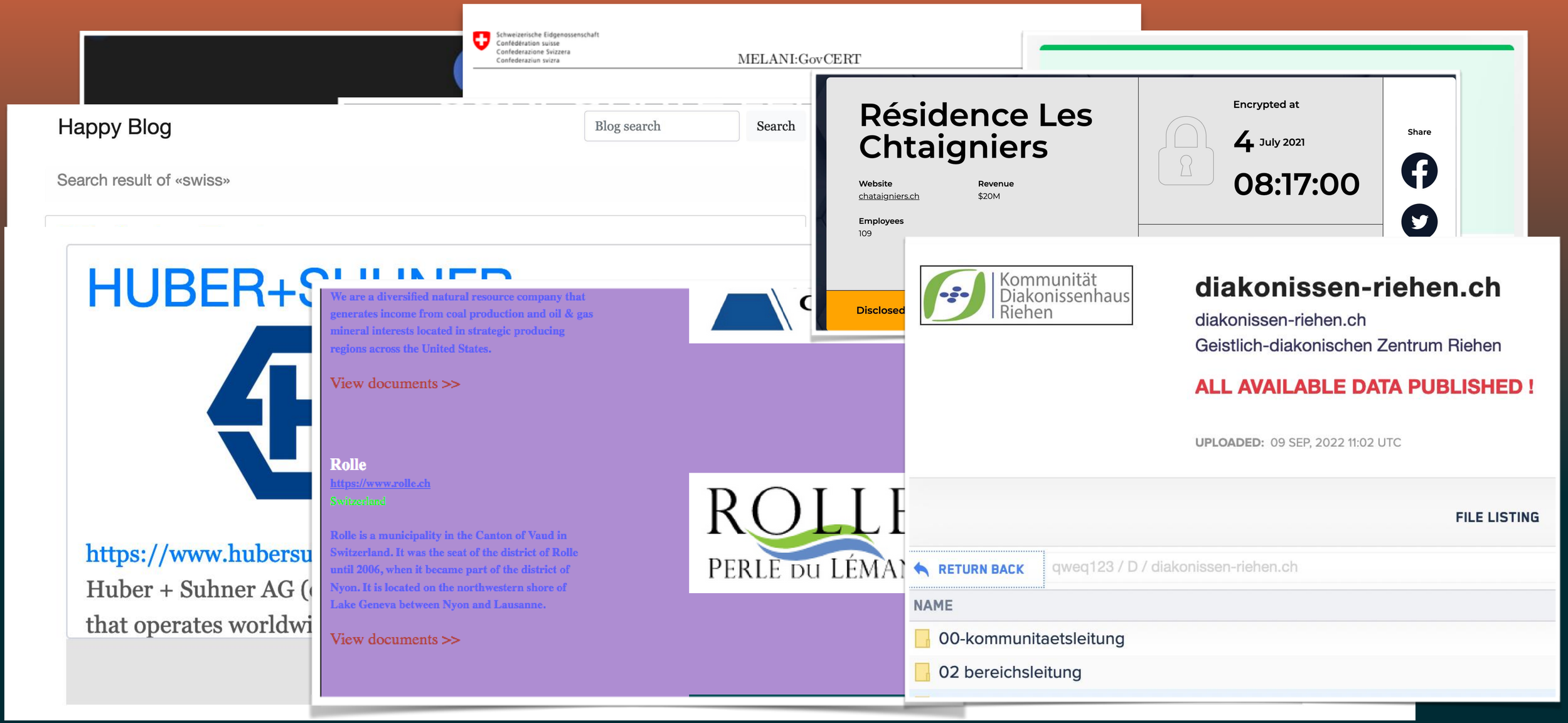
«Underground Economy»: Das sind die Täter

Otto Hostettler, Reporter/Redaktor Beobachter, Buchautor

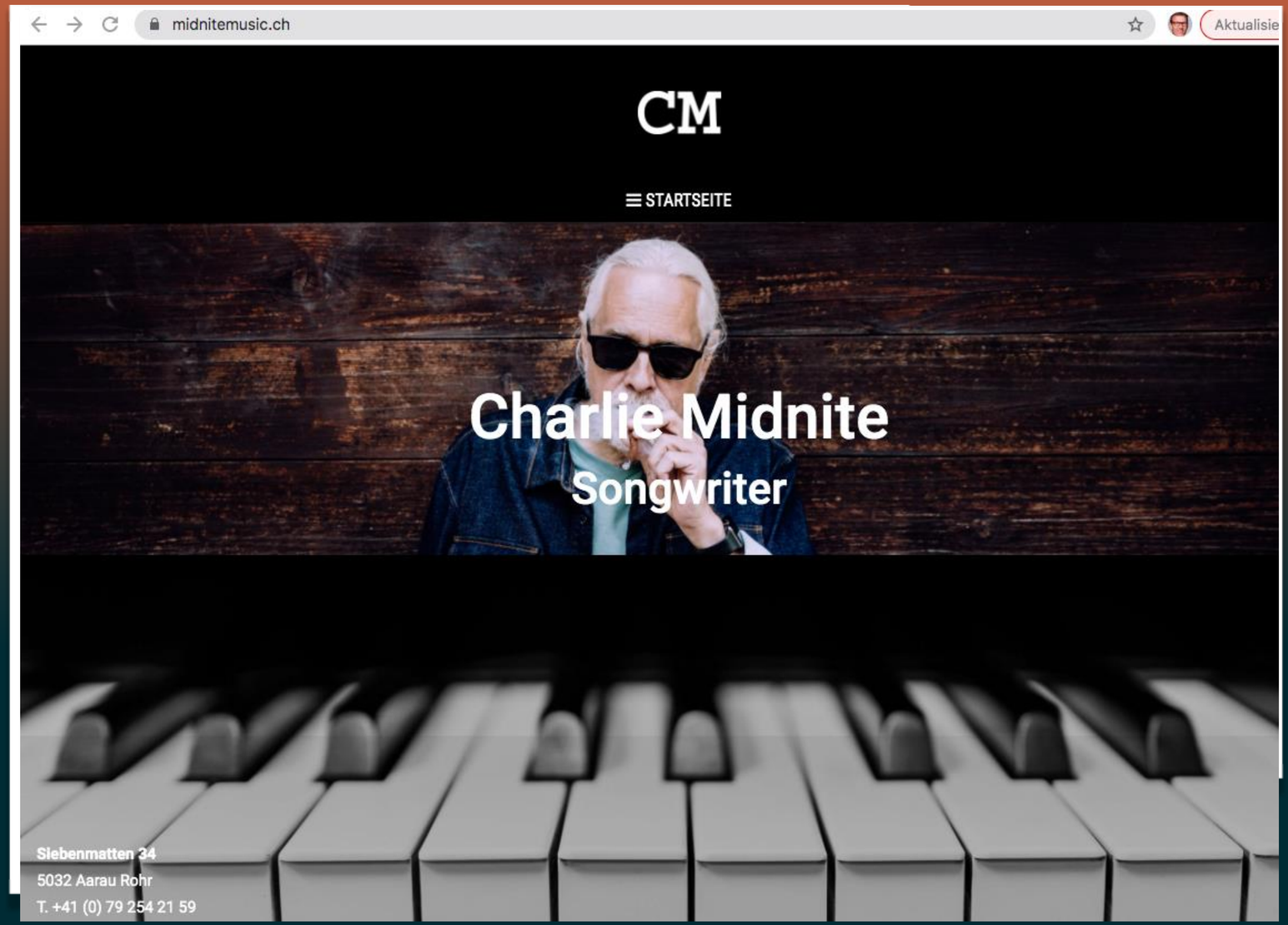
TEFO Technology Forum 2022

Cyber>funk security

Lockbit, Conti, Vice Society



wer steckt hinter Phishing?



Fancy Bear

DNR: FCTDHXS ID:0

NS International

RESERVERING
RESERVATION
InterCityExpress

CIV 1184

Sotnikov,O
04PERSONEN

VERTREK -> AANKOMST

KLASSE

17/04 07:36 UTRECHT CENTRAAL -> BASEL SBB 17/04 14:47 1

TREIN 255 ICE RIJTUIG 39 ZITPLAATS

NIET ROKEN MET MIDDENGANG 02GANG 02RAAM

04 RESERVERING ALLEEN ICM EEN GELDIG VERVOERBEWIJS

PRIJS: EUR *****0.00

8498300876 50 IR DNR:FCTDHXS Ref:

AA0C

Den Haag 130418 11:37 CACASH 1/1

Passagierslijst:

Naam	Voornaam
Sotnikov	O
Minin	A
Serebriakov	E
Morenets	A

Train tickets to Switzerland

- Departure from Utrecht for Bern via Basel
- Planned date: 17 April 2018

wir7eaA0azaAhWTy
????????? ??????
????????? ??????
CW_Structure.pdf
wio7-7wxazaAhVsE
ATORY,0,LINK,,"d
SPIEZ LABORATORY
SPIEZ LABORATORY
emical-weapons-t
hemical-weapons-
hemical-weapon
SPIEZ LABORATORY

4-2018 07:03:01

4-2018 07:03:01

4-2018 07:03:01

4-2018 07:03:07

4-2018 07:03:14

4-2018 07:03:14

Unclassified / For Official Use Only

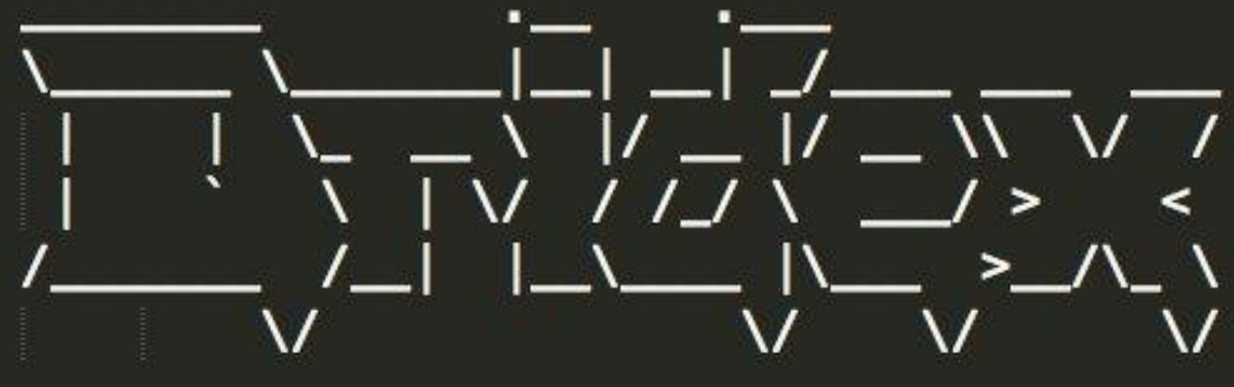
Unclassified / For Official Use Only

in Bern

Energetic Bear, Dragonfly etc

Beispiel Dridex - Evil Corp

03-29-2018: #Dridex banking #malware botnet ID “23005”



First-layer blocklist:
46.105.131[.88:443
198.57.157[.216:3889
149.202.153[.251:3889
67.212.241[.131:443

Wer sind die Täter?

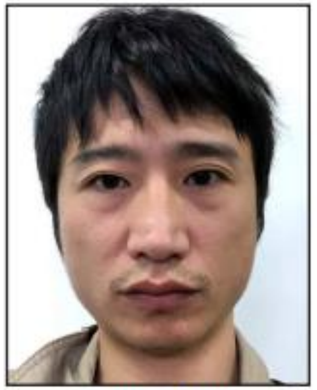
Yakubets.

China: z.B APT 41

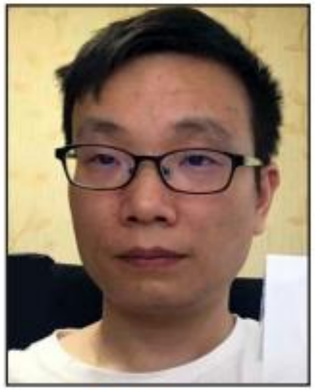
APT 41 GROUP

ZHANG Haoran

TAN Dailin



QIAN Chuan



FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

Lazarus - Nordkoreas Devisenbeschaffer

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Jin Hyok Park, Pak Jin Hek, Pak Kwang Jin	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Park is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and has reported dates of birth in 1984 and 1981.

CAUTION

Motivation der Iraner: Wissenschaft, kommerziell

IRANIAN CYBER ACTORS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

REWARD

The Rewards for Justice Program, United States Department of State, is offering a reward of up to $10 million for information on or about the activities of Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari.

CAUTION

Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari are wanted for their alleged involvement in a coordinated campaign which compromised hundreds of computer networks across the United States and abroad. Between October 2020 and August 2022, the three men allegedly gained unauthorized access to protected networks, exfiltrated data, encrypted computer systems, and extorted victims for ransom, causing damage to and disrupting operations of organizations across multiple sectors, including critical infrastructure, government agencies, and non-profit organizations.

Wiederholungstäter - Der Fall Diabl0/Farid Essebar

Ein Triumph für Hacker

CYBERCRIME. Die Bundesanwaltschaft feierte die Verhaftung von drei Phishing-Betrügern. Doch jetzt fällt ihr die Justiz in den Rücken: Die Hacker erhalten Zehntausende Franken.

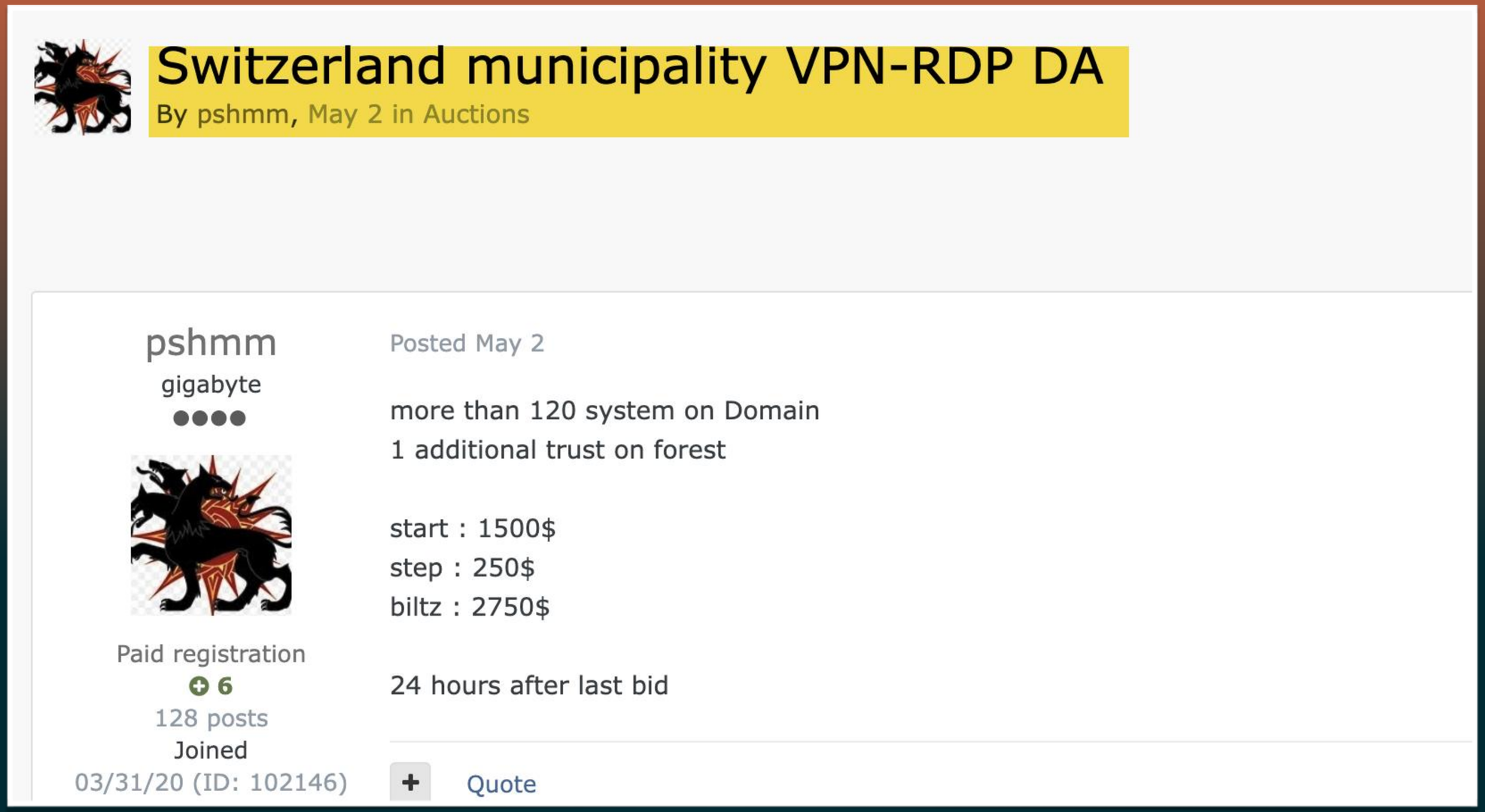
60 000 Franken von der Schweiz: Hacker Farid Essebar

Farid Essebar kann sich die Hände reiben. Die Schweiz muss dem international bekannten Hacker 62 880 Franken Genugtuung zahlen. Der 32-jährige, mehrfach verurteilte Marokkaner mit russischem Pass war Umlauf gesetzt. Essebar wurde damals zu zwei Jahren Haft verurteilt.

Zwei Monate nach Essebar konnte in Thailand ein weiterer Täter dingfest gemacht werden, der dritte Anfang 2016. Ein Erfolg für die Schweiz, auch wenn Zusicherung, dass sie wegen der Datendiebstähle nicht an ein anderes Land ausgeliefert würden.

Der Deal platzte. Der Staatsanwalt des Bundes hatte sich dabei auf die interna-

So ticken die Banden



Switzerland municipality VPN-RDP DA

By pshmm, May 2 in Auctions

pshmm

gigabyte

●●●●

Paid registration

6

128 posts

Joined

03/31/20 (ID: 102146)

Posted May 2

more than 120 system on Domain

1 additional trust on forest

start : 1500$

step : 250$

biltz : 2750$

24 hours after last bid

+ Quote

Aktuelle Entwicklung:
Es geht noch schlimmer!

Abdelkader Cornelius , Gründer & CTO Cyberfunk Security

Cyber>funk
security

Zahlen, Daten ,Fakten

Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
225	+126	+1536	+6045	460623
Groupped by				
PL	+3	+194	+749	30911
ES	+9	+146	+631	35558
RO	+3	+144	+497	32136
TR		+106	+457	23955
US	+29	+131	+385	7195
IT	+17	+92	+372	57908
PT	+1	+65	+278	29799
FR	+12	+60	+219	31238

201 Mrd €

Verursachter Schaden durch Cyberangriffe, Hacker und Internetkriminalität

+358%

Zuwachs an Cybervorfällen in den Jahren 2020-2021

Underground Economy

7 Sekunden	67% Gegenüber 2021
4560% Lockbit	291 CaaS
970 Tage	1:2KK (RAT)
1,21 Mil. Euro	BEC 3 Millionen

Aller Anfang ist einfach

Deutsch
- Darkbase
- Toolbase
- Crime
- Crimemarket
- Darkbase
- Deutschland im Deep Web [Tor]
- Free-Hack
- Hackingboard
- High - Minded
- Kuketz-Blog
- Nydus
- Szenebox
- Toolbase

Russisch
- Xaknet
- 24rc
- 4cheat
- 4pda
- Ahack
- Alligator
- Antichat
- Antiskam
- Bdf
- Bit-Team
- Blackhacker
- Bugtraq
- Codeby
- Community [Tor]
- Comunity
- Coockie
- Cyberforum
- Cybhack
- Dark-Time
- Dark2web
- Darknet.ug
- Delphicode
- Dublikat
- Exploit
- Forumteam

Albanisch
- Itshqip

Niederländisch
- Hackflag

Griechisch
- Greekhacking

Malaysisch
- Dragonforce

Rumänisch
- Rstforums

Türkisch
- Ajanlar
- Arsivh
- Cracker-Team
- Darkhack
- Deltahackerz
- Eternalteam
- Forumgrand
- Garez
- Illegalplatform
- Imhatimi
- Koswog
- Memoryhackers
- Mybb
- Siberdeyiz
- Spyhackerz
- Tahribat
- Tnctr
- Turkhacks
- Turkhackteam
- Turkichackersrulez
- Xhackerz

Arabisch
- Aljyyosh
- Almashhed
- Linuxac
- Nullnoss
- Soqor
- Sqebd
- V4-Team
- Vb4arb
- Vbspiders

Polnisch
- Devilteam
- Hack
- Haker
- Nokiahacking
- Ripz
- Tdhack

Vietnamesisch
- Ceh
- Ugworld
- Hvaonline [Archived]

Aserbaidschanisch
- 1918-Team
- Anti-Armenia

Georgisch
- Csgforum

Indonesisch
- Echo
- Indonesianbacktrack
- Xcode

Portugiesisch
- Caveiratech
- Guiadohacker
- Zwame

Ukrainisch
- Replace

Chinesisch
- 2cto
- 52pojie
- Cctry
- Cnsec
- Hackbase
- Ihonker
- Kafan
- Pediy

Persisch
- Anonymous-Team
- C-Cracking
- Easypc
- Fatehgar
- Guardiran
- Iran-Cyber
- Iransec
- Shabgard
- Tonel

Tschechisch
- Soom

Englisch
- 0day
- 0x00sec
- Addon
- Antionline
- Ascarding
- Babiato
- Bestblackhatforum
- Blackbones
- Blackhatcarding
- Blackhatprotools
- Blackhatsem
- Blackhatworld
- Blackpearl
- Bpcforum
- Cardforum
- Cardingworld
- Cardsharing
- Cardvilla
- Club2crd
- Combo-List.net
- Combo-List.top
- Combolist.top
- Crackcommunity
- Cracked
- Crackia
- Cracking
- Crackingall
- Crackingate
- Crackingboxxx
- Crackingdrift
- Crackingpass
- Crackingpro
- Crackingsoul
- Crackingstation
- Crackingx
- Crax
- Craxnet
- Crdpro

Dänisch
- Shellsec

Französisch
- Hack-Life
- Hackademics
- Instant-Hack
- Leakforum.fr
- Malekal
- N-Pn
- Omerta.la
- Root-me
- Selkis
- Veryleaks
- Zenk-Security

Spanisch
- Elhacker
- Elitehackers
- Indetectables
- Leakhispano
- Level23hacktools
- Underc0de
- Underground

Zugang

This forum is free and open to register

Register

Threads: 79,137, Posts: 377,620, Members: 202,137

Sell CC & CVV (31 Viewing)
Sell CC's & CVV only.

Dumps (6 Viewing)
Selling and cashout dumps only.

Enroll, Accounts, Shops, SSN services
Enroll (COBs, fullz). Sell & Buy Accounts: Banks, PP, MB and more. Search SSN, DOB, CR, etc..

CashOut Services & Drops for Stuff
ATM. Any cashout. Exchange, purchase, electronic currency. Drops for stuff.

Plastic & Documents
Any ID, Scans, Holograms, Skimmers, Labels for sell.

Hosting, Spam, DDoS, Call Services (1 Viewing)
Hosting, Servers, Spam, DDoS, Adult and Call Services.

Security Services
VPN, Proxy/Socks and other related services.

Other Services (2 Viewing)
All other carding services.

UNVERIFIED ADVERTISEMENT (5 Viewing)
All unverified advertisement & free trades area.

НЕПРОВЕРЕННАЯ РЕКЛАМА (8 Viewing)
Вся непроверенная реклама с форума.

Registration

User Name

Password

Please enter a password for your user account. Note that passwords are case-sensitive.

Password: Confirm Password:

Email Address

You need to verify your email to get activation on forum. Notice: protonmail don't receive mails from forum.

Email Address: Confirm Email Address:

Instant Messaging

ICQ Number Jabber ID

Image Verification

Please enter the six letters or digits that appear in the image opposite.

PX6AEj

Refresh Image

Text Verification

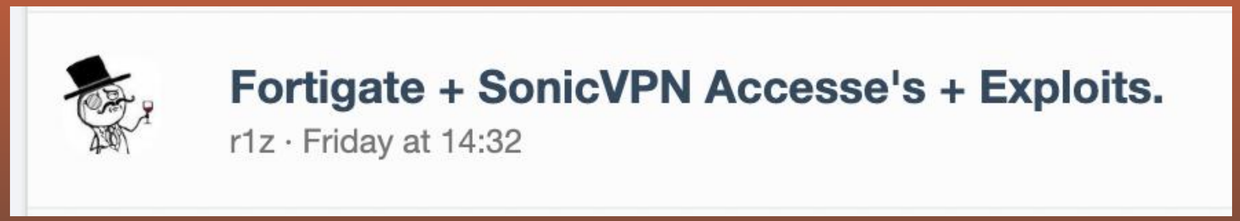
His Last name is Putin and First name is (starts with Vladi.....)? (write first name below) If u're dumb use google with "President of Russia"

Complete Registration

User Name User Name Remember Me?

Password Log in

Zugang zur Infrastruktur



r1z

Still(In)Secure

Premium

Регистрация: 19.07.2019
Сообщения: 561
Реакции: 559
Гарант сделки: 10

Пятница в 14:32

Selling access to 25 of mixed access for Fortigate VPN (**Latest Exploit**) + Sonicwall VPN.

The deal will include both exploits + how to Documentation for easy access & understanding.

Access List from US, and others..only serouse buyers, **not mofo skids !**

This is mixed access from US, Europe and other countries.. its not sale of specific target, depend in your luck) automated exploited of sonicwall + Fortigate exploits.

If you need specific revenue and country, the price will be only for 1 target between 3-5k. (this is big chance for you to get most cheap access ever!)

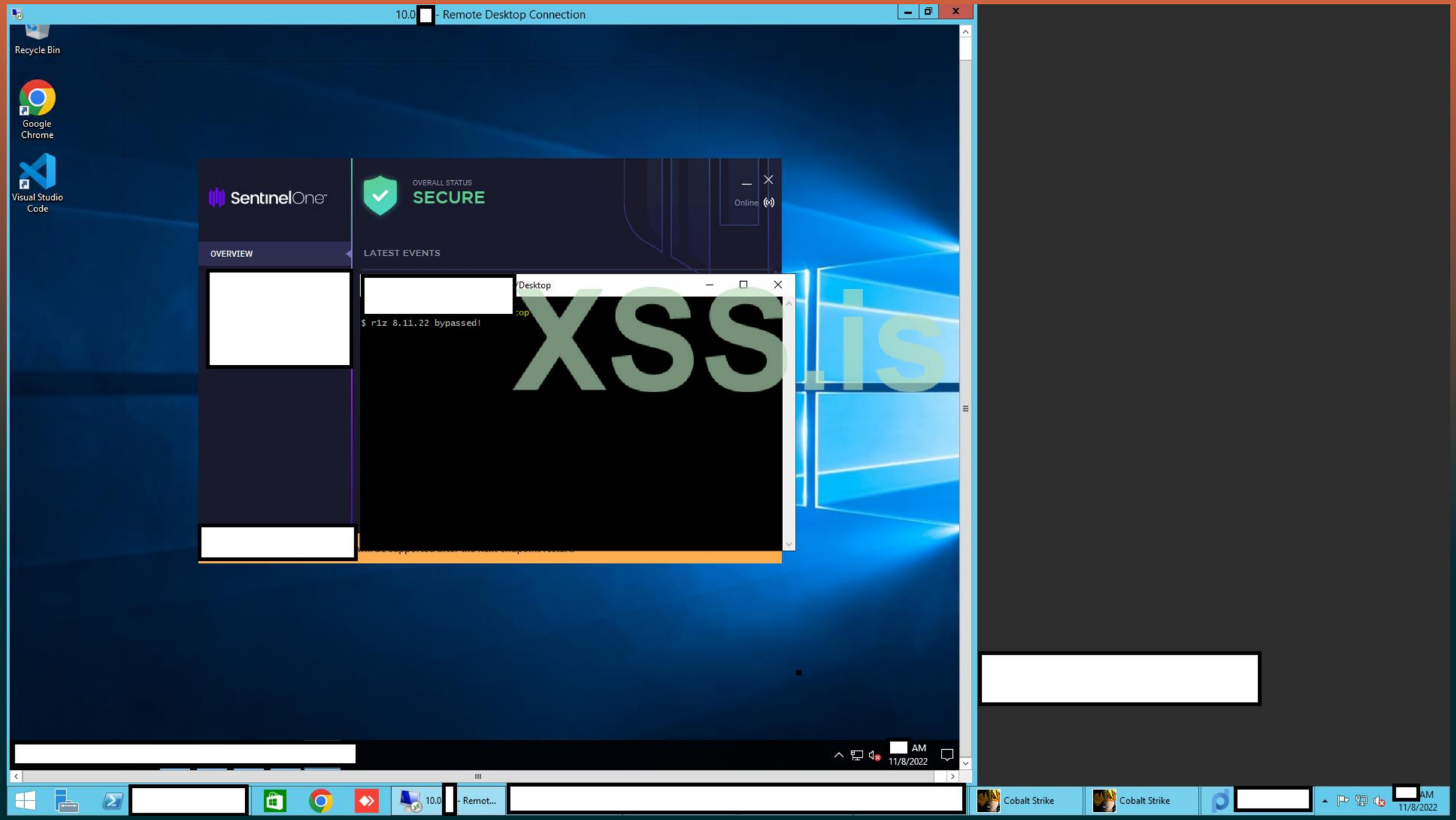
price 5k, pm only! work with guarantee as always, FEES on buyer.

TOX:
A5852A

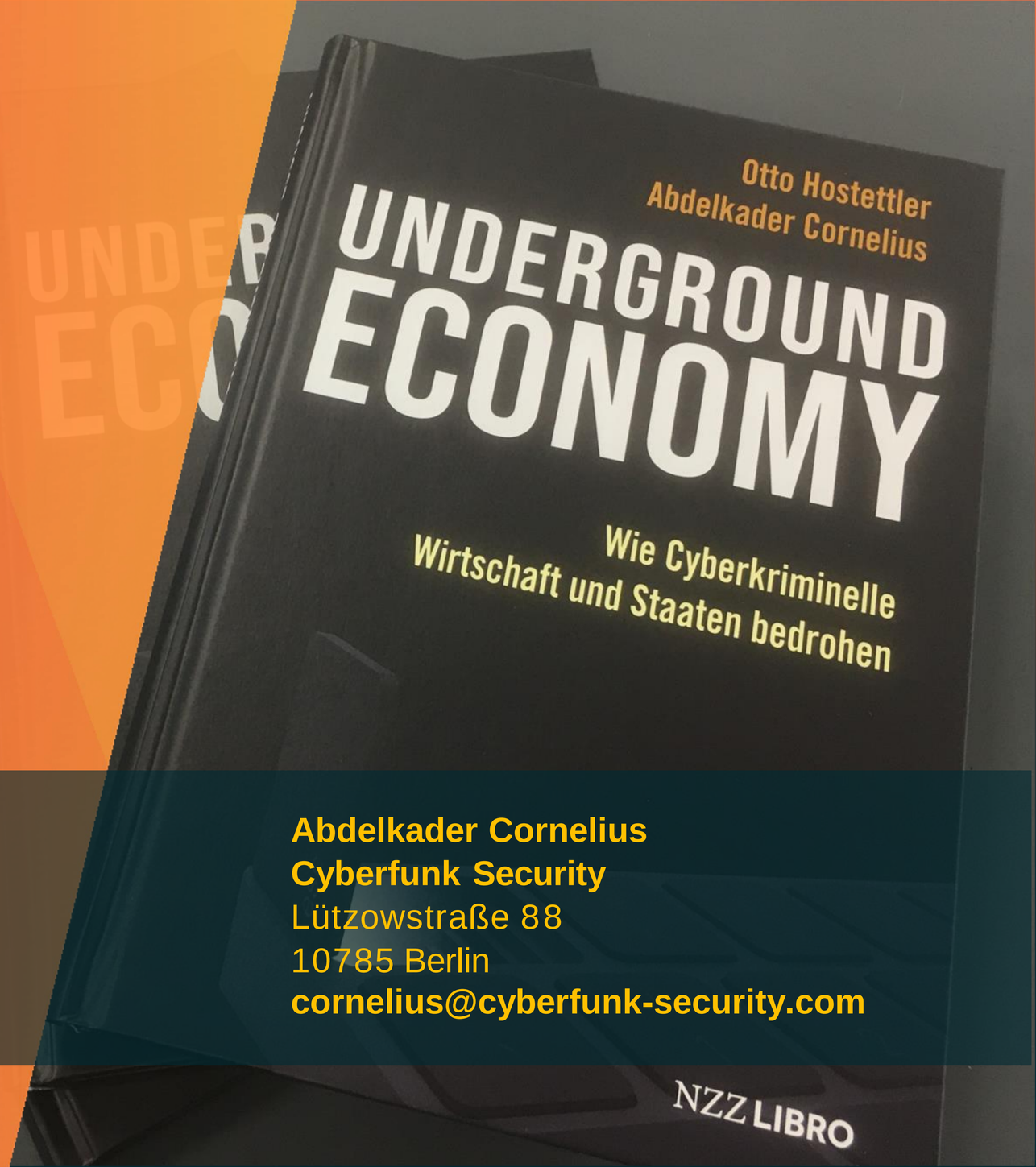
New Update >>> (⌐■_■)
Buy Latest **CobaltStrike 4.7.2 + OPSEC** (Hidden teamserver) setup.
>>> Crypt Service - Powershell Obfuscation bypass - Hidden Teamserver OPSEC **<<<**
Buy 25 Access: Fortigate + SonicVPN Accesse's + Exploits!
XSS Escrow Guarantee!

Жалоба

EDR / XDR


10.0 - Remote Desktop Connection
Recycle Bin
Google Chrome
Visual Studio Code
SentinelOne
OVERALL STATUS
SECURE
Online
OVERVIEW
LATEST EVENTS
Desktop
$ r1z 8.11.22 bypassed!
XSS.is
AM
11/8/2022
10.0 - Remot...
Cobalt Strike
Cobalt Strike
AM
11/8/2022

Vielen Dank für Ihr Vertrauen.



Otto Hostettler
Reporter/Redaktor BEOBACHTER
Ringier Axel Springer Schweiz AG
Tel : +41 (0)76 436 77 59
E-Mail: otto.hostettler@beobachter.ch
Threema-ID VAWHNBPJ

Abdelkader Cornelius
Cyberfunk Security
Lützowstraße 88
10785 Berlin
cornelius@cyberfunk-security.com