
TD SYNNEX
Partner Security Day
LIVE-HACKING

TD SYNNEX

CISA: Katalog bekannter ausgenutzter Schwachstellen

- 1072 Schwachstellen aktuell produktiv ausgenutzt
- 171 Hersteller betroffen
- 426 Produkte betroffen
- 215 Schwachstellen für Ransomware genutzt

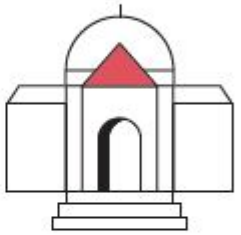
1062	CVE-2009-0			
1063	CVE-2008-3			
1064	CVE-2008-2992	Adobe	Acrobat and Reader	Adobe Reader and Acrobat Input Validation Vulnerability
1065	CVE-2008-0			Adobe Acrobat and Reader Unspecified Vulnerability
1066	CVE-2007-5			Adobe Acrobat and Reader Buffer Overflow Vulnerability
1067	CVE-2007-3010	Alcatel	OmniPCX Enterprise	Alcatel OmniPCX Enterprise Remote Code Execution Vulnerability
1068	CVE-2006-2492	Microsoft	Word	Microsoft Word Malformed Object Pointer Vulnerability
1069	CVE-2006-1			Apache Struts 1 ActionForm Denial-of-Service Vulnerability
1070	CVE-2005-2		nager	HP OpenView Network Node Manager Remote Code Execution Vulnerability
1071	CVE-2004-1464	Cisco	IOS	Cisco IOS Denial-of-Service Vulnerability
1072	CVE-2004-0			lity
1073	CVE-2002-0			lity

Agenda

1. Top 3 Bedrohungen laut BSI?
2. Was ist für Angreifer von Wert?
3. Angriffsvektoren im Live-Hacking demonstriert
    1. Passwörter – wie sicher sind sie?
    2. Social Engineering: Phishing mittels Punycode-Domains
    3. Fehlkonfiguration: Phishing in der Microsoft Cloud
    4. Ungepatchte Software vs. Ransomware
4. Auswertung: Gewinn der Hacker oder Loot

Die Top 3 Bedrohungen laut BSI

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Online-Server	Schwachstellen, offene oder falsch konfigurierte Online-Server

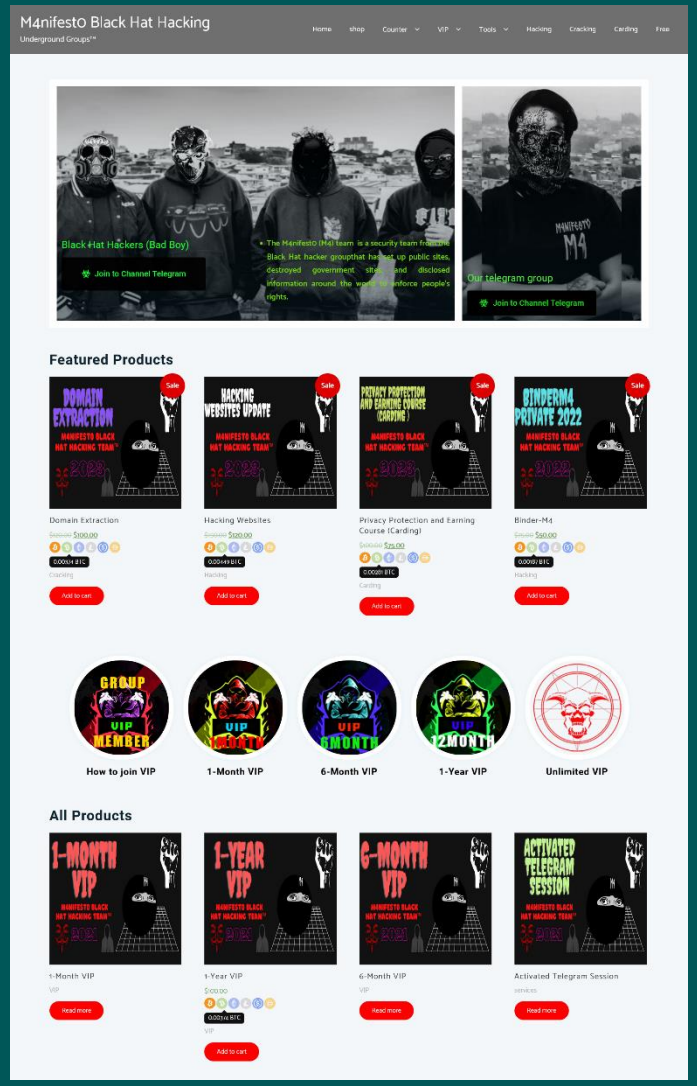
Quelle: BSI

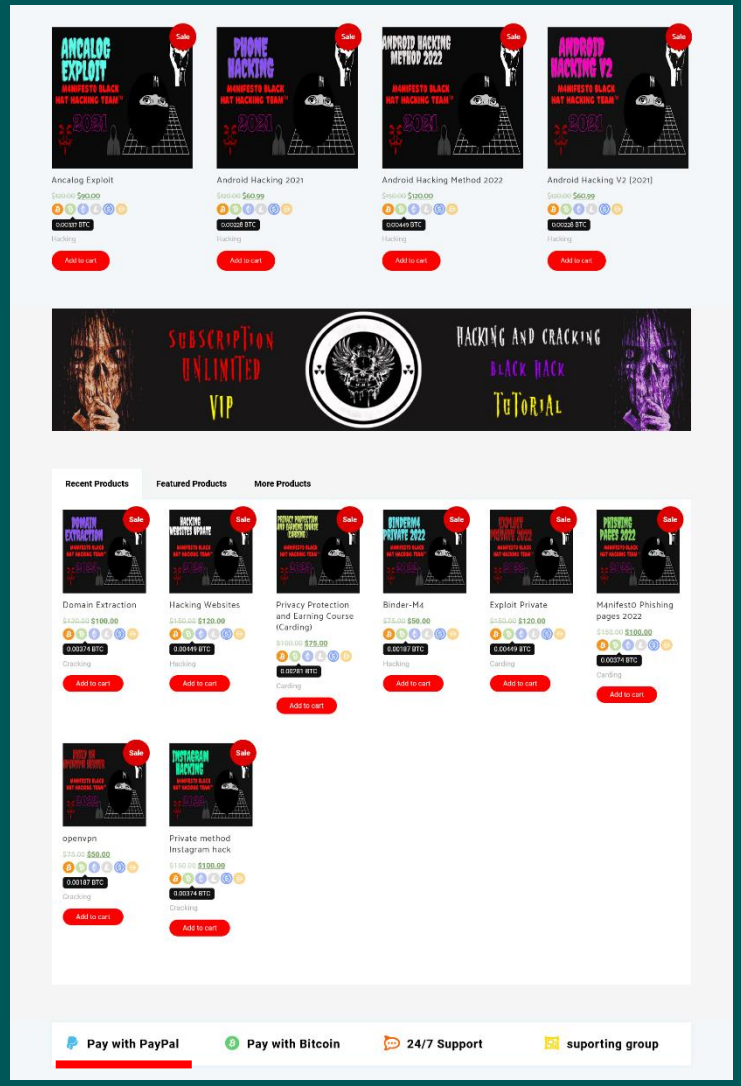
TD SYNNEX

Was ist für Angreifer von Wert?

Kategorie	Produkt	Durchschnittlicher Dark Web Preis (USD)
Kreditkartendaten	Kreditkartendaten, Kontostand bis 5.000 $	$ 120
	Geklonte VISA/Mastercard mit PIN	$ 20
Zahlungsabwicklungsdienste	PayPal-Kontodaten, Mindestguthaben 1.000 $	$ 20
	50 gehackte PayPal-Konto-Logins	$ 150
Krypto-Konten	USA verifiziertes LocalBitcoins-Konto	$ 120
Soziale Medien	Gehacktes Facebook-Konto	$ 45
Gefälschte Dokumente	Personalausweis der Europäischen Union	$ 160

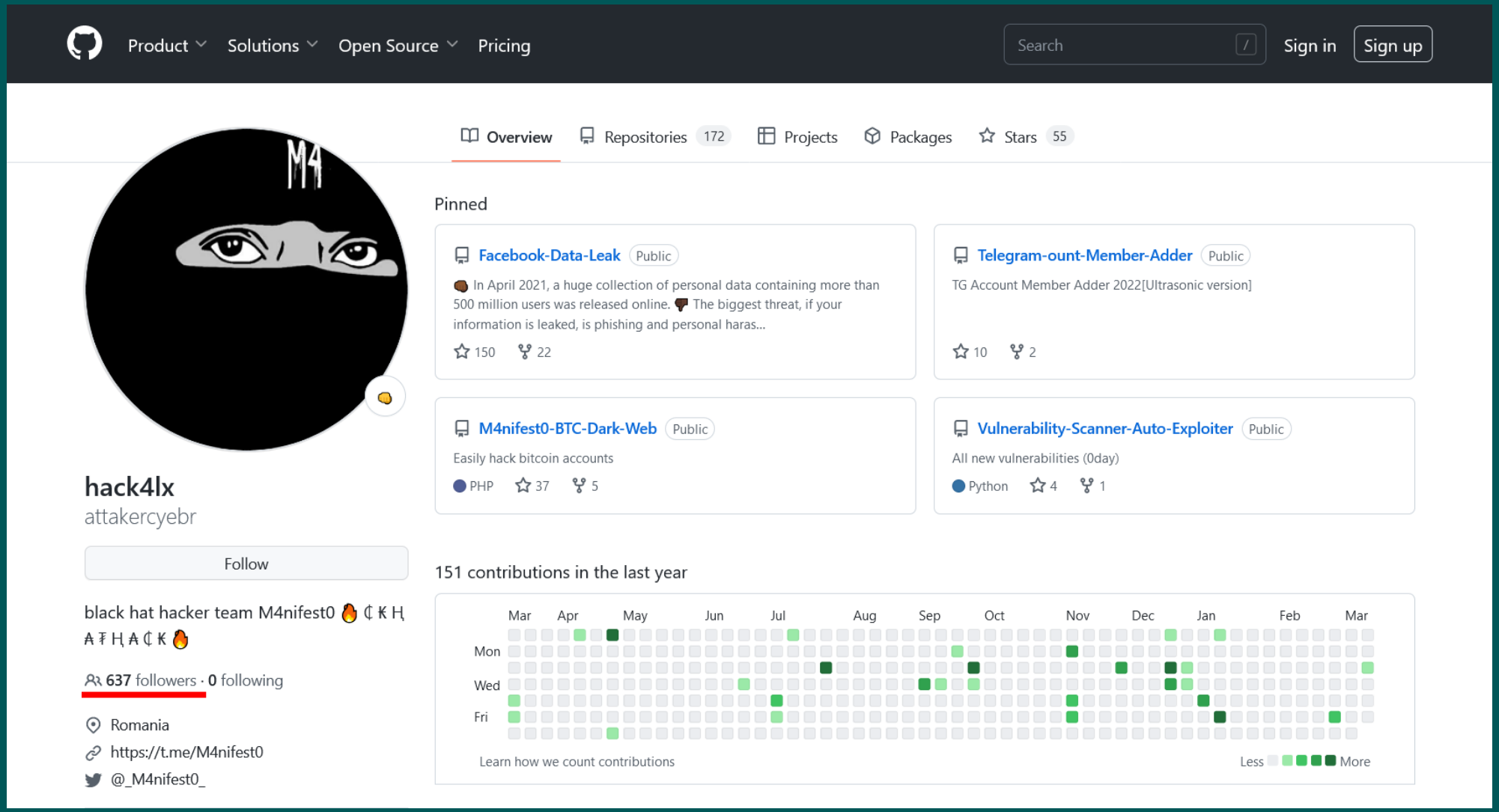
Was ist für Angreifer von Wert?





TD SYNNEX

Was ist für Angreifer von Wert?

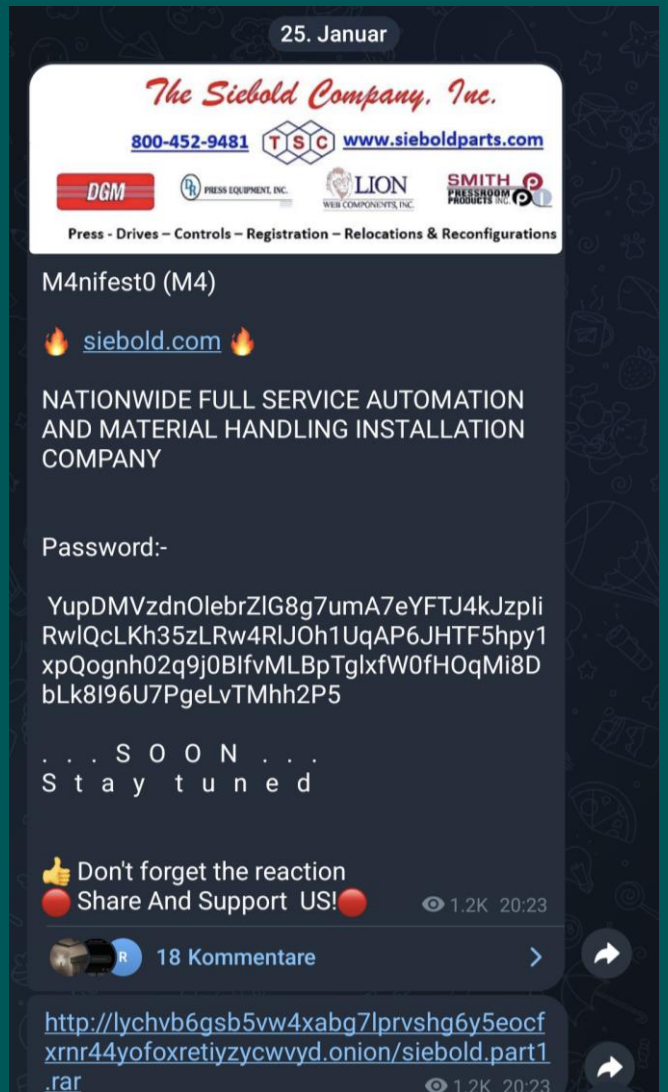


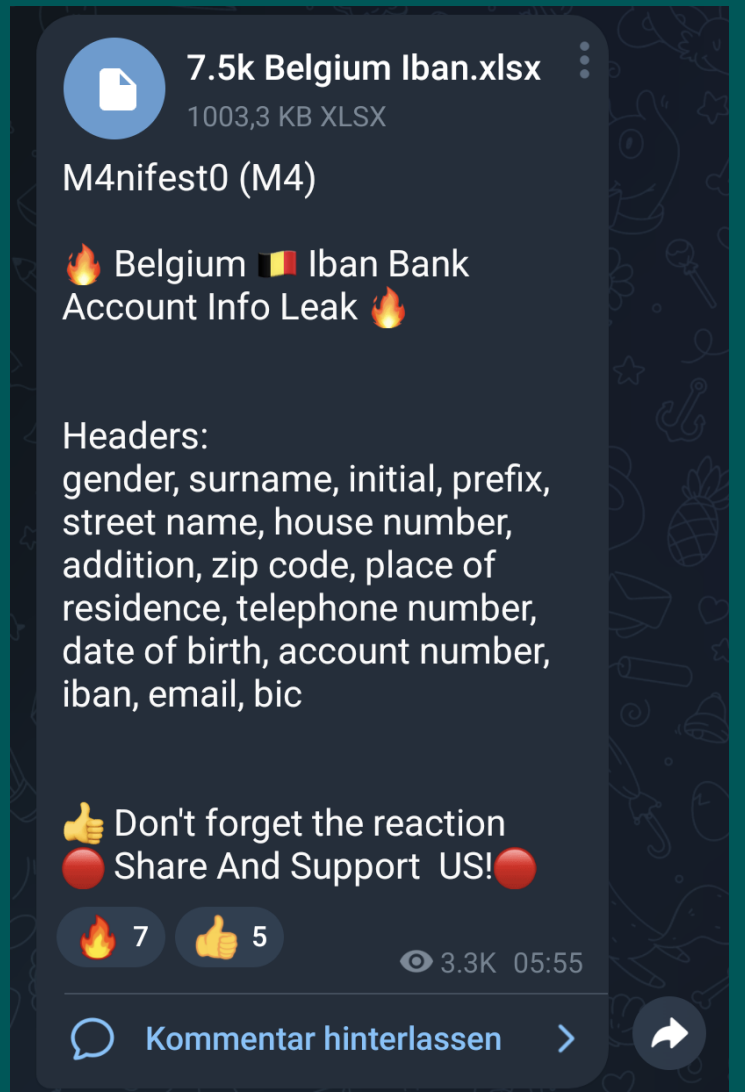
TD SYNNEX

Was ist für Angreifer von Wert? - Datenlecks

```
2465 [redacted]@roadrunner.com,[redacted]@roadrunner.com,jas94mine,smtp.roadrunner.com:587
2466 [redacted]@wanadoo.fr,[redacted]@wanadoo.fr,marionmarie,smtp.wanadoo.fr:587
2467 [redacted]@wanadoo.fr,[redacted]@wanadoo.fr,Morgan2005,smtp.wanadoo.fr:587
2468 [redacted]@wi.rr.com,[redacted]@wi.rr.com,badgers1,dnvrco-pub-iedge-vip.email.rr.com:587
2469 [redacted]@wanadoo.fr,[redacted]@wanadoo.fr,wanadoo,smtp.wanadoo.fr:587
2470 [redacted]@wanadoo.fr,[redacted]@wanadoo.fr,friends,smtp.wanadoo.fr:587
2471 [redacted]@fwgrealestate.com,[redacted]@fwgrealestate.com,brendan,mail.pickelhost.com:25
2472 [redacted]@wanadoo.fr,[redacted]@wanadoo.fr,110574,smtp.wanadoo.fr:587
2473 [redacted]@HanlonLegal.com,[redacted]@HanlonLegal.com,Hanlon,mail.b-io.co:25
2474 [redacted]@sonorangmac.com,[redacted]@sonorangmac.com,hope123,mail.pickelhost.com:25
2475 [redacted]@163.com,[redacted]@163.com,1q2w3e4r,smtp.163.com:25
2476 [redacted]@tin.it,[redacted]@tin.it,chiara,mail.tin.it:587
```

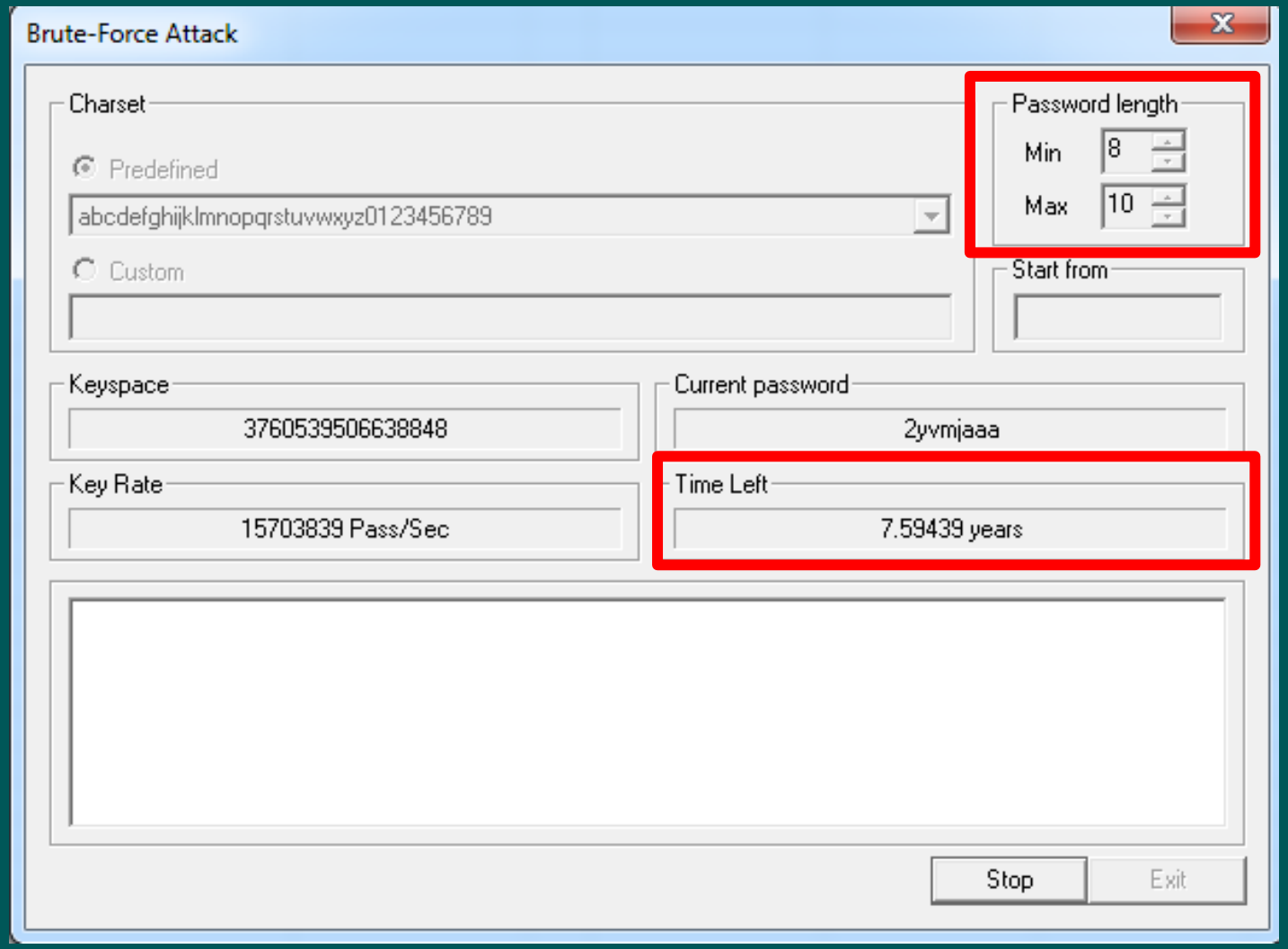
Was ist für Angreifer von Wert? - Datenlecks





TD SYNNEX

Angriffsvektoren: Passwörter – wie sicher sind sie?



TD SYNNEX

Angriffsvektoren:

Social Engineering: Phishing mittels Punycode-Domains

TD SYNNEX

Phishing mittels Punycode-Domains

https://www.bsı.bund.de/Login/Login/login_node.html?rid=J2jCQjM

https://www.bsi.bund.de/Login/Login/login_node.html

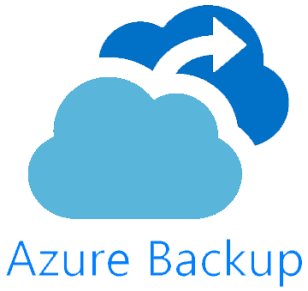
TD SYNNEX

Angriffsvektoren:

Fehlkonfiguration: Phishing in der Microsoft Cloud

Phishing in der Microsoft-Cloud

- Man muss einen User finden, der das Recht hat Applikationen zu registrieren z.B.



Natürlich handelt es sich dabei nicht um das Azure Backup von Microsoft

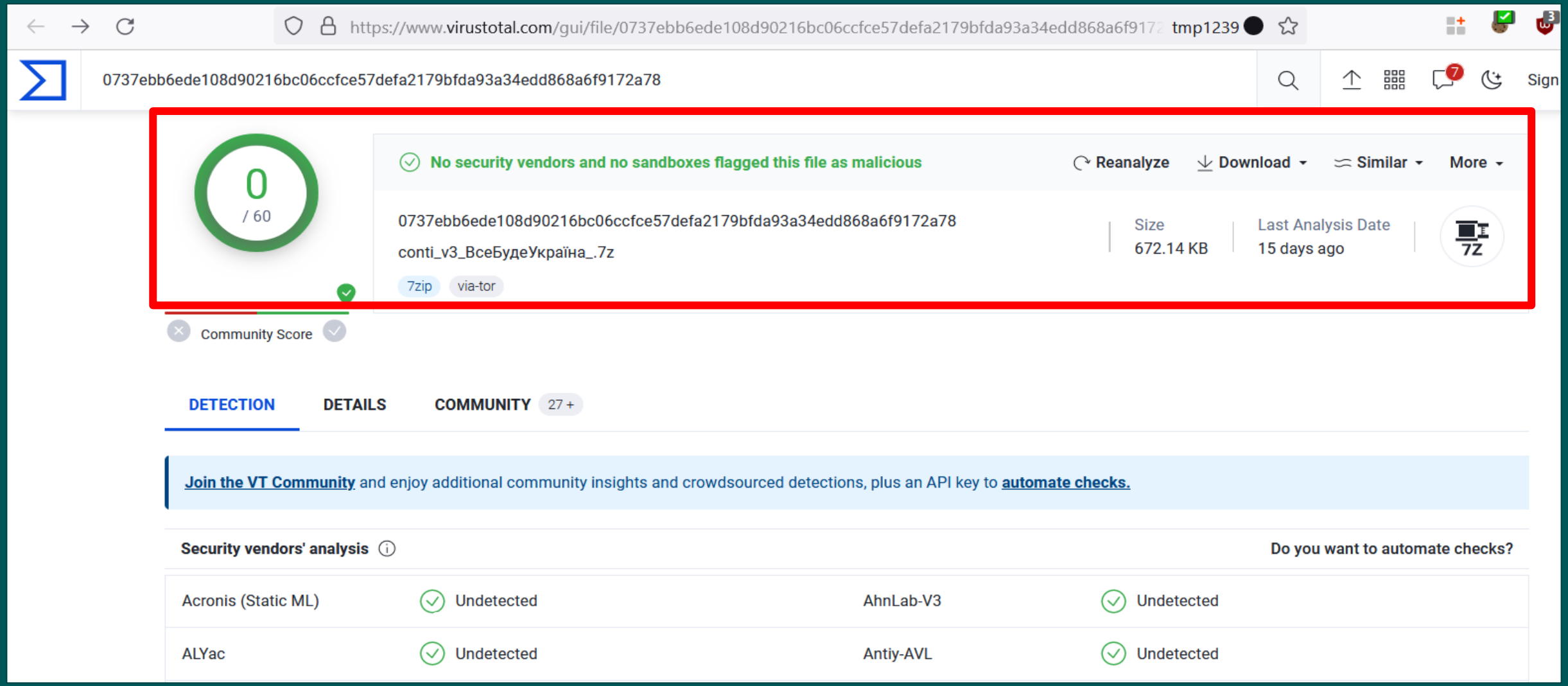
TD SYNNEX

Angriffsvektoren:

Ungepatchte Software vs. Ransomware

TD SYNNEX

Ungepatchte Software vs. Ransomware



HYDRACRYPT

HYDRACRYPT

All Your files and documents were encrypted!

ID : [redacted]

Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It`s your guarantee!
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:
1) Your software`s price will be higher
2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

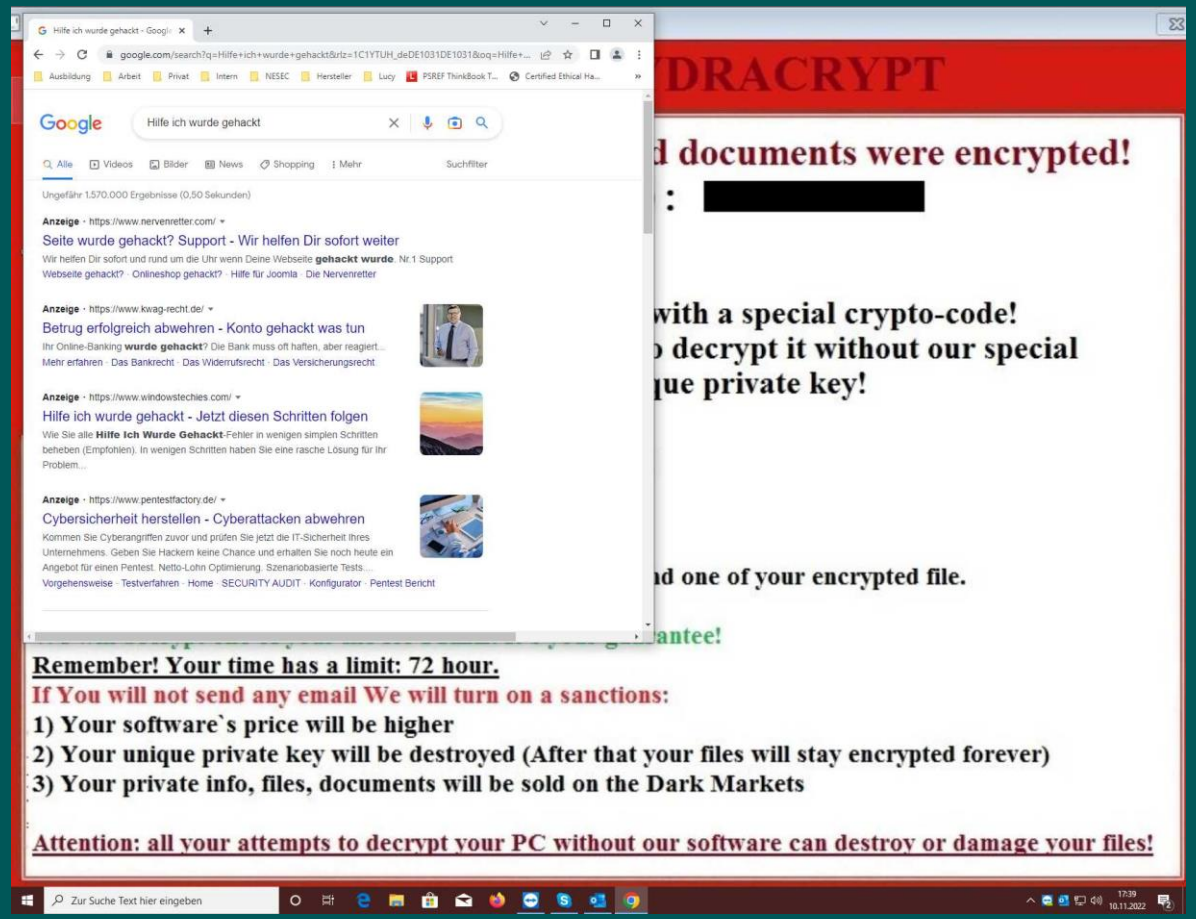
TD SYNNEX

Auswertung:

Gewinn der Hacker oder Loot

Loot

- Login & Passworte BSI & Facebook (Phishing & Browserangriff)
- MS-Token, Datei- und E-Mailzugriff (Office Stealer)
- Kreditkartendaten aus dem Browser
- Lesezeichen der Browser Chrome, IE,
- Zugangsdaten aus Outlook
- Dateien: Keepass-Datenbank, PDFs, Word- und Excel-Dokumente und alle Bilder
- Windows-Passwort des angemeldeten Benutzers im Klartext
- Windows Passwort-Hashes aller Benutzer
- 2 MS Lizenz-Keys
- Installierte Software mit Versionen und die laufenden Prozesse des angegriffenen Rechners
- Die Hostsdatei
- Screenshots und Webcambild
- Neuen administrativen User angelegt
- Kein Bitcoin-Wallet gefunden



CYBERFORCE

TD SYNNEX

That‘s it
Vielen Dank für Ihre Aufmerksamkeit

Arik.Seils@TDSynnex.com

paloalto NETWORKS