
K-Businesscom
// we transform for the better

Puh, schon wieder ein Incident Response Talk? Absolutely!!!111

- *Gideon Teubert, MSc*
- *Senior Analyst, Incident Response Lead*
- *K-BusinessCom AG*

K-Businesscom

Whoami

```
\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
```


Talk GOAL

Get a better understanding about the Austrian cyber security landscape.

Accomplished by providing excerpts of abnormal Attacker Techniques seen at our Austrian incident response encounters.

Agenda

1. Introduction
2. Typical Attack
3. Untypical Attacker Techniques spotted in AT
    1. The Beginner Stuff
    2. The Advanced Stuff
    3. The Pro Stuff
    4. Add. Ransomware
4. Conclusio

Incident Response

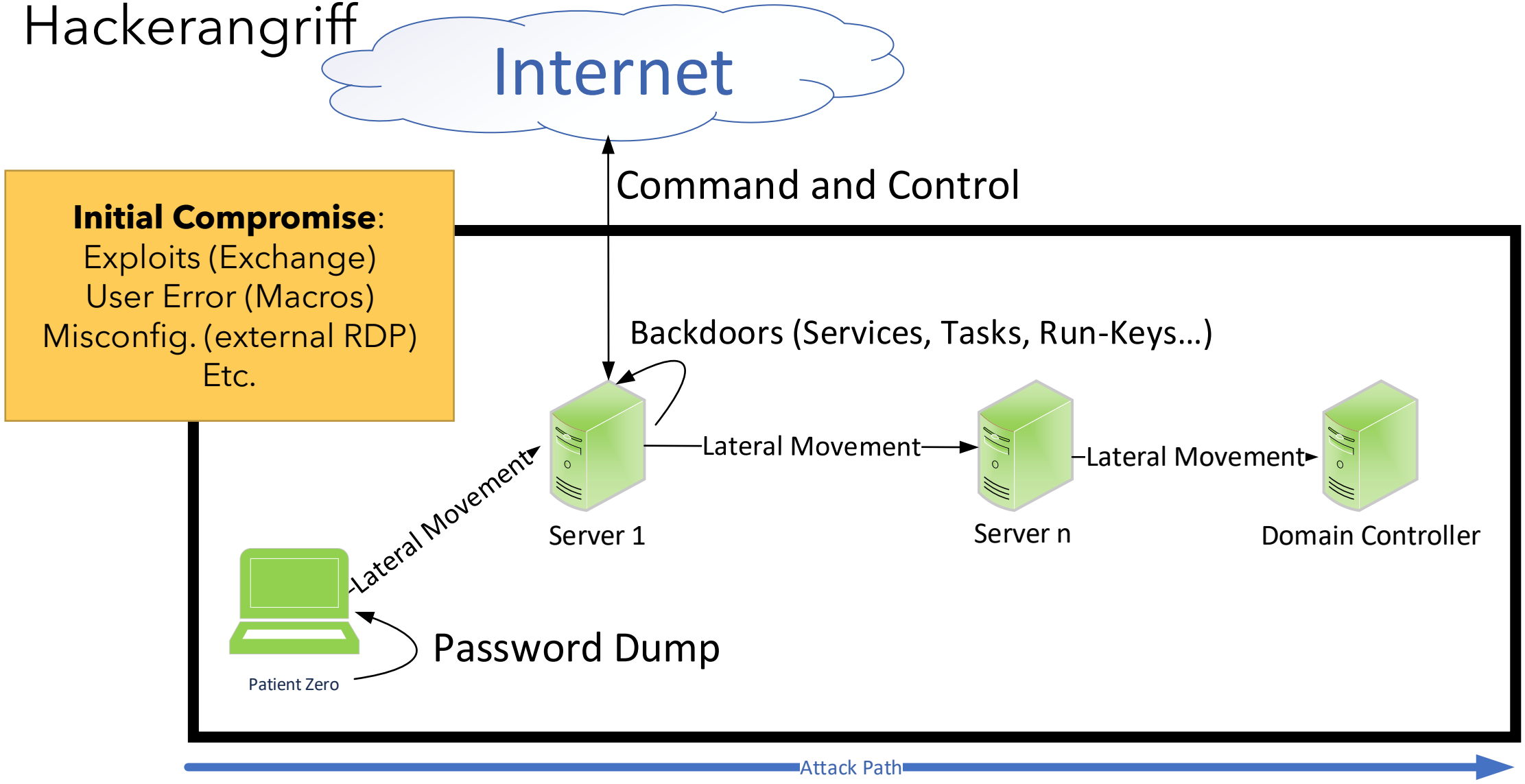
Addressing the aftermath of a security breach / attack to varying degrees.

The fire department of cyber security.

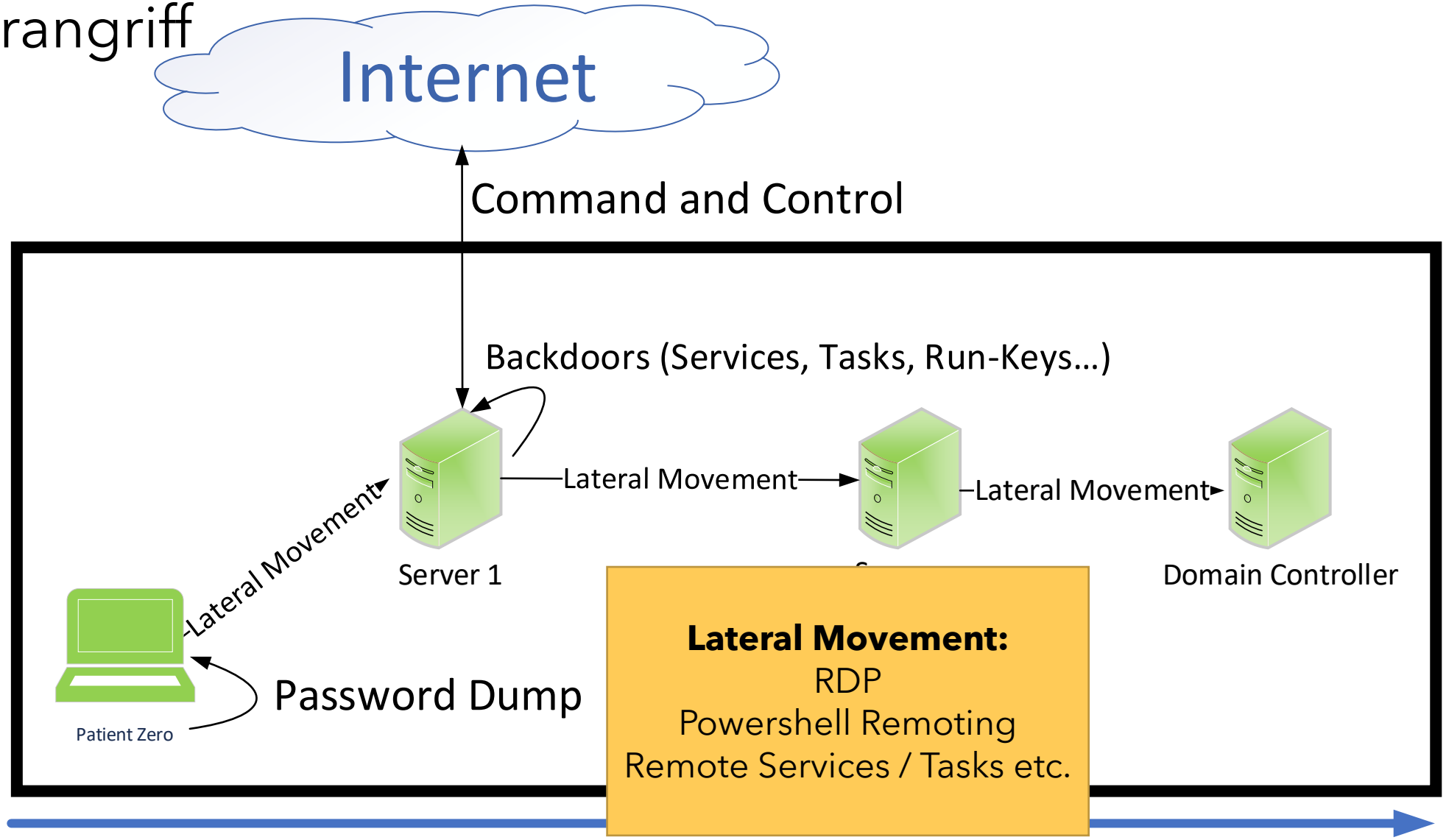
Der typische 0815 Angriff

K-Business.com

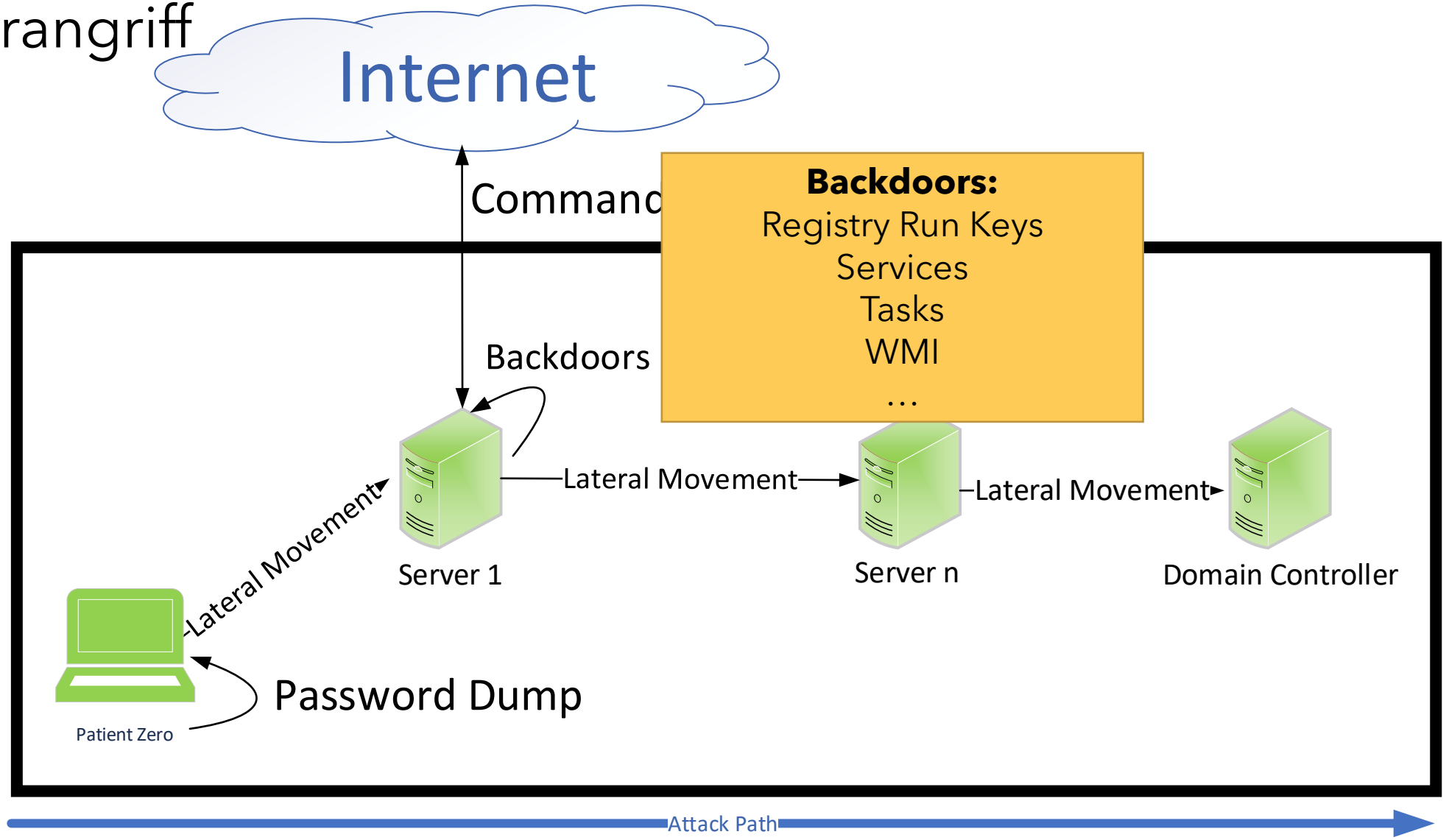
Hackerangriff



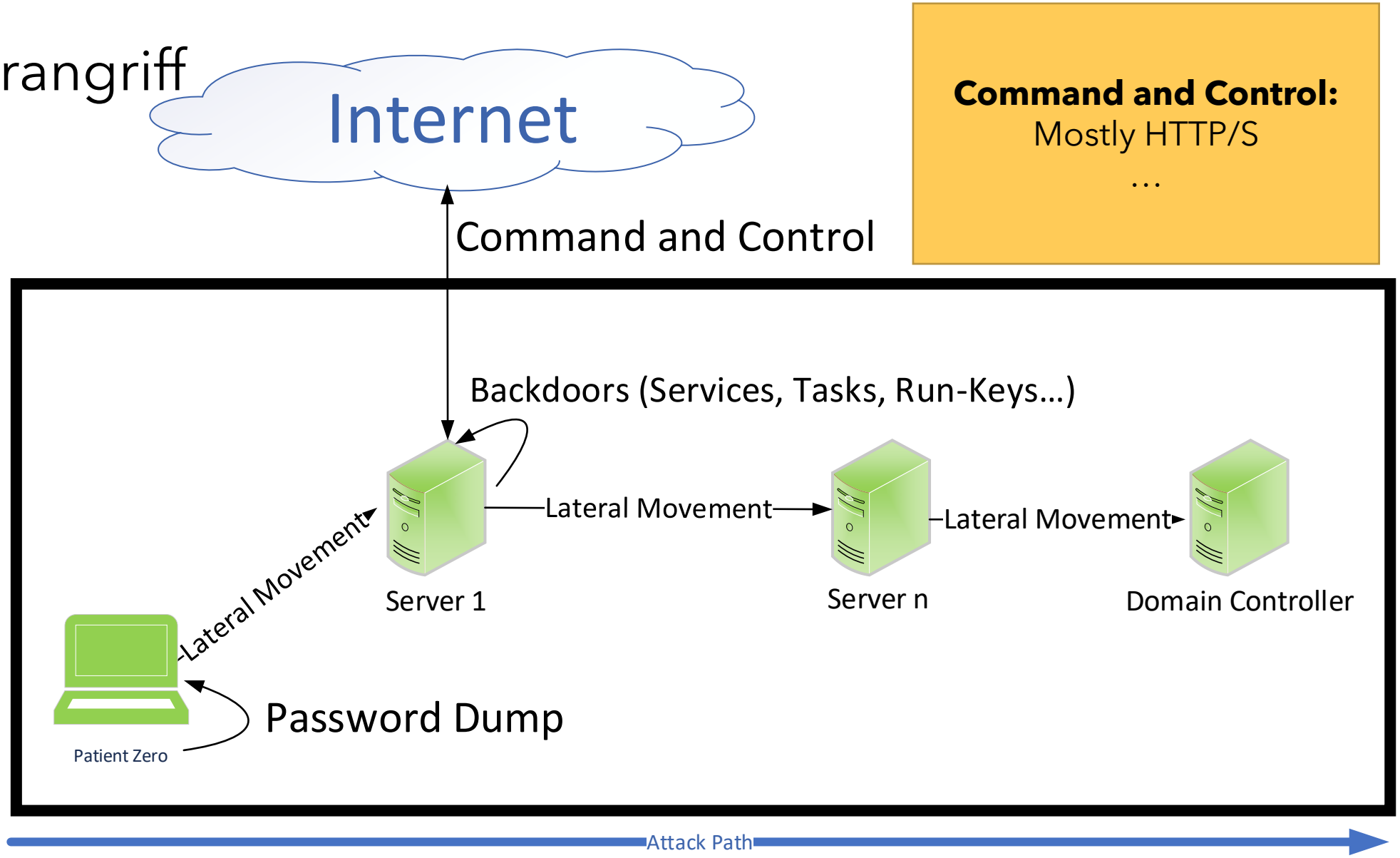
Hackerangriff



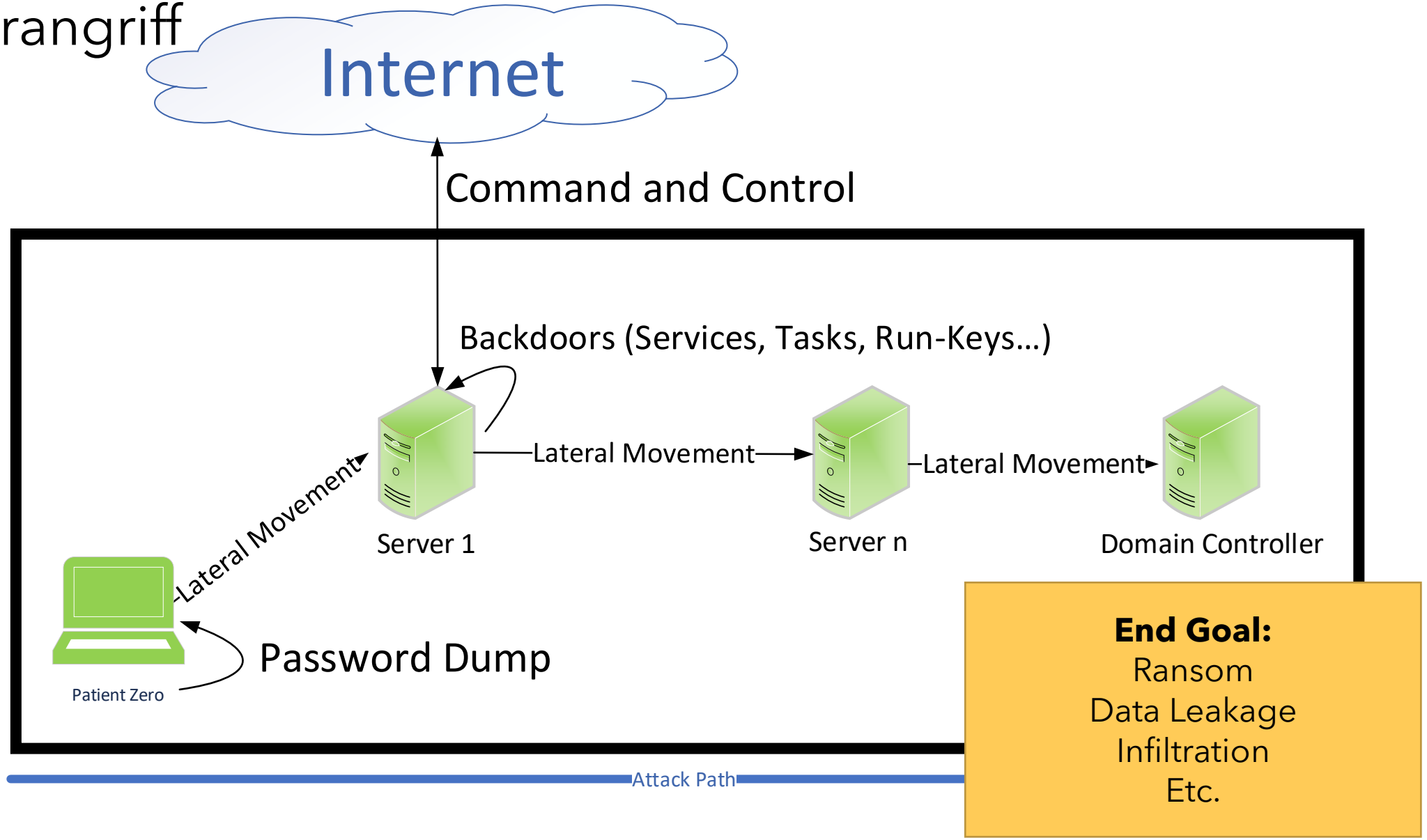
Hackerangriff



Hackerangriff



Hackerangriff



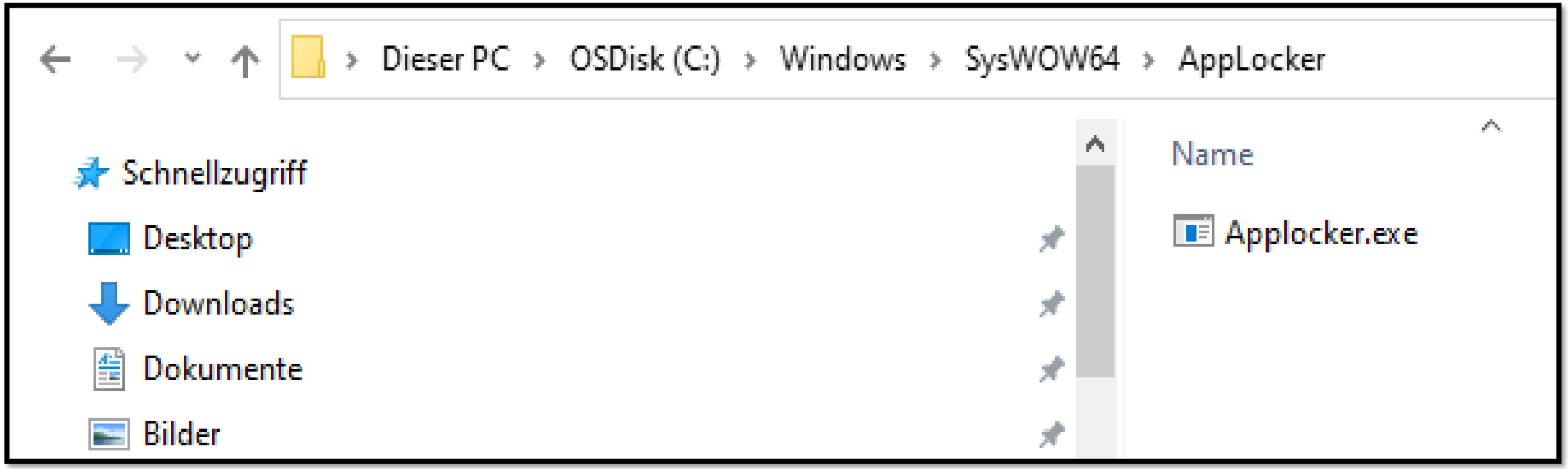
Uncommon Attacker Techniques spotted in the Wild

K-Business.com

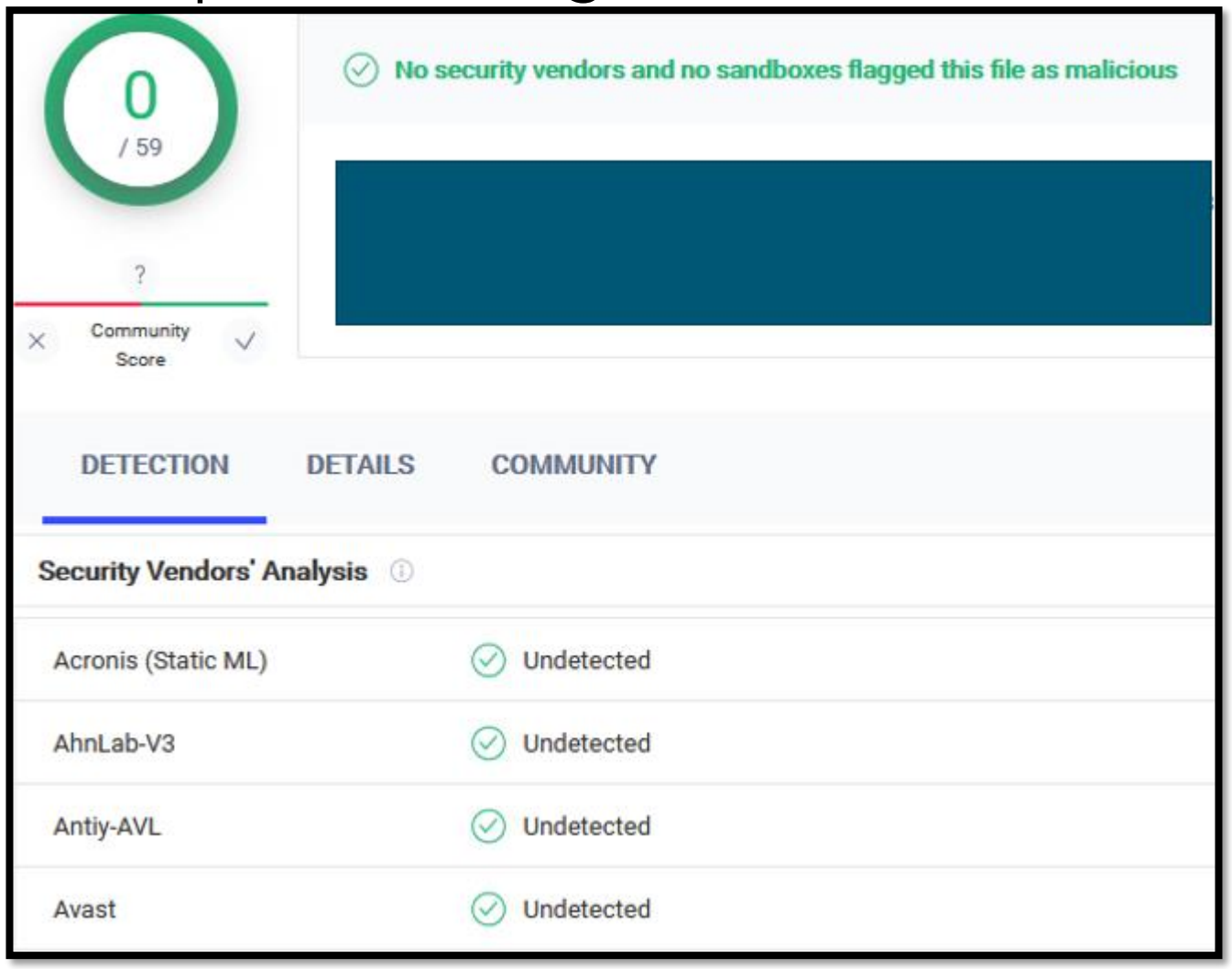
The Beginner Stuff

What is Evasion?

„Evasion = Evading something“ (e.g. Detection)

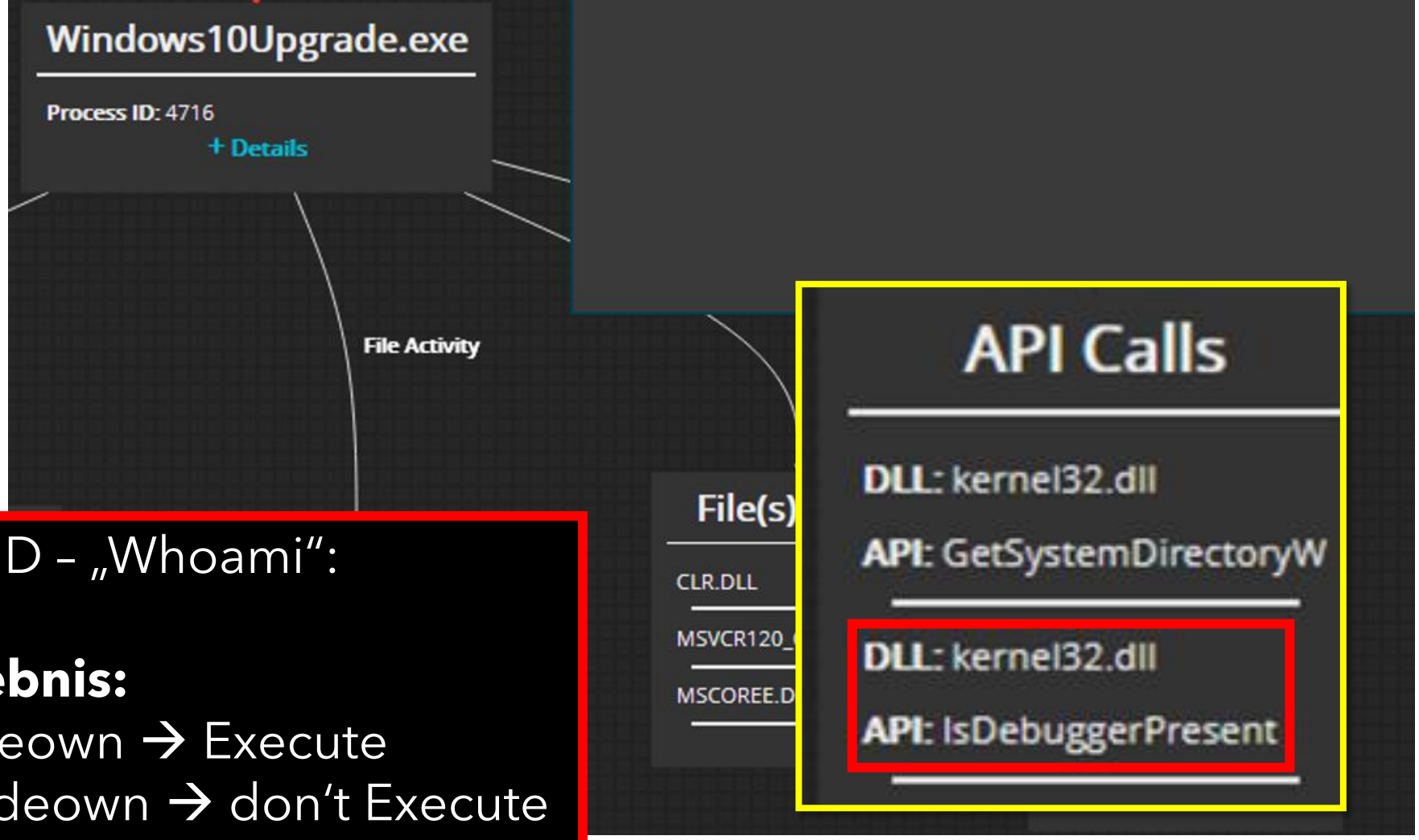


Compile Time right before delivering



// Puh, schon wieder ein Incident Response Talk? Absolutely!!!111

Sandbox Evasion I



Malware - CMD – „Whoami“:

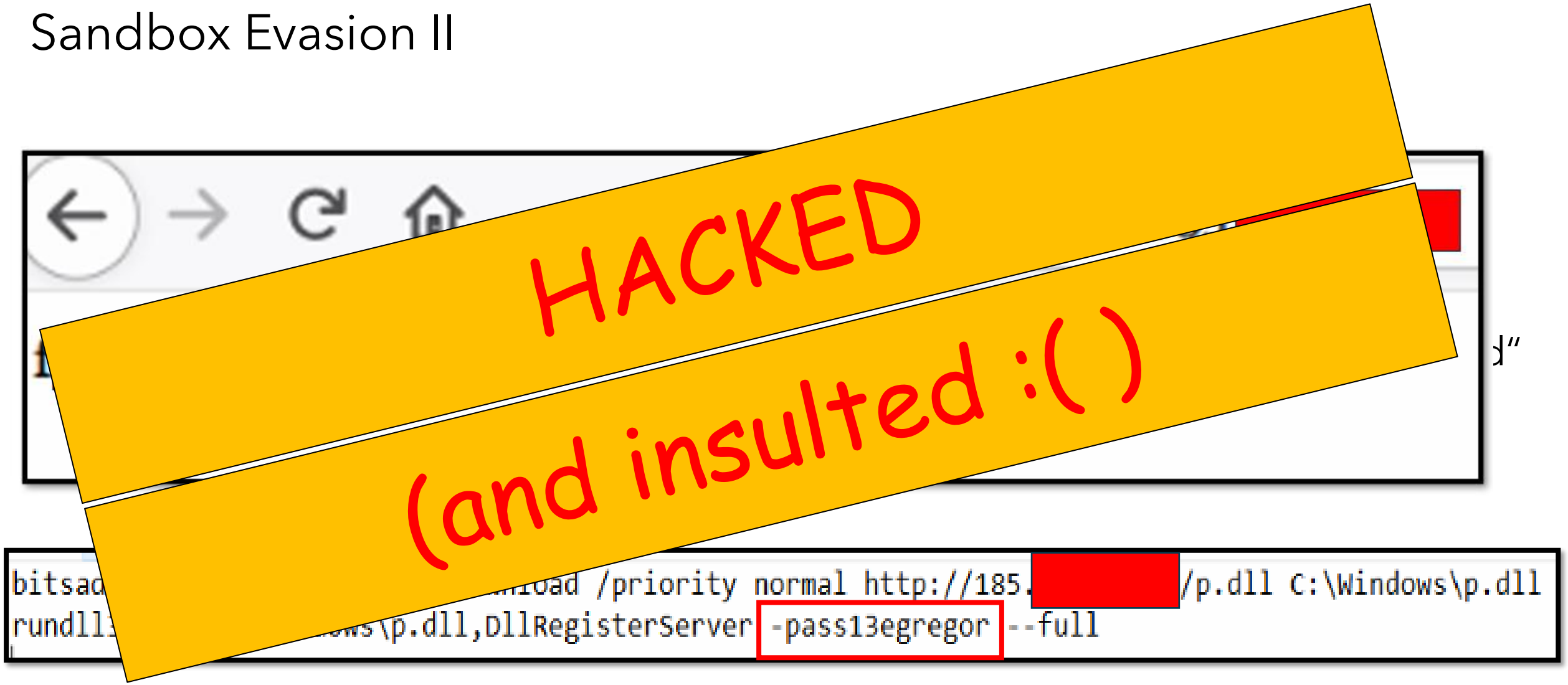
Ergebnis:

a) [domain]\gideown → Execute

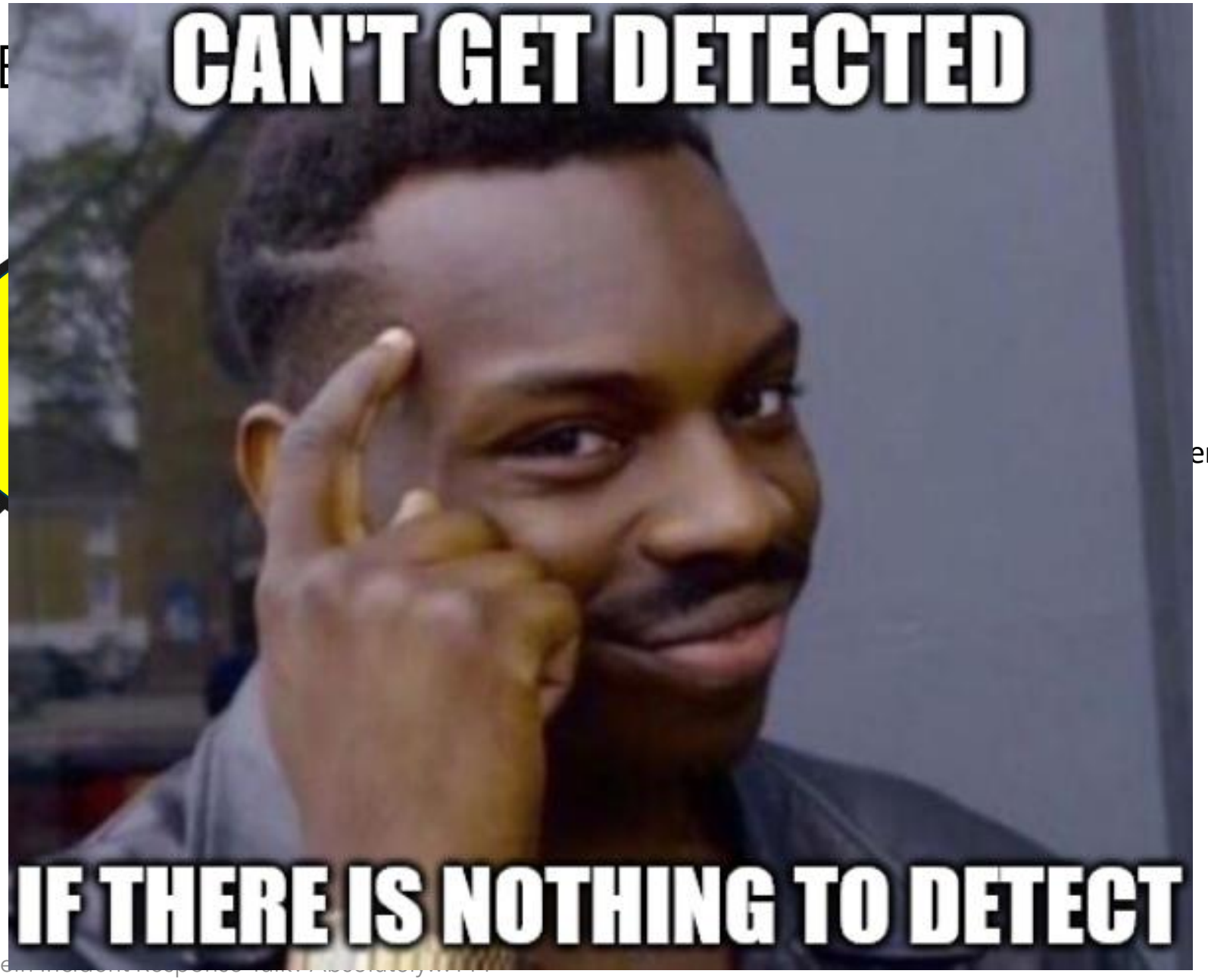
b) [computername]\gideown → don‘t Execute

Does your sandbox have a domain?
Does your company?

Sandbox Evasion II

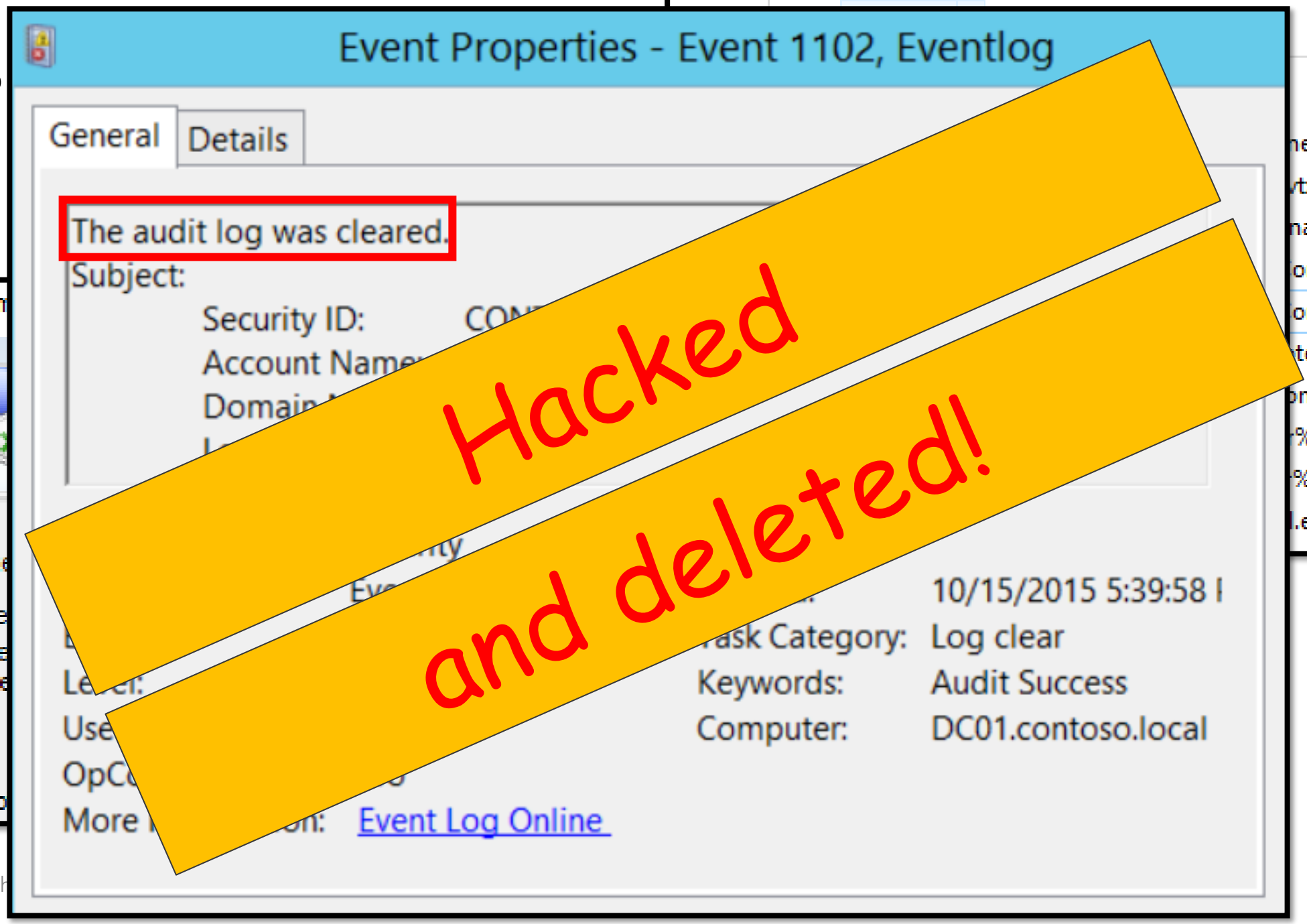


Next level E



er

RDP


Event Properties - Event 1102, Eventlog
General
Details
The audit log was cleared.
Subject:
Security ID:
Account Name:
Domain
Logged:
10/15/2015 5:39:58 I
Task Category:
Log clear
Keywords:
Audit Success
Computer:
DC01.contoso.local
Event Log Online
Hacked
and deleted!

Registry for the Rescue

NTUser.dat of compromised User (RDP Source):

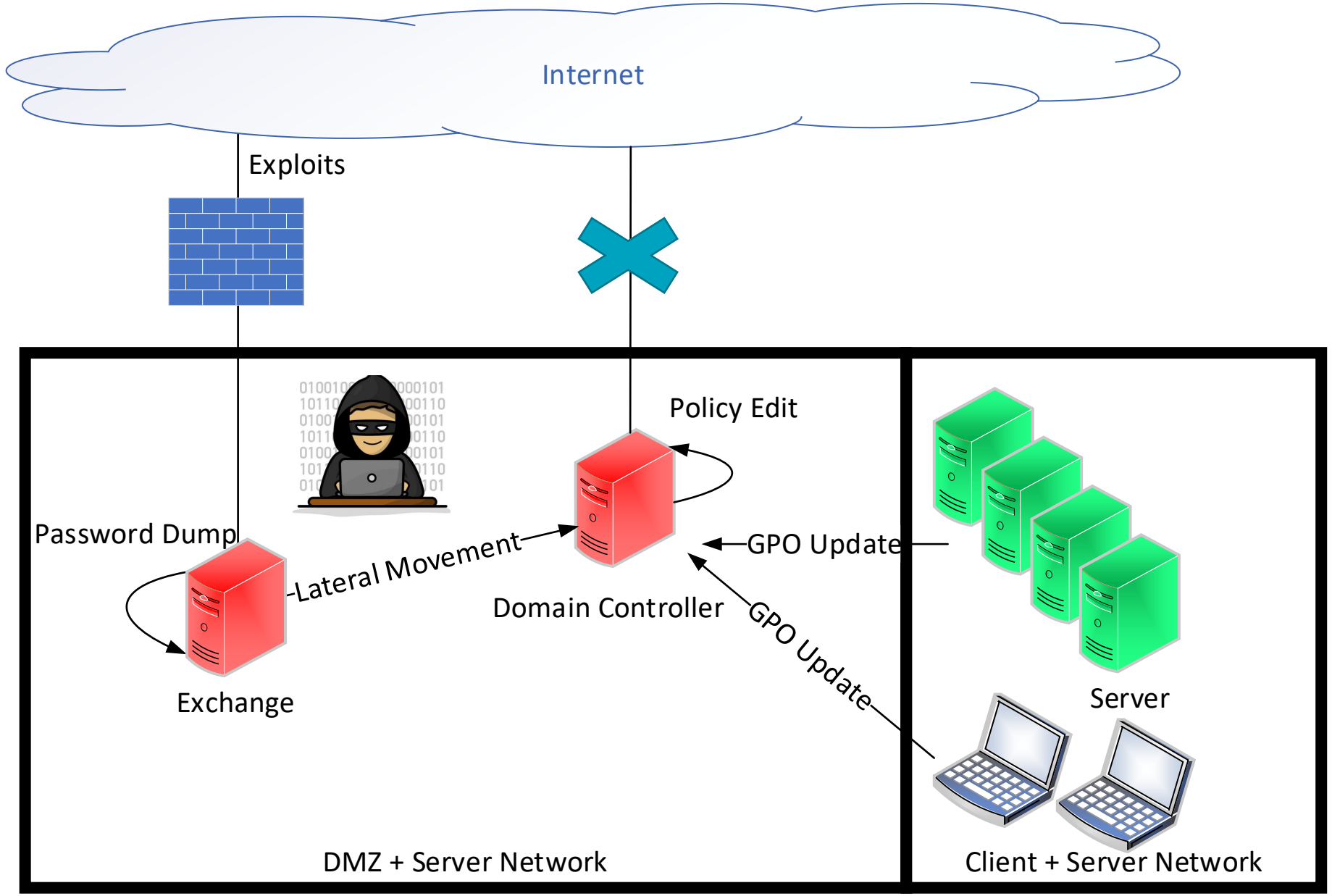
1. RDP Destination
2. Usernames
3. Last Session

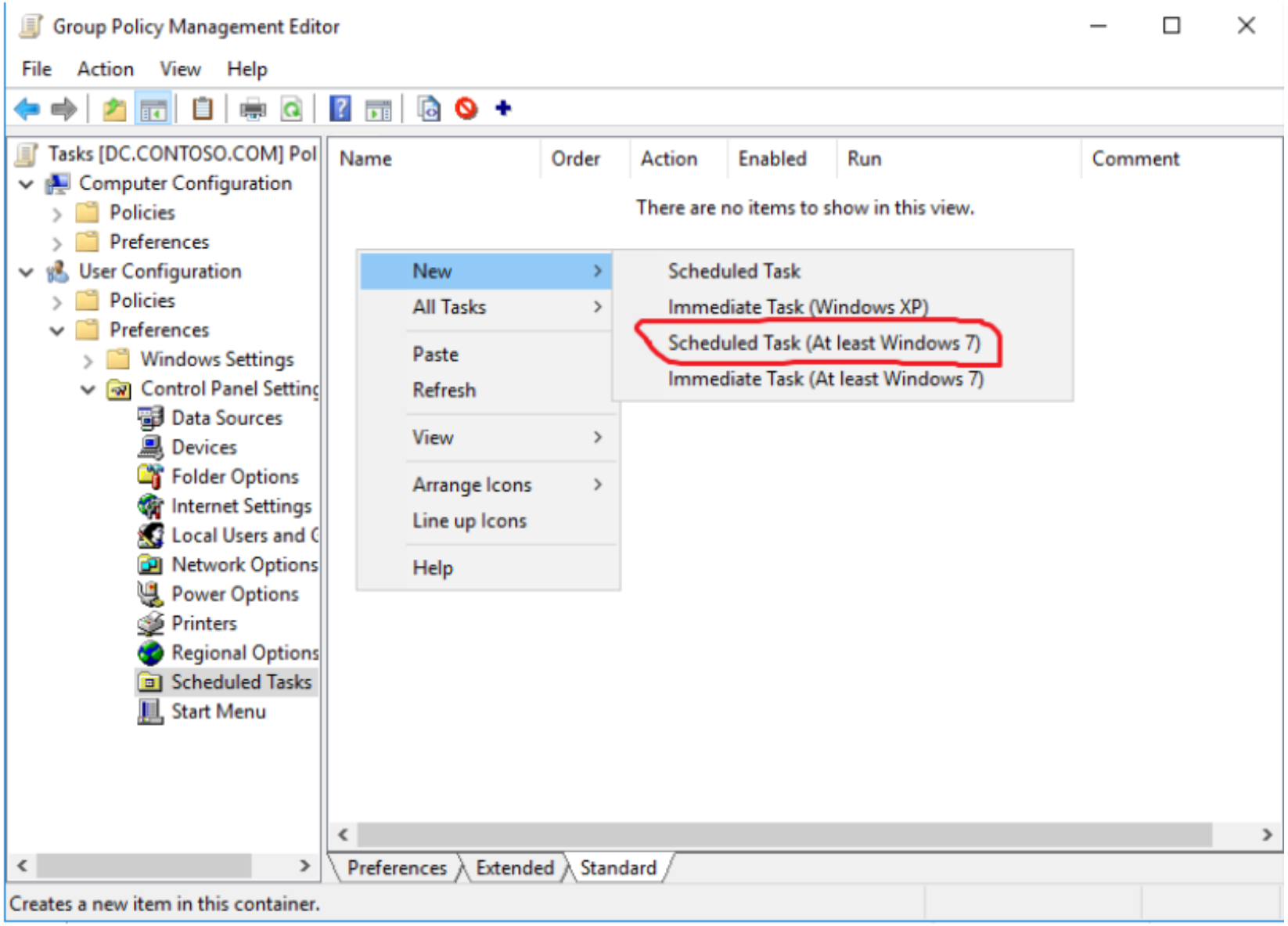
Host Name	Username	Last Modified
148.	\user 1	2021-08-04 13:00:44
172.	user 1	2021-12-21 09:18:01
172.		2021-10-14 13:27:38
172.		2022-03-30 09:38:19
172.		2022-04-06 10:50:44
172.		2022-04-08 10:56:03
172.		2022-03-30 08:25:17
192.	AD\Administrator	2022-04-20 13:13:52

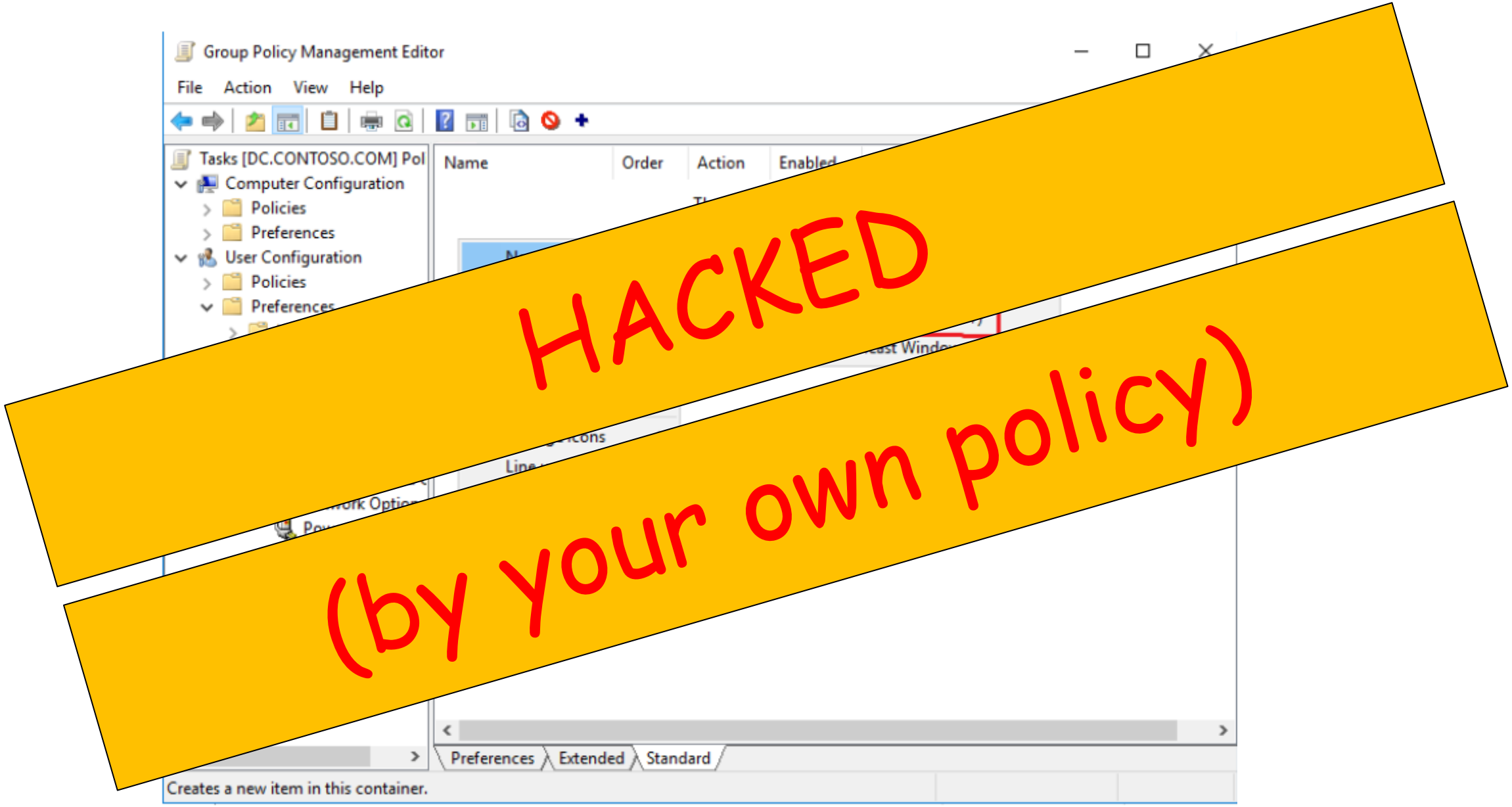
The Advanced Stuff

Uncommon Backdoors

When your DC turns against you


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


Group Policy Management Editor
File Action View Help
Tasks [DC.CONTOSO.COM] Pol
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Windows Settings
Control Panel Setting
Data Sources
Devices
Folder Options
Internet Settings
Local Users and G
Network Options
Power Options
Printers
Regional Options
Scheduled Tasks
Start Menu
Name
Order
Action
Enabled
Run
Comment
There are no items to show in this view.
New
All Tasks
Paste
Refresh
View
Arrange Icons
Line up Icons
Help
Scheduled Task
Immediate Task (Windows XP)
Scheduled Task (At least Windows 7)
Immediate Task (At least Windows 7)
Preferences
Extended
Standard
Creates a new item in this container.

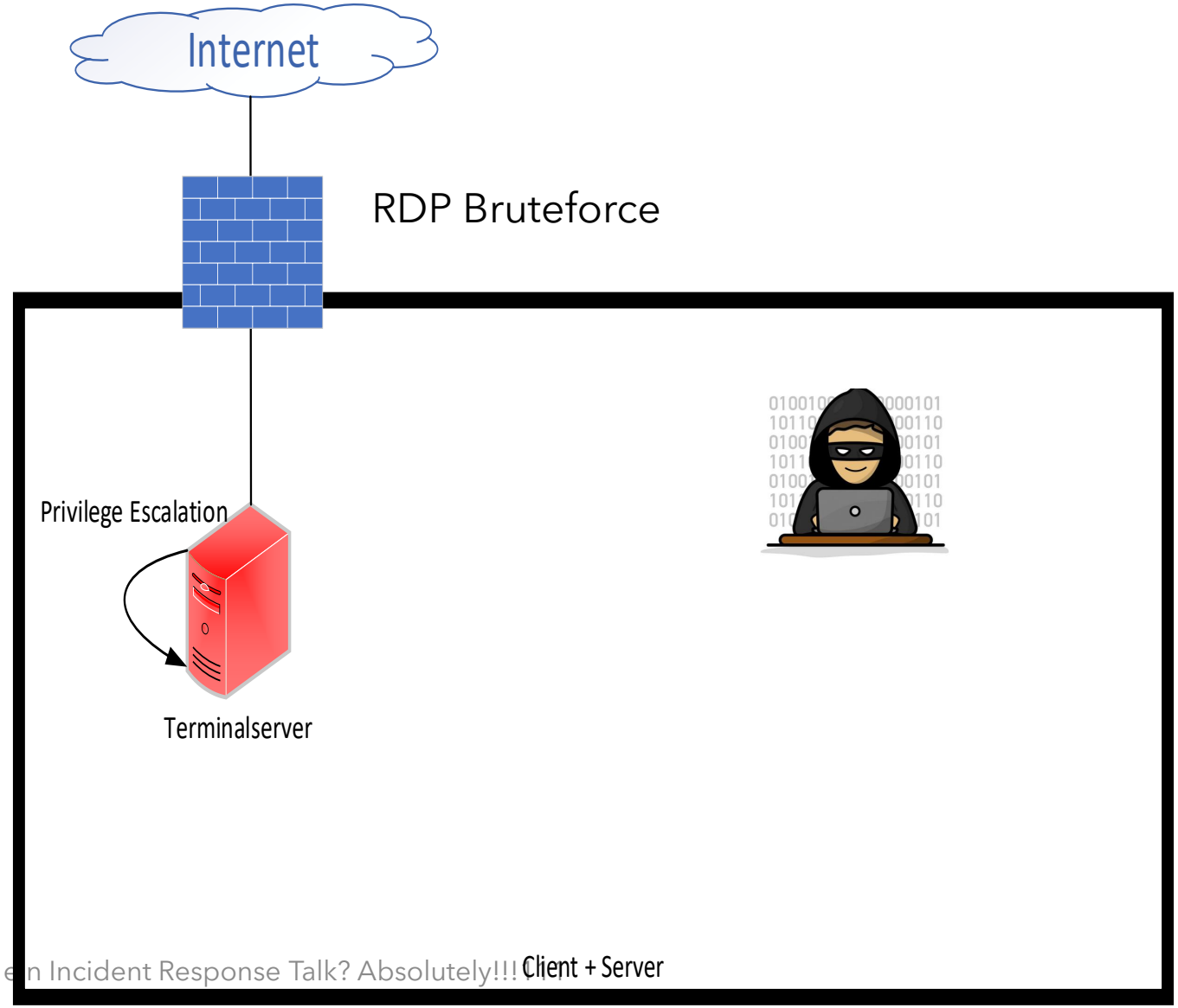

Group Policy Management Editor
File Action View Help
Tasks [DC.CONTOSO.COM] Pol
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Name
Order
Action
Enabled
Preferences
Extended
Standard
Creates a new item in this container.
HACKED
(by your own policy)

Uncommon Backdoors

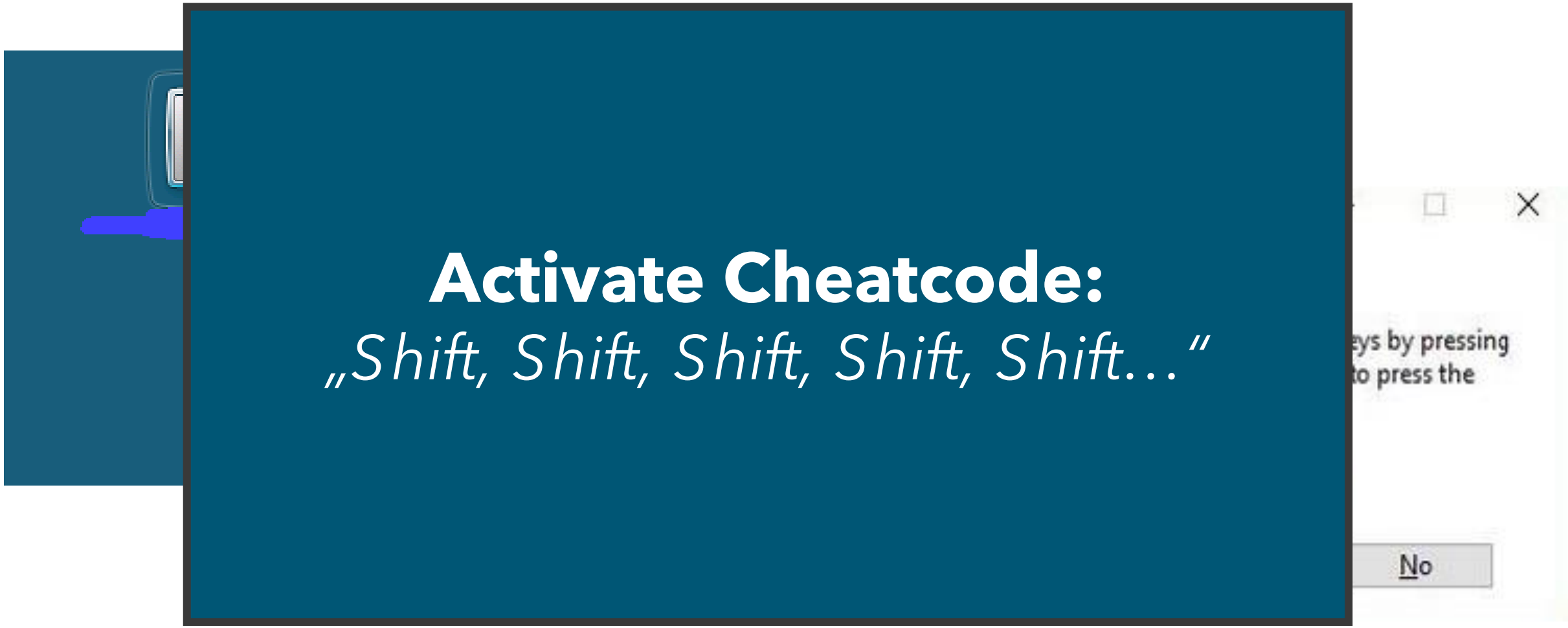
Cheatcode: press shift 5 times, hack a company

#OnDemand Backdoor

Cheatcode: press shift 5 times



Cheatcode: press shift 5 times



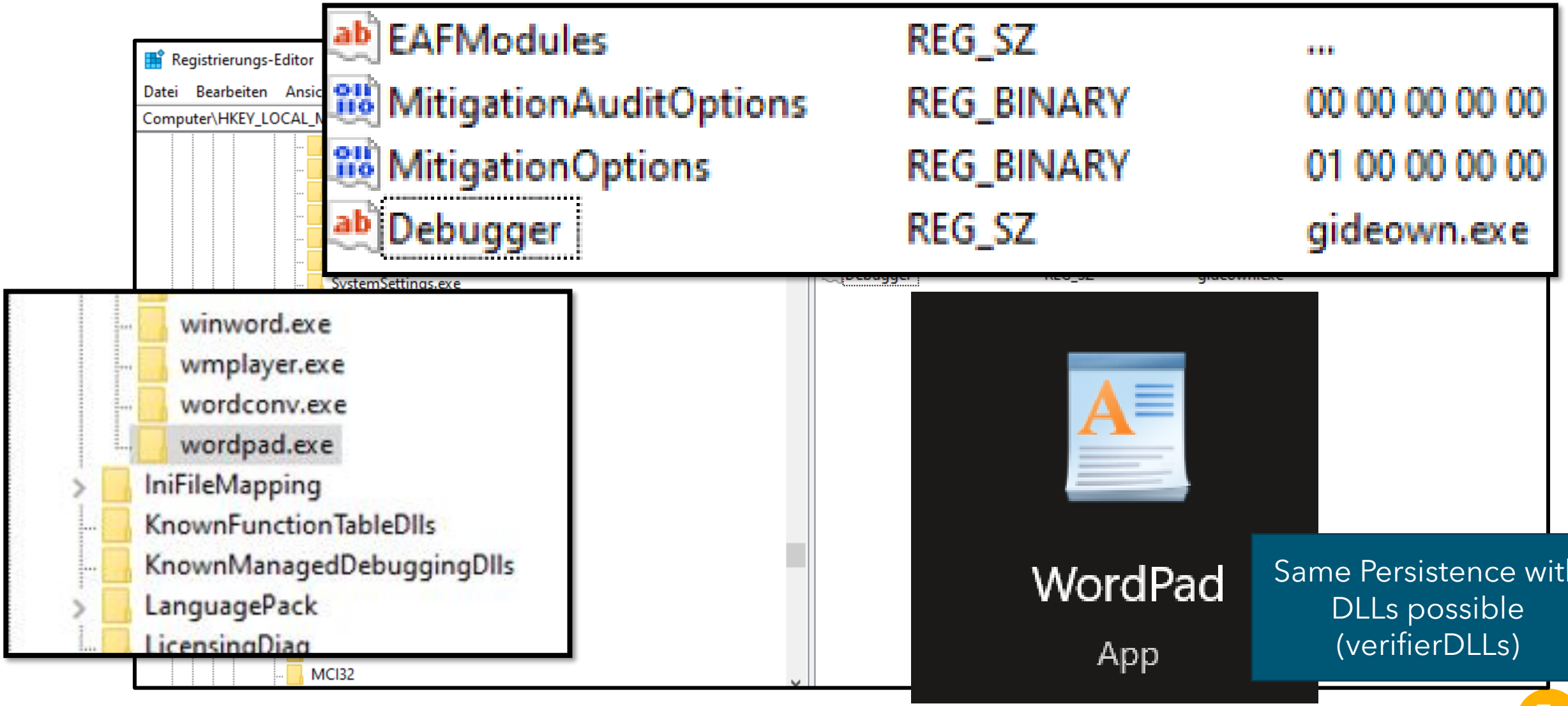
Cheatcode: press shift 5 times

The Pro Stuff

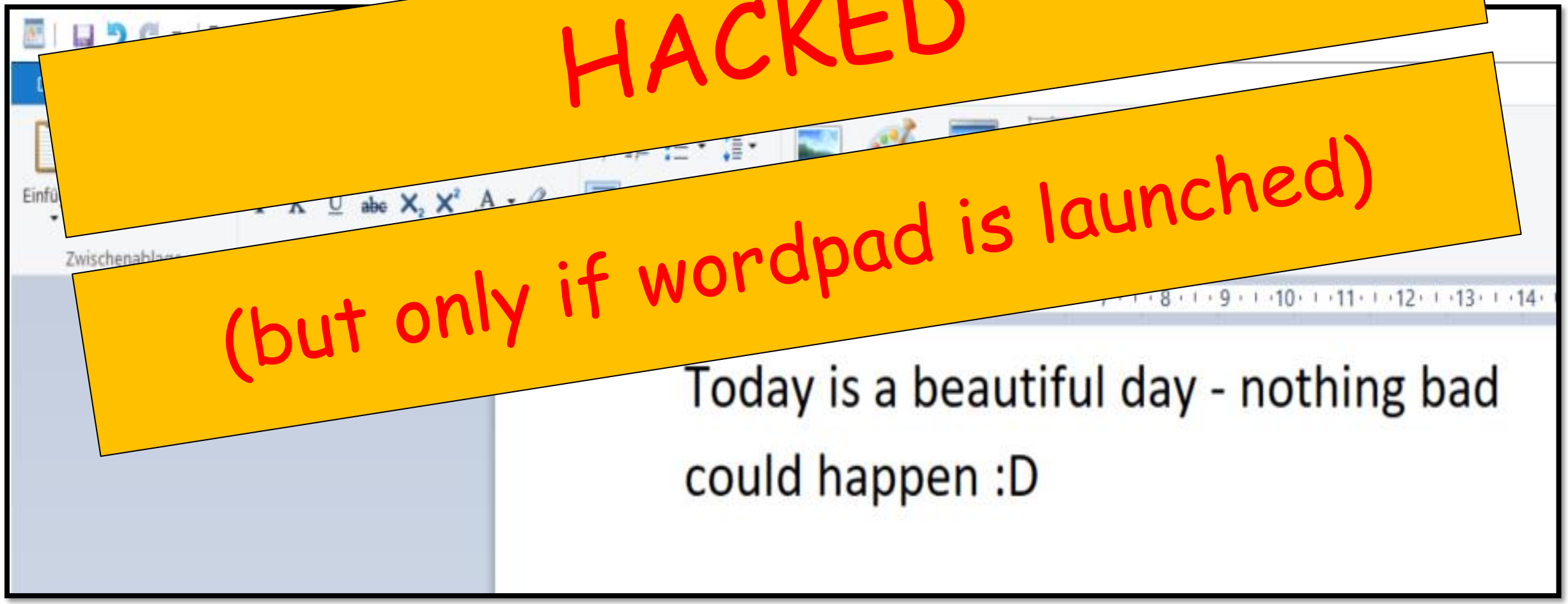
Uncommon Backdoors

Wordpad – what are you doing?!

Wordpad – what are you doing?!



Wordpad – what are you doing?!



Wordpad – what are you doing?!

HACKED

(but only if wordpad i

Today is a bea

The attacker still waiting…

Would you have found it?

Credit to my colleague Erwin Friedl

Uncommon Backdoors

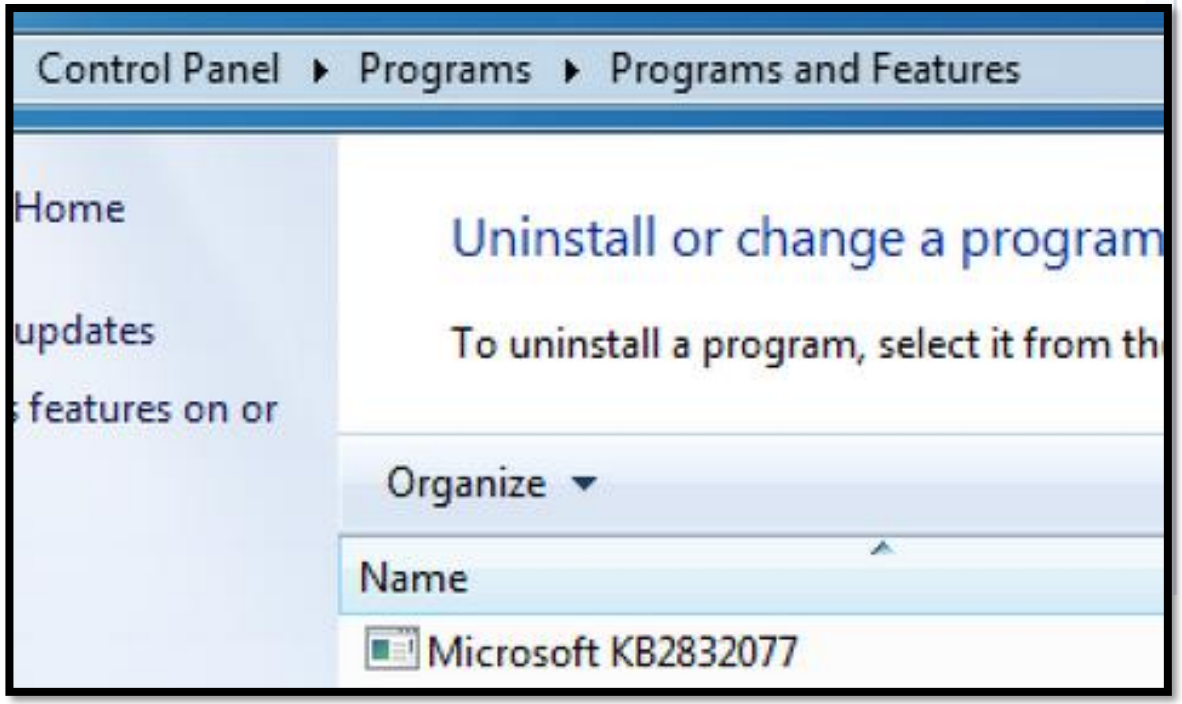
Customer: ***Thank you for patching!***

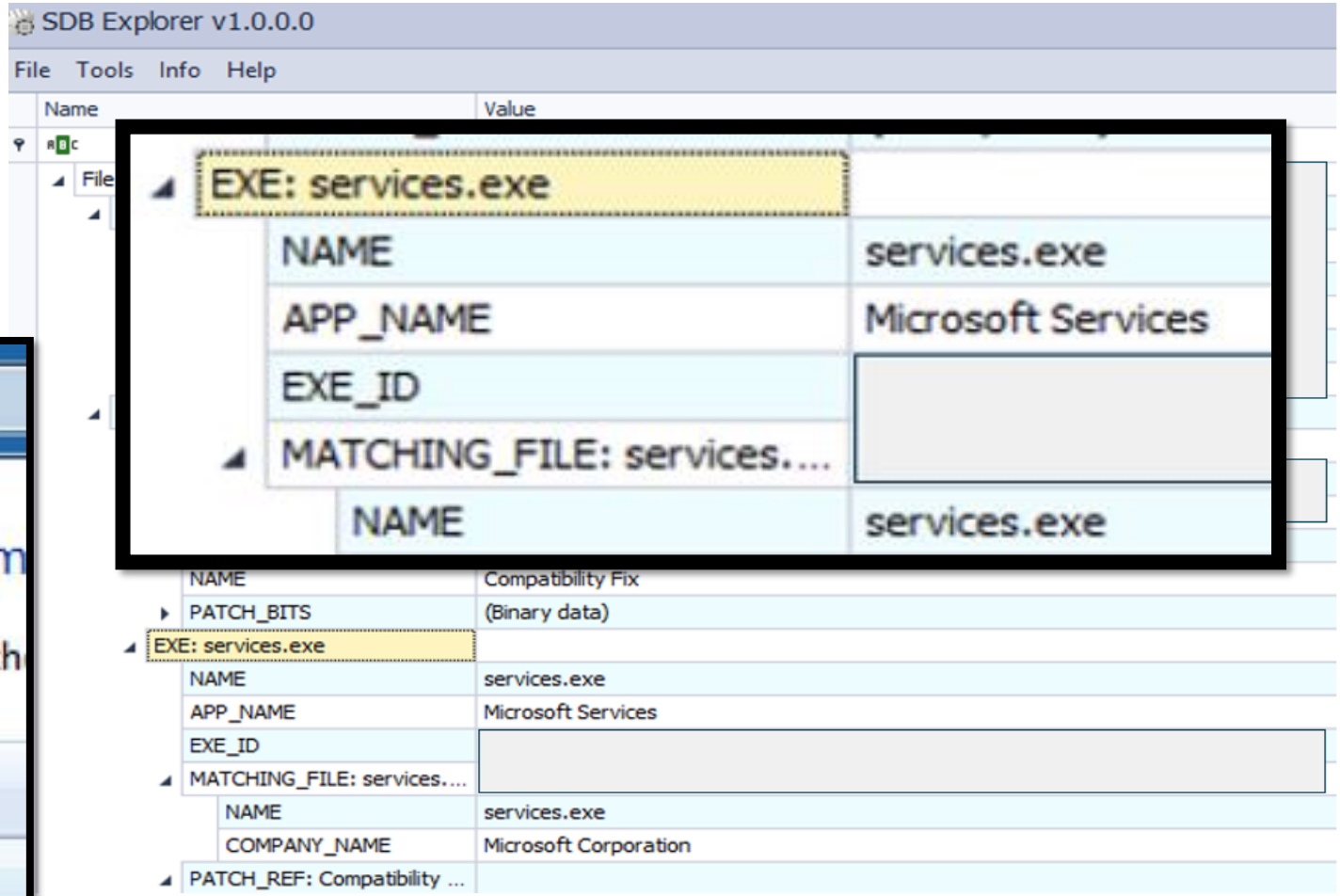
Attacker: ***No problem bro!***

Customer: ***Wait what?!***

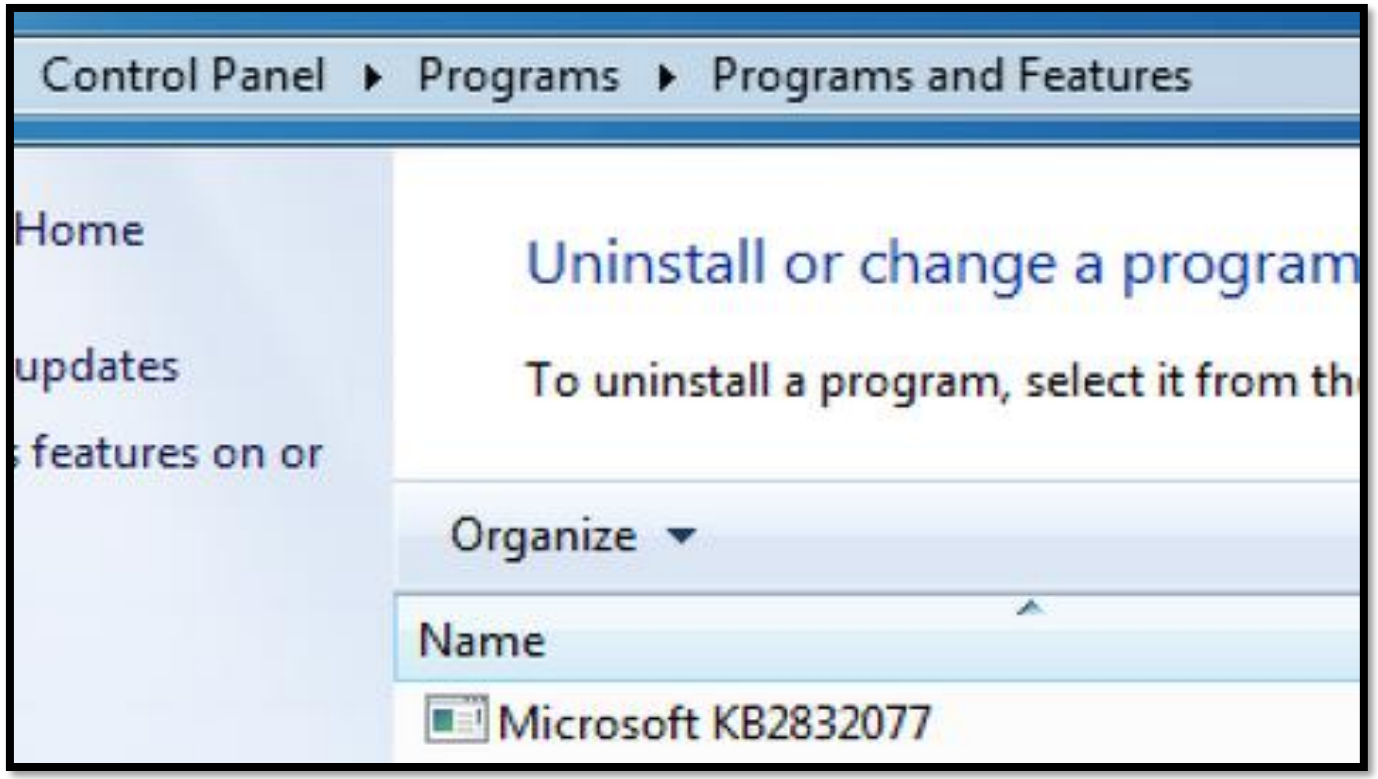
Shimcache Persistence

- PATH:
  - C:\windows\apppatch\custom\custom64\{random-ID}.sdb





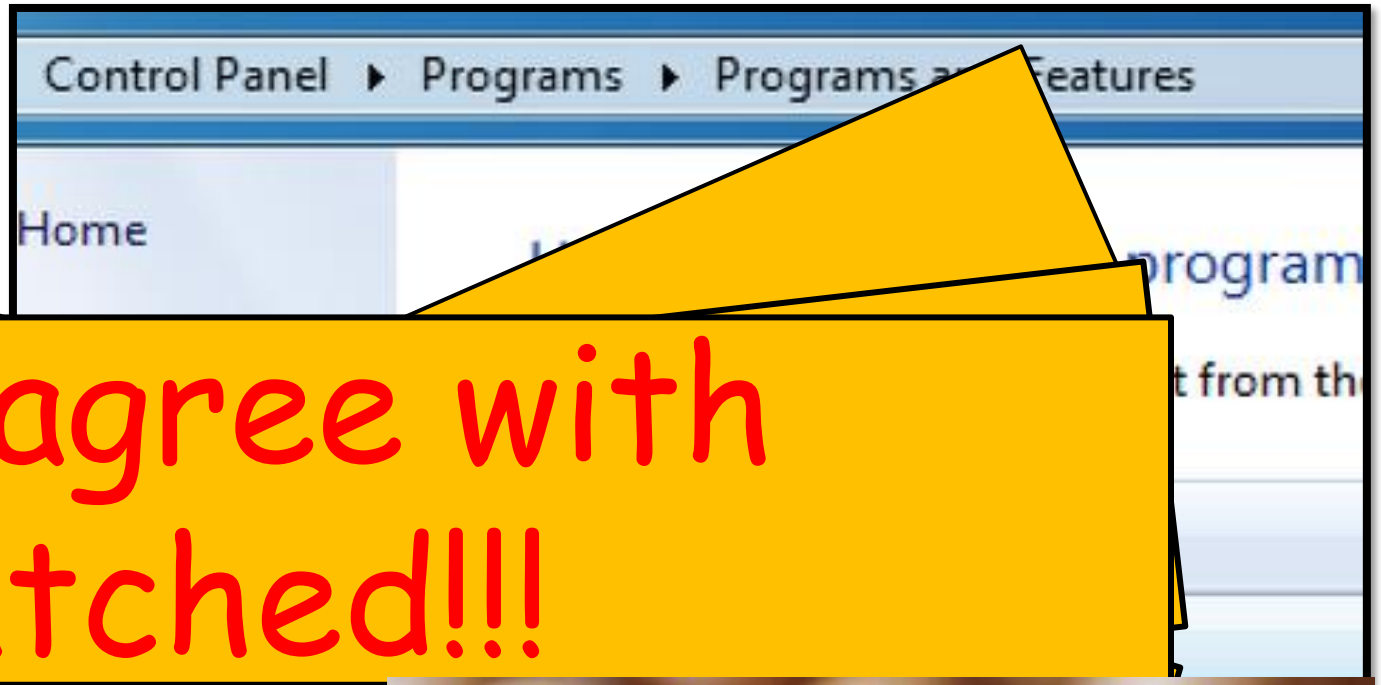
Shimcache Persistence



Side-Facts:

1. Patch for the legitimate service.exe
2. Nomenclature equals windows patches – *KB[Number]*
3. Backdoor when services.exe is started (aka always)
4. Payload hidden in registry
5. Installed on 5 of 4000 Systems to prevent detection / remediation
6. Attacker was dormant for 3-4 months

Shimcache [illegible]istence



Lets agree with hatched!!!

Side-Facts:

1. Patch for [illegible]
2. Nomenclatu[illegible]ies – *KB[Num*
3. Backdoor whe[illegible]s started (aka always
4. Payload hidden [illegible]gistry
5. Installed on 5 of 4000 Systems to prevent detecti[illegible]
6. Attacker was dormant for 3-4 months

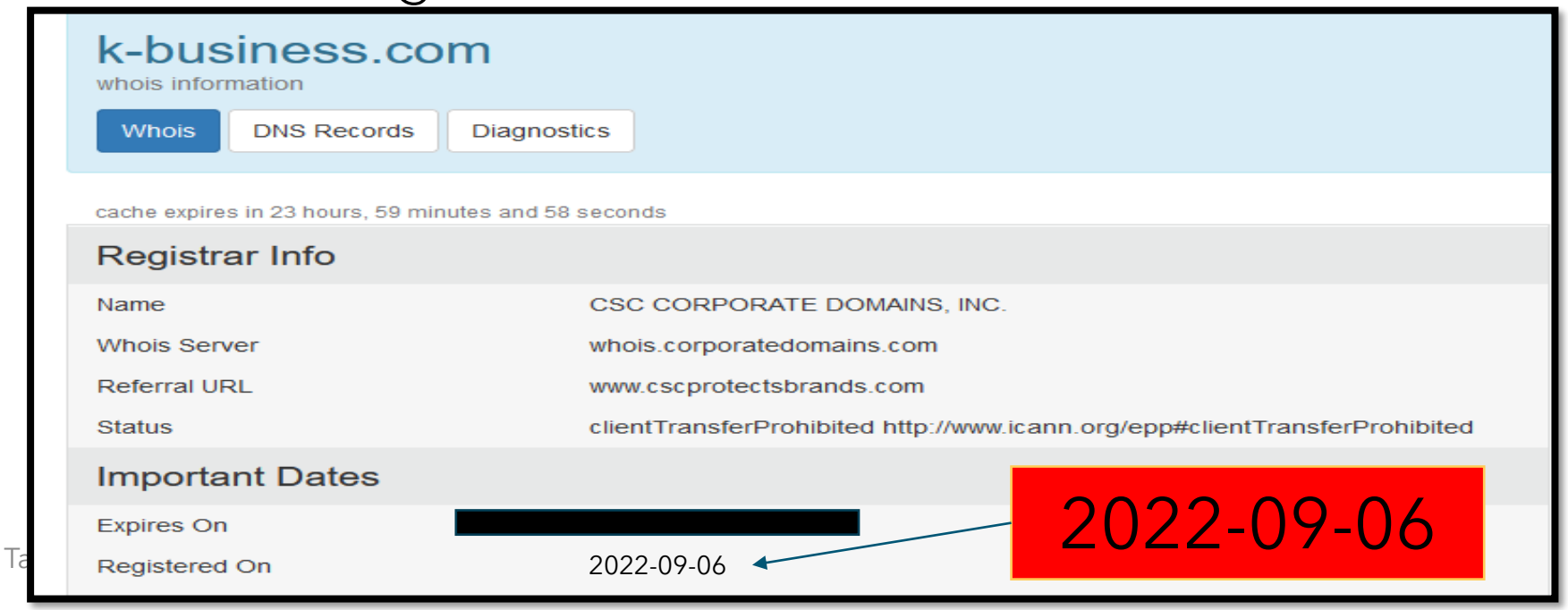
// Puh, schon wieder ein Incident Response Talk? Absolutely!!!111

Baby Domains

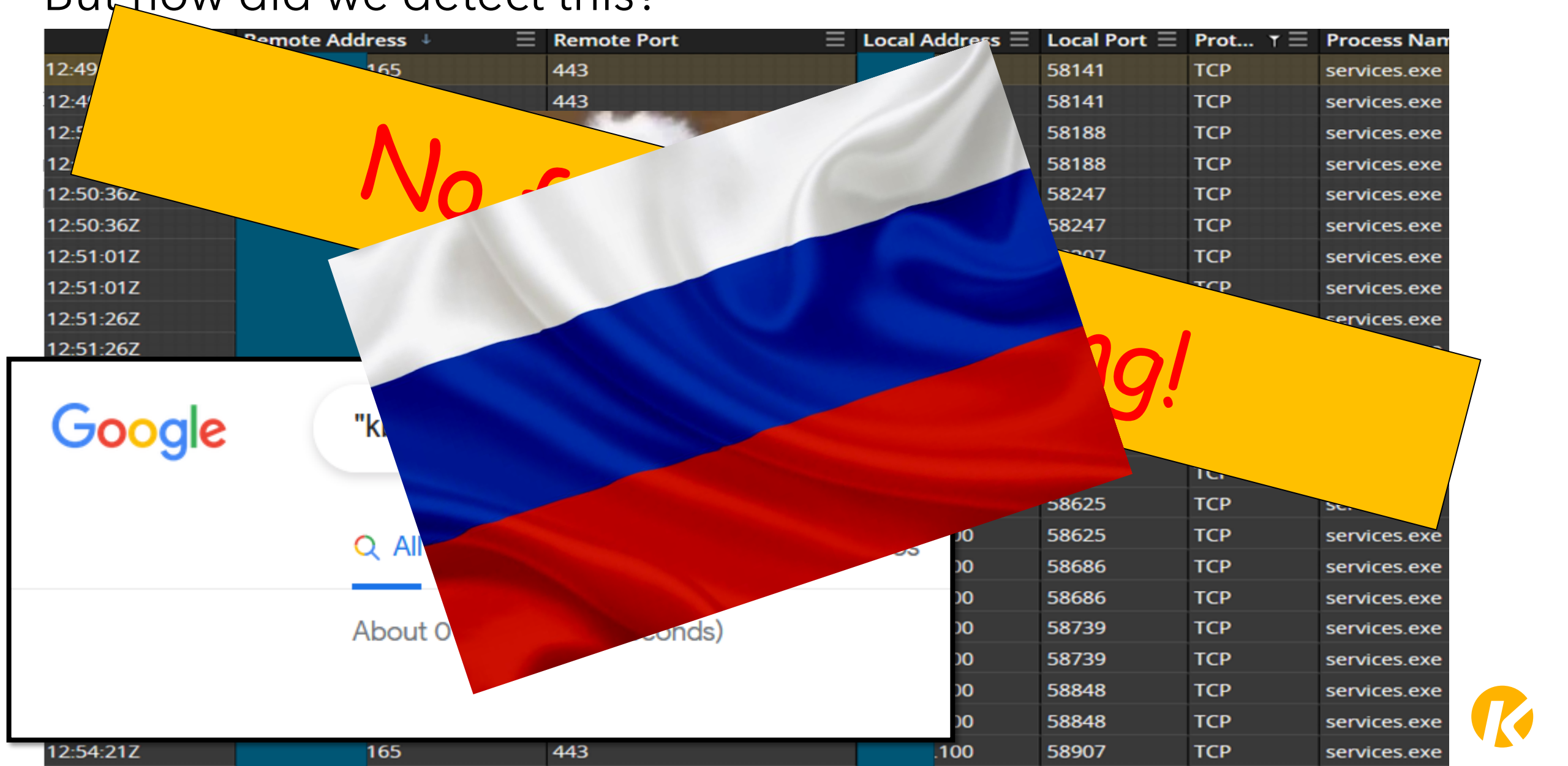
Sample malicious domain:
(Do not access)

microsoft-live-us[.]com

- 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



But how did we detect this?



Add Ransomware

K-Business.com

Ransomware – I think u missed something ?

BianLian Ransomware

- „New Ransomware“ ~ August 22
- Relies on Living-off-the-Land Tools

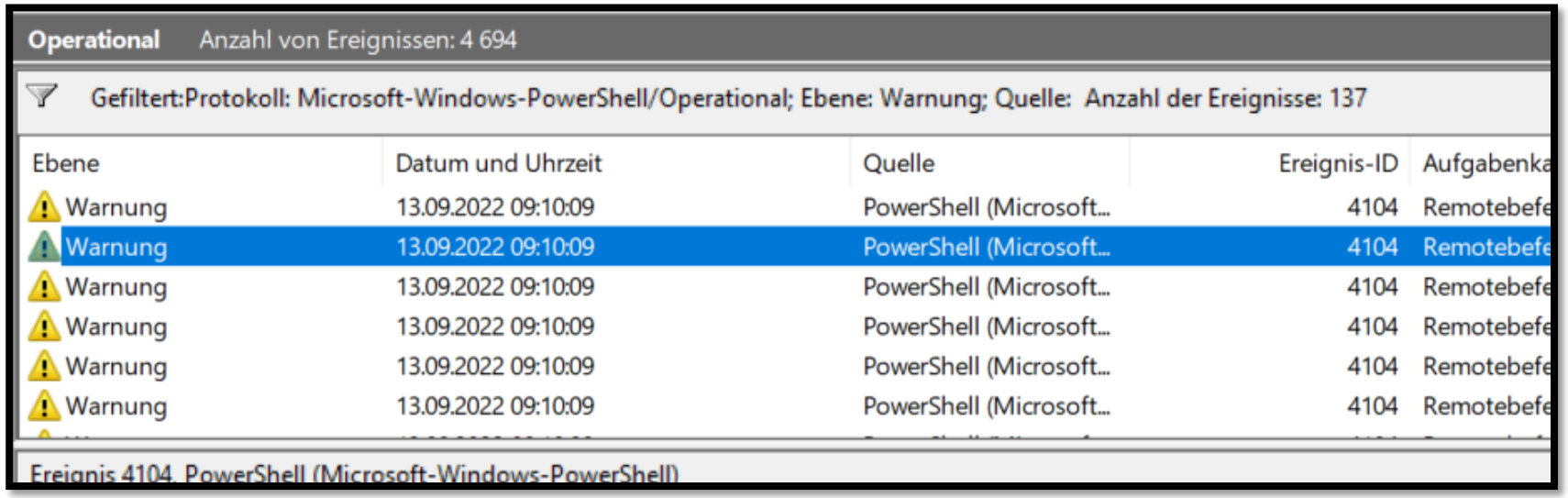
Difficult to detect due to almost no abnormal executables.

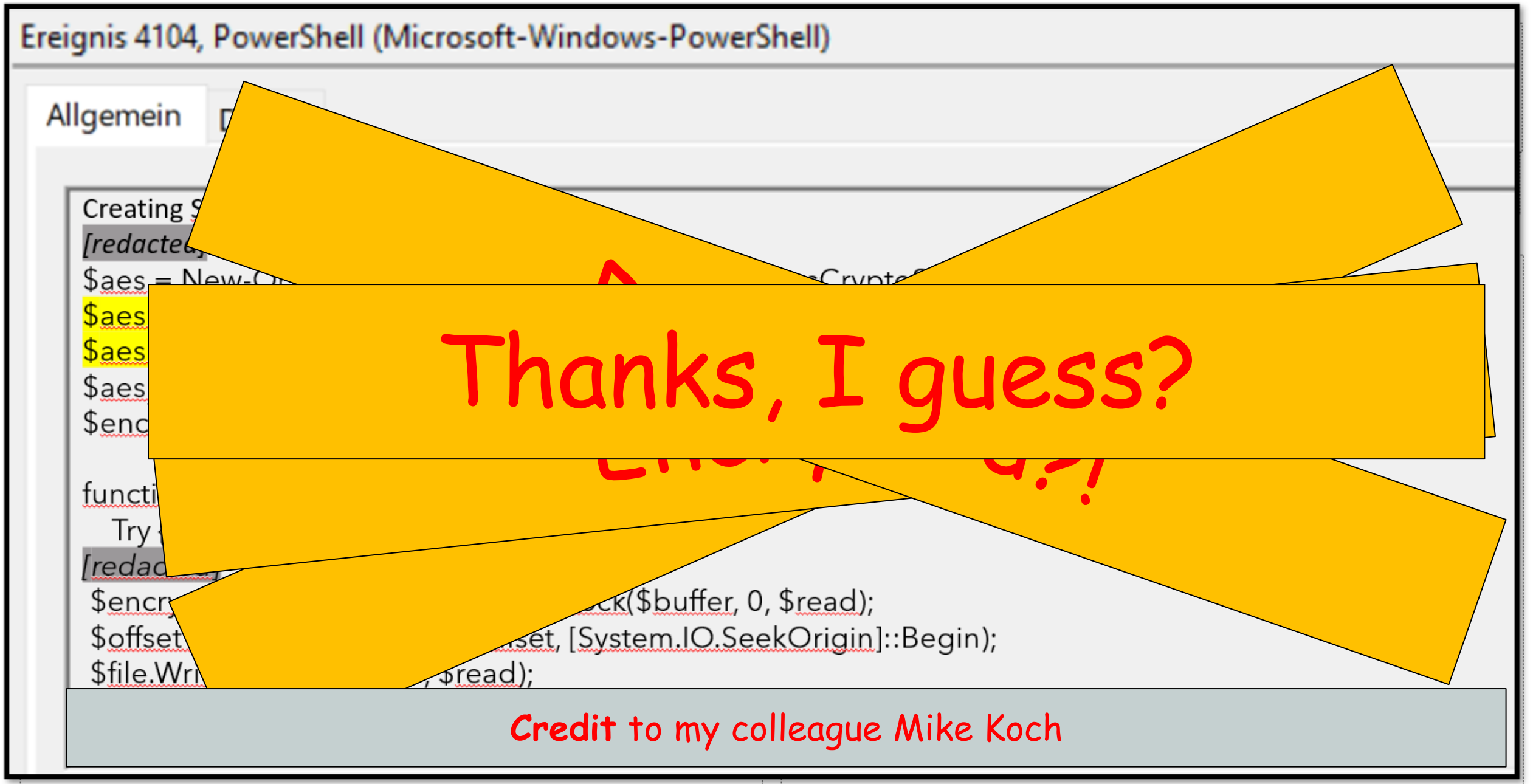
<u>Analysts-Advantage:</u>

LOLBIN logging depends on the customers not the attacker.

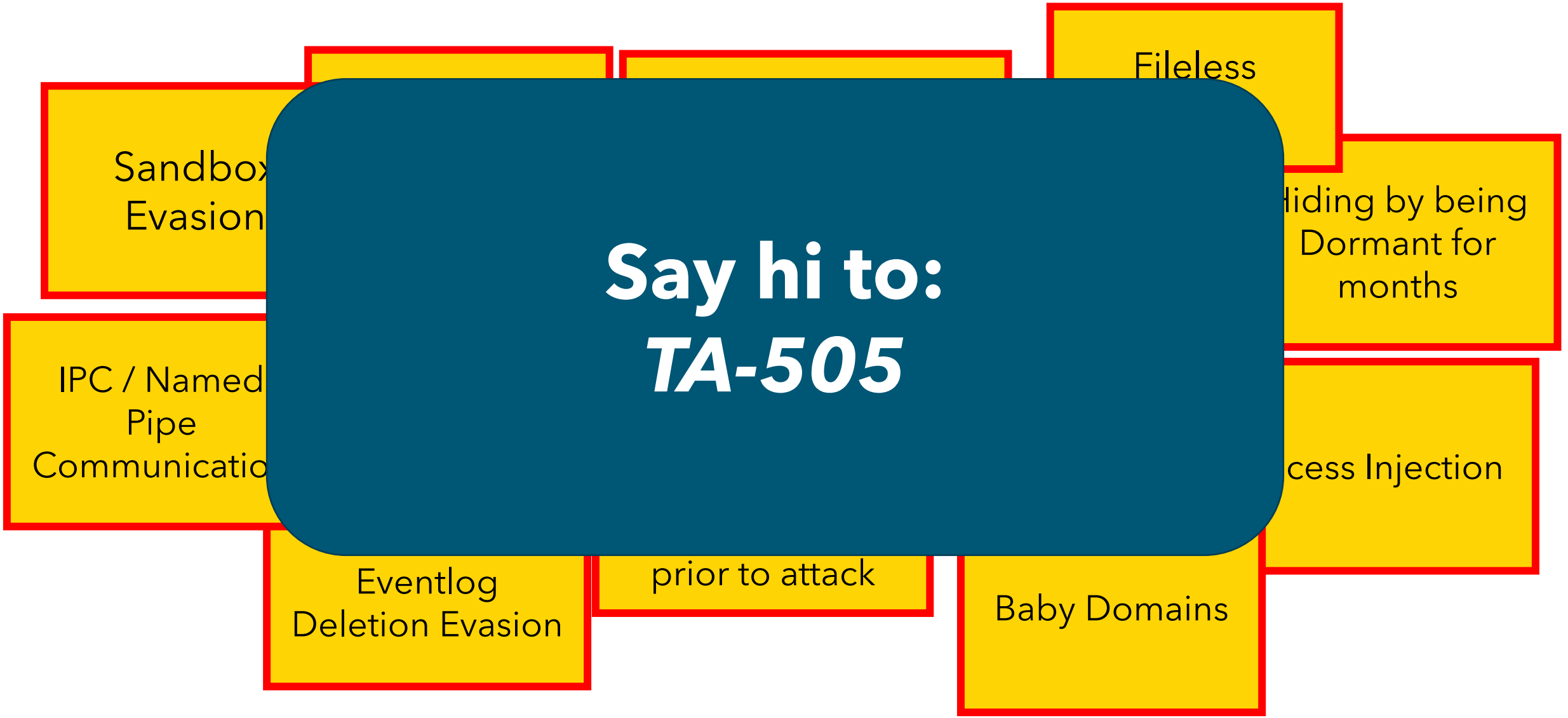
e.g. LOLBins:

- Powershell.exe
- Rundll32.exe
- Reg.exe
- Wscript.exe
- Certutil.exe
- …




Ereignis 4104, PowerShell (Microsoft-Windows-PowerShell)
Allgemein
Creating S
[redacted]
$aes = New-O
$aes
$aes
$aes
$enc
functi
Try
[redac
$encry
$offset
$file.Wri
ck($buffer, 0, $read);
set, [System.IO.SeekOrigin]::Begin);
$read);
Thanks, I guess?
Credit to my colleague Mike Koch

Imagine - all mentioned Techniques come together

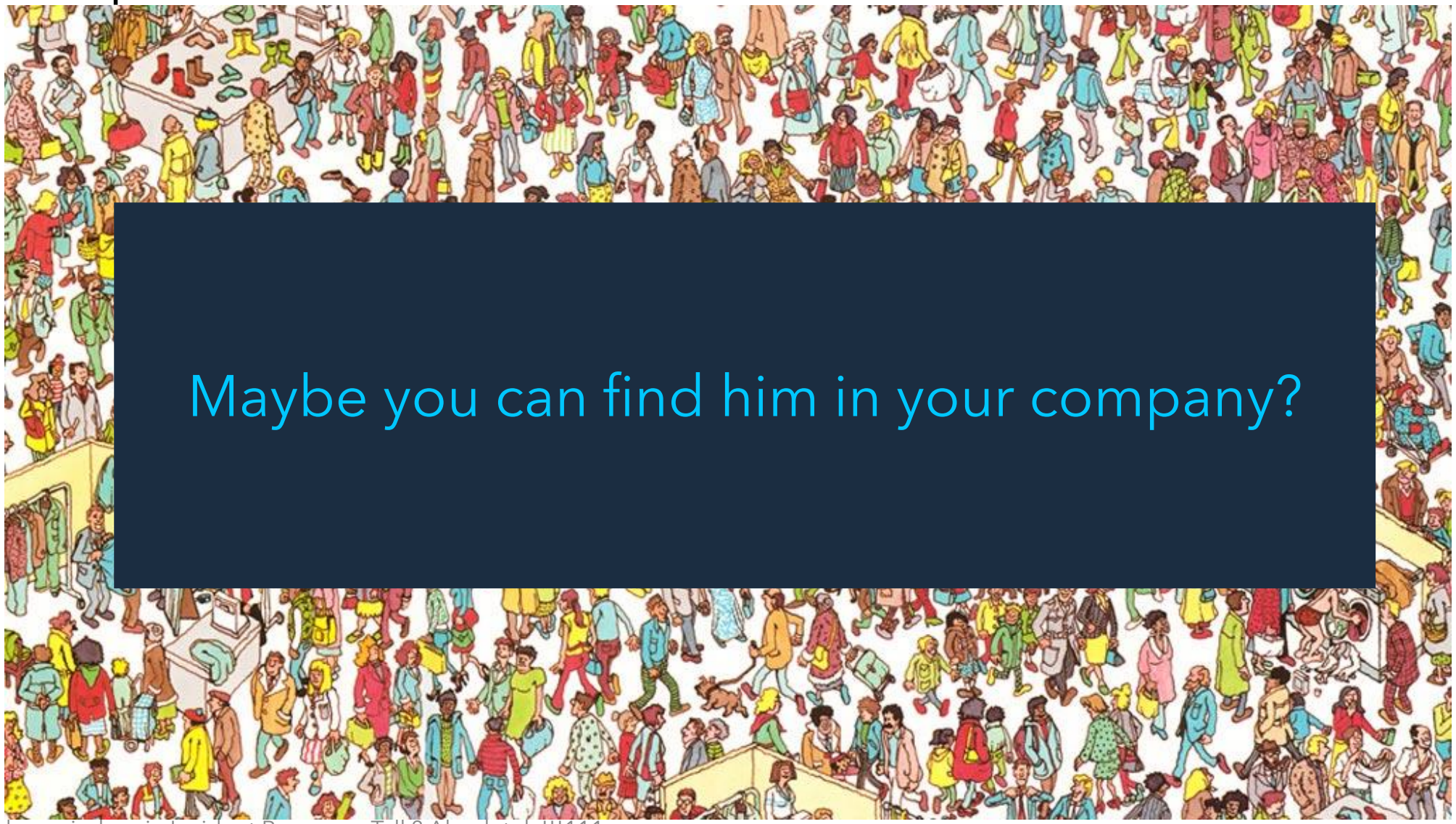

Fileless
Sandbox Evasion
Hiding by being Dormant for months
IPC / Named Pipe Communicatio
cess Injection
Say hi to:
TA-505
Eventlog Deletion Evasion
prior to attack
Baby Domains

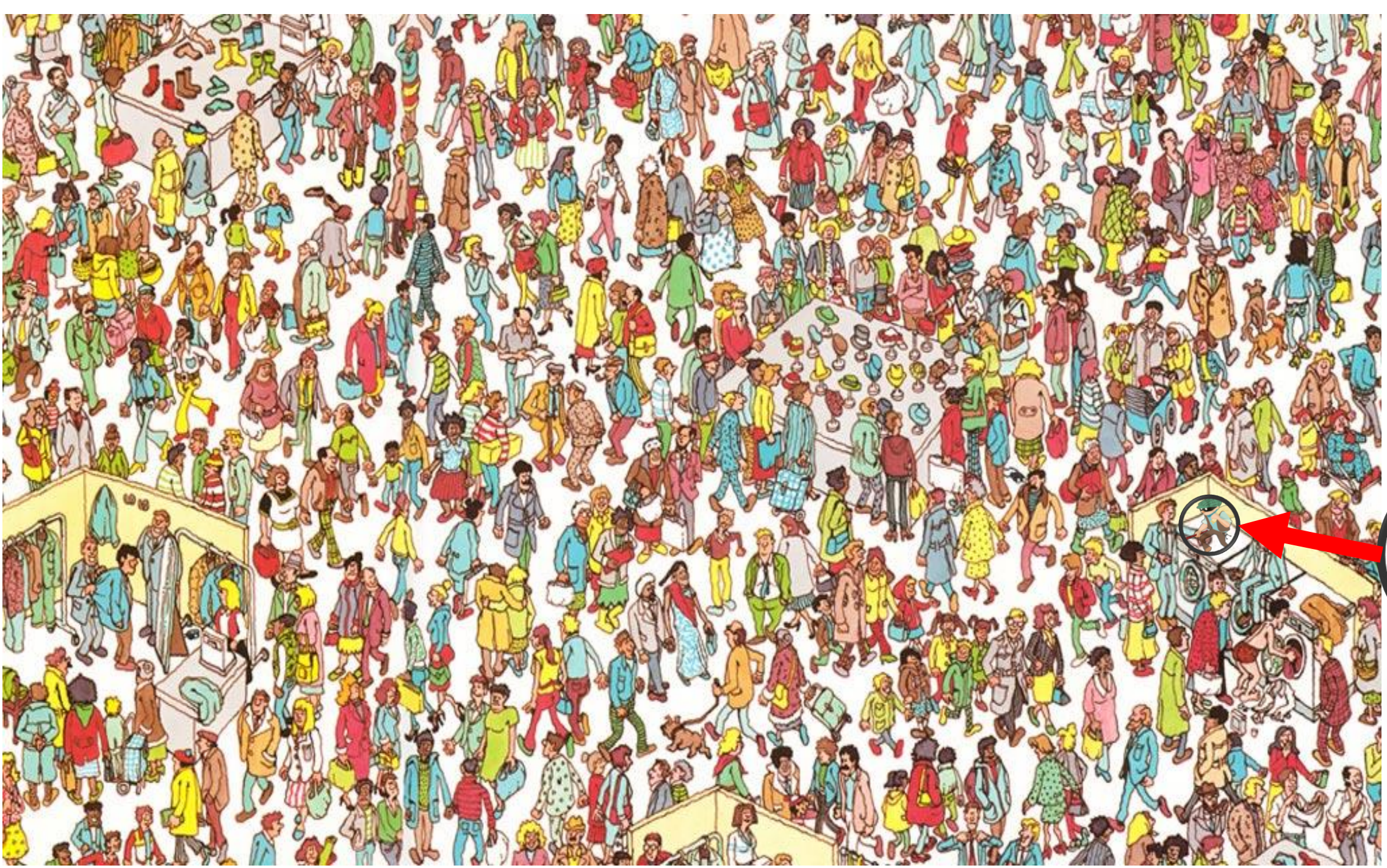
Conclusio

K-Business.com

This is what we know

Can you spot the attacker?





The End

- *Gideon Teubert, MSc*
- *K-BusinessCom AG*
- *Mail: Gideon.Teubert@k-business.com*