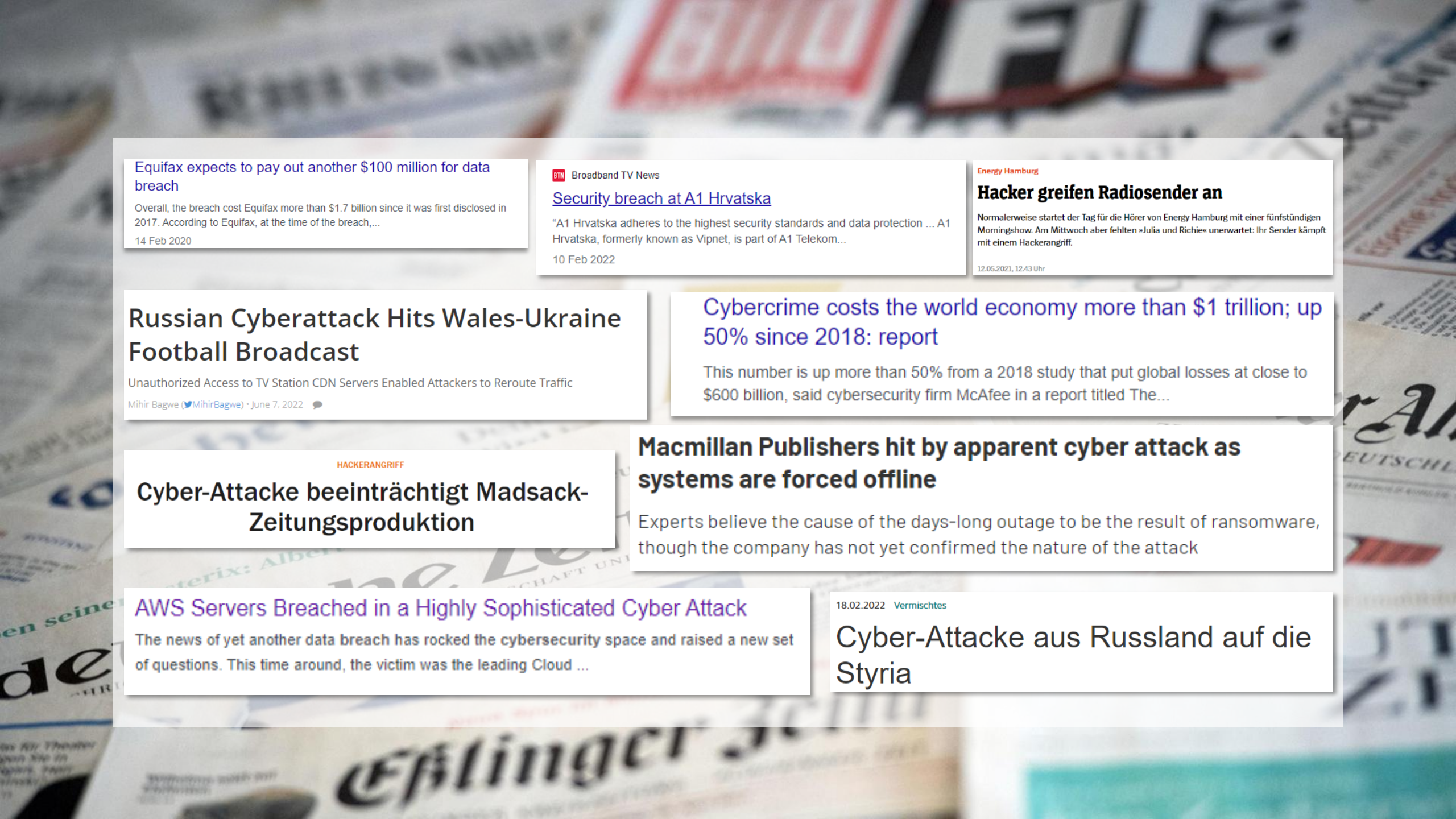
Cybercrime – Wie verändert Digitalisierung die Kriminalität?

Das Wettrüsten im Internet

—

Wien, 06. Dezember 2022



Equifax expects to pay out another $100 million for data breach

Overall, the breach cost Equifax more than $1.7 billion since it was first disclosed in 2017. According to Equifax, at the time of the breach,...

14 Feb 2020

Broadband TV News

Security breach at A1 Hrvatska

“A1 Hrvatska adheres to the highest security standards and data protection ... A1 Hrvatska, formerly known as Vipnet, is part of A1 Telekom...

10 Feb 2022

Energy Hamburg

Hacker greifen Radiosender an

Normalerweise startet der Tag für die Hörer von Energy Hamburg mit einer fünfstündigen Morningshow. Am Mittwoch aber fehlten »Julia und Richie« unerwartet: Ihr Sender kämpft mit einem Hackerangriff.

12.05.2021, 12.43 Uhr

Russian Cyberattack Hits Wales-Ukraine Football Broadcast

Unauthorized Access to TV Station CDN Servers Enabled Attackers to Reroute Traffic

Mihir Bagwe (MihirBagwe) · June 7, 2022

Cybercrime costs the world economy more than $1 trillion; up 50% since 2018: report

This number is up more than 50% from a 2018 study that put global losses at close to $600 billion, said cybersecurity firm McAfee in a report titled The...

HACKERANGRIFF

Cyber-Attacke beeinträchtigt Madsack-Zeitungsproduktion

Macmillan Publishers hit by apparent cyber attack as systems are forced offline

Experts believe the cause of the days-long outage to be the result of ransomware, though the company has not yet confirmed the nature of the attack

AWS Servers Breached in a Highly Sophisticated Cyber Attack

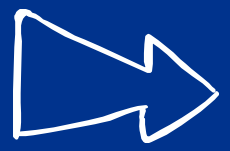
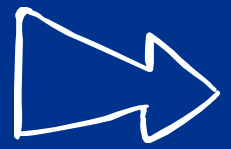
The news of yet another data breach has rocked the cybersecurity space and raised a new set of questions. This time around, the victim was the leading Cloud ...

18.02.2022 Vermischtes

Cyber-Attacke aus Russland auf die Styria


SIGNAL = 0


00:00 - 09:00
NATS

1990  2020  2050

Effective

wirksam

Affordable

leistbar

Deniable

abstreitbar

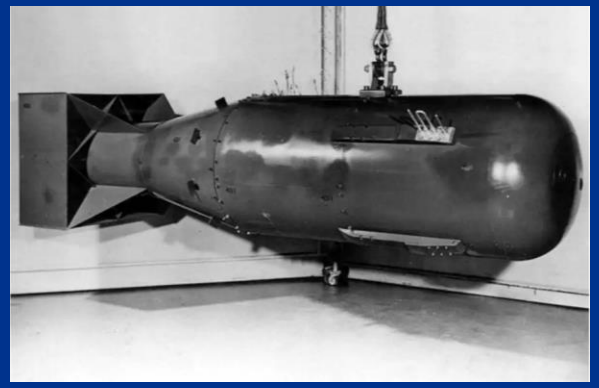

DO WE HAVE A BACKUP?
Stuxnet VIRUS
CHAPPATTE
Int'l Herald Tribune

WW I,

war der Krieg der Chemiker, mit dem Einsatz von Giftgasen

WW II,

war der Krieg der Physiker, mit der Atombombe



WW III,

wenn überhaupt, wird der Krieg der Computerwissenschaftler sein


BEST BEFORE
2020 NO 14

Mehr als 8.000 Sicherheitslücken wurden in Q2 2022 veröffentlicht

Die NVD-Datenbank enthält 8.051 Sicherheitslücken, die im ersten Quartal 2022 veröffentlicht wurden. Das ist ein Anstieg um etwa 25 Prozent gegenüber dem gleichen Zeitraum des Vorjahres. Sollten sich diese Zahlen bestätigen, würde dies einen leichten Anstieg gegenüber dem Vorjahr bedeuten, da im Jahr 2021 rund 22.000 Schwachstellen veröffentlicht wurden.

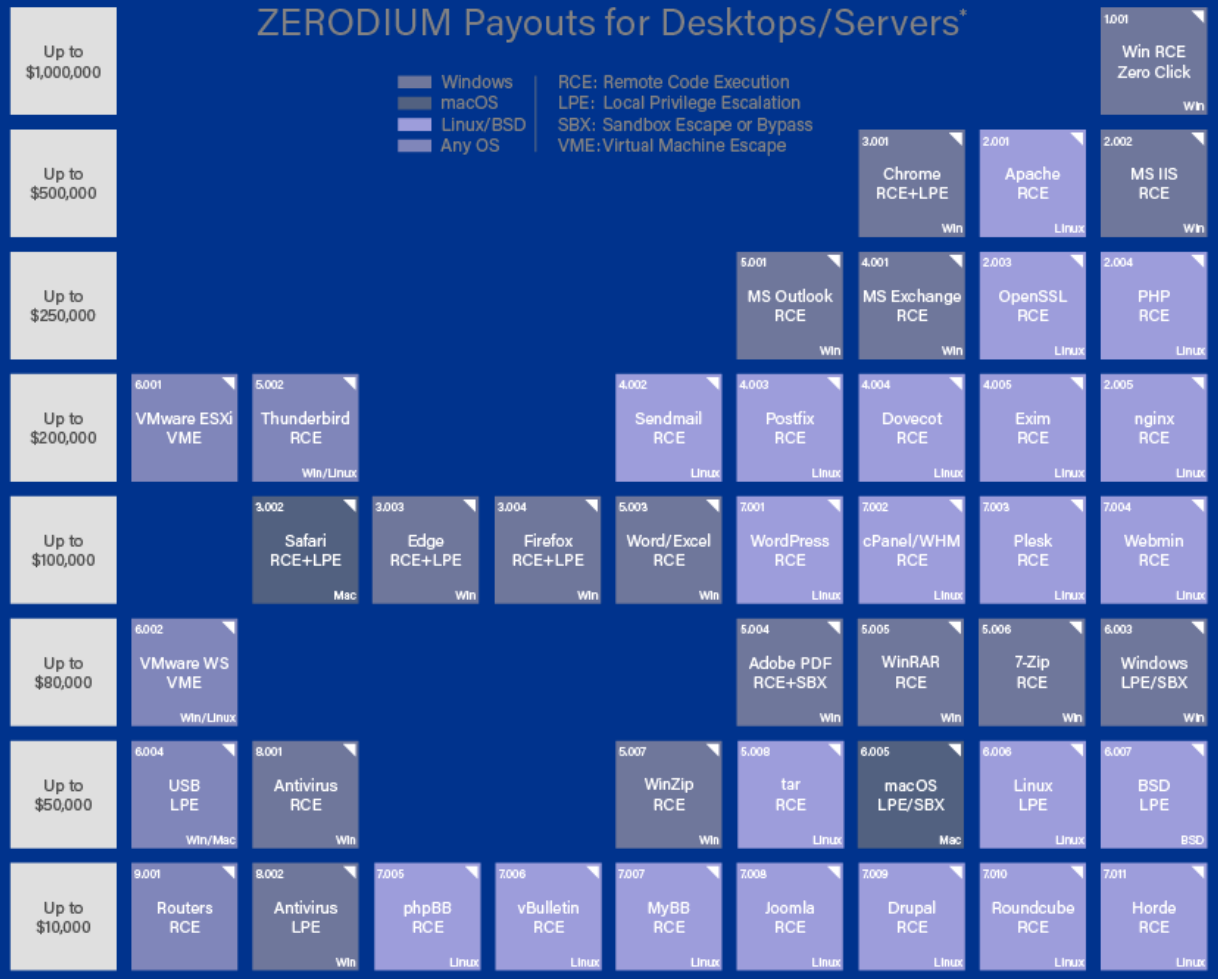
Die durchschnittliche Zeit bis zur Behebung (MTTR) beträgt etwa 58 Tage

Nach Angaben von Edgescan dauerte die Behebung von Schwachstellen im Internet durchschnittlich 57,5 Tage. Das ist eine leichte Verbesserung gegenüber dem Vorjahr, als die MTTR bei 60,3 Tagen lag.
Dies variiert jedoch von Branche zu Branche. Öffentliche Verwaltungen beispielsweise hatten eine MTTR von 92 Tagen, während Organisationen des Gesundheitswesens eine MTTR von nur 44 Tagen hatten. Die Daten zeigen, dass je kleiner eine betroffene Organisation ist, desto schneller erholt sie sich.

Die älteste im Jahr 2020 entdeckte Schwachstelle war 21 Jahre alt

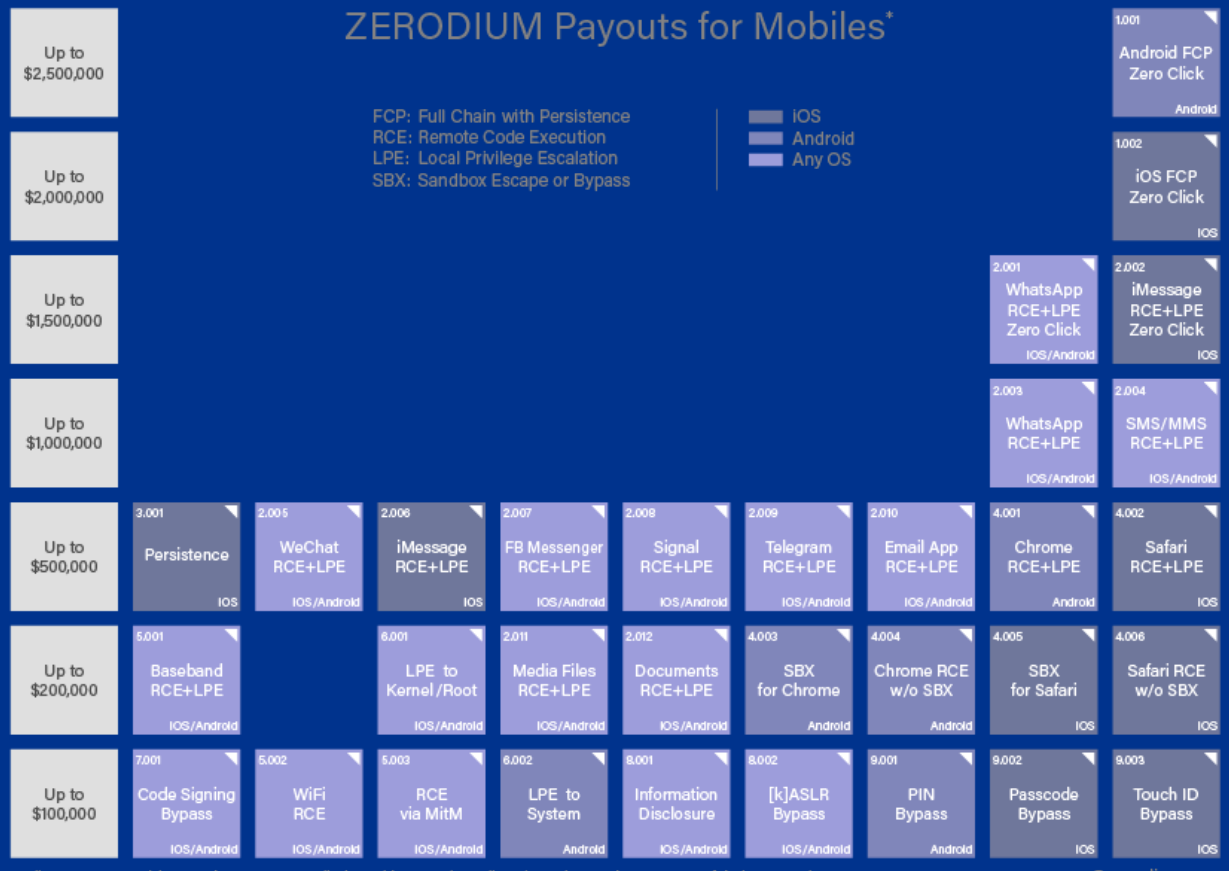
Interessanterweise fand Edgescan eine ziemlich alte Sicherheitslücke, die seit 1999 besteht: CVE-1999-0517. Sie betrifft das Simple Network Management Protocol Version 2 (SNMPv2), das für die Verwaltung von Geräten und Computern in einem IP-Netzwerk verwendet wird. Die Schwachstelle kann unbefugten SNMP-Zugriff über einen erratenen Community-String ermöglichen. Die Schwachstelle hat eine CVSS-Basisbewertung (Common Vulnerability Scoring System) von 7,5 und gilt damit als besonders schwerwiegend.

Exploits pay big money



*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com



*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Hybrid Konflikte

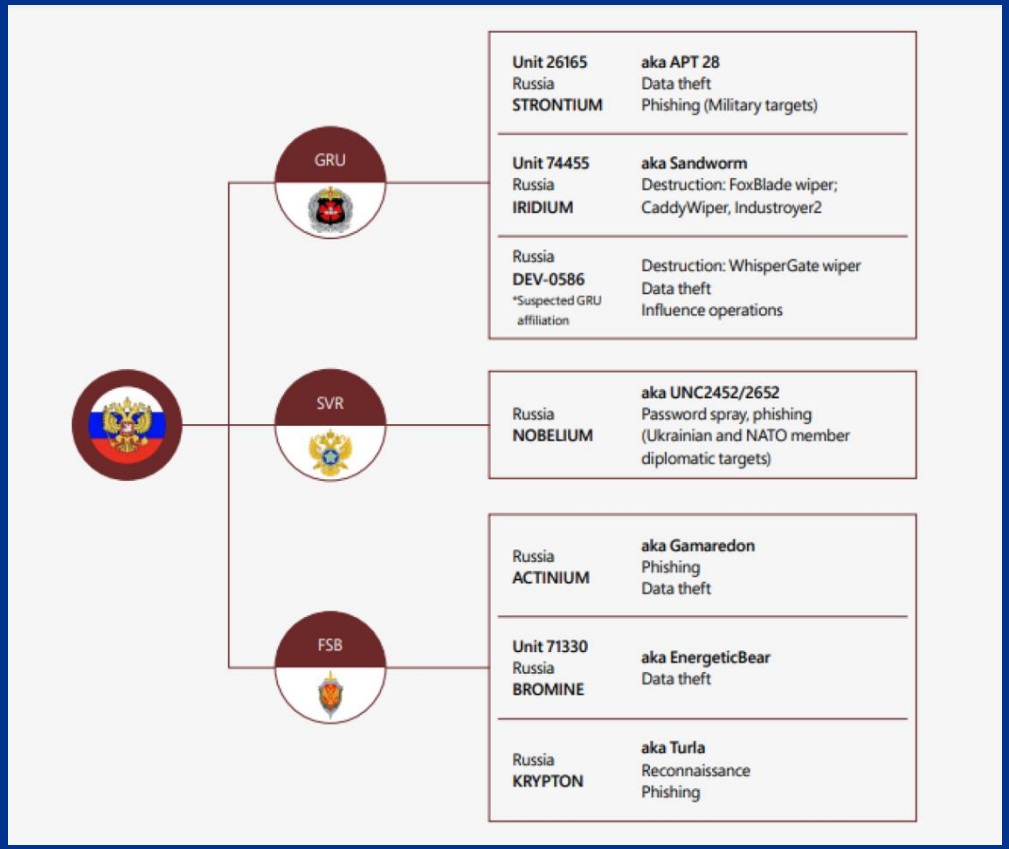
Der Cyberkrieg in der Ukraine begann am 23. Februar 2022.

- Intensiv,
- Unerbittlich
- Experten

Im Fokus sind

- Regierungsbehörden
- kritische Infrastruktur, insbesondere
  - Energie
  - Finanzunternehmen
  - IT
- In jüngster Zeit auch Transport und Logistik

Staatliche russische Einrichtungen als Verantwortliche für die Cyberangriffe



State sponsored	Pro Russia	Pro Ukraine	Independent

40
pro-Russian
Group

State-Sponsored Cyber Operations
- Lorec53
- DEV-0586 (GRU)
- DEV-0665/IRIDIUM (GRU)
- SANDWORM (GRU)
- GAMAREDON (FSB)
- UNC2452 (SVR)

Cyber Threat Groups
- PRIMITIVE BEAR
- VENOMOUS BEAR
- Conti
- Free Civilian
- Stormous Ransomware

1
pro-Russian
Group

- UNC1151

Cybercrime-Groups
- The Cooming Project
- Killnet
- MUMMY SPIDER
- SALTY SPIDER
- SCULLY SPIDER
- SMOKEY SPIDER
- WIZARD SPIDER
- The Xaknet Team

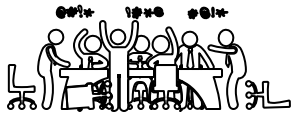
44
pro-Ukrainian Group

- Anonymous
- Against The West
- DDoSecrets
- NB65
- KelvinSec
- IT ARMY of UKRAINE

5
unknown groups

- Mustang Panda
- Curious George

- 26 new groups added, and 11 groups no longer take part in the action



- 128 groups have been involved in cyberspace activity since the beginning of the conflict

Globales Feld von Gegnern

Hybride Konflikte und deren Wirkung

Russische Informations-operationen in den 1980er Jahren

AIDS may invade India

Mystery disease caused by US experiments

NEW YORK:

AIDS, the deadly mysterious disease which has caused havoc in the US, is believed to be the result of the Pentagon's experiments to develop new and dangerous biological weapons.

Now that these menacing experiments are out of the laboratory and out of control, plans are being hatched to hastily transfer them from the US to other countries, primarily developing nations where governments are pliable to Washington's pressures and persuasion.

Some American experts believe that Pakistan may become the next proving ground for these experiments. If this happens, there will be a real danger that AIDS may rapidly spread to India with the grave consequences to the people of the country.

WHO representatives point out that AIDS may soon become problem number one, since as far there are no effective cures to fight it.

The British mass media has pointed to the blood plasma imported from the US as the cause of AIDS, which is spreading in the British Isles where more than 15 patients have been hospitalised, with half of them now dead.

As a result, France and Holland, which use large quantities of blood plasma imported from blood, Britain, the Federal Republic of Germany and Denmark are now considering similar measures.

In recent months, there has been a marked increase in the incidence of this hitherto unknown disease, the so-called Acquired Immune Deficiency Syndrome (AIDS). It is caused, or so scientists suspect, by a new virus which attacks and destroys the immune system of a human being, making him practically defenceless against any infection. Once the AIDS virus penetrates the human organism, it does not become the "killer" but rather acts like a time bomb. The immune system destroyed by it can no longer resist diseases even such as the virus flu. As a result, any [illegible] soon

A well-known American scientist and authority on AIDS in a letter to Editor, Patriot, analyses the history and background of the deadly AIDS which started in the US and has now spread to Europe. The writer, who wants to remain anonymous, has expressed the view that India may soon be the next victim of the disease in the near future.

AIDS has recently been registered in 26 countries, primarily in those which import American blood derivatives. For some of the countries the disease has already become extremely dangerous.

In Zaire, for example, AIDS appeared in 1959 with an outbreak of this disease in New York among immigrants from Haiti. As that time, however, no one seemed to bother to pay any serious attention both on the part of the local authorities and the US public at large. In 1980 there was another sign of AIDS and cases in New York. This time in addition to Haitian immigrants the disease struck local Americans, primarily drug addicts and homosexuals. By February 1981, AIDS had affected large sections of the American population and had been registered in 33 states. New York accounted for 49 per cent of all the cases that had been officially registered in the US by that time.

Concerned American citizens and organizations began to wonder what AIDS, just like other previously unknown diseases such as Legionnaires' disease, the so-called Lesbian

continued on page 7 col. 5

PATRIOT* magazine

SUNDAY, JULY 17

Guerillas And Gorillas

Understanding the reasons why even after a century of political independence the Latin American countries have both their politics deformed and their economy distorted will help to have a better idea of the problems which any post-colonial society faces, writes M. P. Kavalam.

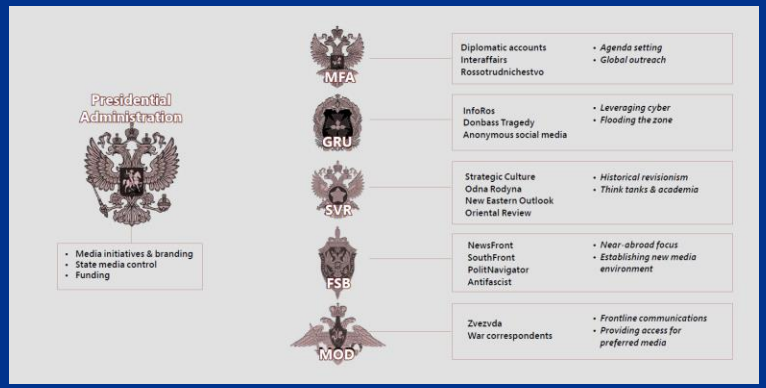
Ramdan In Dubai

Perhaps at no time of the year does Dubai come to the fore as a Muslim city than at Ramdan. For the Arabs, the months of fasting apart from being a deeply religious occasion assumes almost a festive air, writes Rashmi Taneja.

OTHER FEATURES : Public View, Nostalgia, Encounters, Thinking One-dimensionally, Short Story by Bandana Majumdar, Education, Mirror/Windows, Films, Cultural Watch, Sports...

Kinetischer Krieg und Cyberangriffe wurden mit einem dritten Element kombiniert:

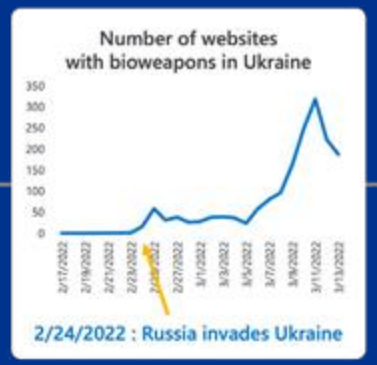
- Die Cyber-Einflussnahme-Operation
- Beeinflussung der Wahrnehmung der Ukrainer
- Beeinflussung der Wahrnehmung der Russen
- Beeinflussung der Wahrnehmung der ROW



Bioweapons campaign timeline

November 29, 2021

February 24, 2022



March 11, 2022

Quelle: History, Philosophy, and Newspaper Library at the University of Illinois at Urbana Champaign

Data Engineer

Ashby College

1,321 contacts

Films, travel and skiing

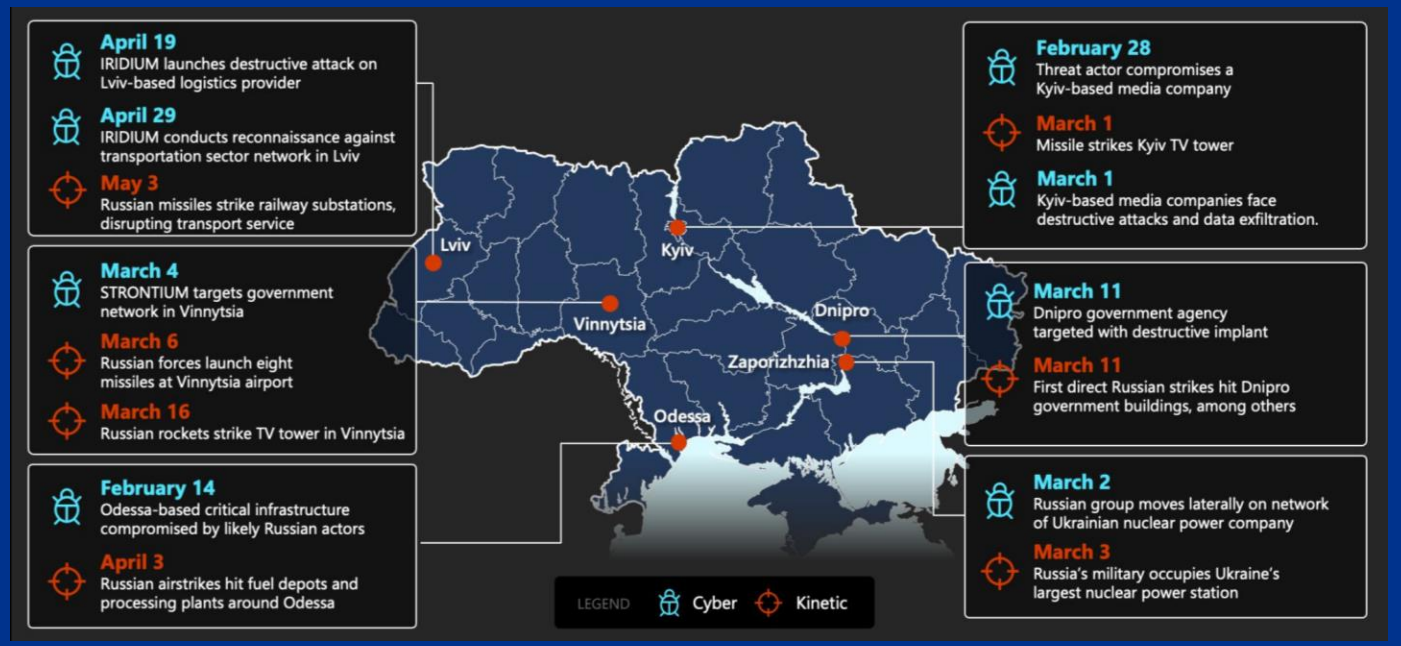
Georgina Wang
Head of Talent Management
GW Recruit

Accept | Ignore | More...

156 likes | 15 comments

Bower Associates

Koordinierte russische Cyber- und Militäroperationen in der Ukraine



TYPES OF ATTACKS

113 DDOS

68 HACK AND LEAK

21 CYBERESPIONAGE

19 MALWARE

17 WIPERS

16 DEFACEMENTS

12 CYBER-ENABLED INFORMATION OPERATIONS

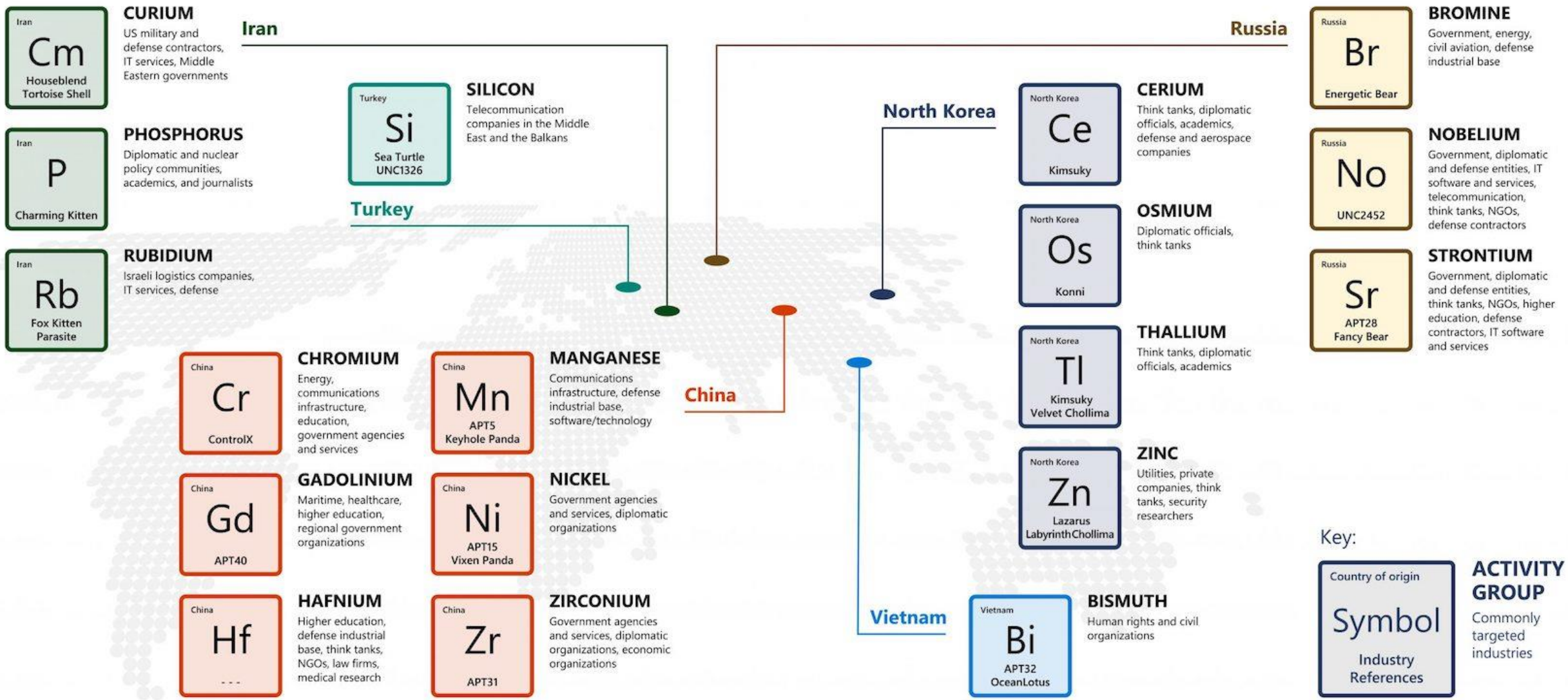
7 RANSOMWARE

2 COORDINATED INAUTHENTIC BEHAVIOR

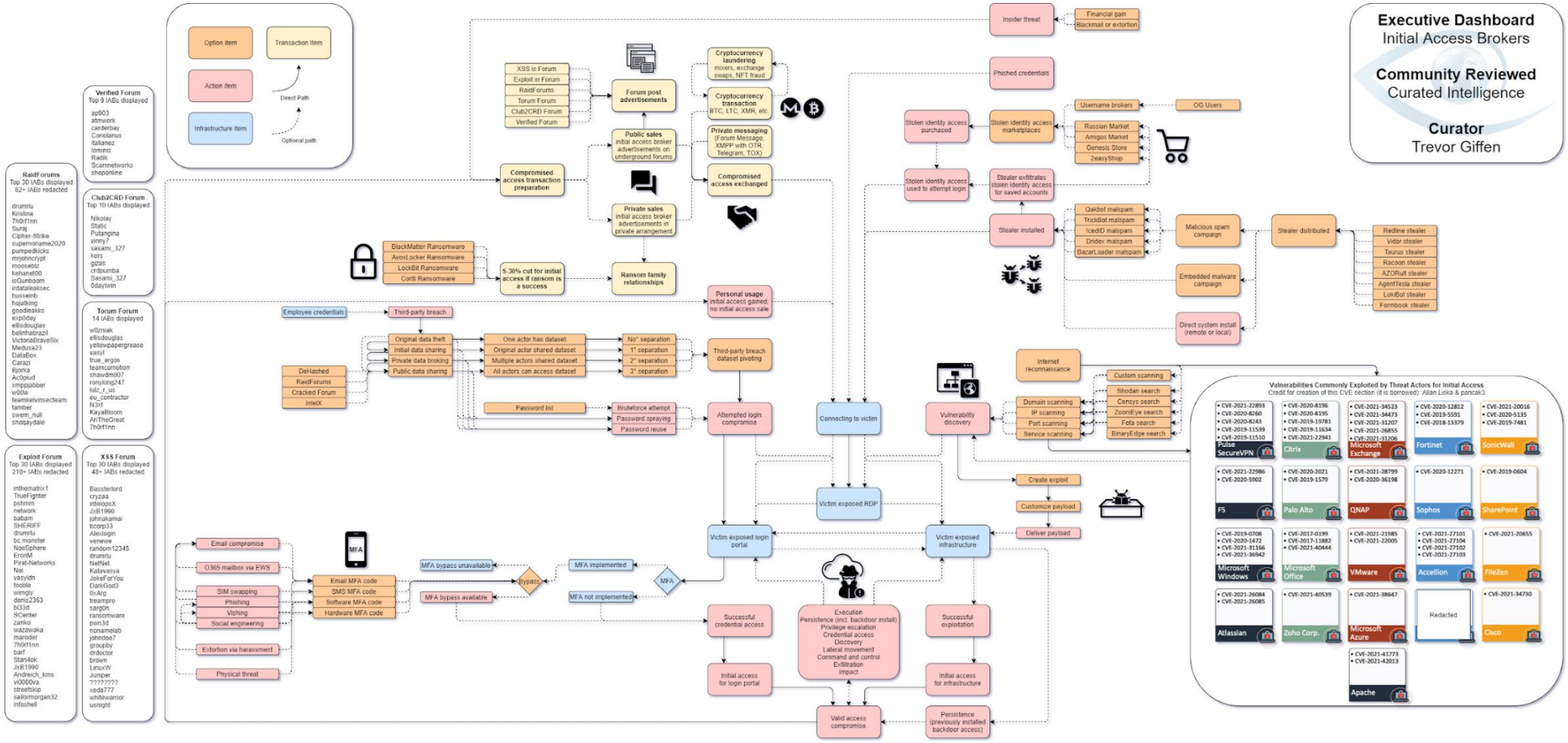
2 FINANCIAL FRAUD

1 SPAM

Sample Nation-State Actors



Erster Zugang: RaaS-Gruppen haben sich von anfänglichen Ingress-Botnetzen abgekoppelt



Source: https://www.curatedintel.org/2021/10/initial-access-broker-landscape.html

	Umsatz/Einheit	Kosten/Einheit	Gewinnspanne	Festnahmen/ Einheit	Todesfälle/Einheit	Marktzutritts-schranken
Kokainhandel 1992	$60,000 /kilo	$5,000 /kilo	91 %	0.5	0.25	sehr hoch
Ransomware 2020	$140,000 /attack $220,000 Q1 2022	$2,500 /attack	98 %	.0008	0	keine

Auswirkungen von Ransomware

25 Tage

Durchschnittliche Zeit von der Entdeckung eines Vorfalls bis zur vollständigen Wiederherstellung

+/- 0% from Q2 2022

66 USD

Preis eines Ransomware-Kits (oder 30% vom Gewinn/dem Partnermodell)

86%

der Ransomware-Angriffe waren mit der Bedrohung verbunden, dass die exfiltrierten Daten veröffentlicht werden

+2% from Q1 2022

42%

der Opfer von Datenlecks haben sich für die Zahlung des Lösegelds entschieden

-11% from Q4 2021

Ransomware costs and payment

50% of those who pay do so in about a week. Delaying payment might be a good nudge towards not paying

258,143 USD

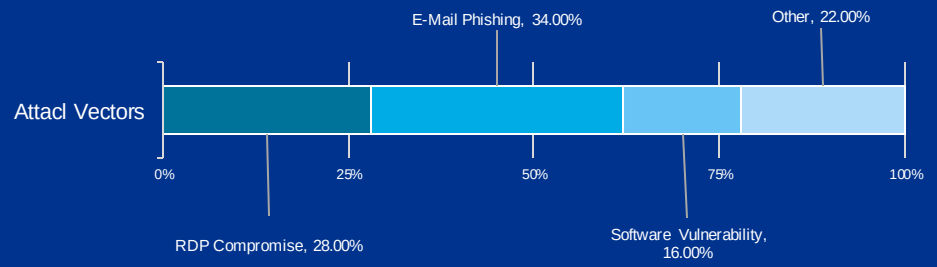
Average payment amount

+13,2% % from Q2 2022

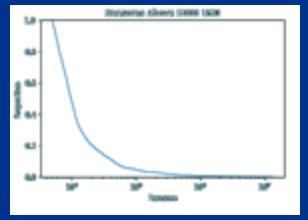
41,987 USD

Median Ransom Payment

+15,5% % from Q2 2022



Schätzung des Schadens durch Ransomware



Die Auswirkungen eines Ereignisses kosten in der Regel **zwischen 10 und 50 % des Jahresumsatzes** des betroffenen Unternehmens.

Dabei wird davon ausgegangen, dass es keine Netzwerktrennung und keinen Endpunktschutz gibt und der Angreifer sich seitlich (lateral movement) bewegen können.

Rechtfertigung der Zahlung für die Unterdrückung von exfiltrierten Daten

1. Die Zahlung mindert das Risiko eines Schadens für die betroffenen Parteien
2. Die Zahlung mindert die Gefahr einer Sammelklage
3. Die Zahlung zeigt den Betroffenen, dass "wir alles getan haben, um ihre Daten zu schützen".
4. Bezahlen begrenzt den Schaden für die Marke durch negative PR

Human operated rasomware targeting and rate of success model

In recent years, ransomware has **moved from a model** where a **single "gang"** would both **develop** and **distribute** a **ransomware** payload to the **ransomware as a service (RaaS)** model. RaaS allows one group to **manage** the **development** of the ransomware payload and **provide services** for **payment** and **extortion** via data leakage to other cybercriminals referred to as "affiliates" for a cut of the profits.

January - June 2022

2.500 potential target organizations	Access Brokers sell access to compromised networks to ransomware-as-a-service affiliates, who run the ransomware attack
60 Encounter activity associated with ransomware attacker	RaaS affiliates prioritize targets by intended impact or perceived profit
20 Are successfully compromised	Attackers take advantage of any security weakness they find in the network, so attacks vary
1 Falls victim to a successful ransomware event	The ransomware payload is the culmination of a chain of malicious activity

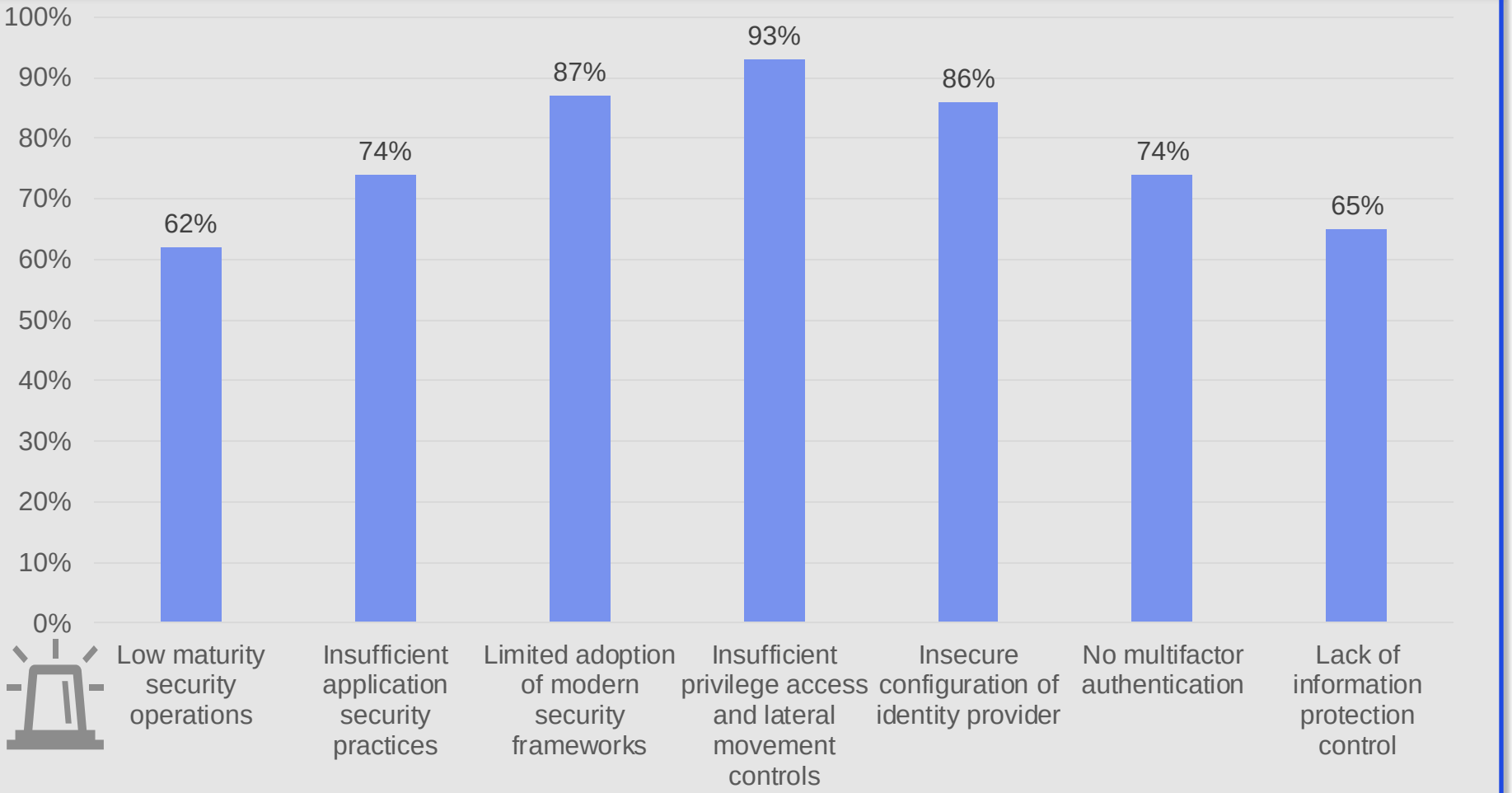
Industrialization of the cybercrime economy, enabling **access to tooling and infrastructure** and expanding cybercriminal capabilities by **lowering** their **skill barrier** to entry.

One-third of **targets** are **successfully compromised** by criminals using these attacks and **5%** of those are **ransomed**.

Every twentieth company that has been **compromised** falls victim to a **successful ransomware event**.

Source: MSTIC Microsoft Defender for Endpoint (EDR) data (January-June 2022)
https://query-prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Summary of most common findings in ransomware response engagements



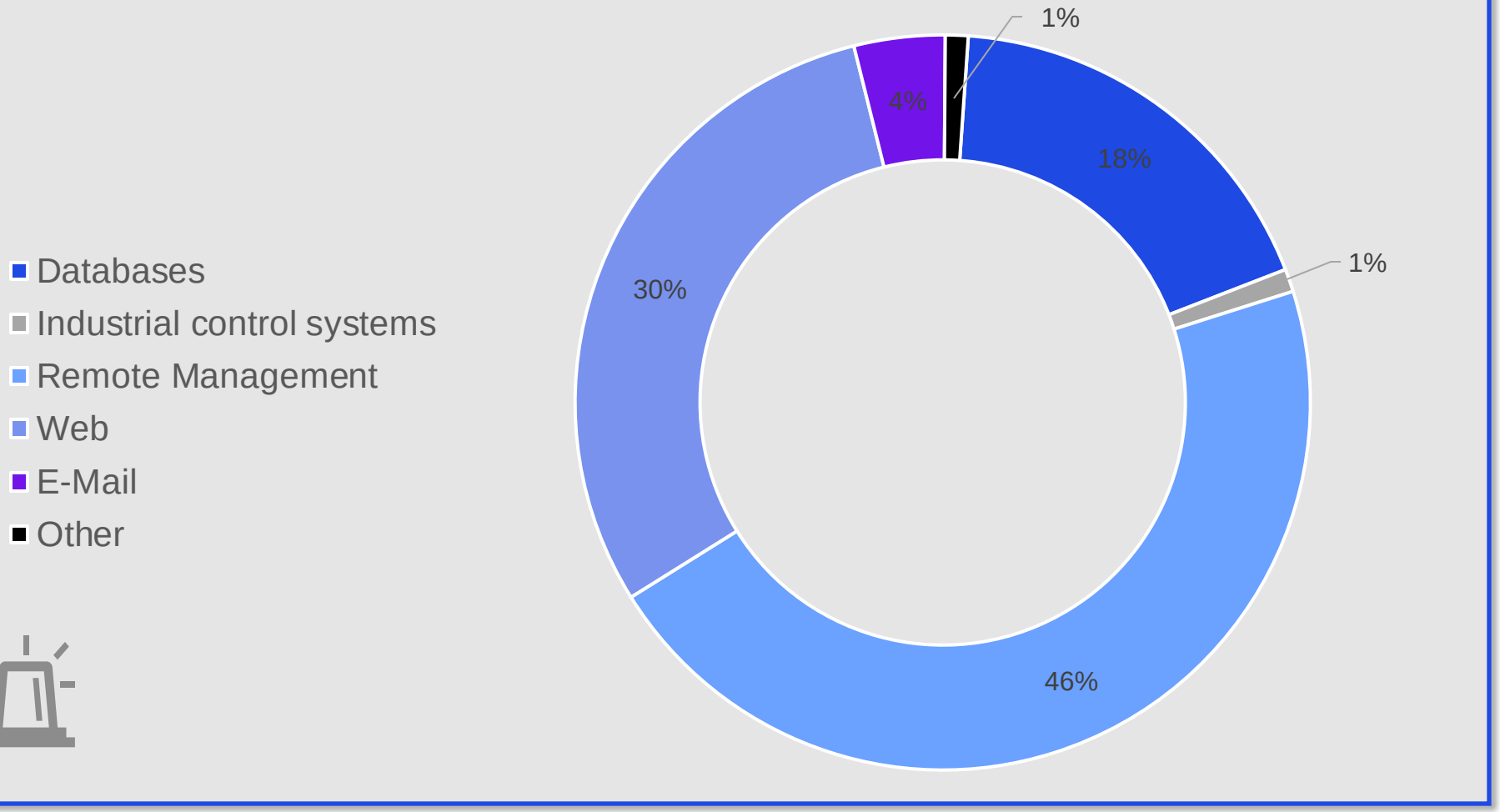
The most common finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls.

Counteracting possibilities

- Multifactor authentication (MFA)
- Privileged Access Management (PAM) solution
- Micro-Segmentation

Source: MSTIC Microsoft Defender for Endpoint (EDR) data (January-June 2022)
https://query-prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Attack-Targets observed through MSTIC sensor network on IoT/OT



Most prevalent were attacks against **remote management devices**, **attacks via web**, and **attacks on databases** (brute forcing or exploits)

Remote management is often done by **suppliers**, so the issue of **third-party risk management** should be considered.

Source: MSTIC Microsoft Defender for Endpoint (EDR) data (January-June 2022)
https://query-prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Zeitliche Betrachtung eines Cyberangriffs

Weitere Handlungsfelder in der Bearbeitung eines Cyberangriffs

- Komplizierte Kommunikationswege, ineffiziente Meetings
- Erste Anzeichen von Überlastung
- Durchhaltefähigkeit beeinträchtigt
- Mehrfache Berichts- und Reporting-Linien
- Aggression im Team aufgrund medialer Berichterstattung
- Erleichterung und Freude
- Lob & Anerkennung
- Persönliche Betroffenheit bei den Familien
- Keine Opfersuche
- Anzweifeln der Kompetenz des zusätzl. Dienstleisters
- Folgeaktivitäten
- Medienanfragen und Berichterstattung in Sozialen Netzwerken
- Einbindung des StB/WP

x-90 Tage

Vorbereitung des Angriffs

- Ungewöhnliches Nutzer- und Systemverhalten wird festgestellt
- Ein Zuordnen zum Angriff ist nicht eindeutig möglich

Beginn des Angriffs

- Samstag Tag-X, 23:50
- Ungewöhnliches Systemverhalten wird festgestellt
- Systeme sind verschlüsselt und Forderungen werden gestellt

Basiskommunikation verfügbar

- Dienstag X+3
- Bestimmte Services sind wieder verfügbar
- Basiskommunikation mittels E-Mail und Microsoft Teams hergestellt

Situation & strategische Entscheidungen

- Donnerstag X+5
- Entscheidungen über die Wiederherstellung des Systems werden getroffen
- Beginn der Wiederherstellung durch Entschlüsselung der Systeme

Basisinfrastruktur

- Sonntag X+8
- Teile der Basisinfrastruktur sind für Kommunikationszwecke wieder verfügbar

Erste Systemübergabe

- Donnerstag X+12
- Übergabe von SAP
- Übergabe Konsolidierungs-system

Stabiler Betrieb der Systeme

- Montag X+16
- 95% der Systeme sind wiederhergestellt und in Betrieb
- Abschluss der Arbeiten
- Laufende Verbesserung der Systemstabilität

Maßnahmen zur Verbesserung

- Donnerstag X+19
- Erarbeitung von Verbesserungsmaßnahmen
- Prüfen der Sofortmaßnahmen
- Ableiten einer strategischen Langzeitplanung

X+365 Tage

Vorbereitung des Angreifers | Angriff und Verschlüsselung | Isolierung und Wiederherstellung | Kurz-, mittel- und langfristige Verbesserungen | Aufarbeitung des Vorfalls

The Cybersecurity Dashboard | October 2022

$17.8 Billion
YTD 2022 Financing Volume

858
YTD 2022 Financing Transactions

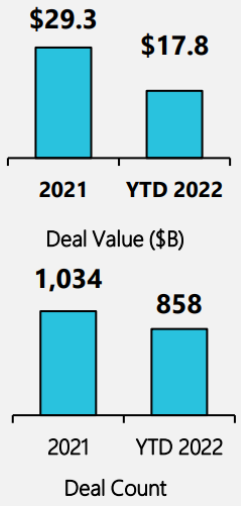
$118.0 Billion
YTD 2022 M&A Volume

224
YTD 2022 M&A Transactions

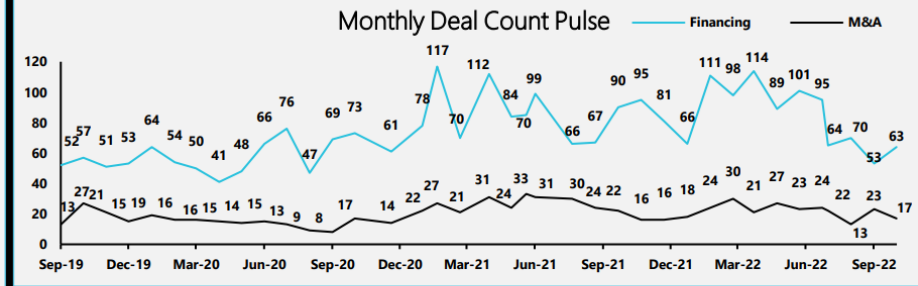
Notable Financing Transactions YTD 2022

Date	Company	Amt. ($M)
02/14/22	securonix	$1,000
01/19/22	1Password	$620
01/27/22	Fireblocks	$550
04/26/22	sonar	$412
10/06/22	ARCTIC WOLF	$401
02/23/22	BlueVoyant	$250
07/29/22	Acronis	$250
07/08/22	Coalition	$250
04/12/22	CRITICALSTART	$215
05/09/22	Abnormal	$210

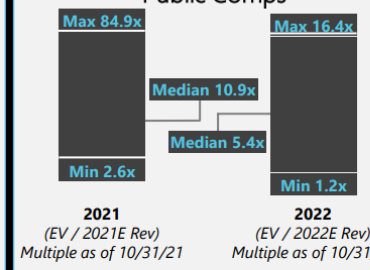
Financing Activity



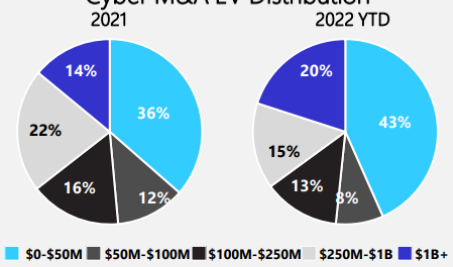
Monthly Deal Count Pulse



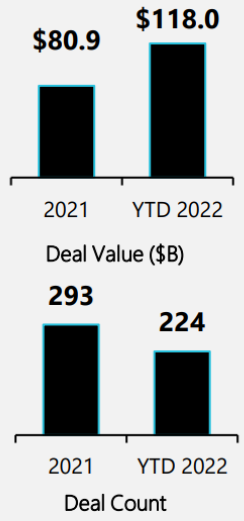
Public Comps



Cyber M&A EV Distribution



M&A

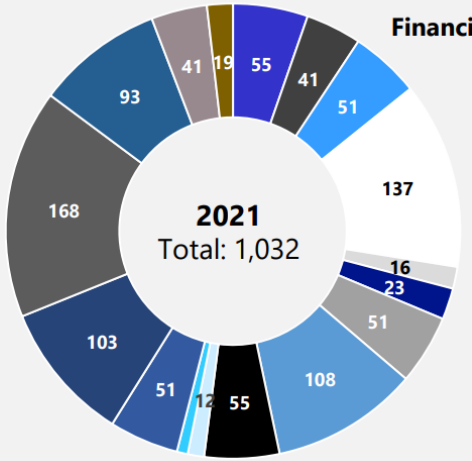


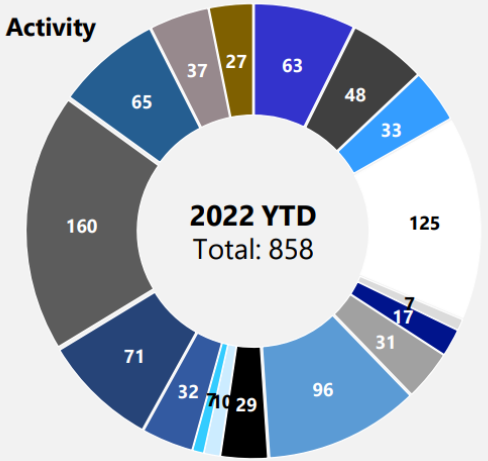
Notable M&A Transactions YTD 2022

Target	Acquirer	EV ($M)
vmware	BROADCOM	$69,207
SailPoint	THOMABRAVO	$6,900
datto	Kaseya	$6,200
MICRO FOCUS	opentext	$5,656
MANDIANT	Google	$5,326
KnowBe4	VISTA	$4,299
Barracuda	KKR	$4,000
PingIdentity	THOMABRAVO	$2,793
VERACODE	TA ASSOCIATES	$2,500
ForgeRock	THOMABRAVO	$2,252

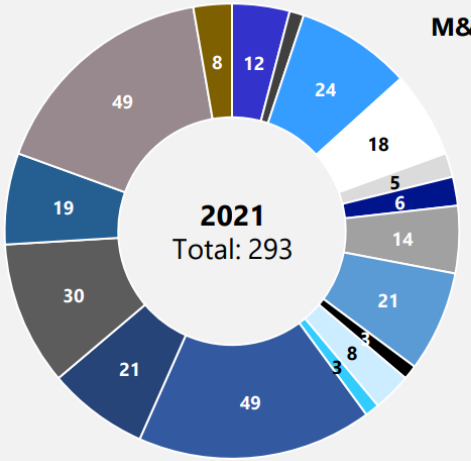
- Application Security
- Blockchain
- Cloud Security
- Data Security
- Digital Risk Management
- Endpoint Security
- Fraud & Transaction Security
- Identity & Access Management
- IoT
- Messaging Security
- Mobile Security
- MSSP
- Network & Infrastructure Security
- Risk & Compliance
- SecOps / IR / Threat Intel
- Security Consulting & Services
- Web Security

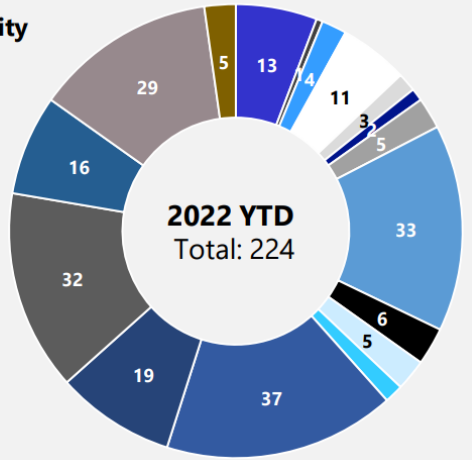
Financing Activity

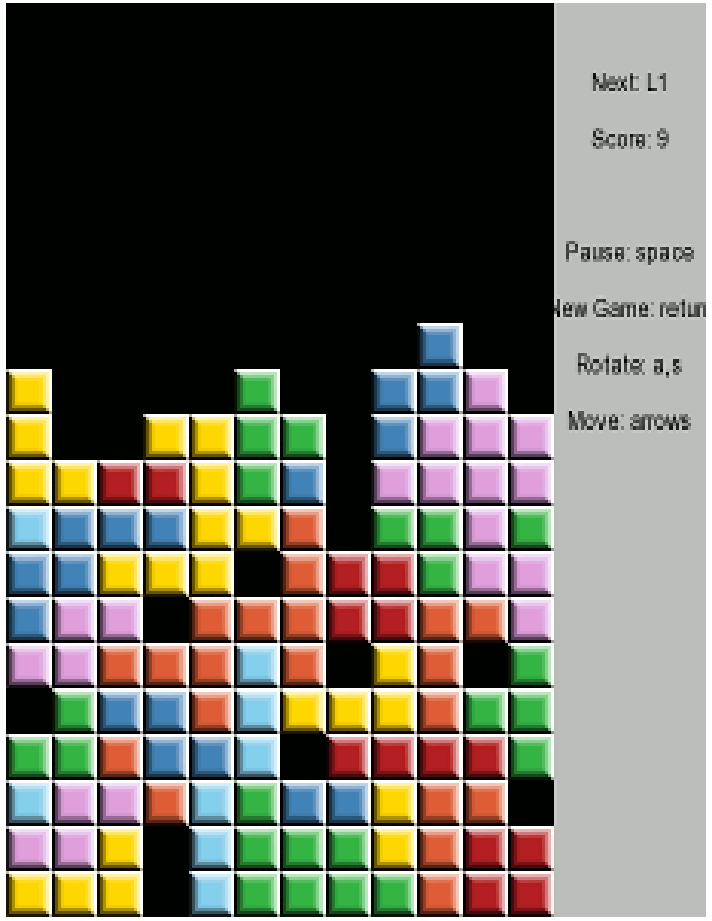




M&A Activity







Cybersicherheit ist zum Wettbewerb geworden: Ich muss besser sein als viele andere, damit ich gar nicht erst in den Fokus der Cyberkriminellen komme.

Pascal Lamia
Leiter für Operative Cybersicherheit im NCSC
und stv. Delegierter des Bundes für Cybersicherheit in der Schweiz.

Hilfe - https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/ansprechstellen.html

Ansprechstellen zum Thema Cybersicherheit

Bundeskanzleramt Cybersicherheit

Das Bundeskanzleramt ist im Cyberbereich für die strategische Koordination innerhalb der öffentlichen Bundesverwaltung in Österreich verantwortlich, die auch die europäische und internationale Koordination umfasst.

Abteilung I/8 – Cybersicherheit, GovCERT, NIS-Büro und ZAS
E-Mail: cybersicherheit@bka.gv.at

Büro für Strategische Netz- und Informationssystemsicherheit (NIS-Büro)

Das Büro für strategische Netz- und Informationssystemsicherheit ist im Bundeskanzleramt als Teil der Abteilung I/8 zuständig für Angelegenheiten im Zusammenhang mit der Umsetzung der rechtlichen Verpflichtungen aus der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) in Österreich und dem Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz).

Web: www.nis.gv.at
E-Mail: nis@bka.gv.at

Computer-Notfallteam für die öffentliche Verwaltung – GovCERT Austria

GovCERT Austria ist das Computer-Notfallteam (Government Computer Emergency Response Team) für die öffentliche Verwaltung in Österreich. Das Bundeskanzleramt leitet in Kooperation mit CERT.at das GovCERT Austria mit dem Ziel, auf Sicherheitsvorfälle im Bereich der Informations- und Kommunikationstechnologien (IKT) reagieren zu können und diese zu verhindern.

Web: GovCERT Austria

Studiendownload & Kontakt

DI Mag. Andreas Tomek

Partner Cyber Security &
Global Head of Cloud Security
CISSP, CISA, CPTS, CPTE, AMBCI

KPMG Security Services GmbH

Porzellangasse 51
1090 Wien

T +43 1 31332-3930
M +43 664 816 0995
F +43 1 31332-3500

atomek@kpmg.at
kpmg.at