EPiC Series in Computing
Volume 78, 2021, Pages 89–97
Proceedings of the European University Information Systems Conference 2021

End-to-end mapping of a spear-phishing attack on HEI in EU

Kurt Nielsen and Helle Betina Kristensen
University College Lillebaelt, Odense, Denmark.
kgni@ucl.dk, hell9675@edu.ucl.dk

Abstract

Spear-phishing is a growing threat to the education sector. This analysis maps a specific attacker and demonstrate a likelihood 15% to be attacked by this attacker. The analysis uses open source intelligence tools to reveal a continued pattern where the actor is reusing infrastructure and procedure against several HEI in Europe.

For a spear-phising attack to become successful, it has to be able to lure the enduser. This study includes a user vulnerability assessment on the specific spear-phishing attacks used in two comparable studies consisting of 36,851 respondents from two educational institutions. The studies show that without prior training, the concrete spear-phishing attack will lure 20 to 49% of all users.

To investigate the high risk of this attack to endusers an eye-tracking study was conducted. The study shows that respondents generally spend more time viewing phishing indicator than one expect by chance, but there seems to be no correlation between viewing indicators and lured to action. Endusers seems to rate the trustworthiness of mails by an overall reading. As a consequence endusers are easily lured by the attacker because of the trustworthiness of the specific spear-phishing mail.

1 Introduction

Every student and staff at HEI in EU has an email account and many have received phishingmail in their universities mailbox. Some phisingmail are easily detected as scam, but others are targeted the user as a student or employee at his or her specific institution. Were phisingmail try to lure a general enduser, spear-phishing is a targeted attempt to trick one or more specific victims into passing on personal information. Spearphishing often uses advanced social engineering in order to target content to the victim.[1]

In 2019, the University of Copenhagen was hit by a major spear-phishing attack where more than 500 accounts were compromised by an email template masquerading as the university's own

S. Bolis, J.-F. Desnos, L. Merakos and R. Vogl (eds.), EUNIS 2021 (EPiC Series in Computing, vol. 78), pp. 89–97

library.[2] It was possible to identify the spear-phishing attack and it was identified as the state-sponsored Iranian group known as Silent Librarian. A name based on the method used in their attacks, where they set up domains that look like the institution's own domain, copy the library's login page and send out emails to staff and students requesting them to renew their account, an action that leads to the group taking over the account.

The FBI claims that this group has compromised approx. 8,000 accounts and is responsible for attacks on 173 educational institutions, including the attack on the University of Copenhagen.[3]

Although there have been a number of technological advances that can limit the vulnerability of this type of attack, the threat is still assumed to be increasing as the effectiveness of phishing emails lies in the attack vector tricking the user into performing an action.

A central aspect therefore is security literacy among users. Scandinavian readers and other minor languages users has long been helped by the poor translation into these languages in phishing emails, which has lead to users being able to spot phishing attempts on wording alone. However, these translations have improved and the analysis will therefore examine how a user reads current phishing attempts and is tricked into clicking on a phishinglink.

The method used consists of three steps:

First, the current and relevant threats to the education sector were examined in threat assessments and technical studies. The technical study used Open Source Intelligence Tools and passive DNS to map the scope and variation as well as the attack vectors. Some parts of infrastructure from the attack on University of Copenhagen was able to be traced back due the historical data from passive DNS which records every misconceived DNS look-up from its sensors.

Second, to verify the vulnerability of users, two awareness campaigns were carried out based on the methods and vectors used by a specific actor. Staff and students at University of Southern Denmark (SDU) were sent 35,714 phishing emails in 2019, all using the same template as used in the attack on the University of Copenhagen, and students at University College Lillebaelt (UCL) were sent 1,137 phishing emails using a different template from the same actor in 2020.

Third, to map how people read the specific spear-phishing attack and to uncover reading habits in terms of IT security, an eye-tracking study using heat maps, gaze plots and Areas of Interest has been carried out on a respondent group of 20 students. Data from the eye-tracking has been analyzed in order to conclude on the cybersecurity literacy among the respondents.

For the purpose of this analysis, the following resources have been used: Open DNS from SIE Europe:https://www.sie-europe.net/.UCL'sNeuroLab: https://www.ucviden.dk/en/projects/neurolab-ucl, DKCERT:www.cert.dk/ phishingkit and various sources on Twitter.

2 Technical analysis

The technical analysis focuses on spear-phishing and has been limited to attack vectors used by groups such as Silent Librarian: DNS look-a-likes, phishing emails and web pages imitating the actual library’s login page. To analyse whether a phishing kit has been active during this period, the registered IT infrastructure was set as a reference point, i.e. when a certificate is registered, when a domain is created and when it is first registered in the sensor networks used in this analysis.

The method of analysis itself can be described as exploratory, as it starts by analysing several specific phishing attacks to uncover the infrastructure used. This information is then compared with other available information, i.e. forensic information on i.e. Twitter, such as @Teamdreier, @andsyn1, @Peterkruse, etc, and so the search goes on.

In principle, the following steps were used in this method:

1. A passive DNS database account was used to analyse whether attackers are using phishing kits with library information. One account was linked to SIE Europe: https: //www.sieeurope.net/ , which is affiliated with several Danish institutions.
2. By using information from multiple phishing emails, it was possible to get a Fully Qualified Domain Name (FQDN) and identify the IP address and IP addresses over time. These included ezlogin.info and IP address 185.51.203.22.
3. This information made it possible to identify the name servers and previous name servers.
4. The use of Open Source Intelligence Tools such as Maltego: https://www.maltego.com/ and certificates in Certstream: https://certstream.calidog.io/ made it possible to view new certificates being published.
5. It is assumed that the group copies Top Level Domains and it has been established that the libraries installed on the aforementioned ".info" were also installed on the ".tk"”and ".cf" domains.
6. By using tools like https://urlscan.io/, one can do a search for the information found in the previous steps and use screenshots to verify if the site used the same phishing kit or variations, such as the phishing campaign used by the phishing domain libary.unt.edu.servicedesk.me/, which tried to trick users into changing their password.

With passive DNS as the focal point, 604 records or Indicators of Compromise (IOC) were identified across 24 Top Level Domain targeting HEI across EU, US and Australia activated since 2015.

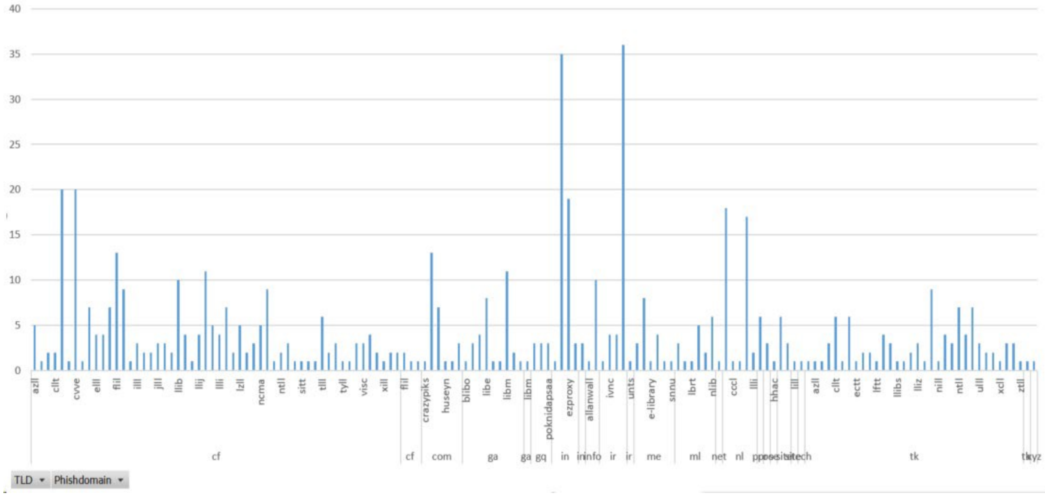
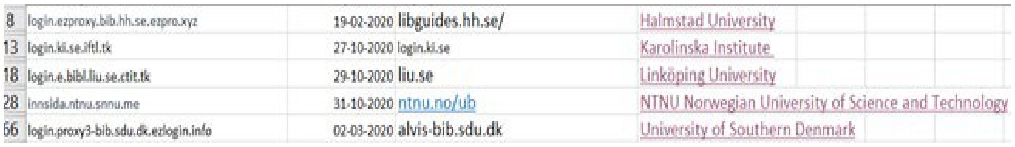


Table 1: Pivot of IOC/phishingsite identified. In the bottom Top Level Domain(TLD), for each TLP the used phishdomain and the total number of IOC for this domain until end of 2020.

In this study we will limit us self to attacks using phishingkits from 1st of January 2020 to 23st of September 2021. In this period, we can see that the actor used five top-level domains: .me, .tk, .cf, .info, .ga and .xyz. Eight of these domains were active in 2020/1: itlt.tk, itlib.me, iftl.tk, ezlogin.info, ezpro.xyz, mosc.me, liblog.info and ersta.me

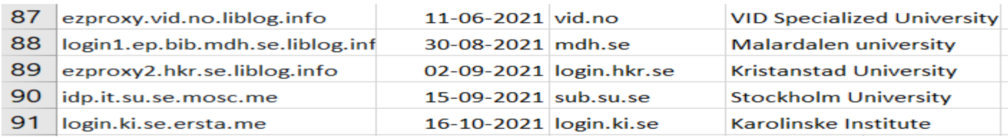
To identify and calculate the risk of an attack we analyze IOC for HEI for a region because the total number of HEI in the world or EU is uncertain. In the Nordic region there is 70 HEI in 2020/1. This study found attacks on Norwegian NTNU, Danish SDU and three Swedish institutions: Halmstad, Linköping University and the Karolinska Institute. Linköbing was hit 2 times in 2020. Karoliske was 1 one time in 2020 and again in 2021. A total of 11 attack of 70 HEI on nordic HEI.

Table 2: The 2020 IOC:



8	login.ezproxy.bib.hh.se.ezpro.xyz	19-02-2020	libguides.hh.se/	Halmstad University
13	login.ki.se.iftl.tk	27-10-2020	login.ki.se	Karolinska Institute
18	login.e.bibl.liu.se.ctit.tk	29-10-2020	liu.se	Linköping University
28	innsida.ntnu.snnu.me	31-10-2020	ntnu.no/ub	NTNU Norwegian University of Science and Technology
66	login.proxy3-bib.sdu.dk.ezlogin.info	02-03-2020	alvis-bib.sdu.dk	University of Southern Denmark

2021 IOC



87	ezproxy.vid.no.liblog.info	11-06-2021	vid.no	VID Specialized University
88	login1.ep.bib.mdh.se.liblog.inf	30-08-2021	mdh.se	Malardalen university
89	ezproxy2.hkr.se.liblog.info	02-09-2021	login.hkr.se	Kristanstad University
90	idp.it.su.se.mosc.me	15-09-2021	sub.su.se	Stockholm University
91	login.ki.se.ersta.me	16-10-2021	login.ki.se	Karolinske Institute

First column phishingsite, date of attack, off. URL, Educational Institution

A semantic view of the first column of Table 2 shows that the attacker reuses the top-level domain from attacks on other educational institutions, where the procedure is the same in terms of building domains. The lower level uses semantics identical to the official domain.

The actor's signature for creating domains uses the following formula:

[genericlogin][specificservice][institution][phishingdomain][topleveldomain]

As the last part of the technical assessment, a survey was conducted to calculate how many spearphishing was sent from attackdomain. The survey was send to all HEI that was victims of the attack. Only three responded and the survey was not conclusive, but estimate was given from 0 to 1000 spear-phishingmail was received from the attacker within the first 14 days after the certificate was published. 1-12 users has positively put in their credentials on the phishingsites.

In summary, with over 600 phishingdomain active since 2015 we can identify the same pattern and reuse of infrastructure, of the same attacker. 11 attacks on the Nordic HEI makes it a likelihood of 15% to be the victim of this attacker in the Nordic. 2 HEI was attacked twice.

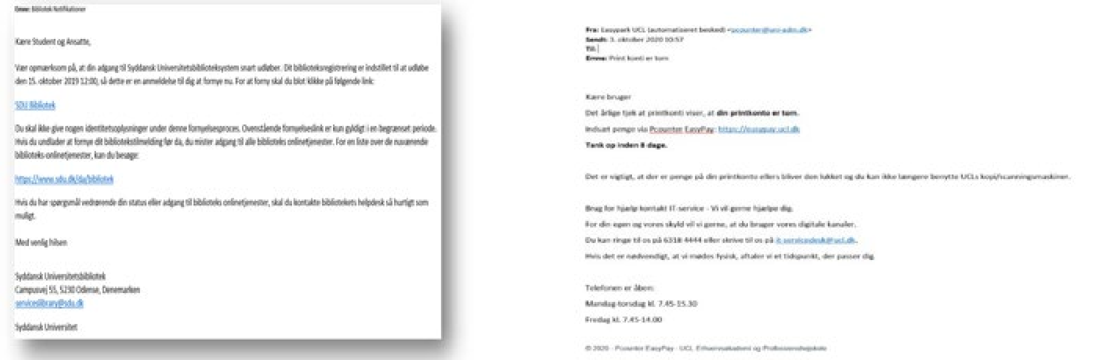
3 Comparable study of user vulnerability

Because an attack seem likely and can be repeated it if of interest to look into how vulnerable endusers are to this specific attack and try to train them. Two studies have been conducted to investigate how vulnerable users are to this type of attack. This study used the DKCERT's phishing service: https://www.cert.dk/da/tjenester/awareness. This is a phishing kit used for training purposes by several Danish educational institutions, where one can run awareness initiatives using different templates.

This study analysed data from two comparable awareness campaigns: SDU in 2019 and UCL in 2020. Both groups were given the same information before campaigns and the users had not received any previous training at the HEI.

Staff and students were briefed on the upcoming campaign using general IT security information, which was formulated as rule-based training information on being alert to email senders and examining links. This information was also published on Facebook, the students learning platform and the staff intranet prior to the awareness campaigns. The emails were sent out in the beginning of October 2019 and 2020 respectively, and the campaign lasted for two weeks. The emails were all sent from the same sender email, and the study registered if the email was delivered, opened, the device used and whether the user clicked on the link.

At SDU, the awareness campaign was carried out for all 35,714 people, consisting of 5,250 employees and 30,464 students. At UCL, the campaign was carried out for a group of 1,137 students. Both respondent groups received an email template used in one of the actor's attacks. SDU received a copy of the attack carried out on the University of Copenhagen and UCL received a copy of a printing account phishing kit.



Emne: Bibliotek Notifikationer

Kære Student og Ansatte,

Vær opmærksom på, at din adgang til Syddansk Universitetsbibliotekssystem snart udløber. Dit biblioteksregistrering er indstillet til at udløbe den 15. oktober 2019 12:00, så dette er en anmeldelse til dig at forny nu. For at forny skal du blot klikke på følgende link:

SDU Bibliotek

Du skal ikke give nogen identitetsoplysninger under denne fornyelsesproces. Ovenstående fornyelseslink er kun gyldigt i en begrænset periode. Hvis du undlader at forny dit bibliotekstilmelding før da, du mister adgang til alle biblioteks onlinetjenester. For en liste over de nuværende biblioteks onlinetjenester, kan du besøge:

https://www.sdu.dk/da/bibliotek

Hvis du har spørgsmål vedrørende din status eller adgang til biblioteks onlinetjenester, skal du kontakte bibliotekets helpdesk så hurtigt som muligt.

Med venlig hilsen

Syddansk Universitetsbibliotek
Campusvej 55, 5230 Odense, Denemarken
servicelibrary@sdu.dk

Syddansk Universitet

Fra: Easypark UCL (automatiseret besked) <[illegible]>
Sendt: 3. oktober 2020 10:57
Til:
Emne: Print konti er tom

Kære bruger

Det årlige tjek af printkonti viser, at **din printkonto er tom.**

Indsæt penge via Pcounter EasyPay: https://easypay.ucl.dk

Tank op inden 8 dage.

Det er vigtigt, at der er penge på din printkonto ellers bliver den lukket og du kan ikke længere benytte UCLs kopi/scanningsmaskiner.

Brug for hjælp kontakt IT-service - Vi vil gerne hjælpe dig.

For din egen og vores skyld vil vi gerne, at du bruger vores digitale kanaler.

Du kan ringe til os på 6318 4444 eller skrive til os på it.servicedesk@ucl.dk.

Hvis det er nødvendigt, at vi mødes fysisk, aftaler vi et tidspunkt, der passer dig.

Telefonen er åben:

Mandag-torsdag kl. 7.45-15.30

Fredag kl. 7.45-14.00

© 2020 · Pcounter EasyPay · UCL Erhvervsakademi og Professionshøjskole

Figure 1: Emails used in SDU’s awareness training in 2019 and in UCL’s in 2020.

Figure 1 shows the used mailtemplates. The email broadcast to SDU experienced some technical problems that caused the broadcast to be divided into three phases. Phase 1, where DKCERT estimated that 33% of the 11,710 emails included contained such great uncertainty that the group was taken out of the study. Phase 2 consisted of 18,754 emails sent to students, of which 8,203 were opened. 5,811 of these were clicked on, which corresponds to 31%. Phase 3 consisted of emails sent to employees only. A total of 5,270 emails were sent, of which 3,332 were opened. 1579 of these were clicked on, which corresponds to 30%. Thus, there is a 30% risk that this attack would be successful.

The analysis has examined variations within each main area. SDU's administrative area and the five faculties. The main area with only administrative staff had the lowest risk of 20%. The highest overall risk was found in employees and students at the Faculty of Health Sciences. They received a total of 2,247 emails, of which 1,307 were opened. 831 of these were clicked on, which corresponds to 37%.

The respondent group at UCL consisted of students in commercial and technological degree programs. They received a total of 1,137 emails, of which 185 were opened. 91 of these were clicked on, which corresponds to 49%. The user vulnerability to this type of attack is thus very large, with a variation of 20–49%.

When the two awareness campaigns were completed, two student groups were selected to complete a questionnaire where they were asked if they would click on three different emails, where the library email was one of the examples. The SDU respondent group consisted of 20 students on the Master of Science in Engineering program (Health and Welfare Technology). The UCL group consisted of randomly selected students from commercial and technological bachelor's degree programs. In both questionnaire a total of 8 out of 20 said they would click on the link, which corresponds to 40%.

The students' ability to transfer skills from the rule-based IT security information received before and during the awareness training until after the training has thus been very limited. The staffs' ability to transfer skills seems better for administrative compared to academic staff.

The IT device on which the respondent read the email could be extracted from the awareness training for those who clicked on the link. The distribution of the 5,811 SDU students and 91 UCL students showed a relatively low proportion of mobile operating systems (19% for SDU and 45% for UCL) indicates that students are mainly using their computers (Mac and Windows) when reading emails from their educational institution. This information is a bit surprising because students normally use their smartphone to communicate with, but mail from these two university is mainly checked on computers. This is useful information in order to understand how the respondents are supported in reading mail. Mail on e.g iOS displayname is the only information shown to the user, whereas on Windows the enduser has the option to read both displayname and real mailaddress in the mailclient.

The questionnaire nor the survey reveal why the spear-phishing from Silent Librarian is so succesfull. To investigate the high risk of this attack to endusers in HEI, an eye-tracking study was conducted. According to the reading of the spearphising awernnes training, we chose to test this on a computer in order to analyse why users are lured by mails from Silent Librarian.

3 Eye tracking study

Eye-tracking technologies are used to measure a person eye movement and can determine what this person is really looking for and how much attention they pay to different component as cybersecurity indicators. Use of eye tracking in cybersecurity have become evident as more research is done to understand the users interaction with phishingsite. Although research within spearphishing is very limited with only 8 researchpapers [4]. This study would like to add an exploratory study to current research to understand the specific attackvector used by Silent Librarian and compare this with other spear-phishingmails.

This study was a qualitative study which was conducted two days after the broadcast of the aforementioned awareness training. It was conducted on UCL's campus in Odense, Denmark on Friday the 9th October 2020.

In this study random chosen students was recruited. 21 students accepted and were placed in front of a computer connected to eye-tracking equipment and asked to answer a series of questions as well as read 3 emails, with the objective of measuring the respondents visual focus when reading emails and whether these focus areas related to aspects concerning IT security. The first student was used to verify the setup and questions. 20 students are included in the study (8 female, age range 19-27, students within commercial and technological degree programs). The study used iMotions software (imotions.com) and no technological problems were identified during the study of the 20 students. After the eye-traking study the student answered question about general cybersecurity to verify if the respondents had general cybersecurity knowledge. On a scale from 1-5 the respondents answered evenly distributed scores on all five questions.

From previous research in phishing it is known that users react to the presence of misspellings, the use of urgency, the mention of financial information and threatening language. All this indicators was created in the three spear- phishing mails in order to compare their trustworthyness to Silent Library mail.

Heat maps were generated to measure the most and least viewed areas, and a gaze plot was then generated for each respondent to uncover reading patterns. Last but not least, the emails contained marked areas where essential IT security information had been placed to see if the respondents read it and if so, how long for. Heat maps show an overall image of areas viewed by respondents. The scale goes from green to red, where red indicates the areas viewed the most by the respondents when presented with the email during the test.

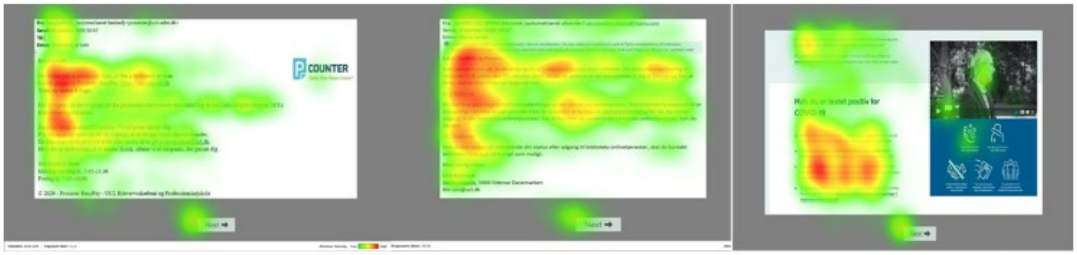
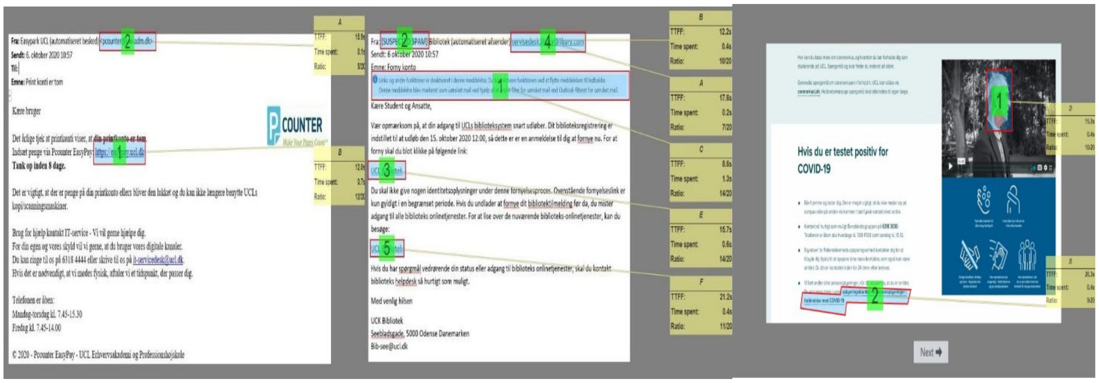


Figure 2: Heat maps average across all respondents for the three emails used in the awareness training. On the left the heat map forthe printing account (financial information), the second is UCL library account/Silent Library and third COVID-19 (threatening language).

The screenshots from Figure 2 show that participants have read to the text area. The entire text of the email has been read, and the heatmap also shows that participants have paid some attention to IT-security information as the sender "pcounter @ uni adm.dk" (top of screenshot) or the weblink (midle of screenshot). All three heatmaps shows that respondents overall spend longer time on securityinformation than expected by chance. This gives us an understanding of the overall reading of phishingmails.We will now analyse the reading patterns of the respondents using gaze plots and Area of Interest (AOI) to come closer to how the reading the three emails are read.AOI were mapped onto the mail post hoc in iMotion and shows an average time of how long respondents have viewed a particular area. These areas were non-overlapping and focused on IT security information. AOI for real mailadress and phishinglink was area normalized for the three mails.



Fra: Easypark UCL (automatiseret besked) <pcounter@uniadm.dk>
Sendt: 6. oktober 2020 10:57
Til:
Emne: Print konti er tom

Kære bruger

Det årlige tjek af printkonti viser, at **din printkonto er tom.**
Indsæt penge via Pcounter EasyPay https://easypay.ucl.dk
Tank op inden 8 dage.

Det er vigtigt, at der er penge på din printkonto ellers bliver den lukket og du kan ikke længere benytte UCLs kopi/scanningsmaskiner.

Brug for hjælp kontakt IT-service - Vi vil gerne hjælpe dig.
For din egen og vores skyld vil vi gerne, at du bruger vores digitale kanaler.
Du kan ringe til os på 6318 4444 eller skrive til os på it-servicedesk@ucl.dk.
Hvis det er nødvendigt, at vi mødes fysisk, aftaler vi et tidspunkt, der passer dig.

Telefonen er åben:
Mandag-torsdag kl. 7.45-15.30
Fredag kl. 7.45-14.00

© 2020 - Pcounter EasyPay - UCL Erhvervsakademi og Professionshøjskole

Fra: [SUSPECTED SPAM] Bibliotek (automatiseret afsender) servisedesk@library.com
Sendt: 6 oktober 2020 10:57
Emne: Forny konto

Links og andre funktioner er deaktiveret i denne meddelelse. Du kan aktivere funktionen ved at flytte meddelelsen til Indbakke.
Denne meddelelse blev markeret som uønsket mail ved hjælp af et filter for uønsket mail end Outlook-filteret for uønsket mail.

Kære Student og Ansatte,

Vær opmærksom på, at din adgang til UCLs biblioteksystem snart udløber. Dit biblioteksregistrering er indstillet til at udløb den 15. oktober 2020 12:00, så dette er er en anmeldelse til dig at fornye nu. For at forny skal du blot klikke på følgende link:

UCL Bibliotek

Du skal ikke give nogen identitetsoplysninger under denne fornyelsesproces. Ovenstående fornyelseslink er kun gyldigt i en begrænset periode. Hvis du undlader at fornye dit bibliotektilmelding før da, du mister adgang til alle biblioteks onlinetjenester. For at lise over de nuværende biblioteks-onlinetjenester, kan du besøge:

UCL Bibliotek

Hvis du har spørgmål vedrørende din status eller adgang til biblioteks onlinetjenester, skal du kontakt biblioteks helpdesk så hurtigt som muligt.

Med venlig hilsen

UCK Bibliotek
Seebladsgade, 5000 Odense Danemarken
Bib-see@ucl.dk

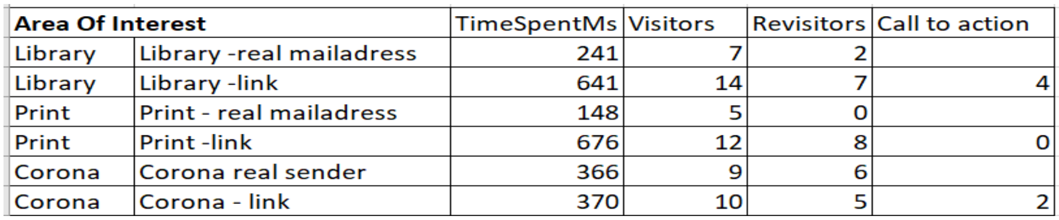
Hvis du er testet positiv for COVID-19

Figure 3: AOI for three spear-phishing emails. The red boxes mark important IT security info.

TTFF	The Time to First Fixation (TTFF) indicates the amount of time that it takes a respondent (or all respondents on average) to look at a specific AOI.
Time spent	Time spent or dwell time quantifies the amount of time that respondents have spent looking at a particular AOI.
Ratio	The ratio provides information about how many of your respondents actually guided their gaze towards a specific AOI.

Concepts and terms of eye tracking. For more information go to https://imotions.com/blog/10-terms-metrics-eye-tracking/

First we can see the reading pattern (TTFF) which normally is from the top and down. In the three mails respondent first fix on the link (call to action) before reading the sender information. From a cyberliteracy point of view this is problematic because the respondents does not know who is the real sender. With a ratio of only between 5-10 of 20 the reading indicates that the respondents do not perceive the sender to be important. However the "Call to action" link shows a different response, where 9-14 out of 20 respondents looked at this AOI.



Area Of Interest		TimeSpentMs	Visitors	Revisitors	Call to action
Library	Library -real mailadress	241	7	2	
Library	Library -link	641	14	7	4
Print	Print - real mailadress	148	5	0	
Print	Print -link	676	12	8	0
Corona	Corona real sender	366	9	6	
Corona	Corona - link	370	10	5	2

Table 3: AOI for each phishingmail: For each spear-phishing two AOI is measured. Realmailadress and link. For each mean time spent/ dwell time in milliseconds, Vistors: How many of the 20 respondents that visit the specific AOI, Revisitors , how many revisited the AOI and how many was called to action. Called to action is established if the respondent during the session clicked on the phishingmail. This was registered as 1, if the responded did not click, it was registered as 0.

The study shows in Table 3 that respondents generally spend more time viewing phishing indicator than one expect by chance. Fixation time was also recorded as an important metrix denoting a period where the eyes are locked towards an object, in this case the area around the link. Data from Fixationtime was clouded therefore it is not possible to calculate mean and standarddeviation on this metrix. Even if we do not have fixationtime we can correlate between timespent, visitor, revisitor and call to action. It is evident that SilentLibrarian outperform the two other spear-phishing mail in regards to effectiveness: 4 clicked on the librarylink, 0 clicked on "printmail".

In accordance with other study, phishingmail with financial information (Print) were associated with least frequent number of fixations and the least amount of overall timespent [5]. AOI in this mail also have the least visitor and revisit. Study has shown that both financial and threatening language will alert the reader and we can see that the respondents use less time to rate the overall trustworthiness and do not click on links.

This is not the case with a phishingmail with the text of renewal of your library account, therefore we can assume that this lure the enduser to click on the link. Further study and analyse is although necessary to identify correlation between different metrix, and the small sample of respondents call for more data to be conclusive.

4 Discussion

With use of Open Source Intelligent Tools it was possible to show the attackers modus operadi and attacks in 2020. The used attackvector of Silent Librarian change to some degree over time to avoid technical solutions like spamfilter and firewall. Therefore we see the use of different Top Level Domain, but still use the same procedure: Reuse of infrastructure and certificate, copy of phishingkit and loginpage from HEI. Therefore, these attacks also can be foreseen by monitoring preused certificate and internet domain. Doing so will allow HEI to predicted and warn other HEI before next attack.

This could be important because the attack from Silent Librarian is highly effective and will most likely lead to security breach. In this study we have two comparable studies consisting of 36,851 respondents from two educational institutions, show that without prior training, the Silent Librarian spear-phishing attack will lure 20 to 49% of all users.

The eye tracking study showed that Silent Librarian high succesrate can be explained by their mailtemplate. Although the study show that respondents glance more frequently at the IT-security indicators within the spear- phishingmail than that could be expected by chance, Slient Librarian use a mailtemplate that lure the endusers.

Data from the eye tracking reveals that it could be becuasue of the lack of adequate cyberlitteracy. The readingpattern reveals respondents fail to extract and conclude on securityinformation. Instead, the respondents seems to make an overall judgement of the trustworthiness of spear-phishing. With respondents, limited cyber literacy it is likely that Silent Librarian could still be successful without the internetdomainconfusion. Respondents does not seems to fixate at the internetadress.

This study has demonstrated that eye-tracking can be used to identify what endusers actually is looking for, how spear-phishing can lure endusers and what information is processed when looking at mail.

Although the complex interaction between human and computer need more study to fully understand spear- phishing, this study assumes to have mapped this specific attacker and what makes it so successful.

5 Reference

[1] Panum, T. K., Hageman, K., Hansen, R. R., & Pedersen, J. M. (2020). Towards Adversarial Phishing Detection. I 13th USENIX Workshop on Cyber Security Experimentation and Test USENIX - The Advanced Computing Systems

[2] https://uniavisen.dk/en/the-university-of-copenhagen-beefs-up-cybersecurity-in-response-to-hackers/

[3] https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamicrevolutionary

[4] Avisha Das , Shahryar Baki (2020)"A Comprehensive Reexamination of Phishing, IEEE Communications Surveys & Tutorials (Volume: 22, Issue: 1

[5] McAlaney and Hills (2020)"Understanding Phishing Email processing and Perceived Trustworthiness Through Eye Tracking", Frontiers in Psychology, Vol. 11, article 1756