Date: November 12, 2014

To: IT Executives and Security Staff

Advisory: University Payroll Theft Scheme

Sharing Guideline: This Advisory may be shared publicly and redistributed without restriction.

The purpose of this advisory is to provide relevant and actionable information for prevention and defense. REN-ISAC is available for questions and assistance in understanding how to deal with the issue.

Universities and colleges have been targeted by spearphishing campaigns designed to steal user credentials for many years. Stolen credentials are used for many purposes, such as sending spam from compromised e-mail accounts, optimizing search engine results for black market pharmaceutical web pages, gaining access to university-licensed resources, and hosting malware.

For roughly the past year, many of these campaigns have used harvested credentials to alter victim's direct deposit information. Targeted individuals include both faculty and administrators from various departments. Several of the attacks appear to have specifically targeted individuals in university medical and dental programs. These e-mails often use subjects related to salary increases to lure victims into clicking on malicious links. Subject lines have included:

- Your Salary Review Documents
- Important Salary Notification
- Your Salary Raise Confirmation
- connection from unexpected IP
- RE: Mailbox has exceeded its storage limit.

The malicious links contained in these e-mails direct victims to webpages controlled by the attackers that look nearly identical to their university's legitimate login portals. Once the attackers harvest the user's credentials, the credentials are commonly used to access the victim's payroll information and re-route direct deposits to a bank account controlled by the attacker. In at least one case, insurance policy information was also changed. The number of personnel targeted in these attacks also varies but reports indicate targets range anywhere from 15 to several hundred.

Documented Attacks

In December 2013, a University of Western Michigan employee had their direct deposit information altered following a successful phishing attack. The victim claims that his single sign on (SSO) credentials were used to access his e-mail and delete the university's automatically generated e-mail notification. Publicly posted media reports highlight several other universities that have been impacted by similar campaigns. These include: Boston University in early January 2014, Texas A&M in July 2013, the University of Iowa in November of 2013, and the University of Michigan in August of 2013.[1,2,3,4] While only a few cases have been reported in the media, estimates of impacted universities and colleges are much larger.

To address these attacks, several entities have released public and private alerts on this activity throughout the past year to include the MS-ISAC, the REN-ISAC, the FBI and The Internet Crime Complaint Center (IC3) among others.[5]

Attack Details

While it is possible that the attackers behind these campaigns have been launching similar attacks on other sectors, there are several reasons why higher educational institutions would be an attractive target. Most universities and colleges provide access to a wide variety of information regarding their technology environment in an effort to support their global research and education missions. Access to this information allows attackers to more easily conduct reconnaissance prior

to an attack. E-mail contact information for faculty and staff can also be easily accessed and used by attackers to create target lists for their campaigns.

In at least one case, a university confirmed that the list of phishing recipients was generated using a scrape of email addresses on the public campus website. The university assessed that this was likely the reason faculty, rather than staff, were the primary targets as this University's website contains faculty profiles with email addresses, but few staff email addresses.

Attempting to harvest credentials through phishing is a common practice, but certain aspects of this campaign indicate that attackers are specifically targeting university and college personnel and conducting some level of reconnaissance prior to their attack. Though it is unknown if these attacks are being conducted by a single group or multiple groups, the tactics, techniques, and procedures (TTPs) used in many of the attacks share very similar characteristics.

Some TTPs include:

- Altering direct deposit account information
- Spoofed to appear as if message came from the appropriate department, e.g. HR for "salary increase" lures or IT department if "mailbox exceeded"
- Spoofed login screens that are a close replica of legitimate login screen
- Targeting of faculty and staff
- Using university images within e-mails text
- Spoofed institutional-specific prompts for additional credential information, e.g., PINS, bank account numbers.
- URLs mimicking legitimate (and accessible) portal URLs
- Use of the "salary increase" approach seems to coincide with end of the fiscal year.

The phishing e-mails have contained official institutional images; often via an HTML image link direct to the resource.

***Subject**: Important Salary Notification*

As part of ***<institution name>*** *standard practice to offer salary increases once a year after an annual review, the Human Resources reviewed you for a salary raise on your next paycheck*

Click below to confirm and access your salary revision documents:

Click Here to access the documents

Sincerely,
Human Resources

Example of the text contained within the e-mail

Examples of spoofed sender e-mail addresses include:

- HRresources @<domain>.edu
- employeebenefits @<domain>.edu

In addition, actors appear to be aware of institution-specific requirements for updating banking information. For example, if the university requires a Personal Identification Number (PIN) or bank account number to change existing settings, the spoofed login screens may prompt users for this information.

The timing of some of these attacks has also been observed coinciding with the end of the fiscal year for many universities and colleges (July 1). This is often when institutions give their employees salary increases,[6] and may help add to the perceived legitimacy of the e-mails. These factors all contribute to a relatively well-planned campaign with an increased likelihood of deceiving unsuspecting users into divulging their personal information.

Prevention Techniques

While educating end users about the dangers of phishing and providing real world examples of what indicators to look for is always a great practice for creating a human line of defense, universities can institute additional measures to help defend their employees from these attacks. It is important to take

into consideration that adding some controls may result in increased costs that entities may or may not be willing to absorb. Suggested defensive measures include:

- Remove self-service direct deposit capabilities, when practical.
- Add two-factor authentication or VPN requirements. This may not completely stop attacks but it makes the attacker's work more difficult.
- Send e-mail alerts to users when direct deposit information has been changed. As mentioned previously, this can be circumvented in some cases.
- Redact sensitive information available to the user in the online system. This will only stop the further loss of personal information such as SSN.
- Require users to enter additional information, like an account number or pin. Attackers who know this can adjust their phishing messages to adapt.
- Implement back-end systems that inspect for suspicious direct deposit account changes, such as those from unusual geographic locations, duplicate DD account numbers, unusual destination account routing numbers.
- Contact information sharing communities such as the ISAC serving your sector to stay informed concerning new attacks and to share your own experience.
- Be cautious about sending emails 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 should be cautious when accessing e-mail and never send account information to others. In addition, users should use caution and double-check the URL when viewing e-mails that prompt an individual to login to verify it belongs to their institution.
- Further recommendations on phishing defense can be found on the US-CERT website.[7]

Additional technical protection and response information is shared on the REN-ISAC trusted information sharing community.

Points of Contact

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)[8]
The mission of the REN-ISAC mission is to aid and promote cybersecurity operational protection and response within the research and higher education (R&E) communities.

SOC@REN-ISAC.net
24x7 Watch Desk (317) 278-6630

References

***NOTE:** Webpages may change or become unavailable over time.*

[1] http://cis.tamu.edu/news/2013/07/Nine_A_M_accounts_compromised_direct_deposit_altered.php
[2] http://www.boston.com/yourcampus/news/boston_university/2014/01/bu_employee_direct_deposit_pay_stolen_through_alleged_internet_scam.html
[3] http://www.annarbor.com/news/university-of-michigan-spear-phishing/
[4] https://it.usu.edu/computer-security/computer-security-threats/articleID=25294
[5] Public Service Announcement, Prepared by the Internet Crime Complaint Center (IC3); http://www.ic3.gov/media/2014/140505.aspx
[6] http://wiki.fool.com/When_Is_the_Fiscal_Year%3F
[7] https://www.us-cert.gov/ncas/tips/ST04-014
[8] http://www.ren-isac.net/