L’ecosistema della scena Hacker

Stefano Chiccarelli

Ethical Hacker

Stefano Chiccarelli
Ethical Hacker

- Head of Cyber Security Consulting
  - Cyber Partners spa a RINA group company
  - 30 anni di esperienza nel settore
- Fondatore della Metro Olografix
- Organizzatore del MOCA
  - (Hacker camp italiano, 2004, 2008, 2012 e 2016)
- Membro del coordinamento di Sikurezza.org
- Co-autore con l'avv. Monti di Spaghetti Hacker
- SySop di una BBS storica telnet: bbs.olografix.org
- Membro steering commitee di RomHack Camp (settembre '22)

Ecosistema della scena «Hacker»

Il mio punto di vista

Cybercrime

Cybercrime as a Service (CaaS)

- Attività Criminali
- Sottobosco nei paesi Cyber-Canaglia
- Black Market
- Gruppi Ransomware

Hacktivism

Political Hackers

- Anonymous
- Chaos Computer Club (CCC)
- Hackmeeting
- Citizen Lab

Researchers

Computer Hackers

- Società di sicurezza
- Security Vendors
- Università
- Threat Intelligence

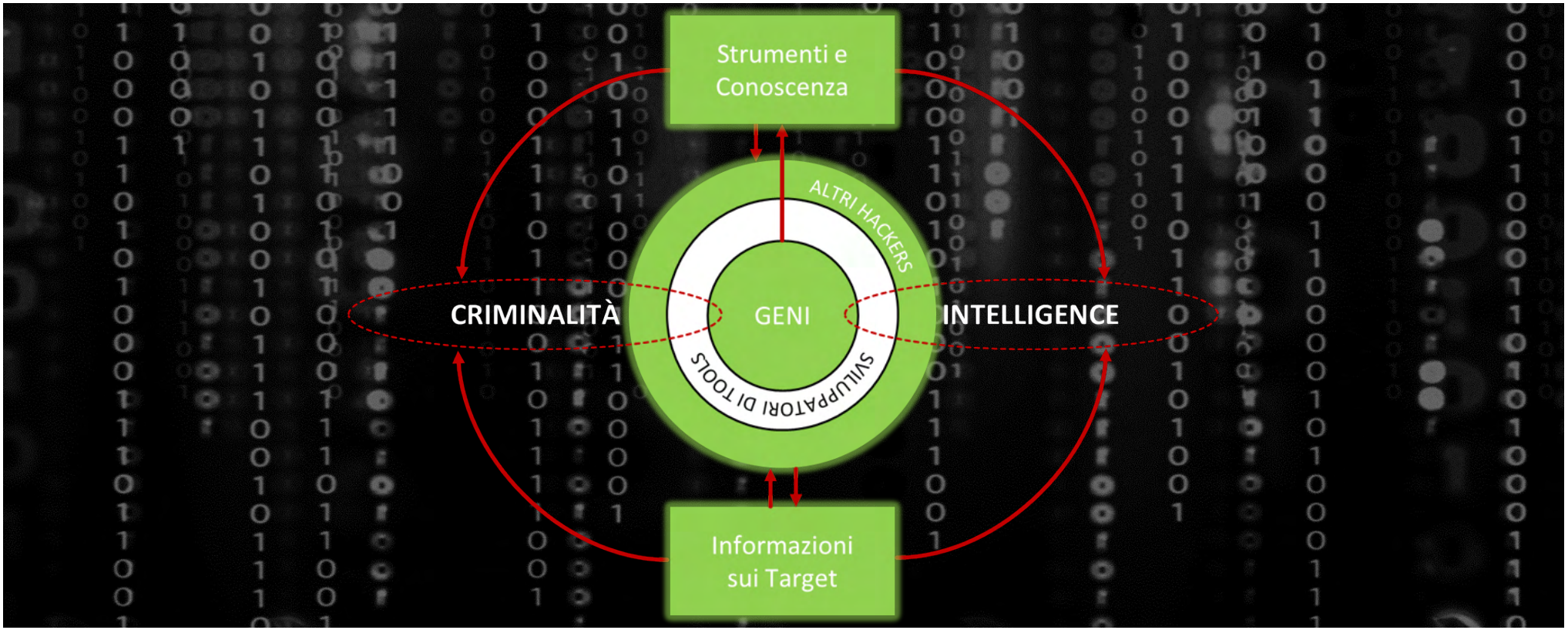
Intelligence

Homeland and Foreign

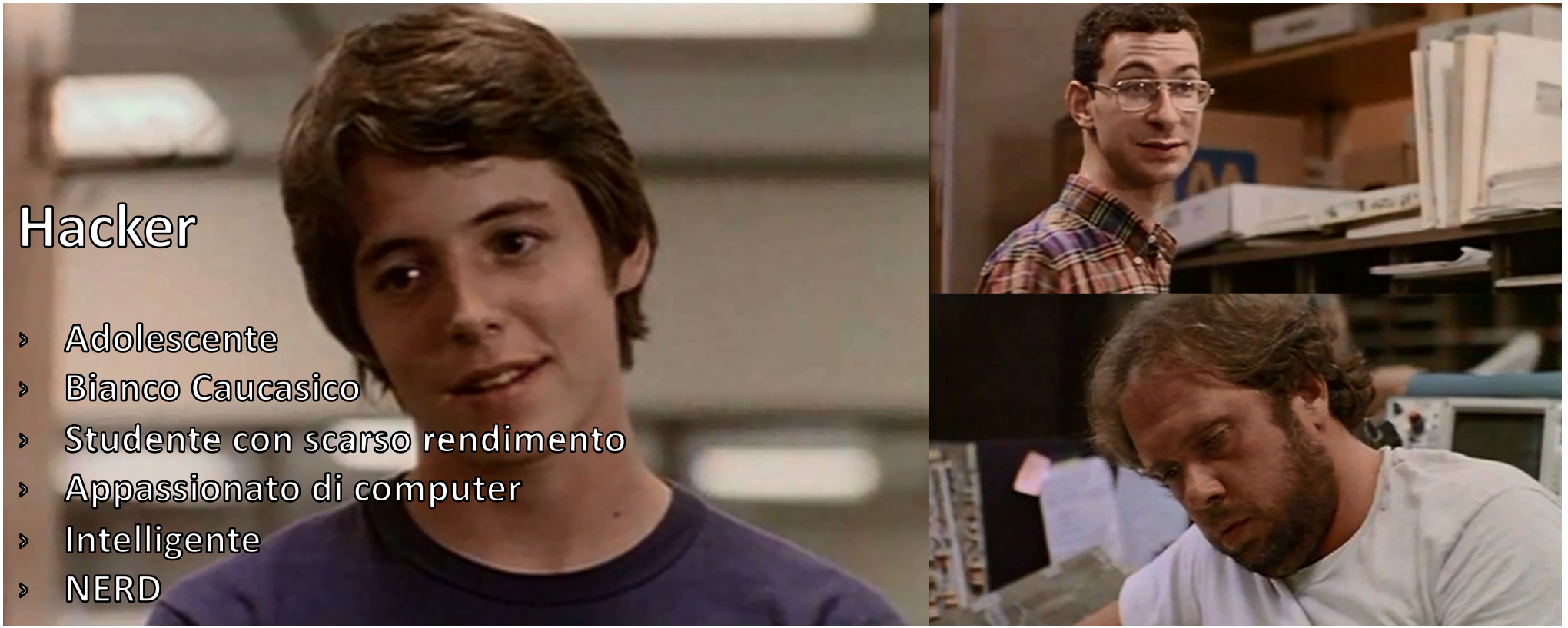
- Spionaggio
- Cyber Defence
- Cyber Warfare
- Agenzie per la Cyber Security

Ecosistema della scena «Hacker»

Flussi di interazione



Ecosistema della scena «Hacker»
Gli stereotipi



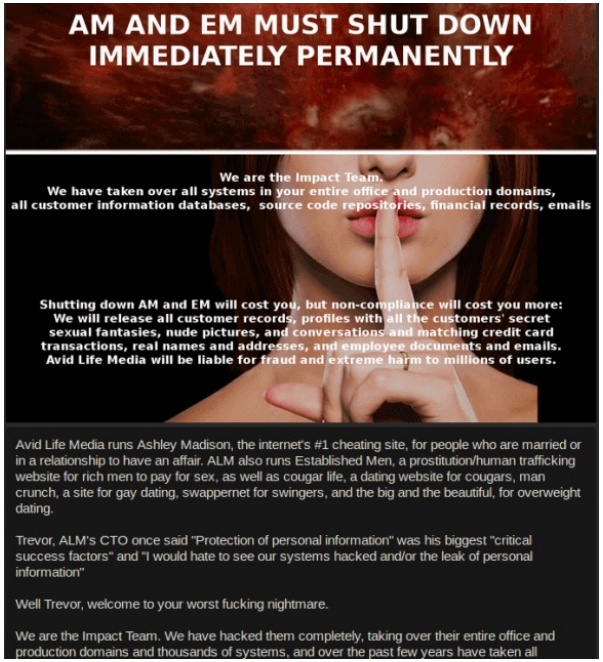

[*] HACKED BY ISLAMIC STATE [*]
لا إله إلا الله
[!] HaCkeD By H4x0rWay
Provincia di Lucca STAMPED by TeaM RaTHacK
Iraq is the Cemetery of Italy ...
hello to the death that awaits you at the hands of the Muiahideen in Iraq
الله رسول محمد
[*] HACKED BY ISLAMIC STATE [*]
[+] Hacked By Shanla.Junianantha404 ![+]
[-] Want To Tell You, If There Is No Perfect [-]
[-] RaUrus Cr3w [-]
[Emperor Security Team]
wGet Abdellah Elmaghribi !
Hacked By Mr.PERSIA
CYBER71
WE HACK TO PROTECT
BANGLADESH
Italiani l33t H4x0r w4s h3r3
Hacked by Islamic State (ISIS)
We Love IRAN
Muslim's H4Cker !


TAKAVAR313.IR
IRAN
SYRIA
Tehran
Tabriz
Rasht
Diyarbakir
Qom
مقام معظم رهبری:
انتقام سختی در انتظار جنایتکارانی است که دست پلید خود را به خون شهید سلیمانی و دیگر شهدای حادثه‌ی دیشب آلودند. او چهره‌ی بین المللی مقاومت است و همه‌ی دلبستگان مقاومت خونخواه اویند.
The Leader of the Revolution reiterated
Martyrdom was his (Shahid Soleymani) reward for years of implacable efforts. With his departure and with God's power, his work and path will not cease and severe revenge awaits those criminals who have tainted their filthy hands with his blood and the blood of the other martyrs of last night's incident
© FDLP


Hacked By IRANIAN HACKER
Mrb3hz4d - Rastin Soleimani
hackedbymrb3hz4d@gmail.com
Telegram: [@ZetaTech_iR2]
Instagram: [@Mrb3hz4d]
Down with America


Contact
Search:
HOME
THE SPANISH PRESIDENCY
AGENDA
DOCUMENTS & NEWS
THE EUROPEAN UNION
You are here : Home
The Spanish presidency
Agenda
Documents & News
The European Union
Spain in focus
Press
Galería Multimedia
TOP SEARCHES
Noticia UE Bruselas UE
Política Presidencia Cultura
Política Cultura
Resultados de búsqueda
¡¡ No se han encontrado Resultados !!
Error
org.opencms.search.CmsSearchException: Búsqueda de "query:[
] fields:[meta, content] sort:[default]" fallida.


Bitcoin, eh? Never heard of it. But perchance you would like to try something better. Something with more "zing". Something named CosbyCoin!
Continue =>
crash.. Holding my Cosbycoin.
bitjet 2 333 Today at 07:33:43 pm by kjj
WiseOldOwl 9 402 Today at 07:32:21 pm by ShadowOfHarbringer
tform to Mt Gox. Anybody interested? « 1
4xCoder 24 1564 Today at 07:32:20 pm by AlexZ
mizerydearia 17 562 Today at 07:19:34 pm by ssaCEO
cryptofo 17 1501 Today at 06:58:32 pm by enmaku

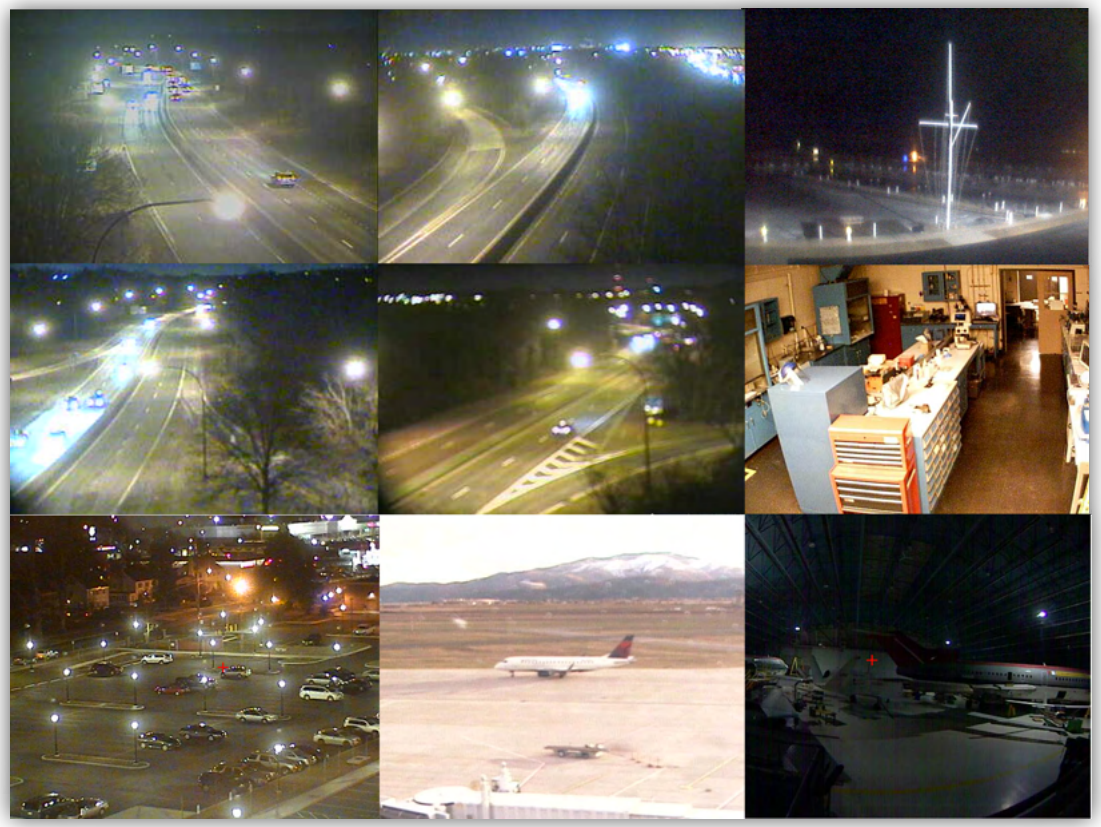

AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY
We are the Impact Team.
We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails
Shutting down AM and EM will cost you, but non-compliance will cost you more: We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails. Avid Life Media will be liable for fraud and extreme harm to millions of users.
Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.
Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"
Well Trevor, welcome to your worst fucking nightmare.
We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

Convergenza degli attacchi

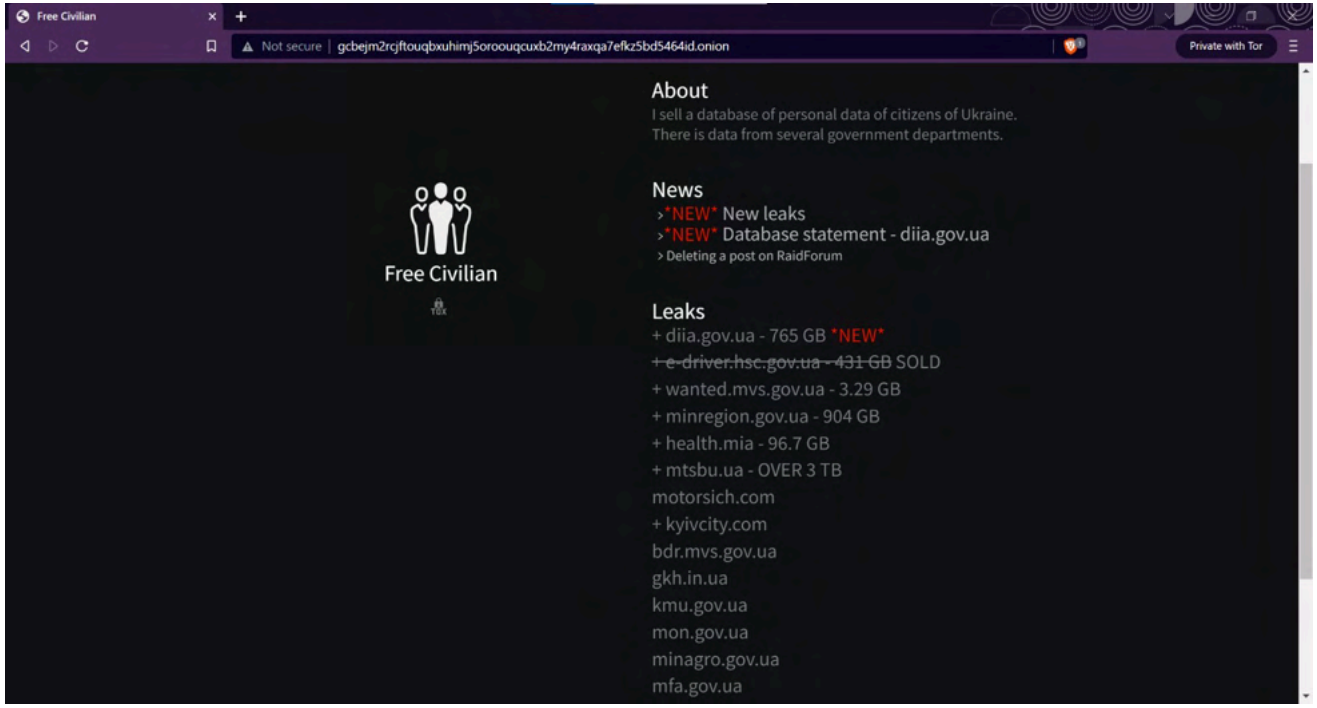
dalla rete al mondo reale

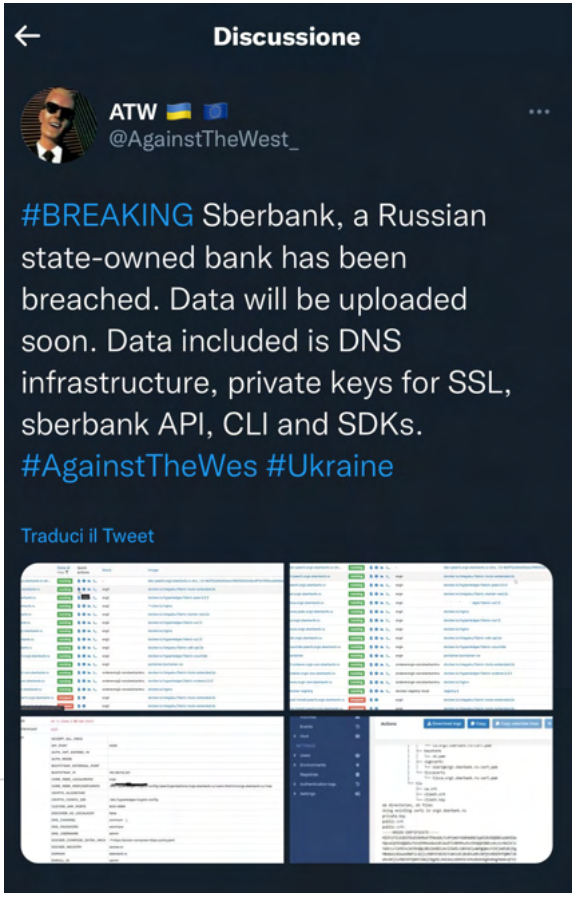
- Infrastrutture di trasporto
- Laboratori di ricerca
- Luoghi pubblici
- Luoghi di aggregazione

E se un attacker ne abusasse ?



Convergenza degli attacchi
Cyber criminalità





"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 39 0 [0.00 B]

Convergenza degli attacchi
Cyber criminalità

GROUP	SUPPORTING	ATTACKS	COMMS	LOC	DATE STARTED
AgainstTheWest	Ukraine	Data Breach/Ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	2022
GhostSec	Ukraine	Hack	Telegram	UNK	2022
IT Army of Ukraine	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
KelvinSecurity HackingTeam	Ukraine	Hack	Telegram	UNK	2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	2022
Anon Liberland & PWN-BAR	Ukraine	DDoS	Twitter	UNK	2022
RaidForums Admin	Ukraine	Sanction	Raidforums	UNK	2022
Netsec	UNK	Hack	Twitter	UNK	2022
Free Civilian	Russia	Data Breach	Onion	UNK	2022
CoomingProject	Russia	Data Breach	Onion	France	2022
Conti Ransomware Gang	Russia	Ransomware	Onion	Global	2022
The Red Bandits	Russia	Data Breach/Hack	Twitter	Russia	2022
CyberGhost	Russia	Hack/Disinformation	UNK	Belarus	UNK
SandWorm	Russia	Hack/DDoS/Disinformation	UNK	Russia	UNK
Gamaredon	Russia	Hack	UNK	Russia	UNK
28-Feb					
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
RaidForums2	Ukraine	DDoS	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hack/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hack/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belarus	Hack	Twitter	Global	2022
1-Mar					
Root User	Ukraine	Radio	Twitter	Ukraine	2022
DeepNetAnon	Ukraine	Radio	Twitter	UNK	2022
FreeUkraineNow	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
1LevelCrew	Ukraine	DDoS	Twitter	UNK	2022
IT Army of Ukraine Psyops	Ukraine	Disinformation	Twitter	Ukraine	2022
Hydra UG	Ukraine	Radio/data breach	Twitter	UNK	2022
Zatoichi	Russia	Disinformation	Twitter	Russia	2022
Stormous Ransomware	Russia	Ransomware	Telegram	UNK	2022

\Molte persone ci chiedono, la nostra comunità internazionale di pentester post-pagati minaccerà l'Occidente su infrastrutture critiche in risposta all'aggressione informatica contro la Russia?
La nostra comunità è composta da molte nazionalità del mondo, la maggior parte dei nostri pentester sono residenti nella CSI, inclusi russi e ucraini, ma ci sono anche americani, britannici, cinesi, francesi, arabi, ebrei e molti altri nella nostra squadra. I nostri programmatori e sviluppatori vivono stabilmente in diversi paesi del mondo in Cina, USA, Canada, Russia e Svizzera. I nostri server si trovano nei Paesi Bassi e alle Seychelles, siamo tutti persone semplici e pacifiche, siamo tutti terrestri.
Per noi sono solo affari e siamo tutti apolitici. Ci interessa solo il denaro per il nostro lavoro innocuo e utile. Conduciamo solo una formazione retribuita per gli amministratori di sistema di tutto il mondo su come configurare correttamente una rete aziendale. Non prenderemo mai parte, in nessun caso, ad attacchi informatici alle infrastrutture critiche di nessun Paese del mondo e entreremo in qualsiasi conflitto internazionale.)

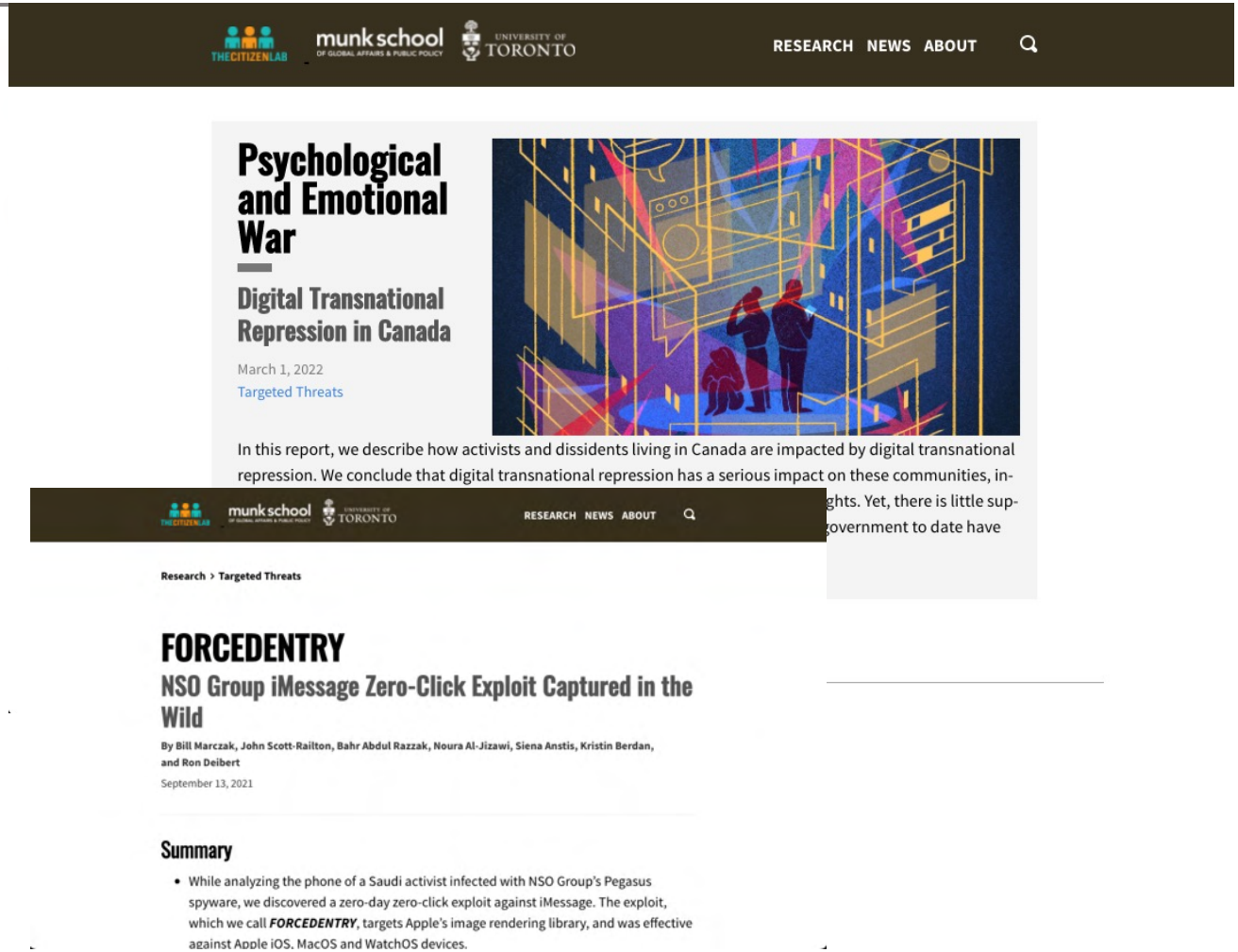
Convergenza degli attacchi

Dalla mondo reale alla rete

Ballando con ... #TANGODOWN

Convergenza degli attacchi

Quale di queste pratiche possiamo oggi considerare Hacktivism?




GLOBAL CYBERNUCLEAR WARFARE!

Guerra cybernucleare globale
Le ragioni dell'insicurezza

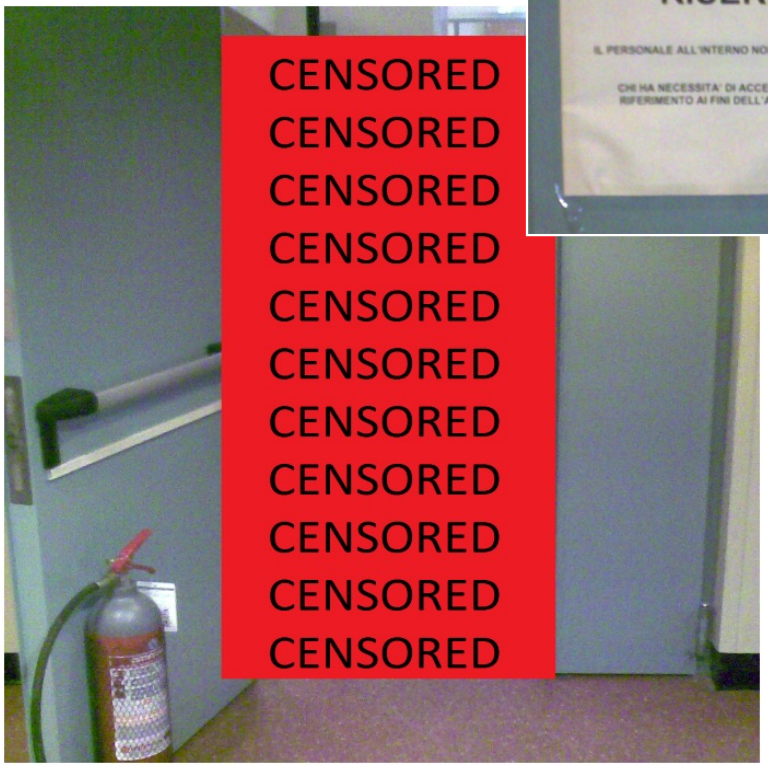
- Il software ed i sistemi sono intrinsecamente insicuri
  - Priorità al time to market
- Le aziende acquisiscono tecnologie fidandosi delle brochure
- Il «landscape» dei vendor è sempre più ampio
- Il budget scarso determina l'acquisizione di tecnologie a basso costo
- Le competenze degli addetti ai lavori sono inadeguate (skill shortage, procedure per le patch lentissime, il cloud)
- Stratificazione delle tecnologie (dagli anni '90 ad oggi)
- Gli utenti sono diventati il target principale attraverso cui si arriva sui sistemi
  - Because there is no patch to human stupidity

Vulnerabilità più frequenti durante i nostri Penetration Test (TOP 5)

1. Cred-WK (Credenziali deboli)
2. Auth-WK (Sistemi di autenticazione deboli)
3. ABU-F (Abuse of functionality)
4. IN-WK (XSS Cross Site Script)
5. IV-WK (SQL Injection)

Advanced Persistent Threat

Non aprite quella porta … ooops!



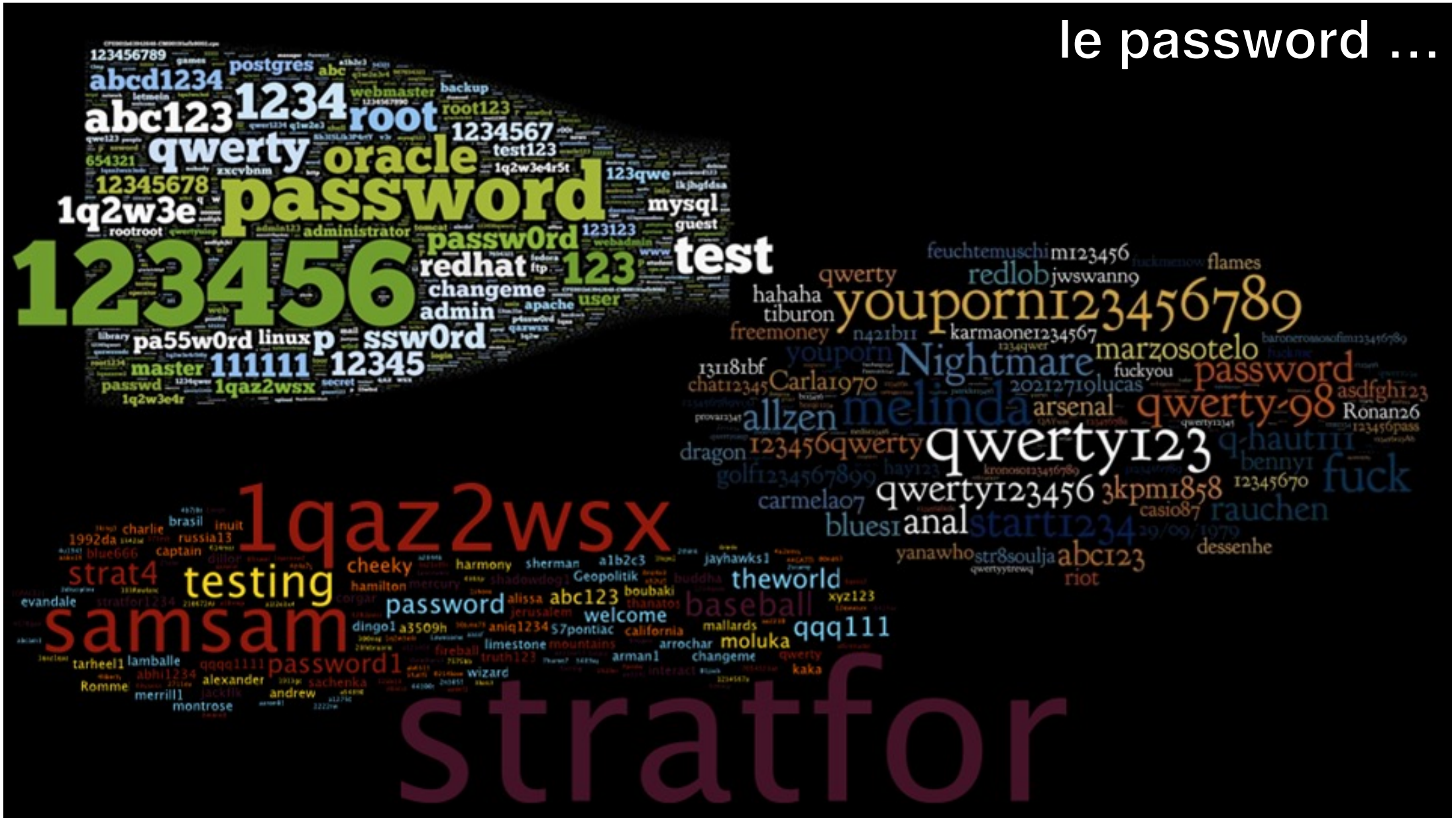
Advanced Persistent Threat

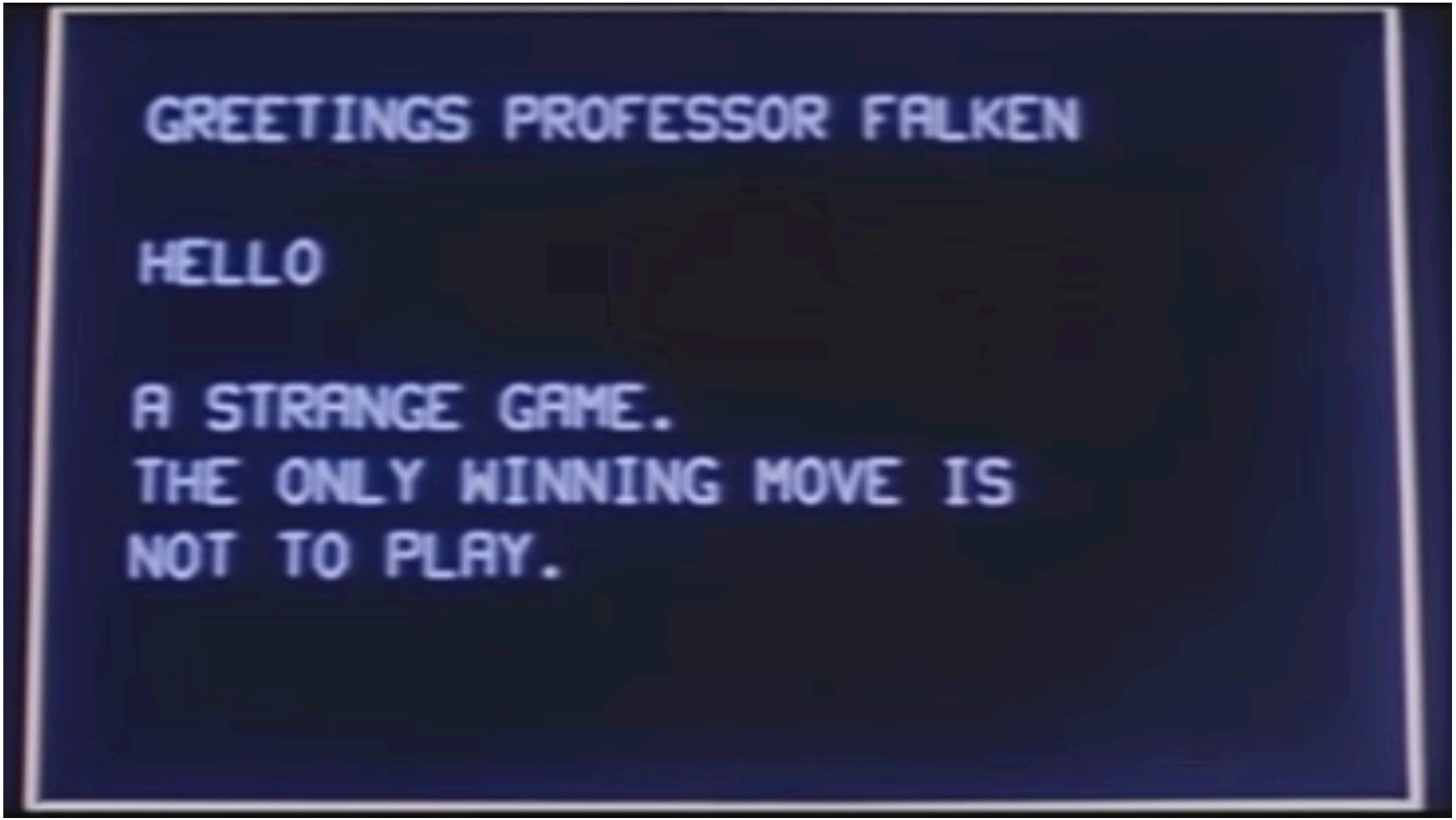
Plug & PWN

```
root@Phear:~# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:c0:b7:67:29:54
          inet6 addr: fe80::2c0:b7ff:fe67:2954/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5130 (5.1 KB)  TX bytes:3224 (3.2 KB)
          Interrupt:19 Base address:0xd020

root@Phear:~# mii-tool eth2
eth2: negotiated 100baseTx-FD, link ok
root@Phear:~#
```

le password ...


123456789
postgres
abcd1234
1234
webmaster
backup
abc123
root
root123
1234567
qwerty
oracle
test123
654321
xxcvbnm
1q2w3e4r5t
123qwe
12345678
password
1q2w3e
mysql
rootroot
administrator
123123
guest
passw0rd
123456
redhat
123
test
changeme
admin
apache
user
pa55w0rd
linux
p
ssw0rd
master
111111
12345
passwd
1qaz2wsx
secret
1q2w3e4r
feuchtemuschi
m123456
flames
qwerty
redlob
jwswann9
hahaha
tiburon
youporn123456789
freemoney
n421b11
karmaone1234567
youporn
Nightmare
marzosotelo
131181bf
fuckyou
password
chat12345
Carla1970
202127 19lucas
asdfgh123
melinda
arsenal
qwerty-98
allzen
Ronan26
dragon
123456qwerty
qwerty123
fuck
golf12345678 99
qwerty123456
3kpm1858
12345670
carmela07
casio87
rauchen
blues1
anal
start1234
29/09/1979
dessenhe
yanawho
str8soulja
abc123
riot
1qaz2wsx
brasil
inuit
charlie
1992da
russia13
blue666
captain
strat4
testing
cheeky
harmony
sherman
a1b2c3
jayhawks1
Geopolitik
theworld
hamilton
password
alissa
abc123
boubaki
baseball
xyz123
evandale
samsam
welcome
dingo1
a3509h
aniq1234
57pontiac
california
mallards
qqq111
limestone
mountains
arrochar
moluka
tarheel1
lamballe
qqqq1111
password1
abhi1234
alexander
arman1
changeme
qwerty
kaka
wizard
Romme
merrill1
andrew
montrose
stratfor


GREETINGS PROFESSOR FALKEN
HELLO
A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.