

Mapping of a spear-phishing attack on HEI and IT security literacy among students

The image shows a screenshot of an email interface with several elements highlighted in red boxes and numbered 1 through 5. To the right of the email content is a table of performance metrics for different parts of the email.

1 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 Outlook-filtre. For uønsket mail ænd Outlook-filtret for uønsket mail.

2 [SUSPEKT SPAM] Bibliotek [automatiseret afsender]

3 UCL Bibliotek

4 service@uclbibliotek@ucl.dk

5 UCL Bibliotek

	B
TTFF:	12.2s
Time spent:	0.4s
Ratio:	10/20

	A
TTFF:	17.6s
Time spent:	0.2s
Ratio:	7/20

	C
TTFF:	8.6s
Time spent:	1.3s
Ratio:	14/20

	E
TTFF:	15.7s
Time spent:	0.6s
Ratio:	14/20

	F
TTFF:	21.2s
Time spent:	0.4s
Ratio:	11/20

Kurt Gammelgaard Nielsen, CIO, University College Lillebaelt

Lesson learned

1. We can use open source intelligence tools to uncover attack vectors/infrastructure
2. Mapping a specific attacker revealed that 8 % of HEI in a region has been attacked.
3. Large scale user vulnerability assessment can be used to evaluate how successful an attack will be. This study consisting of 36,851 respondents from two educational institutions showed that a concrete spear-phishing attack will lure 20 to 49% of users.
4. Eye-tracking study can reveal security literacy among students. This 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.

Spear-phishing attack from Silent Librarian



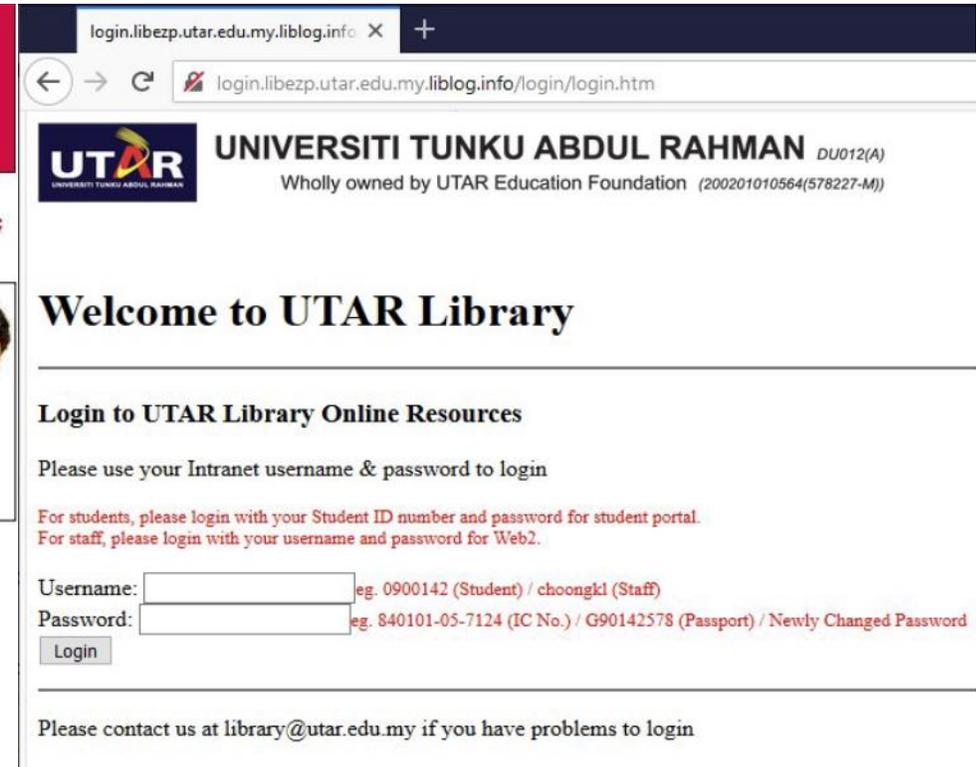
WANTED BY THE FBI

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

CONSPIRACY TO COMMIT COMPUTER INTRUSIONS; CONSPIRACY TO COMMIT WIRE FRAUD; COMPUTER FRAUD - UNAUTHORIZED ACCESS FOR PRIVATE FINANCIAL GAIN; WIRE FRAUD; AGGRAVATED IDENTITY THEFT

Gholamreza Rafatnejad
Ehsan Mohammadi
Seyed Ali Mirkarimi
Abdollah Karima
Mostafa Sadeghi

Sajjad Tahmasebi
Mohammed Reza Sabahi
Roozbeh Sabahi
Abuzar Gohari Moqadam



login.libezp.utar.edu.my.liblog.info X +

login.libezp.utar.edu.my.liblog.info/login/login.htm

UTAR UNIVERSITI TUNKU ABDUL RAHMAN DU012(A)
Wholly owned by UTAR Education Foundation (200201010564(578227-M))

Welcome to UTAR Library

Login to UTAR Library Online Resources

Please use your Intranet username & password to login

For students, please login with your Student ID number and password for student portal.
For staff, please login with your username and password for Web2.

Username: eg. 0900142 (Student) / choongkl (Staff)
Password: eg. 840101-05-7124 (IC No.) / G90142578 (Passport) / Newly Changed Password

Login

Please contact us at library@utar.edu.my if you have problems to login

IP: 185.51.201.112. Timestamp: 2021-06-07

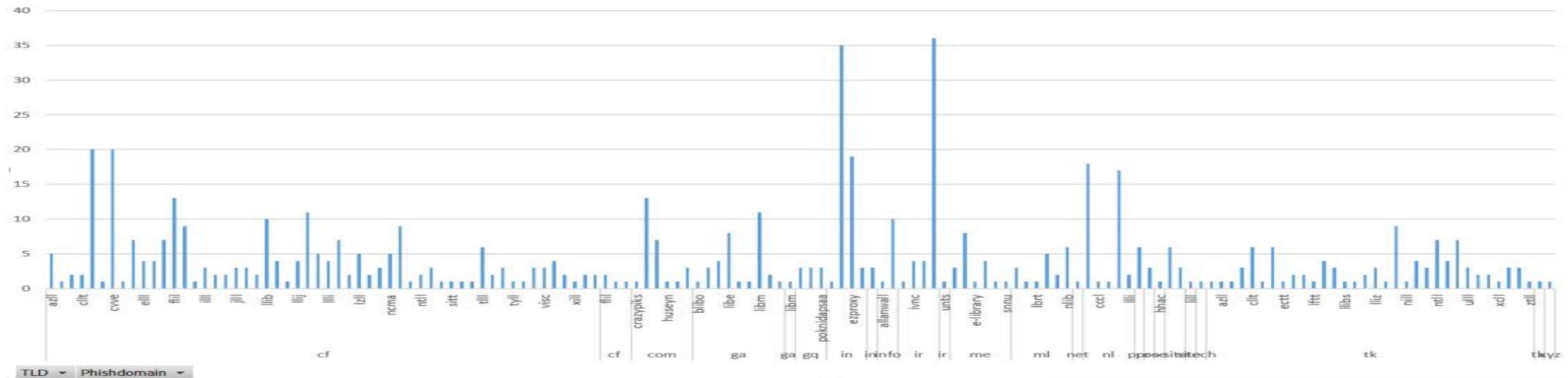
1. Open Source Intelligens Tools

We used passive DNS SIE Europe: <https://www.sie-europe.net/>

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.

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.

Distribution of phishing site over Top Level Domain



70 HEI in the Nordic region: 6 IOC in 2020 = 8% risk of attack

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
56	login.proxy3-bib.sdu.dk.ezlogin.info	02-03-2020	alvis-bib.sdu.dk	University of Southern Denmark

2 Large scale user vulnerability assessment

- User vulnerability assessment on the specific spear-phishing attacks used in two comparable studies consisting of 36,851 respondents from two educational institutions: SDU in 2019 and UCL in 2020.
- This study used the DKCERT's phishing service: <https://www.cert.dk/da/tjenester/awareness>.
- Both groups were given the same information before campaigns.

Leasson learned

Large variation within usergroups: SDU's 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 - 20–49%.

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 been very limited.

The staffs' ability to transfer skills seems better for administrative compared to academic staff.

3. Eye-tracking study

- Conducted on UCL's campus in Odense, Denmark, the 9th October 2020.
- In this study 21 random chosen students were placed in front of a computer connected to eye-tracking equipment (iMotion) 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.

Areas Of Interest (AOI)

The screenshot shows two email messages side-by-side. The left message is from 'EasyPark UCL' and the right is from 'Bibliotek'. Various elements are highlighted with red boxes and numbered 1 through 5. On the right side of the screenshot, there is a table with performance metrics for each AOI.

AOI	TTFF	Time spent	Ratio
2	15.9s	2.1s	520
4	12.2s	0.4s	10/20
1	17.6s	0.2s	7/20
3	8.6s	1.3s	14/20
5	15.7s	0.6s	14/20
6	21.2s	0.4s	11/20

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

Reading of a spear-phishing mail/Security literacy

Stimulus: email ucl bib

Fra: [SUSPECTED SPAM] Bibliotek (automatiseret afsender) servisedesk.library@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 andet 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 [forny](#) 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 [forny](#) 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 [spørgsmål](#) vedrørende din status eller adgang til biblioteks onlinetjenester, skal du kontakte biblioteks [helpdesk](#) så hurtigt som muligt.

Med venlig hilsen

UCK Bibliotek
[Seebladsgade](#), 5000 Odense Danemarken
Bib-see@ucl.dk

Next →

RESPONDENT ANNOTATIONS

Create annotations in the Annotations menu

00:06 00:05 00:04 00:03 00:02 00:01 00:00 00:01 00:02 00:03 00:04 00:05 00:06 00:07

Respondent: Respond2 Stimulus: email ucl bib 00:00:00:000

Conclusion

- Silent Librarian – have gone phishing again!
- We can detect Silent Librarian using passive DNS and predict new attack because of they reuse infrastructure, certificate and method (phishkit).
- The user vulnerability assessment shows that endusers are lured by this spear-phishing. Attack can therefore have high impact on institutions.
- The study shows that respondents generally spend more time viewing phishing indicators than one expects by chance, but are still lured.
- Endusers seem 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 library spear-phishing mail.
- The lack of security literacy among students, suggests that more security information in mailheaders will not protect HEI