Ransomware – what? why?

Tech talks

EAL

March 30th 2017

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

Morten Bo Nielsen – mon@eal.dk

I have added links on the slides for your further reading

Ransomware 101

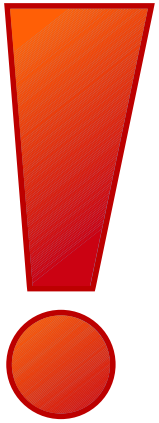
1) Infect machine
2) Encrypt data
3) Demand ransom to give up key

Bonus, because it is cool

- pay ”fine”
  not ransom
- fake!

http://blog.trendmicro.com/mobile-ransomware-fast-growing-yet-unknown-threat/

How do they do it?



- links
- attachments
- embedded images and/or images

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
http://www.esecurityplanet.com/malware/prevent-ransomware-attack.html

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

It sounds so easy!

check out their ad. It's fairly chilling.

Tags: mercy, Philadelphia ransomware

from "ransomware for dummier (brian krebs)"
https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/

But my antivirus...?

What do you think it actually does?

(spoiler: it works mainly with signatures)

97% of malware is unique to a specific endpoint

antivirus doesn't work

https://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

But I just won the lottery!

LOTTO NETHERLANDS
Lotto Winner of 1,500,000.00 Euros
Ref. Number: NL/BC5765268/WW18
Coupon Number: NL/841343/WOT

ELECTRONIC MAIL AWARD WINNING NOTIFICATION
CONGRATULATIONS!!!

We are pleased to inform you of the announcement today of winners of the LOTTO NETHERLANDS held on 15TH March,2017.Your Company or your personal e-mail address is attached to winning number 20-02-2005-02MSW, with serial number S/N-00168 drew the lucky numbers 877-13-865-37-10-81, and consequently won in the first lottery category.

You have therefore been approved for a lump sum pay out of One Million Five Hundred Thousand EUROS (1,500,000.00) in cash credited to file REF NO: NL/BC5765268/WW17 and Coupon NL/841343/WOP.

All participants were selected through our Microsoft computer ballot system drawn form 21,000 names, 3,000 names from each continent, as part of International "E-MAIL" Promotions Program which is conducted once in every four years for our prominent MS WORD user all over the world and for the continues use of E-mail.

Your fund has been deposited in an escrow account with our affiliate Bank here in NETHERLAND, and insured with your REF NO: NL/BC5765268/WW17 and your E-mail address.

You are to keep your ref. number and coupon number from the public, until you have been processed and your money remitted to your personal account. We hope with your prize, you will be happy to promote the use of E-mail and the use of MS WORD.

To claim your winning prize, you must first contact
remittance of your prize money to you. Your assigne

MR.JAMES KELLER
LAAN VAN HOORNWIJCK 56
2289 DG RIJSWIJK
THE NETHERLANDS
TEL: 0031-687-127-704
Email:claimsdirector4@aol.com
www.lotto.nl

All response should be sent to:claimsdirector4@aol

Sincerely,
Mrs. Maria Anderson
International Relation officer

Hello,

Your account has been flagged due to security problem.

For more information and details regarding the security problem please follow the instructions from the link below.

https://www.paypal.co.uk/?lng=en/GB_login

Best Regards,
PayPal
This is an automated email generated by our internal systems.
Copyright © 2017 PayPal, All rights reserved.

no you did not win the lottery
no paypal does not use url shorteners
no your email was not selected to win
no you don't have very rich unknown relatives
no you should not help someone exfiltrate money from an African country

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

Bonus: Is this legit?

Questionnaire survey of English-taught Academy Profession (AP) full degree programmes

Dear Morten Bo Nielsen

The Danish Agency for Higher Education under the Danish Ministry of Higher Education and Science has instructed The Danish Evaluation Institute, EVA, to conduct an investigation of English-taught Academy Profession (AP) full degree programmes. As an important element of the project, EVA is conducting a questionnaire survey of all teachers on English-taught AP full degree programmes. We have been informed that you teach on one or more of these programmes. At this link https://www.inquisiteasp.dk/cgi-bin /qwebcorporate.dll?idx=J7T773&l=english&rk=Q4JQG3 you will find the questionnaire and instructions on how to complete it.

We hope that you will set aside 10 - 15 minutes to complete the questionnaire, as the results represent important documentation for the project.

Questions
If you have any questions on how to complete the questionnaire, please contact Methodology Assistant Laura Marie Kalmark, lmk@eva.dk, telephone +45 3525 5667.

The aim of the project
The aim of the project is to analyse the opportunities and challenges of conducting educational programmes in English. The project will examine the actual teaching situation, the interaction between students and teachers as well as the benefits for students.

Read more about the project on our web page www.eva.dk.

We thank you in advance for completing the questionnaire.

Kind regards

Dina Celia Madsen
Project Manager

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

But I trust my browser.

Go here to be cured

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=edge
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=firefox
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=chrome

(and these are the known ones...)

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

Does the IT dept. fail?

1) Culture and politics
2) Security is hard
3) Technology

Security culture in IT?

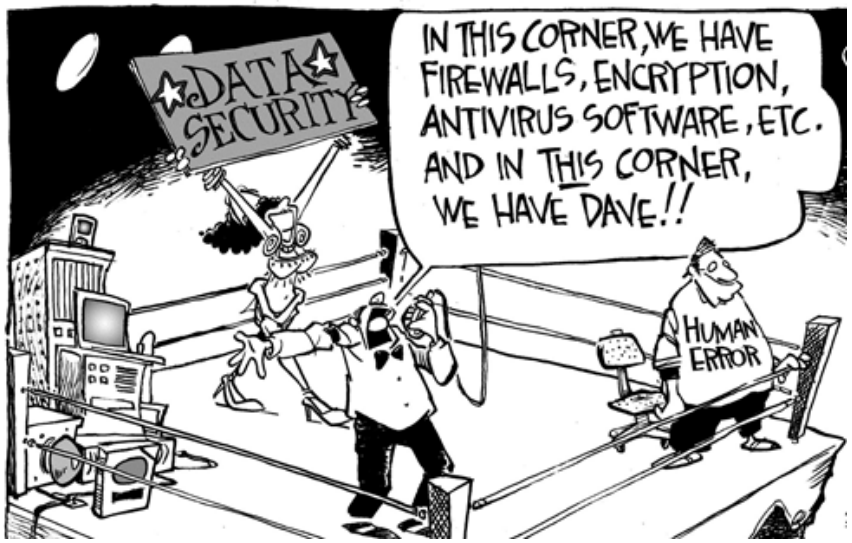
What to do? (IT dept.)

- NG firewals can help
- Security awareness of users
- Proper permissions handling
- Monitor and limit read/writes
- Have an efficient restore process
- and all the other stuff they do every day

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

What to do? (users)

- Security awareness of users
  - don't click yes, yes, ok, next on security popups
  - read them
- Have an efficient restore process
  - does the company have this?
  - Do you at home?



(Dave wins)

and develop non-paranoid secure online habits

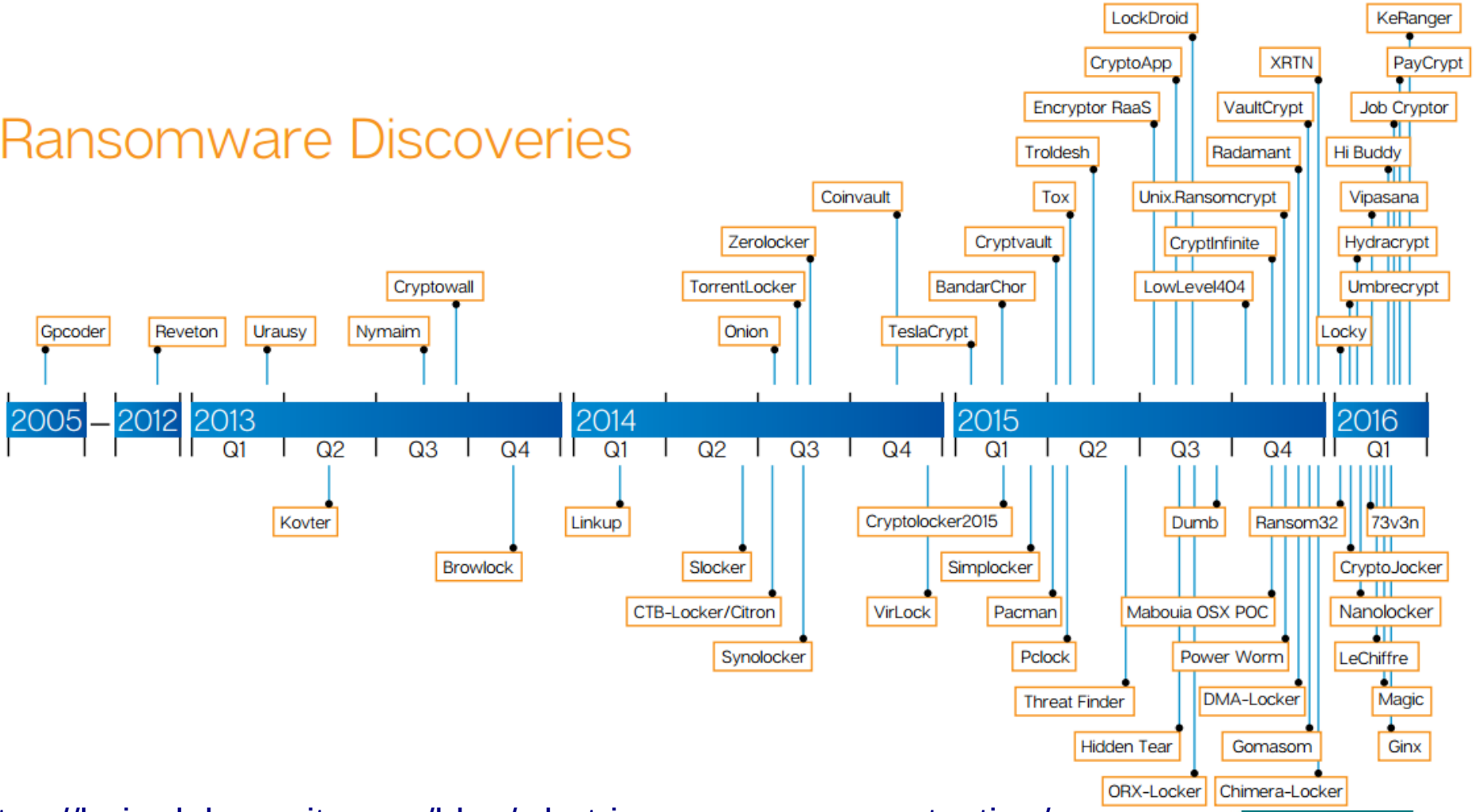
Can you restore your private data?

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

Credits & licences

- Content by Morten Bo Nielsen
  License: Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. (http://creativecommons.org/licenses/by-nc-sa/3.0/)
- EAL logo might be an issue, please check before you use it

Ransomware Discoveries



https://heimdalsecurity.com/blog/what-is-ransomware-protection/

LILLEBÆLT
ACADEMY OF PROFESSIONAL HIGHER EDUCATION

Forudsætningerne for succesfuldt ransomware angreb er:

- Brugere er vandt til at klikke ja til advarsler bare for at udføre deres arbejde.
- Vedhæftninger til emails er ment til at blive åbnet så derfor åbner folk dem.
- Antivirus som produkt er forældet i forhold til altid opdaterede vira.
- Backup er svært og ofte fejlagtigt udført.
- Rettighedsstyring til filer er svært og ofte fejlagtigt udført.
- Alle kan sende mails til alle uden omkostninger for afsender.
- En almindelig PC er blevet hurtig nok til at lave file encryption uden at det kan mærkes under brug.

https://www.version2.dk/artikel/derfor-ransomware-ting-2017-eller-naar-brugeren-venter-pakke-slaar-hjernen-antivirus

Morten Bo Nielsen – mon@eal.dk