[l01] history of cyber attacks

[l01_t02] case study

wim mees

introduction

learning objectives

- understand a real-world recent incident
- be able to discuss the proposed counter measures

case study

the organization

Figure 1: Maastricht university

the organization

Maastricht university

- publication organization with:
  - 4500 employees,
  - 18000 students,
  - 70000 alumni.
- IT infrastructure with:
  - diverse range of servers and workstations,
  - some (not all) managed by the university's central "*ICT Service Centre*" (ICTS),
  - others connected to the same network, yet managed by other entities (research labs, etc.),
  - some (not all) connected to the university's central Windows domain "UNIMAAS",
  - combination of desktops, laptops, and "*Virtual Desktop Infrastructure*" (VDI) virtual hosts accessed through thin clients and local browsers.

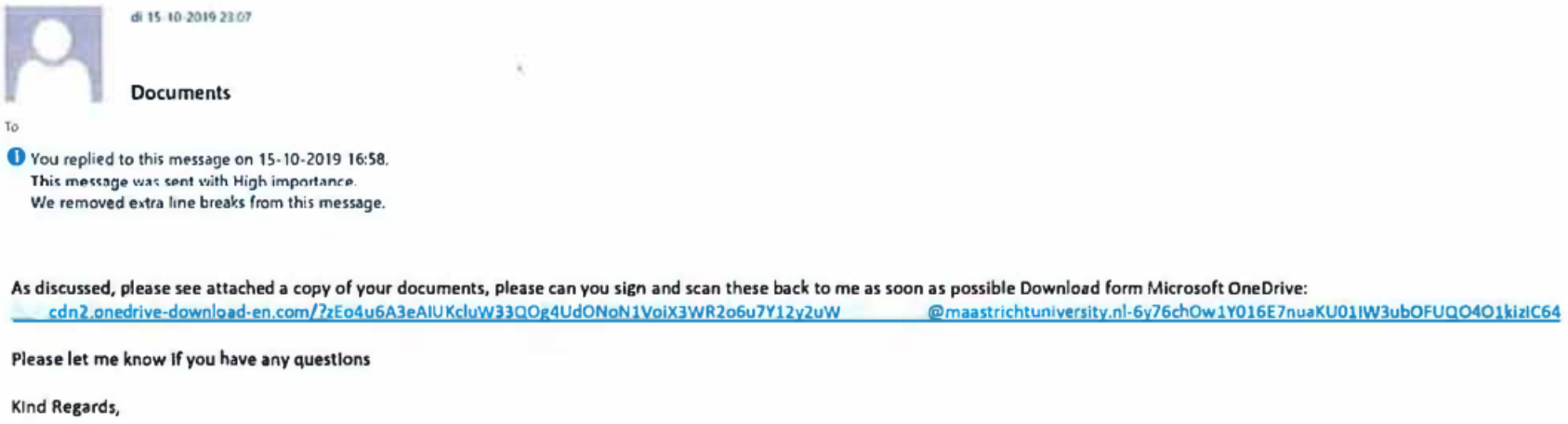
phishing campaign

Figure 2: sowing phase

phishing campaign

151406oct19

- *user1*@maastrichtuniversity.nl receives phishing email with subject "Documents"
- link in email points to Excel document on onedrive.com



di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
cdn2.onedrive-download-en.com/?zEo4u6A3eAIUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kizIC64

Please let me know if you have any questions

Kind Regards,

Figure 3: phishing email

phishing campaign

151455oct19

- *user1* opens the Excel document on workstation *ws1*
- the Excel document contains a macro that:
  - connects to a server "windows-en-us-update.com" with IP address 185.225.17.99
  - downloads a malware known as "SDBBot"
  - executes the malware on workstation *ws1*

phishing campaign

160907oct19

- *user2*@maastrichtuniversity.nl and 5 others receive phishing email with subject "CL meeting schedule.xls"
- link in email points to Excel document on dropbox-eu.com

Figure 4: phishing email

phishing campaign

161252oct19

- *user2* opens the Excel document on virtual desktop *vdi1*
- the Excel document contains a macro that:
  - connects to a server "windows-afx-update.com" with IP address 185.212.128.146
  - downloads the same malware and executes it

phishing campaign

result

- *ws1* and *vdi1* are infected with SDBBot:
  - registry key set to launch malware at startup
  - every 15' a connection is made to CnC-server
    with domainname drm-server13-login-microsoftonline.com
    and IP address 195.123.242.250

lateral movement

Figure 5: harvesting phase

lateral movement

161935oct19

- first remotely controlled manual activities on *vdi1*
- from SDBBot the tool “Meterpreter” is launched
- it is unclear what exactly the attacker does with this tool (due to unavailability of relevant forensic data)

lateral movement

171733oct19

- server *srv1* is compromised
  and is now running "Meterpreter"
- not certain how compromise was performed, however:
  - server was running Windows Server 2003 R2,
    with patch MS17-010 not installed
  - therefore server was vulnerable to EternalBlue,
    that gives access to local SYSTEM account

171740oct19

- server *srv2* gets compromised in same way as *srv1*

lateral movement

201900oct19

- server *srv3* is compromised,
  was running same OS as *srv1* and *srv2*,
  therefore presumably same exploit was used

201902oct19

- server *srv4* is compromised,
  was however not vulnerable to EternalBlue,
  therefore unclear how they got in

lateral movement

- attacker now has local SYSTEM account on 4 servers, and therefore is **local admin** on these servers

241138oct19

- attacker is active on *ws1* under regular user account *user1*:
  - uses PowerSploit, a set of PowerShell scripts used for pentesting
  - scans the host itself for vulnerabilities
  - scans the internal network

241517oct19

- attacker is active on *vdi1* under regular user account *user2*:
  - uses PingCastle to
  - (graphically) map ActiveDirectory (AD) structure of university
  - collect info on AD config to look for attack opportunities

prepare for the kill

Figure 6: preparing the final product

prepare for the kill

211134nov19

- attacker again active on *vdi1*
- at 13:06 he compromises *srv5* that was not fully patched,
  so EternalBlue may have been used again,
  and runs Meterpreter with local SYSTEM account
- at 13:19 the attacker logs on to *srvAD1*,
  this is one of the **AD domain controllers**,
  he is using the Administrator.UNIMAAS account,
  which has **full domain administrator** rights
- hypothesis on how the attacker got in:
  - Administrator.UNIMAAS had a user profile on *srv5*,
    so at some point this account was used to log on to *srv5*
  - the login credentials were extracted from memory on *srv5*

prepare for the kill

- attacker now has access to the most privileged account (Administrator.UNIMAAS)
  and controls the system with the highest access rights (the domain controller *srvAD1*)

191449dec19

- attacker uses a number of tools to prepare the final hit:
  - MeterPreter
  - Cobalt Strike
  - PingCastle
  - AdFind
- he is mapping hosts on the network
  and the processes and services they are running

ransom requested

Figure 7: bring in the profits

ransom requested

- attacker puts a tool called sage.exe on a few servers in C:\Users\Public\Music\
- it runs as a service Winsysstrinsag
- this tool is removed by McAfee AV on one server
- attacker removes McAfee AV from a few servers

231826dec19

- attacker uses sage.exe to launch the ransomware attack on all Windows servers that are part of UNIMAAS domain:
  - disable Windows Defender
  - distribute and launch the ransomware (in file swaqp.exe)
  - it runs as a service called psxexesvc

ransom requested

231852dec19

- result: 267 servers infected with ransomware
  that is rapidly encrypting all non-system files
- these servers include:
  - domain controllers
  - exchange servers
  - file servers
  - backup servers
- attacker used Clop (capital "i") ransomware:
  - RC4 encryption
  - a seperate random key is generated for every file
    and this key is encrypted using a RSA-1024 bit public key
  - only the attacker has the matching private key...
- filenames of encrypted files have .Clop added as extension
- a ClopReadMe.txt file is put in every folder (cfr. next slide)

ransom requested

```
*-*ALL FILES ON EACH HOST IN THE NETWORK HAVE BEEN ENCRYPTED WITH A STRONG ALGORITHM*-*

-Backups were either encrypted or deleted or backup disks were formatted.
-Shadow copies also removed, so F8 or any other methods may damage encrypted data but not
recover.
-If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 3-5 encrypted files
-(Less than 6 Mb each, non-archived and your files should not contain valuable information
-(Databases, backups, large excel sheets, etc.)).
-You will receive decrypted samples.

-MESSAGE THIS INFORMATION TO COMPANY'S CEO, UNLOCKING OF 1 COMPUTER ONLY IS IMPOSSIBLE, ONLY
WHOLE NETWORK.
-ATTENTION-
-Your warranty - decrypted samples.
-Do not rename encrypted files.
-Do not try to decrypt your data using third party software.
-We don`t need your files and your information.

:::CONTACT EMAIL:::

AND

or


NOTHING PERSONAL IS A BUSINESS
PLEASE DO NOT USE GMAIL, MAIL DOES NOT REACH OR GETS INTO THE SPAM FOLDER.
PLEASE CHECK SPAM FOLDER!!! CLOP^_-
```

Figure 8: ClopReadMe.txt

ransom paid

Maastricht University pays €200,000 to Russian hackers

A Dutch university has taken the difficult decision to pay hundreds of thousands of Euros to Russian hackers that compromised its systems through a ransomware attack

By **Kim Loohuis** Published: **06 Feb 2020 15:30**

Maastricht University has paid nearly €200,000 worth of bitcoin to Russian hackers after 267 servers were compromised in December 2019.

Figure 9: https://www.computerweekly.com/news/252477997/Maastricht-University-pays-200000-to-Russian-hackers

conclusions

conclusions

Figure 10: questions or comments ?