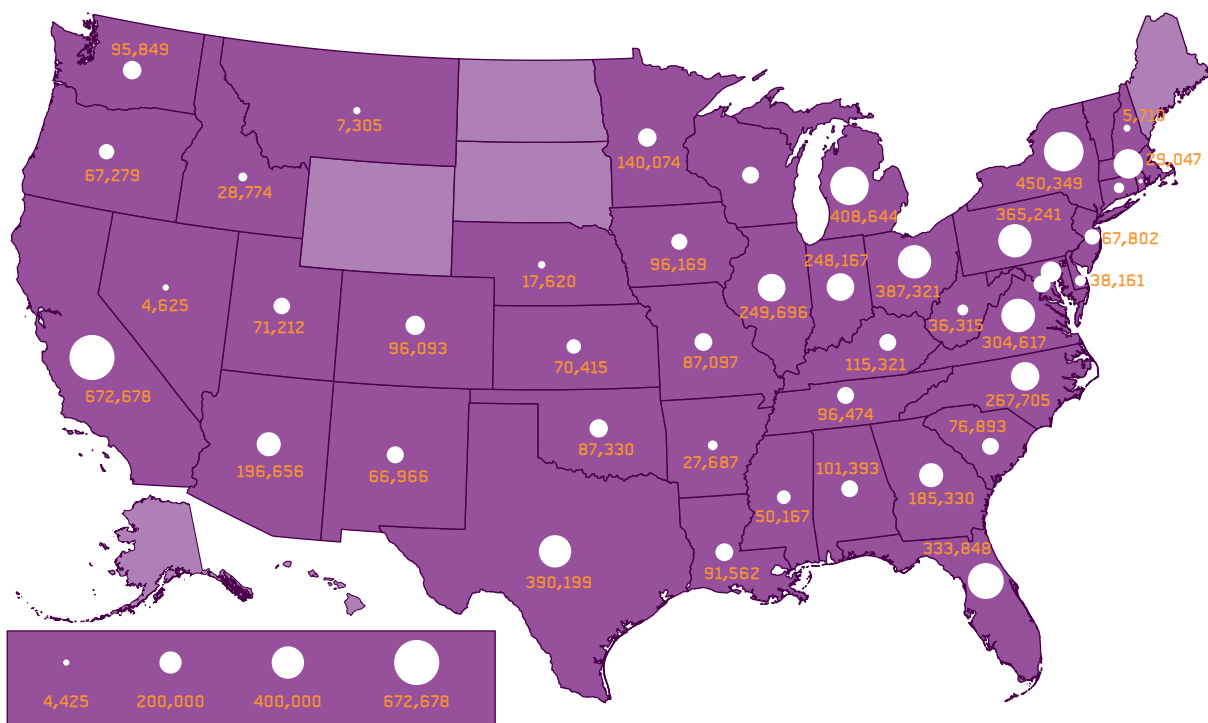
WHY THE MIDWEST? WHY THESE SCHOOLS? NO EASY ANSWERS

When broken down by state, the largest number of credentials posted came from schools in California, followed by New York, Michigan, Texas, and Pennsylvania.

When we compared the Dark Web ID numbers by records by state we found many midwestern states ranks were higher than their population ranks.

Digital Citizens researchers wondered why so many midwestern schools were at the top of the list? Was there some pattern we could find that explained this list? We tested a couple theories to see what might make some HEIs more prevalent on the Dark Web than others.

CHART 05 TOTAL CREDENTIALS FROM 300 LARGEST HIGHER EDUCATION INSTITUTIONS BY STATE



Source: Dark Web ID, a security tool of ID Agent.

Six states had no HEIs in the top 300: Alaska, Hawaii, Maine, North Dakota, South Dakota, and Wyoming. ID Agent researchers did find credentials from schools in those states, but that did not make this list.

SIZE OF THE BREACH DOESN'T MATTER

Below are the ten largest breaches at the 300 HEIs in the United States recorded by Privacy Rights Clearinghouse.

From PRC's list of breaches at academic organizations, we pulled out the the top 300 HEIs and compared that list to ID Agent's HEI-Dark Web rankings (see Chart 06). Some schools that had major breaches are high up on the list, but they are also large schools that

manage enormous numbers of e-mails which could be stolen. Furthermore, several large schools were at the top of the ID Agent list that have not suffered the same massive breaches as other schools. From this list, we didn't see any kind of pattern demonstrating a relationship between large breaches and high availability on the Dark Web. There's no reason to believe that the size of the breach is any more of a factor than the size of the school.

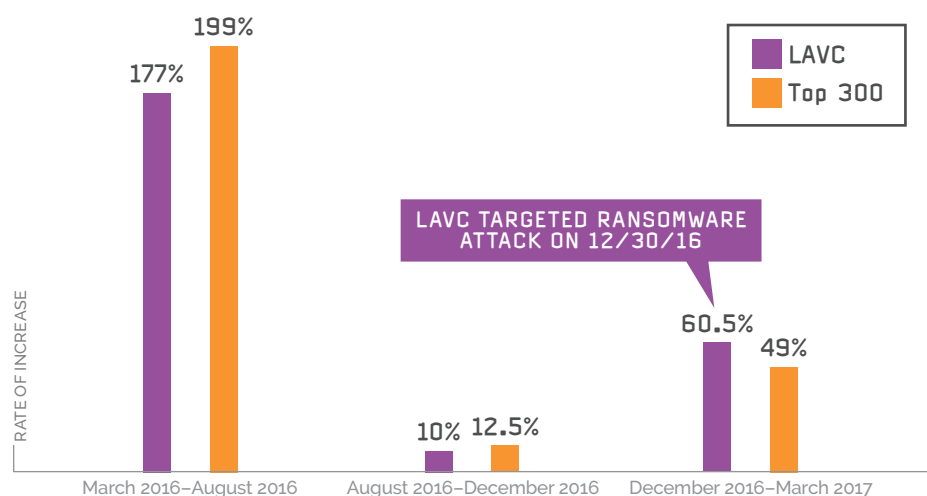
CHART 06 THE TEN LARGEST HEIs BREACHES RECORDED

DATE MADE PUBLIC	COMPANY	RECORDS* BREACHED	DARK WEB ID RANK
3-Mar-17	The Center for Election Systems at Kennesaw State University	7,500,000	148
12-Dec-06	University of California at Los Angeles (UCLA)	800,000	18
15-Dec-10	Ohio State University	750,000	5
25-May-12	University of Nebraska, Nebraska Student Information System, Nebraska College System	654,000	138
15-Feb-12	University of North Carolina at Charlotte	350,000	103
12-Nov-08	University of Florida College of Dentistry	330,000	8
19-Feb-14	University of Maryland	309,079	56
11-Nov-11	Virginia Commonwealth University	176,567	47
7-May-09	University of California, Berkeley	160,000	17
26-Feb-14	Indiana University	146,000	12

Source: Privacy Rights Clearinghouse Chronology of Data Breaches

*A record represents an individual's information and could be an e-mail, a social security number, and/or other personal identifying information.

CHART 07 LOS ANGELES VALLEY COLLEGE CREDENTIALS ON DARK WEB SHOOT UP AFTER RANSOMWARE ATTACK, BUT RATE OF INCREASE IS ONLY SLIGHTLY HIGHER THAN THAT OF THE TOP 300 SCHOOLS



We took a second run at making a connection between breaches and Dark Web availability by looking at a recent attack on a HEI to see if it caused a change. On December 30, 2016, criminals infected the computer network of Los Angeles Valley College (LAVC) with ransomware. Within a week, LAVC paid between \$28,000 and \$30,000 to get control of its website, e-mail, and voicemail before students returned to class in early January.¹³ But just because the hackers gave the school the keys to its digital properties doesn't mean the hackers didn't share some of the data they controlled for a week. In fact, Dark Web ID's searches show that the number of LAVC credential on the Dark Web is up by more than 60 percent. But, in that same period, the number of listings of the top 300 HEIs was up 49 percent. Yes, the LAVC rate in the aftermath of the breach is higher than top 300 HEIs, but it is just a slight deviation from the trendline (see Chart 07).

FOLLOW THE MONEY—COULD BIG R&D GRANTS MAKE SOME HEIs CREDENTIALS MORE APPEALING?

In 2015, the Department of Homeland Security (DHS) published an Intelligence Assessment on higher education. In its Intelligence Assessment, Malicious Cyber Actors Target US Universities and Colleges, DHS concluded “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.”¹⁴

Kim Milford also noted examples in which academic research was a lure that hackers couldn’t resist. “There are cases where attacks were made against research information on intellectual property, such as at prestigious Engineering programs. These are similar to successful and attempted attacks against known technical and innovation R&D leaders in the private sector.” Engineering programs at the University of Virginia¹⁵ and Penn State University¹⁶ are two of the high profile attacks that fit this description.

To see if there was a correlation between research and development grants and Dark Web listings, we compared the list from the National Science Foundation’s National Center for Science and Engineering

Statistics, which tracks federal research and development expenditures at U.S. HEIs, to the list of the top 300 largest HEIs.¹⁷ With just one look at the ten schools with the highest R&D expenditure ranking in 2015 (see comparison in Chart 08 below), we could see what we needed to know.

There is one common name in both the top 10 HEI credentials on the Dark Web and the NCSES list—Michigan. Yet there has never been a public breach at Michigan that ranks on PRC’s top 10, or top 100 for that matter.

Bottom line—the money trail came to a dead end.

We hope another researcher takes up this pursuit. There might be a driver that makes some HEI credentials more likely to be on the Dark Web. Right now, we can’t see other than the most obvious possibility—big schools are more likely to have more stolen credentials on the Dark Web. Even that isn’t perfect, 10th ranked Harvard is the fifth largest school... in the eight school Ivy League.

While none of our theories about why stood up to scrutiny, it didn’t stop us from trying to learn more about what kind of people were posting these stolen credentials on the Dark Web. On that front, we did come up with some interesting answers.

CHART 08 RANKINGS OF HEIs WITH HIGHEST R&D EXPENDITURE RATE VS. RANK OF SCHOOLS WITH CREDENTIALS ON THE DARK WEB

2015 R&D EXPENDITURE RANKING	2015 R&D EXPENDITURE (DOLLARS)	INSTITUTION	CREDENTIALS ON THE DARK WEB RANK	STOLEN E-MAIL ACCOUNTS (MARCH 2017)
1	\$2,305,679	Johns Hopkins University	93	28,544
2	\$1,369,278	University of Michigan, Ann Arbor	1	122,556
3	\$1,180,563	University of Washington, Seattle	19	71,817
4	\$1,126,620	University of California, San Francisco	*	*
5	\$1,101,466	University of California, San Diego	44	46,011
6	\$1,069,077	University of Wisconsin-Madison	21	66,809
7	\$1,036,698	Duke University	38	52,244
8	\$1,022,551	Stanford University	36	52,645
9	\$1,021,227	University of California, Los Angeles	18	72,622
10	\$1,013,753	Harvard University	10	80,100

Sources: Dark Web ID; National Science Foundation, National Center for Science and Engineering Statistics, Higher Education R&D Survey, Rankings by total R&D expenditures 2015.

*Not on the top 300 largest HEIs in the United States.

WHO IS (AND WHO IS NOT) SHARING THESE CREDENTIALS?

To learn more about who is making these stolen credentials available to all takers, we worked with the cybersecurity company GroupSense.

Some of most nefarious threat actors listing this contraband have much different motives than Razvan. Below is one example GroupSense found of a cyber-criminal calling himself AllrHaBi and claiming to be affiliated with the Islamic State. He was sharing stolen e-mails from the University of Michigan (see Image o8).

leveraged and working 24 x 7 to build databases for their cyber espionage teams," Dunn said. "If they get something, they don't want you to know about it. And what they steal can be used to garner intelligence and influence change for many years. Although we saw an example of this in the recent Presidential election, the large majority don't make national headlines."

That doesn't mean nation-states haven't tried to get into University networks. In a 2013 New York Times story, Bill Mellon, the associate dean for research policy at University of Wisconsin, said the school gets "90,000 to 100,000 attempts per day, from China alone, to penetrate our system."¹⁸

But research from the cybersecurity company FireEye shows Chinese-sponsored breaches of American companies since the September 2015 agreement between

President Barack Obama and Chinese President Xi Jinping in which the countries agreed they would not “conduct or knowingly support cyber-enabled theft of intellectual property” for an economic advantage.¹⁹ FireEye’s Will Glass says they’ve seen a difference with academic institutions too. “Along with this overall decline and activity that you’re seeing going on with China, we see that targeting of educational institutions is going down.”

Kim Milford added: "After a number of high profile breaches of science, technology, engineering and mathematics (STEM) department breaches in 2015, the activity slowed down."

From what we see and our interviews with experts, it is more likely that the credentials that Dark Web ID found are coming from hacktivists and cyber vandals looking to embarrass a university or a student or for financial gain in the exfiltration of PII.

Razvan said the most common type of hacker is what he called: "the opportunist", (or) the one that managed to find a vulnerability at random or by chance and has infiltrated a network. Usually this type of person is only looking to deface the site and not actually collect any sensitive data."

IMAGE 08

American Email leaked By Islamic State (AlIrHaB) Email Phone [REDACTED]@umich.edu [REDACTED]@cass.net [REDACTED]@umich.edu
[REDACTED]@umich.edu 734.763-[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu 734-763-[REDACTED]@umich.edu
[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu 734.936-[REDACTED]@umich.edu [REDACTED]@eecs.umich.edu
[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu
[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@gmail.com [REDACTED]@umich.edu
[REDACTED]@umich.edu [REDACTED]@dapcep.org 313-831-[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@engin.umich.edu
[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu 734-615-[REDACTED]@umich.edu [REDACTED]@umich.edu
734-763-[REDACTED]@umich.edu [REDACTED]@umich.edu 734-647-[REDACTED]@umich.edu [REDACTED]@umich.edu 615-[REDACTED]
[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu 647-[REDACTED]@umich.edu [REDACTED]@umich.edu
[REDACTED]@umich.edu 615-[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu 763-[REDACTED]@umich.edu 647-[REDACTED]
[REDACTED]@umich.edu 763-[REDACTED]@umich.edu 734-764-[REDACTED]@umich.edu [REDACTED]@umich.edu 734-615-[REDACTED]
[REDACTED]@umich.edu 734-764-[REDACTED]@umich.edu 734-647-[REDACTED]@umich.edu [REDACTED]@umich.edu
[REDACTED]@umich.edu [REDACTED]@umich.edu 763-[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu
[REDACTED]@umich.edu 764-[REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu [REDACTED]@umich.edu
[REDACTED]@umich.edu 734-647-[REDACTED]@umich.edu 734-764-[REDACTED]@umich.edu 734-936-[REDACTED] and 734-936-[REDACTED]
[REDACTED]@umich.edu [REDACTED]@umich.edu 734.647-[REDACTED]@umich.edu [REDACTED]@umich.edu 734-764-[REDACTED]

GroupSense found AllrHaBi posting a list of 397 stolen e-mails, including 351 @umich.edu, on the Dark Web (See Image 08).

Based on our interviews with experts, we believe that few—if any—of the credentials researchers found on free Dark Web sites came from nation-state hackers. Countries in the hacking business want to keep accessing and utilizing the credentials they've taken and NOT share them with others. The last thing they want to do is let their targets know they have them. In all likelihood, the breaches are the work of disruptors—or threat actors' like the aforementioned hacktivists, terrorists, and insiders with a vendetta.

While some threat actors see low barriers to entry, others see high-value targets. University faculty are often recruited to do important government-funded research. While it is illegal for university resources (including e-mail) to be used for classified research, a rogue nation-state could first target a professor's college e-mail to pinpoint another account where those classified communiques might reside.

Dunn's team at ID Agent frequently scans the Dark Web for their public sector clients and rarely encounters hackers associated with nation-states offering credentials or PII. "Nation-states hackers are highly

CREDENTIALS FOR SALE ON THE DARK WEB?

There is other research that explored the sale of HEI credentials on the clear web. In 2014, researchers from Palo Alto Networks found stolen college e-mails and passwords for sale on Taobao, the largest consumer-to-consumer (C2C) e-commerce platform in China. Some emails sold for as much as \$390.80, while others went for as little as 16 cents.²⁰ If you ask Google search "what is Taobao", the answer describes the site as "similar to eBay, Amazon and Rakutenf."

With the Palo Alto research and the sites Razvan showed us in mind, Digital Citizens investigators expected to find something similar on the Dark Web. As our researchers looked for .edu accounts, we didn't find them. This seemed odd.

We went back to GroupSense. Their researchers found a few cases of .edu accounts for sale on some of the Dark Web's subscription/members only sites. We can't show examples without revealing the sites GroupSense infiltrated, risking potential exposure of the researchers themselves. Images 9 and 10 include the price information GroupSense's researchers found, as well as other information

^f According to Wikipedia, Rakuten Ichiba is the largest e-commerce site in Japan and among the world's largest by sales.

listed in the marketplace's description of the merchandise. The url, the site name, as well as the names of the sellers have been changed.

IMAGE 09

BUY EMAILS NOW! IDENTITY THEFT 101 STEALING, FOR DUMMIES

<http://www.superawesomestolenemails.com/get-an-edu-without-going-to-college>

HANDY DANDY EMAIL FINDER!

EMAIL: .edu
MAX PRICE: any
OWNER: Bad Guy
COUNTRY: any
FEEDS: any
SELLER FEEDS: any
LAST FEEDS: any
MAIL ACCESS: any
PP ATTACHMENT: any

EMAIL	PRICE	OWNER	COUNTRY	FEEDS	SELLER FEEDS	LAST FEEDS	MAIL ACCESS	PP ATTACH
liberty.edu	\$17.05	Bad Guy	United States	341	0	N/A	-	+
wilkes.edu	\$18.55	Bad Guy	United States	371	0	N/A	-	+
u.washington.edu	\$19.95	Bad Guy	United States	397	2	-	-	+
student.usc.edu.au	\$0.60	Bad Guy	Australia	12	0	-	-	+
student.curtin.edu.au	\$1.90	Bad Guy	Australia	38	0	-	-	+
my.westga.edu	\$0.10	Bad Guy	-	0	0	-	-	-
msstate.edu	\$0.10	Bad Guy	-	0	0	-	-	-

IMAGE 10

BUY EMAILS NOW! IDENTITY THEFT 101 STEALING, FOR DUMMIES

<http://www.superawesomestolenemails.com/get-an-edu-without-going-to-college>

HANDY DANDY EMAIL FINDER!

SELLER	EMAIL	CARD EXPIRATION	COUNTRY	LAST ORDER	UPLOAD DATE	PRICE
Bad Guy	swin.edu.au	1-Nov-2010	Australia	N/A	17-Sep-2016	\$2.50
Bad Guy	swin.edu.au	1-Nov-2010	Australia	N/A	17-Sep-2016	\$2.50
Bad Guy	kent.edu	1-May-2018	China Mainland	11-Jul-2016	17-Sep-2016	\$2.50
Bad Guy	kent.edu	1-May-2018	China Mainland	11-Jul-2016	17-Sep-2016	\$2.50
Bad Guy	missouri.edu	1-Nov-2017	Tipton, MO	22-Jul-2016	17-Sep-2016	\$2.50
Bad Guy	zagnail.gonzaga.edu	1-Mar-2019	United States	6-Apr-2016	17-Sep-2016	\$2.50
Bad Guy	msu.edu	1-Apr-2017	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	alumni.iu.edu	1-Sep-2011	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	kent.edu	1-Feb-2019	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	iasfate.edu	1-Jul-2020	United States	13-Jun-2016	17-Sep-2016	\$2.50
Bad Guy	myuwestout.edu	1-Jun-2020	United States	1-Aug-2016	17-Sep-2016	\$2.50
Bad Guy	shsu.edu	1-Aug-2018	United States	3-May-2016	17-Sep-2016	\$2.50
Bad Guy	purdue.edu	1-Nov-2012	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	umich.edu	1-Apr-2015	United States	7-Apr-2016	17-Sep-2016	\$2.50
Bad Guy	student.clayton.edu	1-Oct-2018	United States	20-Apr-2016	17-Sep-2016	\$2.50
Bad Guy	baylone.edu	1-Aug-2012	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	ilstu.edu	1-Nov-2015	United States	11-Jul-2016	17-Sep-2016	\$2.50
Bad Guy	kent.edu	1-Jul-2020	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	indiana.edu	1-Feb-2008	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	brdgew.edu	1-Jan-2019	United States	14-Jul-2016	17-Sep-2016	\$2.50
Bad Guy	zagnail.gonzaga.edu	1-Mar-2019	United States	6-Apr-2016	17-Sep-2016	\$2.50
Bad Guy	msu.edu	1-Apr-2017	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	alumni.iu.edu	1-Sep-2011	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	kent.edu	1-Feb-2019	United States	N/A	17-Sep-2016	\$2.50
Bad Guy	purdue.edu	1-Feb-2020	West Lafayette, IN	29-Mar-2016	17-Sep-2016	\$2.50
Bad Guy	purdue.edu	1-May-2017	West Lafayette, IN	4-Mar-2016	17-Sep-2016	\$2.50
Bad Guy	purdue.edu	1-Feb-2020	West Lafayette, IN	29-Mar-2016	17-Sep-2016	\$2.50
Bad Guy	purdue.edu	1-May-2017	West Lafayette, IN	4-Mar-2016	17-Sep-2016	\$2.50

"As far as these types of hacker categories go, there's a lot more to gain by either keeping the data or leaking it."

GroupSense explained that the more expensive listings—in this case asking for between \$17-\$19 per .edu e-mail account (see Image 09 on the previous page)—generally include more sensitive information, like Social Security numbers, credit card information, or other kinds of information that would appeal to buyers looking to steal identities. Even if the credit card account is expired, they charge a few dollars premium simply because the account details are available. GroupSense's team suspects this site is available for individuals who conduct phishing campaigns and harvest credentials.

But in most cases, GroupSense found cases like Razvan's Project West Wind—with hackers simply giving away .edus. While the faculty, staff, and students who use these accounts treasure the valuable pictures, confidential conversations with friends, medical information, family matters, expense records (often containing credit card information) within these accounts, threat actors dump them onto sites like free tchotchkes or bread served to hold over hungry restaurant customers.

GroupSense found a listing on AlphaBay, currently the biggest of the free Dark Web marketplaces, for a vendor claiming to be able to create .edu accounts for the buyer (see Image 11). The vendor has a good history of sales and shoppers visiting him/her are giving the service a high rating. While we expected more listings for sale, Razvan said the AlphaBay listing was

more typical. "The thing about edu accounts is that most people simply create and then sell them, instead of actually taking them from a site."

As we learn from the comments on the tutorial pages, fake accounts enable scam artists to take advantage of discounts and bargains meant for the university community. Furthermore, a fake .edu could help those criminals running cons like the IC3 warned of. An e-mail from a university account—mentioning job opportunities or other university business—could have been more likely to be seen as legitimate as opposed to a phishing attempt from a stranger with a random account.

THE BIG MONEY FROM STOLEN .EDUS COMES FROM MINING WHAT IS IN THE E-MAILS

For all that can be done with fake emails, access to existing accounts can bring in big returns for cyber criminals. Emily Wilson and her colleagues at Terbium have seen what happens when criminals mine student accounts for medical records, payment information, even weekend plans.

"If you're dealing with a college student's credentials, you can take the information you have and turn it into a full identity packet—not just name, address, and financial information, but credentials for social media, for payment processors, video streaming sites, music sites, etc," Wilson said. "You can profit from lateral movement across a single identity, and you can avoid revealing your data source by simply packaging up additional information (bank accounts here, social media accounts here) into separate listings."

Razvan backed up Wilson's assessment, saying that the accounts had a value you can't necessarily measure in dollars and cents (or bitcoin for that matter): "If you want to add more zombies to your botnet, you're not just gonna give the e-mail list away for others to infect. The opportunist only wants some sort of recognition by defacing it and the hacktivist wants to either leak or use it in some other way."

IMAGE 11

★= .EDU Student Email Accounts ★= LOW FRAUD SCORE - FREE AMAZON PRIME (and many other benefits!) ★= CUSTOM MADE - ANY NAME! ★=★

EDU accounts - with full email access

★= NOT hacked

★= Made to order in the name you provide

BENEFITS OF .EDU EMAIL:

- Get a low fraud score while creating!
- 4 Months free Amazon prime - great for students
- 1 year free NEWEGO PREMIER membership including expedited shipping
- Discounts with AT&T and VERIZON up to 20%
- and many many more...

HOW CAN COLLEGES AND UNIVERSITIES PROVIDE MORE PROTECTION FOR FACULTY, STAFF, AND STUDENTS

Many universities and colleges now have cybersecurity programs, such as the Cybersecurity Institute at University of Massachusetts-Amherst.²¹ These academic centers address the needs cited by Razvan, helping students better understand the complex system architectures that create gaps for cybersecurity threats, and providing a thorough knowledge of defenses.

REN-ISAC provided Digital Citizens researchers with several suggestions on what can be done to make the university community safer.

OFFER EDUCATION ON HOW TO STRENGTHEN PASSWORDS

Password education is an important component of defense. When we did a Google search for "how to make strong passwords on college e-mail accounts" we found on the first page of results a helpful link from the University of Houston with instructions on how to make passwords stronger, how often users should change passwords, and where to go to reset a password.²²

Most higher educational institutions provide similar advice for their communities. As an industry standard, it's risky not to provide some advice on password protection in today's environment.

While many schools would like to offer cybersecurity instruction as part of student orientation, it's difficult to find time amidst orientation requirements on campus safety, student life and education. While cybersecurity professionals figure out other ways to fit it into the student education—pizza is always a draw for students. Faculty and staff are easier to reach. Privacy training is mandated by Federal and state law, and training on robust password practices are a natural fit.

Unfortunately, training and education on password defenses is not a "one and done" initiative. It requires a comprehensive program with frequent reminders, monitoring, and user notifications when new threats are found.

MAINTAIN SEPARATE NETWORKS FOR CRITICAL SYSTEMS

When attackers breach popular online services, such as LinkedIn and DropBox, they generally exfiltrate

WHAT MAKES A PASSWORD SECURE?

Many people reuse their campus username to establish accounts for online services for convenience, they may or may not use their associated .edu password. Password complexity rules differ, sometimes forcing the user to create a different password for the online service. This helps to reduce risks to campus credentials.

Nothing can completely guarantee the security of a password. There are practices that can help reduce risks:

- » Use a mix of uppercase, lowercase, numbers, and special characters
- » Make the password as long as the system allows
- » Think in terms of passphrases instead of passwords
- » Use a random password generator to avoid social engineering
- » Do not re-use university provided password for other systems
- » Change passwords at least annually or if exposure is suspected
- » Consider using a password vault to store passwords
- » Never share passwords with others
- » Report any suspicious activity to local law enforcement or the institutional IT incident response team

usernames and passwords for that service. While the credential pair may be sold or offered as valid credentials for accessing institutional resources, it's unknown if they provide access to institutional systems. The stolen credentials are generally a mix of faculty, staff, and student accounts with varying degrees of access to systems. Most universities and colleges maintain separate networks for students so that students don't generally have access to institutional data. The implementation of an architecture that enforces least privilege and limits access to hosts where sensitive functions are performed or sensitive data is stored via firewalls and access controls lists (ACLs) provides greater protection of institutional data.

TEST FACULTY, STAFF, AND STUDENTS TO SEE WHO CLICKS ON BAD LINKS

We know some threat actors have designed phishing scams to target college students, offering—among other things—work opportunities and easy money.²³ In an informal REN-ISAC poll, cybersecurity professionals ranked “users falling victim to phishing attempt” as their number one security concern.²⁴ Similar to other sectors, higher education institutions are finding great value in implementing phishing assessment simulations for users. Phishing simulations are a good way to provide continuous education and help users avoid falling prey to phishing attacks. Administrators should also be tested. This isn't about shaming anyone. If the top levels of school administrators—as well as IT administrators—see how easy it is to be fooled, they will not be able to write off the problem as a result of young or naïve students

IMPLEMENT MULTI-FACTOR AUTHENTICATION

To protect against phishing campaigns like the widespread and successful university payroll theft scheme perpetrated against faculty and staff in 2014 (and which still continues to plague higher education) many institutions are deploying two-factor authentication. In an informal REN-ISAC poll, 71 percent of respondents indicated adoption of multi-factor authentication.²⁵

ADOPT A DEFENSE IN DEPTH APPROACH

There is no single control that provides absolute security. Higher educational institutions must adopt a multi-vectored program that includes: education, testing and scanning, enhanced authentication techniques, user notifications of changes to their accounts and settings, and robust system logging and monitoring.

System administrators must be cautious about sending e-mails to users that link them directly to login pages, as it could have the unintended consequence of training users to be susceptible to phishing.

Users must likewise adopt a cautious approach to using their credentials. Users and administrators can work together to better protect individual and institutional resources.

In addition, Digital Citizens researchers had a few suggestions as well:

→ Consider a credential monitoring tool such as Dark Web ID or use of the best known web sites haveibeenpwned.com. Automate this process and assign security rules that considers the HEI's risk tolerance.

→ For the HEIs that develop their own software and applications—they should consider bug bounty programs. Bug bounties reward cyber researchers that discover vulnerabilities and report them to a at-risk organization. Its crowd-sourcing for cybersecurity. In the last year, the federal government has adjusted laws that would have once put researchers in legal jeopardy. Now is the time to create programs which could allow concerned individuals the opportunity to offer valuable assistance.

Numerous Fortune 500 companies and government agencies (including the Pentagon²⁶) have implemented bug bounty programs. Some universities are using them successfully for in-house development already.

If you are a software developer considering such an idea, discuss it with all appropriate parties at your HEI's InfoSec Office for appropriate framing and to ensure coordination.

In late 2016, a Distributed Denial of Service (DDoS) attack fueled by a botnet known as “Mirai” crippled the internet in some of America’s largest cities. Internet security blogger Brian Krebs looked at the background of Mirai’s creator—who uses the name of “Anna-Senpai”—and demonstrated the similarities to that of Paras Jha, a student at Rutgers University.²⁷ As Krebs himself points out, and we should also, Jha is not charged with any crimes. Jha was questioned by FBI and his family denies any wrongdoing.²⁸ This is not the first time that Jha’s name has been mentioned in connection with a large scale cyberattack. In October 2015, another programmer claimed Jha bragged about launching a series of DDoS attacks against Rutgers.²⁹

That brings us back to Rohyt Belani’s earlier mentioned comments: “...universities are the test bed for hackers.” If these allegations are true, Jha could be the first of a new generation of hackers with heightened skills honed while going after HEIs.

There will be those who blame HEIs, claiming what they call porous security providing wannabe threat actors a training ground for nefarious activity. Digital Citizens researchers see it differently, largely because of the tremendous information sharing network HEIs have established. Security teams on campuses face

many of the same challenges that those in skyscrapers and military bases are dealing with—and no one has come up with a perfect solution.

While some see problems, we see an opportunity. HEIs can create an environment where a new generation of ethical hackers can develop skills. Also, with encouragement and increased course offerings, HEIs can introduce faculty, staff, and students to learn the newest techniques and practices to keep devices—ranging from tablets and smartphones to the newest generation of Internet of Things connected refrigerators and household appliances—safer. What better place than a university or college to build a more aware and active society?

We know at least one other person who sees that potential—the hacker who released more .edu.s into the wild than any man alive. “How many millions of brilliant minds go through the top 100 universities of the world every year?” asked Razvan. “And how many of them actually decide to find vulnerabilities in their own universities to help secure them? A college or a university should become a central ground within any given area when it comes to cybersecurity or IT in general. But if we don’t change our mentality and laws, we will only stagnate as a society.”

The Digital Citizens Alliance utilized data gathered by Dark Web ID, a security tool of ID Agent, a company known for monitoring stolen user credentials, PII, and financial records that help their clients prevent fraud and cyber incidents.

Dark Web ID is a monitoring platform designed to help both public and private sector organizations detect and manage potential cyber threats to their organization and to their supply chain. Dark Web ID has identified more than 2 billion stolen records from more than 84% of commercial and government organizations in the U.S.

Researchers were asked to search for stolen e-mails and passwords posted on the Dark Web and marketed as being from American colleges and universities. To be considered a college or university in this report, the school had to match the following Scope of recognition: "The accreditation of postsecondary, non-degree-granting institutions and degree-granting institutions in the United States, including those granting associate, baccalaureate and master's degrees, that are predominantly organized to educate students for occupational, trade and technical careers, and including institutions that offer programs via distance education."

Dark Web ID compiled findings from searches beginning in 2009 until March 2, 2017. The research team looked at more than 86,000 unique .edu e-mail domains within more than 13 million .edu e-mail addresses, along with a handful of .com e-mail domains from the following online schools: Full Sail University (@fullsail.com), Kaplan University-Davenport Campus (@khec.com), Ashford University (@bpiedu.com), Colorado Technical University-Online (@careered.com). Approximately 99.7 percent of the e-mails in this research have .edu e-mail addresses. Duplicates were eliminated when possible.

For the purpose of this research paper, the Digital Citizens Alliance used just the 300 largest universities and colleges in the United States.

The data on the university's faculty, staff, and students comes from the National Center for Educational Statistics (NCES) and their Integrated Postsecondary Education Data System (IPEDS), located at <https://nces.ed.gov/ipeds/datacenter/>.

Dark Web ID does not test for the authenticity of each HEI-related credential in the course of this study. However, its analysts did consider the reputation of the relevant hackers before including the data in this study. This study is based on available resources, including published figures, and assumes that e-mails found on the Dark Web which reference a valid HEI domain name pertain either to current or former authorized users with the respective organizations named in this study, or to fraudulently-created credentials. Passwords found on the Dark Web may not necessarily pertain to the active networks or resources of the organizations named in this study and may pertain to third-party networks or resources, such as where .edu credential-holders used .edu names to register at a non-.edu site. Opinions reflect judgment at the time and are subject to change.

APPENDIX A

The 300 Higher Educational Institutions most commonly found on the Dark Web (according to ID Agent). These numbers include stolen e-mails, fake e-mails, and e-mails with domains designed to resemble those of the HEIs.

RANK	INSTITUTION	CREDENTIALS ON THE DARK WEB (MARCH 2017)	RANK	INSTITUTION	CREDENTIALS ON THE DARK WEB (MARCH 2017)
1	University of Michigan-Ann Arbor	122,556	76	University of Missouri-Columbia	34,328
2	Pennsylvania State University-Main Campus	119,350	77	Texas State University	34,172
3	University of Minnesota-Twin Cities	117,604	78	University of Massachusetts-Amherst	34,129
4	Michigan State University	115,973	79	Central Michigan University	34,053
5	Ohio State University-Main Campus	114,032	80	University of South Carolina-Columbia	33,477
6	University of Illinois at Urbana-Champaign	99,375	81	University of Oregon	32,203
7	New York University	91,372	82	Florida International University	32,127
8	University of Florida	87,310	83	Liberty University	31,537
9	Virginia Polytechnic Institute and State University	82,359	84	Kansas State University	30,770
10	Harvard University	80,100	85	Drexel University	30,530
11	Purdue University-Main Campus	79,294	86	University of Akron Main Campus	30,527
12	Indiana University-Bloomington	77,846	87	University of Phoenix-Arizona	30,503
13	Arizona State University-Tempe	77,763	88	Wayne State University	30,237
14	Cornell University	76,798	89	Northeastern University	29,900
15	Columbia University in the City of New York	75,421	90	University of Connecticut	29,047
16	University of Southern California	75,414	91	Georgetown University	28,863
17	University of California-Berkeley	75,058	92	Western Kentucky University	28,853
18	University of California-Los Angeles	72,622	93	Johns Hopkins University	28,544
19	University of Washington-Seattle Campus	71,817	94	Colorado State University-Fort Collins	28,495
20	Massachusetts Institute of Technology	67,608	95	James Madison University	28,345
21	University of Wisconsin-Madison	66,809	96	Western Michigan University	27,982
22	Louisiana State University and Agricultural & Mechanical College	64,660	97	Eastern Michigan University	27,868
23	Temple University	64,350	98	Georgia State University	27,836
24	Kent State University at Kent	63,029	99	University of Arkansas	27,687
25	University of Arizona	60,712	100	Middle Tennessee State University	27,540
26	University of North Carolina at Chapel Hill	59,843	101	Towson University	27,113
27	University of Georgia	59,156	102	University of North Texas	26,917
28	The University of Texas at Austin	58,400	103	University of North Carolina at Charlotte	26,672
29	Florida State University	58,185	104	University of California-Santa Barbara	26,407
30	University of Pennsylvania	57,372	105	Emory University	26,204
31	University of Colorado Boulder	55,988	106	Appalachian State University	26,072
32	University of South Florida-Main Campus	55,746	107	Illinois State University	25,522
33	Texas A & M University-College Station	54,969	108	Mississippi State University	25,147
34	University of California-Davis	53,842	109	New Mexico State University-Main Campus	25,069
35	University of Virginia-Main Campus	53,174	110	University of Mississippi	25,020
36	Stanford University	52,645	111	Old Dominion University	24,977
37	North Carolina State University at Raleigh	52,510	112	Grand Valley State University	24,177
38	Duke University	52,244	113	Washington State University	24,032
39	Ohio University-Main Campus	49,948	114	Boston College	23,221
40	Boston University	48,930	115	University of Utah	23,064
41	The University of Alabama	48,625	116	Tulane University of Louisiana	22,740
42	Northwestern University	46,884	117	Rochester Institute of Technology	22,509
43	The University of Tennessee-Knoxville	46,879	118	University of Louisville	22,229
44	University of California-San Diego	46,011	119	University of Memphis	22,055
45	University of Oklahoma-Norman Campus	45,424	120	California Polytechnic State University-San Luis Obispo	21,845
46	Syracuse University	45,006	121	The University of Texas at El Paso	21,754
47	Virginia Commonwealth University	44,835	122	University of California-Riverside	21,204
48	University of Cincinnati-Main Campus	44,748	123	Southern Illinois University-Carbondale	21,072
49	University of Kentucky	44,399	124	Missouri State University-Springfield	20,648
50	Rutgers University-New Brunswick	44,121	125	Eastern Kentucky University	19,840
51	Iowa State University	43,772	126	Saint Louis University	19,508
52	Clemson University	43,416	127	University of Toledo	19,328
53	Baylor University	43,309	128	Northern Arizona University	19,084
54	University of Pittsburgh-Pittsburgh Campus	42,639	129	Portland State University	18,914
55	Carnegie Mellon University	42,522	130	California State University-Fullerton	18,898
56	University of Maryland-College Park	40,842	131	Sam Houston State University	18,862
57	University of California-Irvine	40,275	132	San Francisco State University	18,685
58	Auburn University	40,148	133	SUNY at Binghamton	18,644
59	Texas Tech University	39,853	134	Oakland University	18,494
60	Oklahoma State University-Main Campus	39,258	135	Florida Atlantic University	17,893
61	University of Iowa	39,165	136	University of Houston	17,704
62	University of Wisconsin-Milwaukee	38,631	137	California State University-Fresno	17,685
63	University of Delaware	38,161	138	University of Nebraska-Lincoln	17,620
64	Ivy Tech Community College	37,658	139	Loyola University Chicago	17,601
65	Georgia Institute of Technology-Main Campus	37,354	140	Utah State University	17,184
66	George Washington University	37,344	141	The University of Texas at Arlington	17,164
67	East Carolina University	37,078	142	California State Polytechnic University-Pomona	16,983
68	University at Buffalo	36,853	143	Indiana University-Purdue University-Indianapolis	16,854
69	Ball State University	36,515	144	SUNY at Albany	16,800
70	University of Kansas	36,488	145	Georgia Southern University	15,779
71	University of New Mexico-Main Campus	35,335	146	Northern Illinois University	15,559
72	George Mason University	35,310	147	Saint Cloud State University	15,204
73	Bowling Green State University-Main Campus	35,299	148	Boise State University	14,921
74	West Virginia University	35,100	149	Nova Southeastern University	14,571
75	University of Central Florida	34,339	150	Kennesaw State University	14,324

CREDENTIALS ON THE DARK WEB (MARCH 2017)			CREDENTIALS ON THE DARK WEB (MARCH 2017)		
RANK	INSTITUTION		RANK	INSTITUTION	
151	Brigham Young University-Idaho	13,853	226	Utah Valley University	2,524
152	Brigham Young University-Provo	13,245	227	Miami University-Oxford	2,483
153	Fordham University	13,214	228	Suffolk County Community College	2,446
154	The University of Texas at San Antonio	12,636	229	Northern Virginia Community College	2,396
155	Troy University	12,298	230	Community College of Allegheny County	2,316
156	Rowan University	12,241	231	CUNY Queens College	2,314
157	California State University-Long Beach	11,893	232	Cuyahoga Community College District	2,303
158	California State University-Chico	11,821	233	Blinn College	2,271
159	St John's University-New York	11,763	234	The Community College of Baltimore County	2,122
160	DePaul University	11,352	235	Bakersfield College	2,103
161	Columbus State Community College	11,232	236	Orange Coast College	2,081
162	Montclair State University	11,168	237	Santa Barbara City College	2,040
163	California State University-Northridge	10,940	238	Palm Beach State College	1,986
164	Portland Community College	9,999	239	Mt San Antonio College	1,894
165	CUNY Bernard M Baruch College	9,623	240	Oakland Community College	1,890
166	San Diego State University	9,279	241	Palomar College	1,853
167	DeVry University-Illinois	9,136	242	Tarrant County College District	1,746
168	Central Piedmont Community College	9,107	243	Capella University	1,723
169	University of Colorado Denver	9,077	244	El Camino Community College District	1,712
170	California State University-Sacramento	8,314	245	University of Maryland-University College	1,691
171	Sinclair Community College	8,278	246	Tidewater Community College	1,684
172	The University of Texas at Dallas	8,197	247	Salt Lake Community College	1,547
173	Weber State University	7,913	248	St Petersburg College	1,544
174	Kaplan University-Davenport Campus	7,853	249	CUNY Borough of Manhattan Community College	1,542
175	Des Moines Area Community College	7,379	250	Collin County Community College District	1,535
176	Montana State University	7,305	251	CUNY Brooklyn College	1,533
177	CUNY Hunter College	7,265	252	College of DuPage	1,486
178	California State University-San Bernardino	7,182	253	CUNY LaGuardia Community College	1,467
179	Community College of Rhode Island	6,997	254	CUNY New York City College of Technology	1,386
180	Central New Mexico Community College	6,562	255	San Diego Mesa College	1,363
181	Oregon State University	6,163	256	Chaffey College	1,248
182	Cleveland State University	6,114	257	Nassau Community College	1,236
183	Austin Community College District	6,067	258	Valencia College	1,227
184	Western Governors University	5,735	259	American Public University System	1,215
185	Southern New Hampshire University	5,710	260	College of Southern Nevada	1,177
186	Columbia College	5,623	261	Colorado Technical University-Online	1,163
187	Walden University	5,543	262	Ashford University	1,123
188	Broward College	5,488	263	Harrisburg Area Community College-Harrisburg	1,098
189	The University of Texas-Pan American	4,946	264	National University	1,057
190	Community College of Philadelphia	4,927	265	CUNY Queensborough Community College	988
191	California State University-Los Angeles	4,921	266	San Jacinto Community College	958
192	Milwaukee Area Technical College	4,885	267	South Texas College	954
193	Richland College	4,867	268	Indian River State College	934
194	CUNY John Jay College of Criminal Justice	4,817	269	Santa Rosa Junior College	917
195	Riverside City College	4,774	270	Grossmont College	908
196	San Jose State University	4,739	271	Glendale Community College	902
197	Lansing Community College	4,727	272	Keiser University-Ft Lauderdale	899
198	Georgia Perimeter College	4,677	273	Chamberlain College of Nursing-Illinois	860
199	Saint Leo University	4,439	274	University of Illinois at Chicago	849
200	Saint Louis Community College	4,367	275	Long Beach City College	773
201	Lone Star College System	4,312	276	Metropolitan State University of Denver	767
202	American River College	4,179	277	Fullerton College	763
203	Wake Technical Community College	4,179	278	Sierra College	743
204	Delgado Community College	4,162	279	Seminole State College of Florida	737
205	CUNY City College	3,560	280	Macomb Community College	687
206	Pima Community College	3,468	281	Mesa Community College	686
207	University of Nevada-Las Vegas	3,448	282	Cerritos College	661
208	Hillsborough Community College	3,388	283	Pasadena City College	627
209	Everest University-South Orlando	3,376	284	Front Range Community College	603
210	Florida State College at Jacksonville	3,280	285	Central Texas College	474
211	Miami Dade College	3,279	286	Southwestern College	460
212	Saddleback College	3,195	287	Diablo Valley College	456
213	Santa Monica College	3,183	288	Fresno City College	447
214	Johnson County Community College	3,157	289	Rio Salado College	444
215	Full Sail University	3,100	290	Los Angeles Valley College	436
216	Grand Canyon University	3,096	291	East Los Angeles College	436
217	Stony Brook University	3,064	292	Santa Ana College	391
218	Montgomery College	3,025	293	CUNY Kingsborough Community College	380
219	San Joaquin Delta College	2,873	294	Excelsior College	348
220	Houston Community College	2,771	295	Columbia Southern University	322
221	San Antonio College	2,747	296	Los Angeles Pierce College	297
222	Tulsa Community College	2,648	297	Los Angeles City College	282
223	Metropolitan Community College-Kansas City	2,623	298	Thomas Edison State College	272
224	El Paso Community College	2,614	299	De Anza College	208
225	City College of San Francisco	2,532	300	American College of Financial Services	137

APPENDIX B

Schools ranked by ratio comparing credentials on the Dark Web to current university community faculty, staff, and student populations at the 300 largest Higher Educational Institutions within the United States (according to ID Agent). These numbers include stolen e-mails, fake e-mails, and e-mails with domains designed to resemble those of the HEIs.

RATIO OF CREDENTIALS ON DARK WEB TO TOTAL FACULTY, STAFF, AND STUDENTS			RATIO OF CREDENTIALS ON DARK WEB TO TOTAL FACULTY, STAFF, AND STUDENTS		
RANK	INSTITUTION		RANK	INSTITUTION	
1	Massachusetts Institute of Technology	2.81:1	76	Illinois State University	1.05:1
2	Carnegie Mellon University	2.4:1	77	University of California-San Diego	1.05:1
3	Cornell University	2.39:1	78	University of Pittsburgh-Pittsburgh Campus	1.04:1
4	Baylor University	2.27:1	79	University at Buffalo	1.04:1
5	Virginia Polytechnic Institute and State University	2.1:1	80	Western Michigan University	1.03:1
6	Pennsylvania State University-Main Campus	1.94:1	81	Kansas State University	1.03:1
7	University of Michigan-Ann Arbor	1.87:1	82	University of Kansas	1.02:1
8	Michigan State University	1.87:1	83	Mississippi State University	1:1
9	Kent State University at Kent	1.87:1	84	Eastern Kentucky University	1:1
10	Bowling Green State University-Main Campus	1.87:1	85	Texas Tech University	1:1
11	University of Illinois at Urbana-Champaign	1.75:1	86	University of Massachusetts-Amherst	0.99:1
12	Louisiana State University and Agricultural & Mechanical College	1.72:1	87	Emory University	0.99:1
13	Harvard University	1.71:1	88	West Virginia University	0.98:1
14	University of Minnesota-Twin Cities	1.71:1	89	University of Iowa	0.98:1
15	Syracuse University	1.68:1	90	University of New Mexico-Main Campus	0.97:1
16	Columbia University in the City of New York	1.66:1	91	SUNY at Binghamton	0.97:1
17	Stanford University	1.64:1	92	California Polytechnic State University-San Luis Obispo	0.96:1
18	University of Virginia-Main Campus	1.64:1	93	University of California-Santa Barbara	0.95:1
19	Clemson University	1.62:1	94	Drexel University	0.94:1
20	Duke University	1.58:1	95	Southern Illinois University-Carbondale	0.91:1
21	Purdue University-Main Campus	1.56:1	96	Loyola University Chicago	0.91:1
22	Ball State University	1.52:1	97	George Mason University	0.91:1
23	Northwestern University	1.51:1	98	University of Memphis	0.9:1
24	University of California-Berkeley	1.5:1	99	The University of Texas at Austin	0.89:1
25	Ohio University-Main Campus	1.49:1	100	Saint Louis University	0.89:1
26	University of North Carolina at Chapel Hill	1.42:1	101	Old Dominion University	0.89:1
27	University of Delaware	1.42:1	102	University of Arkansas	0.88:1
28	Indiana University-Bloomington	1.41:1	103	Wayne State University	0.88:1
29	Temple University	1.41:1	104	Sam Houston State University	0.87:1
30	University of Colorado Boulder	1.39:1	105	University of North Carolina at Charlotte	0.86:1
31	University of Oklahoma-Norman Campus	1.37:1	106	Saint Cloud State University	0.86:1
32	University of Florida	1.37:1	107	Grand Valley State University	0.86:1
33	University of Pennsylvania	1.36:1	108	University of Maryland-College Park	0.85:1
34	Arizona State University-Tempe	1.34:1	109	Texas State University	0.84:1
35	University of Southern California	1.31:1	110	The University of Texas at El Paso	0.84:1
36	University of Georgia	1.31:1	111	University of California-Riverside	0.84:1
37	Ohio State University-Main Campus	1.3:1	112	Missouri State University-Springfield	0.84:1
38	New York University	1.3:1	113	SUNY at Albany	0.82:1
39	New Mexico State University-Main Campus	1.29:1	114	University of South Carolina-Columbia	0.82:1
40	Tulane University of Louisiana	1.28:1	115	Oakland University	0.81:1
41	Boston College	1.26:1	116	University of Connecticut	0.8:1
42	Northeastern University	1.26:1	117	University of Toledo	0.8:1
43	Auburn University	1.26:1	118	University of Louisville	0.78:1
44	Appalachian State University	1.25:1	119	Texas A & M University-College Station	0.77:1
45	Western Kentucky University	1.24:1	120	Georgia State University	0.74:1
46	Oklahoma State University-Main Campus	1.23:1	121	University of Missouri-Columbia	0.74:1
47	University of Wisconsin-Milwaukee	1.23:1	122	Johns Hopkins University	0.72:1
48	North Carolina State University at Raleigh	1.22:1	123	University of Mississippi	0.72:1
49	Georgia Institute of Technology-Main Campus	1.22:1	124	Colorado State University-Fort Collins	0.71:1
50	Georgetown University	1.21:1	125	Fordham University	0.71:1
51	Florida State University	1.21:1	126	California State University-Fresno	0.7:1
52	Virginia Commonwealth University	1.18:1	127	Washington State University	0.68:1
53	Boston University	1.16:1	128	Georgia Southern University	0.67:1
54	University of California-Los Angeles	1.16:1	129	Rowan University	0.67:1
55	James Madison University	1.15:1	130	University of North Texas	0.67:1
56	George Washington University	1.15:1	131	Rutgers University-New Brunswick	0.65:1
57	The University of Alabama	1.14:1	132	California State Polytechnic University-Pomona	0.65:1
58	Central Michigan University	1.14:1	133	Northern Illinois University	0.64:1
59	University of California-Davis	1.14:1	134	California State University-Chico	0.62:1
60	University of Wisconsin-Madison	1.14:1	135	Portland State University	0.61:1
61	University of South Florida-Main Campus	1.13:1	136	Northern Arizona University	0.61:1
62	University of Washington-Seattle Campus	1.12:1	137	Boise State University	0.6:1
63	Rochester Institute of Technology	1.12:1	138	Florida International University	0.58:1
64	Eastern Michigan University	1.12:1	139	San Francisco State University	0.57:1
65	University of Akron Main Campus	1.11:1	140	University of Nebraska-Lincoln	0.57:1
66	East Carolina University	1.11:1	141	Utah State University	0.56:1
67	University of Arizona	1.1:1	142	Troy University	0.55:1
68	University of Oregon	1.1:1	143	University of Utah	0.54:1
69	University of Kentucky	1.1:1	144	Florida Atlantic University	0.53:1
70	Middle Tennessee State University	1.09:1	145	University of Central Florida	0.52:1
71	Iowa State University	1.09:1	146	St John's University-New York	0.51:1
72	University of California-Irvine	1.07:1	147	Nova Southeastern University	0.5:1
73	The University of Tennessee-Knoxville	1.07:1	148	Kennesaw State University	0.5:1
74	University of Cincinnati-Main Campus	1.07:1	149	Montclair State University	0.48:1
75	Towson University	1.06:1	150	CUNY Bernard M Baruch College	0.47:1

RATIO OF CREDENTIALS ON DARK WEB TO TOTAL FACULTY, STAFF, AND STUDENTS			RATIO OF CREDENTIALS ON DARK WEB TO TOTAL FACULTY, STAFF, AND STUDENTS		
RANK	INSTITUTION		RANK	INSTITUTION	
151	California State University-Fullerton	0.45 : 1	226	Western Governors University	0.09 : 1
152	Indiana University-Purdue University-Indianapolis	0.43 : 1	227	Orange Coast College	0.09 : 1
153	Columbus State Community College	0.42 : 1	228	El Paso Community College	0.08 : 1
154	DePaul University	0.41 : 1	229	Suffolk County Community College	0.08 : 1
155	Montana State University	0.4 : 1	230	The Community College of Baltimore County	0.08 : 1
156	Central Piedmont Community College	0.4 : 1	231	CUNY Brooklyn College	0.08 : 1
157	Sinclair Community College	0.39 : 1	232	Cuyahoga Community College District	0.07 : 1
158	The University of Texas at San Antonio	0.39 : 1	233	Oakland Community College	0.07 : 1
159	The University of Texas at Arlington	0.38 : 1	234	Utah Valley University	0.07 : 1
160	University of Houston	0.38 : 1	235	CUNY New York City College of Technology	0.07 : 1
161	Ivy Tech Community College	0.38 : 1	236	Palomar College	0.07 : 1
162	Brigham Young University-Provo	0.37 : 1	237	El Camino Community College District	0.07 : 1
163	Community College of Rhode Island	0.37 : 1	238	CUNY LaGuardia Community College	0.06 : 1
164	Liberty University	0.36 : 1	239	Palm Beach State College	0.06 : 1
165	Brigham Young University-Idaho	0.36 : 1	240	Mt San Antonio College	0.06 : 1
166	California State University-San Bernardino	0.35 : 1	241	Chaffey College	0.06 : 1
167	Cleveland State University	0.32 : 1	242	Lone Star College System	0.06 : 1
168	DeVry University-Illinois	0.32 : 1	243	Tidewater Community College	0.06 : 1
169	Columbia College	0.31 : 1	244	San Diego Mesa College	0.05 : 1
170	The University of Texas at Dallas	0.31 : 1	245	National University	0.05 : 1
171	California State University-Long Beach	0.29 : 1	246	CUNY Queensborough Community College	0.05 : 1
172	Portland Community College	0.29 : 1	247	CUNY Borough of Manhattan Community College	0.05 : 1
173	Des Moines Area Community College	0.29 : 1	248	Collin County Community College District	0.05 : 1
174	Weber State University	0.28 : 1	249	Colorado Technical University-Online	0.05 : 1
175	University of Colorado Denver	0.28 : 1	250	Nassau Community College	0.05 : 1
176	CUNY John Jay College of Criminal Justice	0.28 : 1	251	Harrisburg Area Community College-Harrisburg	0.05 : 1
177	CUNY Hunter College	0.27 : 1	252	Indian River State College	0.05 : 1
178	California State University-Sacramento	0.26 : 1	253	Grossmont College	0.05 : 1
179	Lansing Community College	0.26 : 1	254	College of DuPage	0.05 : 1
180	Milwaukee Area Technical College	0.26 : 1	255	Salt Lake Community College	0.05 : 1
181	San Diego State University	0.25 : 1	256	Capella University	0.05 : 1
182	California State University-Northridge	0.25 : 1	257	Grand Canyon University	0.04 : 1
183	Riverside City College	0.24 : 1	258	Chamberlain College of Nursing-Illinois	0.04 : 1
184	Saint Leo University	0.24 : 1	259	Miami Dade College	0.04 : 1
185	Community College of Philadelphia	0.24 : 1	260	Houston Community College	0.04 : 1
186	Richland College	0.23 : 1	261	Northern Virginia Community College	0.04 : 1
187	Central New Mexico Community College	0.23 : 1	262	St Petersburg College	0.04 : 1
188	Delgado Community College	0.22 : 1	263	Glendale Community College	0.04 : 1
189	The University of Texas-Pan American	0.22 : 1	264	Keiser University-Ft Lauderdale	0.04 : 1
190	Georgia Perimeter College	0.2 : 1	265	Sierra College	0.04 : 1
191	CUNY City College	0.19 : 1	266	Seminole State College of Florida	0.04 : 1
192	California State University-Los Angeles	0.18 : 1	267	Santa Rosa Junior College	0.04 : 1
193	Saint Louis Community College	0.18 : 1	268	University of Maryland-University College	0.03 : 1
194	Oregon State University	0.18 : 1	269	Metropolitan State University of Denver	0.03 : 1
195	Wake Technical Community College	0.18 : 1	270	Tarrant County College District	0.03 : 1
196	Saddleback College	0.15 : 1	271	San Jacinto Community College	0.03 : 1
197	San Joaquin Delta College	0.15 : 1	272	College of Southern Nevada	0.03 : 1
198	Everest University-South Orlando	0.15 : 1	273	Front Range Community College	0.03 : 1
199	Johnson County Community College	0.14 : 1	274	Long Beach City College	0.03 : 1
200	Full Sail University	0.14 : 1	275	South Texas College	0.03 : 1
201	Kaplan University-Davenport Campus	0.14 : 1	276	Fullerton College	0.03 : 1
202	Austin Community College District	0.14 : 1	277	Cerritos College	0.03 : 1
203	American River College	0.14 : 1	278	Mesa Community College	0.03 : 1
204	San Jose State University	0.13 : 1	279	Macomb Community College	0.03 : 1
205	Tulsa Community College	0.13 : 1	280	Valencia College	0.03 : 1
206	Metropolitan Community College-Kansas City	0.13 : 1	281	Southwestern College	0.02 : 1
207	University of Phoenix-Arizona	0.13 : 1	282	Los Angeles Valley College	0.02 : 1
208	Community College of Allegheny County	0.12 : 1	283	Pasadena City College	0.02 : 1
209	Southern New Hampshire University	0.12 : 1	284	Diablo Valley College	0.02 : 1
210	San Antonio College	0.12 : 1	285	University of Illinois at Chicago	0.02 : 1
211	Florida State College at Jacksonville	0.12 : 1	286	Rio Salado College	0.02 : 1
212	Broward College	0.12 : 1	287	Central Texas College	0.02 : 1
213	Pima Community College	0.11 : 1	288	American Public University System	0.02 : 1
214	Blinn College	0.11 : 1	289	Ashford University	0.02 : 1
215	Hillsborough Community College	0.11 : 1	290	Fresno City College	0.02 : 1
216	Miami University-Oxford	0.11 : 1	291	CUNY Kingsborough Community College	0.02 : 1
217	Bakersfield College	0.11 : 1	292	Columbia Southern University	0.01 : 1
218	Santa Barbara City College	0.11 : 1	293	Los Angeles City College	0.01 : 1
219	University of Nevada-Las Vegas	0.11 : 1	294	Los Angeles Pierce College	0.01 : 1
220	Montgomery College	0.11 : 1	295	Santa Ana College	0.01 : 1
221	CUNY Queens College	0.1 : 1	296	Thomas Edison State College	0.01 : 1
222	Stony Brook University	0.1 : 1	297	East Los Angeles College	0.01 : 1
223	Santa Monica College	0.1 : 1	298	De Anza College	0.01 : 1
224	Walden University	0.1 : 1	299	Excelsior College	0.01 : 1
225	City College of San Francisco	0.1 : 1	300	American College of Financial Services	0.01 : 1

APPENDIX C

The number of institutions and credentials on the Dark Web by state (according to ID Agent).

STATE	NUMBER OF SCHOOLS	TOTAL EMAIL ACCOUNTS ON DARK WEB (MARCH 2017)
CA	54	672,678
NY	25	450,349
MI	11	408,644
TX	25	390,199
OH	12	387,321
PA	10	365,241
FL	20	333,848
VA	9	304,617
MA	6	283,888
NC	8	267,705
IL	11	249,696
IN	5	248,167
AZ	9	196,658
GA	7	185,330
MN	4	140,074
KY	4	115,321
WI	3	110,325
MD	6	103,337
AL	4	101,393
IA	4	98,169
TN	3	96,474
CO	6	96,093
WA	2	95,849
LA	3	91,562
OK	3	87,330
MO	6	87,097
SC	2	76,893
UT	7	71,212
KS	3	70,415
NJ	4	67,802
OR	4	67,279
NM	3	66,966
DC	2	66,207
MS	2	50,167
DE	1	38,161
WV	2	36,315
CT	1	29,047
ID	2	28,774
AR	1	27,687
NE	1	17,620
MT	1	7,305
RI	1	6,997
NH	1	5,710
NV	2	4,625

ENDNOTES

- 1 Catalin Cimpanu. Notorious Hacker GhostShell Doxes Himself So He Could Get a Job (Softpedia: March 14, 2016).
- 2 Nicole Perloth. Hackers Breach 53 Universities and Dump Thousands of Personal Records Online (NY, NY: The New York Times, October 3, 2014).
- 3 Steve Ranger. Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you (ZDnet: September 1, 2016).
- 4 Cyber-Related Scams Targeting Universities, Employees, and Students (Federal Bureau of Investigation, May 5, 2014).
- 5 Employment Scam Targeting College Students Remains Prevalent (Federal Bureau of Investigation, January 18, 2017).
- 6 2017 Consumer Mobile Security App Use (Keeper Security: 2017).
- 7 Jeff Stone. Hacker University: Cyberattackers Target Military Reserch, Student Records At 'Soft Target' US Colleges (International Business Times Business: September 30, 2015).
- 8 Jeremy Seth Davis. Biggest breaches of 2016 (SC Magazine: December 14, 2016)
- 9 Threat, vulnerability, risk- commonly mixed up terms (Threat Analysis: 2017).
- 10 Darlene Storm. Hacker breached 63 universities and government agencies (Computerworld: February 15, 2017).
- 11 Levi Gundert. Russian-Speaking Hacker Sells SQLi for Unauthorized Access to Over 60 Universities and Government Agencies (Recorded Future / Cyber Threat Intelligence: February 15, 2017).
- 12 Dan Goodin. Critical Vulnerability under 'massive' attack imperils high-impact sites (Ars Technica: March 9, 2017).
- 13 Catalin Cimpanu. Los Angeles Valley College Pays a Whopping \$30,000 in Ransomware Incident (Bleeping Computer: January 10, 2017) and Veronica Rocha. Los Angeles Valley College pays \$28,000 in bitcoin ransom to hackers (Los Angeles, CA. Los Angeles Times: January 11, 2017).
- 14 U.S. Department of Homeland Security. Malicious Cyber Actors Target US Universities and Colleges (Office of Intelligence and Analysis: January 16, 2015).
- 15 Katie Bo Williams. University of Virginia hack targeted employees with China ties (Washington, D.C., The Hill: August 21, 2015).
- 16 Felicia Schwartz. Penn State's Engineering School Computers Hacked (NY, NY. The Wall Street Journal: May 16, 2015).
- 17 National Science Foundation, National Center for Science and Engineering Statistics, Higher Education R&D Survey, Rankings by total R&D expenditures 2015 (Arlington, VA: Retrieved from <https://ncesdata.nsf.gov/profiles/site?method=rankingBySource&ds=herd>).
- 18 Richard Perez-Pena. Universities Face a Rising Barrage of Cyberattacks (NY, NY. The New York Times: July 16, 2013).
- 19 Tal Kopan, Kristen Holmes, Stephen Collinson. U.S., China say they won't engage in cybertheft (CNN: September 25, 2015).
- 20 Claud Xiao, Rob Downs. Stolen Email Accounts of World's Top Universities Selling on China's Largest C2C Platform (Santa Clara, California, Palo Alto Networks: September 4, 2014).
- 21 University of MassAmherst. University of Massachusetts Amherst Cybersecurity Institute (Amherst, MA: Retrieved from <https://cybersecurity.umass.edu>).
- 22 University of Houston. University Information Technology, Strong Passwords (Houston, TX: Retrieved from <http://www.uh.edu/infotech/services/accounts/passwords/strong-passwords/#about>).
- 23 Megan Raposa. 'Work from home' phishing scam targets students (McLean, VA, USA Today: January 20, 2015).
- 24 Kim Milford and Joanna Grama. This Magic Moment: Reflections on Cybersecurity (Educause Review, September 28, 2015).
- 25 Ibid.
- 26 Sarah Lai Stirland. How DOD embraced bug bounties -- and how your agency can, too (McLean, VA, FCW, cybersecurity: October 24, 2016).
- 27 Brian Krebs. Who is Anna-Senpai, the Mirai Worm Author? (Krebs on Security: January 18, 2017).
- 28 Adam Clark and Mark Mueller. FBI questions Rutgers student about massive cyber attack (NJ.com: January 20, 2017).
- 29 Nikhilesh De. Cybersecurity expert identifies Rutgers students as DDoS perpetrator (New Brunswick, NJ. The Daily Targam: January 23, 2017).

ABOUT DIGITAL CITIZENS

This report was created by the Digital Citizens Alliance, a nonprofit 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet and the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place. While all Digital Citizens hold themselves personally responsible to do all they can to protect themselves and their families, we are also concerned that technologies, standards, and practices are in place that will help keep all of us safe as a community. The industry has a critical role to play in ensuring those safeguards are established and updated as needed to address the continually evolving challenges we face online. We have much work to do, but we can't do it effectively without understanding the problems we face. That is why the Digital Citizens Alliance investigates issues such as those detailed in this report. By sharing our findings with consumers, we hope all Digital Citizens will engage in discussions about these issues.

