

Ransomware



Compass Security - seit 1999

45 Mitarbeiter in Jona, Bern, Berlin



Dienstleistungen der Compass Security



Penetration Tests

Assuming the role of an attacker, we test your devices, networks, services, and applications for vulnerabilities. Using social engineering and red teaming we test the behavior and processes of the whole organization. » [read more](#)



Security Reviews

Experienced IT analysts support you with a second opinion on security concepts and if requested, test the structure, configuration, and source code of your solution. » [read more](#)



Digital Forensics

Our forensic experts help with incident coordination and immediate measures, as well as legally watertight processing of data. In addition, we offer quick and uncomplicated investigation of root causes. » [read more](#)



Security Trainings

Benefit from our analysts' knowledge of penetration testing, network analysis, digital forensics, secure mobile apps, and other applications, or choose to receive training in our specially created lab. » [read more](#)



FileBox

FileBox is a solution for both secure file transfer and secure file storage. It provides you with the ability to securely exchange documents. » [read more](#)



Hacking-Lab

Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. » [read more](#)





Worin liegt das
Business Modell der
Angreifer bei Locky,
WannaCry und Petya?

Motive für Hacker Attacken?

**GAME
HACK**



[ENABLE FILTERS]

Total notifications: **229,887** of which **91,599** single ip and **138,288** mass defacements

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

 - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	 Domain	OS	View
2017/09/26	amm4Washere			R		 dpesdm.sukabumikab.go.id/readm...	Linux	mirror
2017/09/26	GAZA	H	M	R		 saaelp.mg.gov.br	Linux	mirror
2017/09/26	GAZA	H	M	R		 cedrodoabaete.mg.gov.br	Linux	mirror
2017/09/26	GeNErAL			R		 www.sonora.gob.mx/by.htm	Linux	mirror
2017/09/26	Panataran					 jumalarkeologipapua.kemdikbud...	Linux	mirror
2017/09/26	Mister Spy					 www.pechenigi-rda.gov.ua//spy.gif	Linux	mirror
2017/09/26	Typical Idiot Security		M			 stopthinkconnect.gov.bd/b0x.htm	Linux	mirror
2017/09/26	Xinox Crew	H	M			 diariooficial.ibaiti.pr.gov.br	Linux	mirror
2017/09/26	Xinox Crew	H	M			 ventania.pr.gov.br	Linux	mirror
2017/09/26	Xinox Crew	H	M	R		 japira.pr.gov.br	Linux	mirror
2017/09/26	Xinox Crew	H	M	R		 ibaiti.pr.gov.br	Linux	mirror
2017/09/26	Xinox Crew	H	M			 cmfiaeira.pr.aov.br	Linux	mirror

Quelle: <http://www.faz.net>

Date	Notifier	H	M	R	L	★ Domain	OS	View
2017/09/22	Hawk_B404					www.jiaan.li/msg.htm	Linux	mirror
2017/09/15	AnonymousFox	H	M			fussballtraining.li	Linux	mirror
2017/09/15	AnonymousFox	H	M			headhunters.li	Linux	mirror
2017/09/08	LUN4T1C0					exklusivtaxi.li/media/media/cs...	Linux	mirror
2017/09/08	LUN4T1C0					ichbin.li/b0x.txt	Linux	mirror
2017/09/07	LUN4T1C0					cest.li/b0x.txt	Linux	mirror
2017/09/07	LUN4T1C0					anandayoga.li/b0x.txt	Linux	mirror
2017/09/02	Fallaga Team	H	M			beer.li	Linux	mirror
2017/08/08	suliman_hacker		M			gola.li/ksa.html	Linux	mirror
2017/08/03	crash-d4rk-h4cker	H				montinari.li	Linux	mirror
2017/07/30	GeNErAL		M			spira.li/by.htm	Win 2008	mirror
2017/07/30	GeNErAL		M	R		in.spira.li/by.htm	Win 2008	mirror
2017/07/22	T1KUS90T		M			youthhostel.li/shutup.htm	Linux	mirror
2017/07/08	Mr.ToKeiChun69		M			ingenious.li/id.php	Linux	mirror
2017/07/02	Mr.ToKeiChun69	H	M			weiyi.li	Linux	mirror
2017/06/11	Jingklong		M	R		www.micromedia.li/idn.htm	Linux	mirror
2017/05/31	SH@Rk M!ND	H				onlinemoviewatchs.li	Unknown	mirror
2017/05/22	chinafans					monoma.li/o.php	Linux	mirror
2017/05/10	GHoST61		M	R		vanessa.li/gh.html	Linux	mirror
2017/04/17	siyahi	H	M			pvo.li	Linux	mirror
2017/04/08	TheWayEnd	H	M			lightingdesign.li	Linux	mirror
2017/03/18	GeNErAL					beauty-nails.li/by.htm	Linux	mirror
2017/03/03	chinafans					muehleholzmarkt.li/x.txt	Linux	mirror
2017/02/21	Shade					tab.li/sh.html	Linux	mirror
2017/02/06	MrHax	H	M	R		topo-lifestyle.li	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Mirror saved on: 2017-09-22 20:15:04

Notified by: Hawk_B404

Domain: <http://www.jiaan.li/msg.htm>

IP address: 45.32.81.49 

System: Linux

Web server: Apache

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-09-22 20:15:04

st@mped by Hawk_B404



We Are :

Mit gestohlenen Kreditkarten bezahlt Polizei fahndet nach mutmaßlichem Betrüger



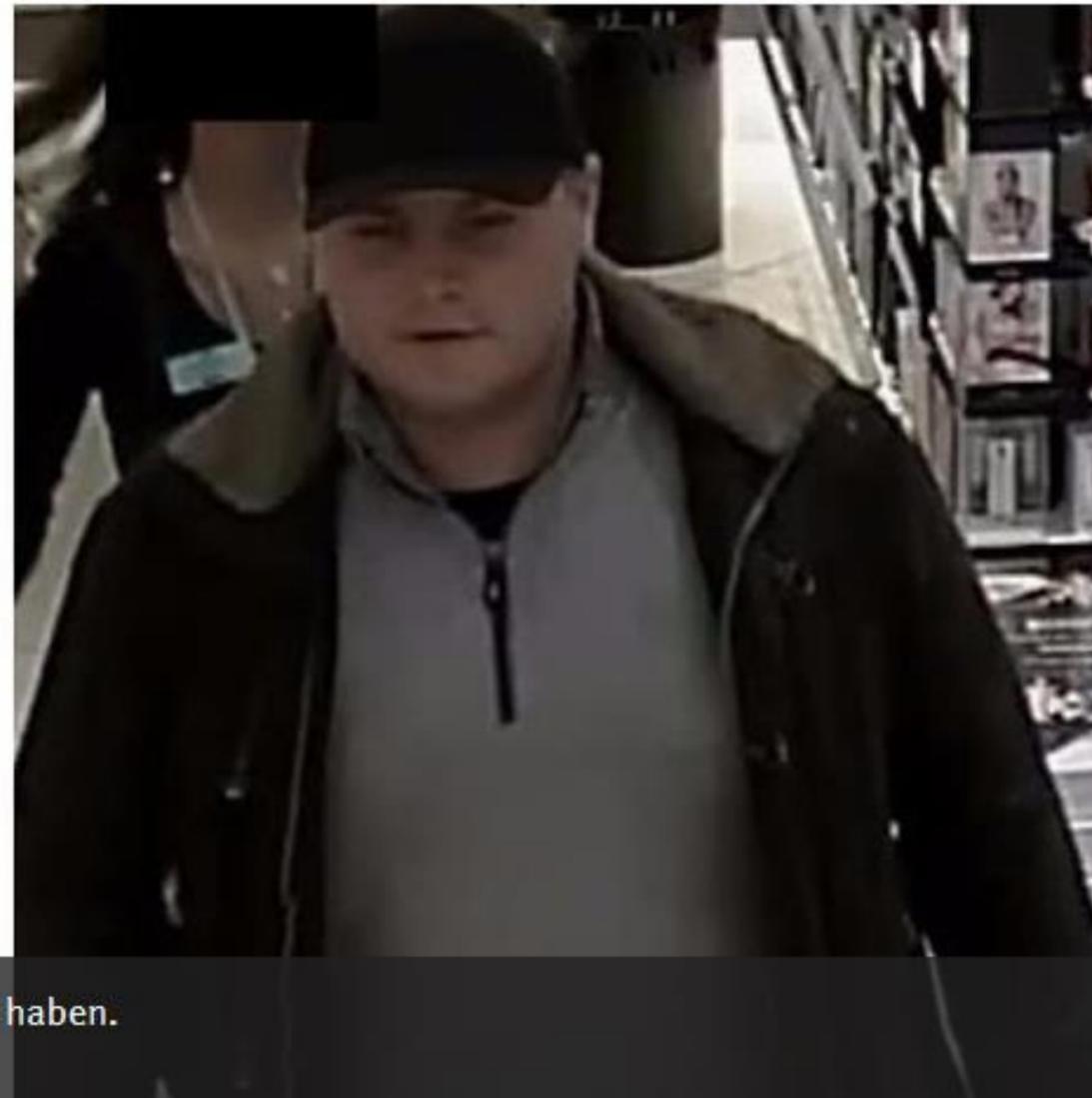
🕒 20.06.17, 11:38 Uhr

✉ EMAIL

📘 FACEBOOK

🐦 TWITTER

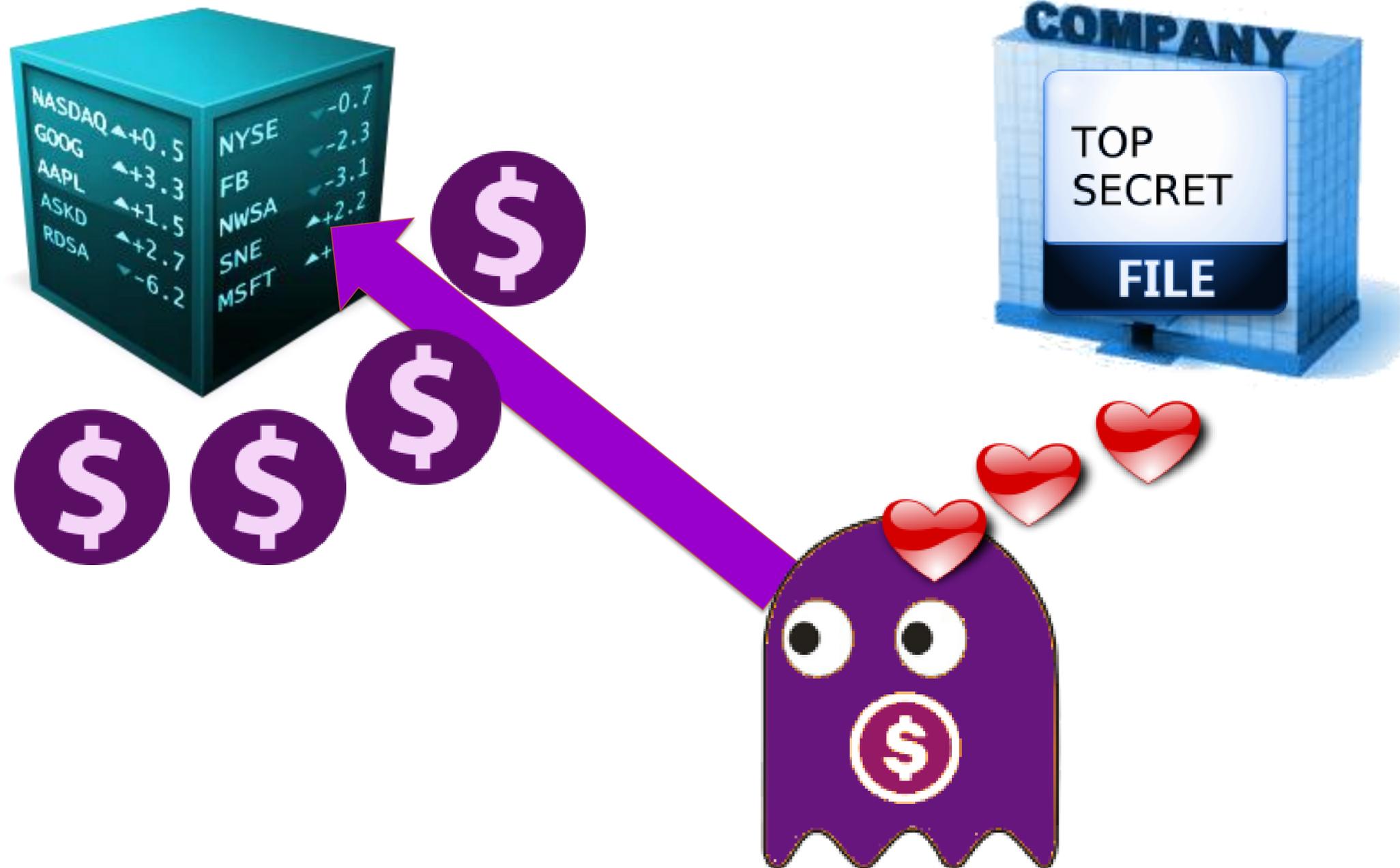
📧 MESSENGER



Dieser Mann soll mehrfach mit gestohlenen Kreditkarten bezahlt haben.
Foto: Polizei Berlin/Collage: BLZ

Quelle: <http://www.berliner-zeitung.de>

Diebstahl Quartalsreport von börsenkotierten Firmen



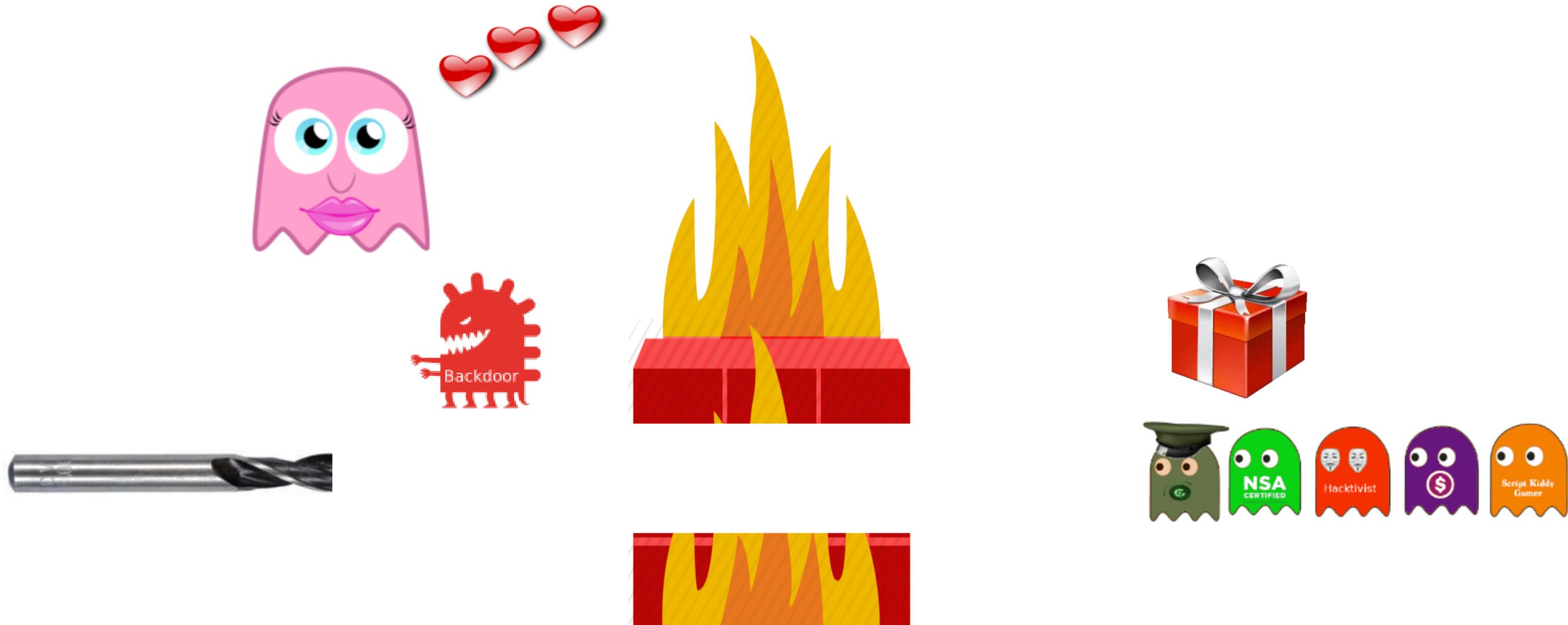
Cyber Crime Business Modelle

- 1) Veräußerung der gestohlenen Güter
- 2) Insider Business
- 3) Erpressung



Angriffe über den Mensch

Angriff auf den «Mensch»



Infektion «Blackout»



SRF

Infektion durch E-Mail



Microsoft Office
Word Document

Infektion durch Web Downlaod



The image shows a screenshot of a computer security warning dialog box. At the top, there is a red horizontal bar with a white octagonal warning icon containing an exclamation mark, followed by the text "SPYWARE ERKANNT!". Below this bar is a white dialog box with a grey border. On the left side of the dialog box is a yellow triangular warning icon with a black exclamation mark. To the right of the icon, the text reads: "Auf Ihrem System wurde Spyware erkannt. Wegen der vorhandenen Malware läuft Ihr Computer langsamer als sonst." At the bottom right of the dialog box is a button labeled "jetzt beheben". A large, green, tilted banner with a red border and red text "NICHT KLICKEN!!!!" is overlaid on the bottom right corner of the dialog box.

SPYWARE ERKANNT!

Auf Ihrem System wurde Spyware erkannt.
Wegen der vorhandenen Malware läuft Ihr Computer langsamer als sonst.

jetzt beheben

NICHT KLICKEN!!!!

Was macht Locky, WannaCry & Co?



Fachjargon = Ransomware

Locky

We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)
3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

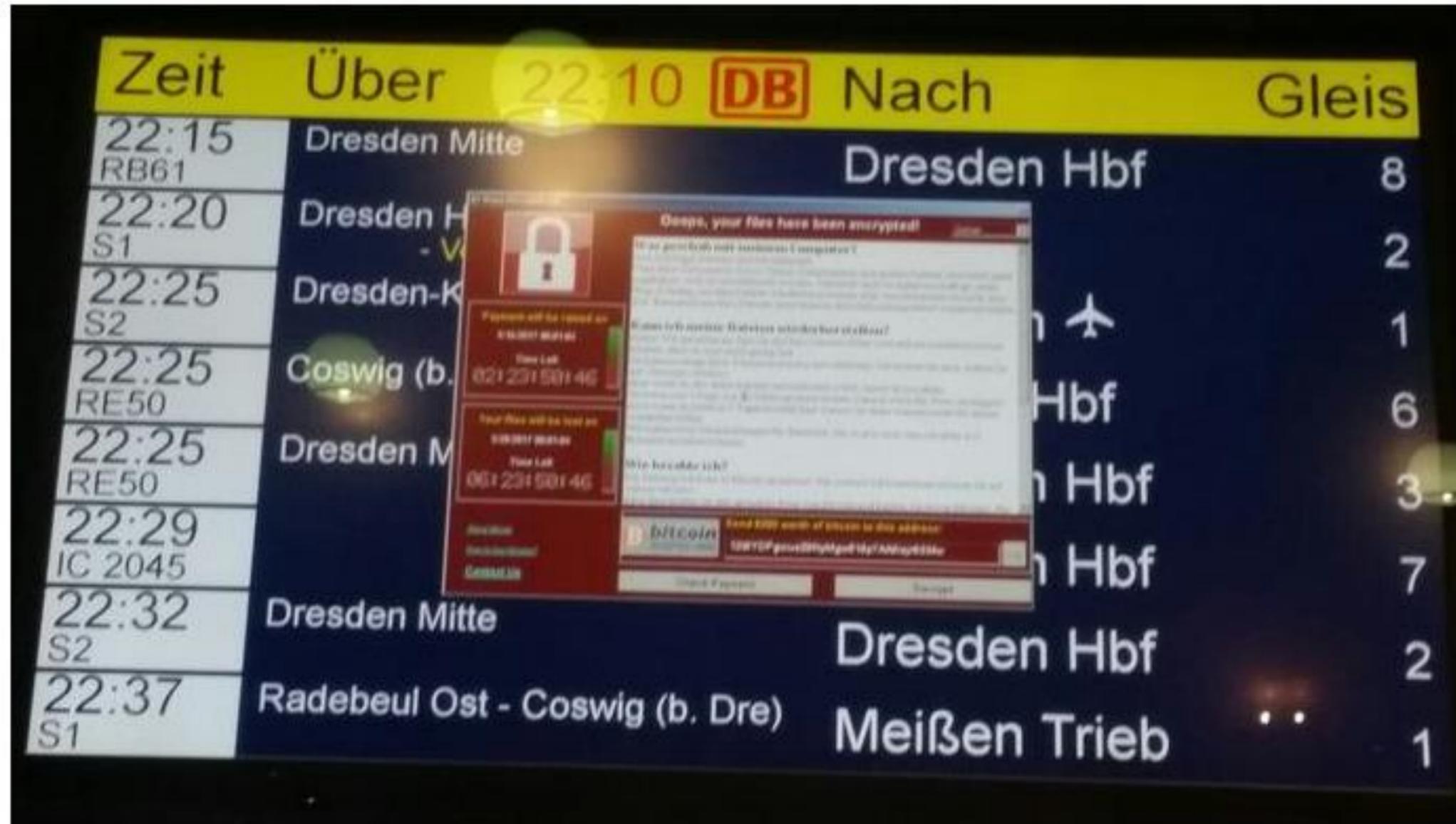
- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - Recommended for fast, simple service.

WannaCry

Ransomware WannaCry befällt Rechner der Deutschen Bahn

13.05.2017 11:22 Uhr - Volker Briegleb

vorlesen



(Bild: Martin Wiesner)

Petya

WHILE IT IS SIMILAR TO OTHER RANSOMWARE, THERE ARE A FEW ELEMENTS THAT MAKE PETYA UNIQUE:



PETYA USES THE "BLUE SCREEN OF DEATH."



PETYA HAS THE ABILITY TO MODIFY, OVERWRITE OR WIPE FILES.



PETYA LEVERAGES THE ETERNALBLUE VULNERABILITY WITHIN WINDOWS.

https://pictures.brafton.com/x_0_0_0_14138462_800.jpg

Snowden -> ShadowBrokers -> WannaCry & Co.

```
bglidr1-a-fixed.sancharnet.in__61.1.128.17 mail.issas.ac.cn__159.226.121.1 orange.npix.net__211.43.194.48
bglipp1-a-fixed.sancharnet.in__61.1.128.71 mail.pmo.ac.cn__159.226.71.3 orion.platino.gov.ve__161.196.215.67
bj02.cww.com__202.84.16.34 mailscan3.cau.ctm.net__202.175.36.180 outweb.nudt.edu.cn__202.197.0.185
butt-head.mos.ru__10.30.1.130 mails.cneic.com.cn__218.247.159.113 pdns.nudt.edu.cn__202.197.0.180
dcproxy1.thrunet.com__210.117.65.44 mail.siom.ac.cn__210.72.9.2 petra.nic.gov.jo__193.188.71.4
dmn2.bjpeu.edu.cn__202.204.193.1 mailsrv02.macau.ctm.net__202.175.3.120 pop.net21pk.com__203.135.45.66
dns2.net1.it__213.140.195.7 mailsvra.macau.ctm.net__202.175.3.119 postbox.mos.ru__10.30.10.32
doors.co.kr__211.43.193.9 mail.tropmet.res.in__203.199.143.2 post.netchina.com.cn__202.94.1.48
enterprise.telesat.com.co__66.128.32.67 mail.tsinghua.edu.cn__166.111.8.17 public2.zz.ha.cn__218.29.0.200
eol1.egyptonline.com__206.48.31.2 mail.zzu.edu.cn__222.22.32.88 rayo.pereira.multi.net.co__206.49.164.2
fw433.npic.ac.cn__168.160.71.3 mbi3.kuicr.kyoto-u.ac.jp__133.103.101.21 sea.net.edu.cn__202.112.5.66
gambro3.cs.tl__243.154.62 mcd-su-2.mos.ru__10.34.100.2 sedesol.sedesol.gob.mx__148.233.6.164
gate.techno__17.9.148.61 netcoc5cn.clarent.com__213.132.50.10 segob.gob.mx__200.38.166.2
hakuba.ja__3 mipsa.ciae.ac.cn__202.38.8.1 sky.kies.co.kr__203.236.114.1
imms1.ma__54 mn.mn.co.cu__216.72.24.114 smmu-ipv6.smmu.edu.cn__202.121.224.5
indy.fj__132 most.cob.net.ba__195.222.48.5 smtp.2911.net__218.245.255.5
jur.unn__132 nbi.kmulti.pk__202.141.224.4 smtp.mcau.ctm.net__202.175.36.220
kacstse__43.13 ntp2.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
known.c__43.13 ntp3.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
kserv.k__43.13 ntp4.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
laleh.it__43.13 ntp5.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
laleh.itro__43.13 ntp6.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
m0-s.san.ru__43.13 ntp7.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
mail1.371.net__43.13 ntp8.mtpr.mn__210.11.210.3 smtp.nu.ctm.net__202.175.36.220
mail.bangla.net__203.188.252.3 n02.unternehmen.com__62.116.144.147 sps01.office.ctm.net__202.175.4.38
mail.edi.edu.cn__218.104.71.61 nd11mx1-a-fixed.sancharnet.in__61.0.0.46 sunhe.jinr.ru__159.93.18.100
mailgate.sbell.com.cn__202.96.203.173 ndl1mc1-a-fixed.sancharnet.in__61.0.0.46 sussl.cressoft.com.pk__202.125.140.194
mail-gw.jbic.go.jp__210.155.61.54 ndl1mx1-a-fixed.sancharnet.in__61.0.0.46 tx.micro.net.pk__203.135.2.194
mailgw.thtf.com.cn__218.107.133.12 ndlipp1-a-fixed.sancharnet.in__61.0.0.71 ultra2.tsinghua.edu.cn__166.111.120.10
mail.hallyn.ac.kr__210.115.225.25 no1.unternehmen.com__62.116.144.150 unknown.counsellor.gov.cn__61.151.243.13
mail.hangzhouit.gov.cn__202.107.197.199 no3.unternehmen.org__62.116.144.190 unk.vver.kiae.rr__144.206.175.2
mailhub.mnaffet.gov.rw__62.56.174.152 ns1.2911.net__202.99.41.9 voyager1.telesat.com.co__66.128.32.68
mail.hz.zh.cn__202.101.172.6 ns1.multi.net.pk__202.141.224.34 web-ccfr.tsinghua.edu.cn__166.111.96.91
mail.imamu.edu.sa__212.138.48.8 ns2.rosprint.ru__194.84.23.125 webnetra.entelnet.bo__166.114.10.28
ws.xjb.ac.cn__159.226.135.12
www21.counsellor.gov.cn__130.34.115.132
www21.counsellor.gov.cn__61.151.243.13
www.cacmail.com__195.68.99.20
```



NSA's Target List Leaked!

Wurm Funktionalität



Infektion



Lokal



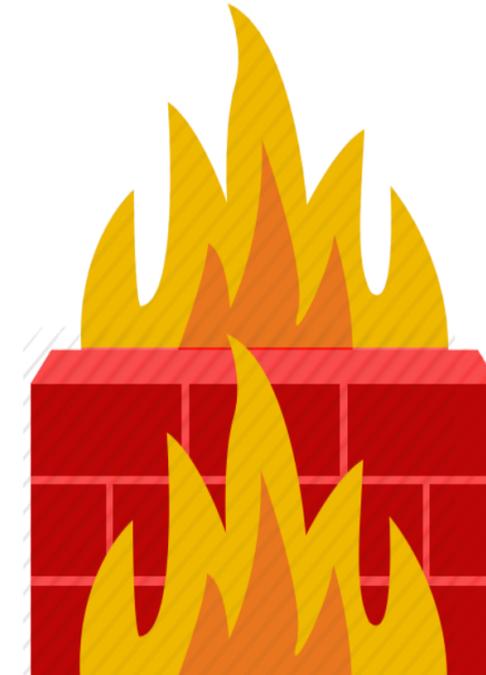
Firmennetz





Schlussfolgerung

Wie können Sie sich schützen?



Gesunder Menschenverstand



Kopf einschalten

Habe ich wirklich einen Verwandten in Nigeria?

Habe ich wirklich im Lotto gewonnen?

Meine Bank würde niemals eine Sicherheitsfrage per Mail stellen!

Kritisch sein bei Mail-Rechnungen mit Word Anhang

Nicht alles miteinander - kein Gmail während E-Banking



**falls doch, nutzen Sie
Smart Browsing**

Empfehlungen



Automatisierte Updates



Unterschiedliche
Passworte



Backup Einrichten mit Windows

Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

i File History doesn't recognize this drive.
[Select another drive](#)

File History is on

Copy files from: Libraries, Desktop, Contacts, and Favorites

Copy files to:



Win8ButBackup (D:)
Unknown error

Files last copied on 16.02.2016 17:24.

[Run now](#)

Turn off

Lassen Sie die USB Disk
nicht permanent am PC
eingesteckt!

Backup Einrichten unter OSX



Time Machine

Time Machine

OFF ON

E1OSXBackup
224 GB of 2 TB available
Oldest backup: 16 April 2015
Latest backup: 11 February 2016
Next backup: When disk is connected

Select Disk...

Time Machine keeps:

- Local snapshots as space permits
- Hourly backups for the past 24 hours
- Daily backups for the past month
- Weekly backups for all previous months

The oldest backups are deleted when your disk becomes full.

Show Time Machine in menu bar Options... ?

Lassen Sie die USB Disk nicht permanent am PC eingesteckt!

Überprüfen Sie verdächtige Dateien mit VirusTotal



SHA256: 931e8aa2fb6341a84b74698984840379e71eb5f3e56e38340f34141897396806

File name: Sigcheck.zip

Detection ratio: 0 / 54

Analysis date: 2016-03-02 18:13:03 UTC (18 hours, 43 minutes ago)



www.virustotal.com

- Analysis
- File detail
- Additional information
- Comments 0
- Votes

Antivirus	Result	Update
ALYac	✓	20160302
AVG	✓	20160302
AVware	✓	20160302
Ad-Aware	✓	20160302
AegisLab	✓	20160302
Agnitum	✓	20160301
AhnLab-V3	✓	20160302
Antiy-AVL	✓	20160302



124ba8b

Anti-Viren Produkt



Es kommt weniger auf das Produkt an, sondern auf die Konfiguration und ob Sie es täglich updaten!!



Was können Sie als Firma tun?



Bottom line is :

- Patch your systems. (Especially MS17-010) — Keep in mind that WannaCry **itself** is still active — *our killswitch prevented 80K infections in the past 7 days alone !*
- Have a backup strategy. This is your best strategy against the rising threats of ransomware.
- Have a worse case scenario plan. Companies need incident response and recovery plans.

The image shows a composite of two screenshots. The top screenshot is a Windows Update window. It displays the title 'Windows Update' and a red warning message: '*Some settings are hidden or managed by your organization.' Below this, the 'Update status' section shows a progress bar with a refresh icon and the text 'Checking for updates...'. A link for 'Update history' is visible at the bottom. To the right of this screenshot is a 3.5-inch floppy disk with a white label that has 'INDEX' at the top and 'Backup' written in cursive in the center.

The bottom screenshot is a website for 'CLEONDRIS'. It features a dark blue navigation bar with 'Contact us' and 'Sign in' links. Below the navigation bar is the company name 'CLEONDRIS' in large, bold, black letters. Underneath the name is a horizontal menu with links for 'SNAPGUARD', 'DATA MANAGER', 'BUY', 'DOWNLOAD', 'SUPPORT', and 'COMPANY'. The main content area has a blurred background with the text 'STAY RELAXED USING SNAPGUARD®'. At the bottom of this area, there is a 'NetApp' logo with 'Alliance Partner' written below it, and a blue button that says 'TRY NOW'.



Was tun wenn es trotzdem passiert?

- Profis machen lassen (nicht selbst basteln)
- Ransomware Playbook

Windows Defender Advanced Threat Protection - Ransomware response playbook

Language: English

Download

This playbook discusses how enterprises can leverage Windows Defender ATP to detect, investigate, and mitigate ransomware threats in their networks.

+ Details

+ System Requirements

+ Install Instructions

<https://www.microsoft.com/en-us/download/details.aspx?id=55090>

<https://www.demisto.com/playbook-for-handling-ransomware-infections/>

- 1) Verstehen Ransomware Angriff
- 2) Disconnect infizierter PC/Server vom Netzwerk, Wifi, LAN
- 3) Disconnect persönliche USB Disks von Laptop, PC
- 4) Ursache finden infizierter PC
- 5) Gibt es andere Geräte mit den gleichen Symptomen?
- 6) Stoppen der Infektion
 - * E-Mail
 - * Web Proxy
 - * USB Stick, CDROM, Handy
- 7) Erst mit Wiederherstellung beginnen, wenn geringes Risiko für Re-Infektion



Worin liegt das
Business Modell der
Angreifer bei Locky,
WannaCry und Petya?



Business Modell Erpressung

Vielen Dank für Ihre Aufmerksamkeit



Ivan Bütler

Gründer, CEO von Compass Security, Lehrbeauftragter HSR, Experte SATW



ivan.buetler@compass-security.com



ICT Security Expert ED



***ICT Berufsbildung
Formation professionnelle
Formazione professionale***