CyberSecurity – Res Publica eine Verortung!

Joe.pichlmayr@cybersecurityaustria.at

Pichlmayr.j@ikarus.at

ENISA Threat Expecation 2030

Heute….

Londoner Kliniken: Cyberangriff sorgt für abgesagte Operationen

Ein Ransomware-A
dringende Operati

Londoner Kliniken mussten Operationen absagen. (Bild: hxdbzxy/Shutterstock.com)

Supply-Chain Attack!

ser wie das
das King's
e absagen

Heute….


Gestrichen
LH 1943
CROWDSTRIKE
WELT
NACHRICHTENSENDER
FR 9164
Terminal 2
Bildquelle: WELT Screenshots

Security

Microsoft lost it
hack

SIGN IN / UP

Zack Whittak

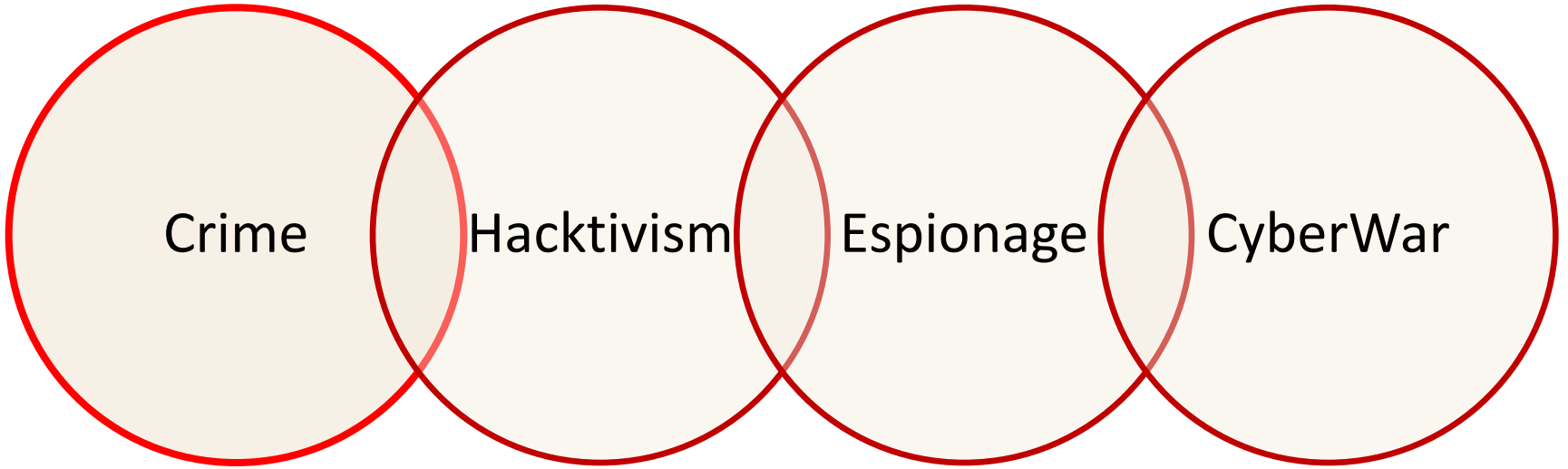
RESEARCH

54

Cyber-Angreifer erbeuten E-Mails aus Microsofts Cybersicherheitsabteilung

Die kriminelle Gruppe Midnight Blizzard hat sich Zugang zu E-Mails von Microsoft-Mitarbeitern verschafft. Sie wollte wohl wissen, was Microsoft über sie weiß.

137



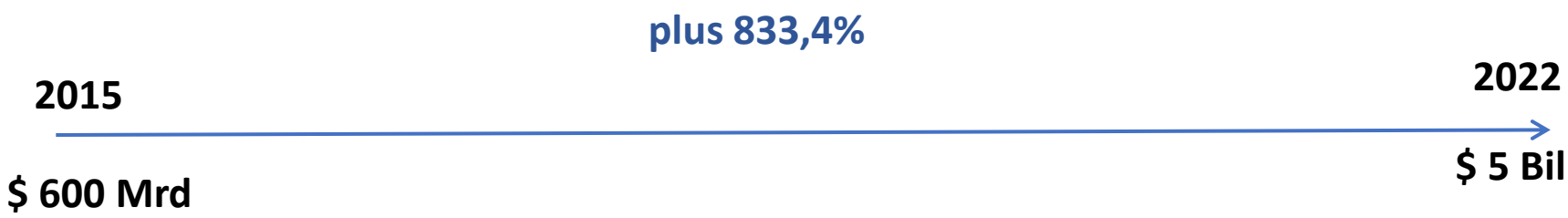
- **Logische Evolution im Angriffsvektor**
  - Vom Einzeltäter zu organisierten hoch-spezialisierten Gruppen
- **Hochkomplexe Nachfrage/Angebot Situation**
  - Fast jeder Bedarf kann “befriedigt” werden
- **Hochspezialisiertes KnowHow**
  - Global agierende Angreifer verfügen über ausreichen KnowHow
- **Finanzielle Motive**
  - Identitätsdiebstahl, Online-Banking und Kreditkartenmißbrauch, Informationsverwertung…

Hochentwickelte Angriffsinfrastrukturen sind für jederman zugänglich !

Successtory CyberCrime

5 Billionen Dollar schwer wird der Markt für CyberCrime eingeschätzt

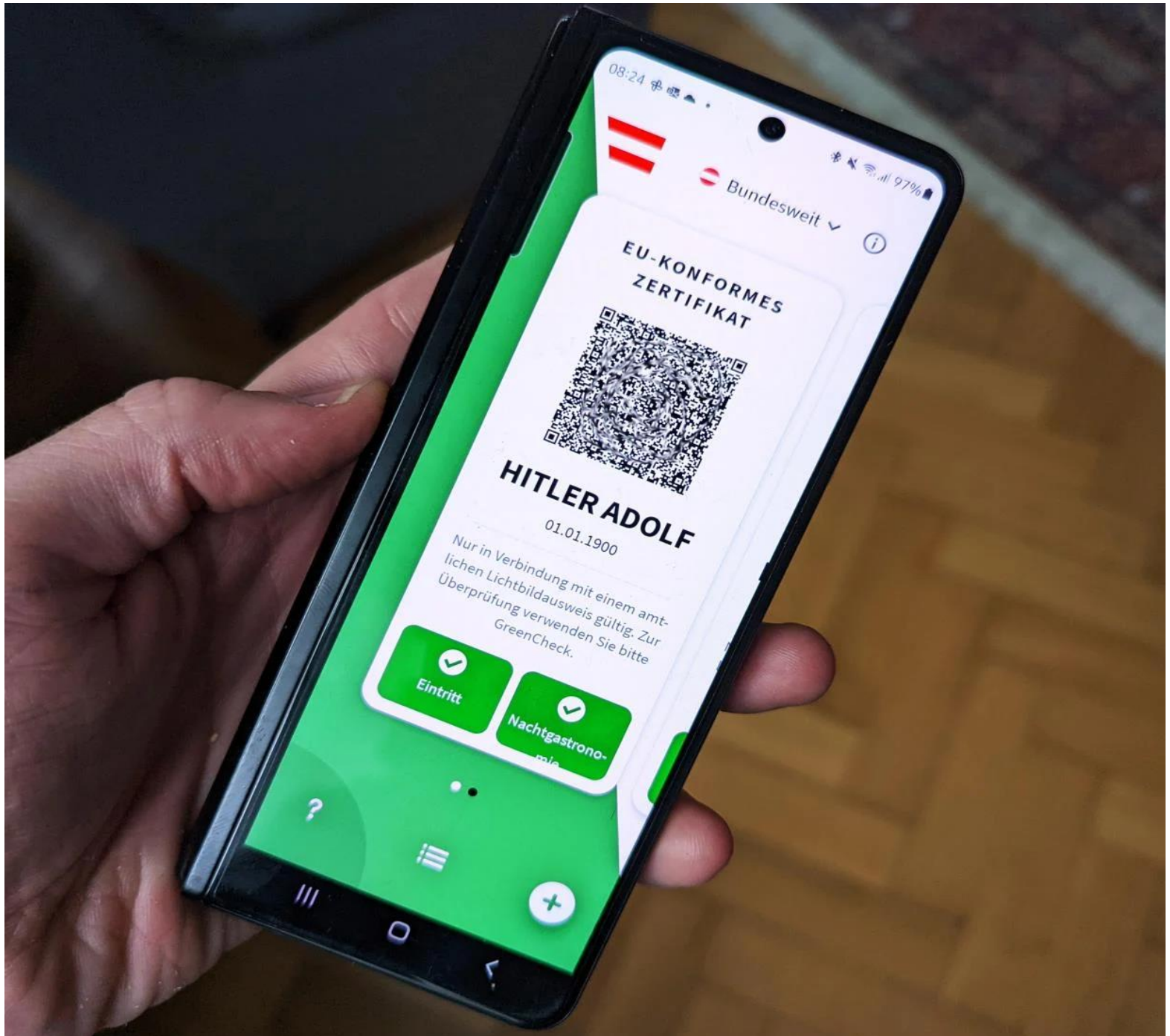
CyberCrime wäre die 3. größte Volkswirtschaft der Welt (lt WEF)



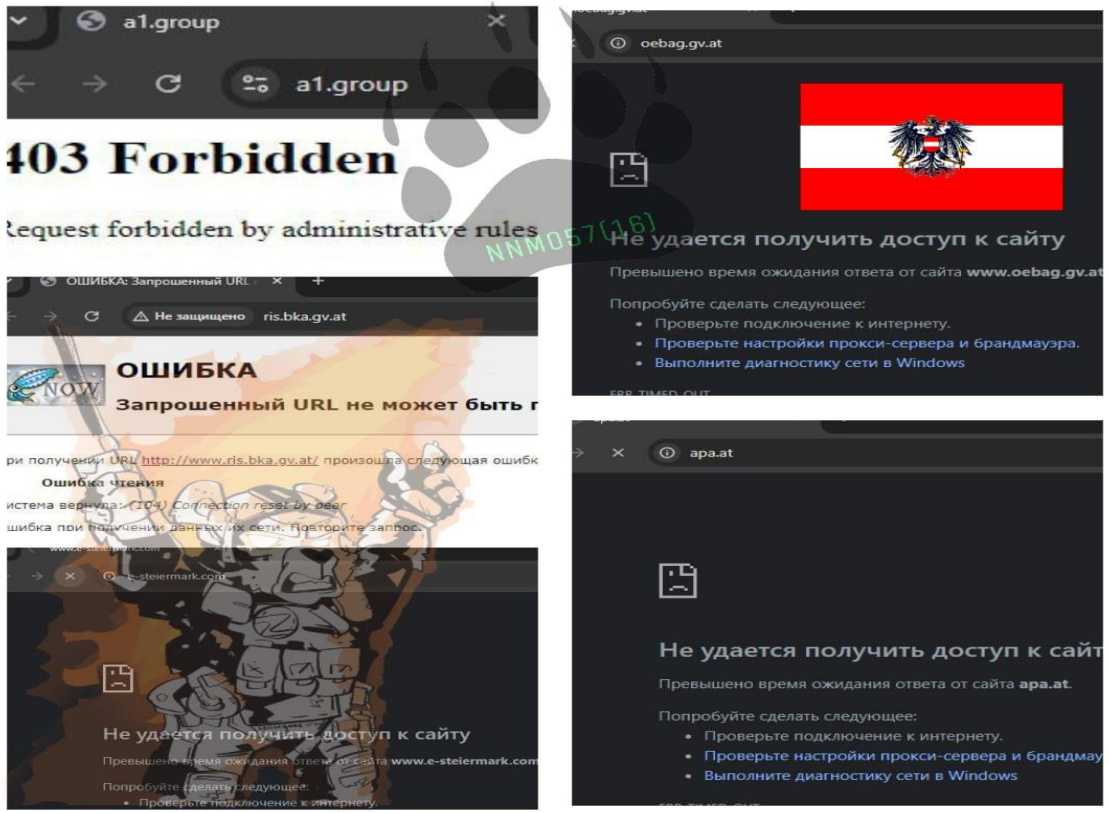
Schadensschätzung 2023: 8 Billionen

https://cybernews.com/editorial/cybercrime-world-third-economy/

https://bit.ly/2NkEbbP


08:24
97%
Bundesweit
EU-KONFORMES ZERTIFIKAT
HITLER ADOLF
01.01.1900
Nur in Verbindung mit einem amtlichen Lichtbildausweis gültig. Zur Überprüfung verwenden Sie bitte GreenCheck.
Eintritt
Nachtgastrono-

Hacktivism



29 сентября граждане Австрии будут выбирать членов 28-го созыва Национального совета — нижней палаты парламента страны. Согласно опросам, ожидается, что ультраправая Австрийская партия свободы (FPÖ) станет лидером, получив 27% голосов и сформировав самую большую фракцию в парламенте. На втором месте, по прогнозам, окажется оппозиционная Социал-демократическая партия Австрии (SPÖ) с поддержкой 23% избирателей. На третьем месте, вероятно, будет Австрийская народная партия (ÖVP) с 22% поддержки, которая входит в правящую коалицию текущего созыва.Мы решили снова навестить Австрию и проверить, как обстоят дела с кибербезопасностью перед предстоящими выборами. Как оказалось, с момента нашего последнего визита ничего не изменилось😈

Am 29. September wählen die österreichischen Bürger die Mitglieder des 28. Umfragen zufolge wird die rechtsextreme Freiheitliche Partei Österreichs (FPÖ) mit 27 Prozent der Stimmen voraussichtlich an der Spitze liegen und die größte Fraktion im Parlament bilden. An zweiter Stelle wird die oppositionelle Sozialdemokratische Partei Österreichs (SPÖ) mit 23 Prozent der Wählerstimmen erwartet. An dritter Stelle wird voraussichtlich die Österreichische Volkspartei (ÖVP) mit 22 % Unterstützung stehen, die Teil der derzeitigen Regierungskoalition ist.Wir haben beschlossen, Österreich erneut zu besuchen, um uns im Vorfeld der bevorstehenden Wahlen über die Cybersicherheit zu informieren. Wie sich herausstellte, hat sich seit unserem letzten Besuch nichts geändert😈.

NoName057(16) DDoSia Target Monitor

🔴 - Targets tool DDoSia 2024-09-25 (updated at 12:55):

Domains .at:

⚠️ www.data.gv.at --> 194.37.74.30

⚠️ www.bmaw.gv.at --> 85.158.225.253

⚠️ www.bmeia.gv.at --> 80.120.70.125

⚠️ www.govcert.gv.at --> 194.37.74.39

⚠️ www.verwaltung.steiermark.at --> 192.26.237.85

⚠️ www.land-oberoesterreich.gv.at --> 194.48.48.82

⚠️ www.bundeskanzleramt.gv.at --> 85.158.224.156

⚠️ oegovwiki.gv.at --> 194.37.74.42

⚠️ www.evi.gv.at --> 20.50.2.18

⚠️ horn.gv.at --> 62.212.163.30

⚠️ www.moelbling.gv.at --> 37.235.57.101

⚠️ www.tirol.gv.at --> 194.8.61.86

⚠️ anmeldung.tirol.gv.at --> 194.8.61.73

⚠️ www.bmlv.gv.at --> 193.171.152.62

⚠️ www.rechnungshof.gv.at --> 194.232.44.12

⚠️ www.jobboerse.gv.at --> 213.133.104.178

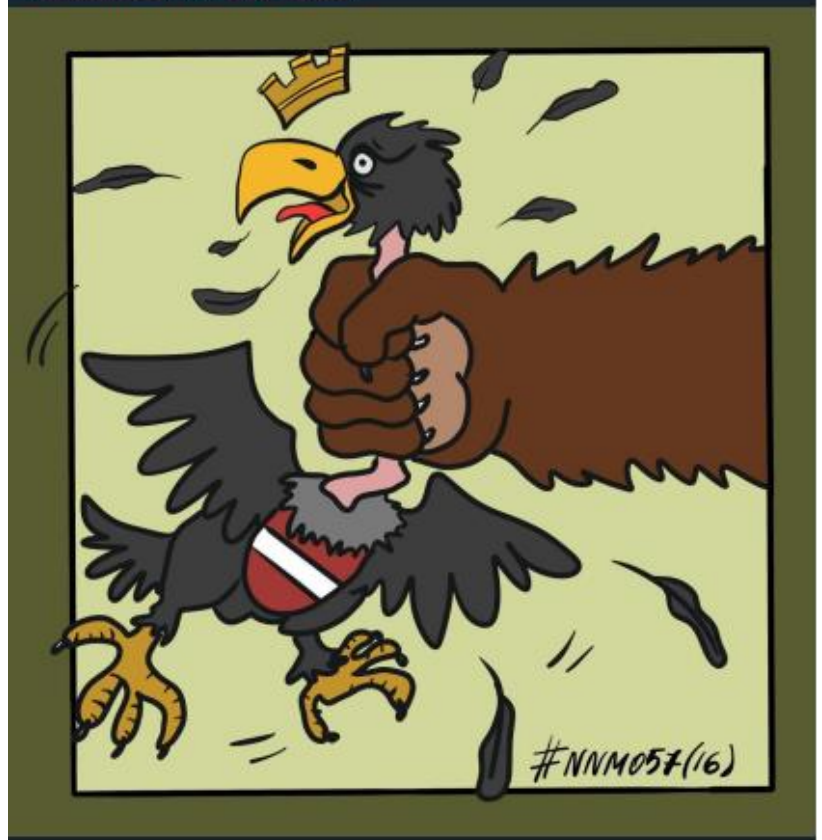
⚠️ www.noe.gv.at --> 194.232.42.155

⚠️ www.kirchschlag.gv.at --> 62.212.163.172

⚠️ hitzendorf.gv.at --> 20.71.225.220

⚠️ www.staedtebund.gv.at --> 193.200.113.177

NoName057(16). Eng version



Here ~~Murzilka magazine~~ the largest Austrian newspaper Kronen Zeitung, with a readership of 3 million people, is interested:

✅ "Were the attacks or just a dress rehearsal?"

✅ "Were the attacks, just a trial run for a much larger attack on Sunday?"

Dear Editorial Board, we answer - The rehearsal is over, the attacks will be integrated into your life as long as the Austrian government spits on its citizens and sponsors the overdue Zelensky, and with your own taxes. Pass this on to all your readers 😈

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

❤️ 3 👍 1 🥰 1 👏 1 🤝 1

IOC Olympic Comitee

pivotMalware

Industroyer

WADA – World AntiDoping Agency

White House

Python/TeleBot.AA backdoor

OSZE

IoC

xTunnel

American Democratic National Committee

LoJax

SEDNIT

CredRaptor

Win32/KillDisk SHA-1

APT28, Fancy Bear,
Sofacy, Pawn Storm,
STRONTIUM, Tsar Team

Hidden IV

TV5Monde

NATO

Deutscher Bundestag

BCS-server

Intercepter-NG

Bank of America

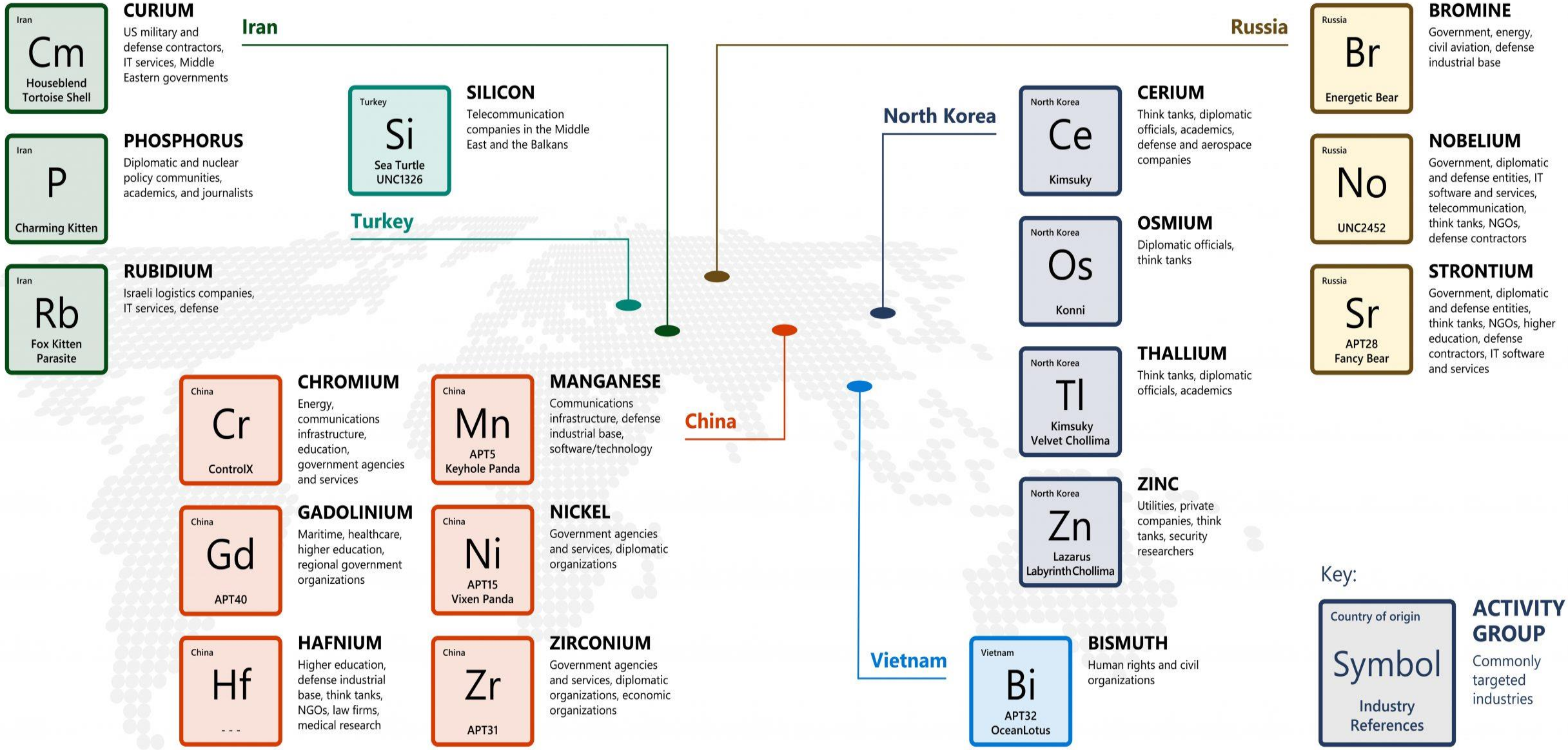
Aber das ist nur ein kleiner Teil..

2020 SolarWinds – SupplyChain Attack via Orion ->18.000 US-Firmen

vom 23. Februar bis zum 8. April 237 Cyberangriffe

die Dateien in Hunderten von Systemen in Dutzenden von Organisationen im Land unwiderruflich zerstörten.

Sample Nation-State Actors

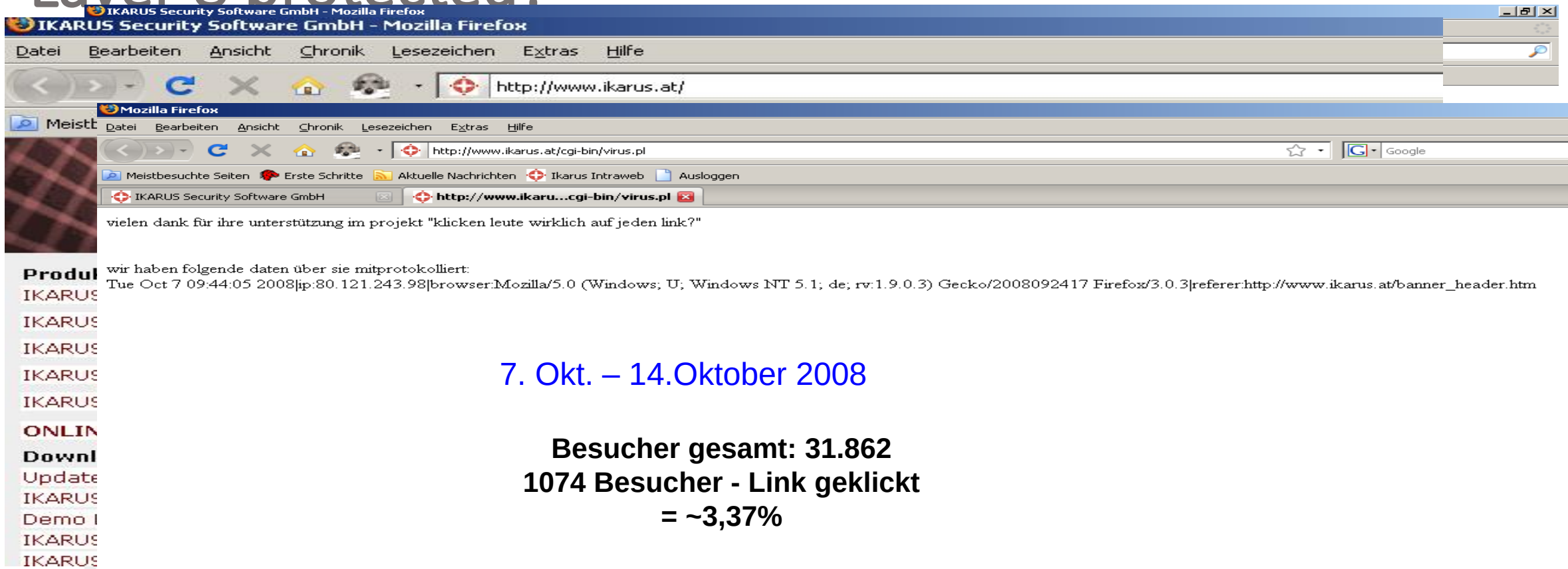


Superkompliziert ?

Superschwierig?

Supereinfach!

Layer 8 protected?



7. Okt. – 14.Oktober 2008

Besucher gesamt: 31.862
1074 Besucher - Link geklickt
= ~3,37%

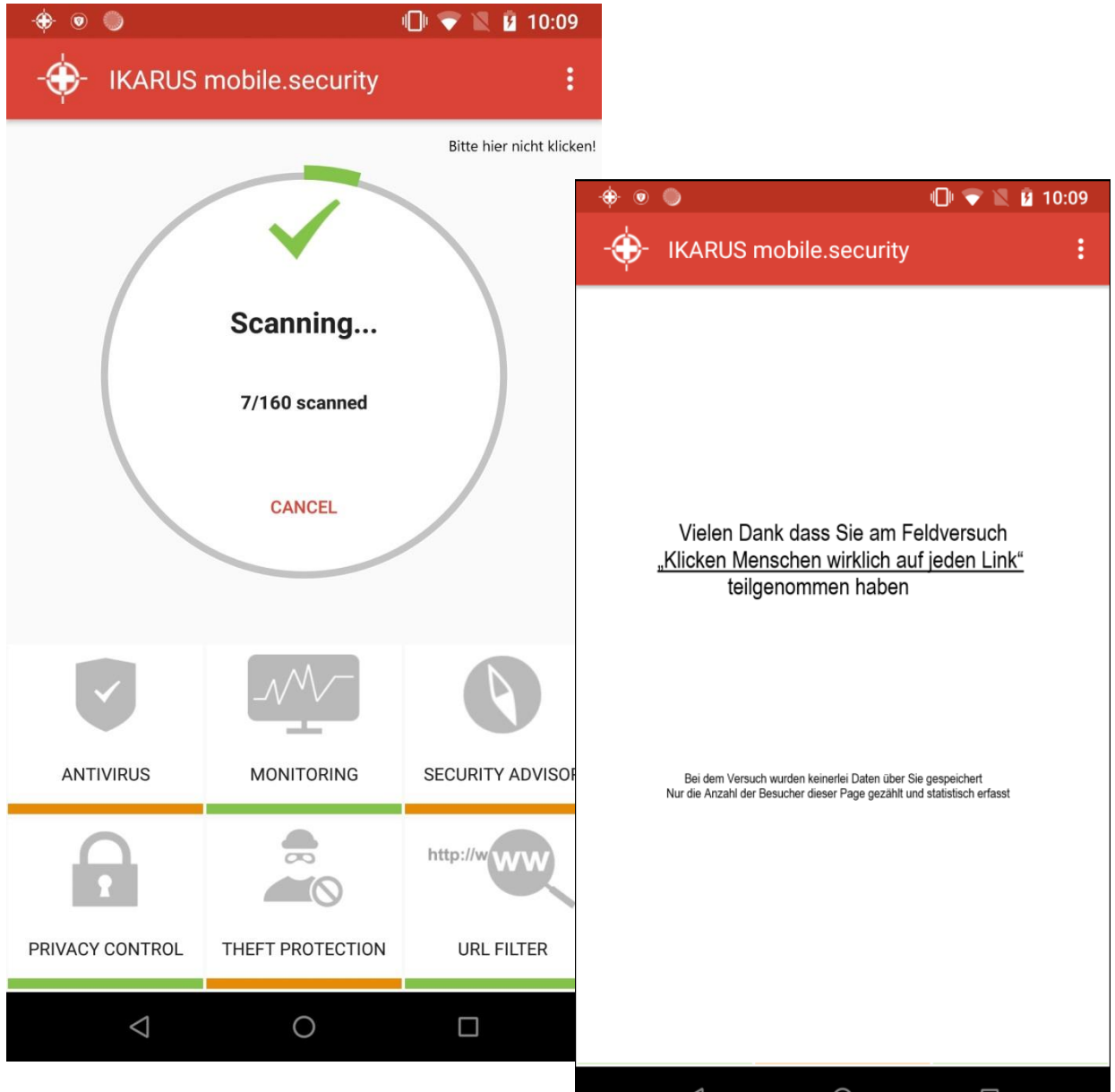
Bedenklich:
Englischsprachige User sogar direkt aus „translate.google.com“

10 Jahre später…

2. bis 12 Oktober 2018

IKARUSmobile - SecurityApp

Installbase = 228.761
75,6 % views on MainScreenpage = 172.943
Klickrate = 5,4% entspricht 9.338



Starlink-Antenne heimlich auf US-Kriegsschiff montiert

Plötzlich war da auf der USS Manchester ein WLAN namens STINKY. Die Betreiberin leugnete, bis sie vor dem Militärgericht stand.

Die USS Manchester (LCS 14) ist von der sanften Anmut eines Cybertrucks. Da fällt eine Starlink-Antenne mehr oder weniger nicht auf. (Bild: US Navy)

Ungenehmigte Handynutzung Schuld?

Russland macht eigene Soldaten für ukrainischen Angriff mit 89 Toten verantwortlich

In der Neujahrsnacht starben russischen Angaben zufolge 89 Soldaten durch Raketen aus der Ukraine. Telefonsignale hätten es den Ukrainern erlaubt, „die Koordinaten des Standorts von Militärpersonal“ auszumachen. Britische Geheimdienste verweisen auf weitere „unprofessionelle Praktiken“ des Militärs und geben diesem eine Mitschuld an der Opferzahl.

Edward Snowden (2013): Snowden, ein ehemaliger NSA-Mitarbeiter, enthüllte geheime Überwachungsprogramme der US-Regierung. Obwohl er Zugang zu hochsensiblen Informationen hatte, verließ er die Sicherheitsprotokolle und gab vertrauliche Dokumente an die Presse weiter.

Eine Betrachtung

self replicating code, Construction Kits, file infector, polymorphism, trojan malware, exploiting, backdoors, sniffer macro virus, packet manipulation, worms, bot nets, denial of service, mobile malware, rootkit/ stealth

Steigende Zahl, Komplexität und "Intelligenz" von Angriffen

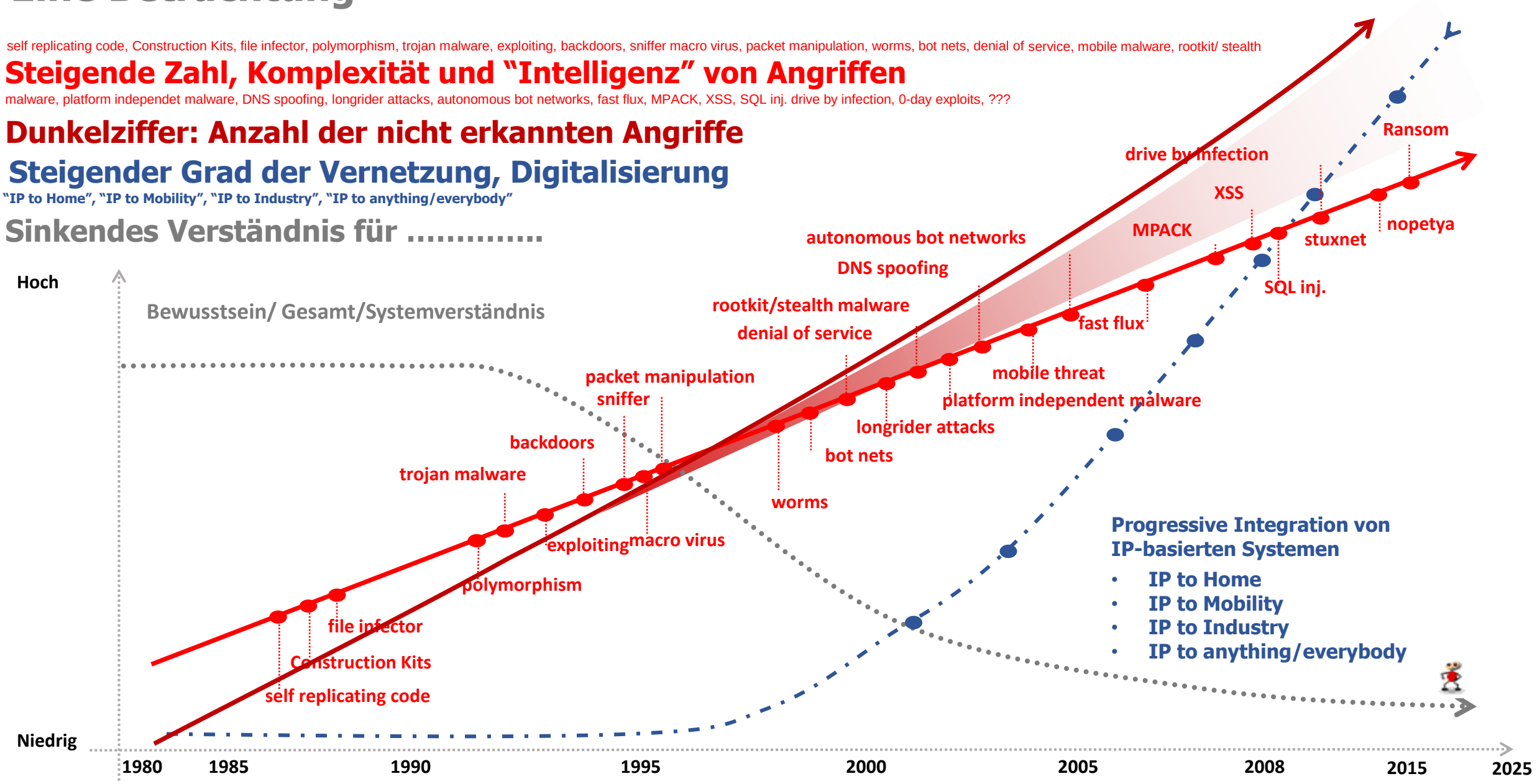
malware, platform independet malware, DNS spoofing, longrider attacks, autonomous bot networks, fast flux, MPACK, XSS, SQL inj. drive by infection, 0-day exploits, ???

Dunkelziffer: Anzahl der nicht erkannten Angriffe

Steigender Grad der Vernetzung, Digitalisierung

"IP to Home", "IP to Mobility", "IP to Industry", "IP to anything/everybody"

Sinkendes Verständnis für .....



Wir fassen zusammen

self replicating code, Construction Kits, file infector, polymorphism, trojan malware, exploiting, backdoors, sniffer macro virus, packet manipulation, worms, bot nets, denial of

Steigende Zahl, Komplexität und Intelligenz von Angriffen

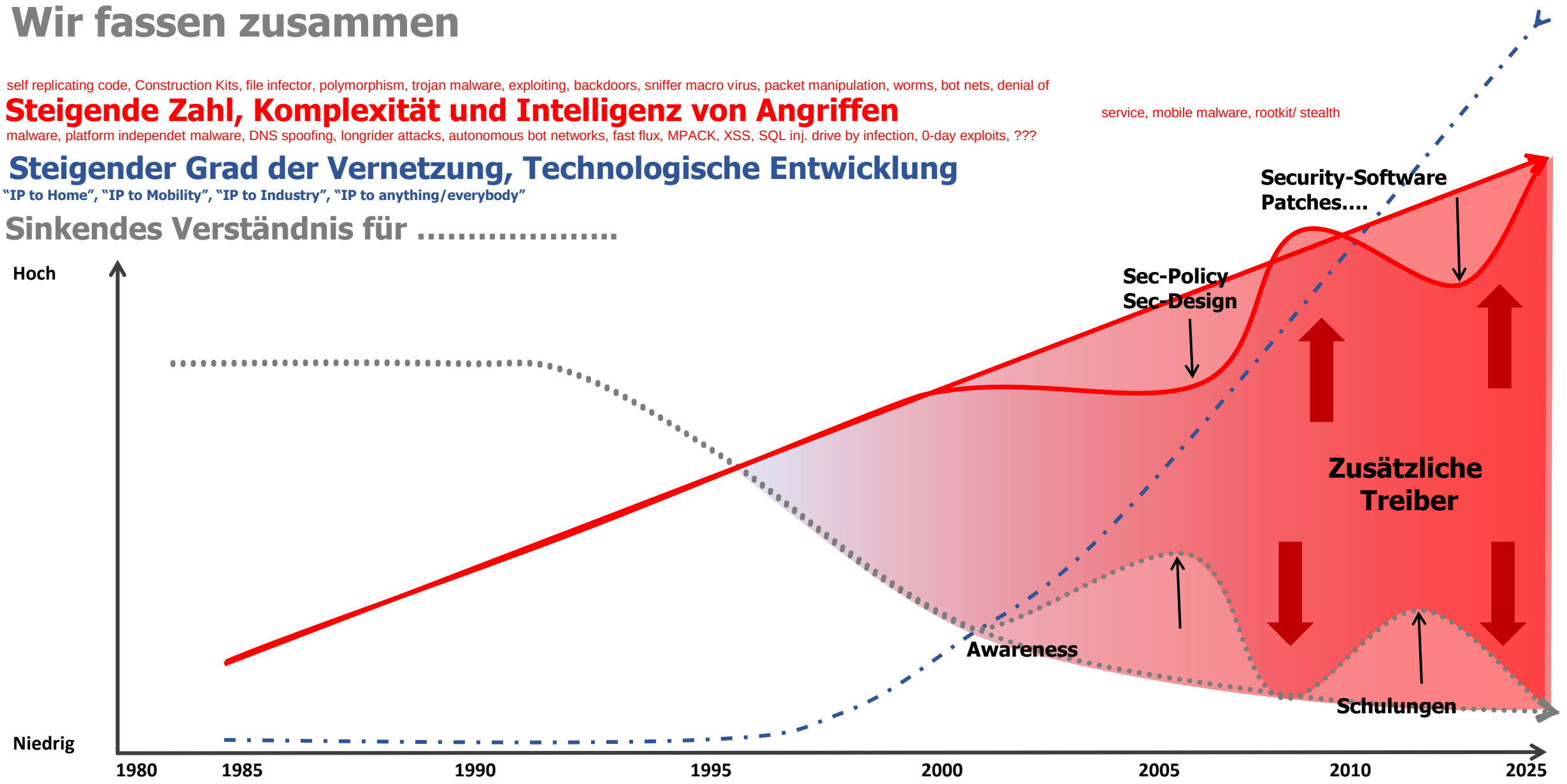
service, mobile malware, rootkit/ stealth

malware, platform independet malware, DNS spoofing, longrider attacks, autonomous bot networks, fast flux, MPACK, XSS, SQL inj. drive by infection, 0-day exploits, ???

Steigender Grad der Vernetzung, Technologische Entwicklung

"IP to Home", "IP to Mobility", "IP to Industry", "IP to anything/everybody"

Sinkendes Verständnis für .....



CYBER SECURITY AUSTRIA

CyberSecurity

– res publica –

ES geht uns alle an!

www.cybersecurityaustria.at

Vielen DANK

und Kopf hoch

Joe Pichlmayr, CEO Ikarus, Vorstand CybersecurityAustria, joe@ikarus.at