



Partner Security Day

LIVE-HACKING

CISA: Katalog bekannter ausgenutzter Schwachstellen

1062	CVE-2009-0001				
1063	CVE-2008-3362				
1064	CVE-2008-2992	Adobe	Acrobat and Reader	Adobe Reader and Acrobat Input Validation Vulnerability	
1065	CVE-2008-0655	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Unspecified Vulnerability	
1066	CVE-2007-5053	Adobe	Acrobat and Reader	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-2006-1046	Apache	Struts	Apache Struts 1 ActionForm Denial-of-Service Vulnerability	
1070	CVE-2005-2152	HP	OpenView Network Node Manager	HP OpenView Network Node Manager Remote Code Execution Vulnerability	
1071	CVE-2004-1464	Cisco	IOS	Cisco IOS Denial-of-Service Vulnerability	
1072	CVE-2004-0912	Microsoft	Exchange	Microsoft Exchange Remote Code Execution Vulnerability	
1073	CVE-2002-0669	Microsoft	Exchange	Microsoft Exchange Remote Code Execution Vulnerability	

• **1072 Schwachstellen aktuell produktiv ausgenutzt**

• **171 Hersteller betroffen**

• **426 Produkte betroffen**

• **215 Schwachstellen für Ransomware genutzt**

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



Identitätsdiebstahl

Sextortion
Phishing

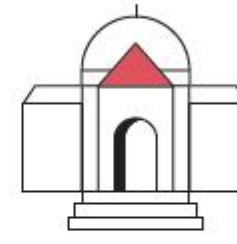
Wirtschaft



Ransomware

Abhängigkeit innerhalb der
IT-Supply-Chain
Schwachstellen, offene oder falsch
konfigurierte Online-Server

Staat und Verwaltung



Ransomware

APT
Schwachstellen, offene oder
falsch konfigurierte Online-Server

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?

M4nifesto Black Hat Hacking
Underground Groups™

Home shop Cartier VIP Tools Hacking Cracking Carding Free



Black Hat Hackers (Bad Boy)

Join to Channel Telegram



Our telegram group

Join to Channel Telegram

Featured Products



Domain Extraction

Original: \$100.00

Discount: \$50.00

0.0004 BTC

Cracking

Add to cart



Hacking Websites

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Privacy Protection and Earning Course (Carding)

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Binder-M4

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



How to join VIP



1-Month VIP



6-Month VIP



1-Year VIP



Unlimited VIP

All Products



1-Month VIP

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



1-Year VIP

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



6-Month VIP

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Activated Telegram Session

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Ancalog Exploit

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Phone Hacking

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Android Hacking Method 2022

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Android Hacking V2 (2021)

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



SUBSCRIPTION UNLIMITED VIP

HACKING AND CRACKING BLACK HAT TUTORIAL

Recent Products



Domain Extraction

Original: \$100.00

Discount: \$50.00

0.0004 BTC

Cracking

Add to cart



Hacking Websites

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Privacy Protection and Earning Course (Carding)

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Binder-M4

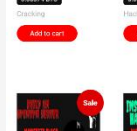
Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Exploit Private

Original: \$100.00

Discount: \$50.00

0.0004 BTC

Cracking

Add to cart



Manifesto Phishing pages 2022

Original: \$100.00

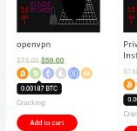
Discount: \$50.00

0.0004 BTC

Cracking

Add to cart

Featured Products



1-Month VIP

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Private method Instagram hack

Original: \$50.00

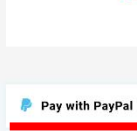
Discount: \$25.00

0.0004 BTC

Cracking

Add to cart

More Products



Ancalog Exploit

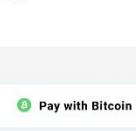
Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart



Phone Hacking

Original: \$50.00

Discount: \$25.00

0.0004 BTC

Cracking

Add to cart

Pay with PayPal

Pay with Bitcoin

24/7 Support

supporting group

Was ist für Angreifer von Wert?


[Product](#)
[Solutions](#)
[Open Source](#)
[Pricing](#)

[Sign in](#)
[Sign up](#)

[Overview](#)
[Repositories 172](#)
[Projects](#)
[Packages](#)
[Stars 55](#)



hack4lx
attakercyabr

Follow

black hat hacker team M4nifest0 🔥 ⚔️ 🇸🇪
A 7 H A C K 🔥

637 followers · 0 following

📍 Romania
🔗 <https://t.me/M4nifest0>
🐦 @_M4nifest0_

Pinned

 [Facebook-Data-Leak](#) Public

In April 2021, a huge collection of personal data containing more than 500 million users was released online. 🗡️ The biggest threat, if your information is leaked, is phishing and personal harass...

☆ 150 🍴 22

 [Telegram-ount-Member-Adder](#) Public

TG Account Member Adder 2022[Ultrasonic version]

☆ 10 🍴 2

 [M4nifest0-BTC-Dark-Web](#) Public

Easily hack bitcoin accounts

📄 PHP ☆ 37 🍴 5

 [Vulnerability-Scanner-Auto-Exploiter](#) Public

All new vulnerabilities (0day)

📄 Python ☆ 4 🍴 1

151 contributions in the last year

	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Mon													
Wed													
Fri													

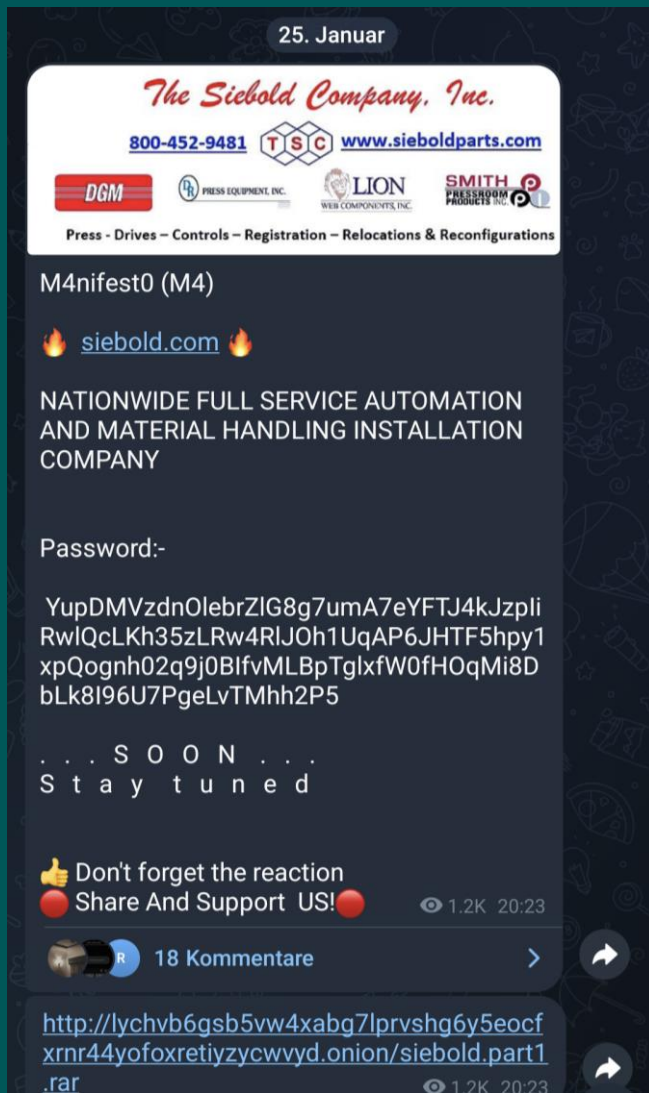
Learn how we count contributions

Less More

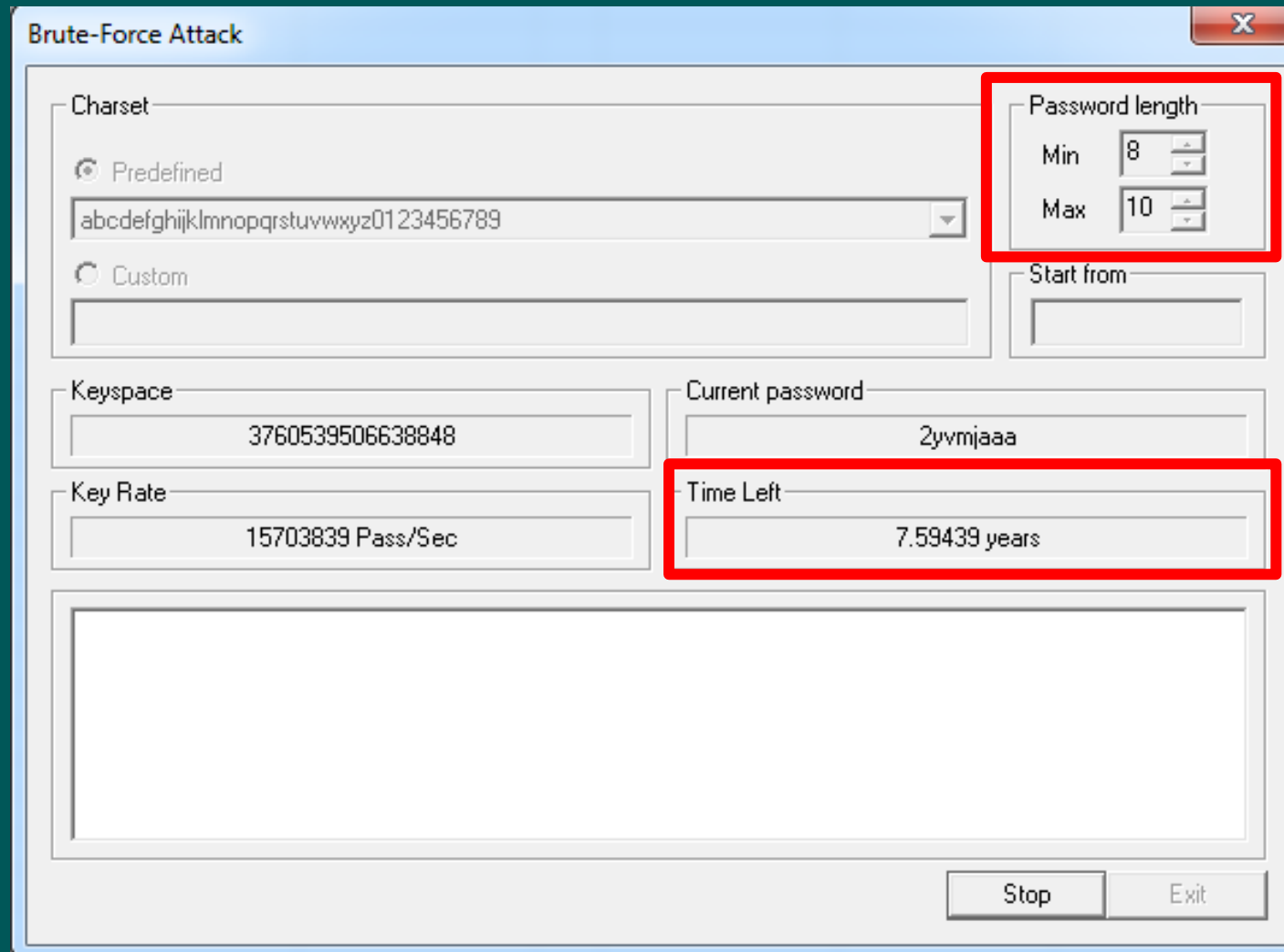
Was ist für Angreifer von Wert? - Datenlecks

```
2465 c[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



Angriffsvektoren: Passwörter – wie sicher sind sie?



The screenshot shows a 'Brute-Force Attack' window with various configuration options. Two areas are highlighted with red rectangles: the 'Password length' section and the 'Time Left' section.

Brute-Force Attack

Charset

☒ Predefined
abcdefghijklmnopqrstuvwxyz0123456789

☐ Custom

Password length

Min: 8
Max: 10

Start from

Keyspace
3760539506638848

Current password
2yvmjaaa

Key Rate
15703839 Pass/Sec

Time Left
7.59439 years

Stop **Exit**

Angriffsvektoren:

Social Engineering: Phishing mittels Punycode-Domains

Phishing mittels Punycode-Domains

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

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

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.

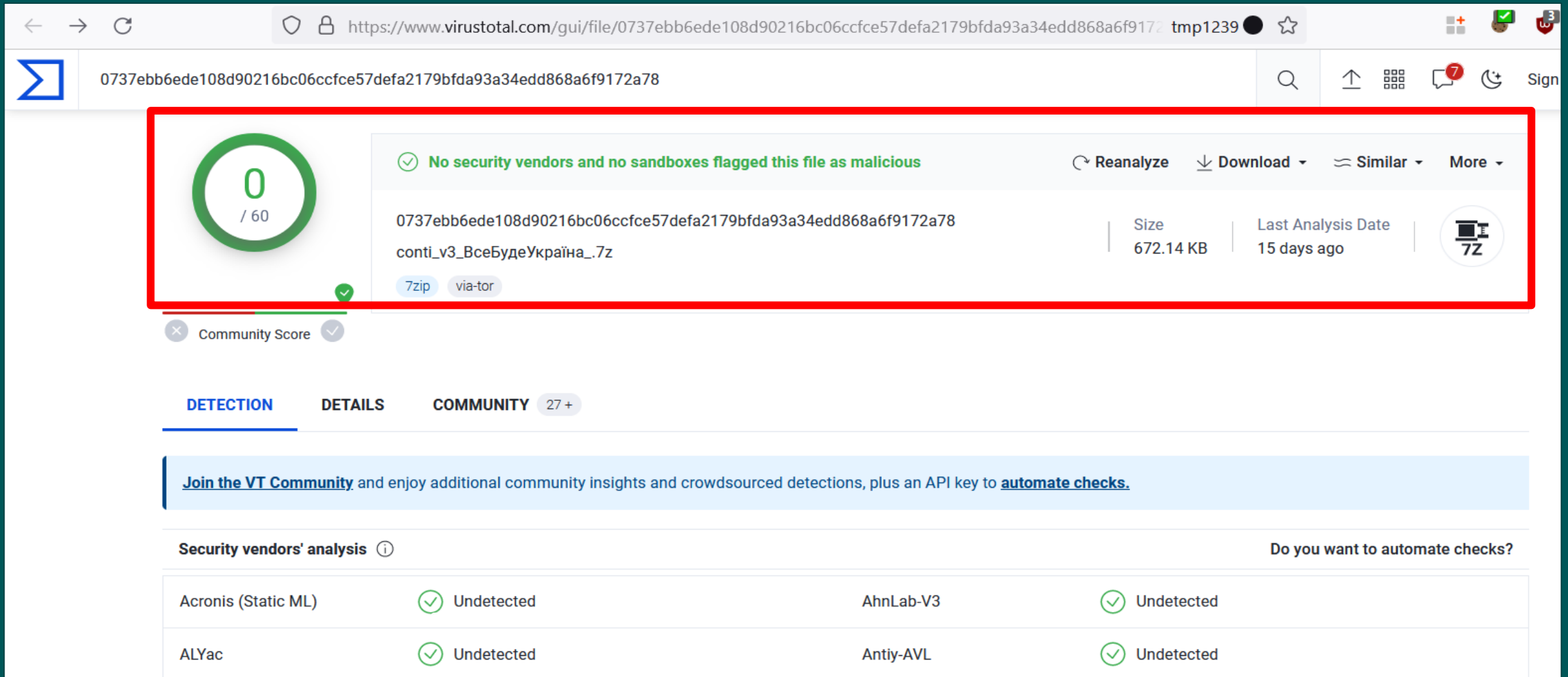


Natürlich handelt es sich dabei nicht um das Azure Backup von Microsoft

Angriffsvektoren:

Ungepatchte Software vs. Ransomware

Ungepatchte Software vs. Ransomware



0737ebb6ede108d90216bc06ccfce57defa2179bfda93a34edd868a6f9172a78

0 / 60

✓ No security vendors and no sandboxes flagged this file as malicious

Reanalyze Download Similar More

0737ebb6ede108d90216bc06ccfce57defa2179bfda93a34edd868a6f9172a78

Size: 672.14 KB | Last Analysis Date: 15 days ago

7zip via-tor

Community Score

DETECTION DETAILS COMMUNITY 27 +

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected

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**

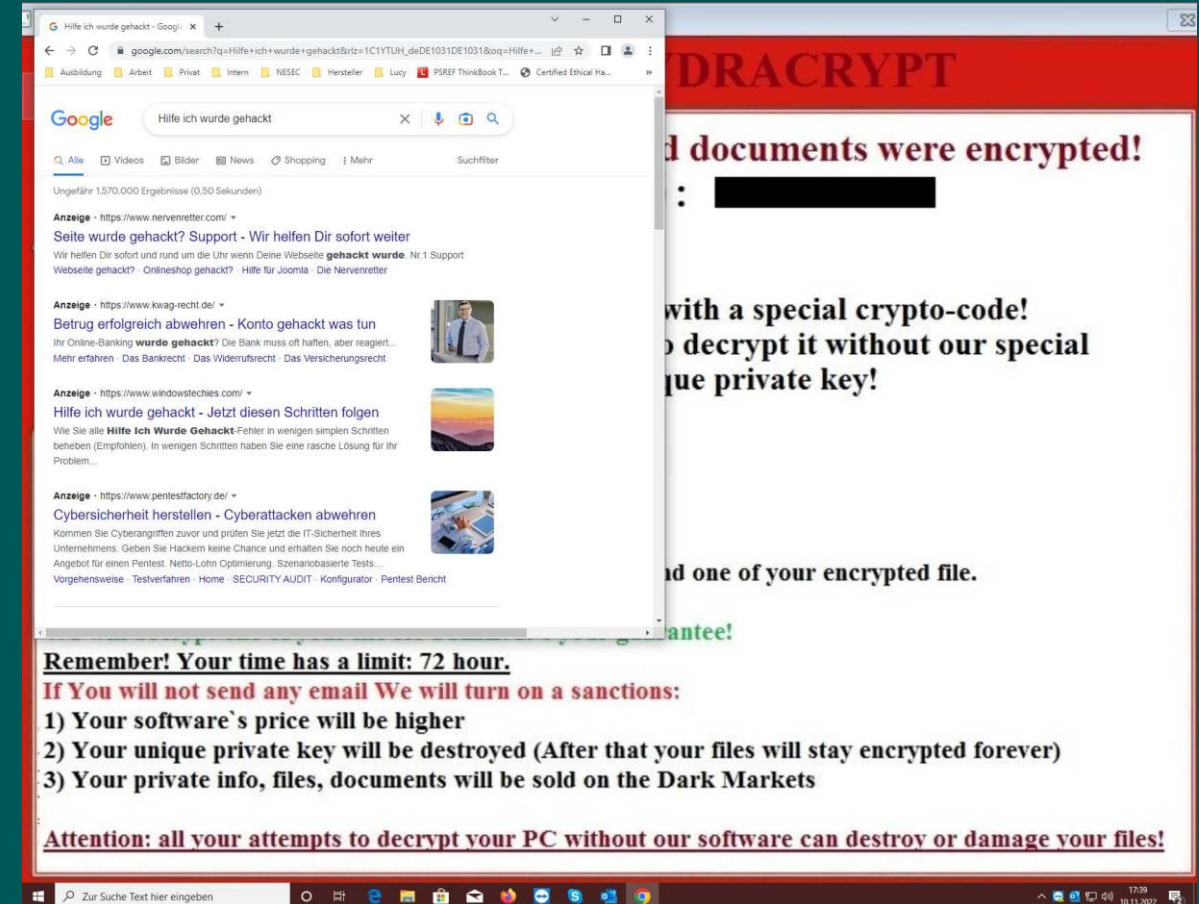
Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

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**



That's it
Vielen Dank für Ihre Aufmerksamkeit

Arik.Seils@TDSynnex.com