

ARES

CYBER INTELLIGENCE

Defend the Web: Becoming a Cyber Security Hero

ARE YOU SECURE?

WIR

Gründung 2019
Headquarter Traun (OÖ)
Expansion Rumänien, Israel, UAE
14 Mitarbeiter => 50% Frauen!!!

est. 2019



“Prepared for the unknown”

Jürgen Weiss

Cyber Crisis Manager

#164 Cybercrime Cases

Negotiations

4 Ransomware Payments

Cybercrime Profiler

Intern. Ausbildung US (NIST), Israel (Negotiations, Profiling)

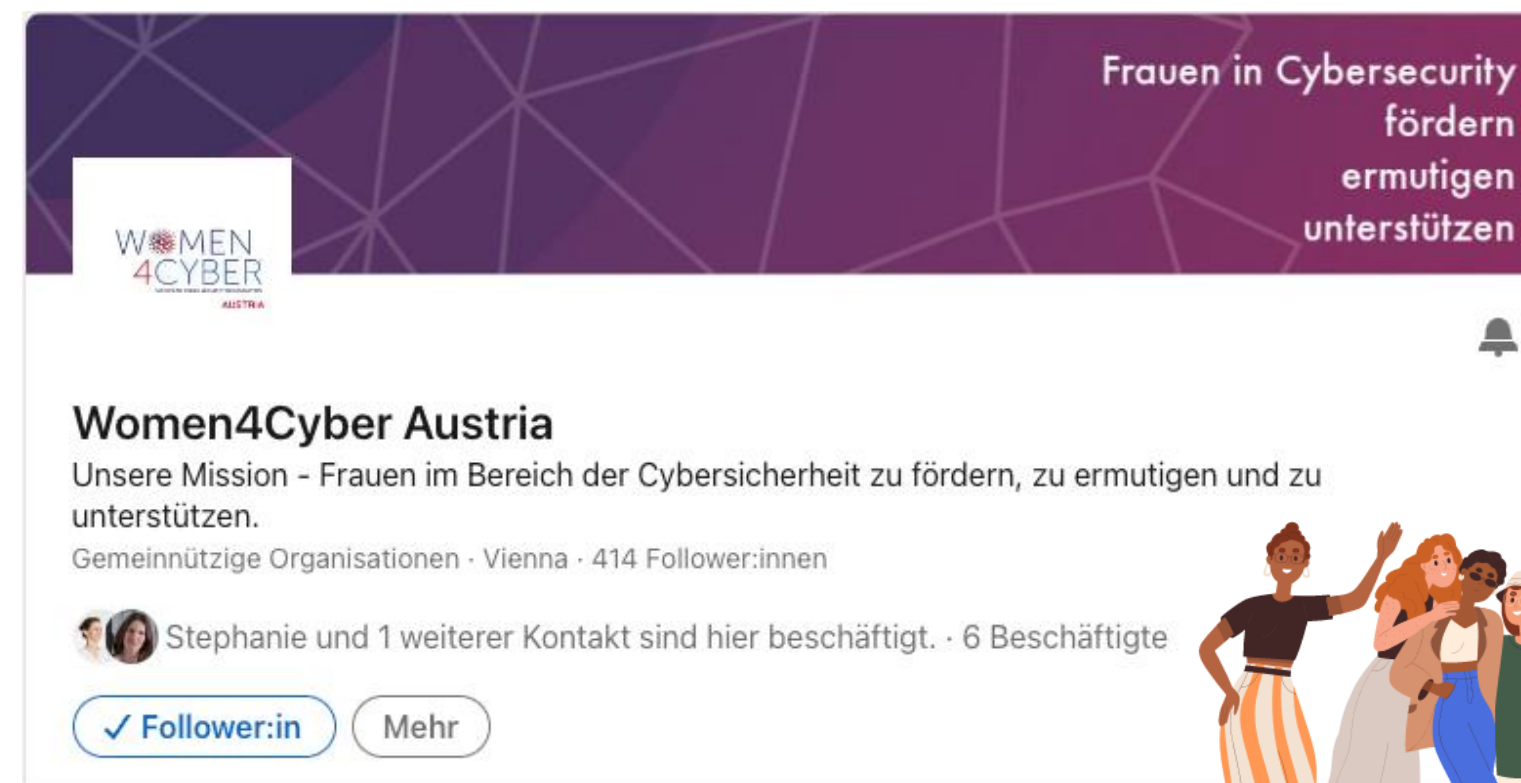
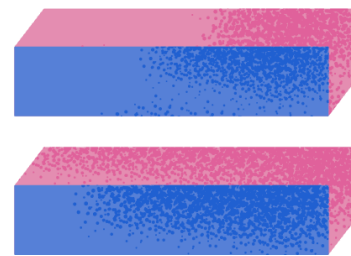
Open Source & Darknet Intelligence



INTERNATIONALER WELTFRAUENTAG 8. März 2023



<https://women4cyber.eu/>



173.5 billion USD

Global Cyber Security Market in 2022

266.2 billion USD

Global Cyber Security Market in 2027

2,7 Mio.

Unbesetzte Stellen WELTWEIT

8,9% Wachstum

WELTWEIT

3,5 Mio.

Cyber Ressourcen bis 2025 benötigt

Cybersecurity EU

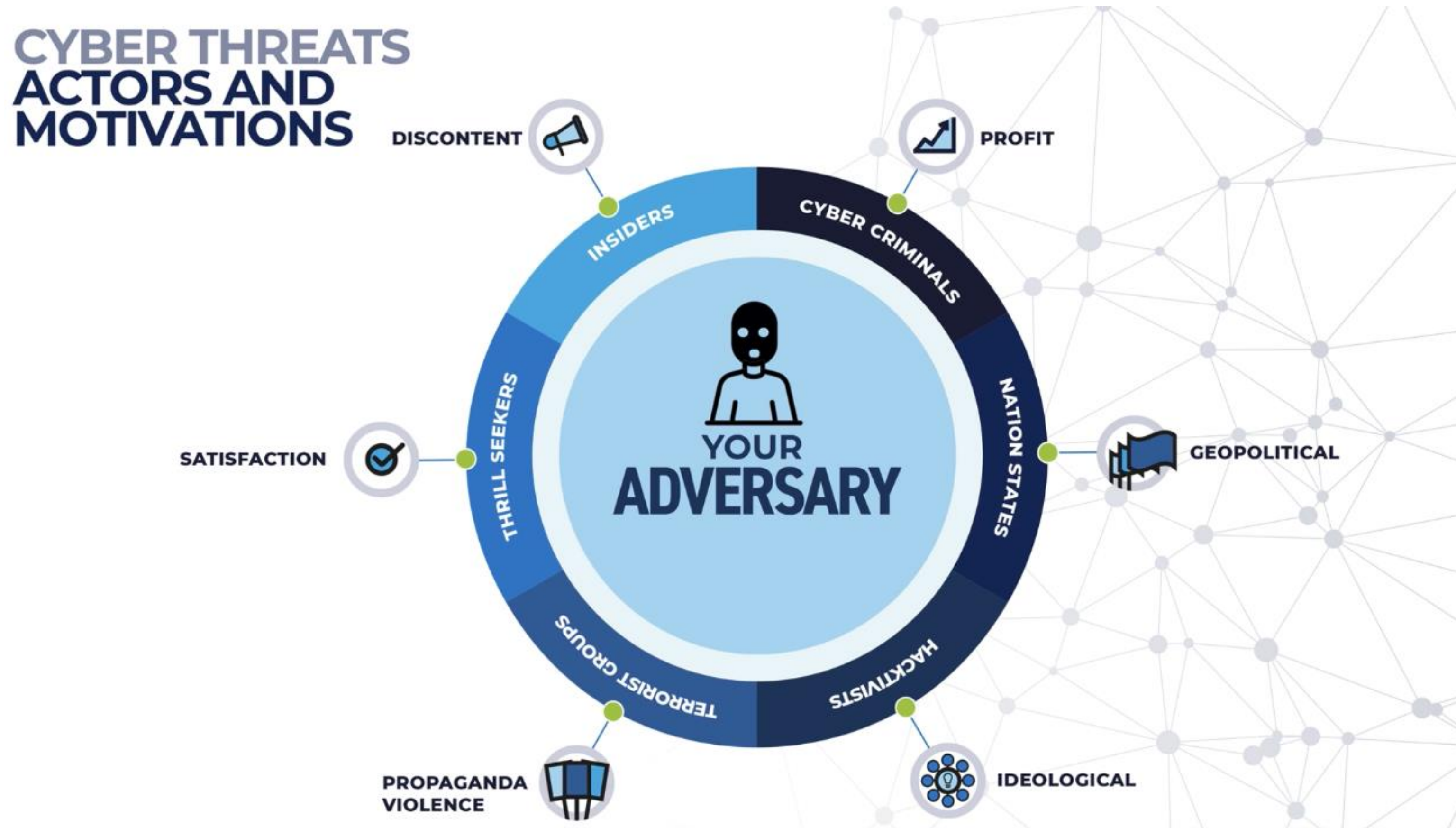
2023 wird der Cybersecurity Markt in Europa auf 43 Mrd. EUR wachsen und bis 2027 um 9.7% vergrößern!



BECOME A CYBER HERO



CYBER Criminals (HACKER)



THE UNDERGROUND CYBERCRIME ECONOMY

— TOP 10 — ROLES

ORGANISATIONAL LEADERS

Often "People Persons" without technical skills. The leaders assemble the team and choose the target

PROGRAMMERS

Who develop the exploits and malware to commit cybercrimes

DISTRIBUTORS

Who trade and sell stolen data and act as escrows for the goods/services provided by other specialists

TECH EXPERTS

Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases and more

HACKERS

Who search for and exploit applications, systems and network vulnerabilities

FRAUDSTERS

Who create and deploy various social engineering schemes, such as phishing and spam

TELLERS

Who are charged with transferring and laundering illicitly gained proceeds through digital/crypto currency services and different world currencies.

MONEY MULES

Who complete electronic transfers between bank accounts. The money mules often use students and a combination of "witting" and "unwitting" agents

CASHIERS

Who control drop accounts and provide names and accounts to other criminals for a fee

HOSTED SYSTEM PROVIDERS

Who offer safe hosting "bullet proof hosting" of illicit content servers and sites

CYBERCRIME PRICELIST

ATTACK TOOLS

MALWARE

BASIC BANKING TROJAN KIT WITH SUPPORT	€100	OFFICE MACRO DOWNLOADER GENERATOR	€5
PASSWORD STEALING TROJAN	€25-100	MALWARE CRYPTER SERVICE (MAKE HARD TO DETECT)	€20-40
ANDROID BANKING TROJAN	€200	RANSOMWARE KIT	€10-1800

RANSOMWARE

SOPHISTICATED LICENSE FOR WIDESPREAD ATTACK	€200	PC MALWARE INSTALLATION	€1
UNSOPHISTICATED LICENSE FOR TARGETED ATTACK	€50	1 MILLION MALICIOUS SPAM	€400

SOFTWARE

REMOTE DESKTOP CONTROL TOOL	€100	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE	€700
-----------------------------	------	---	------

PAYMENT

CREDIT/ DEBIT CARD FOR ONLINE USE	€5	BANK ACCOUNT LOG-IN WITH ACCESS TO MAIL, SECURITY ANSWER, ETC	€25
CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC	€10	EXISTING PAYPAL ACCOUNT	€1
BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)	€5		

DATA

PERSONAL INFORMATION

SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION	€3	CREDIT REPORT 750+ CREDIT SCORE	€150
--	----	---------------------------------	------

DATABASE RECORDS

1 MILLION COMPROMISED EMAIL / PASSWORDS	€25
---	-----

SERVICES

HACKING

EMAIL ACCOUNT	€100	SOCIAL MEDIA ACCOUNT	€100
CMS WEBSITE (WORDPRESS, ETC)	€300		

MALWARE

PC MALWARE INSTALLATION	€1	MALICIOUS FILE ENCRYPTION	€25
-------------------------	----	---------------------------	-----

USER OBFUSCATION

BULLET PROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC)	€150	VIRTUAL PRIVATE NETWORK (VPN)	€20
---	------	-------------------------------	-----

FAKE DOCUMENTS

DIGITAL COPY OF FAKE CREDIT / DEBIT CARD	€25	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD	€15
DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT	€25		

DDoS

DDoS SERVICE 24 HR DURATION	€50-1000
-----------------------------	----------

SPAM

500 SMS (FLOODING)	€20	1 MILLION EMAIL SPAM	€200
500 PHONE CALLS (FLOODING)	€20		

Ransomware Attacken

- Attackieren IT/OT-Systeme
- Verschlüsseln Server und Backups
- Zerstören ihre Daten und IT-Infrastruktur
- legen Produktionen lahm
- Exfiltrieren Daten und verkaufen diese an Dritte weiter
- Tatbestand Erpressung



**„HOW
DOES IT
FEEL?“**



RED TEAM

VS

BLUE TEAM



RED TEAM

**Vulnerability Assessment
& Penetration Testing**

Threat Hunting

Exploit Development

**Cyber Threat
Intelligence**

Malware Analysis

Social Engineering



PURPLE TEAM

**Red Team and
Blue Team working
collaboratively to improve
the cybersecurity
posture of the
organisation**



BLUE TEAM

Incident Responders

Security Operations

IT Network & Systems

CIO & CISO office



JOIN OUR TEAM

ares-ci.com

emergency@ares-ci.com

+43 800 0800 22

myincident.ai

