k-business.com

Aus dem Alltag zweiter IT-Forensiker

Incident Response & digitale Forensik

Nina Azimikhah und Gideon Teubert

Euro6,95 IDG COMMUNICATIONS COMPUTERWELT 01 2022

transform!

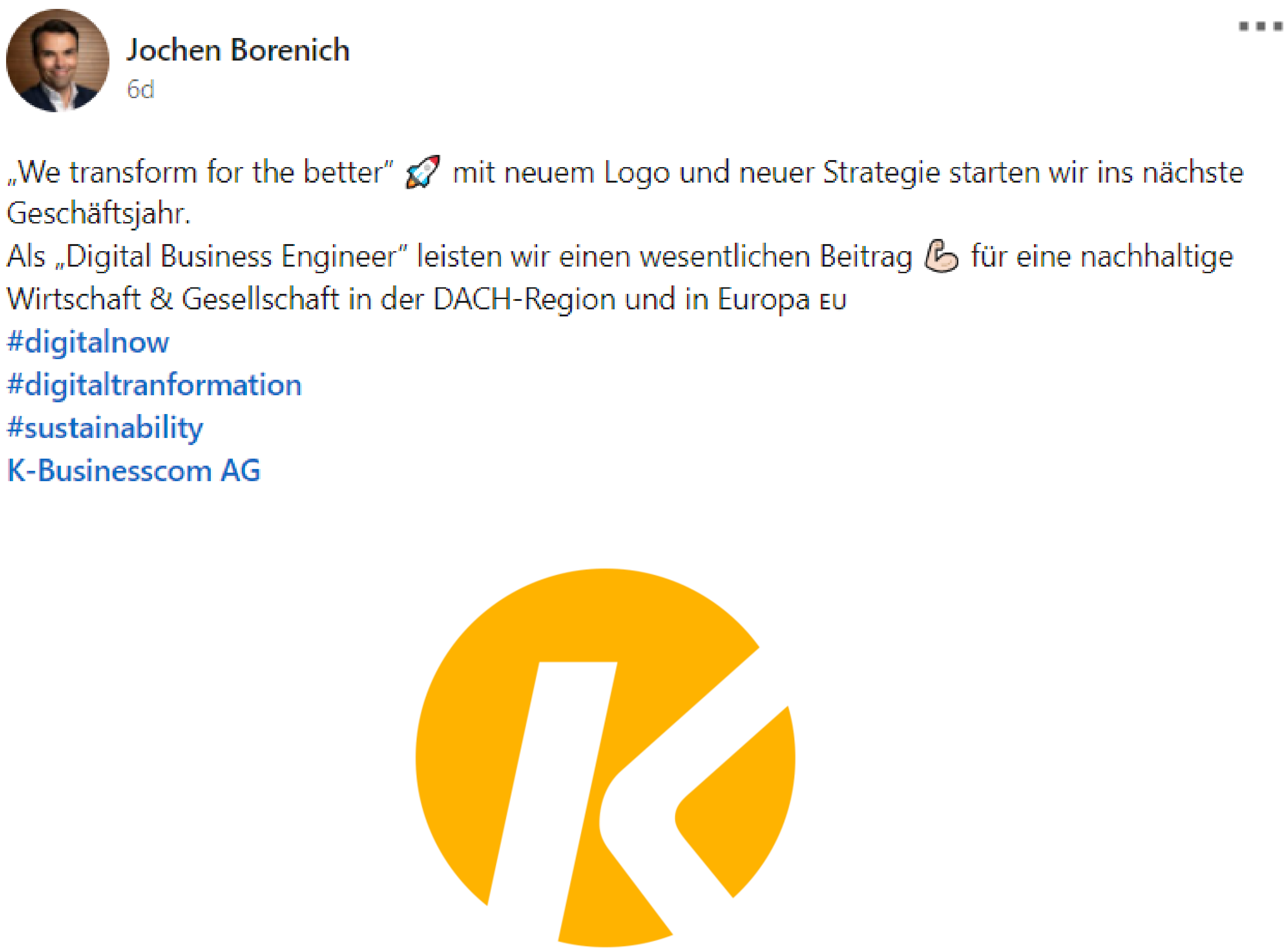
DAS MAGAZIN FÜR DEN DIGITALEN WANDEL

SMART CITIES
So schneidet Wien im globalen Ranking ab

DIGITAL HEALTH
Die Pharmaindustrie als Innovationsmotor

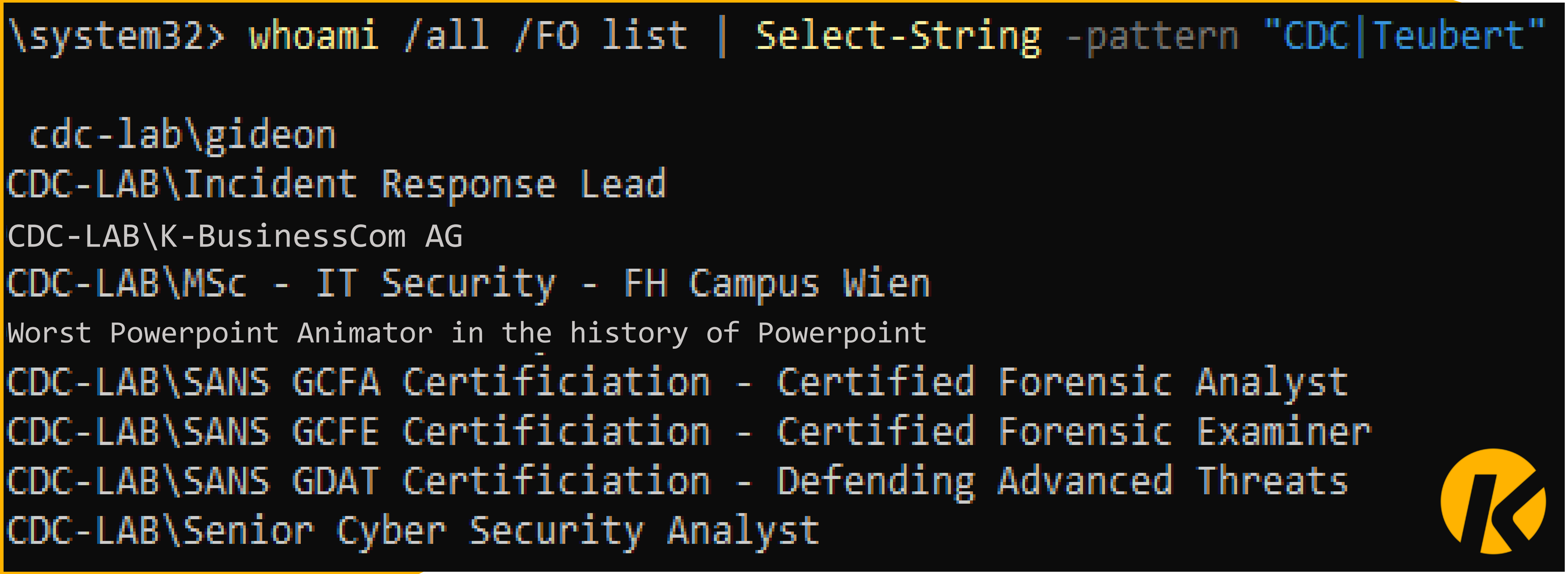
JOCHEN BORENICH & FRANZ SEMMERNEGG, K-BUSINESSCOM

»We transform for the better«



Jochen Borenich
6d

„We transform for the better" 🚀 mit neuem Logo und neuer Strategie starten wir ins nächste Geschäftsjahr.
Als „Digital Business Engineer" leisten wir einen wesentlichen Beitrag 💪 für eine nachhaltige Wirtschaft & Gesellschaft in der DACH-Region und in Europa EU
#digitalnow
#digitaltranformation
#sustainability
K-Businesscom AG



```
\system32> whoami /all /FO list | Select-String -pattern "CDC|Teubert"

 cdc-lab\gideon
CDC-LAB\Incident Response Lead
CDC-LAB\K-BusinessCom AG
CDC-LAB\MSc - IT Security - FH Campus Wien
Worst Powerpoint Animator in the history of Powerpoint
CDC-LAB\SANS GCFA Certificiation - Certified Forensic Analyst
CDC-LAB\SANS GCFE Certificiation - Certified Forensic Examiner
CDC-LAB\SANS GDAT Certificiation - Defending Advanced Threats
CDC-LAB\Senior Cyber Security Analyst
```

PS:>WHOAMI

- Nina Azimikhah
- MSc – IT Security – FH Campus Wien
- Senior Cyber Security & TI Analyst @ K-BusinessCom AG // Threat Intelligence Lead
- Lecturer @ FH Technikum Wien // Digital Forensics & Incident Response
- SANS GCFA Certification – Certified Forensic Analyst
- SANS GNFA Certification – Network Forensic Analyst
- Twitter: @ninz0r

Disclaimer

Please don’t sue us :)

Picture Sources:

1) Loki 1: https://www.lego.com/de-de/product/mighty-micros-thor-vs-loki-76091
2) Loki 2: https://m.media-amazon.com/images/I/51rBlGTglmL._AC_.jpg
3) Ronan: https://www.amazon.de/LEGO-Marvel-Guardians-Galaxy-Minifigure/dp/B01L36CQ7E
4) Thanos 1: https://www.amazon.com/LEGO-Thanos-Minifigure-Gauntlet-Infinity/dp/B07JBCN37D
5) Thanos 2: https://www.sunhotsell.com/?category_id=4928079
6) Hulk: https://www.amazon.de/LEGO-Marvel-Super-Heroes-Figur/dp/B00979MYY0
7) Dr. Strange: https://www.ebay.at/itm/Lego-Doctor-Strange-76060-Super-Heroes-Minifigure/174035195718
8) Gauntlet: https://www.lego.com/de-de/product/infinity-gauntlet-76191
9) Captain America: https://legomarveldc.fandom.com/wiki/Captain_America
10) Ironman: https://www.lego.com/cdn/cs/set/assets/blt8651c6bf964ce8fb/76203_alt2.png
11) Black Widow: https://m.media-amazon.com/images/I/519m2UltygL._AC_.jpg
12) Panic Lego: https://www.nerdfitness.com/wp-content/uploads/2012/06/Lego-Help-Get-Back-On-Track-590x391.jpg

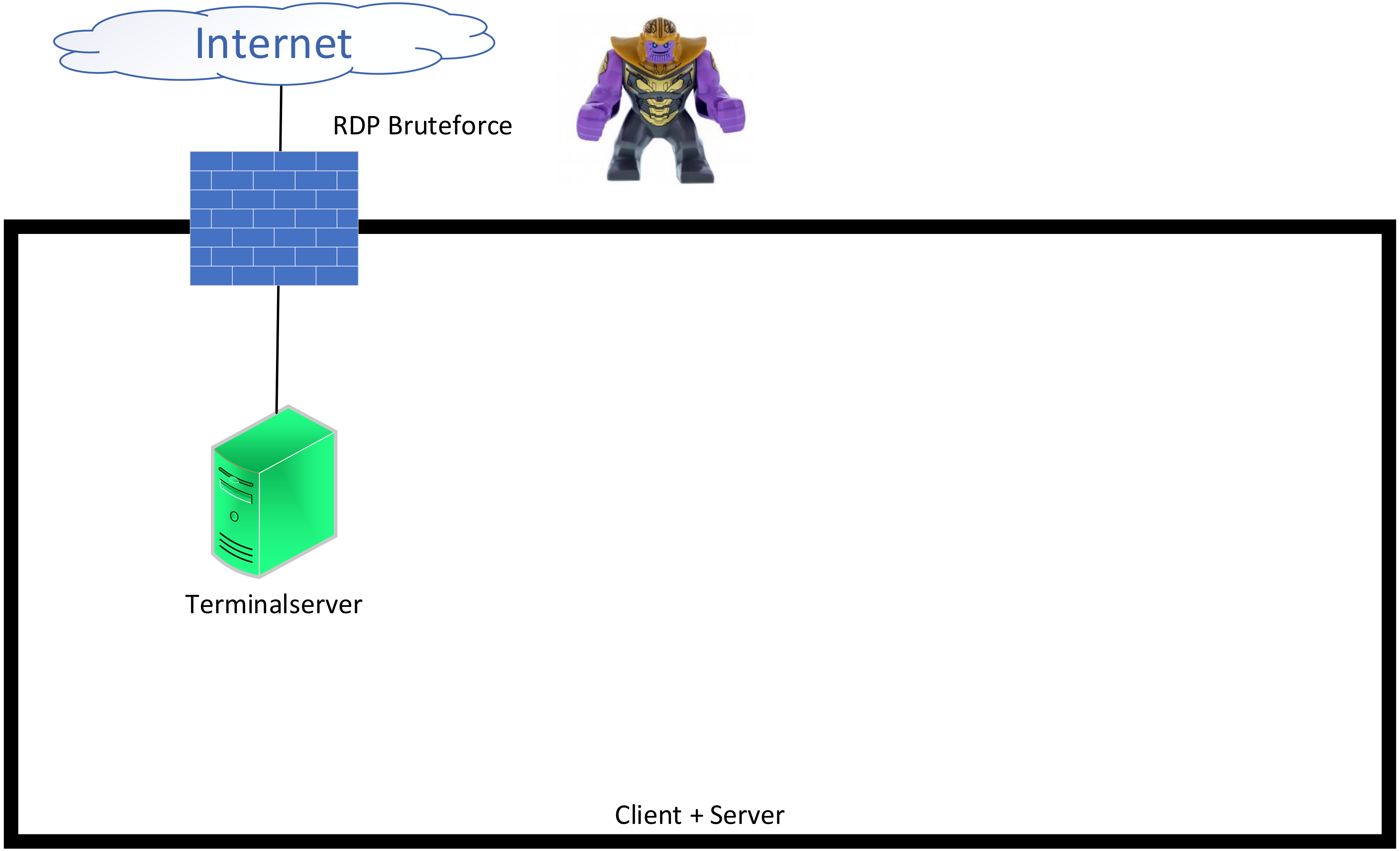
Incident Response

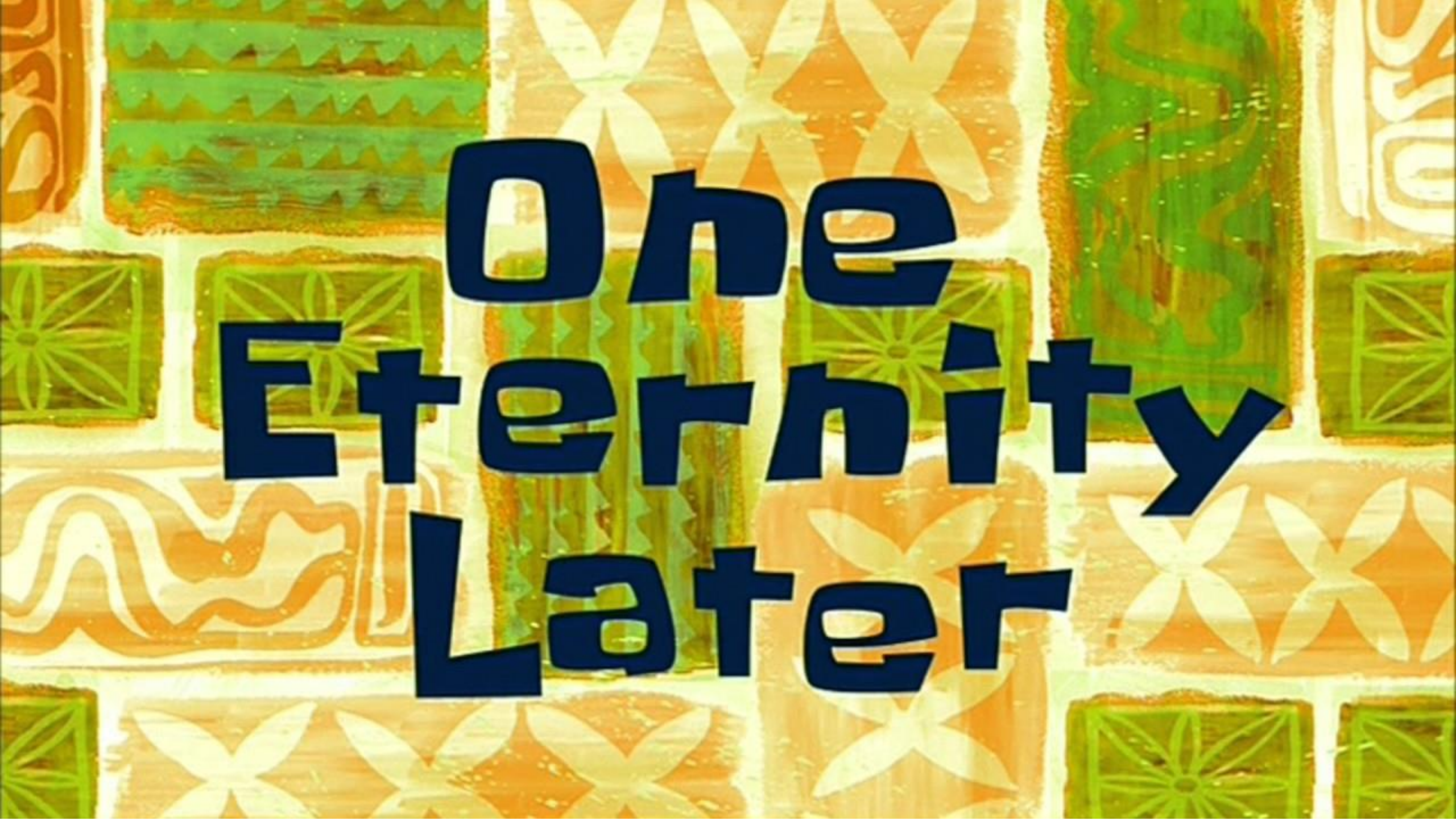
Addressing the aftermath of a security breach / attack to varying degrees.

The fire department of cyber security.

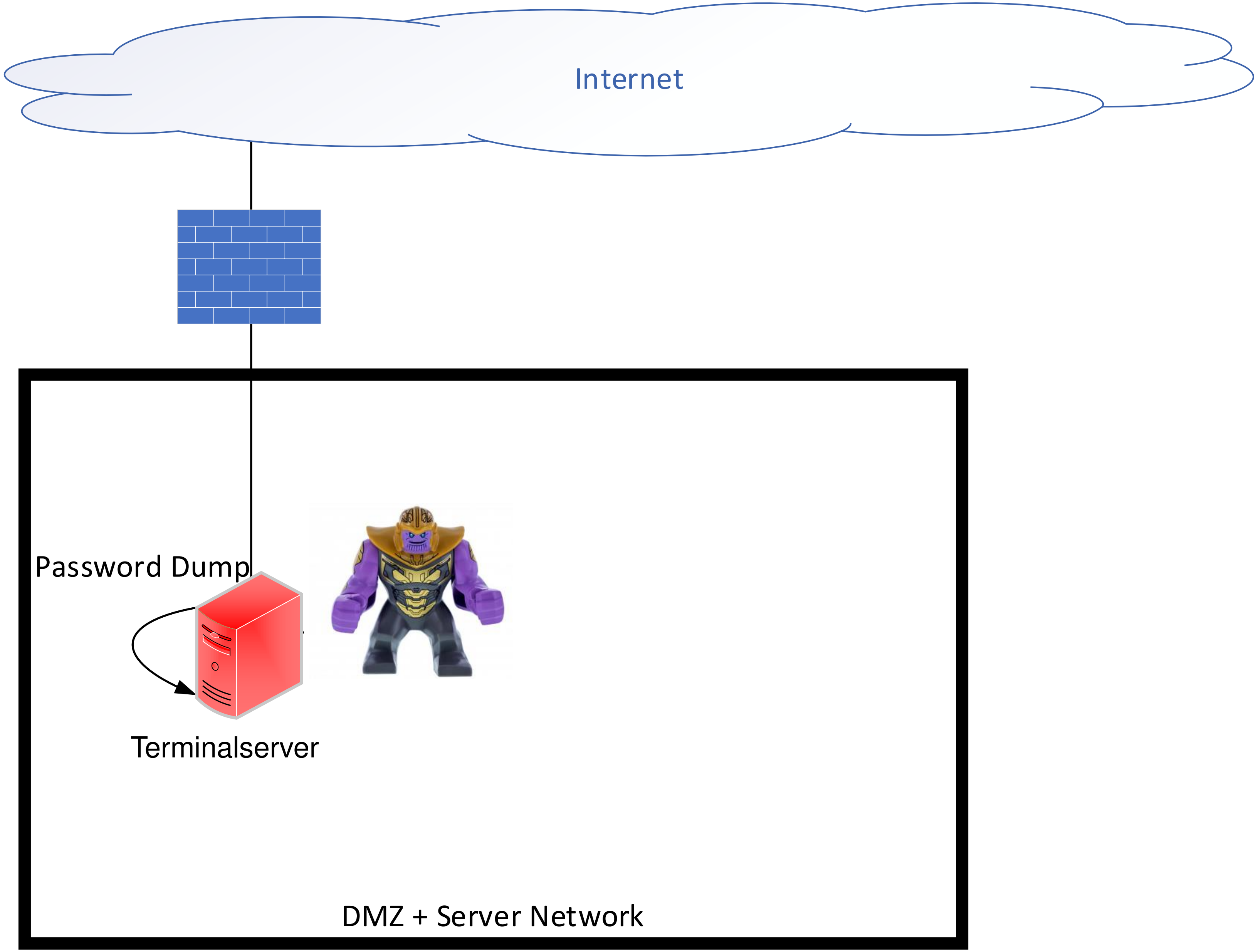
01 Attack #1

I dictate your policy!!!

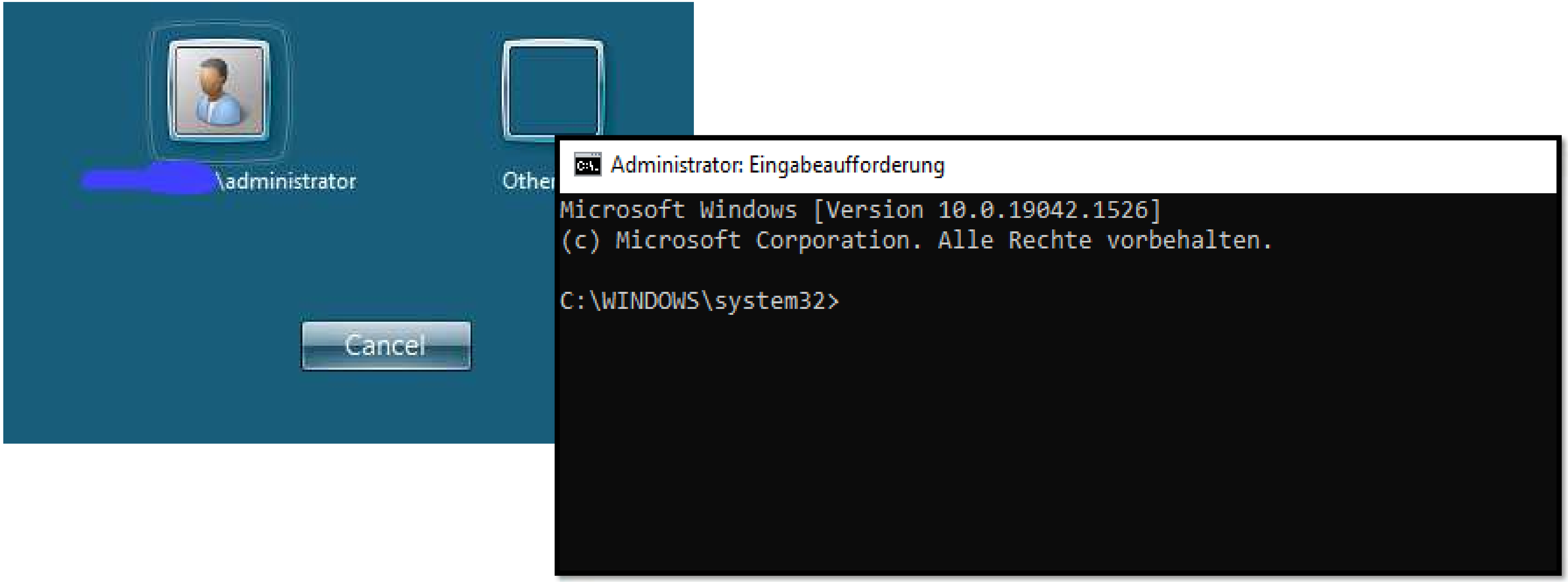

Internet
RDP Bruteforce
Terminalserver
Client + Server



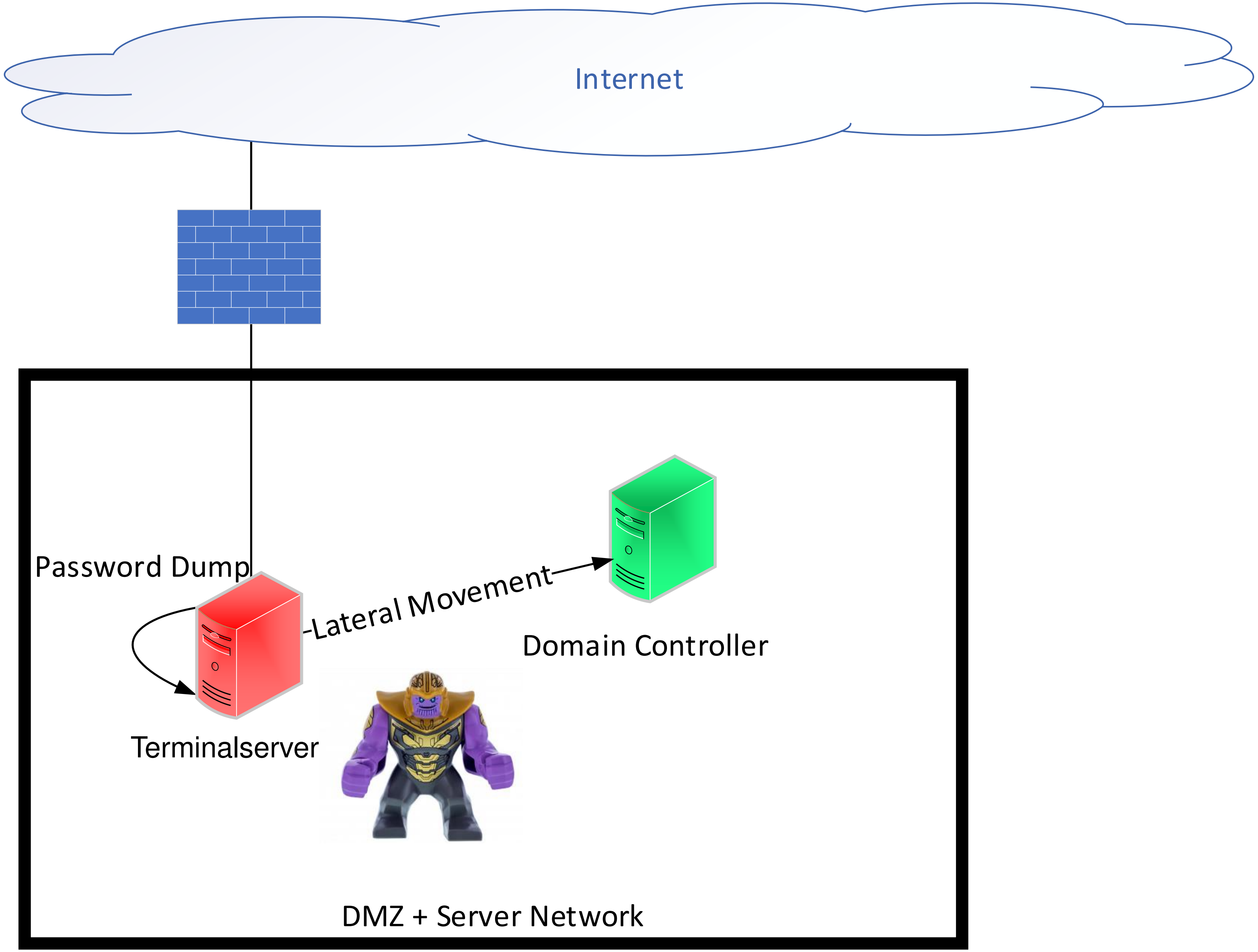
One Eternity Later

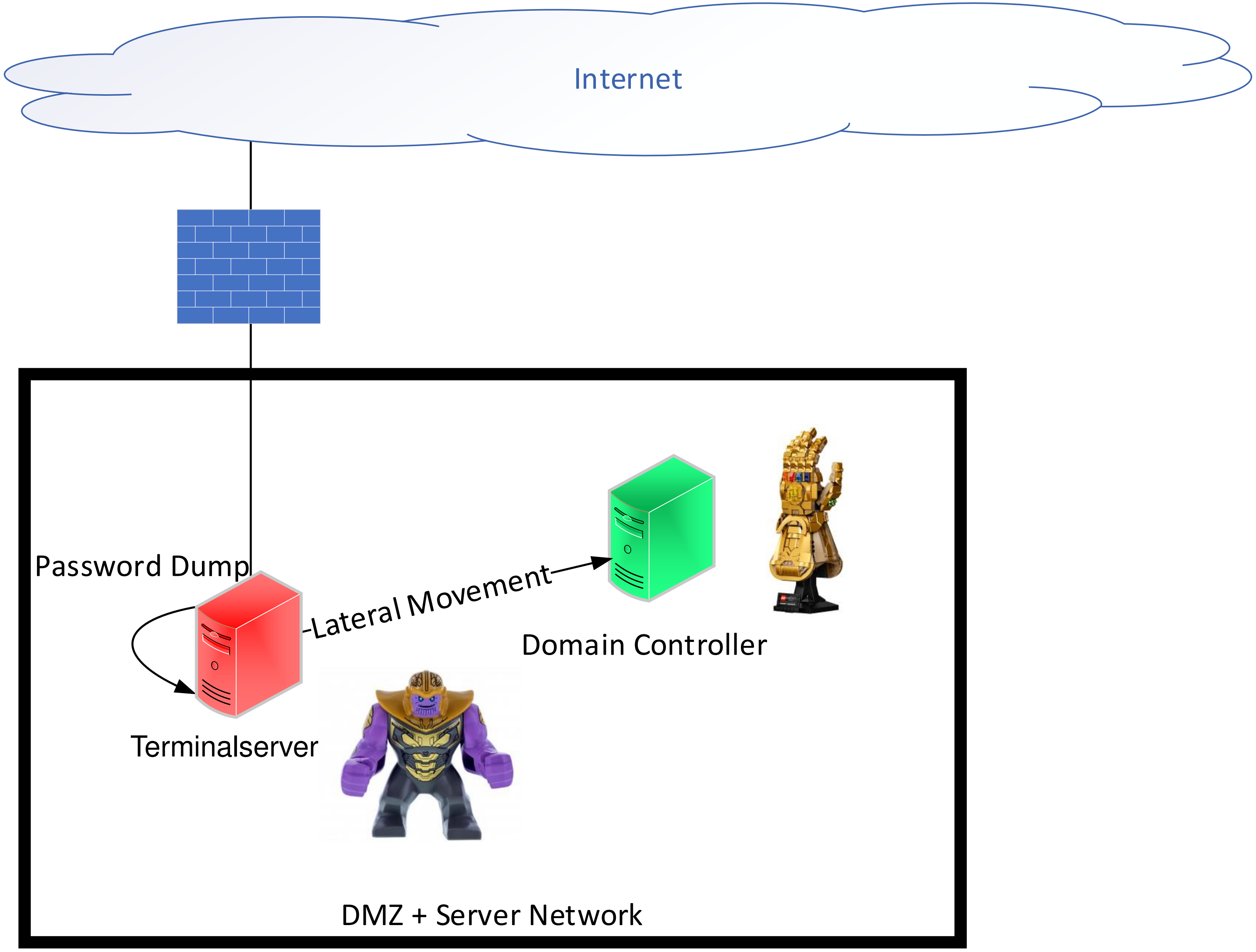

Internet
Password Dump
Terminalserver
DMZ + Server Network

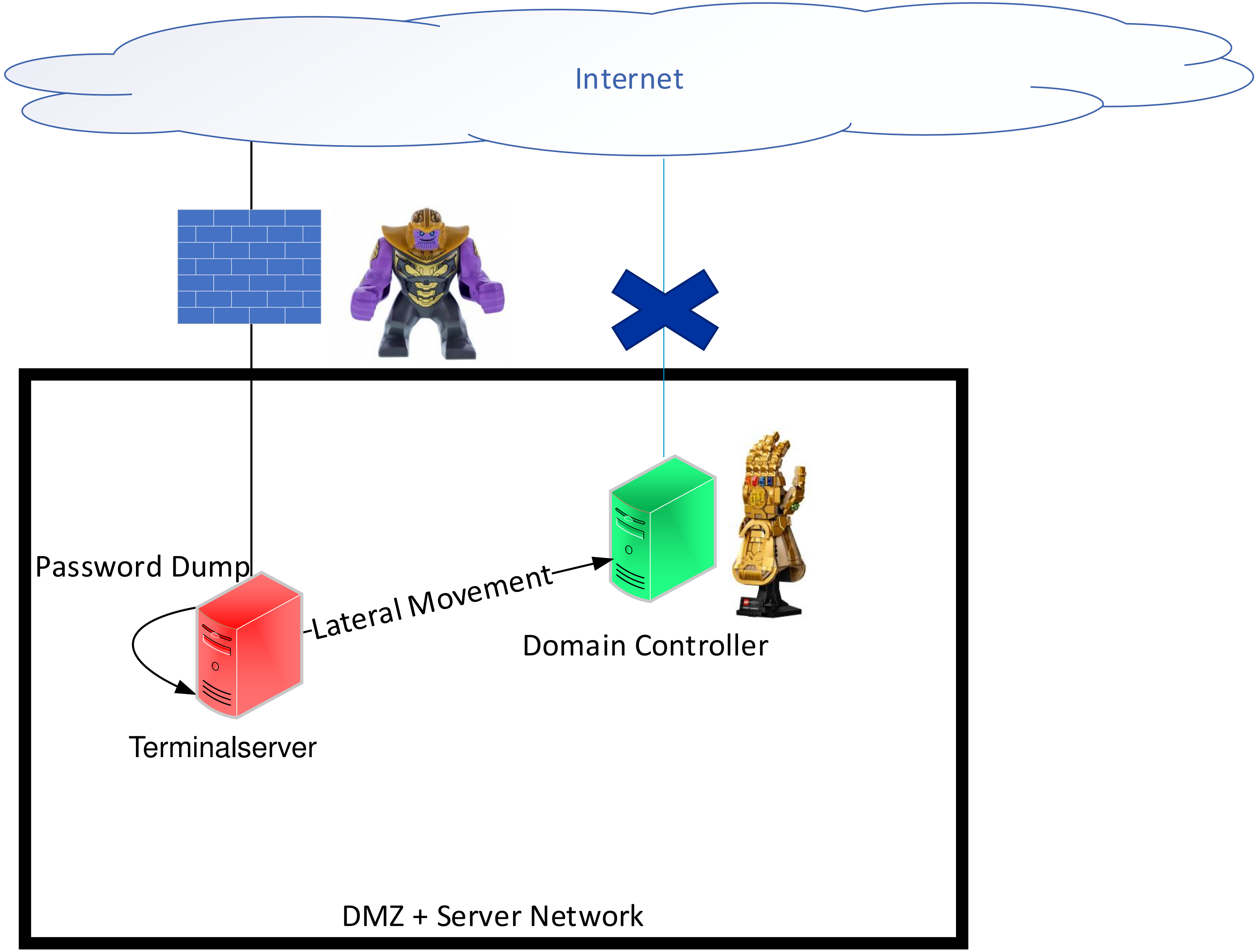
On-Demand Backdoor

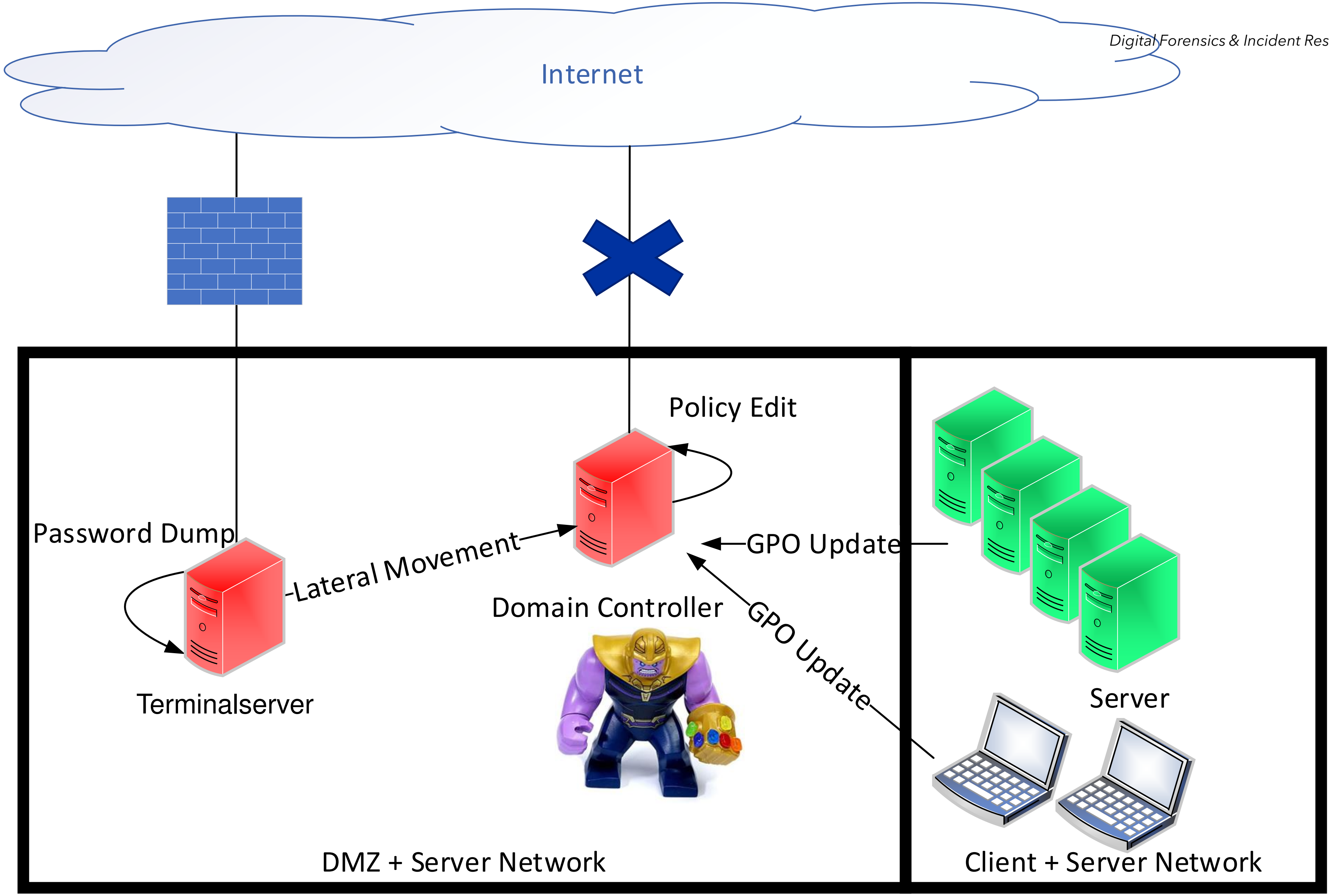


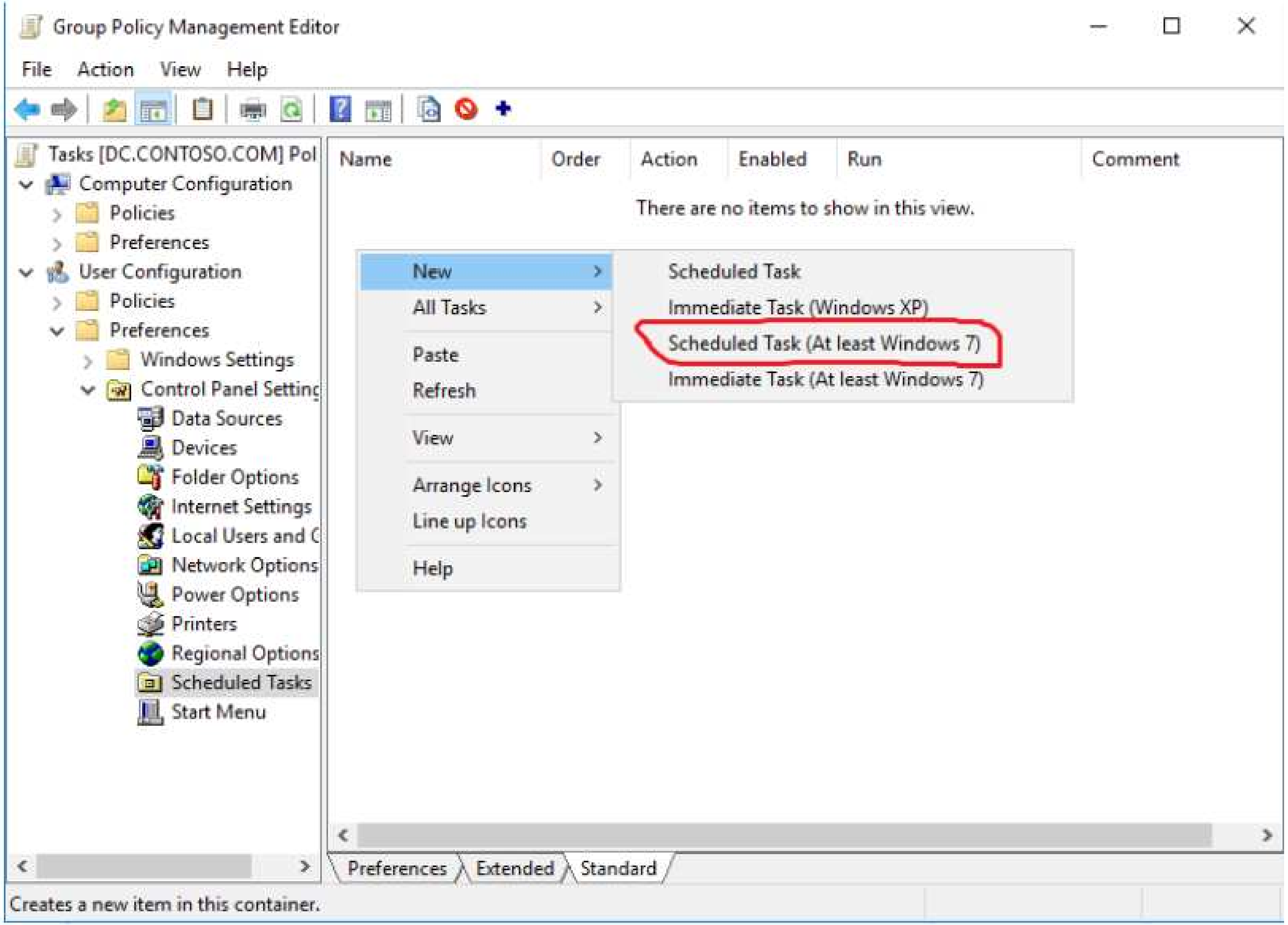
```
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>
```


Internet
Password Dump
Lateral Movement
Domain Controller
Terminalserver
DMZ + Server Network


Internet
Password Dump
Lateral Movement
Domain Controller
Terminalserver
DMZ + Server Network

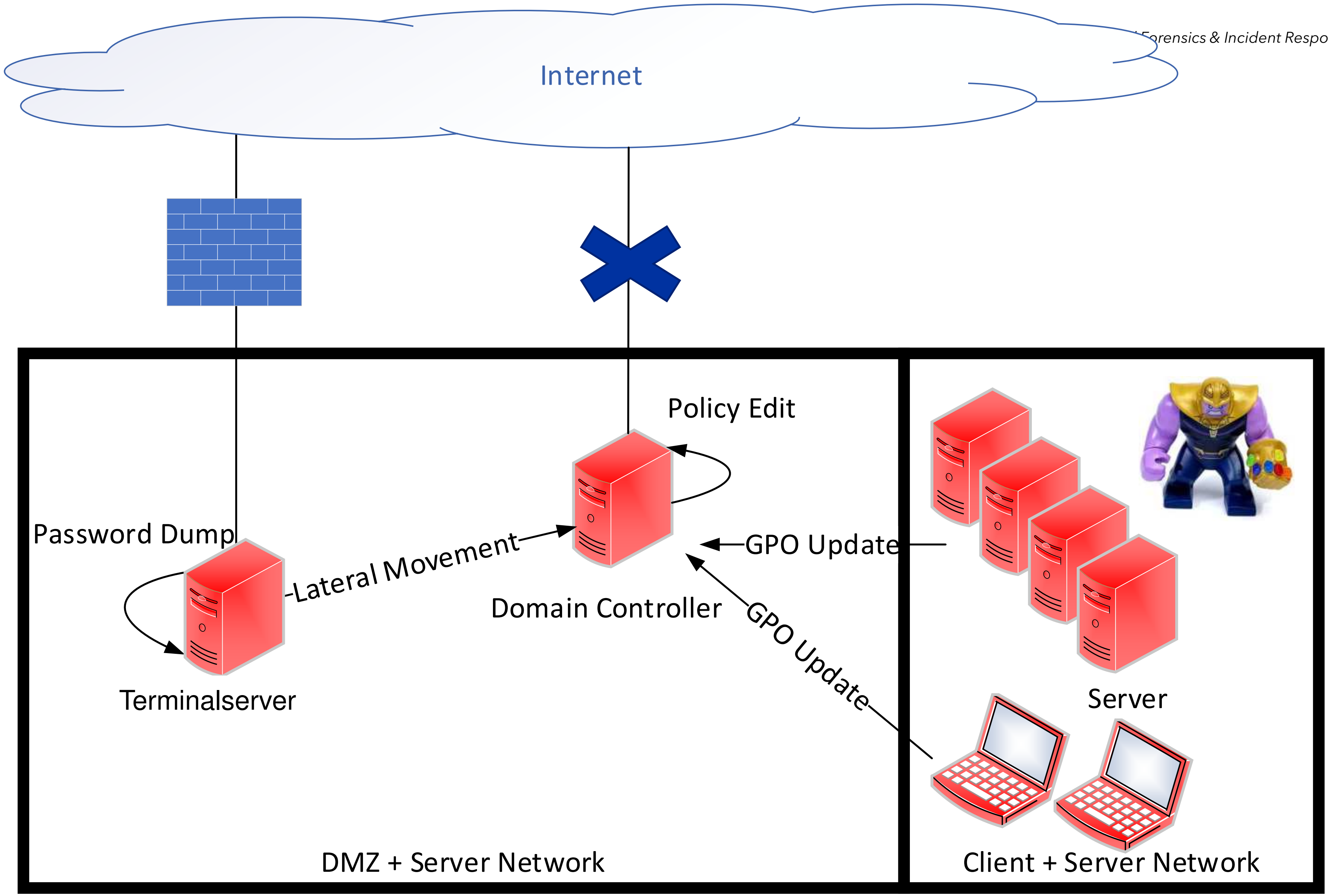

Internet
Password Dump
Lateral Movement
Domain Controller
Terminalserver
DMZ + Server Network


Internet
Policy Edit
Password Dump
Lateral Movement
GPO Update
Domain Controller
GPO Update
Terminalserver
Server
DMZ + Server Network
Client + Server Network



There are no items to show in this view.

Creates a new item in this container.


Internet
Policy Edit
Password Dump
Lateral Movement
GPO Update
Domain Controller
GPO Update
Terminalserver
Server
DMZ + Server Network
Client + Server Network

Extraordinary Stuff

Sandbox Evasion

Communication only through Beachhead

GPO Persistence

No Artifact known by any AV

Reached “Isolated” Systems through Beachhead

Custom Backdoor

50:50

83

15	€ 1 MILLION
14	€ 500.000
13	€ 125.000
12	€ 64.000
11	€ 32.000
10	€ 16.000
9	€ 8.000
8	€ 4.000
7	€ 2.000
6	€ 1.000
5	€ 500
4	€ 300
3	€ 200
2	€ 100
1	€ 50

How long was the attacker active within the company - to take over the whole domain?

A: ~ 12 hours

B: ~ 14 days

C: ~ 1 hour

D: ~ 1 month

50:50

83

15	€ 1 MILLION
14	€ 500.000
13	€ 125.000
12	€ 64.000
11	€ 32.000
10	€ 16.000
9	€ 8.000
8	€ 4.000
7	€ 2.000
6	€ 1.000
5	€ 500
4	€ 300
3	€ 200
2	€ 100
1	€ 50

How long was the attacker active within the company - to take over the whole domain?

A: ~ 12 hours

B: ~ 14 days

C: ~ 1 hour

D: ~ 1 month

02 Attack #2

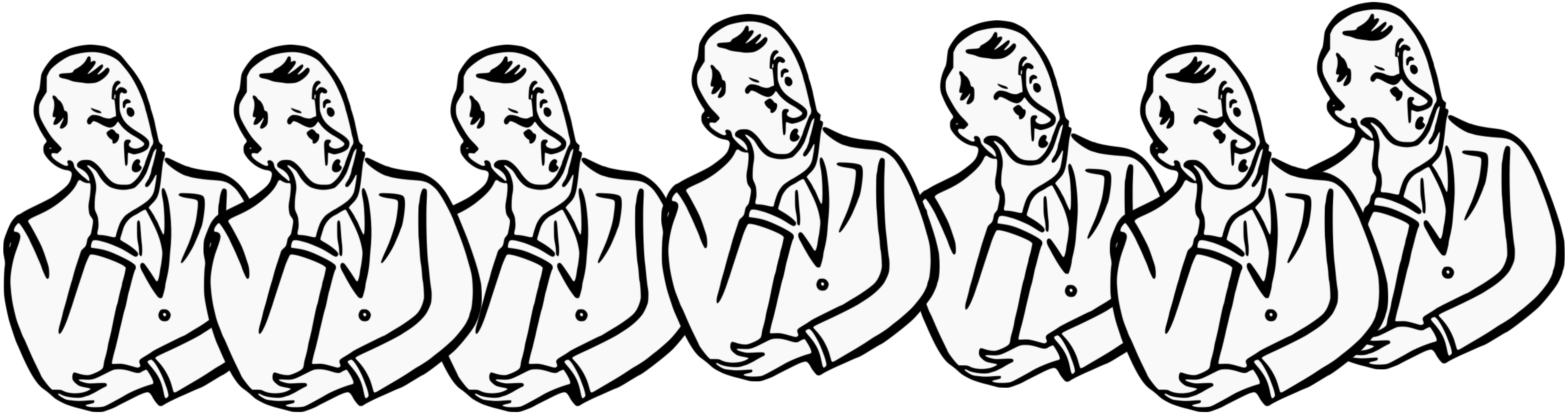
*There are no **Advanced Persistent Threats** in Austria – Right? RIGHT?!*
Let me introduce you to: TA-505

Hmmmmmmm...?

Slow internet connection

… due to hundreds of GB transferring to a sharing platform

… to a sharing platform and nobody knows why



Slow Internet Connection (Data Leakage)

IR Trigger

Bloodhound, Powerview…

Internal Recon

Winhelper

Shimcache Persistence

Cobalt Strike

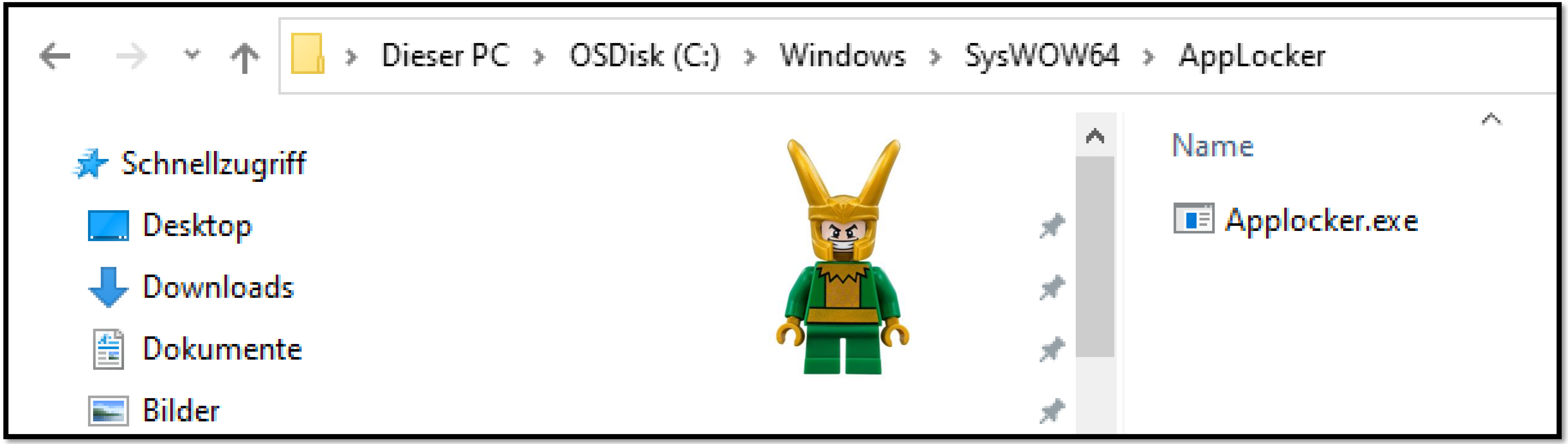
Backdoors

Command and Control

Evasion

Applocker – what are you doing?!

Do you spot the problem?



Dieser PC › OSDisk (C:) › Windows › SysWOW64 › AppLocker

Name

Applocker.exe

Command and Control

- C&C to seemingly legitimate domains.
- Encrypted connections (https)
- C&C domains partly newly registered (aka not flagged by security vendors)
- Data Exfil to non-malicious File Sharing Host

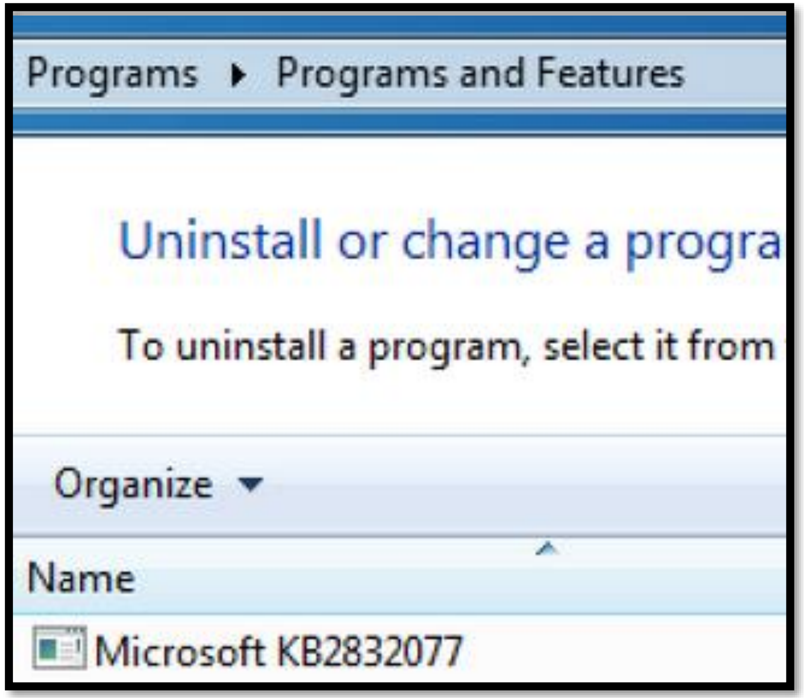
Sample malicious domain:
(Do not access)

microsoft-live-us[.]com

Shimcache Persistence

Attacker installed a „Microsoft“ Patch

- Patches the legitimate service.exe
- Services.exe was clean when scanned
- Nomenclature of normal windows patches



Programs ▸ Programs and Features

Uninstall or change a progra

To uninstall a program, select it from

Name

Microsoft KB2832077

Installed only on a handful of systems to prevent detection / remediation

Summary Attack #3

Slo
Co

Powershell - Invoke UserHunter

po
w
e

Cobalt Strike

More Cobalt Strike

Meterpreter Backdoors

helper

Shimcache Persistence

Backdoor encryption

re

Evasive

Fileless Malware

ike,
ter,
ipe

Malware Signature Change 1-day prior to

Process Injection

More Cobalt Strike

IR Trigger

Internal Recon

Backdoors

Command and Control

Others

Summary Attack #3

Slo
Co

Powers
Invo
UserH

Cobalt St

More
S

Not our official logo. Please don't tell our marketing :)

s Malware

ike,
ter,
pe

Process Injection

balt

IR Trigger

Internal Recon

Backdoors

Command and Control

Others

☎ 👤 50:50

83

15	€ 1 MILLION
14	€ 500.000
13	€ 125.000
12	€ 64.000
11	€ 32.000
10	€ 16.000
9	€ 8.000
8	€ 4.000
7	€ 2.000
6	€ 1.000
5	€ 500
4	€ 300
3	€ 200
2	€ 100
1	€ 50

How long did the attacker had full control over the company until the attack was discovered?

A: ~ 2 weeks

B: ~ Less than 12 hours

C: ~ 5-7 days

D: > 4 months

50:50

83

15	€ 1 MILLION
14	€ 500.000
13	€ 125.000
12	€ 64.000
11	€ 32.000
10	€ 16.000
9	€ 8.000
8	€ 4.000
7	€ 2.000
6	€ 1.000
5	€ 500
4	€ 300
3	€ 200
2	€ 100
1	€ 50

How long did the attacker had full control over the company until the attack was discovered?

A: ~ 2 weeks

B: ~ Less than 12 hours

C: ~ 5-7 days

D: > 4 months

03 Conclusio

What is really happening in Austria?

So – what should we do?

Incident Response is reactive firefighting.

Better approach:

Gain visibility and proactively monitor your environment instead of using a reactive approach (Incident Response).

Use the combination of

Prevent + Detect + Respond

Transition

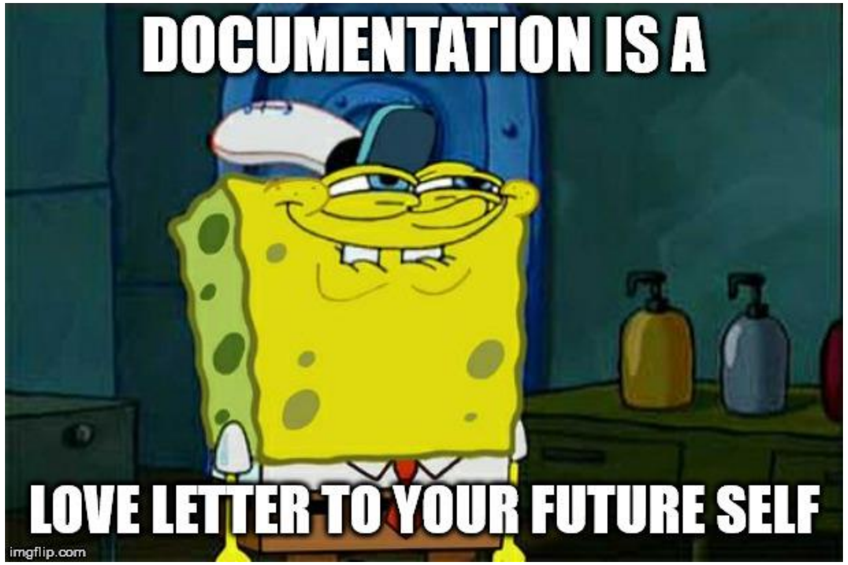
Gideon

Nina

04 Digital Forensics - Chain of Custody

Differences to IR

- Often not time critical
- Not really about malware or trojans
- More about „did the person do it or not?“
- Chain of custody
- Documentation, Documentation, Documentation



Types of experts

- Consultant
  - Report serves as argumentation aid
  - Report does not count as evidence in court
  - Report is objectively considered by judge

- Certified expert witness („Allgemein beeideter und gerichtlich zertifizierter Sachverständiger“)
  - An exam is taken at court
  - Has to take an oath

05 Data Theft

Case: Employee Data Theft

- Company: Marvel
- Employee Slothman „stole“ confidential data
- Gave them to competitor „DC“
- Slothman is going to start working at DC
- Behaved very suspicious during last work week
- Left company at 2021/11/26
- Pre investigation took place

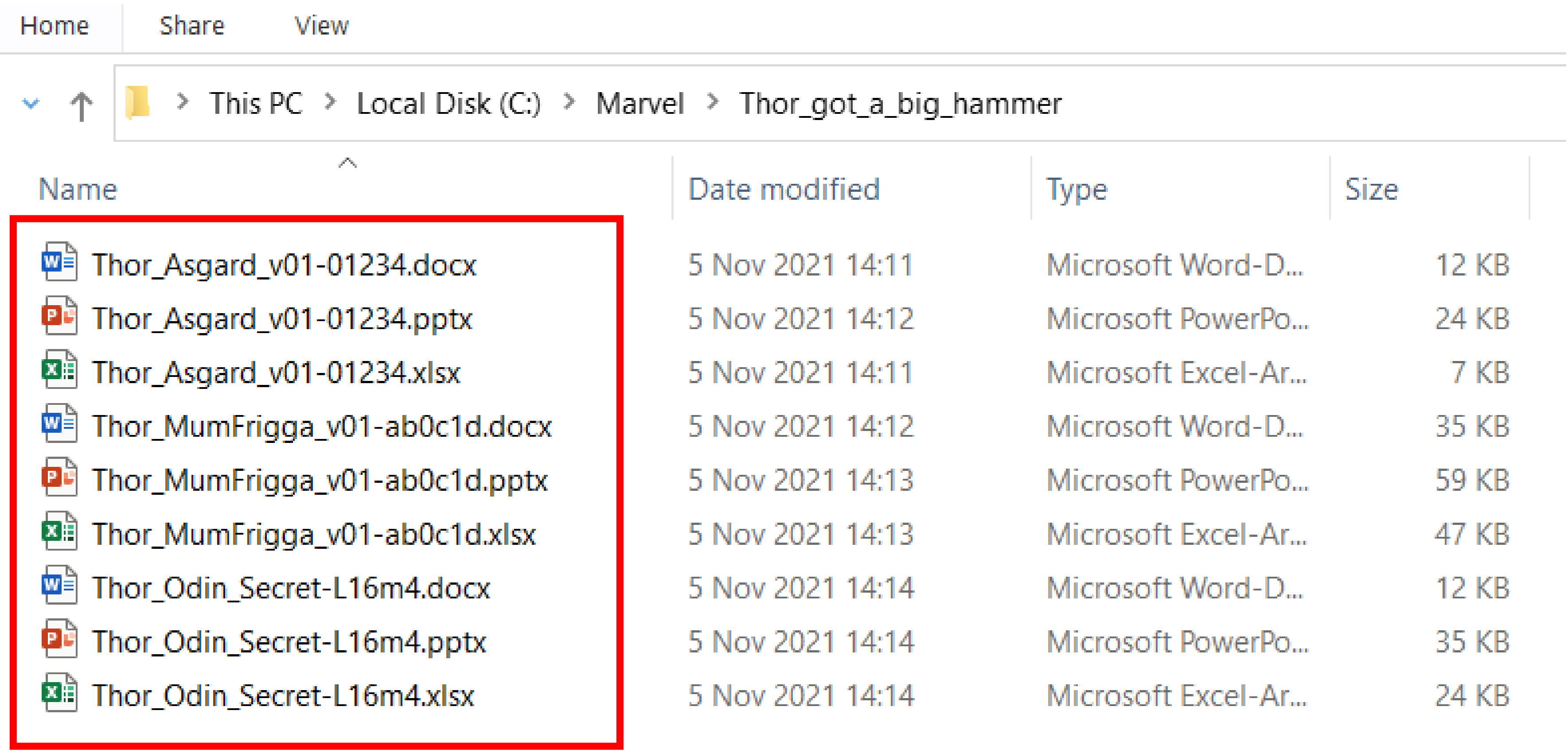
Case: Employee data theft

- Affected devices
- 1 notebook with a hard drive (HDD)
- 1 USB drive (BYOD)
- Client sent us
  - list of unique data names which are VERY sensitive – level confidential
  - MD5 Hashes
  - Time period: 01.11.2021 – 26.11.2021

Data…

…we are looking for

Screenshot of file names („IOCs")



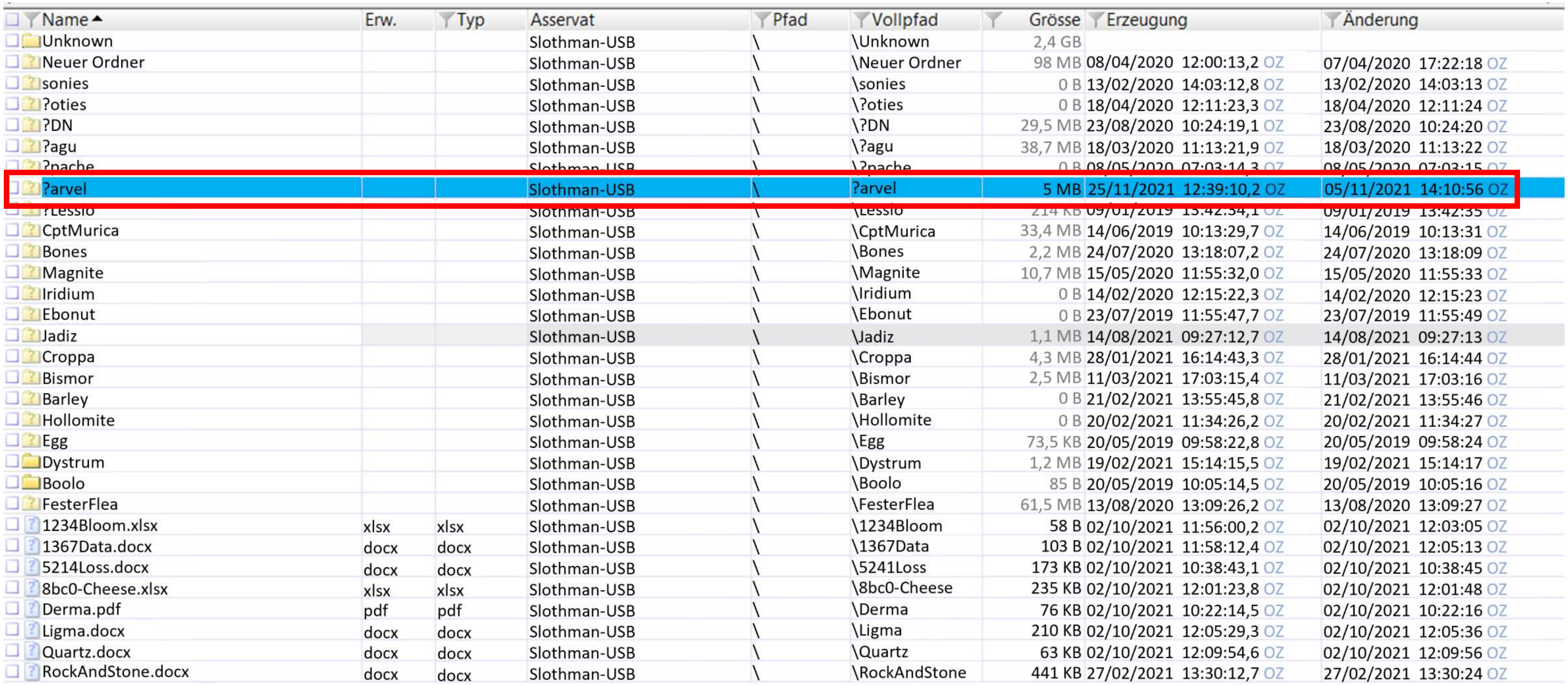
This PC > Local Disk (C:) > Marvel > Thor_got_a_big_hammer

Name	Date modified	Type	Size
Thor_Asgard_v01-01234.docx	5 Nov 2021 14:11	Microsoft Word-D...	12 KB
Thor_Asgard_v01-01234.pptx	5 Nov 2021 14:12	Microsoft PowerPo...	24 KB
Thor_Asgard_v01-01234.xlsx	5 Nov 2021 14:11	Microsoft Excel-Ar...	7 KB
Thor_MumFrigga_v01-ab0c1d.docx	5 Nov 2021 14:12	Microsoft Word-D...	35 KB
Thor_MumFrigga_v01-ab0c1d.pptx	5 Nov 2021 14:13	Microsoft PowerPo...	59 KB
Thor_MumFrigga_v01-ab0c1d.xlsx	5 Nov 2021 14:13	Microsoft Excel-Ar...	47 KB
Thor_Odin_Secret-L16m4.docx	5 Nov 2021 14:14	Microsoft Word-D...	12 KB
Thor_Odin_Secret-L16m4.pptx	5 Nov 2021 14:14	Microsoft PowerPo...	35 KB
Thor_Odin_Secret-L16m4.xlsx	5 Nov 2021 14:14	Microsoft Excel-Ar...	24 KB

First step

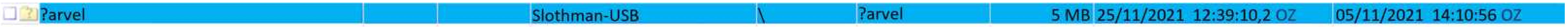
- Acquisition of USB and HDD according to Chain of Custody
- Started investigating USB drive
  - Was empty
- Next:
  - File carving and file recovery on USB drive
  - Filesystem: FAT32
- Was any suspicious on the USB drive?
- Timeline Analysis
- Time period: 01.11.2021 – 26.11.2021

Carved and Recovered Files on USB



Name ▲	Erw.	Typ	Asservat	Pfad	Vollpfad	Grösse	Erzeugung	Änderung
Unknown			Slothman-USB	\	\Unknown	2,4 GB		
Neuer Ordner			Slothman-USB	\	\Neuer Ordner	98 MB	08/04/2020 12:00:13,2 OZ	07/04/2020 17:22:18 OZ
sonies			Slothman-USB	\	\sonies	0 B	13/02/2020 14:03:12,8 OZ	13/02/2020 14:03:13 OZ
?oties			Slothman-USB	\	\?oties	0 B	18/04/2020 12:11:23,3 OZ	18/04/2020 12:11:24 OZ
?DN			Slothman-USB	\	\?DN	29,5 MB	23/08/2020 10:24:19,1 OZ	23/08/2020 10:24:20 OZ
?agu			Slothman-USB	\	\?agu	38,7 MB	18/03/2020 11:13:21,9 OZ	18/03/2020 11:13:22 OZ
?pache			Slothman-USB	\	\?pache	0 B	08/05/2020 07:03:14,3 OZ	08/05/2020 07:03:15 OZ
?arvel			Slothman-USB	\	?arvel	5 MB	25/11/2021 12:39:10,2 OZ	05/11/2021 14:10:56 OZ
?Lessio			Slothman-USB	\	\Lessio	214 KB	09/01/2019 13:42:34,1 OZ	09/01/2019 13:42:35 OZ
CptMurica			Slothman-USB	\	\CptMurica	33,4 MB	14/06/2019 10:13:29,7 OZ	14/06/2019 10:13:31 OZ
Bones			Slothman-USB	\	\Bones	2,2 MB	24/07/2020 13:18:07,2 OZ	24/07/2020 13:18:09 OZ
Magnite			Slothman-USB	\	\Magnite	10,7 MB	15/05/2020 11:55:32,0 OZ	15/05/2020 11:55:33 OZ
Iridium			Slothman-USB	\	\Iridium	0 B	14/02/2020 12:15:22,3 OZ	14/02/2020 12:15:23 OZ
Ebonut			Slothman-USB	\	\Ebonut	0 B	23/07/2019 11:55:47,7 OZ	23/07/2019 11:55:49 OZ
Jadiz			Slothman-USB	\	\Jadiz	1,1 MB	14/08/2021 09:27:12,7 OZ	14/08/2021 09:27:13 OZ
Croppa			Slothman-USB	\	\Croppa	4,3 MB	28/01/2021 16:14:43,3 OZ	28/01/2021 16:14:44 OZ
Bismor			Slothman-USB	\	\Bismor	2,5 MB	11/03/2021 17:03:15,4 OZ	11/03/2021 17:03:16 OZ
Barley			Slothman-USB	\	\Barley	0 B	21/02/2021 13:55:45,8 OZ	21/02/2021 13:55:46 OZ
Hollomite			Slothman-USB	\	\Hollomite	0 B	20/02/2021 11:34:26,2 OZ	20/02/2021 11:34:27 OZ
Egg			Slothman-USB	\	\Egg	73,5 KB	20/05/2019 09:58:22,8 OZ	20/05/2019 09:58:24 OZ
Dystrum			Slothman-USB	\	\Dystrum	1,2 MB	19/02/2021 15:14:15,5 OZ	19/02/2021 15:14:17 OZ
Boolo			Slothman-USB	\	\Boolo	85 B	20/05/2019 10:05:14,5 OZ	20/05/2019 10:05:16 OZ
FesterFlea			Slothman-USB	\	\FesterFlea	61,5 MB	13/08/2020 13:09:26,2 OZ	13/08/2020 13:09:27 OZ
1234Bloom.xlsx	xlsx	xlsx	Slothman-USB	\	\1234Bloom	58 B	02/10/2021 11:56:00,2 OZ	02/10/2021 12:03:05 OZ
1367Data.docx	docx	docx	Slothman-USB	\	\1367Data	103 B	02/10/2021 11:58:12,4 OZ	02/10/2021 12:05:13 OZ
5214Loss.docx	docx	docx	Slothman-USB	\	\5241Loss	173 KB	02/10/2021 10:38:43,1 OZ	02/10/2021 10:38:45 OZ
8bc0-Cheese.xlsx	xlsx	xlsx	Slothman-USB	\	\8bc0-Cheese	235 KB	02/10/2021 12:01:23,8 OZ	02/10/2021 12:01:48 OZ
Derma.pdf	pdf	pdf	Slothman-USB	\	\Derma	76 KB	02/10/2021 10:22:14,5 OZ	02/10/2021 10:22:16 OZ
Ligma.docx	docx	docx	Slothman-USB	\	\Ligma	210 KB	02/10/2021 12:05:29,3 OZ	02/10/2021 12:05:36 OZ
Quartz.docx	docx	docx	Slothman-USB	\	\Quartz	63 KB	02/10/2021 12:09:54,6 OZ	02/10/2021 12:09:56 OZ
RockAndStone.docx	docx	docx	Slothman-USB	\	\RockAndStone	441 KB	27/02/2021 13:30:12,7 OZ	27/02/2021 13:30:24 OZ

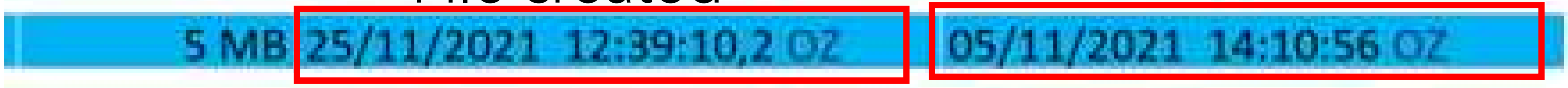
Closer look at timestamp



```
□ ?arvel                    Slothman-USB     \     ?arvel     5 MB 25/11/2021 12:39:10,2 OZ   05/11/2021 14:10:56 OZ
```

File created

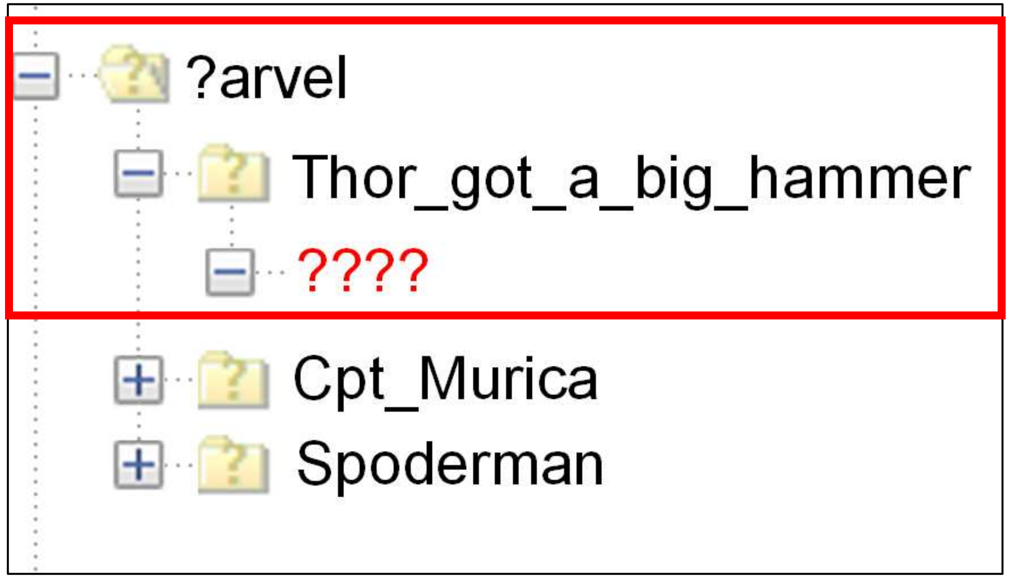
File modified



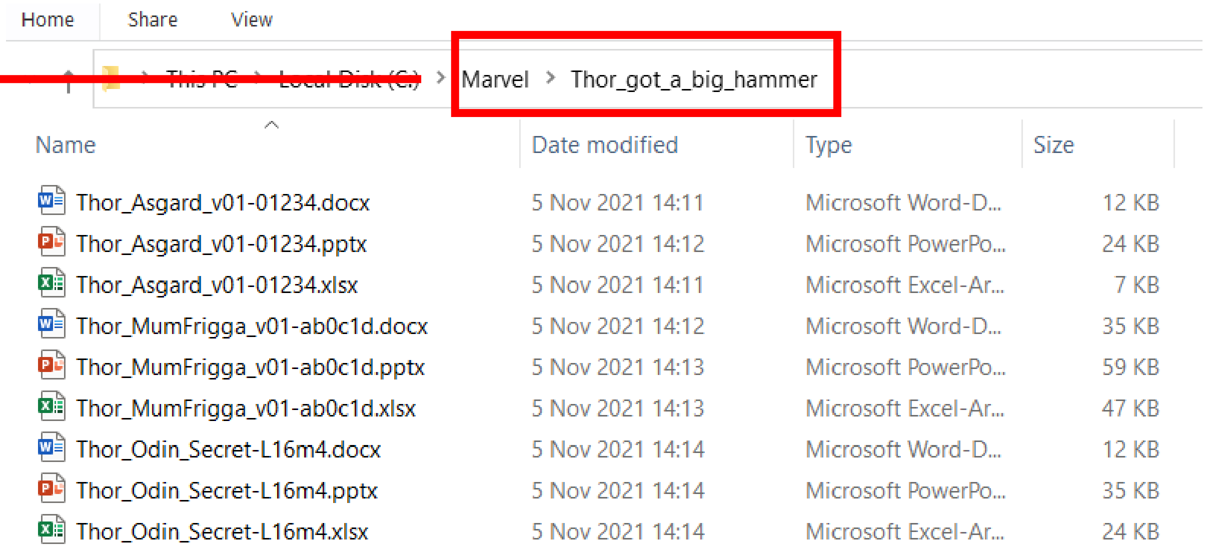
```
5 MB 25/11/2021 12:39:10,2 OZ   05/11/2021 14:10:56 OZ
```

- If date „File created“ newer (or after) than „File modified“ → file was copied

Folder Structure of ?arvel



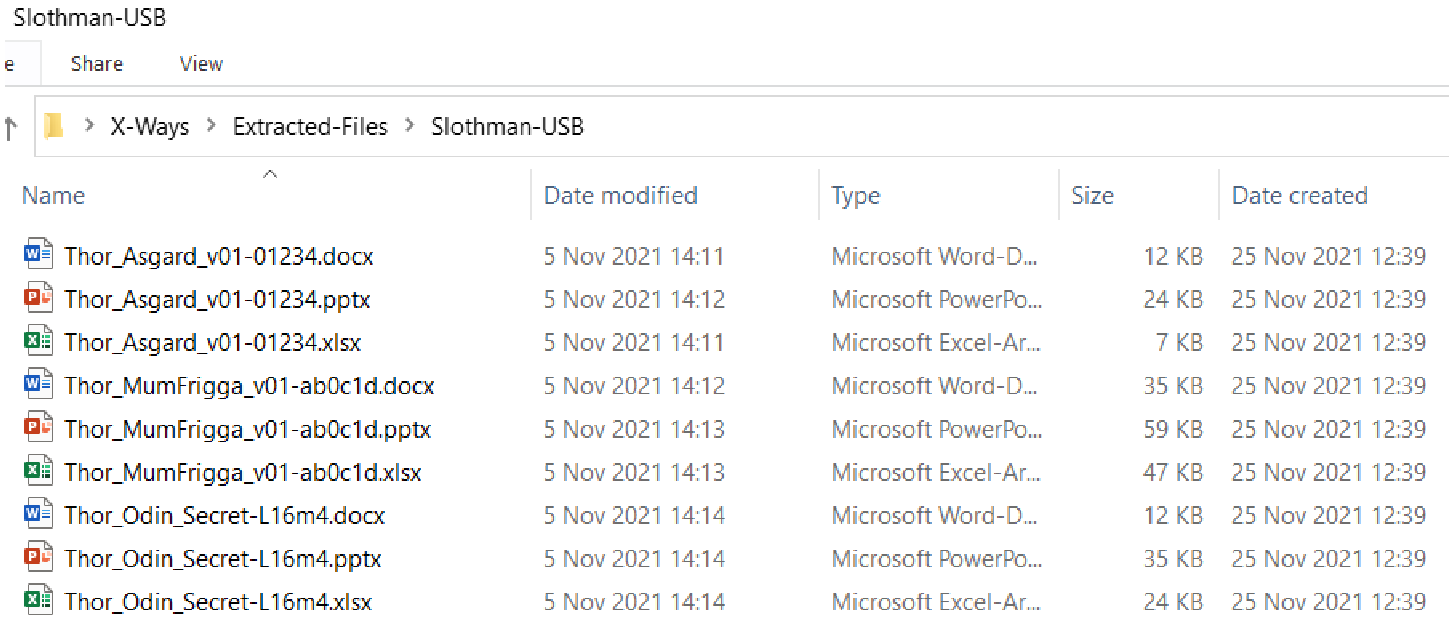
?arvel
Thor_got_a_big_hammer
????
Cpt_Murica
Spoderman



This PC > Local Disk (C:) > Marvel > Thor_got_a_big_hammer

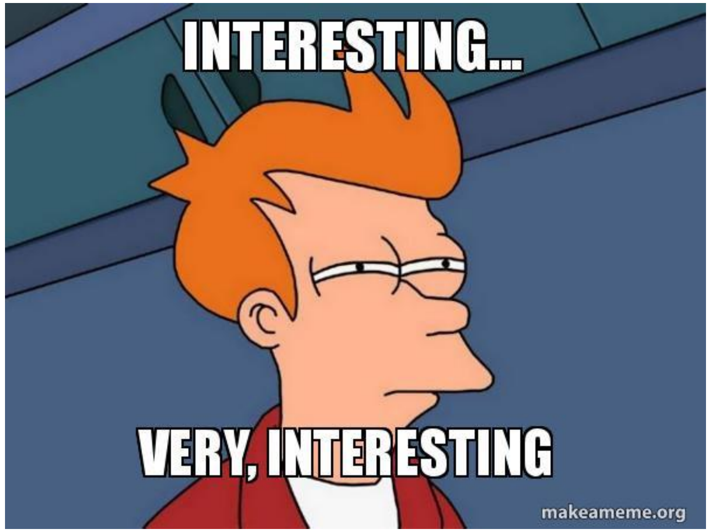
Name	Date modified	Type	Size
Thor_Asgard_v01-01234.docx	5 Nov 2021 14:11	Microsoft Word-D...	12 KB
Thor_Asgard_v01-01234.pptx	5 Nov 2021 14:12	Microsoft PowerPo...	24 KB
Thor_Asgard_v01-01234.xlsx	5 Nov 2021 14:11	Microsoft Excel-Ar...	7 KB
Thor_MumFrigga_v01-ab0c1d.docx	5 Nov 2021 14:12	Microsoft Word-D...	35 KB
Thor_MumFrigga_v01-ab0c1d.pptx	5 Nov 2021 14:13	Microsoft PowerPo...	59 KB
Thor_MumFrigga_v01-ab0c1d.xlsx	5 Nov 2021 14:13	Microsoft Excel-Ar...	47 KB
Thor_Odin_Secret-L16m4.docx	5 Nov 2021 14:14	Microsoft Word-D...	12 KB
Thor_Odin_Secret-L16m4.pptx	5 Nov 2021 14:14	Microsoft PowerPo...	35 KB
Thor_Odin_Secret-L16m4.xlsx	5 Nov 2021 14:14	Microsoft Excel-Ar...	24 KB

File Extraction



X-Ways > Extracted-Files > Slothman-USB

Name	Date modified	Type	Size	Date created
Thor_Asgard_v01-01234.docx	5 Nov 2021 14:11	Microsoft Word-D...	12 KB	25 Nov 2021 12:39
Thor_Asgard_v01-01234.pptx	5 Nov 2021 14:12	Microsoft PowerPo...	24 KB	25 Nov 2021 12:39
Thor_Asgard_v01-01234.xlsx	5 Nov 2021 14:11	Microsoft Excel-Ar...	7 KB	25 Nov 2021 12:39
Thor_MumFrigga_v01-ab0c1d.docx	5 Nov 2021 14:12	Microsoft Word-D...	35 KB	25 Nov 2021 12:39
Thor_MumFrigga_v01-ab0c1d.pptx	5 Nov 2021 14:13	Microsoft PowerPo...	59 KB	25 Nov 2021 12:39
Thor_MumFrigga_v01-ab0c1d.xlsx	5 Nov 2021 14:13	Microsoft Excel-Ar...	47 KB	25 Nov 2021 12:39
Thor_Odin_Secret-L16m4.docx	5 Nov 2021 14:14	Microsoft Word-D...	12 KB	25 Nov 2021 12:39
Thor_Odin_Secret-L16m4.pptx	5 Nov 2021 14:14	Microsoft PowerPo...	35 KB	25 Nov 2021 12:39
Thor_Odin_Secret-L16m4.xlsx	5 Nov 2021 14:14	Microsoft Excel-Ar...	24 KB	25 Nov 2021 12:39



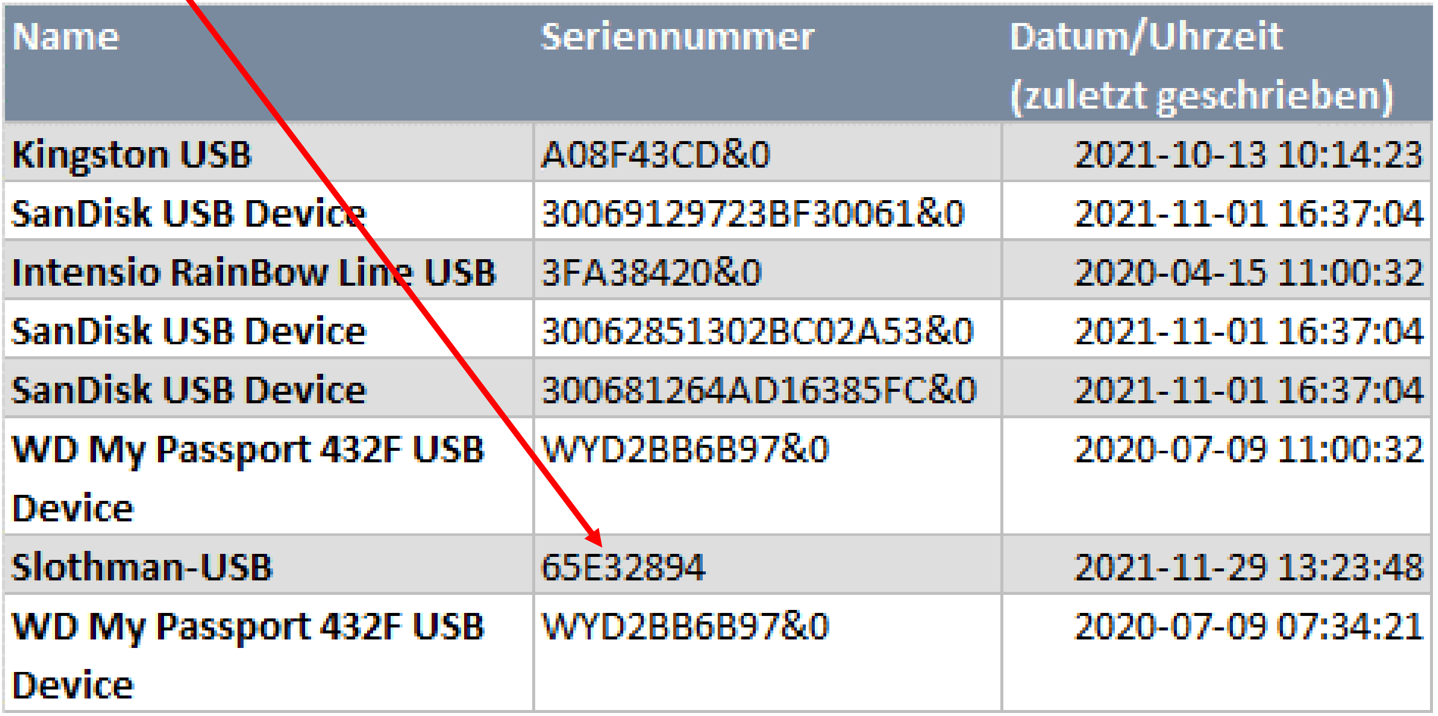
Second Step

Prove that files were copied from HDD to USB drive

Serial number USB: 65E32894

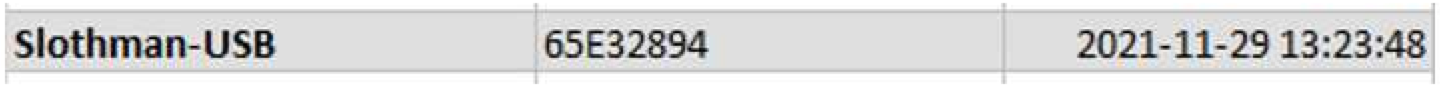
Registry key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet##\Enum\USBStore

Tracks USB devices plugged into a machine (Last time written)

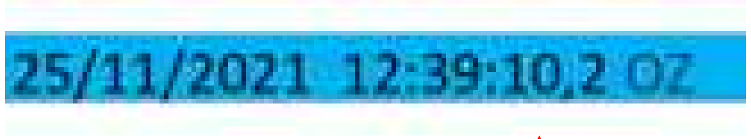


Name	Seriennummer	Datum/Uhrzeit (zuletzt geschrieben)
Kingston USB	A08F43CD&0	2021-10-13 10:14:23
SanDisk USB Device	30069129723BF30061&0	2021-11-01 16:37:04
Intensio RainBow Line USB	3FA38420&0	2020-04-15 11:00:32
SanDisk USB Device	30062851302BC02A53&0	2021-11-01 16:37:04
SanDisk USB Device	300681264AD16385FC&0	2021-11-01 16:37:04
WD My Passport 432F USB Device	WYD2BB6B97&0	2020-07-09 11:00:32
Slothman-USB	65E32894	2021-11-29 13:23:48
WD My Passport 432F USB Device	WYD2BB6B97&0	2020-07-09 07:34:21

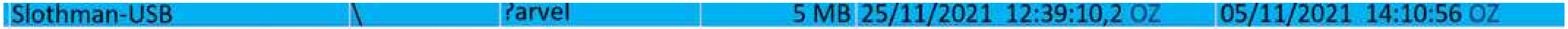
Timestamp USB drive was plugged into machine



Slothman-USB	65E32894	2021-11-29 13:23:48



25/11/2021 12:39:10,2 OZ



Slothman-USB	\	?arvel	5 MB	25/11/2021 12:39:10,2 OZ	05/11/2021 14:10:56 OZ

29.11.2021 ???

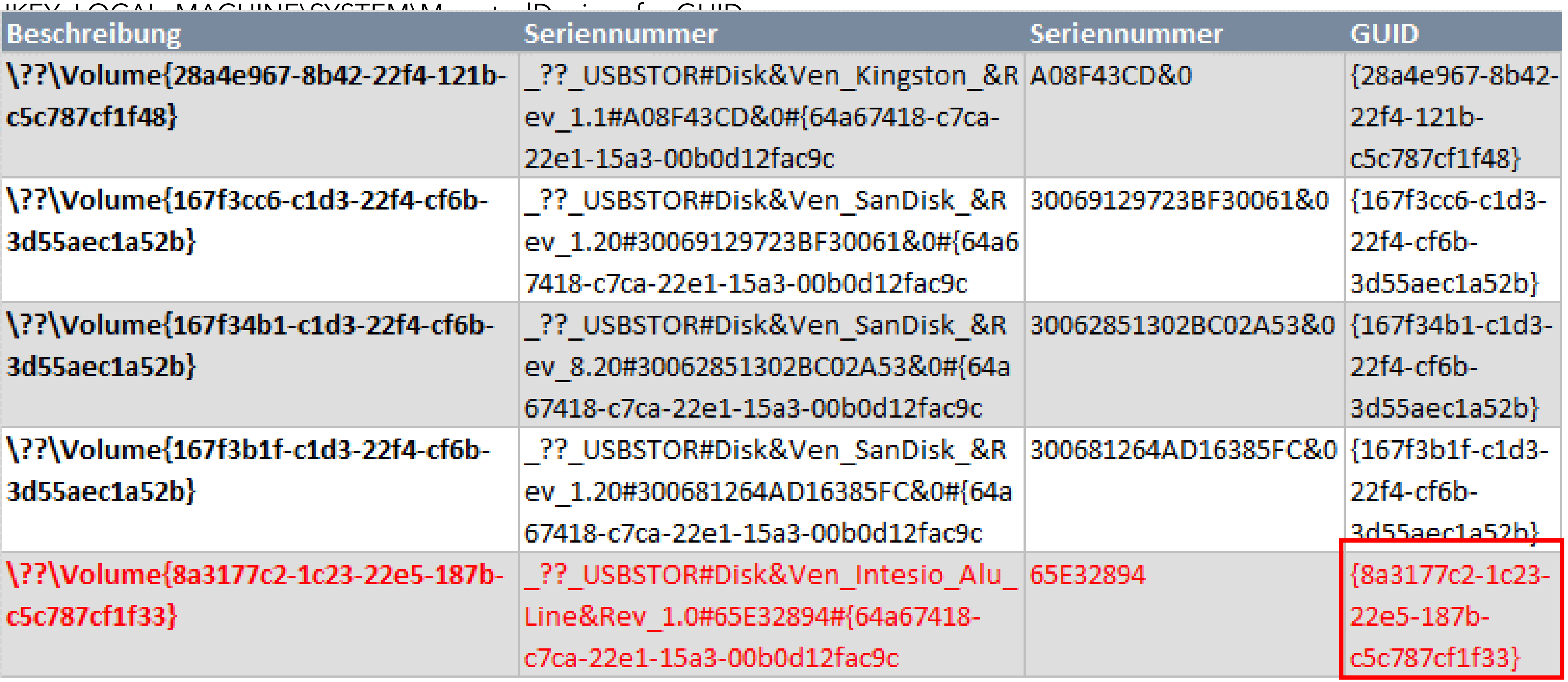
- 29.11.2021: Pre-investigation of the notebook through client‘s IT support

Other Artefacts…

…that can be used to identify if USB was plugged into machine by Slothman

Check HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices for GUID

GUID is



Beschreibung	Seriennummer	Seriennummer	GUID
\??\Volume{28a4e967-8b42-22f4-121b-c5c787cf1f48}	_??_USBSTOR#Disk&Ven_Kingston_&Rev_1.1#A08F43CD&0#{64a67418-c7ca-22e1-15a3-00b0d12fac9c	A08F43CD&0	{28a4e967-8b42-22f4-121b-c5c787cf1f48}
\??\Volume{167f3cc6-c1d3-22f4-cf6b-3d55aec1a52b}	_??_USBSTOR#Disk&Ven_SanDisk_&Rev_1.20#30069129723BF30061&0#{64a67418-c7ca-22e1-15a3-00b0d12fac9c	30069129723BF30061&0	{167f3cc6-c1d3-22f4-cf6b-3d55aec1a52b}
\??\Volume{167f34b1-c1d3-22f4-cf6b-3d55aec1a52b}	_??_USBSTOR#Disk&Ven_SanDisk_&Rev_8.20#30062851302BC02A53&0#{64a67418-c7ca-22e1-15a3-00b0d12fac9c	30062851302BC02A53&0	{167f34b1-c1d3-22f4-cf6b-3d55aec1a52b}
\??\Volume{167f3b1f-c1d3-22f4-cf6b-3d55aec1a52b}	_??_USBSTOR#Disk&Ven_SanDisk_&Rev_1.20#300681264AD16385FC&0#{64a67418-c7ca-22e1-15a3-00b0d12fac9c	300681264AD16385FC&0	{167f3b1f-c1d3-22f4-cf6b-3d55aec1a52b}
\??\Volume{8a3177c2-1c23-22e5-187b-c5c787cf1f33}	_??_USBSTOR#Disk&Ven_Intesio_Alu_Line&Rev_1.0#65E32894#{64a67418-c7ca-22e1-15a3-00b0d12fac9c	65E32894	{8a3177c2-1c23-22e5-187b-c5c787cf1f33}

Existing User on Notebook

- User profiles
  - Marvel
  - Nick_Fury
  - Slothman
  - Admin
- Check NTUSER.dat of Slothman if USB drive was plugged in
- \NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

NTUser.dat of Slothma

Datum/Uhrzeit	Moun	
2021-10-13 10:14:23	{28a4 22f4-1 c5c787	gston_&Rev_1.1
2021-11-25 12:38:01	{8a317 22e5-1 c5c787	esio_Alu_Line&Rev_1.0
2021-11-01 16:37:04	{167f3 22f4-c 3d55a	Disk_&Rev_1.20

tinder
It's a Match!
{8a3177c2-1c23-22e5-187b-c5c787cf1f33}
{8a3177c2-1c23-22e5-187b-c5c787cf1f33}

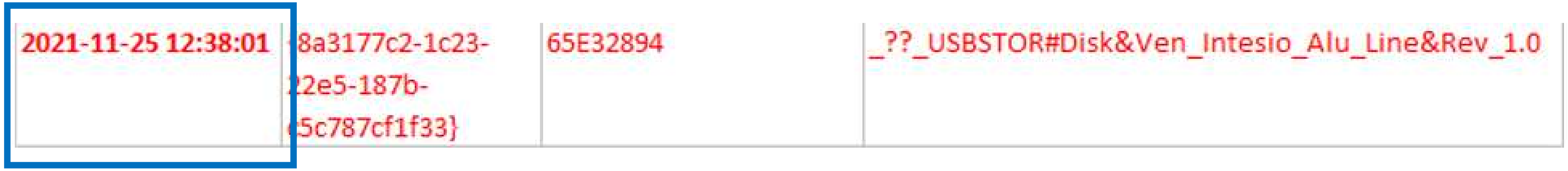
MountedDevices

\??\Volume{8a3177c2-1c23-2 c5c787cf1f33}		{8a3177c2-1c23-22e5-187b-c5c787cf1f33}

What we know so far…

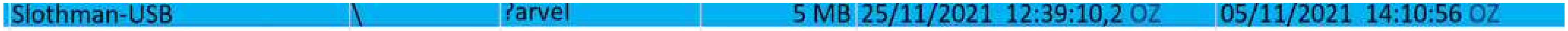
- USB drive contains „stolen“ files
- USB device was inserted by user into machine
- Did Slothman copy the files from HDD to the USB drive?

Conntected usb drive with user profile of Slothman

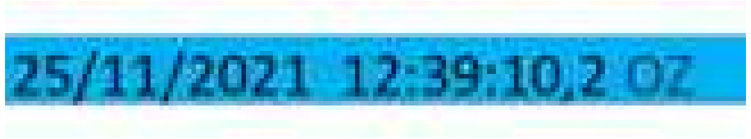


2021-11-25 12:38:01	8a3177c2-1c23- 2e5-187b- 5c787cf1f33}	65E32894	_??_USBSTOR#Disk&Ven_Intesio_Alu_Line&Rev_1.0

Time when the file was copied to the USB drive:

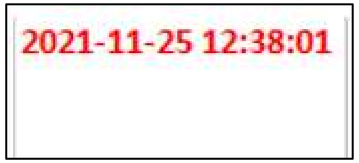


Slothman-USB	\	?arvel	5 MB	25/11/2021 12:39:10,2 OZ	05/11/2021 14:10:56 OZ



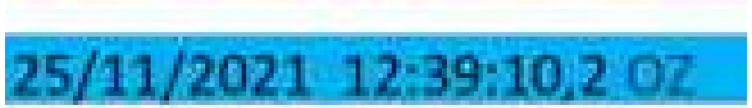
25/11/2021 12:39:10,2 OZ

Connected USB drive with user profile Slothman to the notebook



2021-11-25 12:38:01

→



25/11/2021 12:39:10,2 OZ

Copied file to the USB

Let‘s check for other artefacts

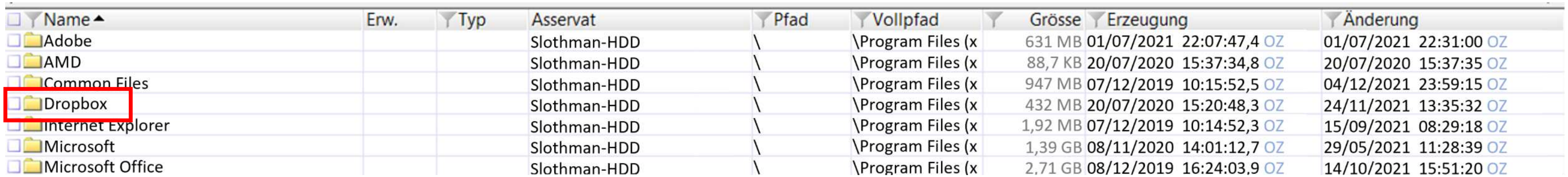
- Artefacts that might show us if user leaked data
  - Emails sent?
  - Dropbox or OneDrive installed?

- Emails are stored locally at
  - %USERPROFILE%\AppData\Local\Microsoft\Outlook
  - .ost files available
- Encrypted and also questionable if we are allowed to investigate
  - Privacy

Dropbox or OneDrive installed?

- OneDrive → used in daily business, not so interesting
- Dropbox installed?
  - App usually installed at C:\Program Files (x86)\Dropbox
  - Installer file dropped at: C:\Users\<username>\AppData\Roaming\Dropbox\installer
  - Synched Folder: C:\Users\<username>\Documents\My Dropbox → can be changed during installation

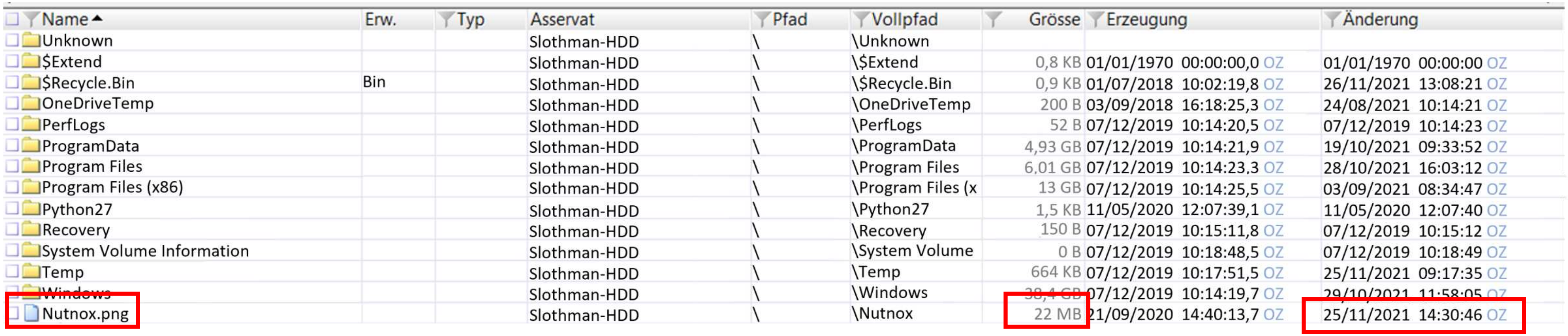
C:\Program Files (x86)



Name	Erw.	Typ	Asservat	Pfad	Vollpfad	Grösse	Erzeugung	Änderung
Adobe			Slothman-HDD	\	\Program Files (x	631 MB	01/07/2021 22:07:47,4 OZ	01/07/2021 22:31:00 OZ
AMD			Slothman-HDD	\	\Program Files (x	88,7 KB	20/07/2020 15:37:34,8 OZ	20/07/2020 15:37:35 OZ
Common Files			Slothman-HDD	\	\Program Files (x	947 MB	07/12/2019 10:15:52,5 OZ	04/12/2021 23:59:15 OZ
Dropbox			Slothman-HDD	\	\Program Files (x	432 MB	20/07/2020 15:20:48,3 OZ	24/11/2021 13:35:32 OZ
Internet Explorer			Slothman-HDD	\	\Program Files (x	1,92 MB	07/12/2019 10:14:52,3 OZ	15/09/2021 08:29:18 OZ
Microsoft			Slothman-HDD	\	\Program Files (x	1,39 GB	08/11/2020 14:01:12,7 OZ	29/05/2021 11:28:39 OZ
Microsoft Office			Slothman-HDD	\	\Program Files (x	2,71 GB	08/12/2019 16:24:03,9 OZ	14/10/2021 15:51:20 OZ

- Dropbox installation – check
- But… C:\Users\Slothman\Documents\My Dropbox did not exist ☹
- What to do? Let's check other directories, maybe user changed path to synch folder

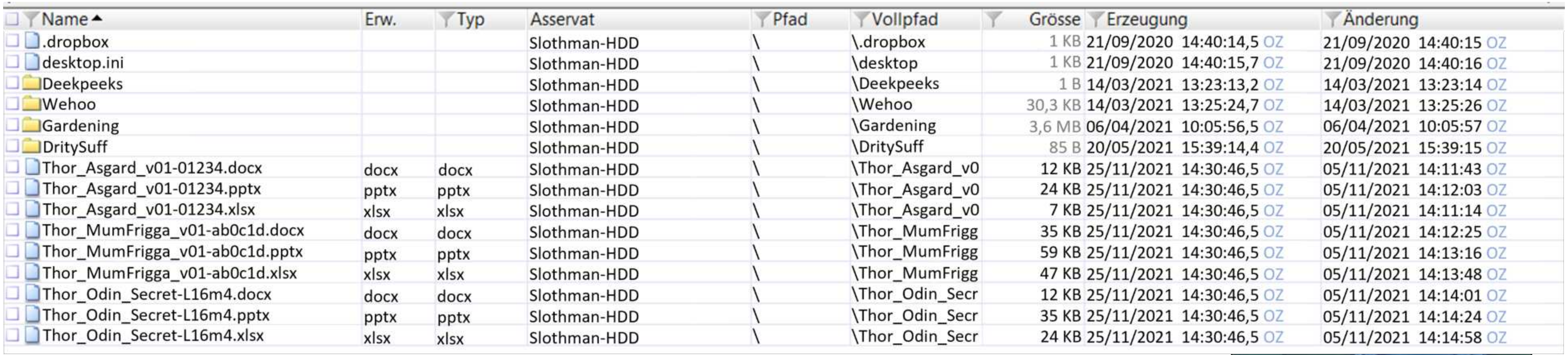
Let‘s search the Synch Folder



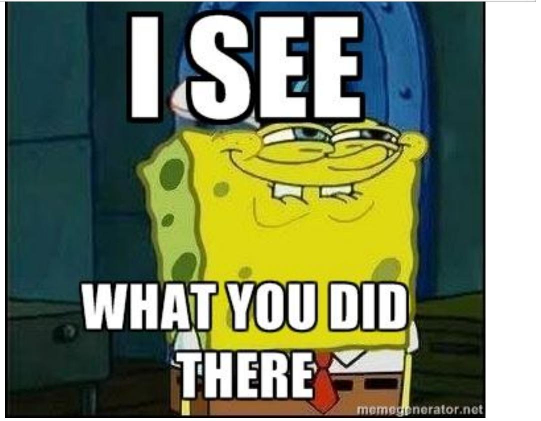
Name ▲	Erw.	Typ	Asservat	Pfad	Vollpfad	Grösse	Erzeugung	Änderung
Unknown			Slothman-HDD	\	\Unknown			
$Extend			Slothman-HDD	\	\$Extend	0,8 KB	01/01/1970 00:00:00,0 OZ	01/01/1970 00:00:00 OZ
$Recycle.Bin	Bin		Slothman-HDD	\	\$Recycle.Bin	0,9 KB	01/07/2018 10:02:19,8 OZ	26/11/2021 13:08:21 OZ
OneDriveTemp			Slothman-HDD	\	\OneDriveTemp	200 B	03/09/2018 16:18:25,3 OZ	24/08/2021 10:14:21 OZ
PerfLogs			Slothman-HDD	\	\PerfLogs	52 B	07/12/2019 10:14:20,5 OZ	07/12/2019 10:14:23 OZ
ProgramData			Slothman-HDD	\	\ProgramData	4,93 GB	07/12/2019 10:14:21,9 OZ	19/10/2021 09:33:52 OZ
Program Files			Slothman-HDD	\	\Program Files	6,01 GB	07/12/2019 10:14:23.3 OZ	28/10/2021 16:03:12 OZ
Program Files (x86)			Slothman-HDD	\	\Program Files (x	13 GB	07/12/2019 10:14:25,5 OZ	03/09/2021 08:34:47 OZ
Python27			Slothman-HDD	\	\Python27	1,5 KB	11/05/2020 12:07:39,1 OZ	11/05/2020 12:07:40 OZ
Recovery			Slothman-HDD	\	\Recovery	150 B	07/12/2019 10:15:11,8 OZ	07/12/2019 10:15:12 OZ
System Volume Information			Slothman-HDD	\	\System Volume	0 B	07/12/2019 10:18:48,5 OZ	07/12/2019 10:18:49 OZ
Temp			Slothman-HDD	\	\Temp	664 KB	07/12/2019 10:17:51,5 OZ	25/11/2021 09:17:35 OZ
Windows			Slothman-HDD	\	\Windows	38,4 GB	07/12/2019 10:14:19,7 OZ	29/10/2021 11:58:05 OZ
Nutnox.png			Slothman-HDD	\	\Nutnox	22 MB	21/09/2020 14:40:13,7 OZ	25/11/2021 14:30:46 OZ

Let's just double click on Nutnox.png…

…and see what happens



□ Name ▲	Erw.	Typ	Asservat	Pfad	Vollpfad	Grösse	Erzeugung	Änderung
□ .dropbox			Slothman-HDD	\	\.dropbox	1 KB	21/09/2020 14:40:14,5 OZ	21/09/2020 14:40:15 OZ
□ desktop.ini			Slothman-HDD	\	\desktop	1 KB	21/09/2020 14:40:15,7 OZ	21/09/2020 14:40:16 OZ
□ Deekpeeks			Slothman-HDD	\	\Deekpeeks	1 B	14/03/2021 13:23:13,2 OZ	14/03/2021 13:23:14 OZ
□ Wehoo			Slothman-HDD	\	\Wehoo	30,3 KB	14/03/2021 13:25:24,7 OZ	14/03/2021 13:25:26 OZ
□ Gardening			Slothman-HDD	\	\Gardening	3,6 MB	06/04/2021 10:05:56,5 OZ	06/04/2021 10:05:57 OZ
□ DritySuff			Slothman-HDD	\	\DritySuff	85 B	20/05/2021 15:39:14,4 OZ	20/05/2021 15:39:15 OZ
□ Thor_Asgard_v01-01234.docx	docx	docx	Slothman-HDD	\	\Thor_Asgard_v0	12 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:11:43 OZ
□ Thor_Asgard_v01-01234.pptx	pptx	pptx	Slothman-HDD	\	\Thor_Asgard_v0	24 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:12:03 OZ
□ Thor_Asgard_v01-01234.xlsx	xlsx	xlsx	Slothman-HDD	\	\Thor_Asgard_v0	7 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:11:14 OZ
□ Thor_MumFrigga_v01-ab0c1d.docx	docx	docx	Slothman-HDD	\	\Thor_MumFrigg	35 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:12:25 OZ
□ Thor_MumFrigga_v01-ab0c1d.pptx	pptx	pptx	Slothman-HDD	\	\Thor_MumFrigg	59 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:13:16 OZ
□ Thor_MumFrigga_v01-ab0c1d.xlsx	xlsx	xlsx	Slothman-HDD	\	\Thor_MumFrigg	47 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:13:48 OZ
□ Thor_Odin_Secret-L16m4.docx	docx	docx	Slothman-HDD	\	\Thor_Odin_Secr	12 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:14:01 OZ
□ Thor_Odin_Secret-L16m4.pptx	pptx	pptx	Slothman-HDD	\	\Thor_Odin_Secr	35 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:14:24 OZ
□ Thor_Odin_Secret-L16m4.xlsx	xlsx	xlsx	Slothman-HDD	\	\Thor_Odin_Secr	24 KB	25/11/2021 14:30:46,5 OZ	05/11/2021 14:14:58 OZ



Project – done

- Report will be delivered (Gutachten)
  - With evidence
- The judge/lawyer will contact you most probably very often
- Data has to be stored for a longer period of time

This is the End ;(

Nina Azimikhah, MSc
Senior Cyber Security Analyst & Threat Intel Lead
Cyber Defense Center

K-BusinessCom AG (ehm. Kapsch)
Wienerbergstraße 53
1120 Wien | Österreich

Nina.Azimikhah@k-business.com
www.kapsch.net

Gideon Teubert, MSc
Senior Cyber Security Analyst & Incident Response Lead
Cyber Defense Center

K-BusinessCom AG (ehm. Kapsch)
Wienerbergstraße 53
1120 Wien | Österreich

Gideon.Teubert@k-business.com
www.kapsch.net