



CAAS – CYBER-CRIME AS A SERVICE

MAGENTA SECURITY KONFERENZ
08. MÄRZ 2018
THOMAS KÖNIGSHOFEN

AGENDA

- CaaS: Definitionen und Abgrenzungen
- Bedrohungspotenzial
- Beschaffung der Tools
- Typische Angebote und Geschäftsmodelle
- Gegenmaßnahmen



Quelle: CaaS analysis report. Y. Zheng A. Chaudhry



ERLEBEN, WAS VERBINDET.

CAAS – DEFINITIONEN UND ABGRENZUNGEN

SaaS → Software as a Service

PaaS → Platform as a Service

CaaS → Crime as a Service; Cyber-Crime as a Service

CRIME AS A SERVICE:

Das Dienstleistungsangebot an Dritte, gegen Bezahlung Straftaten zu begehen.

Cyber-Crime as a Service:

Das Dienstleistungsangebot an Dritte, gegen Bezahlung computergestützte Straftaten zu begehen oder dabei zu unterstützen

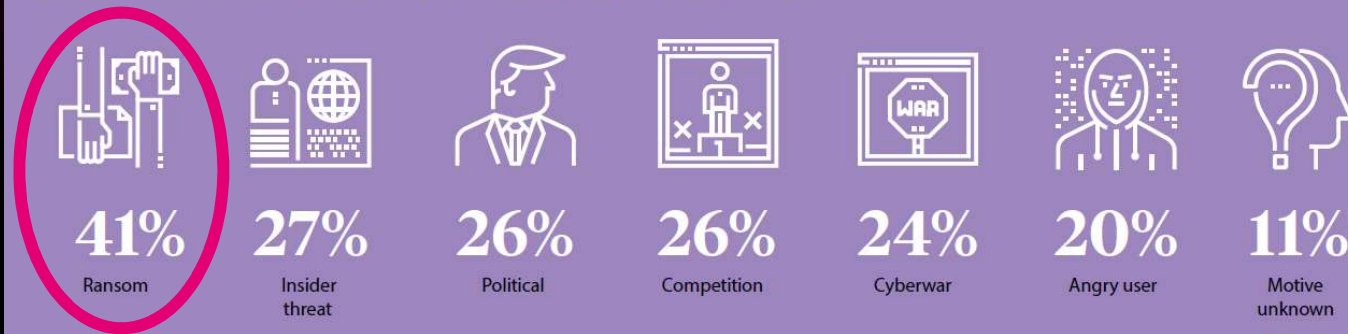


CYBERCRIME – DAS BEDROHUNGSPOTENZIAL

WHY HACKERS HACK

MOTIVES BEHIND CYBERATTACKS

GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK



Radware 2017



ERLEBEN, WAS VERBINDET.

CYBERCRIME – DAS BEDROHUNGSPOTENZIAL

Fast 55 Milliarden Euro Schaden pro Jahr

bitkom

Schäden in Deutschland in Milliarden Euro (Basis: Selbsteinschätzung)

	Schadenssummen in Mrd. Euro
Kosten für Ermittlungen und Ersatzmaßnahmen	21,1
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	15,4
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	15,4
Kosten für Rechtsstreitigkeiten	11,0
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	10,5
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	6,9
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	6,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,3
Sonstige Schäden	4,5
Gesamtschaden innerhalb der letzten 2 Jahre	109,6



ERLEBEN, WAS VERBINDET.

CYBERCRIME AS A SERVICE- BESCHAFFUNG

Surface Web

Darknet

What is the Tor Browser?

The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

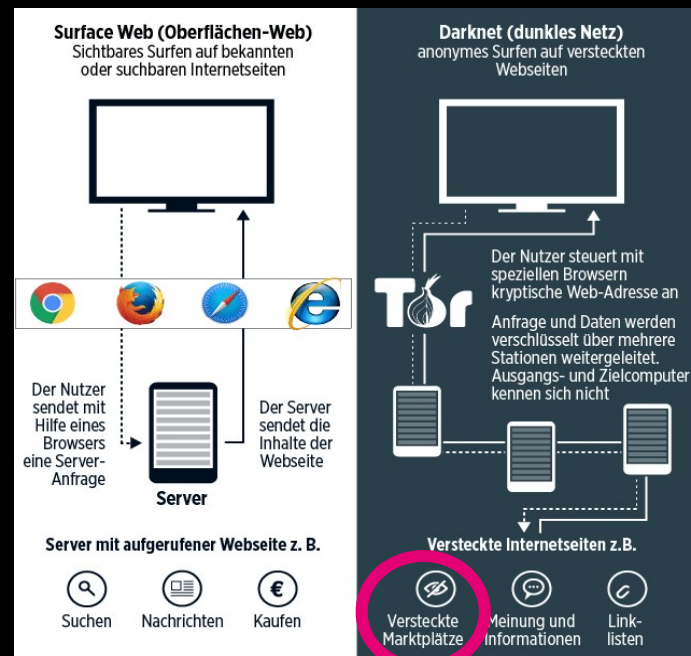
The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable).

DOWNLOAD
Tor Browser

Installation Instructions
Windows • Mac OS X • Linux

Do you like what we do? Please consider making a donation >

Quelle: freepik.com



Quelle: info.BILD.de // Bundesregierung, Kompetenzzentrum öffentliche IT, dpa



ERLEBEN, WAS VERBINDET.

CYBERCRIME AS A SERVICE- BESCHAFFUNG

Bestsellers

- Walther P22 \$752.65 [Add to Cart](#)
- Glock 17 & Gemtech Tundra \$2,223.45 \$1,599.99 [Add to Cart](#)
- Beretta PX4 Storm Type F \$1,223.90 [Add to Cart](#)
- 9x19mm Parabellum \$0.30 [Add to Cart](#)
- Glock 26 Gen4 \$1,027.94
- Glock 17 Gen4 \$1,027.94
- CIA Model PAP \$1,956.64 \$1,401.56
- Glock 32 Gen4 \$1,027.94

Wall' Market Home **User-CR** FAQ Forum Support Refrally Log Out

Search for...

Featured Listings

- Drugs [20]
- Counterfeits [2]
- Jewelry & Gold [2]
- Carding Ware [2]
- Services [2]
- Software & Malware [2]
- Security & Hosting [2]
- Fraud [2]
- Digital goods [2]
- Guides & Tutorials [2]

Bubba Kush BC Bud AAAA+
From \$4.50/Gram (-0.0046 BTC)
Ships From: CA
Ships Worldwide
First

HQ FullInfo DE Random CC Classic
Dripark [Level 1]
From 7,000/Piece (-0.0076 BTC)

HQ PAYPALS DE FULLINFO UA+IP-2h REPLACE!! 100 FOR 50€
Alice133 [Level 1]
From 6,450/Piece (-0.0055 BTC)

Active Filters Clear

Active vendor

Categories

- Drugs **12149**
- Benzos 716
- Cannabis 3064
- Dissociatives 218
- Ecstasy 2177
- Opioids 723
- Prescription 1065
- Psychedelics 1125

Drugs

Filter Popularity - This month Sort

1oz (28g) "AA" Grade - Blue Dream - Service en Francais disponible BTC 0.4983 [Buy It Now](#)

TopShell420 (99.9%) **Level 6 (1077)**

FAVORITE

"OCT 27" 2 grams of MANGO (much higher quality than PINEAPPLE) AAA+++ BTC 0.0553 [Buy It Now](#)

Mister_Mittens (99.8%) **Level 6 (801)**

Products

Name	Vendor	Price	Rating
NETFLIX UNLIMITED ACCOUNT	ProfessorDark Level 1 Trusted	From \$1.00	★★★★★ (4.2)
BRAZZERS UNLIMITED ACCOUNT	ProfessorDark Level 1 Trusted	From \$1.00	★★★★★ (4.0)
NSA HACKING -FORENSIC TOOLKIT + BONUS 11 FBI TOOLS	SoftKingUS Level 1 Trusted	From \$3.99	★★★★★ (0.0)
Penis Enlargement Exercises	ProfessorDark Level 1 Trusted	From \$0.99	★★★★★ (0.0)
eBooks pack of tutorial on CC & PP to BTC, Carding, PGP security	SafeServSmith Level 1	From \$0.88	★★★★★ (0.0)
49 GENERATORS Premium Access Accounts	darkmarket Level 1 Trusted	From \$29.90	★★★★★ (5.0)
Windows Product Key	ProfessorDark Level 1 Trusted	From \$0.99	★★★★★ (3.5)
UBER FAKE DRIVER HACK! MAKE OVER 2000+ USD Month	Twithe Level 1	From \$1.50	★★★★★ (0.0)



ERLEBEN, WAS VERBINDET.

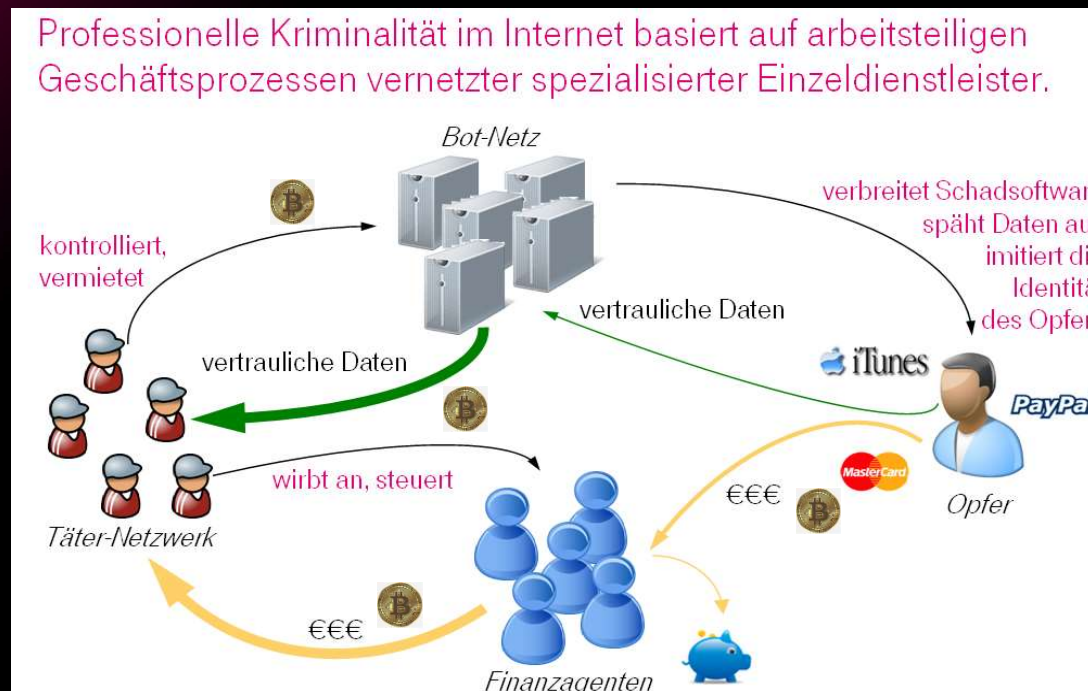
CYBERCRIME AS A SERVICE- TYPISCHE ANGEBOTE

- Ransomware (-toolkits)
- Bereitstellung von Botnetzen für verschiedene kriminelle Aktivitäten
- DDoS-Attacken
- Malware-Herstellung und -Verteilung
- Datendiebstahl
- Verkauf/Angebot sensibler Daten, z. B. Zugangs- oder Zahlungsdaten
- Vermittlung von Finanz- oder Warenagenten
- Kommunikationsplattformen zum Austausch von kriminellm Know-how, wie beispielsweise Foren
- „Infection on Demand“ (Verteilung von Schadsoftware auf Anforderung/Abruf)
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität
- Test-Portale zum Testen der Schadsoftware auf Detektierbarkeit durch Sicherheitsprodukte
- „Dropzones“ zum Ablegen illegal erlangter Informationen bzw. Waren



CAAS – TYPISCHE GESCHÄFTSMODELLE

Professionelle Kriminalität im Internet basiert auf arbeitsteiligen Geschäftsprozessen vernetzter spezialisierter Einzeldienstleister.



ERLEBEN, WAS VERBINDET.

CAAS – ZU ERWARTENDE TRENDS

Einzeltäter spezialisieren sich
Täter schließen sich zu Netzwerken zusammen
Täter-Netzwerke bekommen Strukturen der OK
Klassische OK bedient sich Täter-Netzwerken
Klassische OK übernimmt die Täter-Netzwerke
„Geschäftsausdehnung“ in allen Bereichen



**DIE GEFAHR
NIMMT
TENDENZIELL
ZU!**



ERLEBEN, WAS VERBINDET.

CAAS – GEGENMASSNAHMEN

INTEGRIERTES SICHERHEITSMANAGEMENT

- Awareness
- Präventionsmaßnahmen, z.B. Honeypots
- Detektionsmaßnahmen, z.B. Anomalie-Programme
- ...

INFORMATIONEN- UND ERFAHRUNGSAUSTAUSCH

- mit Betroffenen (Opfer-Netzwerke)
- mit Sicherheits-Experten (Experten-Netzwerke)
- mit Sicherheitsbehörden (Modi Operandi, Maßnahmen der Strafverfolgung)
- ...



DISKUSSION



**MAGENTA
SECURITY**



VIELEN DANK!



ERLEBEN, WAS VERBINDET.