Unternehmen im Visier von Cyberkriminellen

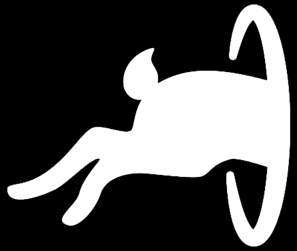
Ivano Somaini, Compass Security Schweiz AG

Unternehmen im Visier von Cyberkriminellen

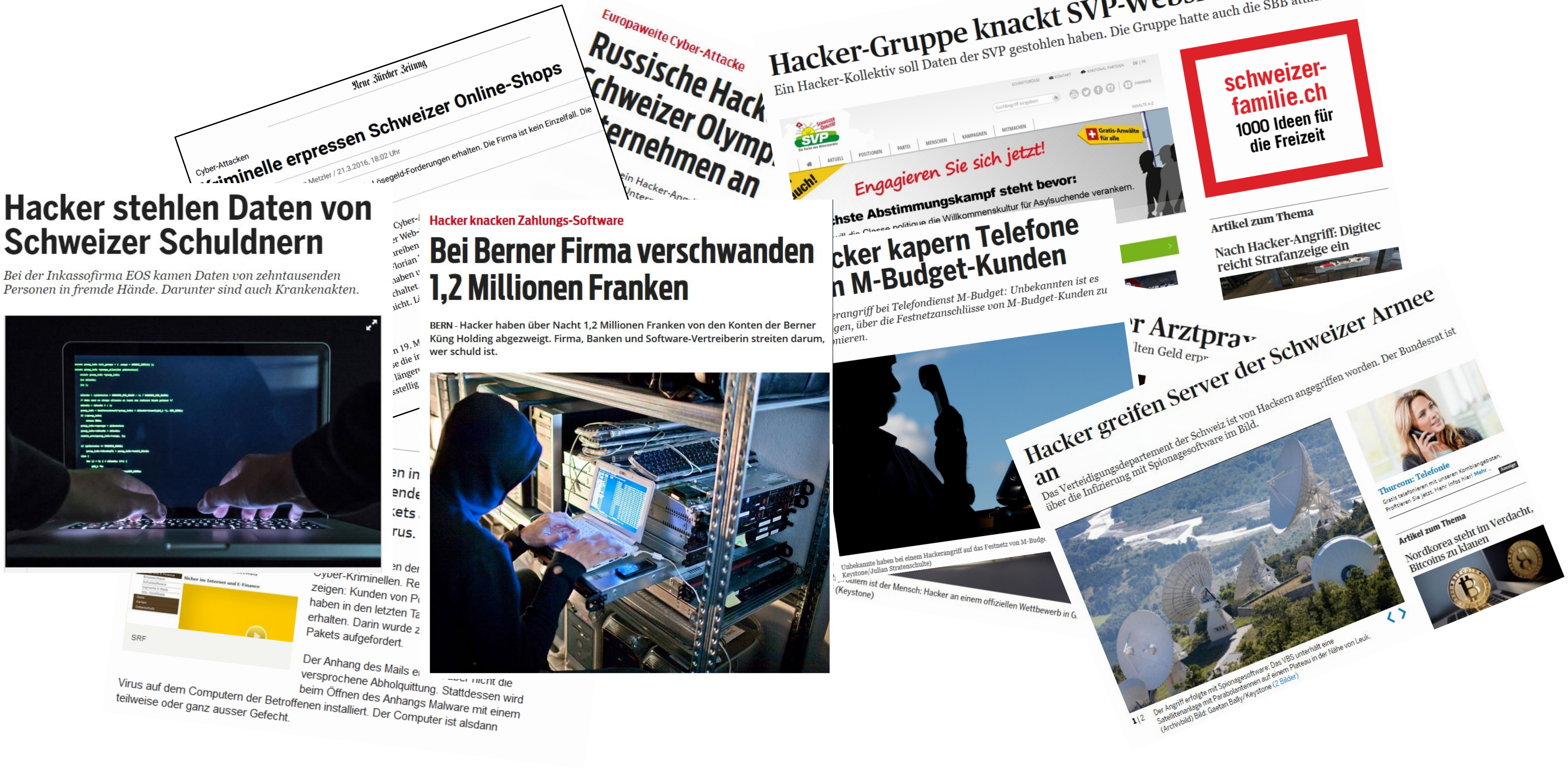
Live Hacking Demo

Ivano Somaini, Regional Manager Zürich
Compass Security Schweiz AG

FOLLOW THE WHITE RABBIT



Cybercrime is Here and Now!



Neue Zürcher Zeitung

Cyber-Attacken

Kriminelle erpressen Schweizer Online-Shops

Metzler / 21.3.2016, 18:02 Uhr

Lösegeld-Forderungen erhalten. Die Firma ist kein Einzelfall. Die

Europaweite Cyber-Attacke

Russische Hack
Schweizer Olymp
ternehmen an

ein Hacker-Ang
Untern

Hacker-Gruppe knackt SVP-Website

Ein Hacker-Kollektiv soll Daten der SVP gestohlen haben. Die Gruppe hatte auch die SBB attackiert.

Artikel zum Thema

Nach Hacker-Angriff: Digitec reicht Strafanzeige ein

Hacker stehlen Daten von Schweizer Schuldnern

Bei der Inkassofirma EOS kamen Daten von zehntausenden Personen in fremde Hände. Darunter sind auch Krankenakten.

Cyber-
er Web-
reiben
Florian
haben v
chaltet.
nicht. L

n 19. M
se die i
länger
sstellig

en in
ende
kets
rus.

en der
Cyber-Kriminellen. Re
zeigen: Kunden von P
haben in den letzten Ta
erhalten. Darin wurde z
Pakets aufgefordert.

Der Anhang des Mails e
versprochene Abholquittung. Stattdessen wird
beim Öffnen des Anhangs Malware mit einem
Virus auf dem Computern der Betroffenen installiert. Der Computer ist alsdann
teilweise oder ganz ausser Gefecht.

Hacker knacken Zahlungs-Software

Bei Berner Firma verschwanden 1,2 Millionen Franken

BERN - Hacker haben über Nacht 1,2 Millionen Franken von den Konten der Berner Küng Holding abgezweigt. Firma, Banken und Software-Vertreiberin streiten darum, wer schuld ist.

cker kapern Telefone
n M-Budget-Kunden

erangriff bei Telefondienst M-Budget: Unbekannten ist es
gen, über die Festnetzanschlüsse von M-Budget-Kunden zu
nieren.

Unbekannte haben bei einem Hackerangriff auf das Festnetz von M-Budge
Keystone/Julian Stratenschulte)

oblem ist der Mensch: Hacker an einem offiziellen Wettbewerb in G
(Keystone)

r Arztpra
lten Geld erp

Hacker greifen Server der Schweizer Armee an

Das Verteidigungsdepartement der Schweiz ist von Hackern angegriffen worden. Der Bundesrat ist über die Infizierung mit Spionagesoftware im Bild.

1 | 2 Der Angriff erfolgte mit Spionagesoftware: Das VBS unterhält eine Satellitenanlage mit Parabolantennen auf einem Plateau in der Nähe von Leuk. (Archivbild) Bild: Gaetan Bally/Keystone (2 Bilder)

Artikel zum Thema

Nordkorea steht im Verdacht, Bitcoins zu klauen

PROFIT

— HACKERS —

$ 445’000’000’000

Who are the Hackers?

Script-Kiddie / Disgruntled Employee

Age

- 9 – 18 years

Impact

- Low

Motivation / Purpose

- For fashion, it’s cool, to boast and brag
- To give vent of their anger, attract mass-media attention

Black Hat / White Hat

Age

- 15 – 50 years

Impact

- Medium

Motivation / Purpose

- To demonstrate their power, attract mass-media attention
- For curiosity (to learn) and altruistic purposes
- For curiosity (to learn) and egoistic purposes

Organized Crime / Nation State

Age

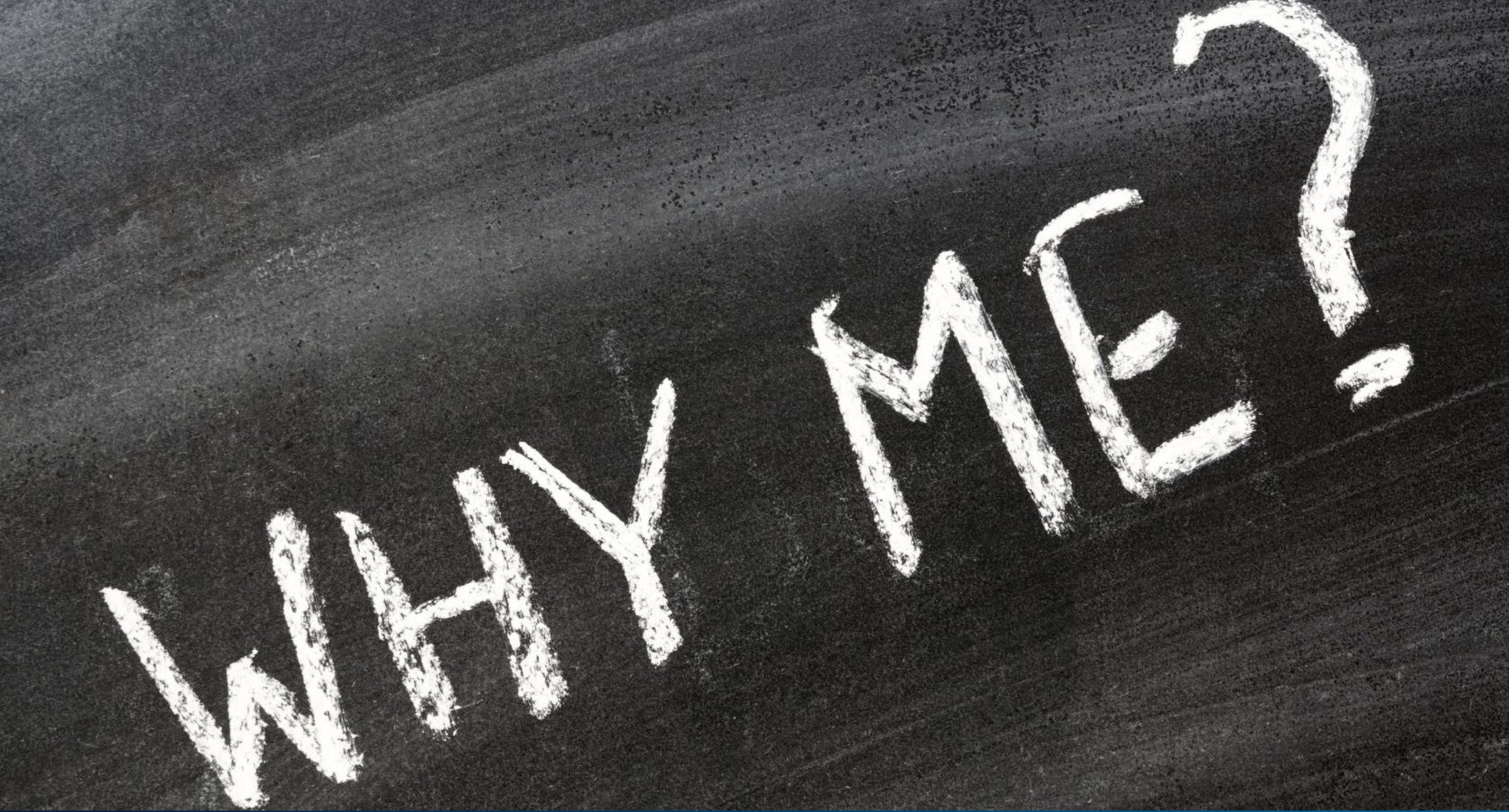
- 18 – 50 years

Impact

- High

Motivation / Purpose

- For profit
- Espionage/Counter-Espionage, Activity-Monitoring
- Monitoring, Controlling, Crashing Enemy Systems



WHY ME?

Why Attack Me?

Untargeted, Mass Attacks

- Random targets
- Weakest victims (e.g. simple passwords)
- E.g. spam, phishing, etc
- Unpatched systems

Targeted Attacks

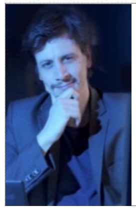
- Efficient
- Usually combined with social engineering
- High success rate

Intermediate Targets

- In the Cross Fire of the attacker and his primary target

Cybercrime Organization

Cybercrime Supply Chain



Organization Leaders

Manage the team and define the goals/targets

Coders

Program the malwares

Hackers

Look for and exploit vulnerabilities in programs and networks

Money Mules

Transfer the money using electronic and/or physical channel

Distributors

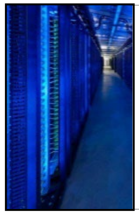
Buy and sell stolen data

Fraudsters

Target potential victims with social engineering techniques like phishing

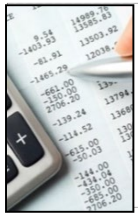
Tellers

Wash the illegal incomes through transfer to digital financial services



Tech Experts

Monitor, repair and grow the infrastructure of the criminal enterprise

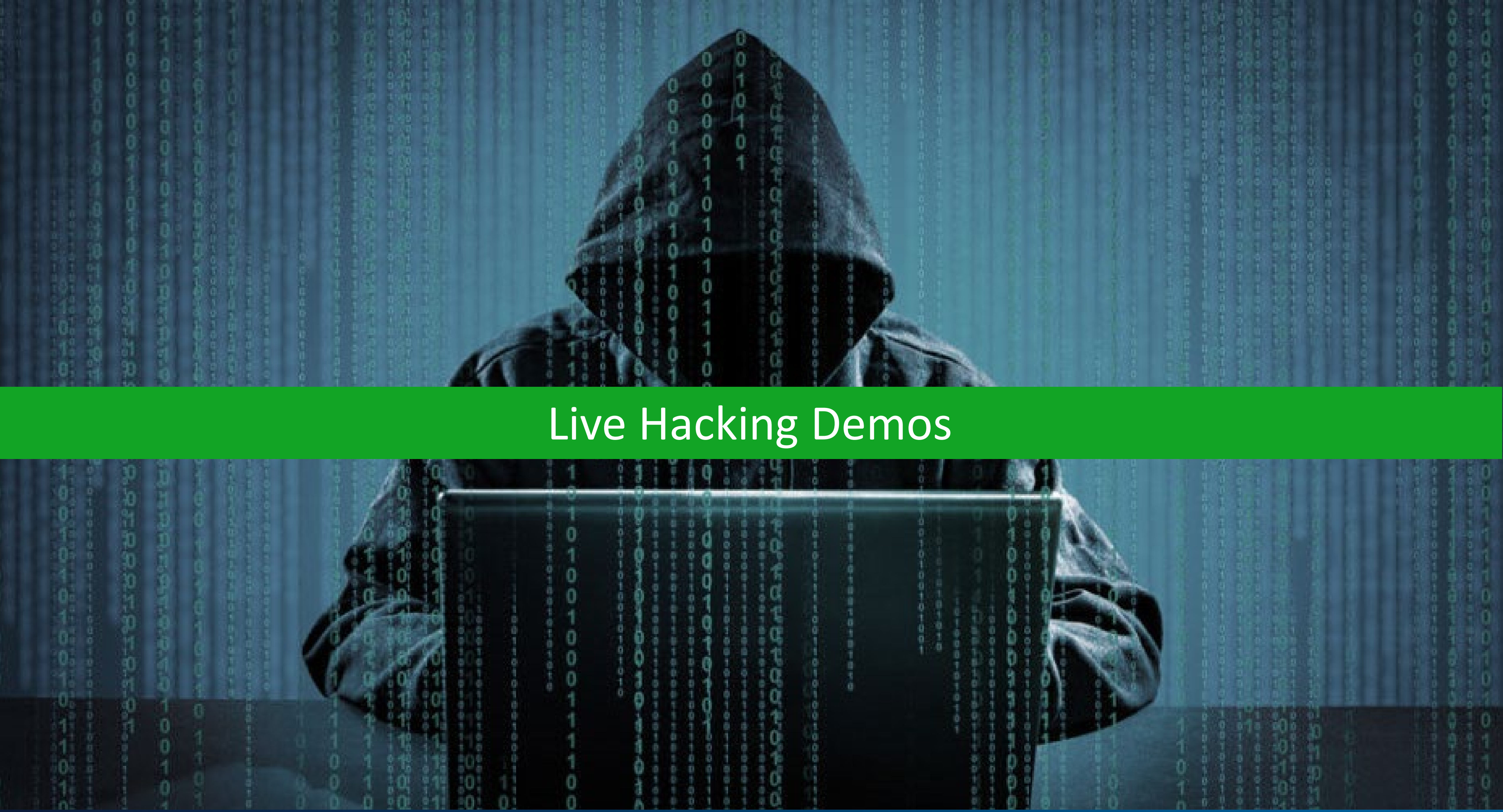


Cashiers

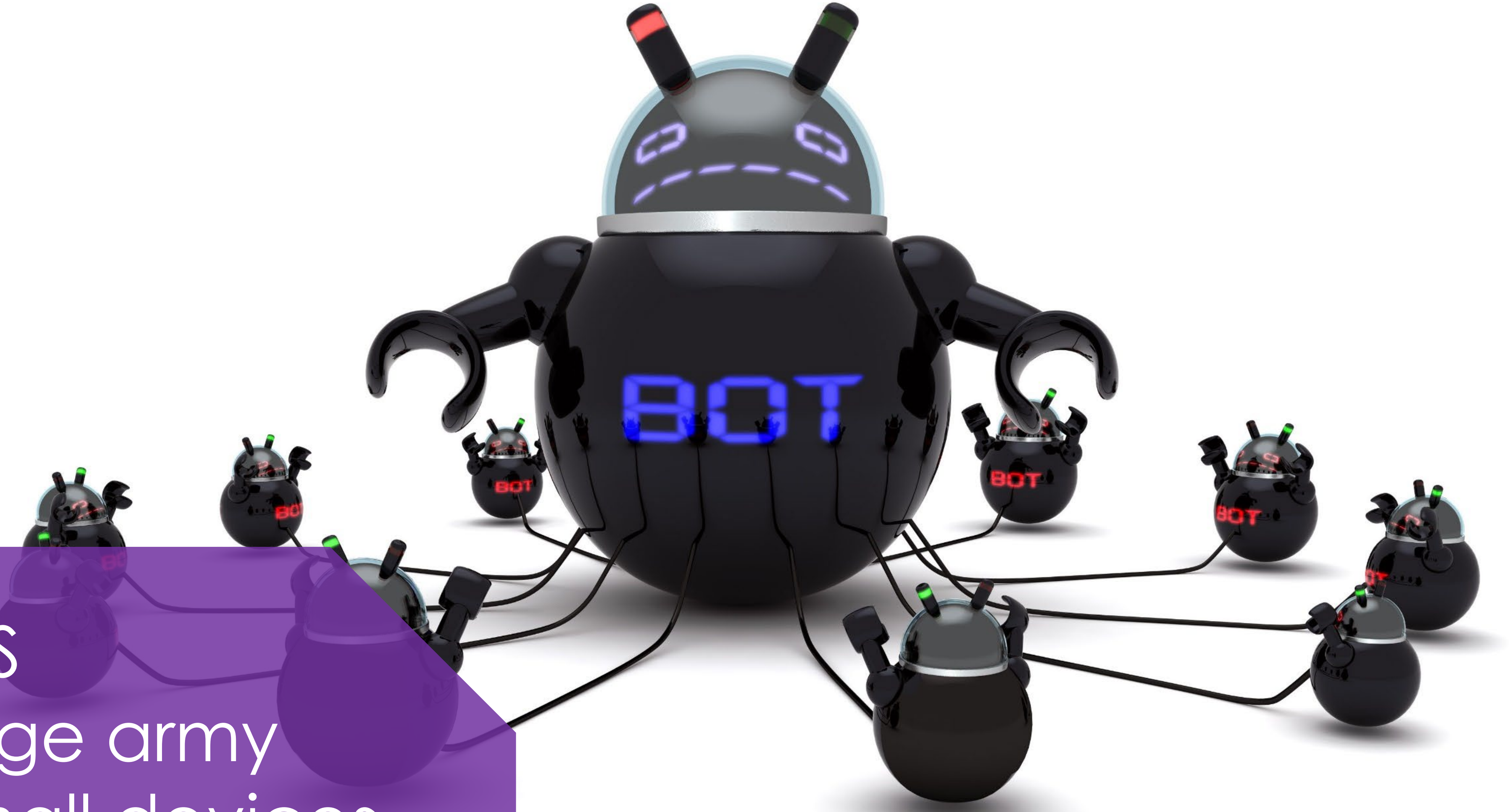
Control the hacked accounts and deliver credentials to other criminals against payment

Hosted System Providers

Host illegal servers

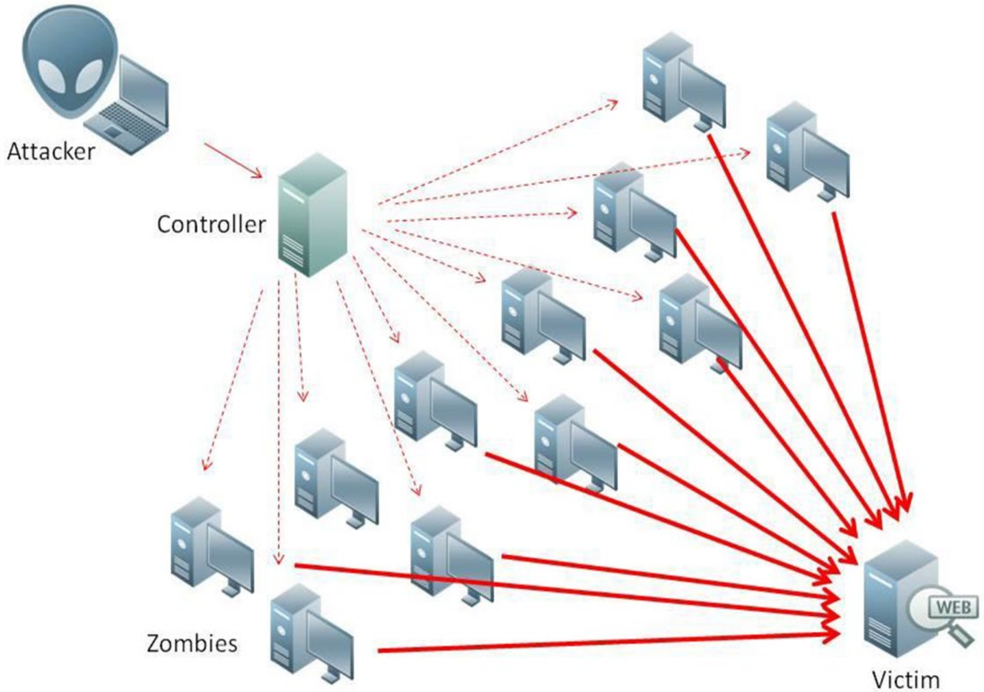


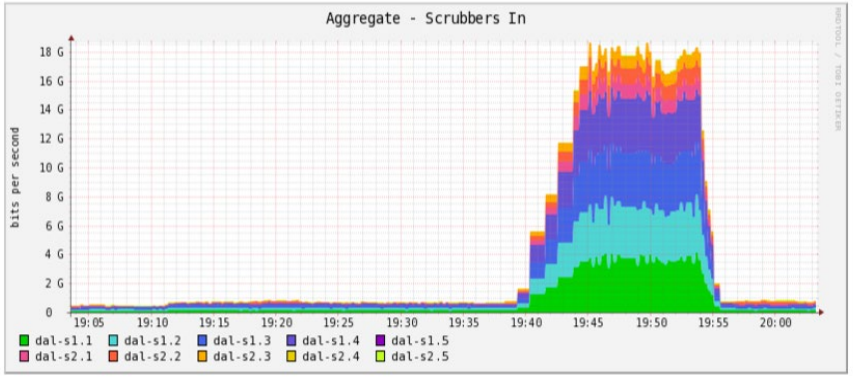
Live Hacking Demos



DDoS
A huge army of small devices

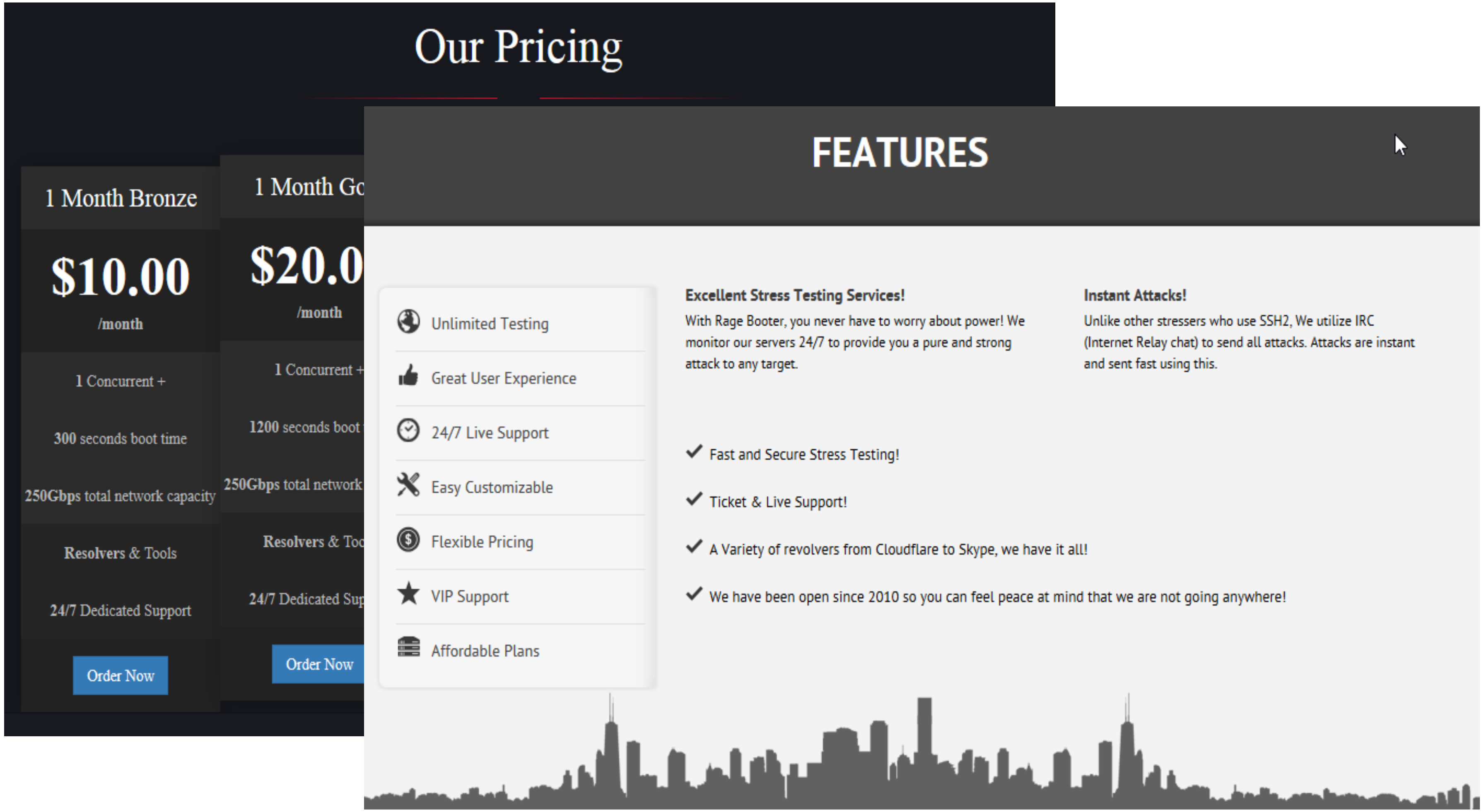
Distributed Denial of Service (DDoS)





Distributed Denial of Service (DDoS)

“Network Stressers”



Our Pricing

1 Month Bronze	1 Month Go
$10.00 /month	$20.0 /month
1 Concurrent +	1 Concurrent +
300 seconds boot time	1200 seconds boot
250Gbps total network capacity	250Gbps total network
Resolvers & Tools	Resolvers & Too
24/7 Dedicated Support	24/7 Dedicated Sup
Order Now	Order Now

FEATURES

- Unlimited Testing
- Great User Experience
- 24/7 Live Support
- Easy Customizable
- Flexible Pricing
- VIP Support
- Affordable Plans

Excellent Stress Testing Services!
With Rage Booter, you never have to worry about power! We monitor our servers 24/7 to provide you a pure and strong attack to any target.

Instant Attacks!
Unlike other stressers who use SSH2, We utilize IRC (Internet Relay chat) to send all attacks. Attacks are instant and sent fast using this.

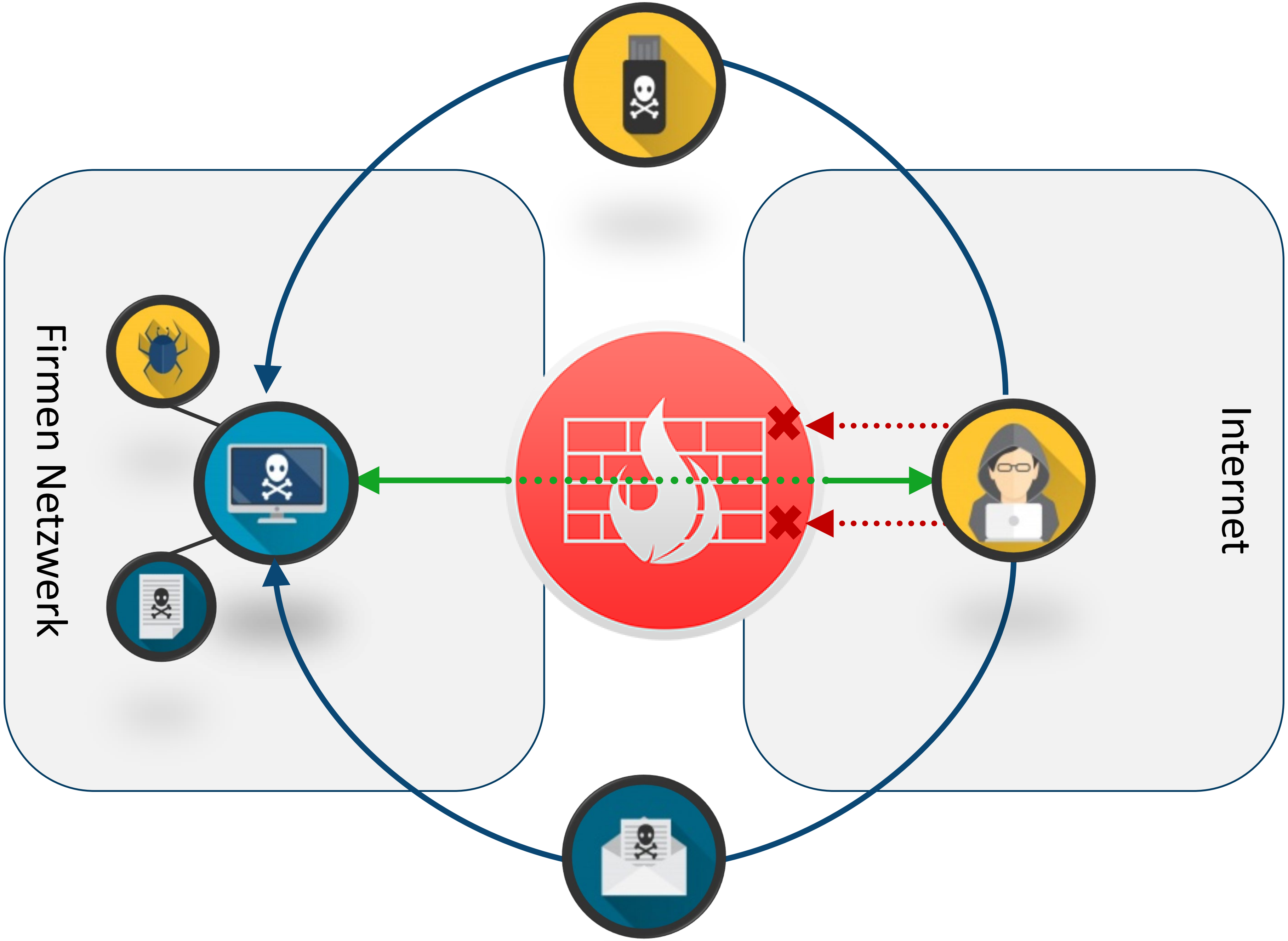
✓ Fast and Secure Stress Testing!

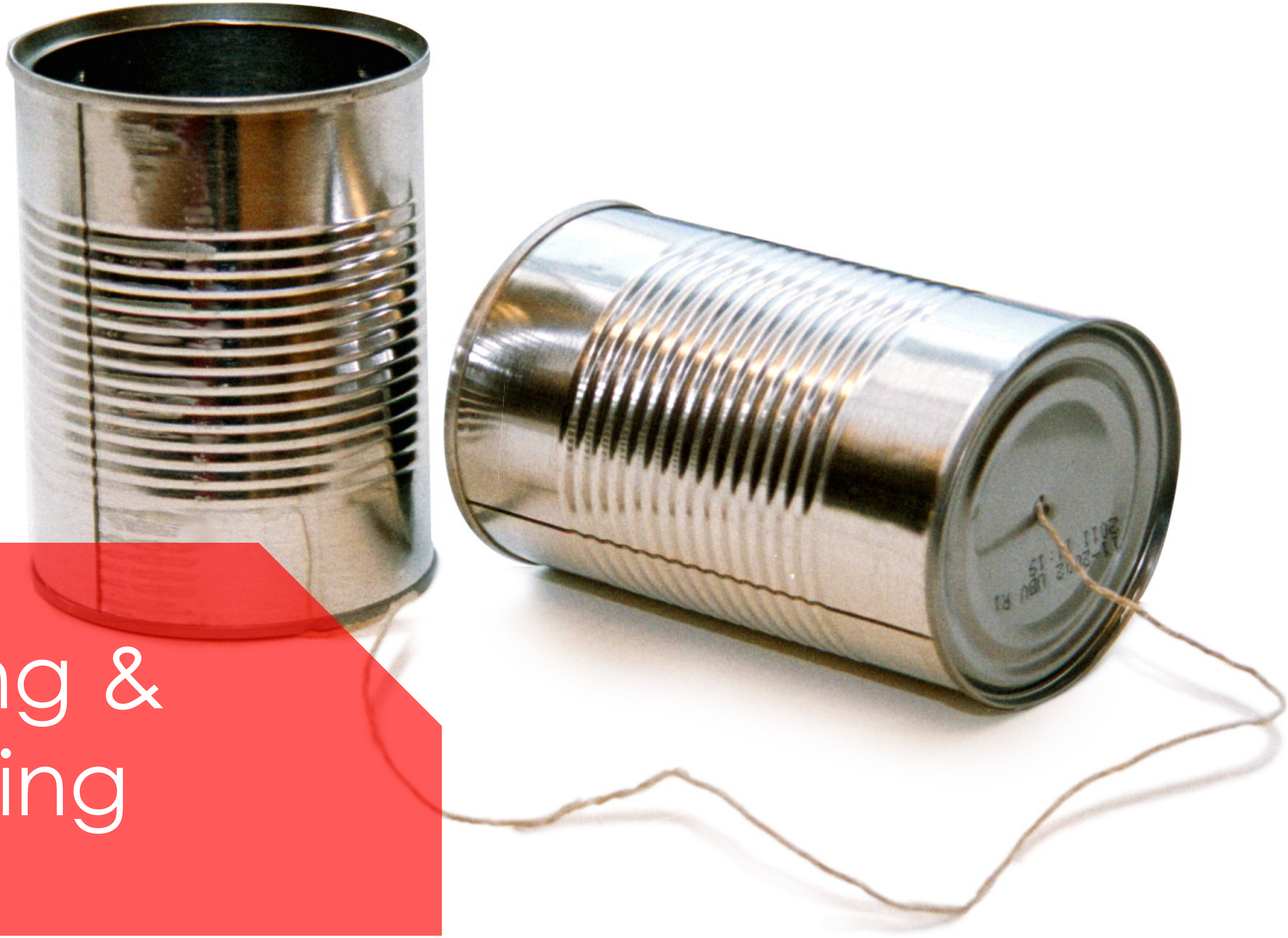
✓ Ticket & Live Support!

✓ A Variety of revolvers from Cloudflare to Skype, we have it all!

✓ We have been open since 2010 so you can feel peace at mind that we are not going anywhere!

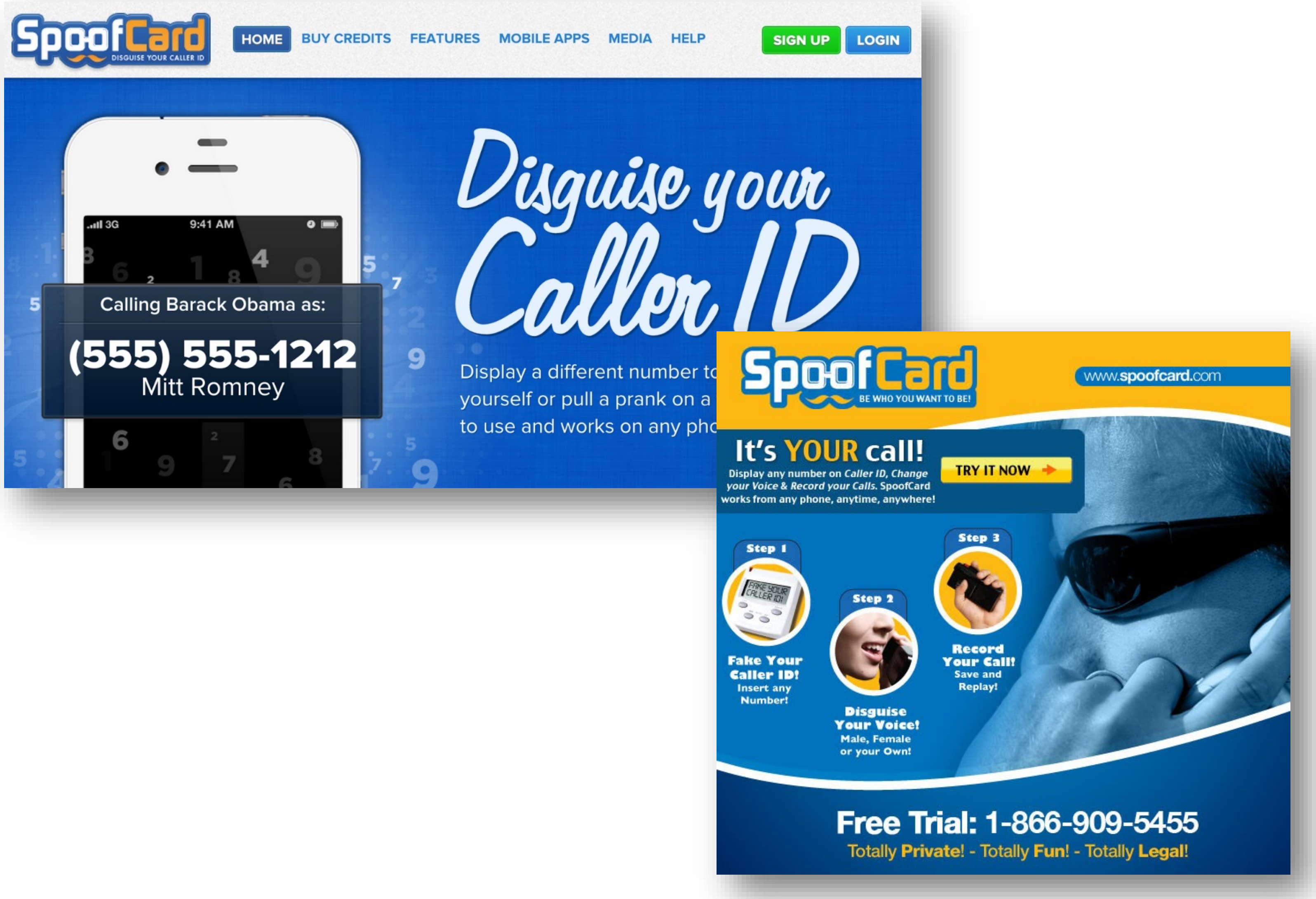
“Lost” USB Stick


Firmen Netzwerk
Internet



Vishing & SMShing

Caller ID Spoofing


SpoofCard
DISGUISE YOUR CALLER ID
HOME
BUY CREDITS
FEATURES
MOBILE APPS
MEDIA
HELP
SIGN UP
LOGIN
3G 9:41 AM
Calling Barack Obama as:
(555) 555-1212
Mitt Romney
Disguise your Caller ID
Display a different number to
yourself or pull a prank on a
to use and works on any pho
SpoofCard
BE WHO YOU WANT TO BE!
www.spoofcard.com
It's YOUR call!
Display any number on Caller ID, Change your Voice & Record your Calls. SpoofCard works from any phone, anytime, anywhere!
TRY IT NOW
Step 1
FAKE YOUR CALLER ID!
Fake Your Caller ID! Insert any Number!
Step 2
Disguise Your Voice! Male, Female or your Own!
Step 3
Record Your Call! Save and Replay!
Free Trial: 1-866-909-5455
Totally Private! - Totally Fun! - Totally Legal!

Countermeasure

Prevention for enterprises

- Raise awareness about security and computer threats in the enterprise
- Teach collaborators through an internal security course
- Establish clear guidelines for social medias
- Encrypt sensitive data
- Keep the protection systems for hard- and software up to date
- Enforce good practices for passwords
- Backup your data

Prevention for individuals

- Different password for each online service
- Use a password manager
- Update your software on a regular basis (OS, browser , Java, Flash, …)
- Use a recent and up-to-date antivirus
- Be careful with every incoming email (Phishing?)
- Don’t blindly trust the sender of E-Mail, SMS, whatsapp, etc…
- Backup your data

CONCLUSIONS
A.
B.

Cybercrime is highly organized

and

profit oriented

They will go after easy and profitable target

Don’t be the low-hanging fruit!

COMPASS
SECURITY