CyberSecurity

– res publica –

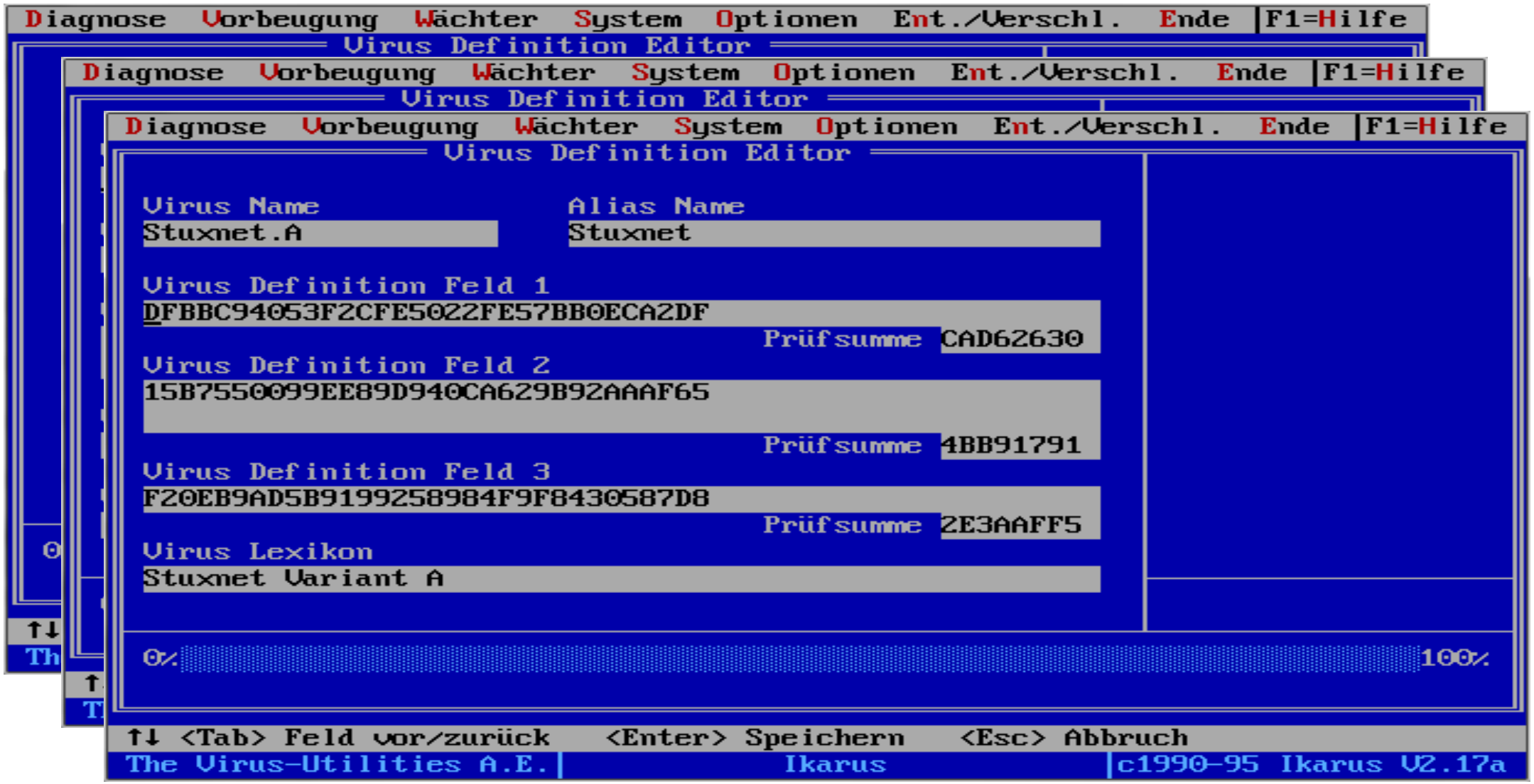
Es geht uns ALLE an !

www.cybersecurityaustria.at

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

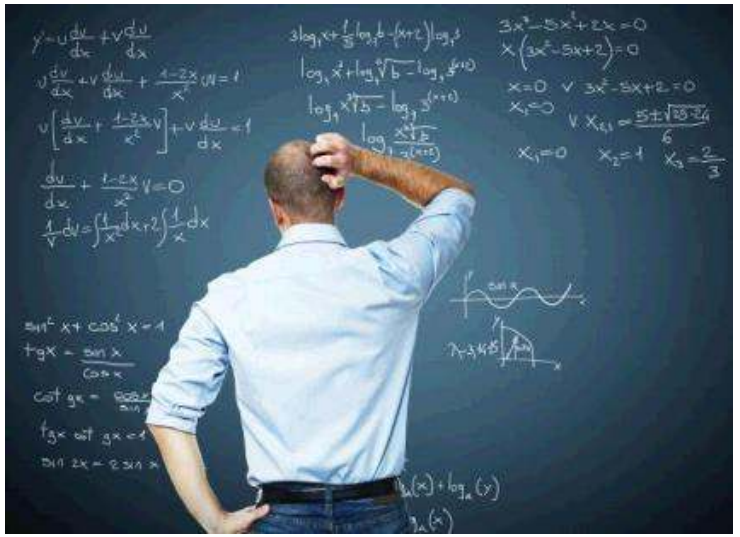

PC Tools Deluxe R6.22
Disk View/Edit Service
Path=A:
Absolute sector 0000000, System BOOT
value
elcome to
ngeon
86 Basit
(put) Lt
COMPUTER
S..730 NI
CK ALLAMA
0176(00B0) 20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20 IQBAL TOWN
0192(00C0) 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52 LAHOR
0208(00D0) 45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E E-PAKISTAN..PHON
0224(00E0) 45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38 E :430791,443248
0240(00F0) 2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20 ,280530.
Home=beg of file/disk End=end of file/disk
ESC=Exit PgDn=forward PgUp=back F2=chg sector num F3=edit F4=get name
BASF
VIRUSVAARA!
Älä käytä!
BRAIN.A
Microsoft

Selbst ist der Mann.....



Gute alte Zeit…

- Durchschnittliche Anzahl von Angriffen durch Schadprogramme
  - sehr niedrig, weniger als einige hundert pro Monat



- Typische Angriffe (damals)
  - einfach erkennbar, zumeist Zerstörung von Systemen/Daten
  - nur wenige hoch spezialisierte Angriffe "in freier Wildbahn“

- Kaum finanzielles Interesse
  - Angriffe sollten zumeist nur demonstrieren was möglich ist bzw. wer “den coolsten Virus/Angriff” gemacht hat

- Abhängigkeit von einer funktionierenden IT-Umgebung
  - weniger kritisch als heute
  - IT Ausfälle waren leichter zu kompensieren, da nicht alle Arbeiten von der IT abhängig waren

Gesamtnacktzahl

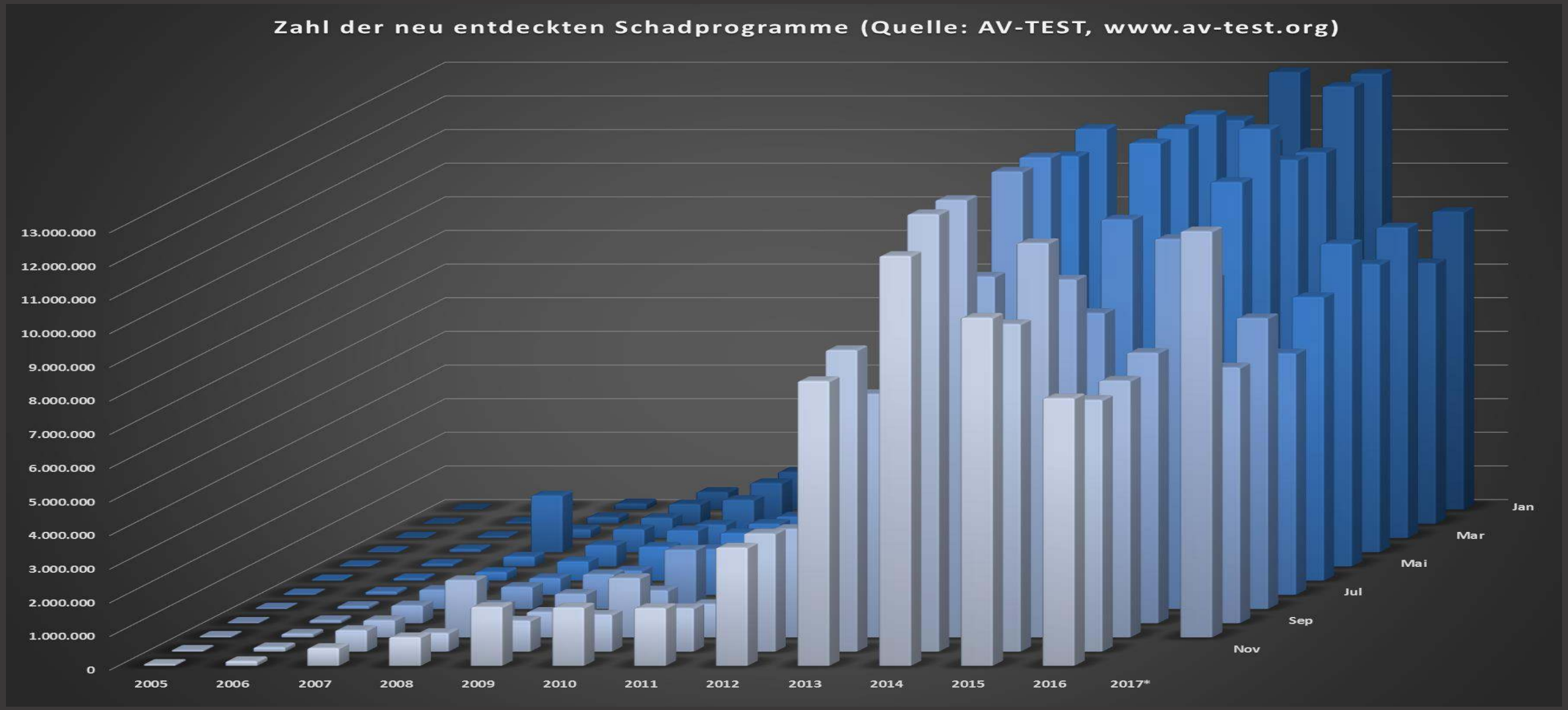
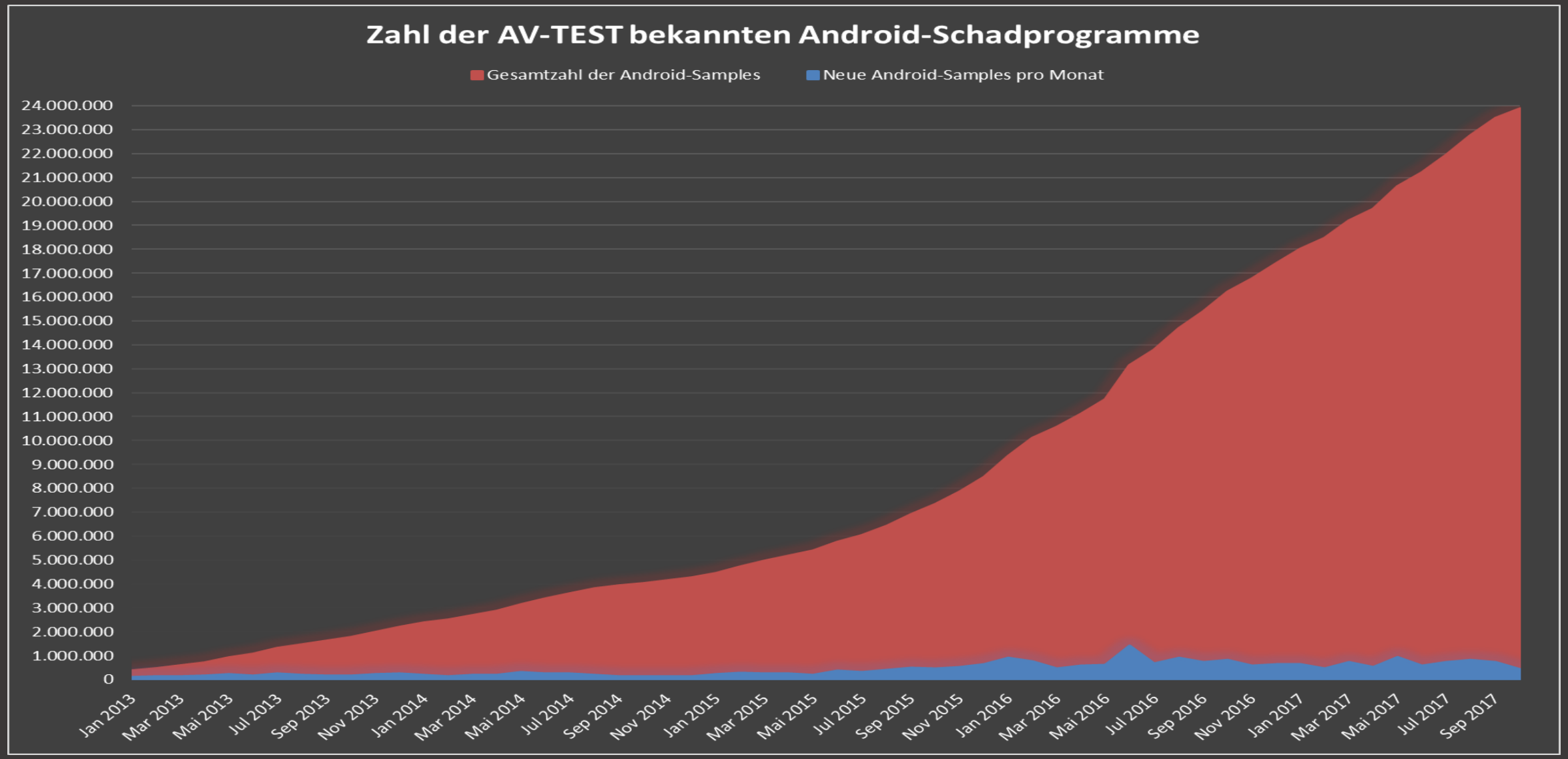


Table: T_VBASE Samples

Year	Month	Count	Accumulated
⊞ 2015	Total	16.207.874	16.207.874
⊞ 2016	Total	16.857.833	33.065.707
⊟ 2017	1	1.281.104	34.346.811
	2	1.052.945	35.399.756
	3	1.129.348	36.529.104
	4	1.055.355	37.584.459
	5	1.262.208	38.846.667
	6	974.613	39.821.280
	7	1.393.360	41.214.640
	8	991.026	42.205.666
	9	851.061	43.056.727
	10	860.826	43.917.553
	11	1.093.937	45.011.490
	12	1.068.103	46.079.593
	Total	13.013.886	46.079.593
⊟ 2018	1	2.176.660	48.256.253
	2	1.424.330	49.680.583
	3	1.221.398	50.901.981
	Total	4.822.388	50.901.981
Total		50.901.981	50.901.981

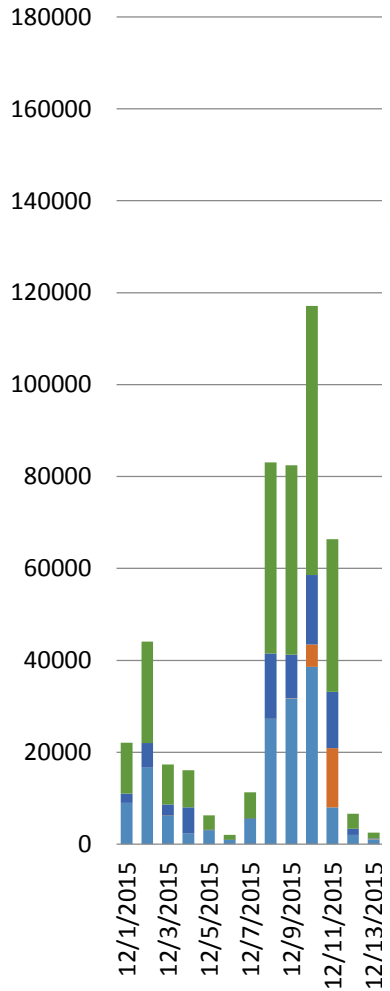
	Jan	Feb	Mar	Oct	Nov	Dec	TOTAL
1984	0	0	0	0	0	12	12
1985	41	23	67	36	60	28	553
1986	75	34	59	38	43	27	909
1987	46	31	127	254	51	75	1.399
1988	102	133	57	158	115	113	1.728
1989	182	258	74	694	249	143	2.623
1990	667	264	235	189	2.792	770	9.027
1991	263	659	339	635	556	145	18.386
1992	481	412	451	18.653	6.416	1.497	36.818
1993	873	627	813	468	393	571	12.298
1994	9.424	681	2.840	2.132	1.112	954	28.625
1995	1.923	783	655	1.635	1.153	1.108	15.974
1996	1.494	8.492	1.328	1.704	3.443	3.472	36.822
1997	9.318	3.805	14.774	9.020	14.863	5.467	137.806
1998	11.767	3.399	58.160	13.269	4.027	5.853	177.535
2012	3.135.714	2.410.582	2.750.538	2.3	224.406	3.509.259	3.513.831	34.446.953
2013	4.731.939	5.802.849	5.791.814	6.0	233.202	8.961.333	8.462.157	83.194.284
2014	9.206.953	5.861.014	9.235.784	8.4	568.645	14.763.240	12.180.461	143.140.451
2015	13.262.547	11.306.324	12.412.679	14.6	719.830	9.733.742	10.344.859	143.974.553
2016	12.950.733	12.993.271	11.461.997	11.6	629.305	7.479.877	7.951.142	127.473.381
2017*	8.852.322	7.743.482	9.227.587	8.5	070.442			87.870.864
2008	523.494	580.657	595.260	1.703.593	554.564	851.491	8.378.929
2009	1.118.142	1.207.722	1.128.000	758.368	919.858	1.750.590	12.396.824
2010	1.470.794	1.827.866	1.855.211	1.762.269	1.099.735	1.732.159	17.569.911
2011	1.697.473	1.673.091	1.656.884	990.347	1.291.495	1.717.242	18.207.575
2012	3.135.714	2.410.582	2.750.538	3.224.406	3.509.259	3.513.831	34.446.953
2013	4.731.939	5.802.849	5.791.814	7.233.202	8.961.333	8.462.157	83.194.284
2014	9.206.953	5.861.014	9.235.784	14.568.645	14.763.240	12.180.461	143.140.451
2015	13.262.547	11.306.324	12.412.679	11.719.830	9.733.742	10.344.859	143.974.553
2016	12.950.733	12.993.271	11.461.997	7.629.305	7.479.877	7.951.142	127.473.381
2017*	8.852.322	7.743.482	9.227.587	12.070.442			87.870.864
TOTAL	57.276.274	51.741.879	56.582.784	62.442.298	49.218.869	49.294.107	**685.359.044**

Android

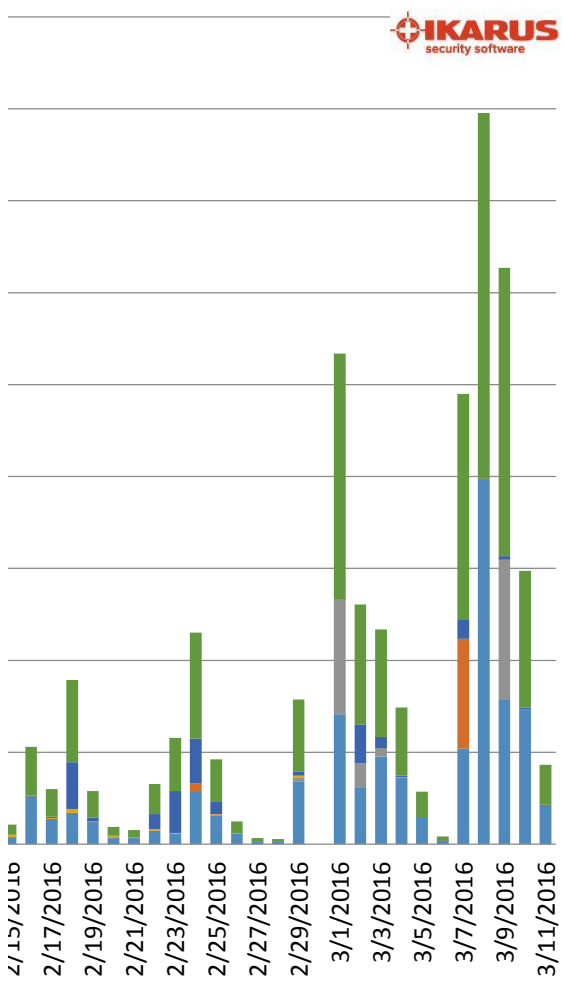

Zahl der AV-TEST bekannten Android-Schadprogramme
Gesamtzahl der Android-Samples
Neue Android-Samples pro Monat
24.000.000
23.000.000
22.000.000
21.000.000
20.000.000
19.000.000
18.000.000
17.000.000
16.000.000
15.000.000
14.000.000
13.000.000
12.000.000
11.000.000
10.000.000
9.000.000
8.000.000
7.000.000
6.000.000
5.000.000
4.000.000
3.000.000
2.000.000
1.000.000
0
Jan 2013
Mar 2013
Mai 2013
Jul 2013
Sep 2013
Nov 2013
Jan 2014
Mar 2014
Mai 2014
Jul 2014
Sep 2014
Nov 2014
Jan 2015
Mar 2015
Mai 2015
Jul 2015
Sep 2015
Nov 2015
Jan 2016
Mar 2016
Mai 2016
Jul 2016
Sep 2016
Nov 2016
Jan 2017
Mar 2017
Mai 2017
Jul 2017
Sep 2017

Ransom

in Österreich



	⊞ 2015	⊞ 2016	⊞ 2017	Gesamt
fullname	Gesamt	Gesamt	Gesamt	
Ransom.Win32.Exxroute		10689		10689
Ransom.Win32.Lyposit			5876	5876
Trojan.AndroidOS.Locker	3302	13371	21873	38546
Trojan.AndroidOS.Lockerpin		611	4334	4945
Trojan.AndroidOS.SLocker		1771	164	1935
Trojan.Ransomer	468	29424	1754	31646
Trojan-Downloader.CTBLocker	7507	494		8001
Trojan-Ransom.AndroidOS.PornLocker	1876	9504	293	11673
Trojan-Ransom.Cerber		3213	149	3362
Trojan-Ransom.CryptoWall3	3993	9056	1808	14857
Trojan-Ransom.CTBLocker	5615	305	1202	7122
Trojan-Ransom.Locky	6096	10580	6026	22702
Trojan-Ransom.Nemucod	103	25009		25112
Trojan-Ransom.Script.CryptoWall		1575		1575
Trojan-Ransom.Script.Locky		182936	13290	196226
Trojan-Ransom.Script.Nemucod	39739	186509	87	226335
Trojan-Ransom.Script.TeslaCrypt	2783	6108	98	8989
Trojan-Ransom.Win32.Blocker	14662	8770	3556	26988
Trojan-Ransom.Win32.PornoBlocker	3962	4149	2619	10730
Virus.PolyRansom	5947	224		6171
Virus-Ransom.FileLocker	21751	8330	336	30417
Gesamt	142468	539891	87828	770187



Report generation time: 17.11.2017 10:55:33

Schiller Reloaded

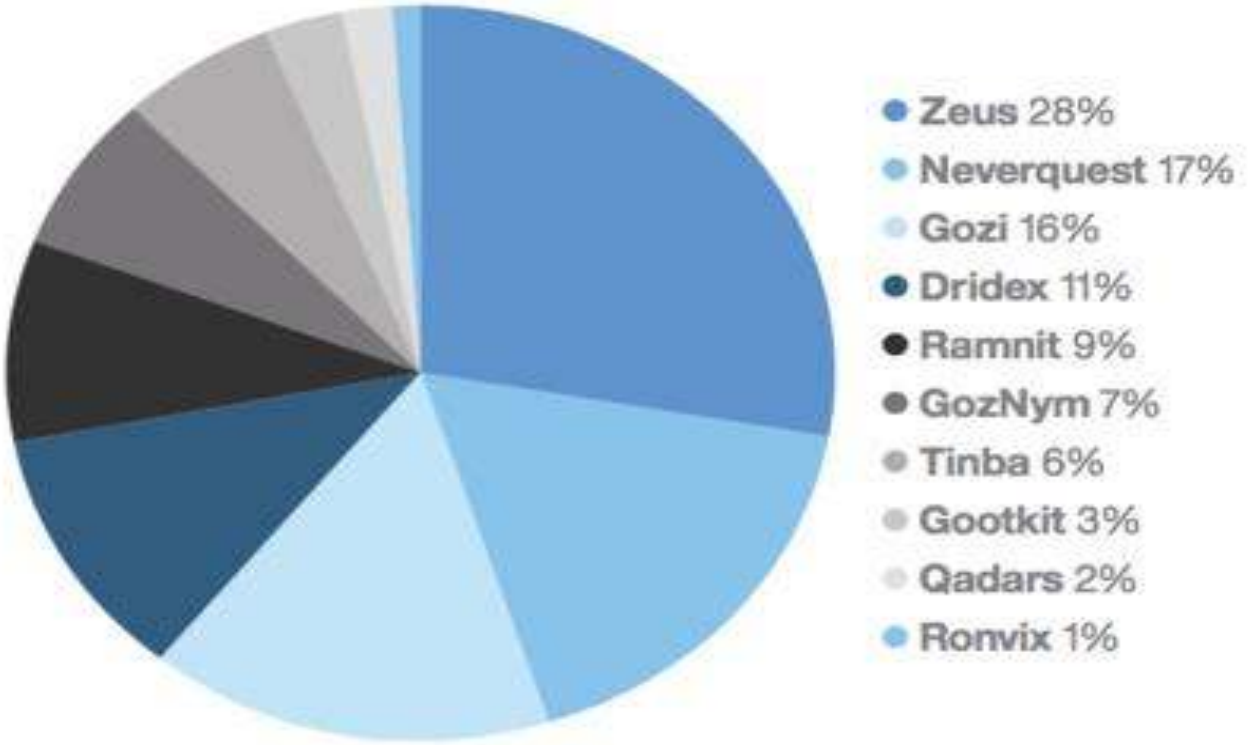
Ransomware

- Entwicklung von Ransomware
- Bedrohungsszenarien auf Grund der arbeitsteiligen Spezialisierung
- Was wird nach PC/Tablett und Smartphone verschlüsselt?
- Was kann ich dagegen Unternehmen ?

Rund 350 aktive Ransom-Familien

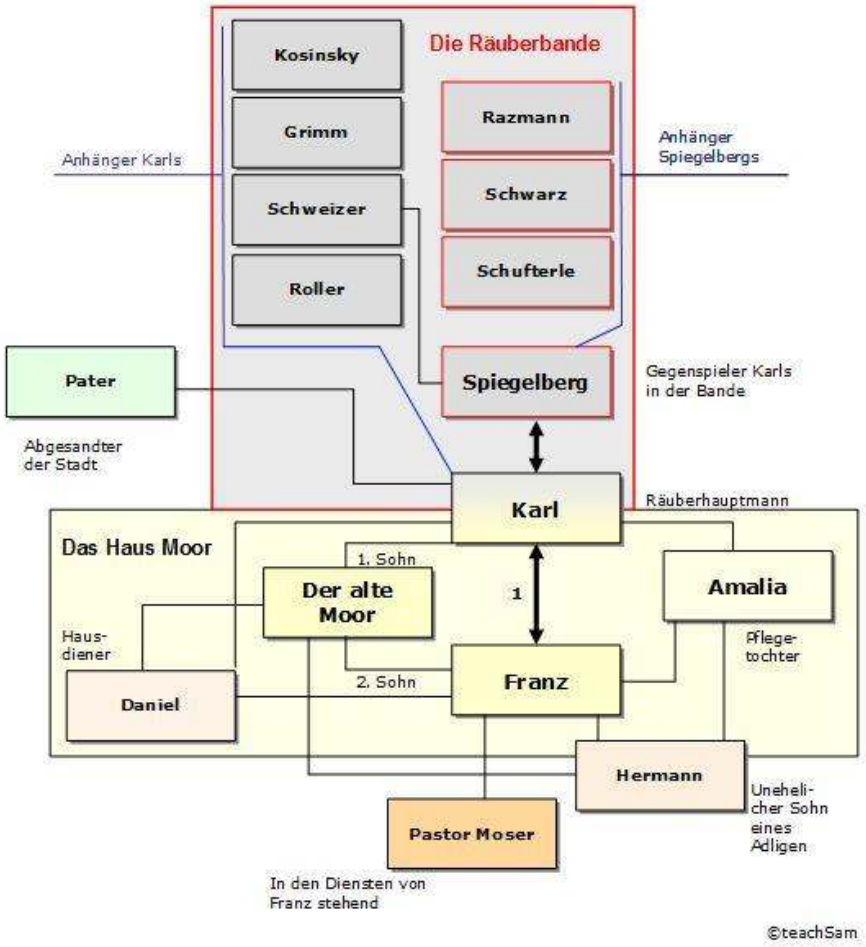
777, 7ev3n, 7h9r, 7zipper, 8lock8, ACCDFISA v2.0, AdamLocker, AES_KEY_GEN_ASSIST, **AES-NI**, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Alma Locker, Alpha, AMBA, **AnDROid**, AngryDuck, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ASN1 Encoder, AutoLocky, AxCrypter, BadBlock, BadEncript, Bandarchor, BankAccountSummary, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitStak, Black Feather, Black Shades, Blocatto, Booyah, BrainCrypt, Brazilian Ransomware, BTCamant, Bucbi, BuyUnlockCode, Cancer, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, CHIP, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Coverton, Cripton, CrptXXX, **Cry9**, **Cryakl**, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt38, CryptConsole, CryptFuck, CryptInfinite, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLuck, CryptoMix, CryptoMix Revenge, CryptON, Crypton, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, CTB-Faker, CTB-Locker, Damage, Deadly, DEDCryptor, DeriaLock, Dharma (.dharma), Dharma (.wallet), Digisom, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, Domino, Done, **DoNotChange**, DXXD, DynA-Crypt, ECLR Ransomware, EdgeLocker, EduCrypt, El Polocker, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Enjey Crypter, EnkripsiPC, Erebus, Evil, Exotic, Fabiansomware, Fadesoft, Fantom, FenixLocker, FindZip, FireCrypt, FLKR, Flyper, FS0ciety, FuckSociety, FunFact, GC47, GhostCrypt, Globe, **Globe (Broken)**, Globe3, GlobeImposter, GlobeImposter 2.0, GOG, GoldenEye, Gomasom, GPCode, HadesLocker, HappyDayzz, Heimdall, **Help50**, HelpDCFile, Herbst, Hermes, Hermes 2.0, Hi Buddy!, HollyCrypt, HolyCrypt, Hucky, HydraCrypt, IFN643, iRansom, Ishtar, Jack.Pot, Jager, JapanLocker, Jigsaw, Jigsaw (Updated), JobCrypter, JuicyLemon, Kaenlupuf, Karma, Karmen, Kasiski, KawaiiLocker, KeRanger, KeyBTC, KEYHolder, KillerLocker, KimcilWare, Kirk, Kolobo, Kostya, Kozy.Jozy, Kraken, KratosCrypt, Krider, Kriptovor, KryptoLocker, L33TAF Locker, LambdaLocker, LeChiffre, LLTP, Lock2017, Lock93, Locked-In, LockLock, Locky, Lortok, LoveServer, LowLevel04, **MafiaWare**, Magic, Maktub Locker, Marlboro, MarsJoke, Matrix, Meteoritan, MirCop, MireWare, Mischa, MNS CryptoLocker, Mobef, MOTD, MRCR1, n1n1n1, NanoLocker, NCrypt, NegozI, Nemucod, Nemucod-7z, Netix, Nhtnwcuf, NMoreira, NMoreira 2.0, Nuke, NullByte, **NxRansomware**, ODCODC, OpenToYou, OzozaLocker, PadCrypt, PayDay, PaySafeGen, **PClock**, PClock (Updated), Philadelphia, Pickles, PopCornTime, Potato, PowerLocky, PowerShell Locker, PowerWare, **Pr0tector**, PrincessLocker, PrincessLocker 2.0, Project34, Protected Ransomware, PyL33T, R980, RAA-SEP, Radamant, Radamant v2.1, RanRan, RansomCuck, RansomPlus, RarVault, Razy, REKTLocker, RemindMe, RenLocker, Roga, Rokku, RoshaLock, RotorCrypt, Roza, Russian EDA2, SADStory, Sage 2.0, SamSam, Sanction, **Sanctions**, Satan, Satana, S ellLocker, Shigo, ShinoL imple_Encoder, Smrss32, SNSLocker, Spora, Sport, SQ_, Stampado, SuperCrypt, Surprise, SZFLocker, Team XRat, Telec aCrypt 2.x, TeslaCrypt 3 4.0, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troldesh / Shade, TrueCrypter, TrumpLocker, UCCU, UmbreCrypt, Un nown Crypted, Unknow vn XTBL, Ur 2 2.0, UserFil V8Locker, VaultCrypt, VenisRansomware, Venus Vortex, VxLock, **Wanna** ire Locker, V onderCrypte , Xorist, Xort, XRTN, XTP Locker 5.0, XYZWare nsom, zCrypt, Zekwacry ZimbraCryp

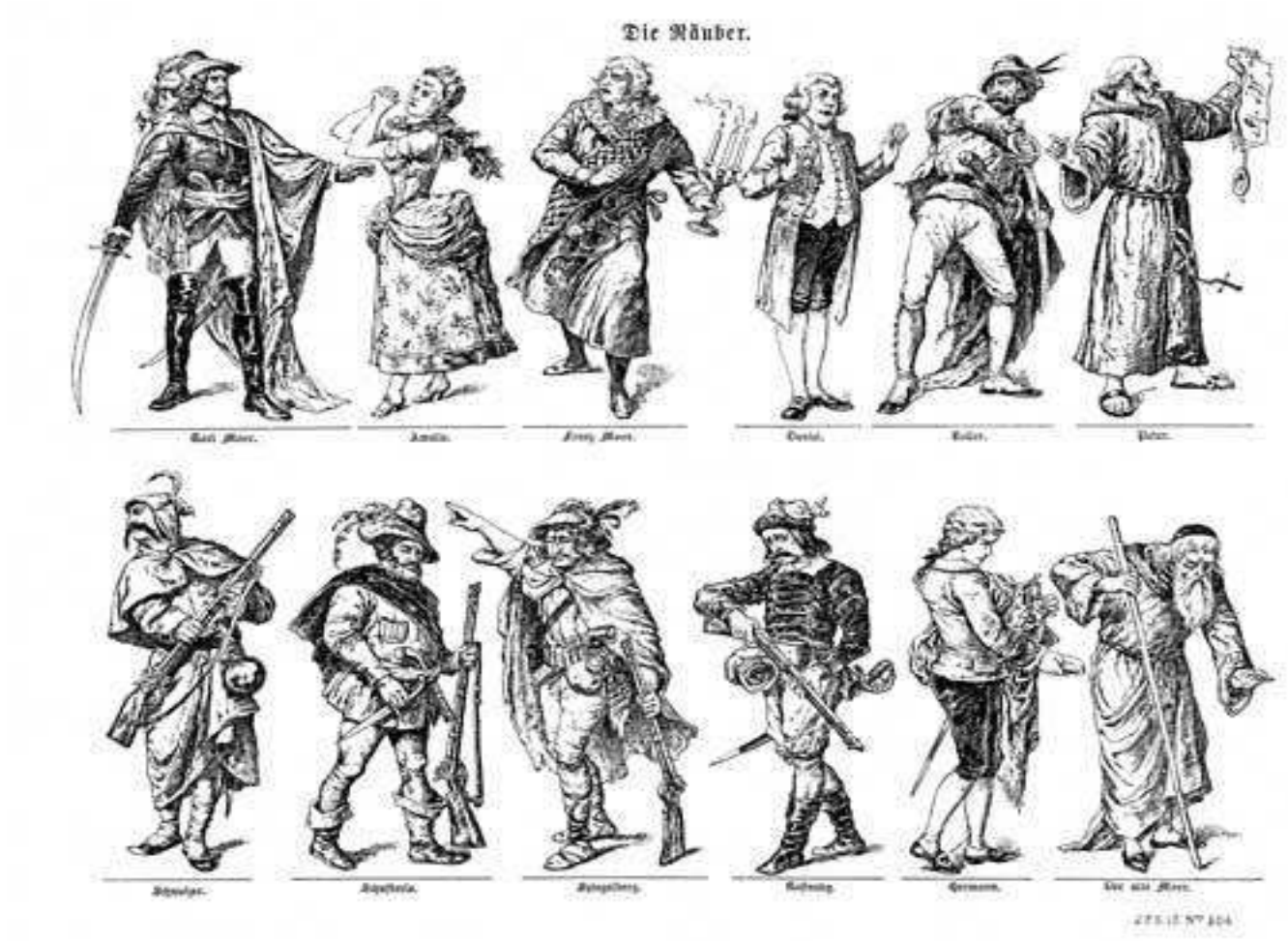
Top – OnlineBanking Trojans 2017



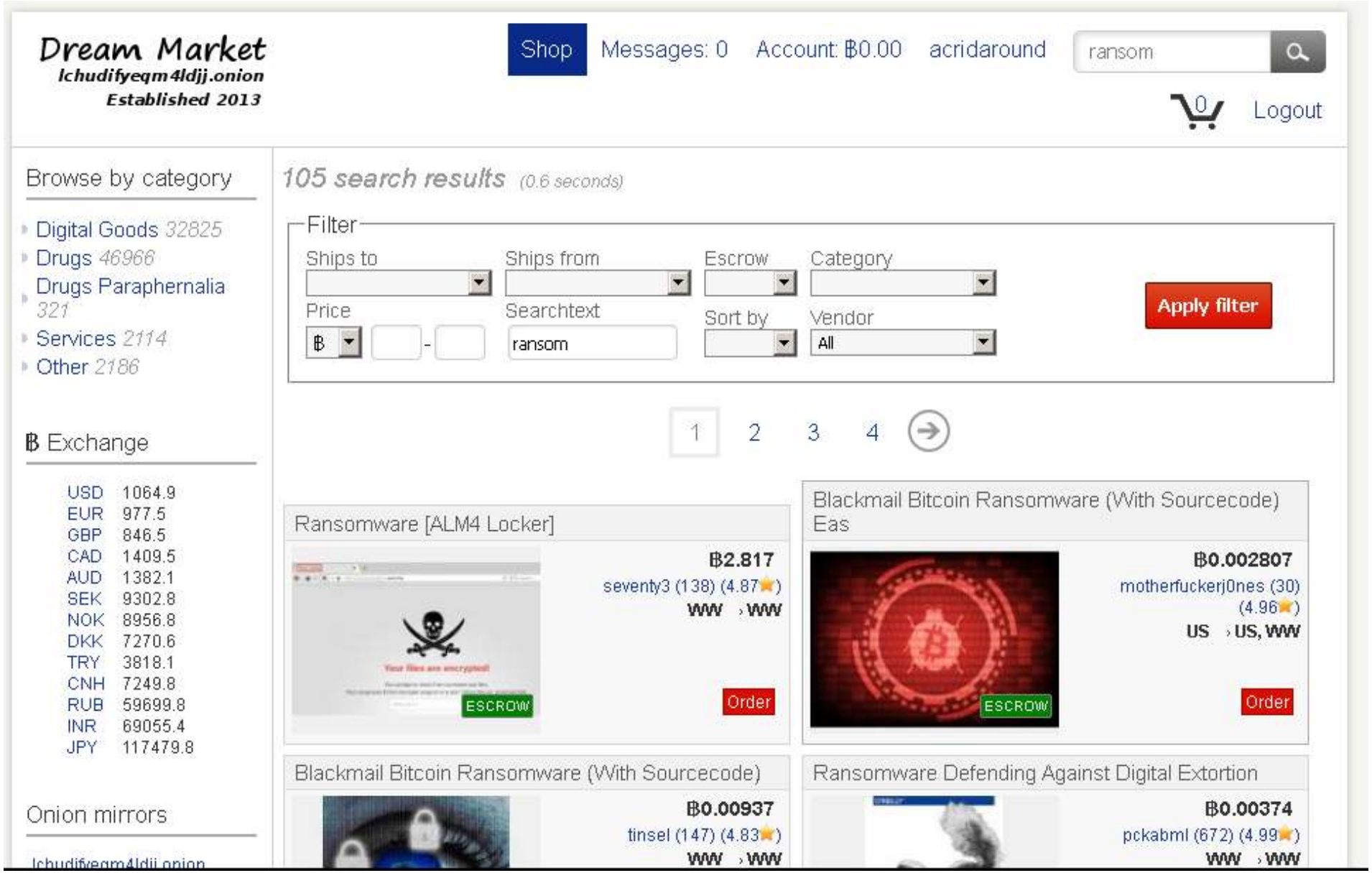
Quelle: IBM XForce

Arbeitsteilig Organisiert

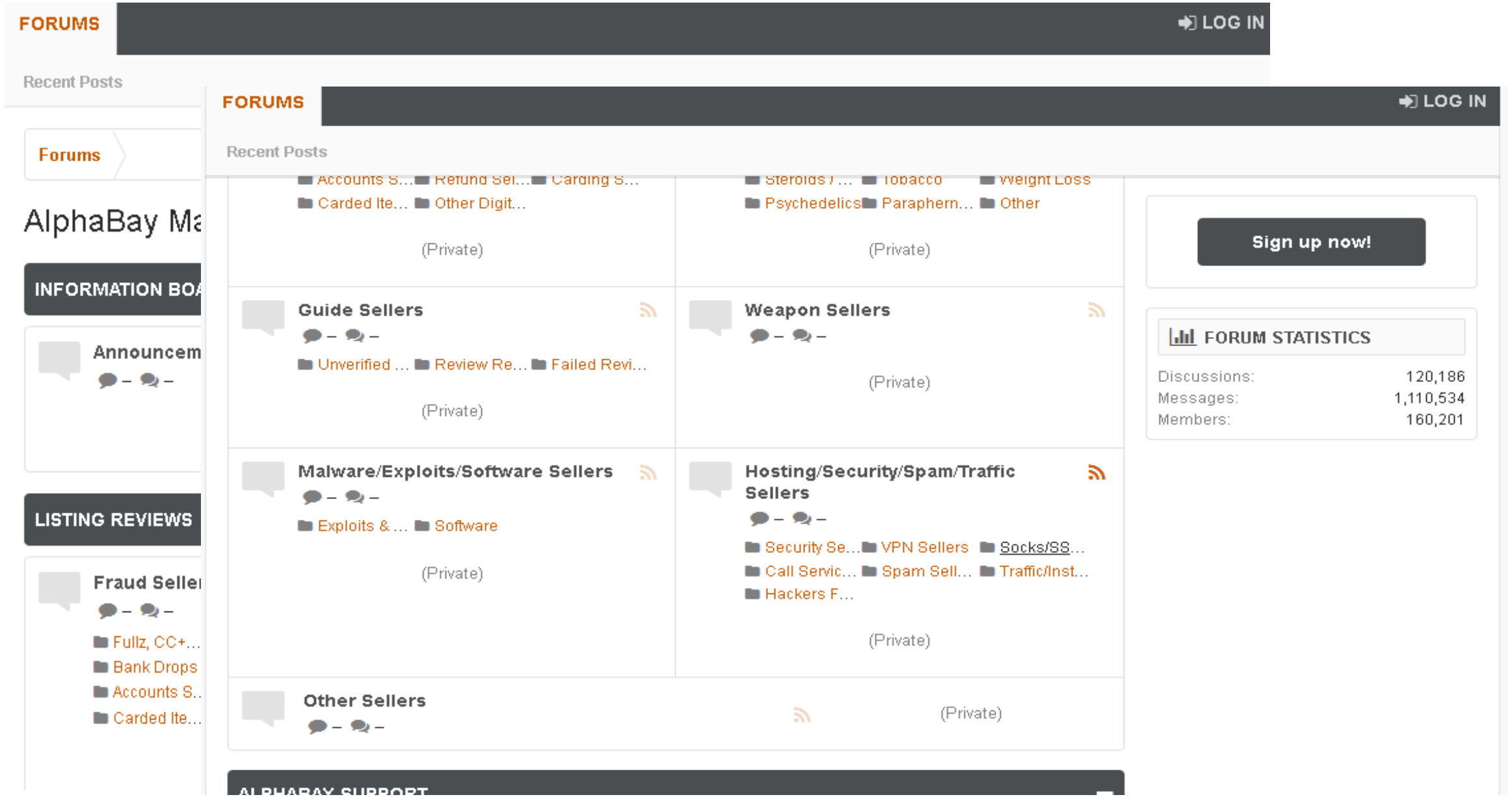




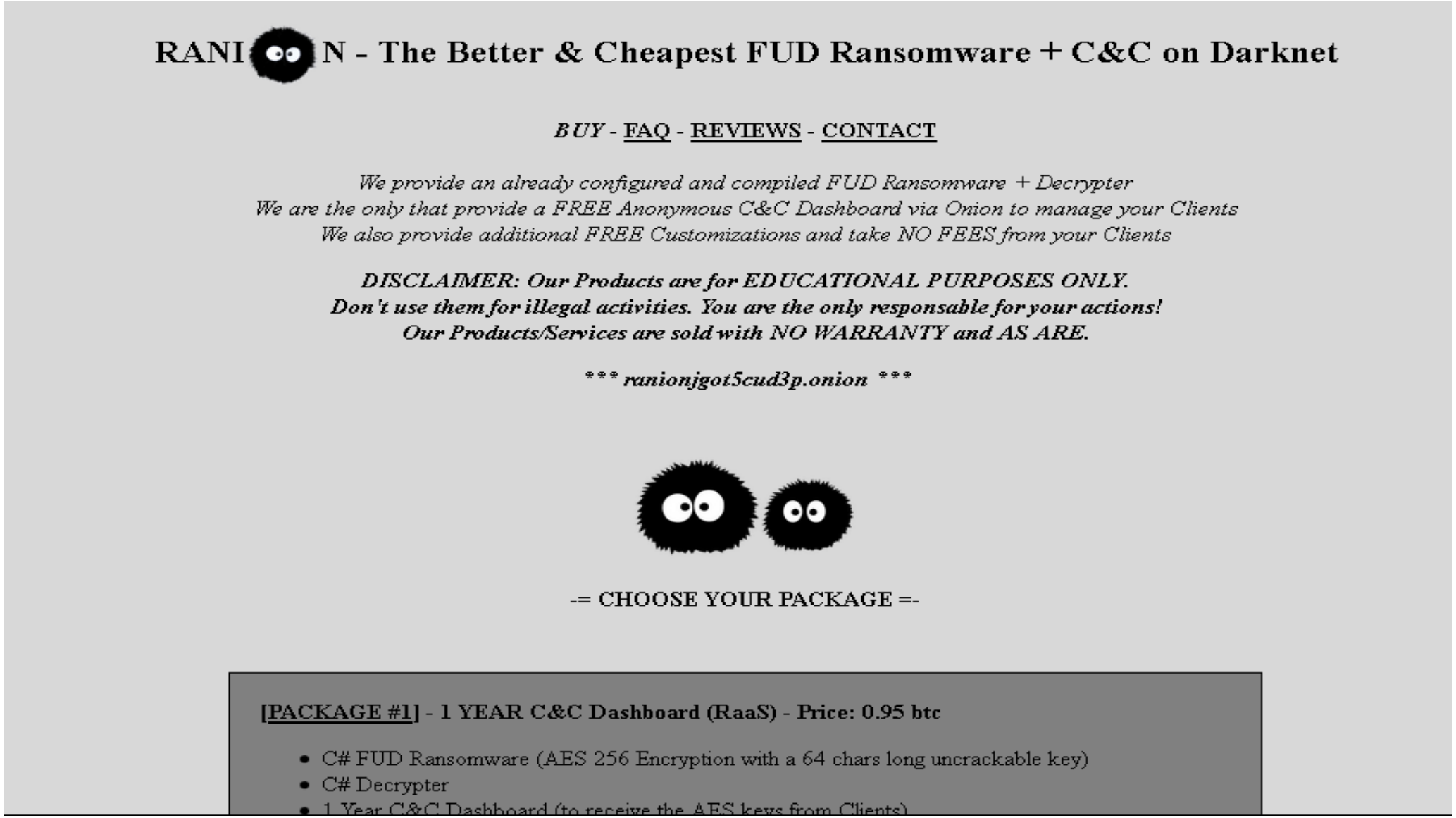
Silkroad /Darknet/ HiddenWeb



Für Bastler und Tüfftler



Try and Buy – von Massenware bis Konfektion



RANI N - The Better & Cheapest FUD Ransomware + C&C on Darknet

BUY - **FAQ** - **REVIEWS** - **CONTACT**

We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsable for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.

*** ranionjgot5cud3p.onion ***

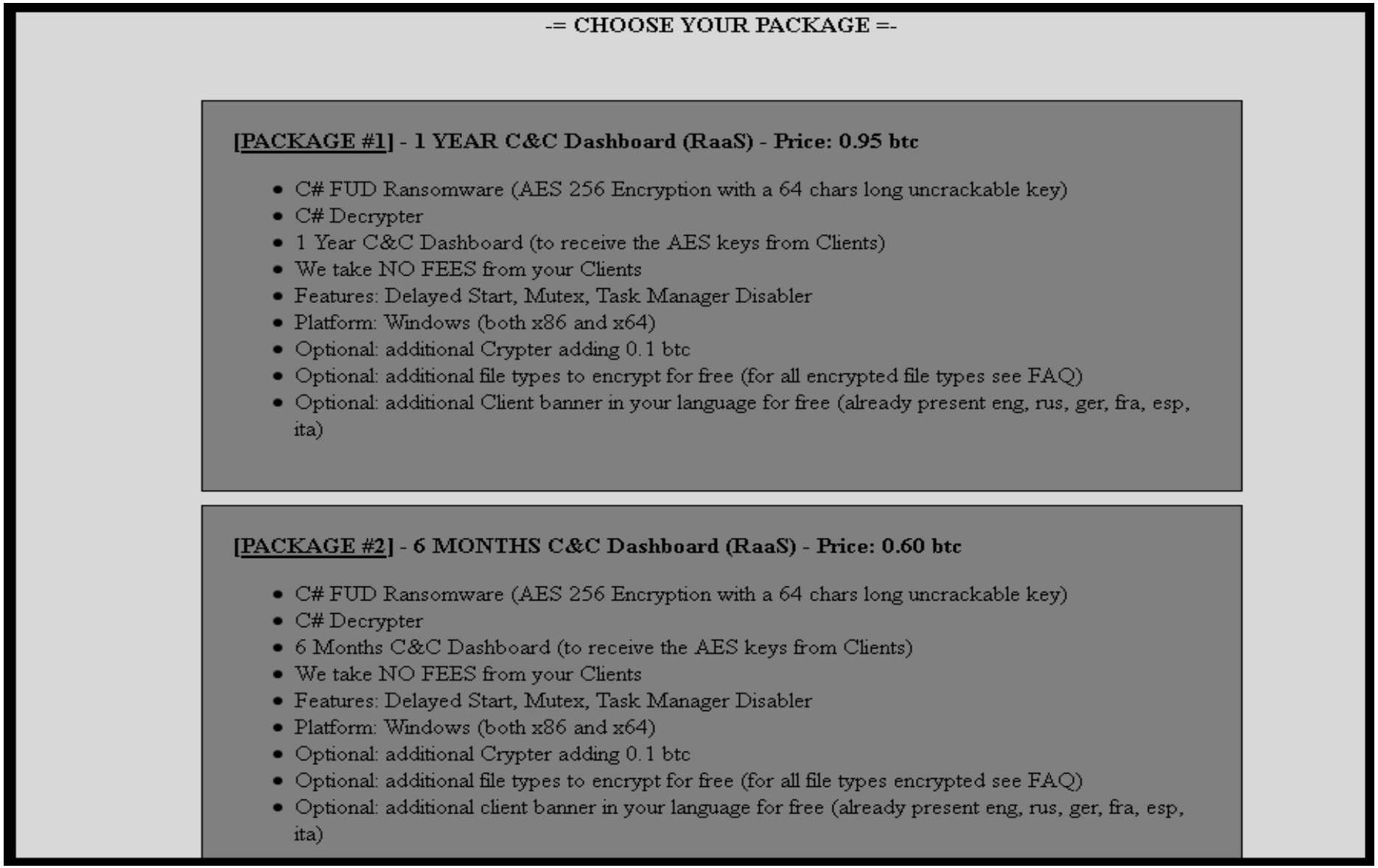
-= CHOOSE YOUR PACKAGE =-

[PACKAGE #1] - 1 YEAR C&C Dashboard (RaaS) - Price: 0.95 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- 1 Year C&C Dashboard (to receive the AES keys from Clients)

FUD=Fear Uncertainty Doubt / Furcht, Ungewissheit, Zweifel

Ransomware as a Service - Raas



-= CHOOSE YOUR PACKAGE =-

[PACKAGE #1] - 1 YEAR C&C Dashboard (RaaS) - Price: 0.95 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- 1 Year C&C Dashboard (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler
- Platform: Windows (both x86 and x64)
- Optional: additional Crypter adding 0.1 btc
- Optional: additional file types to encrypt for free (for all encrypted file types see FAQ)
- Optional: additional Client banner in your language for free (already present eng, rus, ger, fra, esp, ita)

[PACKAGE #2] - 6 MONTHS C&C Dashboard (RaaS) - Price: 0.60 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- 6 Months C&C Dashboard (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler
- Platform: Windows (both x86 and x64)
- Optional: additional Crypter adding 0.1 btc
- Optional: additional file types to encrypt for free (for all file types encrypted see FAQ)
- Optional: additional client banner in your language for free (already present eng, rus, ger, fra, esp, ita)

Wer taugt als Opfer für Ransomware?

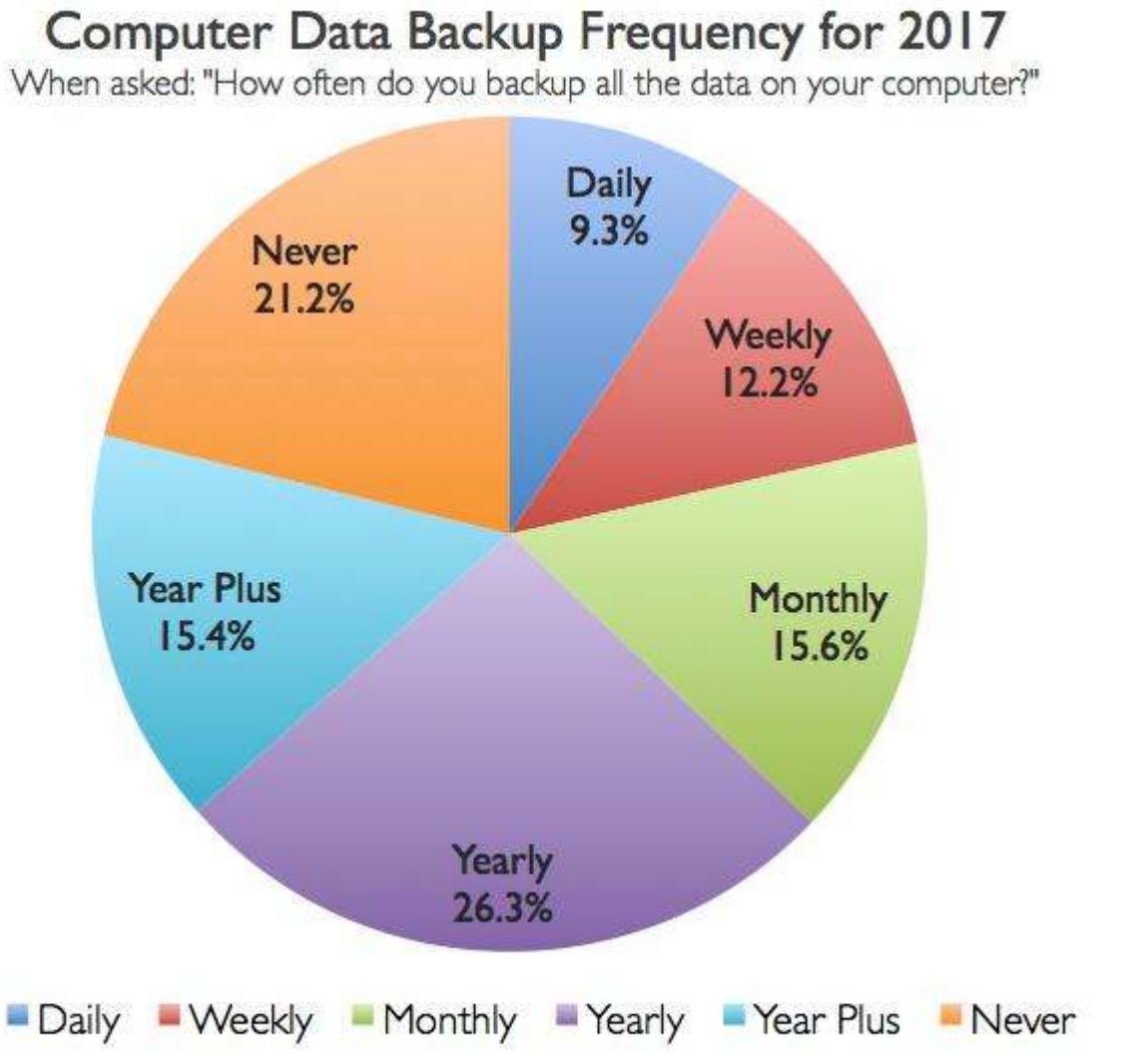
Generell:

Jeder der Geld hat und bereit ist, aus welchem Grund auch immer, Lösegeld zu zahlen!

Neu:

„Soft Targets“ wie Krankenhäuser, Webhoster, …

Einzig sichere Schutz...??



/www.backblaze.com/blog/backup-awareness-survey/

Lets get it Started

Ransomware – die Arten

Gibt es in zwei Ausprägungen:

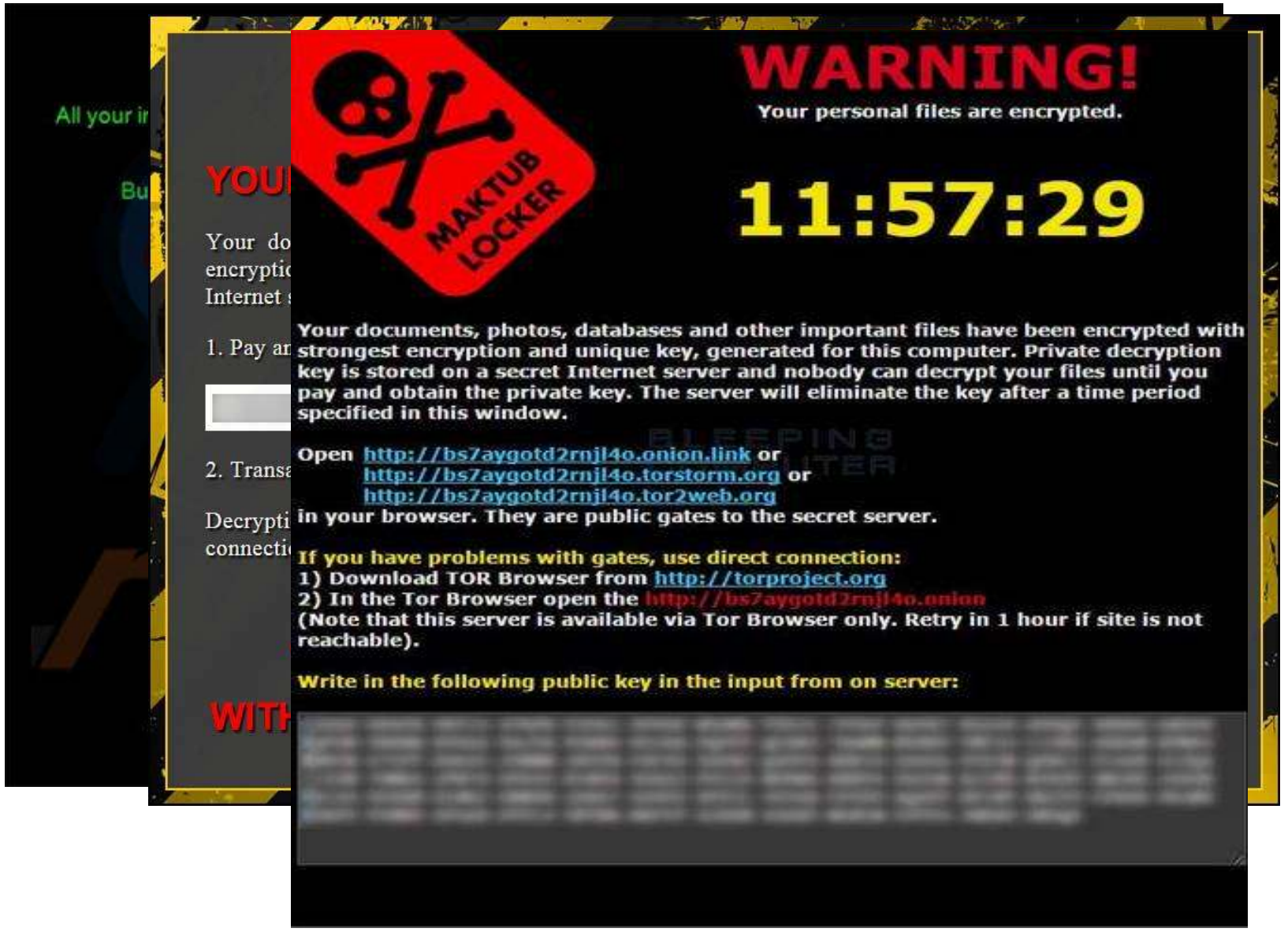
- Lockerware (37%)
  - sperrt den Zugriff
- Cryptoware (63%)
  - verschlüsselt die Dateien


BUNDESKRIMINALAMT
ABTEILUNG FÜR
COMPUTERKRIMINALITÄT
ACHTUNG !
IHR COMPUTER IST AUS EINEM ODER MEHREREN DER UNTEN AUFGEFÜHRTEN GRÜNDE GESPERRT
VIDEO REC: ON
JAHR
TAG
MONAT
BEI
OFFENSE / KRIMINALITÄT
2012
21
06
CYBERCRIME
Die Seriennummer Ihrer Verletzung
ITC-BZXCCDD/FF
IP-ADRESSE
ISP
LAGE
Austria
Sie haben gegen das Gesetz über «Urheberrecht und verwandte Schutzrechte» (Video, Musik, Software) verstoßen und unrechtmäßig urheberrechtliche Inhalte genutzt, bzw. verbreitet und somit gegen Art. 128 des Strafgesetzbuches der Bundesrepublik Deutschland verstoßen.
Art. 128 des Strafgesetzbuches zieht eine Strafe in Höhe von 2 bis 500 Mindestlöhnen oder eine Freiheitsstrafe von 2 bis 8 Jahren in Betracht.
Sie haben verbotene pornografische Inhalte eingesehen oder verbreitet (Child Porno/Zoofilia etc.) und damit gegen Art. 202 des Strafgesetzbuches der Bundesrepublik Deutschland verstoßen. Art. 202 des Strafgesetzbuches zieht eine Freiheitsstrafe von 4 bis 12 Jahren in Betracht.
Von ihrem Computer aus wurde ein rechtwidriger Zugang zu Computerdaten durchgeführt oder Sie.... Art. 208 des Strafgesetzbuches zieht eine Strafe in Höhe von 100.000€ und/oder Freiheitsstrafe von 4 bis 9 Jahren in Betracht.
Von ihrem Computer aus wurde ein rechtswidriger Zugang ohne ihre Kenntnis durchgeführt. Womöglich ist ihr Computer von schädlichen Programmen befallen, diesbezüglich verstoßen sie das Getz über die "Fahrlässige
PayPal
Geben Sie Ihre Kartennummer *
example: 4444 4444 4444 4444
Ukash
Geben Sie Ihre Kartennummer *
example: 6334444444444444
paysafecard
Geben Sie Ihre Kartennummer *
example: 0004444444444444
Strafe zahlen
* Wählen Sie eine der Arten der Bezahlung
Norton by Symantec
VeriSign Secured
AVIA
Agip
Esso
OMV
Q1
Westfalen
epay
Der Polizeipräsidentin Vienna Platz der Luftbrücke 6D-12101 Vienna

Cryptoware

- Verschlüsselt Daten auf PCs, Servern, in Netzlaufwerken und Mobilen Devices
- Verbreitung meistens über Spams als Links(www.badurl.xxx – drive by Infektionen) oder Anhänge (rechnung.doc.zip), seit neuestem auch über Exploits ohne User-Interaktion (WannaCry)
- Geräte nach Infektion beschränkt nutzbar
- Preis 300 – 8000 €, je nach „Projekt“ und Zielgruppe
- Zahlung: Bitcoins
- Entschlüsselung aufgrund der symmetrischen und asymmetrischen Schlüssel nur unter extremem Aufwand oder gar nicht möglich (2048 Bit Schlüssel)

Aggressives Geschäftsmodel

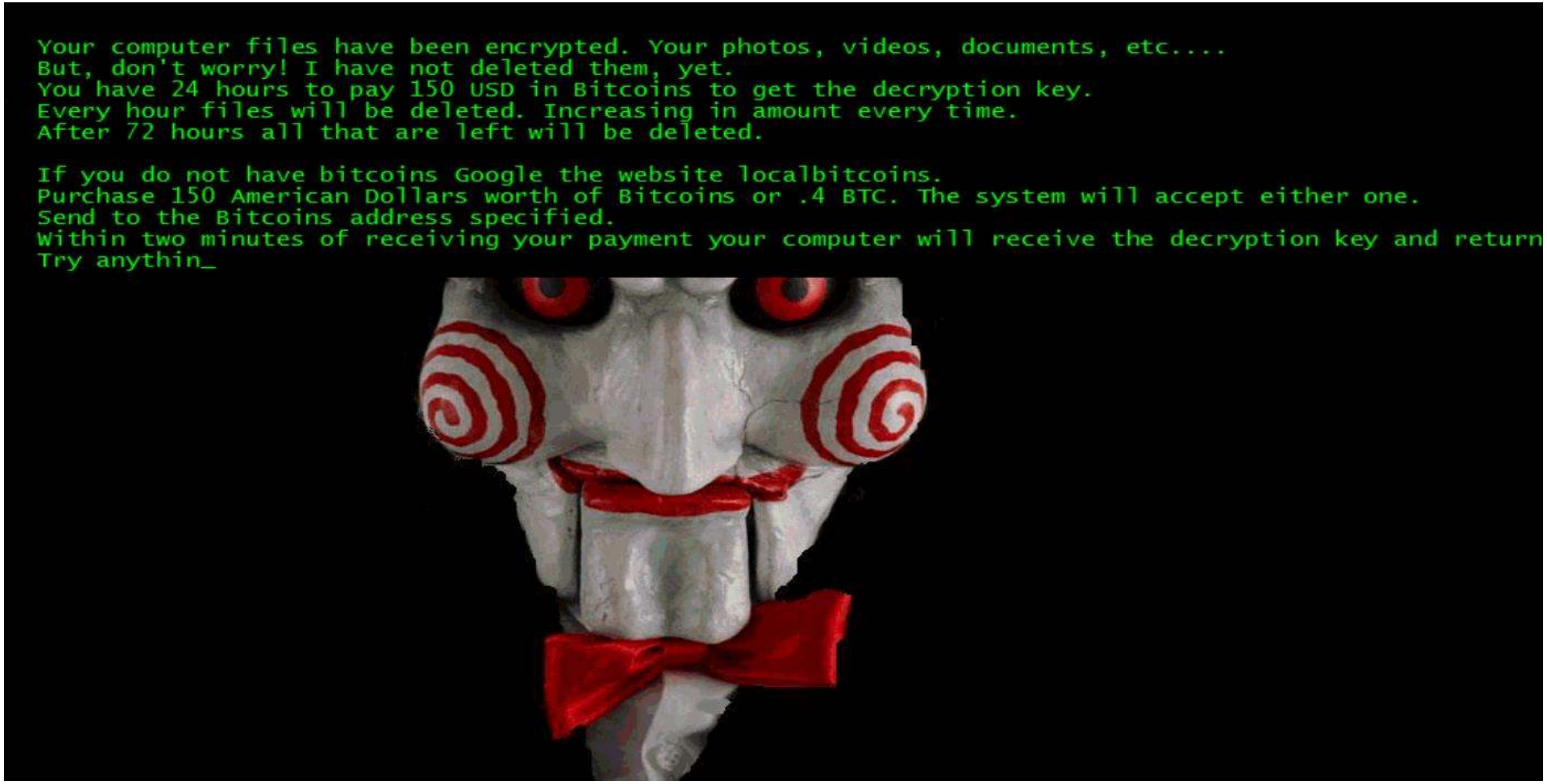


Keine Zeitliche Limitierung

4 Tage

12 Stunden

Ransom Trojan Jigsaw



Wenn 72 Stunden nach der Infektion noch kein Lösegeld bezahlt wurde, werden ALLE Dateien gelöscht

Zahlungsanreiz: Jede Stunde wird eine Datei gelöscht - bei einem Neustart 1.000.

Ransomware Chimera – richtig teuer

Ihrem Namen im Internet veröffentlichen.

Angriffsvektor - eMail

- SPAM-E-Mail mit www.badurl.xx
- User Interaktion (Layer 8 Epic!)
- Anruf beim IT-Helpdesk - Check des PCs
- Ernüchterung

„Zustellung“ CrytoWall 4.0

hits: 472
ip's: 11
first seen: 11.12.2015 13:15:05
filename: Quittung.N2331X347.zip:Quittung.N2331X347.exe
scancenter: TA-Prof
filesize: 258548
last alert: 11.12.2015 15:11:41 hits = 133
md5: c2b18f218569f09e8be75d4594de364d
sample: http://mmwstat.isc.local/cgi-bin/genstatistic.pl?md5=c2b18f218569f09e8be75d4594de364d&module=download

Verschickt jeweils viele E-Mails pro Bot – verhältnismäßig geringe Menge an Bots involviert (meist weniger als 250 pro Welle – dafür bis zu 500 Mails pro Bot)

Subject (count, subject)
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015

Filename (count, filename)
464 Quittung.N2331X347.zip:Quittung.N2331X347.exe
5 rfc822-message:Quittung.N2331X347.zip:Quittung.N2331X347.exe
2 Quittung.N2331X347.exe
1 Ihre A1 Bestellung N3818257-6 vom 12.12.2015:Quittung.N2331X347.zip:Quittung.N2331X347.exe

Fromaddress (count, from)
152 admin <robot@a1.net>
11 admin <admin@a1.net>
7 robot <Admin@a1.net>
6 Admin <email@a1.net>
6 Admin <Office@a1.net>
6 manager <Admin@a1.net>
5 Buro <info@a1.net>
5 contact <a1@a1.net>
5 Hilfe <Office@a1.net>
5 info <admin@a1.net>

Sender (count, fqdn(ip))
306 194-17-250-10.customer.telia.com(194.17.250.10)
152 bsmtp8.bon.at(213.33.87.20)

„Zustellung“ TESLACrypt

Verschickt jeweils nur 1 E-Mail pro Bot – verhältnismäßig geringe Versandmenge (meist zwischen 100-500 E-Mails pro Welle – dafür bis zu 50 Wellen pro Stunde!!)

hits: 123
ip's: 123
first seen: 14.12.2015 17:35:12
filename: invoice_90002995_scan.zip:invoice_copy_lIdT8p.js
scancenter: scancenter-ikarus
filesize: 49390
md5: 594a6d5ecbf499573e16766179ce68cd
sample: http://mmwstat.isc.local/cgi-bin/genstatistic.pl?md5=594a6d5ecbf499573e16766179ce68cd&module=download

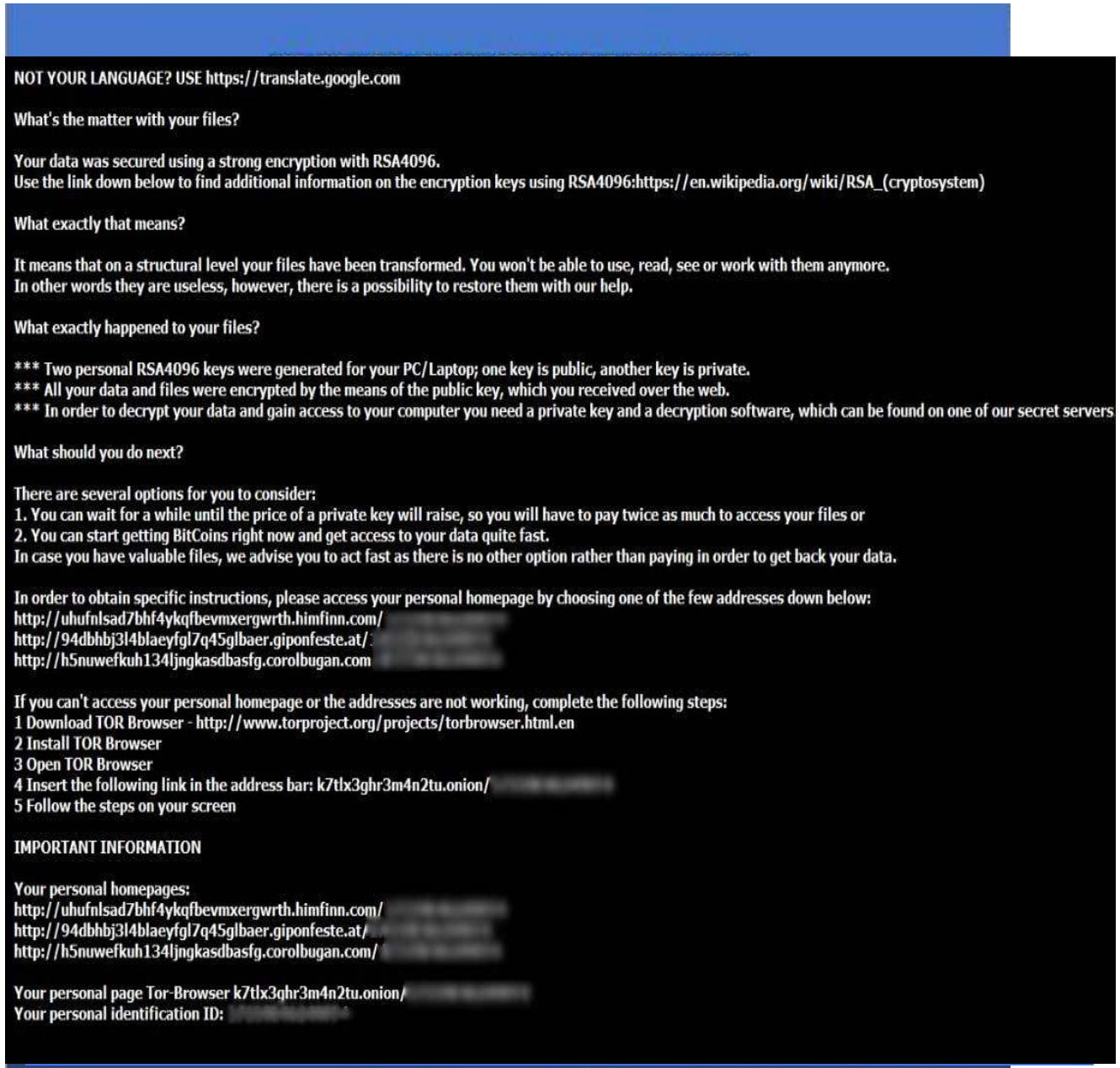
Subject (count, subject)
1 Your order #08626994
1 Your order #07043532
1 Your order #06666111
1 Your order #04603860
1 Your order #04217521
1 Your order #03481485
1 Your order #02651130
1 Your order #02346385
1 Your order #02174802
1 Your order #00788256

Filename (count, filename)
1 invoice_08626994_scan.zip:invoice_copy_lIdT8p.js
1 invoice_07043532_scan.zip:invoice_copy_lIdT8p.js
1 invoice_06666111_scan.zip:invoice_copy_lIdT8p.js
1 invoice_04603860_scan.zip:invoice_copy_lIdT8p.js
1 invoice_04217521_scan.zip:invoice_copy_lIdT8p.js
1 invoice_03481485_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02651130_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02346385_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02174802_scan.zip:invoice_copy_lIdT8p.js
1 invoice_00788256_scan.zip:invoice_copy_lIdT8p.js

Keine EXE/ZIP-Files, sondern ein hoch – obfuscatetes JavaScript – als Erstinfektor – der die eigentliche Malware erst nachlädt

Fromaddress (count, from)
1 Angelita Kent <KentAngelita93109@gourmetfoodmixes.net>
1 Angelica Michael <MichaelAngelica6291@aumeilleurdelafrance.com>
1 Anastasia Osborne <OsborneAnastasia69@petitegrace.com.br>
1 Amanda Manning <ManningAmanda8531@hts.net.id>
1 Alta Ruiz <RuizAlta449@bestel.com.mx>
1 Alma Kramer <KramerAlma363@thepartnersource.com>
1 Alison Long <LongAlison2256@adpi-me.com>
1 Alfredo Rush <RushAlfredo90916@evnetics.com>
1 Alfreda Bush <BushAlfreda194@business.telecomitalia.it>

Ransom Trojan TESLA Crypt



NOT YOUR LANGUAGE? USE https://translate.google.com

What's the matter with your files?

Your data was secured using a strong encryption with RSA4096.
Use the link down below to find additional information on the encryption keys using RSA4096:https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What exactly that means?

It means that on a structural level your files have been transformed. You won't be able to use, read, see or work with them anymore.
In other words they are useless, however, there is a possibility to restore them with our help.

What exactly happened to your files?

*** Two personal RSA4096 keys were generated for your PC/Laptop; one key is public, another key is private.
*** All your data and files were encrypted by the means of the public key, which you received over the web.
*** In order to decrypt your data and gain access to your computer you need a private key and a decryption software, which can be found on one of our secret servers

What should you do next?

There are several options for you to consider:
1. You can wait for a while until the price of a private key will raise, so you will have to pay twice as much to access your files or
2. You can start getting BitCoins right now and get access to your data quite fast.
In case you have valuable files, we advise you to act fast as there is no other option rather than paying in order to get back your data.

In order to obtain specific instructions, please access your personal homepage by choosing one of the few addresses down below:
http://uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com/
http://94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at/
http://h5nuwefkuh134ljngkasdbasfg.corolbugan.com

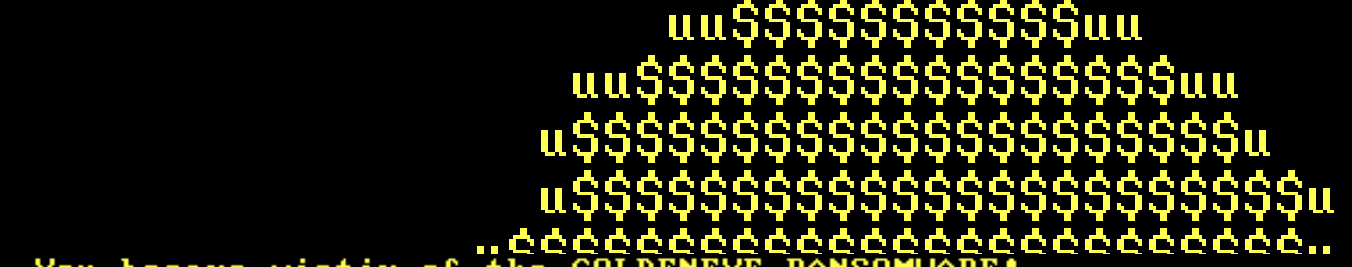
If you can't access your personal homepage or the addresses are not working, complete the following steps:
1 Download TOR Browser - http://www.torproject.org/projects/torbrowser.html.en
2 Install TOR Browser
3 Open TOR Browser
4 Insert the following link in the address bar: k7tlx3ghr3m4n2tu.onion/
5 Follow the steps on your screen

IMPORTANT INFORMATION

Your personal homepages:
http://uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com/
http://94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at/
http://h5nuwefkuh134ljngkasdbasfg.corolbugan.com/

Your personal page Tor-Browser k7tlx3ghr3m4n2tu.onion/
Your personal identification ID:

- ✓ Stealth Mode
- ✓ Bleibt unter dem Radar bis zum nächsten Backup
- ✓ Verschlüsselt Backups
- ✓ Netzwerk infiltriert und Dateien verschlüsselt



You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

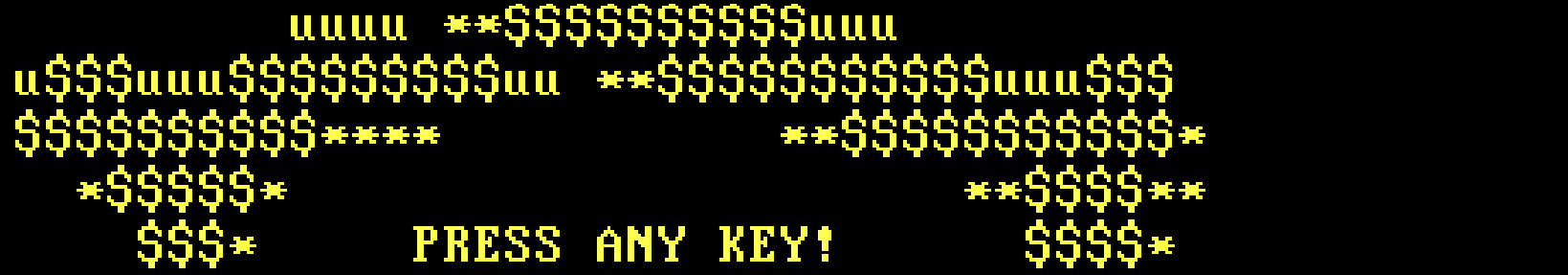
   http://goldenhjnqvc2lld.onion/[redacted]
   http://golden2uqpiqcs6j.onion/[redacted]

3. Enter your personal decryption code there:

[redacted]

If you already purchased your key, please enter it below.

Key: _

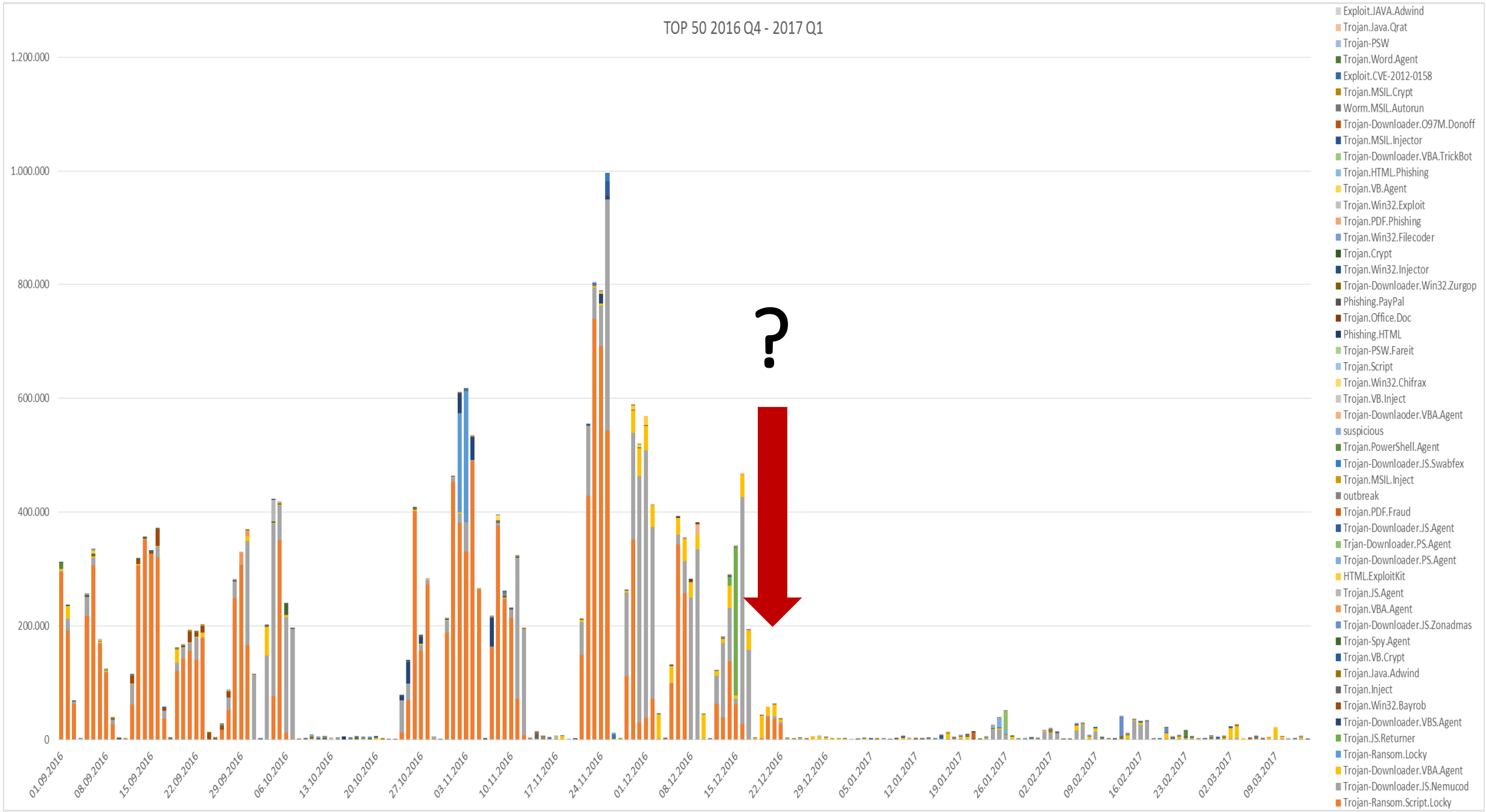


Zwischenbilanz

- Der AIDS Trojaner anno 1989 „kostete“ 189 USD. Überraschenderweise ist der Preis für Ransomware über die Jahre nicht dramatisch angestiegen.

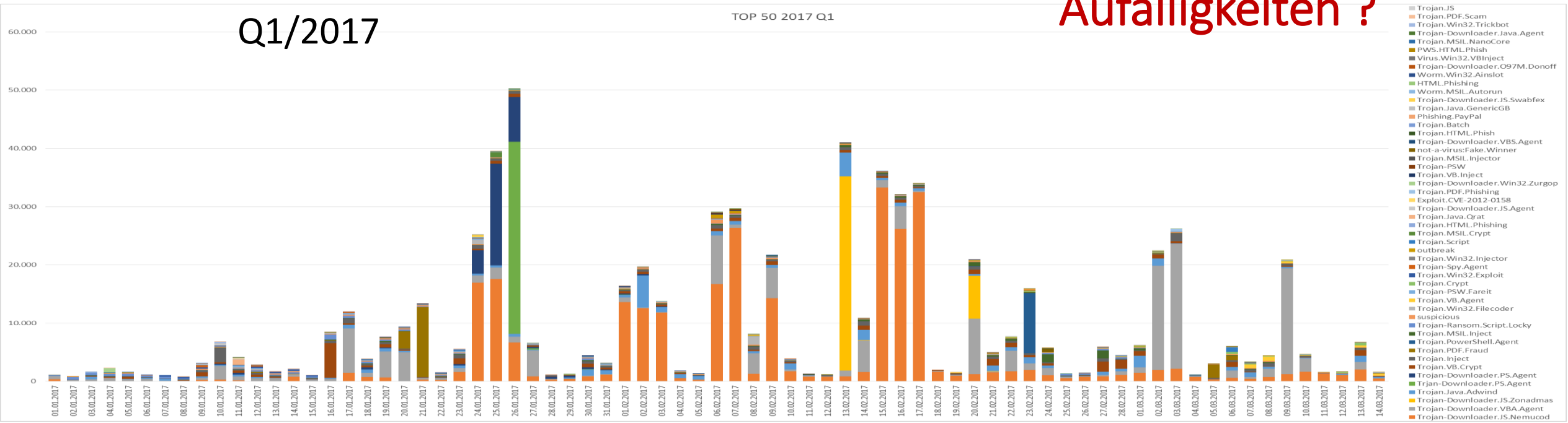
- Wenn man die Inflation zwischen 1989 und 2016 mit einbezieht entsprechen die 350 USD von heute den 189 USD von 1989!

- Conclusio: nicht alles wird teurer ;-)

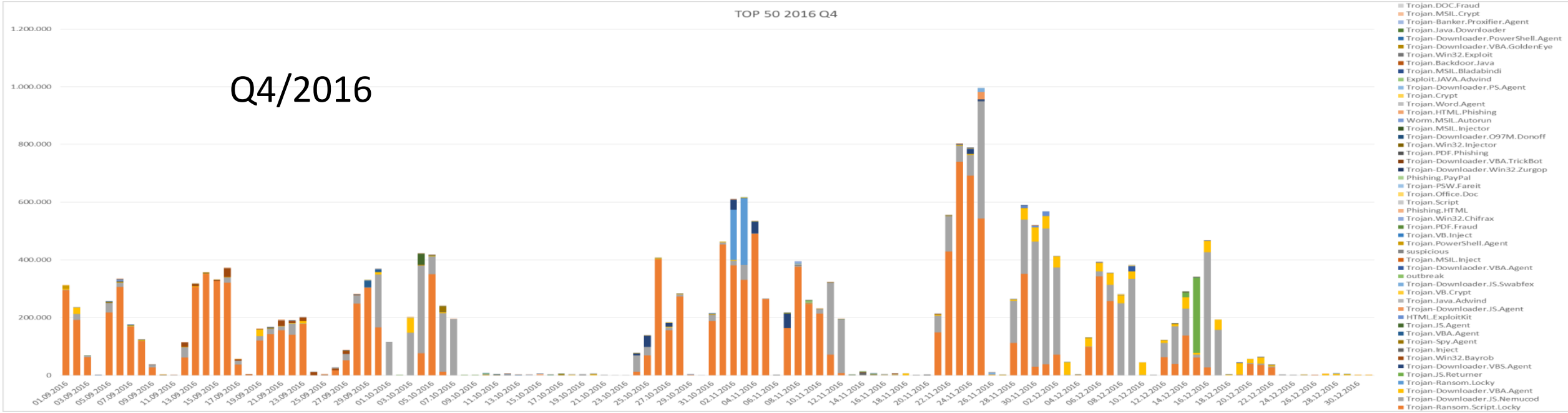

TOP 50 2016 Q4 - 2017 Q1
1.200.000
1.000.000
800.000
600.000
400.000
200.000
0
?
01.09.2016
08.09.2016
15.09.2016
22.09.2016
29.09.2016
06.10.2016
13.10.2016
20.10.2016
27.10.2016
03.11.2016
10.11.2016
17.11.2016
24.11.2016
01.12.2016
08.12.2016
15.12.2016
22.12.2016
29.12.2016
05.01.2017
12.01.2017
19.01.2017
26.01.2017
02.02.2017
09.02.2017
16.02.2017
23.02.2017
02.03.2017
09.03.2017
Exploit.JAVA.Adwind
Trojan.Java.Qrat
Trojan-PSW
Trojan.Word.Agent
Exploit.CVE-2012-0158
Trojan.MSIL.Crypt
Worm.MSIL.Autorun
Trojan-Downloader.O97M.Donoff
Trojan.MSIL.Injector
Trojan-Downloader.VBA.TrickBot
Trojan.HTML.Phishing
Trojan.VB.Agent
Trojan.Win32.Exploit
Trojan.PDF.Phishing
Trojan.Win32.Filecoder
Trojan.Crypt
Trojan.Win32.Injector
Trojan-Downloader.Win32.Zurgop
Phishing.PayPal
Trojan.Office.Doc
Phishing.HTML
Trojan-PSW.Fareit
Trojan.Script
Trojan.Win32.Chifrax
Trojan.VB.Inject
Trojan-Downlaoder.VBA.Agent
suspicious
Trojan.PowerShell.Agent
Trojan-Downloader.JS.Swabfex
Trojan.MSIL.Inject
outbreak
Trojan.PDF.Fraud
Trojan-Downloader.JS.Agent
Trjan-Downloader.PS.Agent
Trojan-Downloader.PS.Agent
HTML.ExploitKit
Trojan.JS.Agent
Trojan.VBA.Agent
Trojan-Downloader.JS.Zonadmas
Trojan-Spy.Agent
Trojan.VB.Crypt
Trojan.Java.Adwind
Trojan.Inject
Trojan.Win32.Bayrob
Trojan-Downloader.VBS.Agent
Trojan.JS.Returner
Trojan-Ransom.Locky
Trojan-Downloader.VBA.Agent
Trojan-Downloader.JS.Nemucod
Trojan-Ransom.Script.Locky

Aufälligkeiten ?

Q1/2017



Q4/2016

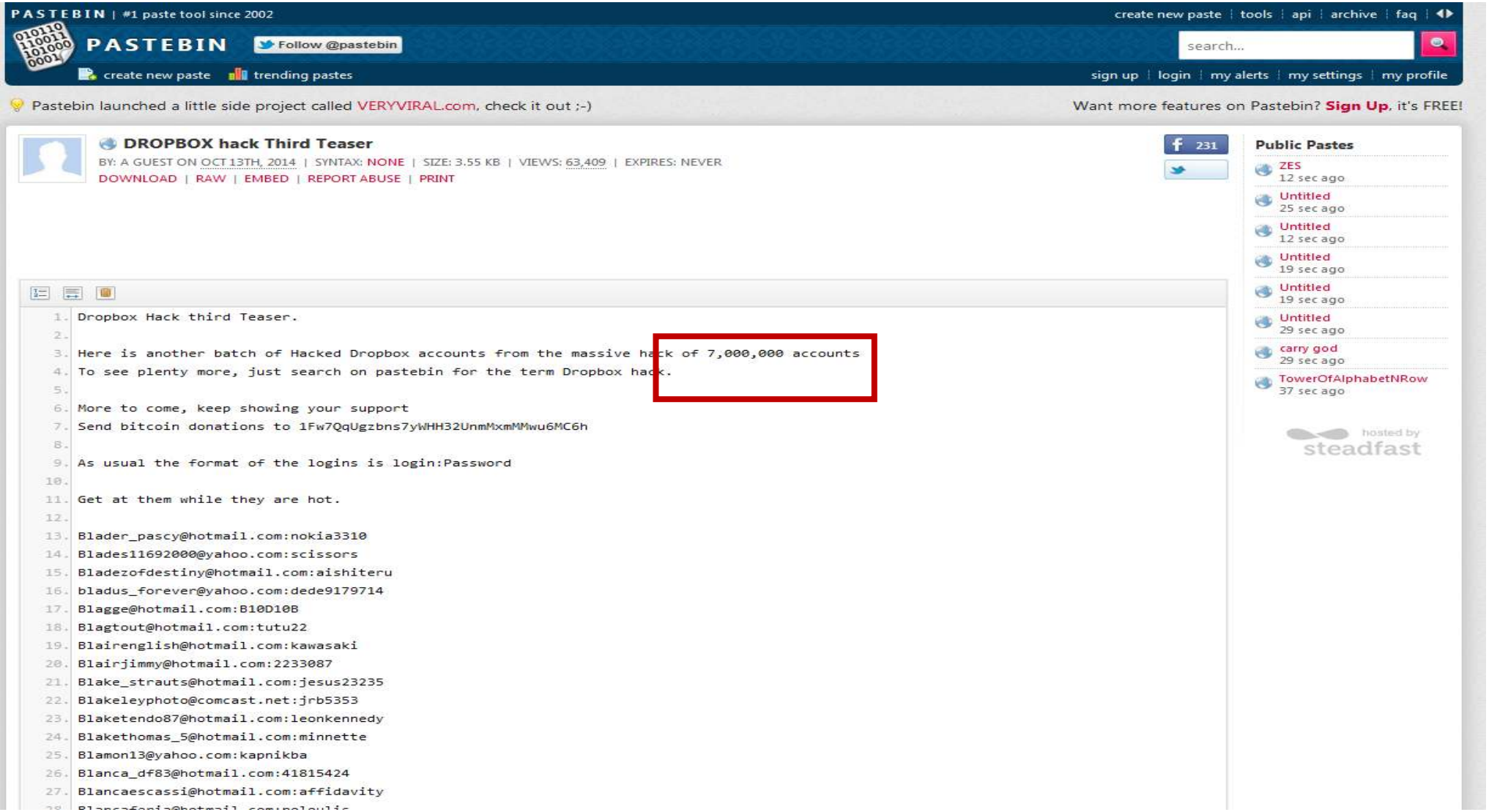


Alternierende Verbreitungswege

- Sozial Media (Dropbox, Facebook, Twitter, tumblr…)
- Malvertizing, Foren, CMS – drupal, joomla, wordpress
- Mobile Browser (auch Safari) und APK´s
- USB-Sticks
- Preinstalled (devices, firmware)
- Others…

Warum einen ?

Wenn man 7 Millionen haben kann ?



vulnerable Firmware

Mehr Gigabyte mehr Heiterkeit…

*** Product may vary based on local distribution.**

- Features Latest Intel® 6th generation Core Processors
- Ultra compact PC design at only 0.6L (46.8 x 112.6 x 119.4mm)
- Supports 2.5” HDD/SSD, 7.0/9.5 mm thick (1 x 6 Gbps SATA 3)
- 1 x M.2 SSD (2280) slot
- 2 x SO-DIMM DDR3L slot (1600MHz)
- Intel® IEEE 802.11 ac ,Dual Band Wi-Fi & Bluetooth 4.2 NGFF M.2 card
- HDMI plus Mini DisplayPort Outputs (Supports dual displays)
- Intel® HD Graphics 520
- 4 x USB 3.0
- Intel Gigabit lan
- Headset and Microphone jack
- VESA mounting Bracket (75 x 75mm + 100 x 100mm)
- **UEFI-Ransomware**

Jackpot – Angriff gegen Webhoster

ZDNet / Sicherheit / Cyberkriminalität

Ransomware: Webhoster zahlt 1 Million Dollar Lösegeld

Die Angreifer verschlüsselten die Daten auf 153 Servern und auch das Backup. Die zuvor auf Windows ausgerichtete Schadsoftware Erebus wurde für Angriffe auf Linux-Systeme modifiziert. Mit veralteter und angreifbarer Software machte es der südkoreanische Hoster den Erpressern leicht.

von Bernd Kling am 20. Juni 2017 , 18:47 Uhr

Der südkoreanische Webhoster Nayana ist Opfer einer Ransomware-Attacke geworden und hat sich mit über einer Million Dollar Lösegeld freigekauft. Das Unternehmen zahlte die Rekordsumme von 1,3 Milliarden Won (1,14 Millionen Dollar), um wieder an die verschlüsselten Daten zu kommen.

Nayana wurde am 10. Juni angegriffen und informierte daraufhin die Aufsichtsbehörde Korea Internet and Security Agency (KISA). Von der Verschlüsselung betroffen waren 153 von insgesamt 300 Servern, und damit wurden auch Tausende von Websites unerreichbar. Die Angreifer sperrten die ursprünglichen Daten und das Backup mit einem Passwort, sodass Nayana auch keine Wiederherstellung möglich wear.

http://www.zdnet.de/88301695/ransomware-webhoster-zahlt-1-million-dollar-loesegeld/?inf_by=594b78cd671db8db4c8b4585

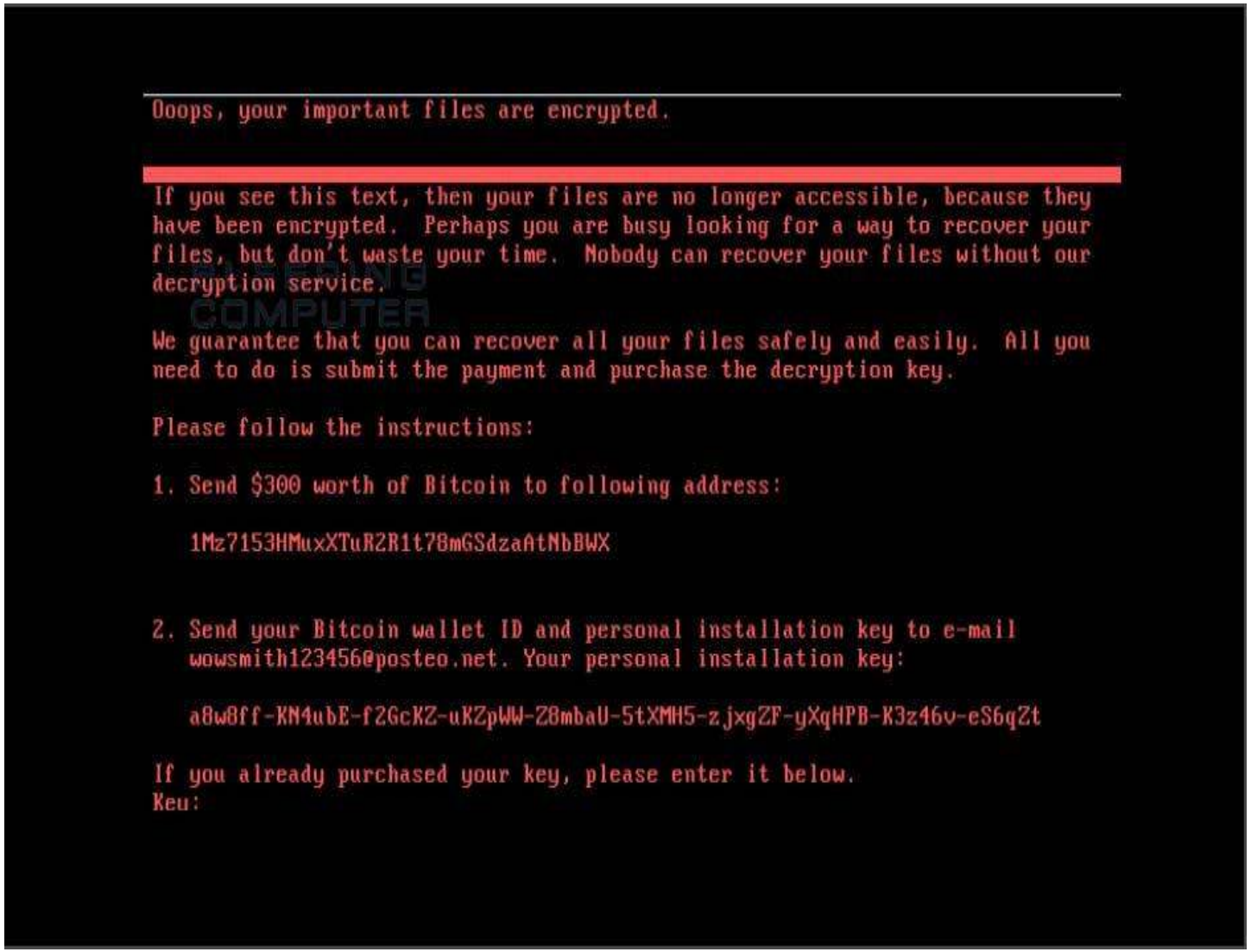
Wanna Cry: neuer Aufschrei

Erstmals Worm-Technologie mit Ransomware verknüpft. Die Attacke lässt sich in zwei Hauptbereiche unterteilen:

- den schon seit Anfang Februar bekannten Ransom-Trojan Teil, der für die Verschlüsselung der Systeme und die Abwicklung der Lösegeld-Forderung verantwortlich ist und
- den SMB-Wurm (eine modifizierte Variante des Eternalblue-Exploits), der für die rasante Verbreitung des Ransom-Trojan Codes im Netzwerk sorgt.

Der Angriff wurde von Europol hinsichtlich seines Ausmaßes als noch nie da gewesenes Ereignis beschrieben:
230.000 Computer in 150 Ländern

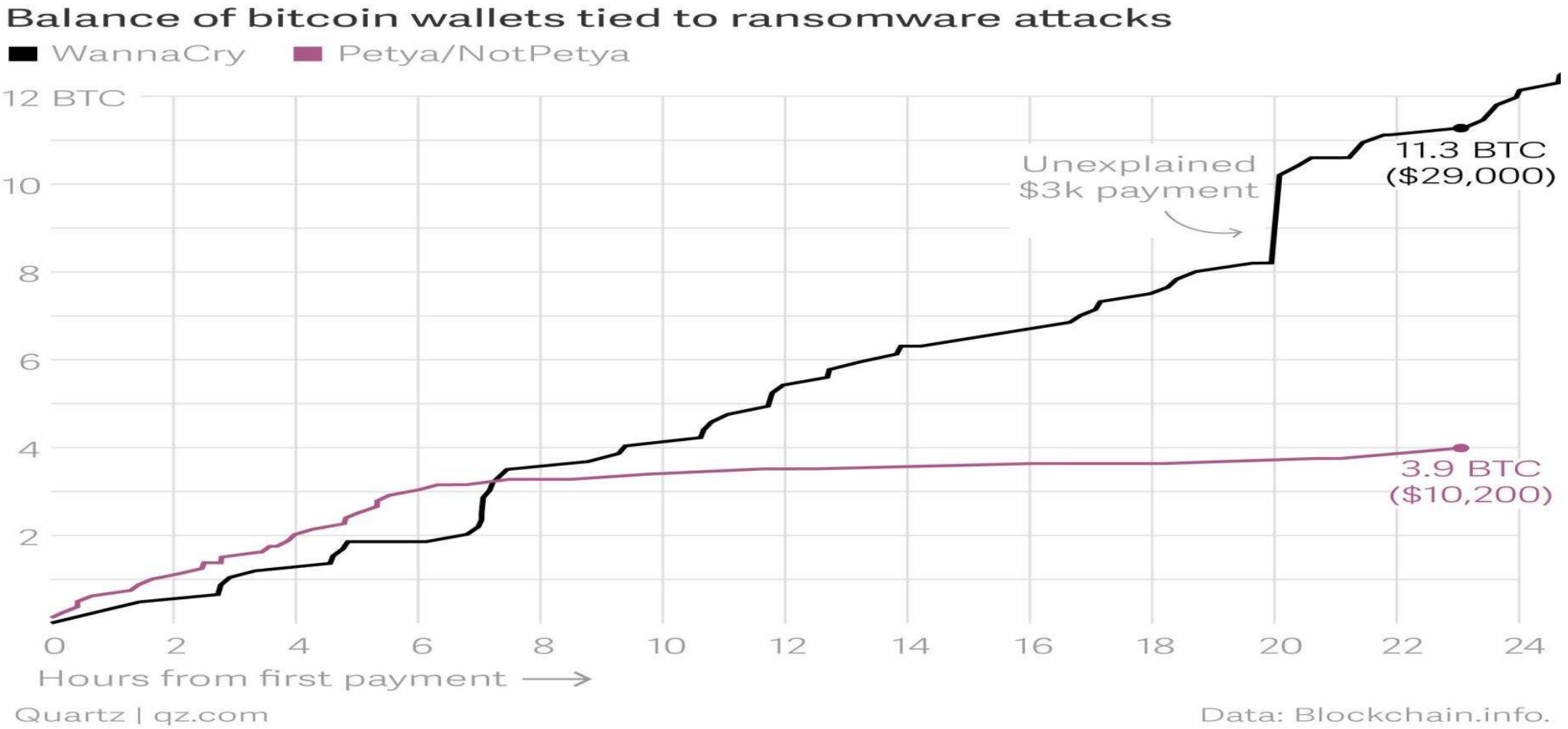
Petya / NoPetya



- Keine zwei Monate nach der aufsehenerregenden Attacke des Erpressungstrojaners WannaCry rollt eine zweite Ransomware-Welle um den halben Globus

Alles deutet auf eine politisch motivierte Cyberattacke hin.

Geschätzter Schaden 4 Mrd



https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses//

Zukunft

- IoT Vernetzung von TV, Kaffeemaschine, Kühlschrank
- NAS (Trojan.Synolocker für Synology)
- Linux basierende Systeme wie Raspberry Pi, Router, usw
- Gadgets (Smartwatch) durch infizierte APK-Installation am Smartphone automatischer Push auf die Uhr
- „smart“ Cars (diversester Hersteller)
- Es wird NICHT mehr nur um Geld gehen

Gegenmaßnahmen

- OS, Java und Browser immer am aktuellsten Stand halten (Patchen)
- Virenscanner
- SPAM-Filter
- Backups
- Network Protection, Firewall(s) & IPS
- %appdata% und %startup% via Grouppolicies am Ausführen von Executables hindern
- Makros Deaktivieren oder nur signierte Makros verwenden!
- **MERKE!** ERST die Malware entfernen und DANACH die Files entschlüsseln!!!

Klingt nicht optimal

Die Entwicklungen und Erkenntnisse der Bedrohungsbilder der letzten Jahre zeigen wie stark sich die Anforderungen an CyberSecurityStrategien ändern:

- Immer mehr “High-Level” Anlagen und Unternehmen mit sehr hohen Sicherheitsbedürfnissen werden erfolgreich gehackt/attackiert
- Existierende Sicherheitssysteme sind NICHT in der Lage Unternehmen ausreichend vor qualifizierten Attacken zu schützen (ATP-Problem)
- Professionalisierung der Angriffe führt zum Verlust von Petabytes an Informationen sowie zum Sprung über Systemgrenzen
- Die Mehrheit der angegriffenen Unternehmen/Organisationen bemerken nie oder (zu)spät dass sie überhaupt angegriffen wurden

Erste Conclusio

Wir wissen nun:

Malware-Zahlen immer noch enorm hoch

Die Zahl der damit durchgeführten Angriffe wächst proportional

Merke !

Auch die Komplexität der Angriffe steigt

proportional zu jedem abgewehrten Angriff

actio - reactio

Nation driven

#metoo

Cybercriminal

Hacktivist

Ego-Driven Attack

Angriffe gegen Sicherheitsindustrie

- **Kurzfassung:** Security-Unternehmen wurden von Unbekannten Angreifern infiltriert. Schlüsselunternehmen wie INTEL, Google, CISCO; RSA, KPN, Diginotar, TurkTrust; bit9 gehackt – Verschlüsselungsalgorithmen und Zertifikate gestohlen bzw fälschlich ausgestellt – Grundlage für weitere Angriffe
- **Profil:** Extrem komplexe Attacke um gezielt Zertifikate und Verschlüsselungssysteme unterlaufen zu können um Einbrüche in hochgesicherte Umgebungen zu ermöglichen(Lockheed Martin, Northrop Grumman..)
- **Methode: S**pearphishing via email von "Kollegen" mit einem Excel-Sheet. Escalation of privileges an den Sysadmin - "öffnet" Netzwerk für Angriffe von aussen
- **Auswirkung:** Hundertausend RSA Tokens zurück- sowie hundertausende Zertifikate wiederrufen - Zertifikaten die immerhin von Firmen wie Google, Microsoft, der CIA und vielen anderen verwendet wurden. Mit den gestohlenen /manipulierten Daten konnten andere Attacken erfolgreich abgeschlossen werden

Erosion of the Foundations of Security

« Vorige | Nächste »

Millionen Android-Smartphones mit Rootkit ab Werk

22.11.2016 07:41 Uhr – Ronald Eikenberg

vorlesen

(Bild: dpa, Britta Pedersen)

Ein Android-Updater der eher unbekannten Firma Ragentek ist nicht nur extrem unsicher, er verhält sich auch wie ein Rootkit. Das Programm steckt in etlichen Smartphone-Modellen chinesischer Hersteller, welche auch auf dem hiesigen Markt vertreten sind.

Massive Sicherheitslücken

In Millionenfach Verwendeten Systemen

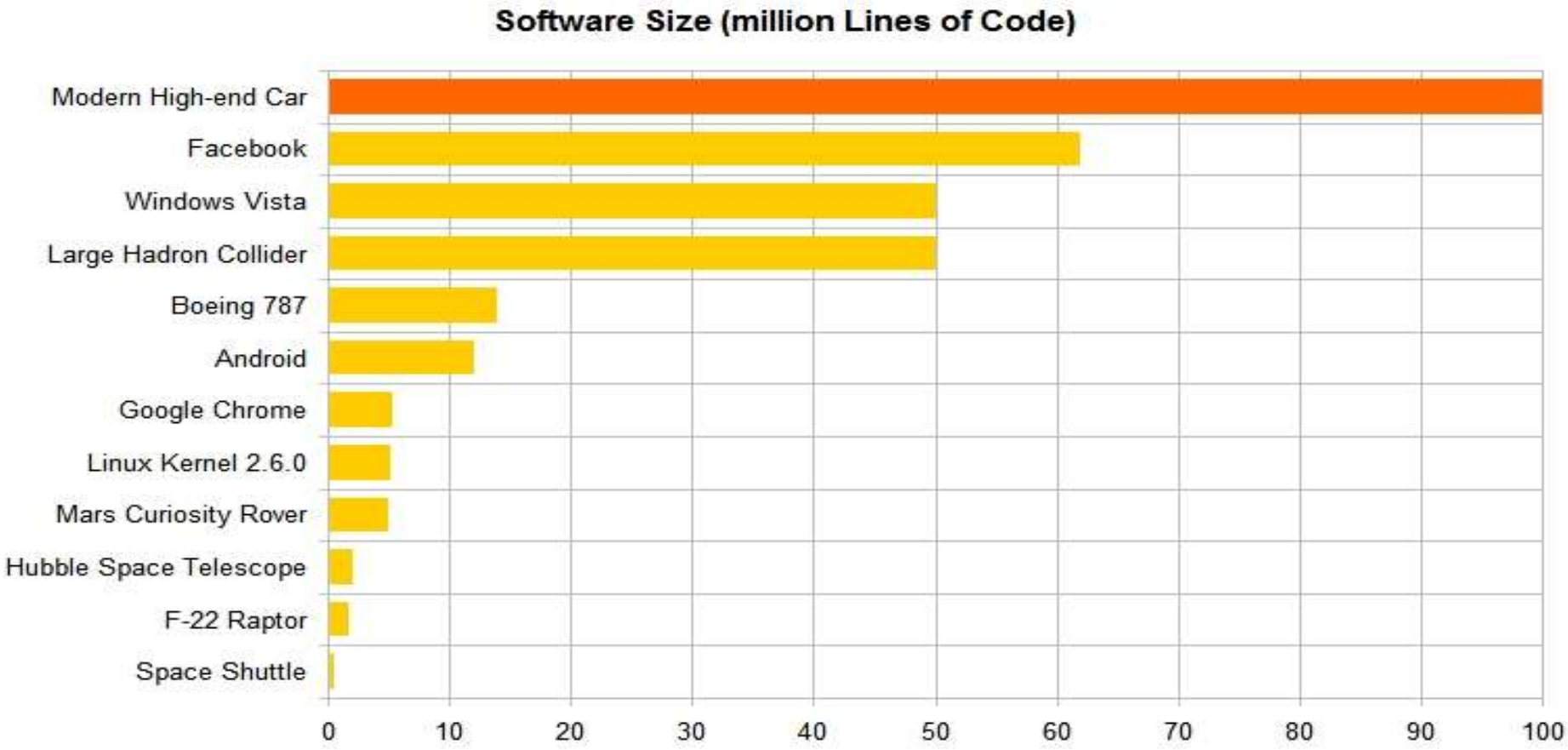
Heartbleed-bug

Sicherheitslücke Shellshock

Der **Heartbleed-Bug** ist ein schwerwiegender
der Open-Source-Bibliothek OpenSSL, durch
verschlüsselte TLS-Verbindungen private Dat
Servern ausgelesen werden
können.

m NIST verwendeten Bewertung des
otentials erhält Shellshock eine Bewertung von 10
dem Maximum!

Fehlerquelle: „weils einfach mehr wird“



"In der Forschung sind wir glücklich, wenn wir einige 10.000 Codezeilen nachweislich sicher machen können," sagt etwa Michael Waidner vom Fraunhofer-Institut für Sichere Informationstechnologie .

Massive Sicherheitslücken

In Millionenfach Verwendeten Prozessoren

Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are software patches against Meltdown.

Spectre

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre

Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. However, it is possible to prevent specific known exploits based on Spectre through software patches.

Firewall ?

TOP SECRET//COMINT//REL USA, FVEY

FEEDTROUGH

TOP SECRET//COMINT//REL TO USA, FVEY

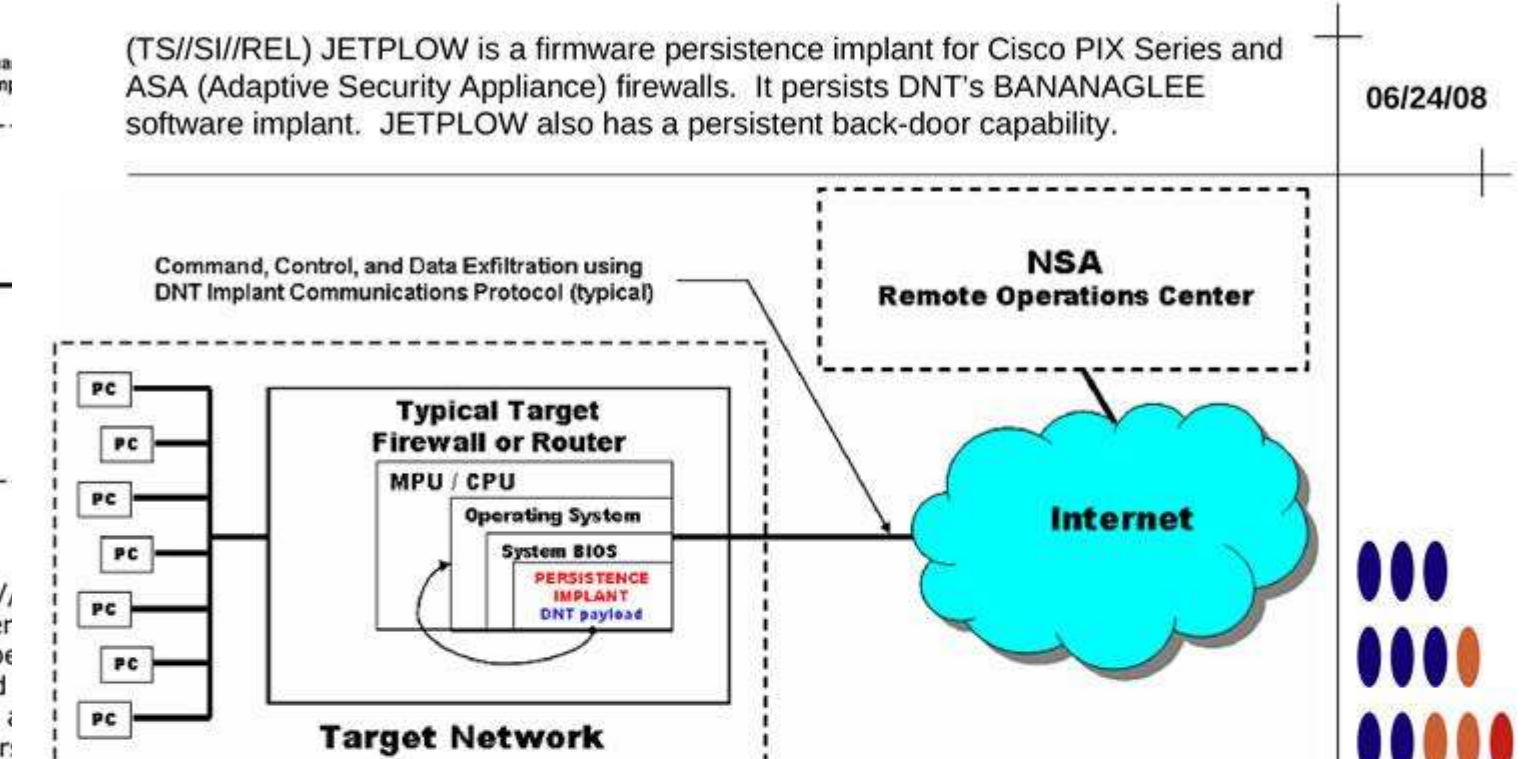
TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



Jeder – wirklich jeder – ist angreifbar

International Edition | London, United Kingdom 8° | Sign in | MyCNN

CNN | News | Regions | Video | TV | Features | Opinions | More... | Search CNN

Entire US political system 'under attack' by Russian hacking, experts warn

Meanwhile, some US commentators on cybersecurity issues have suggested that these attacks are not a surprise but appear to be a new spin on an old strategy

The hacks have created a dilemma for American voters. Photograph: Tek Image/Getty Images/Science Photo Library RF

… cyber attacks & industrial state of the art …

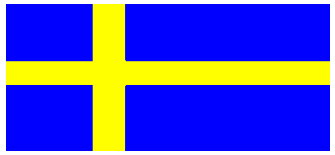
Deutsche Telekom

Ein "Amateur" konnte weite Teile des Telekom Netzes infiltrieren

Source: http://www.spiegel.de/netzwelt/web/deutsche-telekom-stoerung-war-misslungener-botnet-angriff-a-1123544.html

"Britain´s newest warship running Swiss Cheese OS (Windows XP)", **The Register, June 27th, 2017**

Source: https://www.theregister.co.uk/2017/06/27/hms_queen_elizabeth_running_windows_xp



Namen, Adressen,Photos von air force Piloten, SEAL teams, logistikl Kapazitäten , … , **Falkvinge, The Hacker News, July 24th, 2017**

Source: http://thehackernews.com/2017/07/sweden-data-breach.html

Exploit „EternalBlue" von den „Shadow Brokers" aus Archiven der NSA gestohlen

- ➔ ***WannaCry attack***
- ➔ *announcements for more exploits are made*

Source: https://www.cnet.com/au/news/Hackers-behind-stolen-nsa-tool-for-wannacry-more-leaks-coming

2017 Cyber Attacken im Finanzbereich

Deloitte.

US Börsenaufsicht SEC

4 Mrd USD Verlust CEO Rücktritt

EQUIFAX®

größtes US-Bonitätsauskunftsbüro

https://www.equifaxsecurity2017.com/

Source: https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html 23.03.2018

Cyber Bedrohung - Wirtschaftskriminalität

- **Kriminalität**
  - Diebstahl von Informationen (Online skimming)
  - Erpressung - Ransomeware; z.B. CryptoLocker, Locky, etc.
  - Finanztransaktionen, etc.

Ransomware

ATM, 2014

Quelle: instagram.com/kimkardashia

Promi Photos aus der iCloud 9.2014

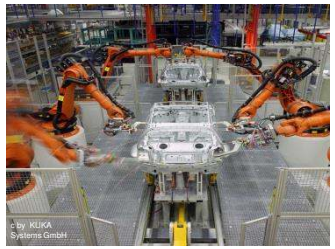
Online skimmig

2015, law firms were the seventh most frequent target

- **Sabotage**
  - Zerstörung oder Manipulation von IT- und Produktionssystemen
  - Kommunikationsstörung durch DDoS Attacken

YAHOO!

2013, 2016
alle Kunden

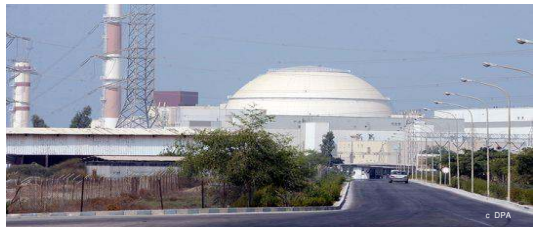


Stahlproduktion, Germany 12.2014
News in it governance,

TalkTalk
Brighter Phone & Broadband

***4 Mio customer data*, 2015, 2016**

- **Spionage**
  - Forschungsdaten, Produktionsprozess, Ausschreibungen, etc.
  - Steganographie



Atomic Power Plant Iran (Stuxnet), 6.2010

German Government
6.2015 ff bis 2018

RUAG
Aerospace Defence Technology

Sources: News in it governance, Standard, AIT Research

Cyber Bedrohung - Terror/Propaganda

- **Terror**

IDs thefts

"Malaysia arrests hacker for supplying U.S. targets to Islamic State", Reuters, 16.10.2015

Twitter Falschmeldung über das White House → Dow Jones Wertverlust an der Börse, April 2013

- **Propaganda**
  - Übernahme von Webseiten, Plazierung von Botschaften in Sozialen Medien, etc.
  - Erpressung

Source: Der Standard

Sony Pictures, 11.2014

TV5MONDE

9. April 2015

Cyber Bedrohung– Propaganda/Kriminalität

Fancybear

“Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team. We stand for fair play and clean sport”.

Source: https://fancybear.net/

“Russia Today', Moscow based Russia's biggest news channel website (RT.com) …. Hackers have replaced “Russia” or “Russians” with “Nazi” or “Nazis” word from the headlines….”

Source: https://www.grahamcluley.com/russia-today-website-defaced/

Google Translate machte aus „Russland“ „Mordor“

Source: http://www.spiegel.de/netzwelt/web/google-translate-macht-aus-russland-mordor-a-1070756.html

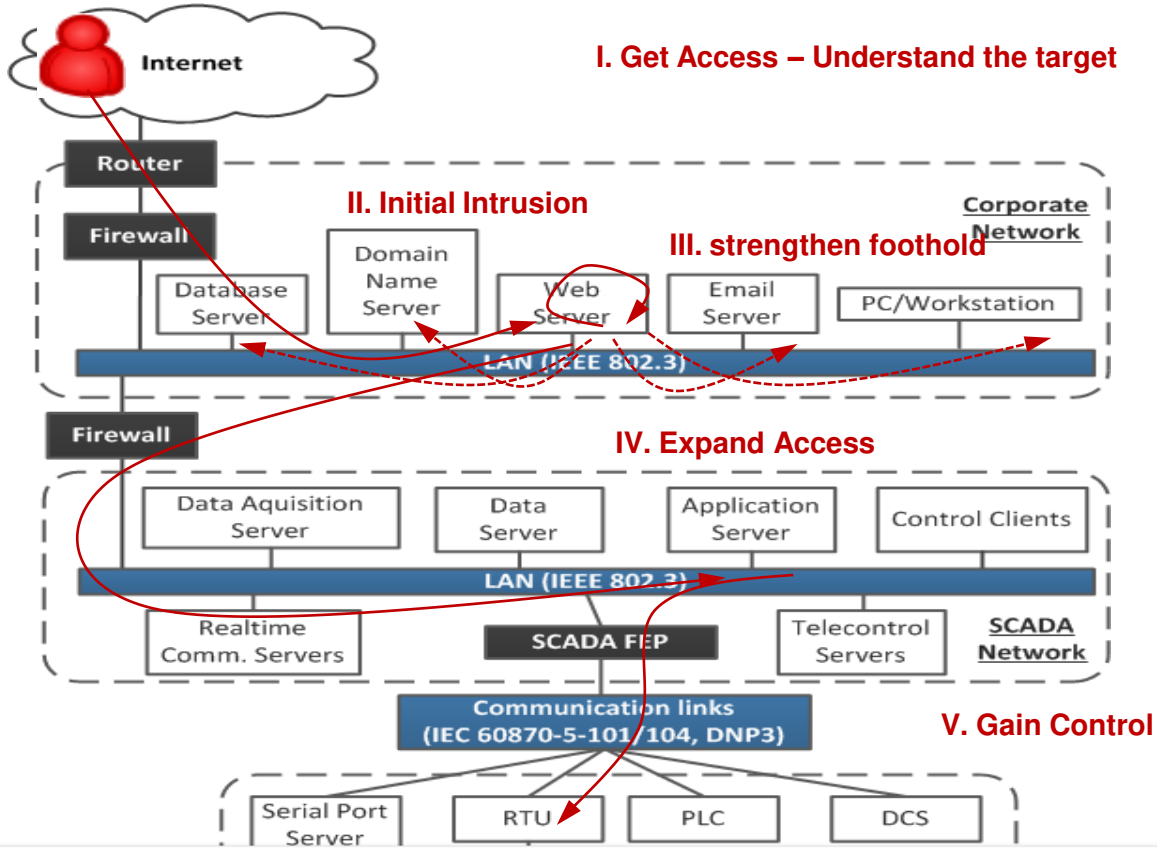
60.000 gemeldete Verfälschungen monatlich im DACH Raum

Quelle: nimbusec, zone-h.org

Advanced Persistent Threats (APT)

1. **Social engineering**
   - Zugriff verschaffen (public information, etc.)
2. **Initiale Intrusion - exploit weaknesses**
   - Phishing, SW vulnerabilities, configuration errors, stolen login information, weak passwords, etc.
3. **Position absichern– lateral mov.**
   - Stays invisible in the system, Command & Control Capabilities, be immune to security responses, access control from within the trusted environment
4. **Zugriffsmöglichkeiten erweitern**
   - Search directories, e-mail boxes, admin workspaces, etc.
   - Map the internal network structure and find login credentials for further services
5. **Kontrolle über Zielsystem**
   - Discover machines/devices which hold the most valuable information
   - send fabricated control messages

Attacks spans weeks or months and is developed for a dedicated purpose



25.3.2015: e-mail attack
23.12.2015: „shut down“

Analysis confirms coordinated hack attack caused Ukrainian power outage

BlackEnergy was key ingredient used to cause power outage to at least 80k customers.

am GMT

Share Tweet Email 33

last month's first known hacker-caused power outage used highly destructive malware to gain a foothold into multiple regional distribution power companies in Ukraine and delay restoration efforts once electricity had been shut off, a newly published analysis confirms.

The malware, known as BlackEnergy, allowed the attackers

FURTHER READING

2. Conclusio

Beachte!

Wir wissen/lernen nur von jenen Angriffe die erkannt und verifziert werden konnten !

Es gibt hinlänglich Beweise dafür, das unsere Sicherheitskonzepte und -Systeme uns nur bedingt schützen können

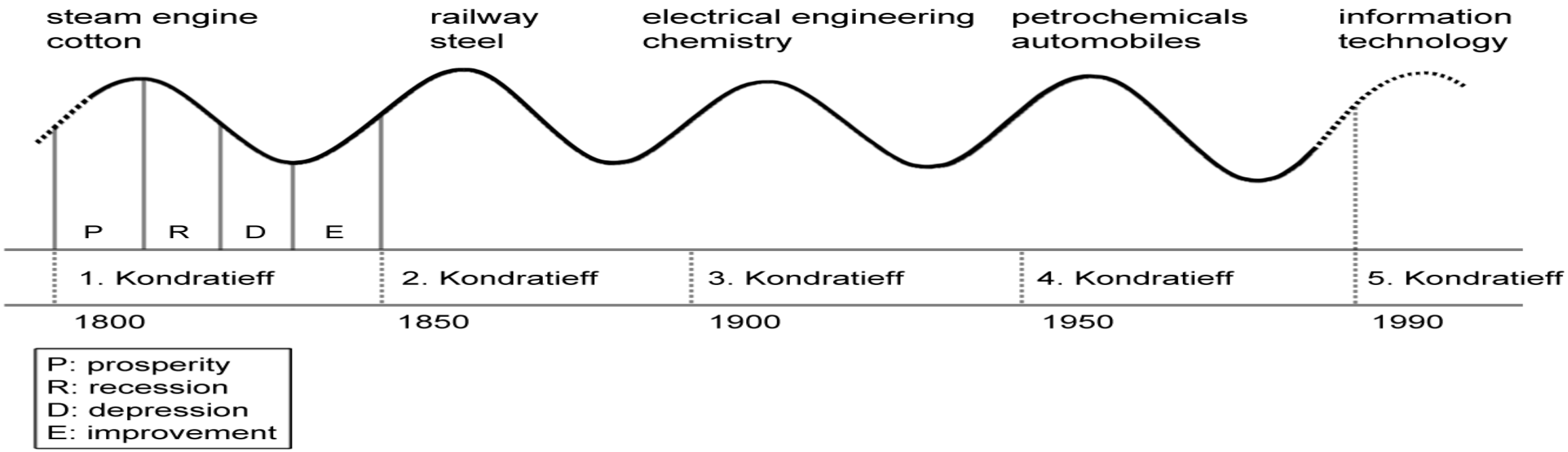
We always fight the last war !

Aufgemerkt!

Wir übertragen unsere – zweifelsfrei nur bedingt erfolgreichen Strategien – auf wirkliche kritische Umgebungen

Es wird es jetzt richtig spannend

Geschichtlich betrachtet beruhte die Expansion des Westens
bis in die 1970er Jahre auf der Fähigkeit, immer neue und immer größere Energiemengen erschließen und verwerten zu können.

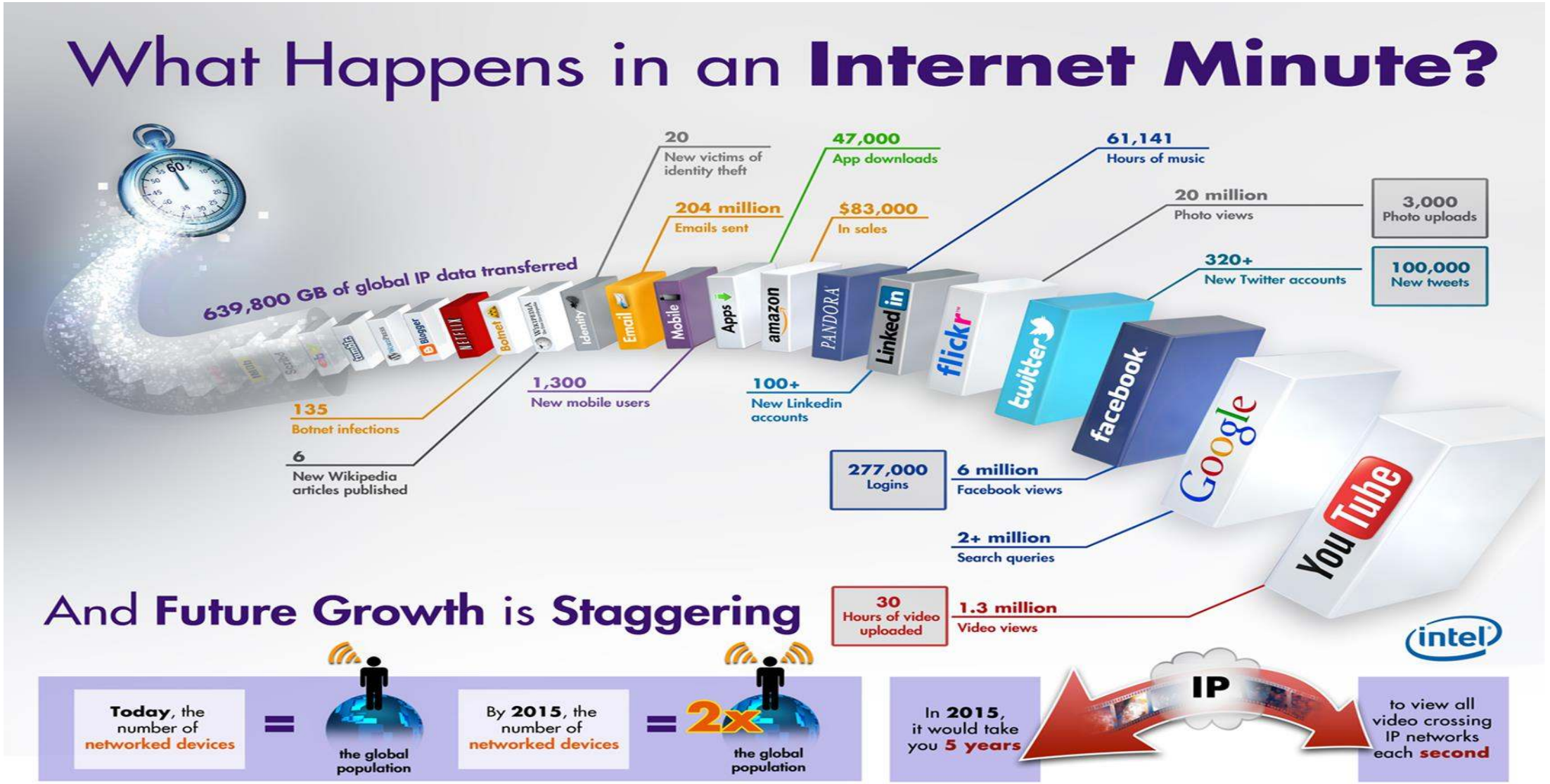


In den 1970er Jahren kam es zu einem folgenträchtigen Rollentausch:.

Übergang von einem Energie- zu einem informationsgetriebenen Strukturwandel.

http://www.sechster-kondratieff.de/sechster_kondratieff_fortsetzung.html

Ergbnis dieses Strukturwandels: **Cyberspace !**



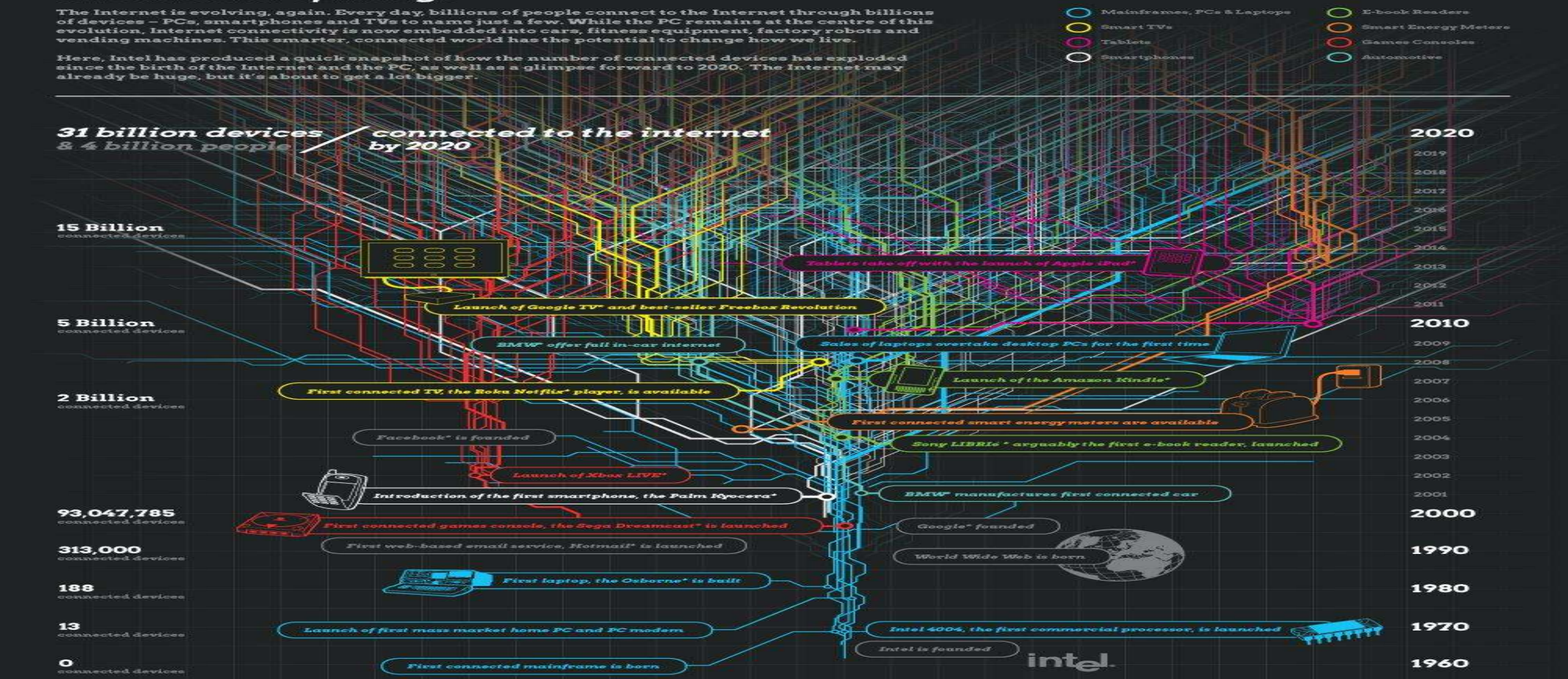
Beeindruckende Zahlen und extrem Komplex

aber nichts im Vergleich zu dem was auf uns zu kommt…..

The Internet of Things

The Internet is evolving, again. Every day, billions of people connect to the Internet through billions of devices – PCs, smartphones and TVs to name just a few. While the PC remains at the centre of this evolution, Internet connectivity is now embedded into cars, fitness equipment, factory robots and vending machines. This smarter, connected world has the potential to change how we live.

Here, Intel has produced a quick snapshot of how the number of connected devices has exploded since the birth of the Internet and the PC, as well as a glimpse forward to 2020. The Internet may already be huge, but it's about to get a lot bigger.

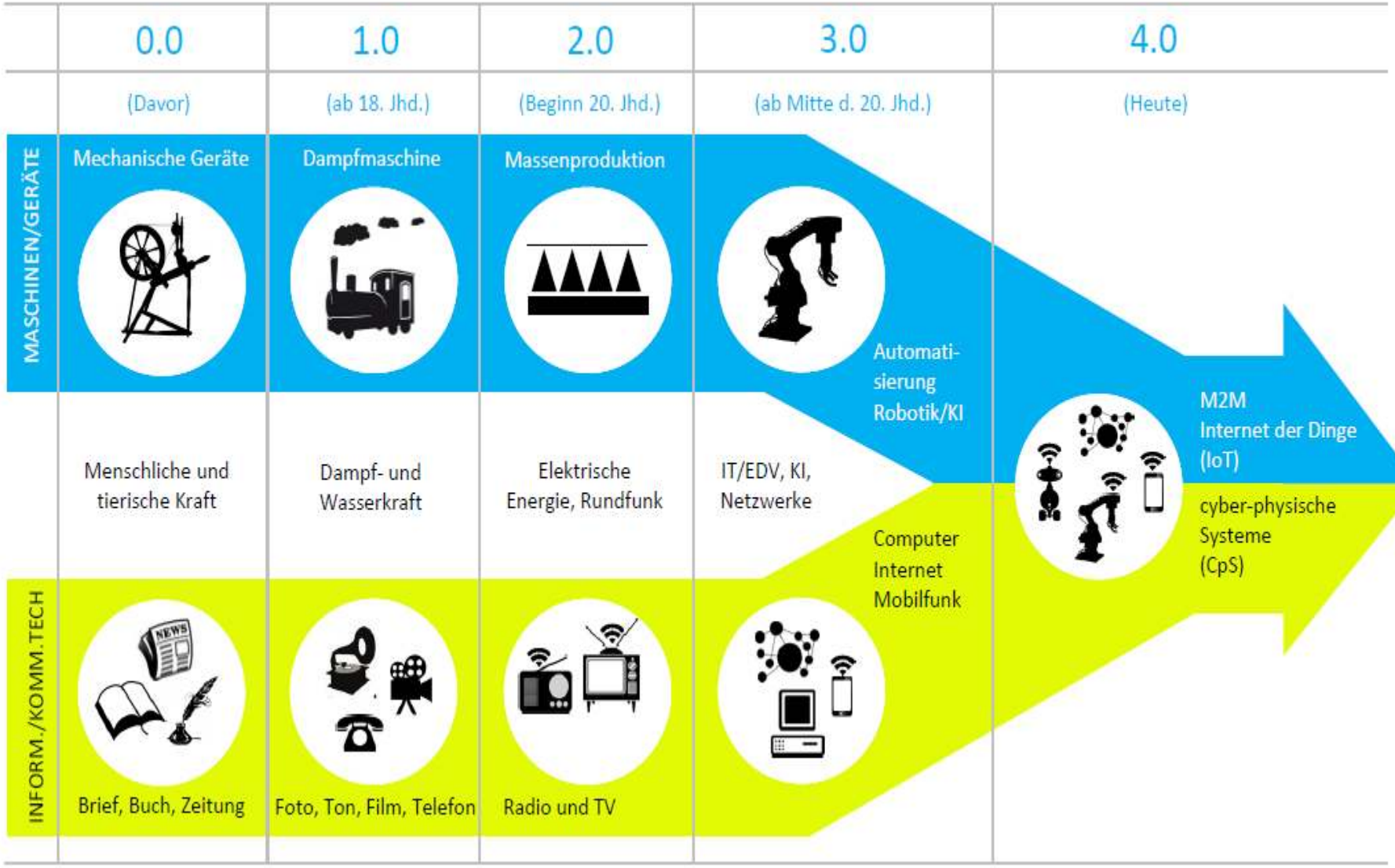


More than one million PCs sold every day

80% of all PCs shipped today have Intel® Inside

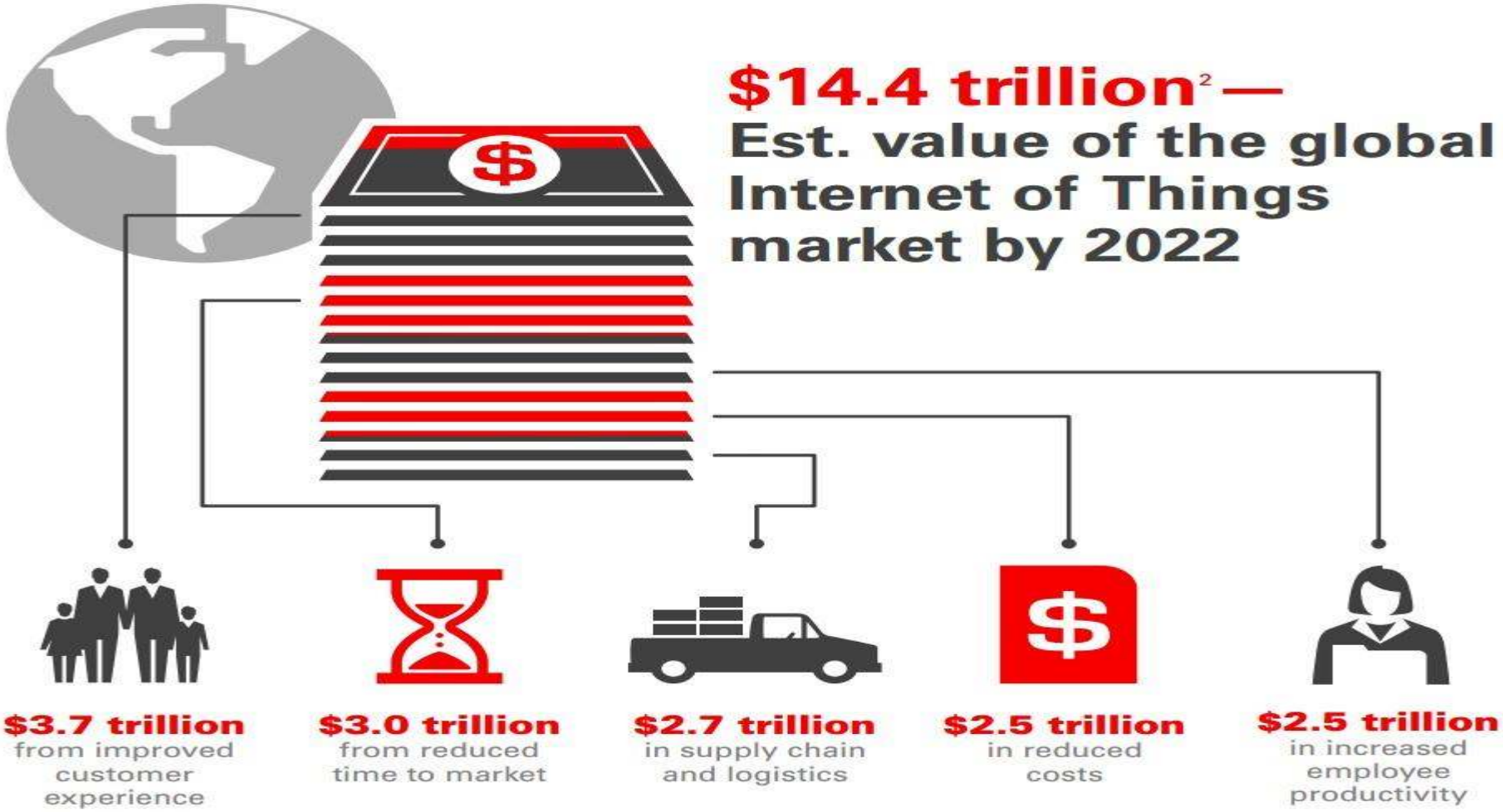
The data referenced in this document came from a variety of sources. For a full list please visit: www.intel.co.uk/internetofthings

Grundlegende Trends dieser Entwicklung



- ✓ Smart Grids
- ✓ Smart Robots
- ✓ Smart Buildings
- ✓ Smart Mobil
  - Verkehr
  - Automobil
- ✓ Smarte Fabriken
- ✓ E-Health
- ✓ Digitale Assistenz
- ✓ Militär

Estimated Market potential



http://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/#305877dd48a0

Was ist das Digitalisierung ?

ubiqitär

intersektoral

pervasiv

konvergent

exponentiell

3. Conclusio

Erkenntnis

Angreifer sind längst im “Internet of Things angekommen”

Ein Beispiel

Mirai-Wurm – IoT-Botnet (Mirai=Zukunft)

cameradome-20161118-03.pcap

File Edit View Go

tcp.stream eq 12

No.	Time
2086	95.308393
2087	95.413049
2088	95.417241
2089	95.419618
2090	95.521022
2091	95.523854
2092	95.657464
2095	98.538577
2096	98.639550
2097	98.639608
2098	98.642883
2099	98.749931
2100	98.760263
2101	98.897786
2102	98.898514
2103	99.010530

```
0000  00 12 15 4c
0010  00 31 ef ab
0020  01 0a e1 ee
0030  1c 84 0d 47
```

cameradome-20

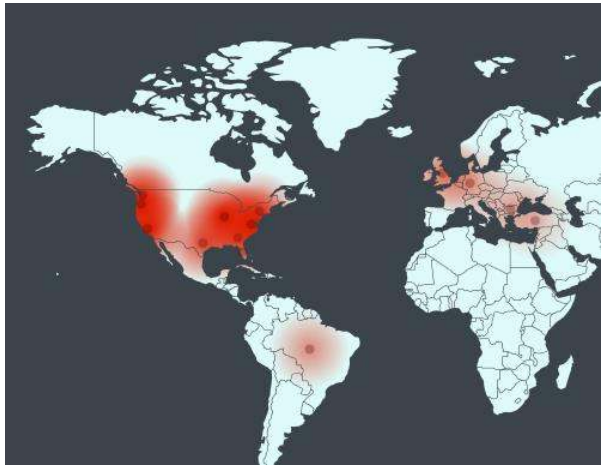
Wireshark · Follow TCP Stream (tcp.stream eq 12) · cameradome-20161118-03

```
.....LocalHost login: .....admin
admin
Password: 1111111

Login incorrect
LocalHost login: admin
admin
Password: 1234

Login incorrect
LocalHost login: root
root
Password: xmhdipc

.[1;32mWelcome to Monitor Tech..[0;39m
# enable
system
ping ; sh
enable
-sh: enable: not found
cat /proc/mounts; /bin/busybox VNLJT
# system
-sh: system: not found
# ping ; sh
BusyBox v1.16.1 (2014-04-11 14:47:44 CST) multi-call binary.

Usage: ping [OPTIONS] HOST

# cat /proc/mounts; /bin/busybox VNLJT
rootfs / rootfs rw 0 0
/dev/root / cramfs ro,relatime 0 0
proc /proc proc rw,relatime 0 0
```

16 client pkt(s), 34 server pkt(s), 28 turns.

“This security camera was infected by malware 98 seconds after it was plugged in”

DDoS-Attacke legt Twitter, Amazon Netflix, Paypal, Spotify und andere Dienste lahm



Bildquelle: akamai.com

Das US-Unternehmen Dyn teilte am Freitag mit, es untersuche eine Reihe von Angriffen auf seine DNS-Infrastruktur.

Dyn betreibt nicht nur den Service DynDNS zur dynamischen Aktualisierung von Domain-Einträgen, sondern ist auch Provider für die klassischen DNS-Systeme vieler großer US-Konzerne.

21.10.2016

https://www.dynstatus.com/incidents/nlr4yrr162t8

https://www.heise.de/newsticker/meldung/DDoS-Attacke-legt-Twitter-Netflix-Paypal-Spotify-und-andere-Dienste-lahm-3357289.html

Frustrierter PlayStation-Spieler legte Teile des Internets lahm

(Bild: Sony)

Wütender Gamer ? Sic !

Der recht simpel angelegte Angriff sollte lediglich das PlayStation Network lahmlegen

Er habe sich für seinen Angriff ein Bot-Netz von rund 150.000 internetfähigen Geräten für einen Zeitraum "gemietet", darunter auch Kameras, Glühbirnen und Haushaltsgeräte.

https://www.heise.de/security/meldung/Frustrierter-PlayStation-Spieler-legte-Teile-des-Internets-lahm-3492276.html

Driverless …unter anderen Gesichtspunkten..

Charlie Miller und Chris Valasek's konnten mit Hilfe eines manipulierten Mobilfunk-Anrufs den Zugriff auf Jeep´s "internet-connected entertainment system" erlangen und von dort "mission critical functions" erreichen.

Aus einer Entfernung von 12 Meilen, konnten Hacker des Keen Security Labs – das Bremssystem eines Tesla S nur mit einem Laptop manipulieren.
Zudem konnten Sie die Kontrolle über das Infotainmentsystem, Comfort-Funktionen (Türen, Fensterheber, Seitenspiegel) und das Lichtsystem erlangen – **während das Auto fuhr !**

it governance, September 2016 -https://youtu.be/c1XyhReNcHY,

Source: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

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 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, ???

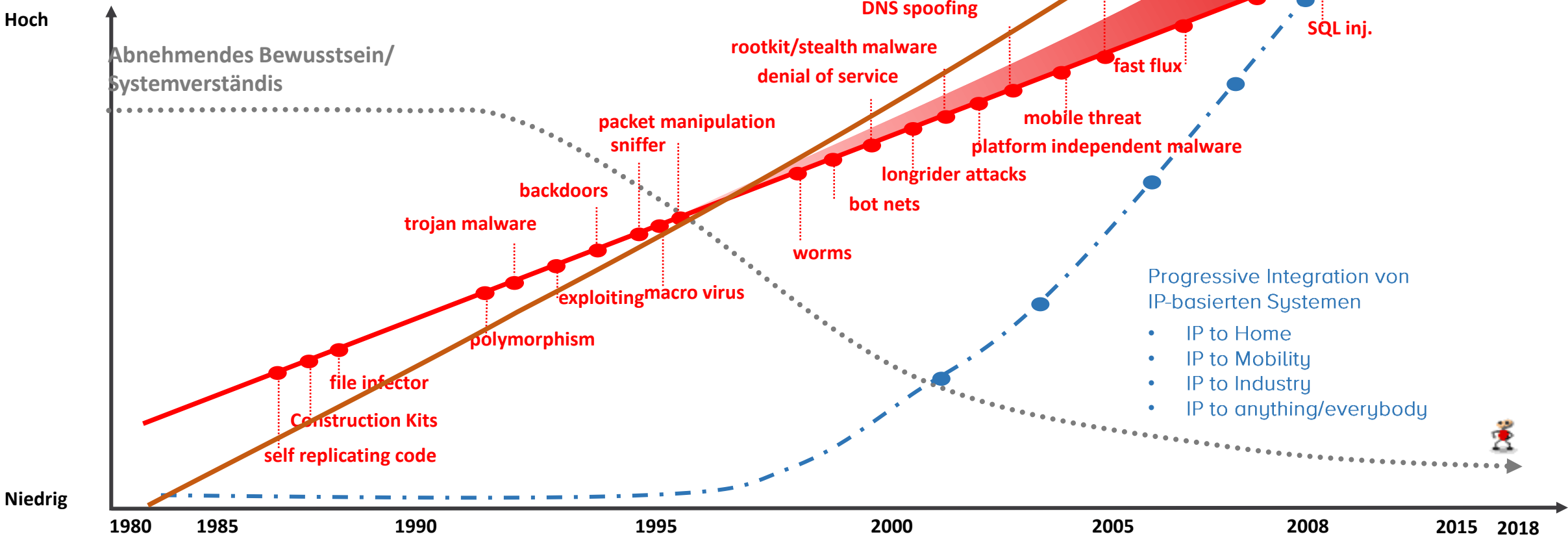
Steigende Zahl, Komplexität und Intelligenz von Angriffen

Dunkelziffer: Anzahl der nicht bekannten Attacken/Malware

Steigender Grad der Vernetzung, technologische Entwicklung

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

Sinkendes Verständnis für .....



Wir fassen zusammen

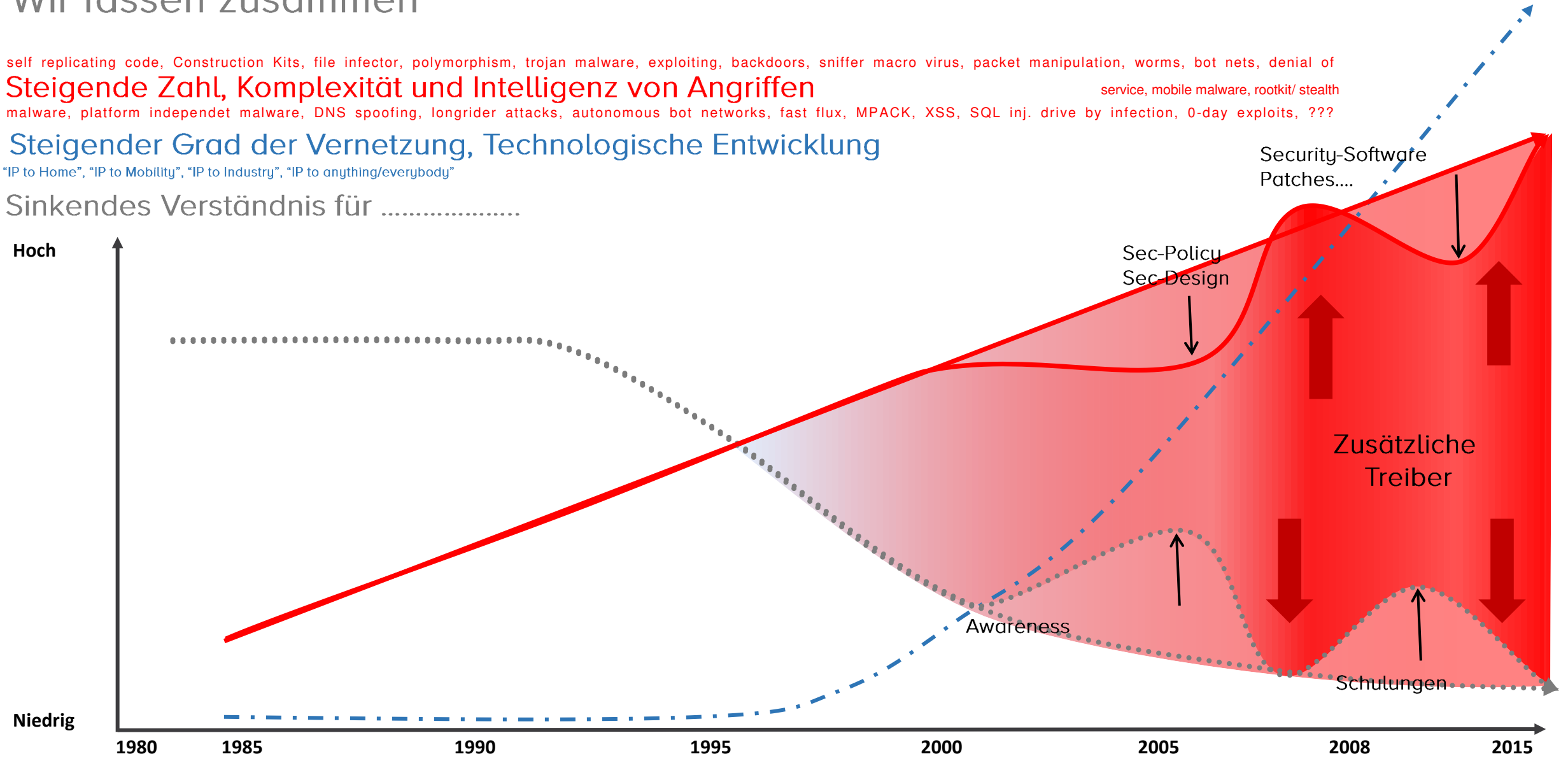
self replicating code, Construction Kits, file infector, polymorphism, trojan malware, exploiting, backdoors, sniffer macro virus, packet manipulation, worms, bot nets, denial of service, mobile malware, rootkit/ stealth malware, platform independet malware, DNS spoofing, longrider attacks, autonomous bot networks, fast flux, MPACK, XSS, SQL inj. drive by infection, 0-day exploits, ???

Steigende Zahl, Komplexität und Intelligenz von Angriffen

Steigender Grad der Vernetzung, Technologische Entwicklung

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

Sinkendes Verständnis für .....



3. Conclusio

Erkenntnis!

Es braucht das dringende Bewusstsein, dass mit diesen enormen Chancen auch enorme Risiken verbunden sind – die es zu meistern gilt.

Kein Einzelner -
Nicht mehr wenige!

Nur wir alle !!
Dafür brauchen wir IHR Interesse !

CyberSecurity

– res publica –

ES geht uns alle an!

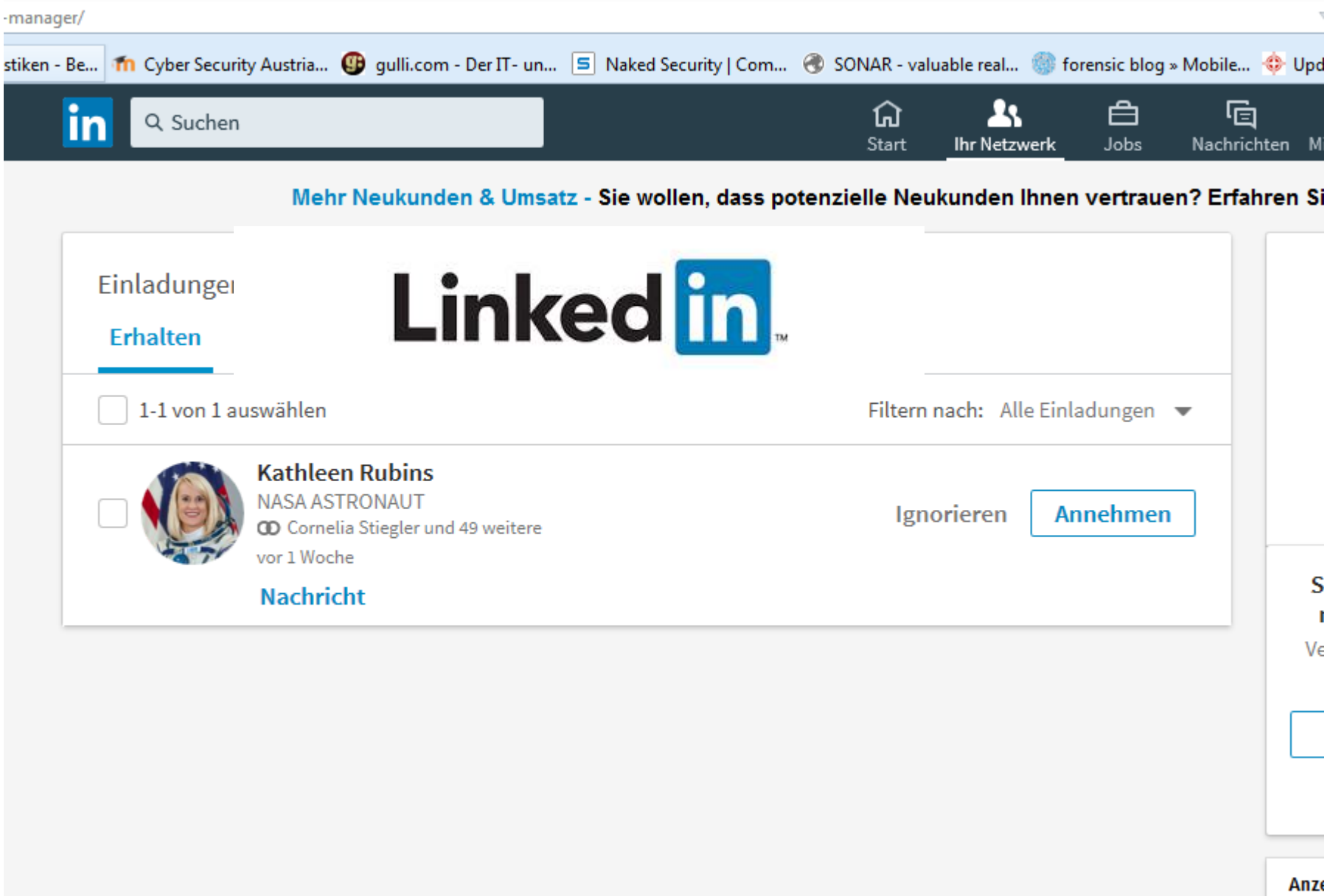
www.cybersecurityaustria.at

Vielen DANK

und Kopf hoch ☺

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

Goldgrube „linkedin“



Kathleen Rubins • 1.

NASA ASTRONAUT

Austria area • 500+

Nachricht

Gemeinsam

50 gemeinsame Kontakte

Sie und Kathleen Rubins kennen Martin Bredl, Alexander Glaub und 48 weitere Personen.

Kontakte anzeigen (500+)

Kontaktinformationen

Kathleen Rubins' Profil
linkedin.com/in/davidbergot

Webseite
la-boite-a-finances.com/ (Unternehmenswebseite)

la-boite-a-finances.com/blog/ (Blog)

Telefonnummer
0180888301 (Geschäft)

Adresse
Paris La Défense

E-Mail
david.bergot@la-boite-a-finances.com

Geburtstag
25. Oktober

Weniger anzeigen

www.la-boite-a-finances.com

Meistbesucht | IKARUS Intranet - Ho... | VBASE Statistiken - Be... | Cyber Security Austria... | gulli.com - Der IT- un... | Naked Security | Com... | SONAR - valuable real... | forensic blog » Mobile... | Update-Log

LBF CONSEIL
Gestion de Patrimoine
La Boîte à Finances

À propos

Accueil » **La Boîte à Finances**

Être conseillé en ligne et rester libre.

Bienvenue sur la plateforme de **Conseil en Gestion de Patrimoine en ligne** de "L

Nos services s'adressent aux particuliers et chefs d'entreprise à la recherche d'u
patrimoniale, de réductions d'impôt ou encore de placements performants à frais réd

Structuré et équipé pour exercer à distance, tout particulièrement en ligne, par Intern

Notre plateforme *FinTech* est conçue pour celles et ceux qui n'ont pas de temps à
simplement privilégient Internet pour la gestion de leur patrimoine... nous sommes ph

Google Index
Alexa
SimilarWeb
SEMRush
BuiltWith

Recently Analyzed Websites

mehrnews.com
unihosiery.com
staceysnacksonline.com
globcat.com
grandfilm44.in
carhartt-wip.jp
globalknivar.com
wmiis.com

la-boite-a-finances.com Free traffic, earnings, rankings report

la-boite-a-finances.com receives about 39 visits and 39 (1 per visitor) pageviews per day which should earn about $0.14/day from content advertising revenue. Estimated site value is $148.68. According to Alexa Traffic Rank la-boite-a-finances.com is ranked number 3,561,173 in the world, and its traffic has increased drastically (300 percent) over the past 3 months. This website attracts most of its visitors from Unknown Country (0 percent).

Traffic & Earnings Report

Website	la-boite-a-finances.com
Website Value	**$94000**
Alexa Rank	3

Fake-profile auf linkedin

Start | XING | Hannes Spissak | LinkedIn | hannes spissak - Google-S...

https://www.linkedin.com/profile/view?id=402888652&authType=name&authToken=rm7G&invAcpt=40792440_I5971545125665406976_500&csrfToken=ajax%3A0137902416309091378&trk=nav_utilities_invites_name

Meistbesucht | IKARUS Intra

PREMIUM | Nach Personen, Stellen, Unternehmen usw. suchen ... | Erweitert

Start | Profil | Netzwerk | Stellenmarkt | Interessen | Business-Services | Premium gratis testen

Hannes Spissak

1.

Operations Manager at mobilkom austria

Österreich | Telekommunikation

Aktuell mobilkom austria

Nachricht senden

359
Kontakte

at.linkedin.com/pub/hannes-spissak/b2/b15/1a4/de

Kontaktdaten

Über mich

Berufserfahrung

Operations Manager
mobilkom austria

mobilkom austria

Empfehlungen

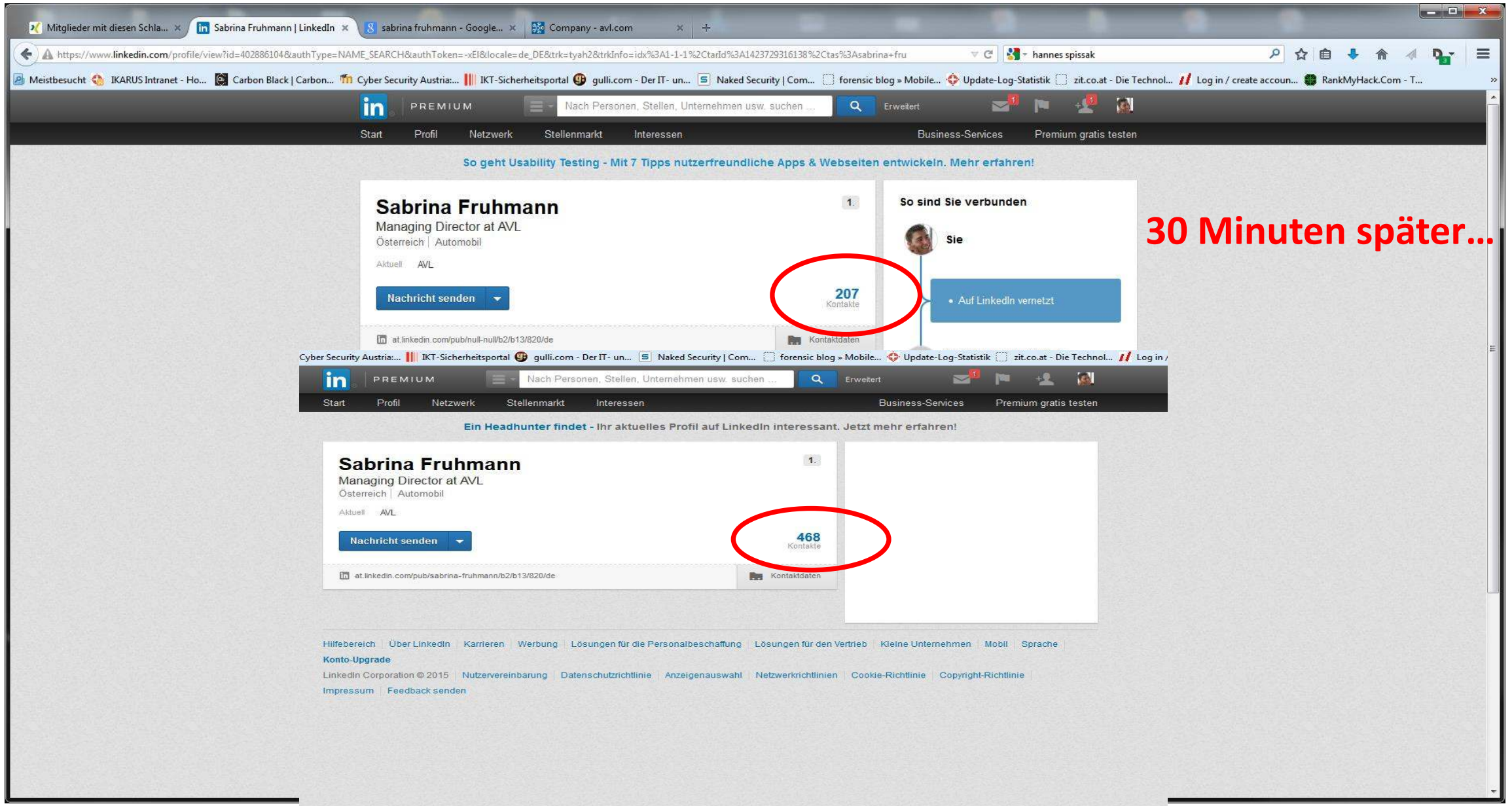
So sind Sie verbunden

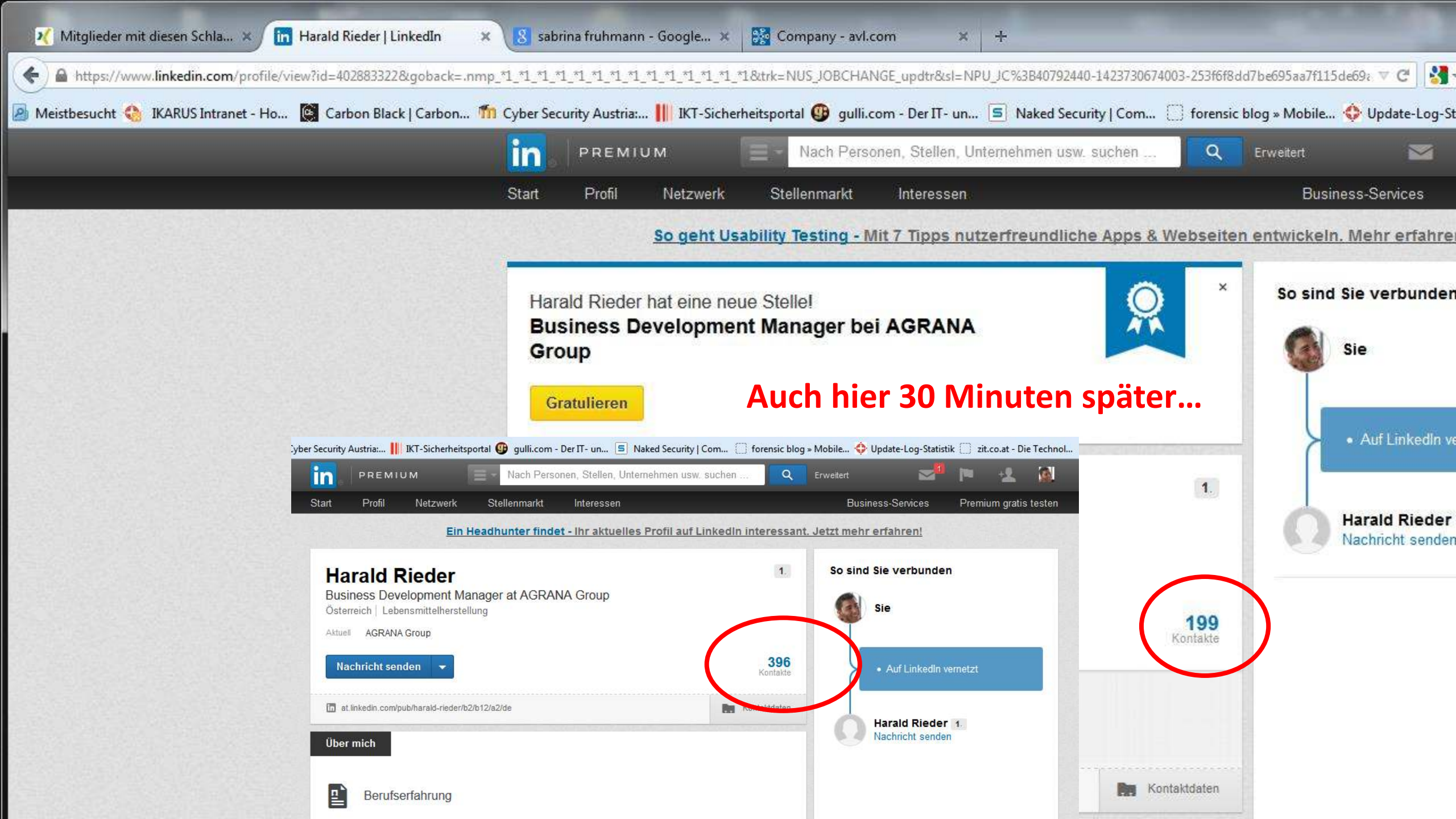
Sie

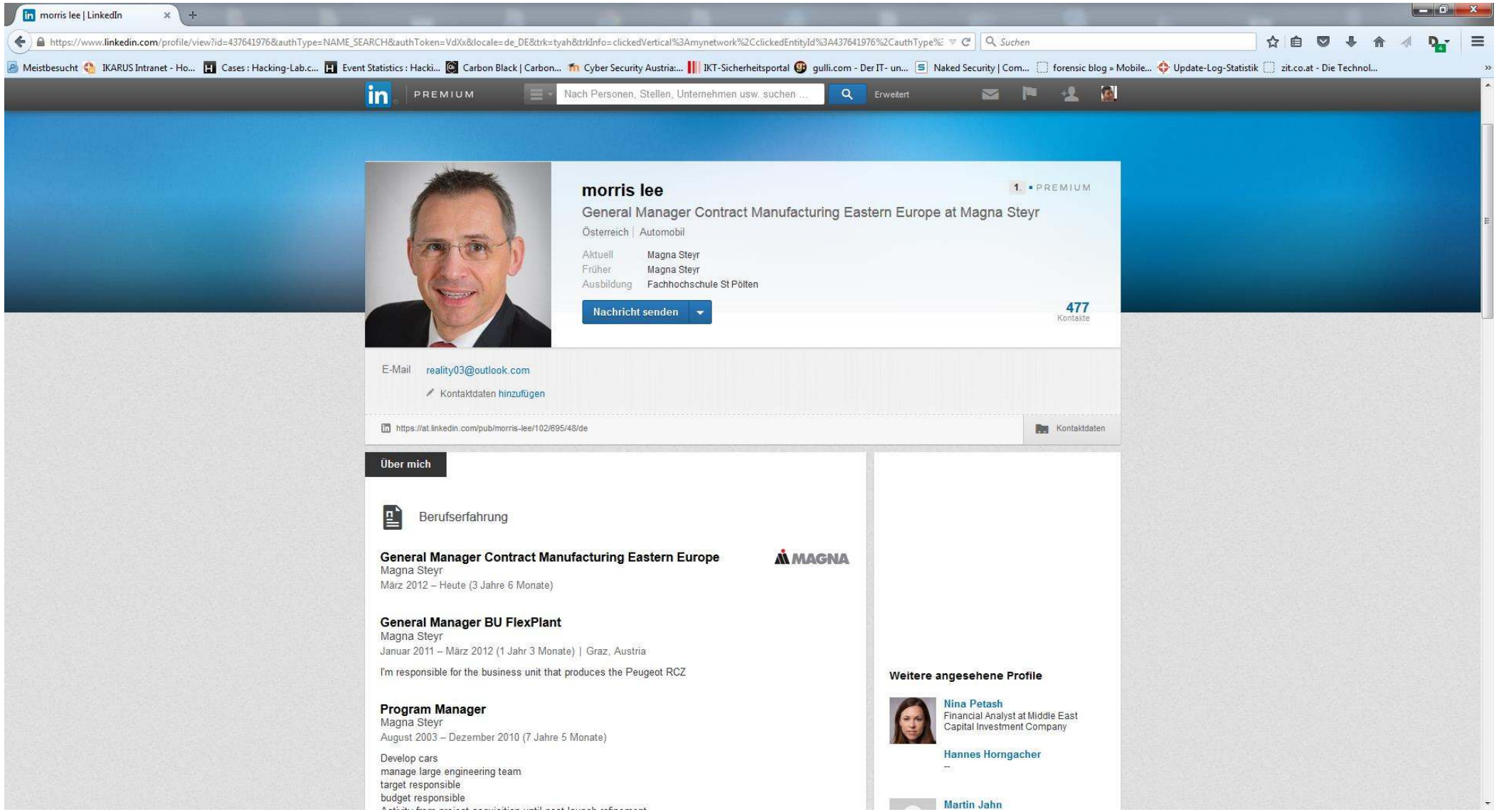
• Auf LinkedIn vernetzt

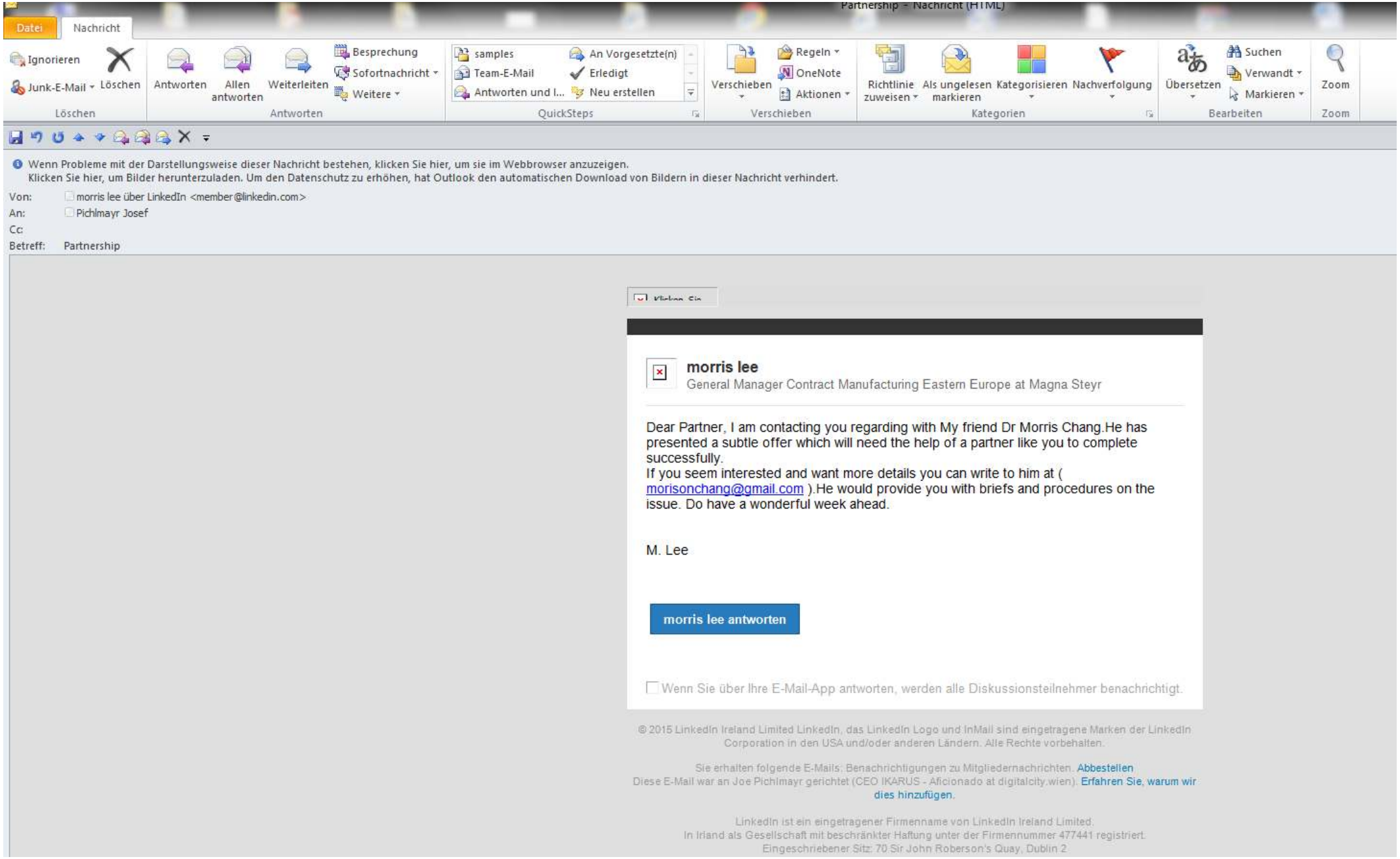
Hannes Spissak 1.
Nachricht senden

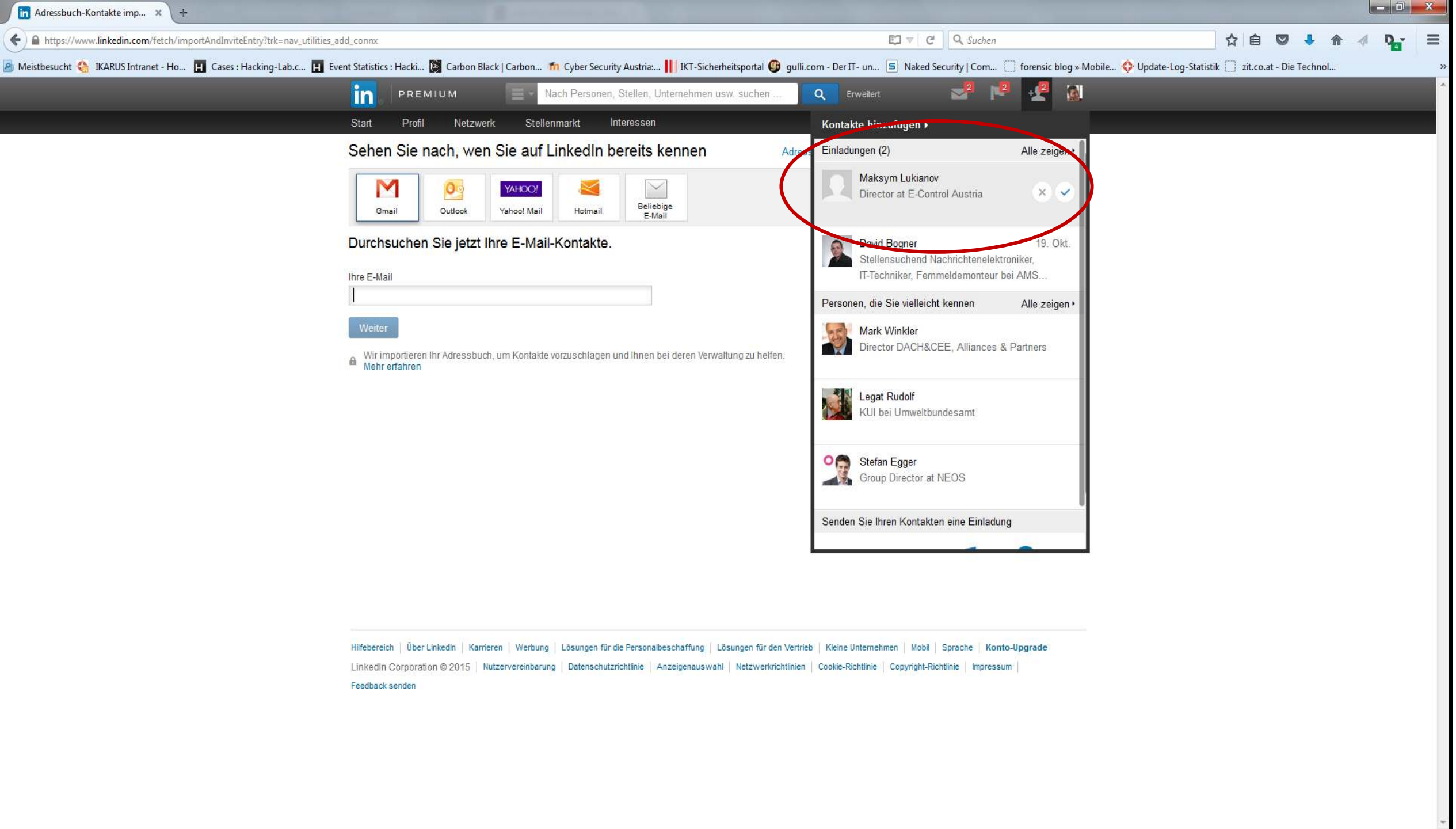
Wie kommt man zu Kontakten…




Mitglieder mit diesen Schla...
Harald Rieder | LinkedIn
sabrina fruhmann - Google...
Company - avl.com
https://www.linkedin.com/profile/view?id=402883322&goback=.nmp_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1_*1&trk=NUS_JOBCHANGE_updtr&sl=NPU_JC%3B40792440-1423730674003-253f6f8dd7be695aa7f115de69
Meistbesucht
IKARUS Intranet - Ho...
Carbon Black | Carbon...
Cyber Security Austria:...
IKT-Sicherheitsportal
gulli.com - Der IT- un...
Naked Security | Com...
forensic blog » Mobile...
Update-Log-St
PREMIUM
Nach Personen, Stellen, Unternehmen usw. suchen ...
Erweitert
Start
Profil
Netzwerk
Stellenmarkt
Interessen
Business-Services
So geht Usability Testing - Mit 7 Tipps nutzerfreundliche Apps & Webseiten entwickeln. Mehr erfahre
Harald Rieder hat eine neue Stelle!
Business Development Manager bei AGRANA Group
Gratulieren
Auch hier 30 Minuten später...
So sind Sie verbunden
Sie
Auf LinkedIn ve
Harald Rieder
Nachricht senden
Cyber Security Austria:...
IKT-Sicherheitsportal
gulli.com - Der IT- un...
Naked Security | Com...
forensic blog » Mobile...
Update-Log-Statistik
zit.co.at - Die Technol...
PREMIUM
Nach Personen, Stellen, Unternehmen usw. suchen ...
Erweitert
Start
Profil
Netzwerk
Stellenmarkt
Interessen
Business-Services
Premium gratis testen
Ein Headhunter findet - Ihr aktuelles Profil auf LinkedIn interessant. Jetzt mehr erfahren!
Harald Rieder
1.
Business Development Manager at AGRANA Group
Österreich | Lebensmittelherstellung
Aktuell AGRANA Group
Nachricht senden
396
Kontakte
at.linkedin.com/pub/harald-rieder/b2/b12/a2/de
Über mich
Berufserfahrung
So sind Sie verbunden
Sie
Auf LinkedIn vernetzt
Harald Rieder 1.
Nachricht senden
1.
199
Kontakte
Kontaktdaten


morris lee | LinkedIn
https://www.linkedin.com/profile/view?id=437641976&authType=NAME_SEARCH&authToken=VdXx&locale=de_DE&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2CclickedEntityId%3A437641976%2CauthType%3
Meistbesucht
IKARUS Intranet - Ho...
Cases : Hacking-Lab.c...
Event Statistics : Hacki...
Carbon Black | Carbon...
Cyber Security Austria:...
IKT-Sicherheitsportal
gulli.com - Der IT- un...
Naked Security | Com...
forensic blog » Mobile...
Update-Log-Statistik
zit.co.at - Die Technol...
PREMIUM
Nach Personen, Stellen, Unternehmen usw. suchen ...
Erweitert
morris lee
1. PREMIUM
General Manager Contract Manufacturing Eastern Europe at Magna Steyr
Österreich | Automobil
Aktuell Magna Steyr
Früher Magna Steyr
Ausbildung Fachhochschule St Pölten
Nachricht senden
477
Kontakte
E-Mail reality03@outlook.com
Kontaktdaten hinzufügen
https://at.linkedin.com/pub/morris-lee/102/695/48/de
Kontaktdaten
Über mich
Berufserfahrung
General Manager Contract Manufacturing Eastern Europe
Magna Steyr
März 2012 – Heute (3 Jahre 6 Monate)
MAGNA
General Manager BU FlexPlant
Magna Steyr
Januar 2011 – März 2012 (1 Jahr 3 Monate) | Graz, Austria
I'm responsible for the business unit that produces the Peugeot RCZ
Program Manager
Magna Steyr
August 2003 – Dezember 2010 (7 Jahre 5 Monate)
Develop cars
manage large engineering team
target responsible
budget responsible
Weitere angesehene Profile
Nina Petash
Financial Analyst at Middle East Capital Investment Company
Hannes Horngacher
--
Martin Jahn


Partnership - Nachricht (HTML)
Datei
Nachricht
Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Sofortnachricht
Weitere
Löschen
Antworten
samples
Team-E-Mail
Antworten und l...
An Vorgesetzte(n)
Erledigt
Neu erstellen
QuickSteps
Verschieben
Regeln
OneNote
Aktionen
Verschieben
Richtlinie zuweisen
Als ungelesen markieren
Kategorisieren
Nachverfolgung
Kategorien
Übersetzen
Suchen
Verwandt
Markieren
Bearbeiten
Zoom
Zoom
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.
Von: morris lee über LinkedIn <member@linkedin.com>
An: Pichlmayr Josef
Cc:
Betreff: Partnership
morris lee
General Manager Contract Manufacturing Eastern Europe at Magna Steyr
Dear Partner, I am contacting you regarding with My friend Dr Morris Chang.He has presented a subtle offer which will need the help of a partner like you to complete successfully.
If you seem interested and want more details you can write to him at (morisonchang@gmail.com).He would provide you with briefs and procedures on the issue. Do have a wonderful week ahead.
M. Lee
morris lee antworten
Wenn Sie über Ihre E-Mail-App antworten, werden alle Diskussionsteilnehmer benachrichtigt.
© 2015 LinkedIn Ireland Limited LinkedIn, das LinkedIn Logo und InMail sind eingetragene Marken der LinkedIn Corporation in den USA und/oder anderen Ländern. Alle Rechte vorbehalten.
Sie erhalten folgende E-Mails: Benachrichtigungen zu Mitgliedernachrichten. Abbestellen
Diese E-Mail war an Joe Pichlmayr gerichtet (CEO IKARUS - Aficionado at digitalcity.wien). Erfahren Sie, warum wir dies hinzufügen.
LinkedIn ist ein eingetragener Firmenname von LinkedIn Ireland Limited.
In Irland als Gesellschaft mit beschränkter Haftung unter der Firmennummer 477441 registriert.
Eingeschriebener Sitz: 70 Sir John Roberson's Quay, Dublin 2


Adressbuch-Kontakte imp...
https://www.linkedin.com/fetch/importAndInviteEntry?trk=nav_utilities_add_connx
Suchen
Meistbesucht
IKARUS Intranet - Ho...
Cases : Hacking-Lab.c...
Event Statistics : Hacki...
Carbon Black | Carbon...
Cyber Security Austria:...
IKT-Sicherheitsportal
gulli.com - Der IT- un...
Naked Security | Com...
forensic blog » Mobile...
Update-Log-Statistik
zit.co.at - Die Technol...
PREMIUM
Nach Personen, Stellen, Unternehmen usw. suchen ...
Erweitert
Start
Profil
Netzwerk
Stellenmarkt
Interessen
Sehen Sie nach, wen Sie auf LinkedIn bereits kennen
Gmail
Outlook
Yahoo! Mail
Hotmail
Beliebige E-Mail
Durchsuchen Sie jetzt Ihre E-Mail-Kontakte.
Ihre E-Mail
Weiter
Wir importieren Ihr Adressbuch, um Kontakte vorzuschlagen und Ihnen bei deren Verwaltung zu helfen.
Mehr erfahren
Kontakte hinzufügen
Einladungen (2)
Alle zeigen
Maksym Lukianov
Director at E-Control Austria
David Bogner
19. Okt.
Stellensuchend Nachrichtenelektroniker, IT-Techniker, Fernmeldemonteur bei AMS...
Personen, die Sie vielleicht kennen
Alle zeigen
Mark Winkler
Director DACH&CEE, Alliances & Partners
Legat Rudolf
KUI bei Umweltbundesamt
Stefan Egger
Group Director at NEOS
Senden Sie Ihren Kontakten eine Einladung
Hilfebereich | Über LinkedIn | Karrieren | Werbung | Lösungen für die Personalbeschaffung | Lösungen für den Vertrieb | Kleine Unternehmen | Mobil | Sprache | Konto-Upgrade
LinkedIn Corporation © 2015 | Nutzervereinbarung | Datenschutzrichtlinie | Anzeigenauswahl | Netzwerkrichtlinien | Cookie-Richtlinie | Copyright-Richtlinie | Impressum
Feedback senden

Maksym Lukianov | LinkedIn

https://www.linkedin.com/profile/view?id=AAkAABsPRocBskLIE4hyi1uZSU3K6tB-xrXNJaA&authType=NAME_SEARCH&authToken=E68U&locale=de_DE&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2Cclickec

Meistbesucht | IKARUS Intranet - Ho... | Cases : Hacking-Lab.c... | Event Statistics : Hacki... | Carbon Black | Carbon... | Cyber Security Austria:... | IKT-Sicherheitsportal | gulli.com - Der IT- un... | Naked Security

PREMIUM

Nach Personen, Stellen, Unternehmen usw. suchen ...

Erweitert

Start | Profil | Netzwerk | Stellenmarkt | Interessen | Business-Services

Maksym Lukianov

1

Director at E-Control Austria

Österreich | IT und Services

Aktuell E-Control Austria

Nachricht senden

35
Kontakte

https://at.linkedin.com/pub/maksym-lukianov/108/57/407/de

Kontaktdaten

Über mich

Berufserfahrung

Director
E-Control Austria

Empfehlungen

Maksym Lukianov | LinkedIn

https://www.linkedin.com/profile/view?id=AAkAABsPRocBskLIE4hyi1uZSU3K6tB-xrXNJaA&authType=NAME_SEARCH&authToken=E68U&locale=de_DE&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2Cclickec

Meistbesucht | IKARUS Intranet - Ho... | Cases : Hacking-Lab.c... | Event Statistics : Hacki... | Carbon Black | Carbon... | Cyber Security Austria:... | IKT-Sicherheitsportal | gulli.com - Der IT- un... | Naked Security

PREMIUM | Nach Personen, Stellen, Unternehmen usw. suchen ... | Erweitert

Start | Profil | Netzwerk | Stellenmarkt | Interessen | Business-Services

Maksym Lukianov

1

Director at E-Control Austria

Österreich | IT und Services

Aktuell E-Control Austria

Nachricht senden

35
Kontakte

E-Mail maksymlukianov54@rediffmail.com

Kontaktdaten hinzufügen

https://at.linkedin.com/pub/maksym-lukianov/108/57/407/de

Kontaktdaten

Über mich

Berufserfahrung

Director
E-Control Austria