Ransomware

proIT
Verband der IT-Profis in Liechtenstein

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**

https://cybersecurity.li/

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

Motive für Hacker Attacken?

GAME HACK

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					★	jurnalarkeologipapua.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			★	cmfigueira.pr.gov.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

Home News Events Archive Archive Onhold Notify Stats Register Login search...

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

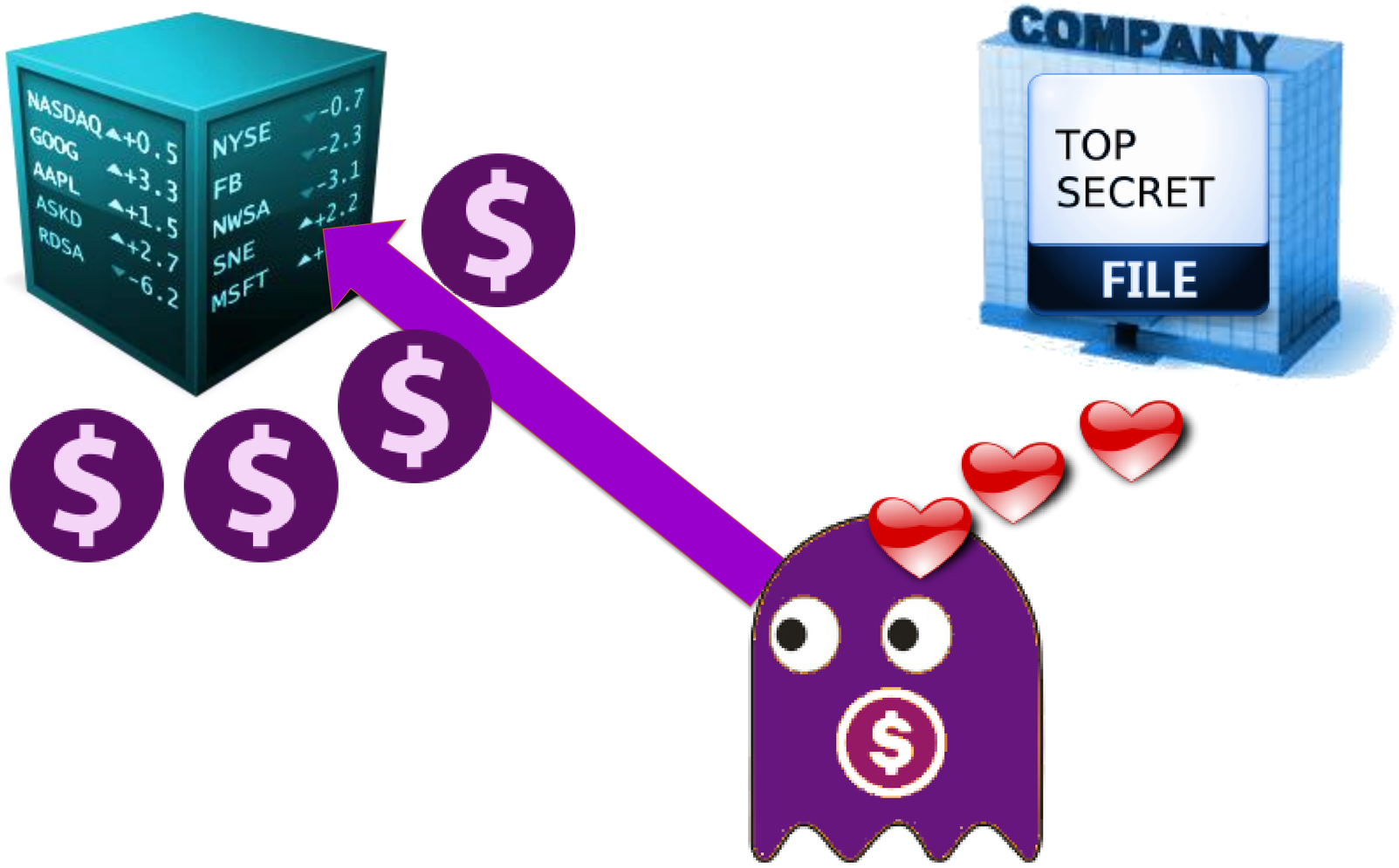
20.06.17, 11:38 Uhr

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

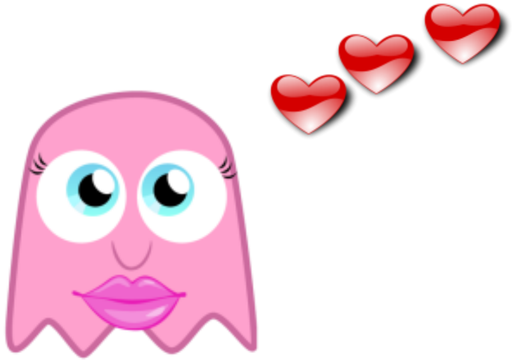
1) Veräusserung der gestohlenen Güter

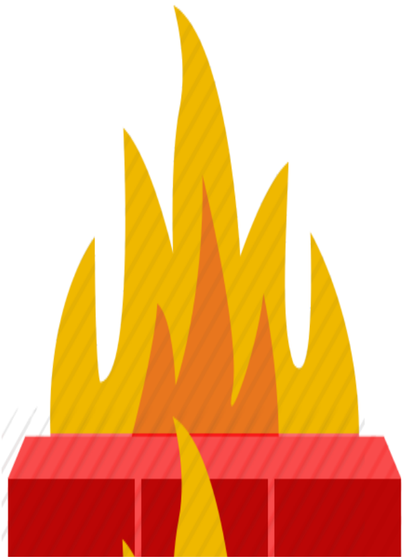
2) Insider Business

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

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

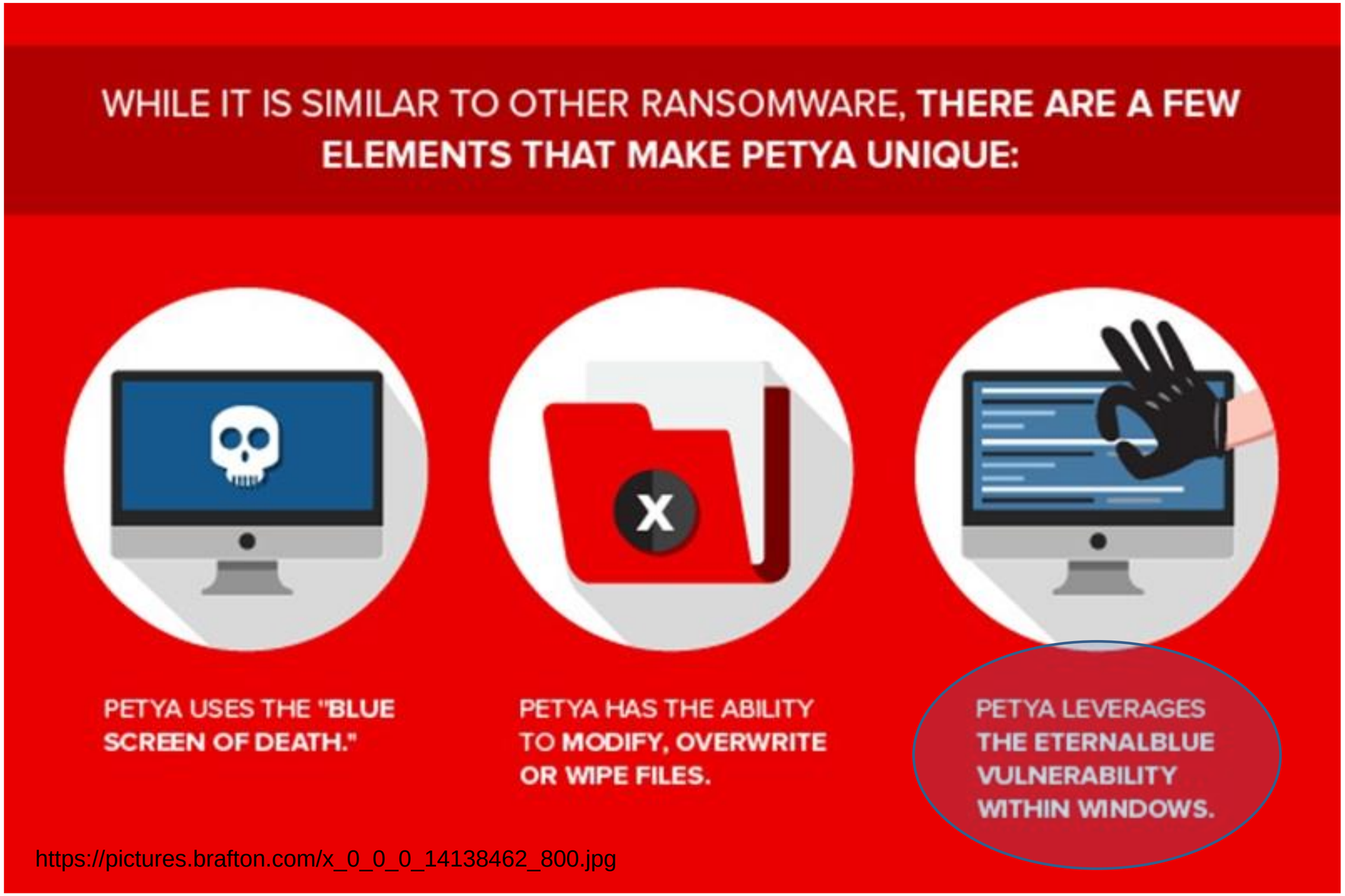
Ransomware WannaCry befällt Rechner der Deutschen Bahn

13.05.2017 11:22 Uhr – Volker Briegleb

vorlesen

(Bild: Martin Wiesner)

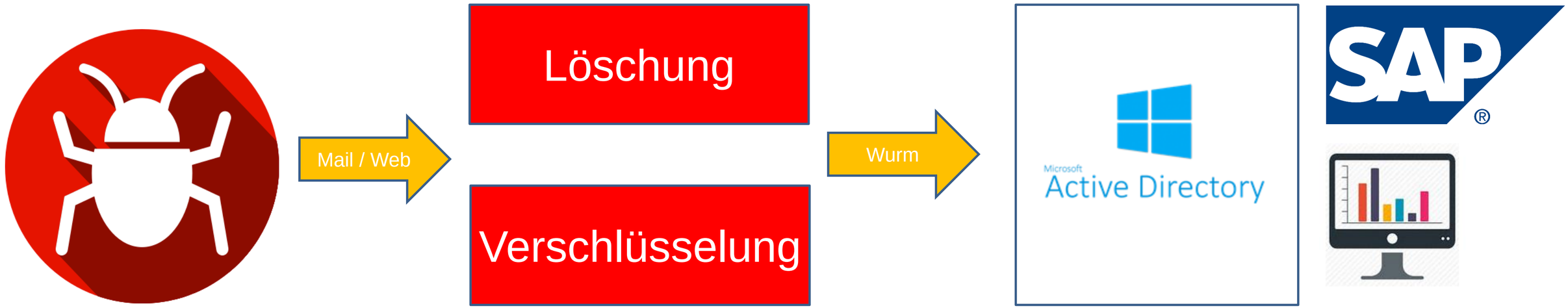
Petya



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

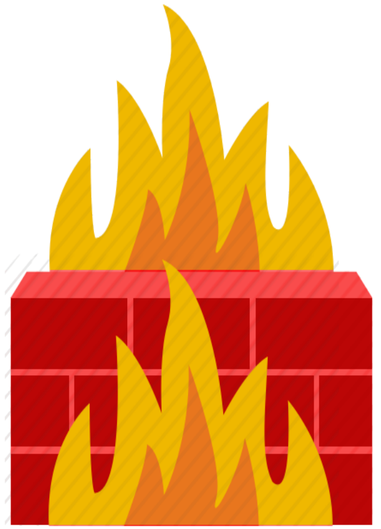
Snowden -> ShadowBrokers -> WannaCry & Co.

Wurm Funktionalität



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.

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:

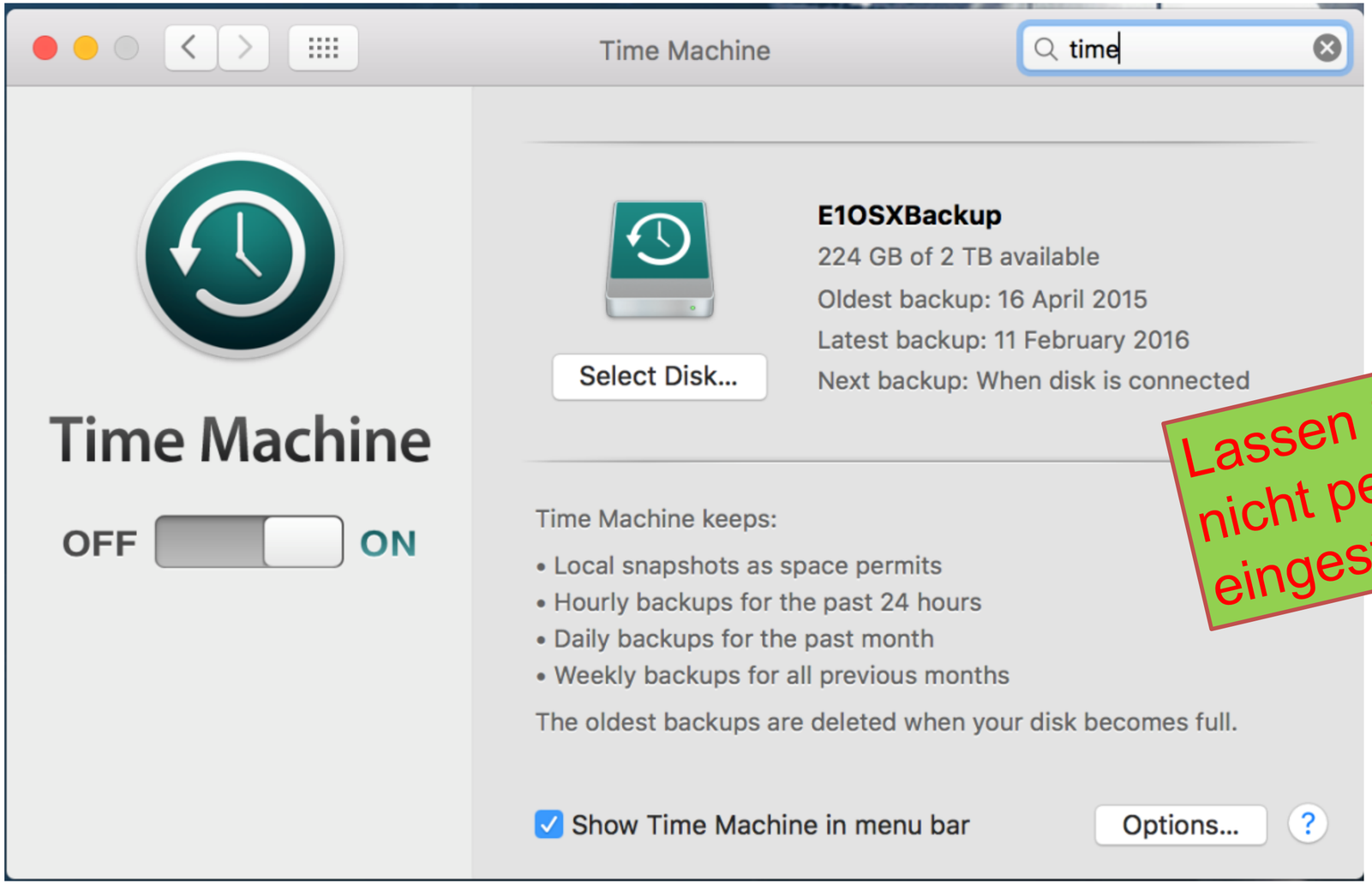
Win8ButBackup (D:)
Unknown error

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



Lassen Sie die USB Disk nicht permanent am PC eingesteckt!

Überprüfen Sie verdächtige Dateien mit VirusTotal

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

l24ba8b

Anti-Viren Produkt

bitdefender

KASPERSKY ANTI-VIRUS

Webroot AntiSpyware CORPORATE EDITION with AntiVirus

F-SECURE

AVG Anti-Virus System

McAf Proven

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

Panda Software

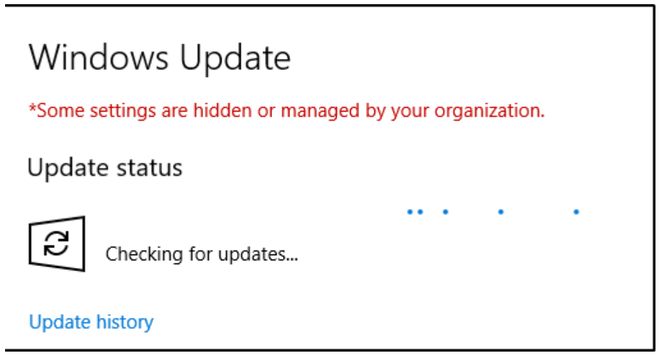
symantec.

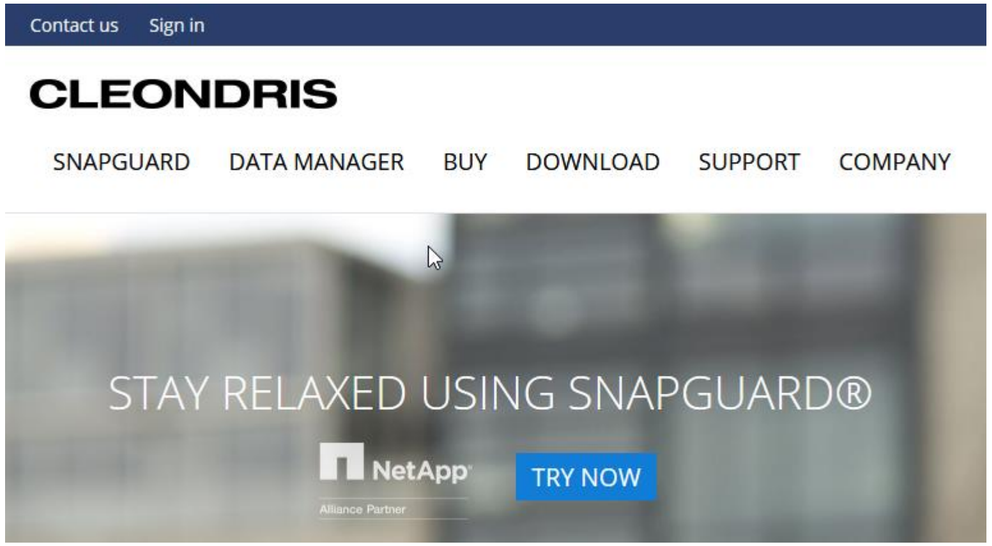
TREND MICRO

Was können Sie als Firma tun?

Bottom line is :

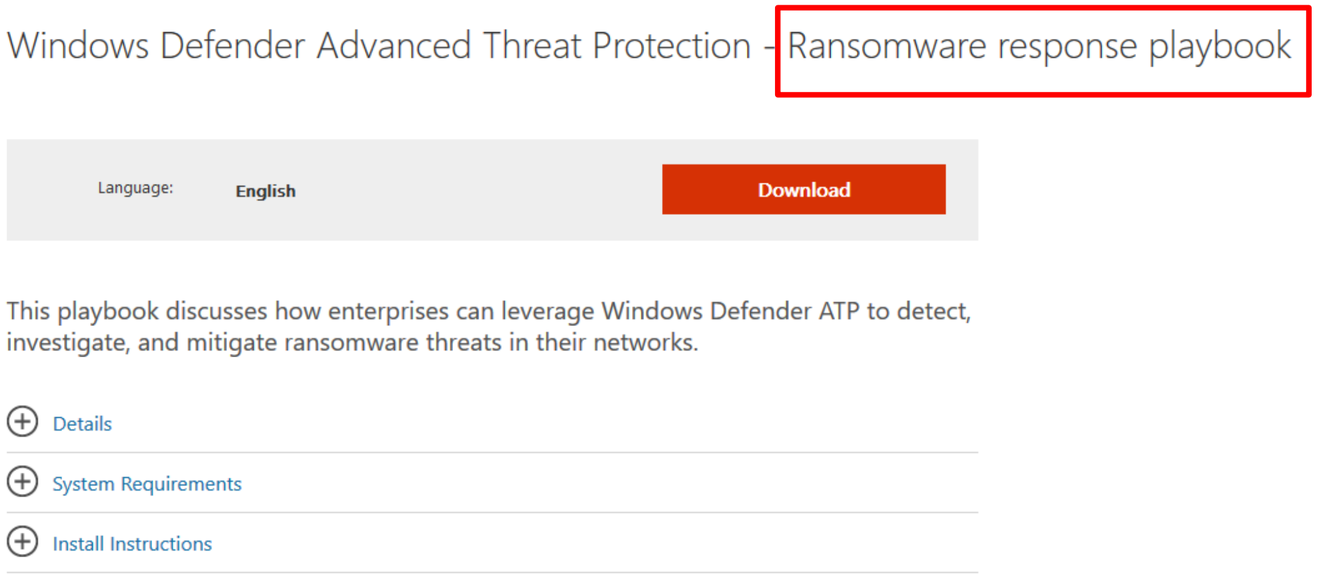
- Patch your systems. (Especially MS17–010) — Keep in mind that WannaCry **itself** is still active — *our killswitch prevented 80K infections in the past 7 days alone !*
- Have a backup strategy. This is your best strategy against the rising threats of ransomware.
- Have a worse case scenario plan.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





Was tun wenn es trotzdem passiert?

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



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

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

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

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

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

satw it's all about technology

EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

ICT Security Expert ED

ICT Berufsbildung
Formation professionnelle
Formazione professionale