radware

Every second counts

The Current Economics of Cyber Attacks

Ron Winward

Security Evangelist

October 17, 2016

What Are We Talking About

Historical Context

Does Hacking Pay?

Cyber Attack Marketplace

Economics of Defenses: Reality Check

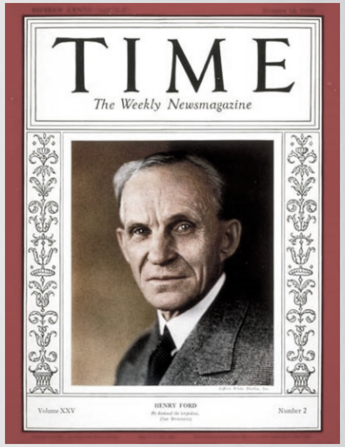
Once Upon a Time…

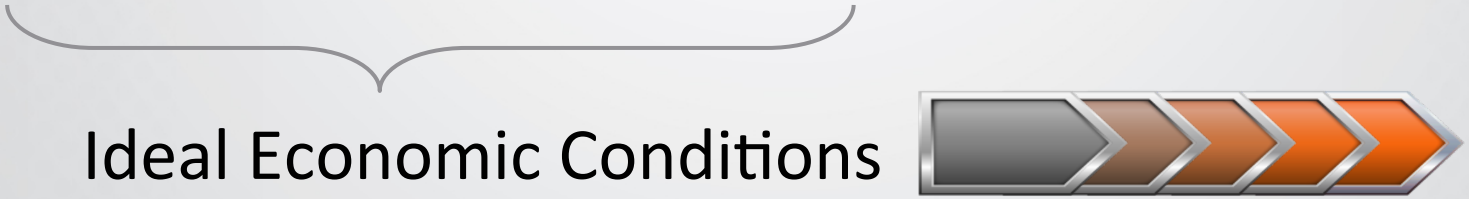
Story of the Automobile

Ideal economic conditions help fuel and grow this industry

Better Roads

Assembly Line





Ideal Economic Conditions

Growth

Cyber Attacks Reaching a Tipping Point

More Resources

Availability of low cost resources

More Targets

More high value, increasingly vulnerable targets leads to more valuable information

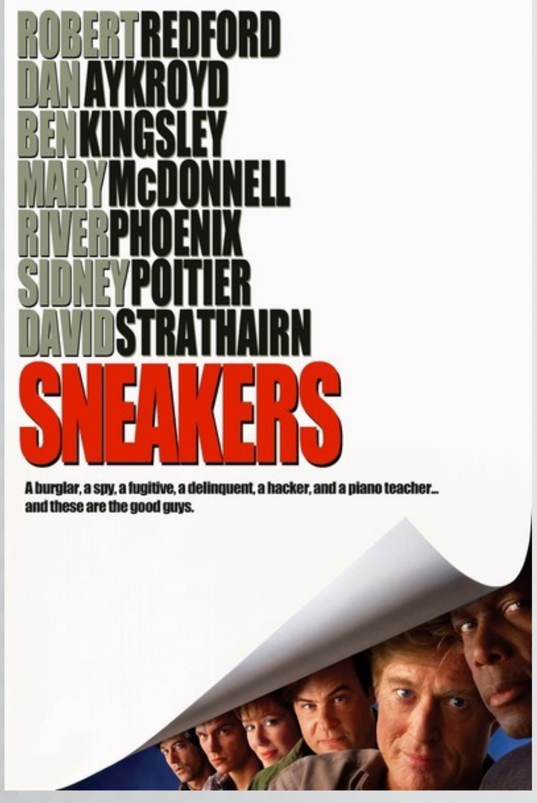
More Mature

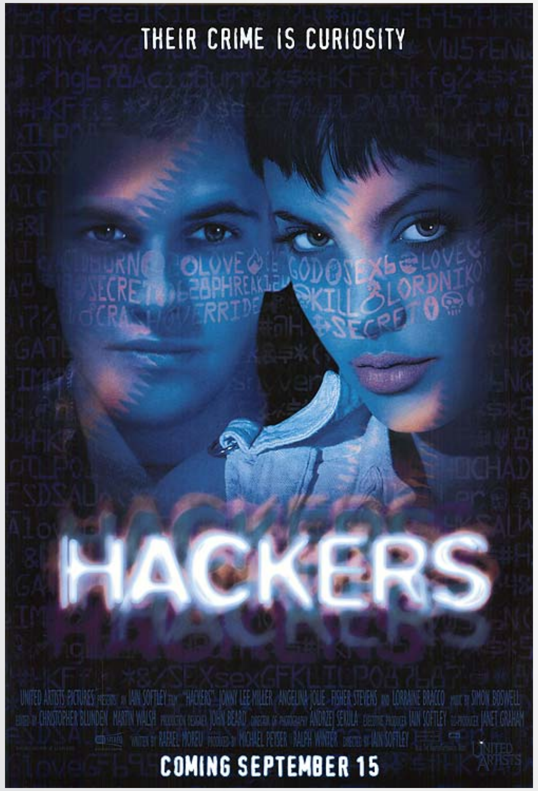
A level of maturity that drives efficiency and ensures anonymity

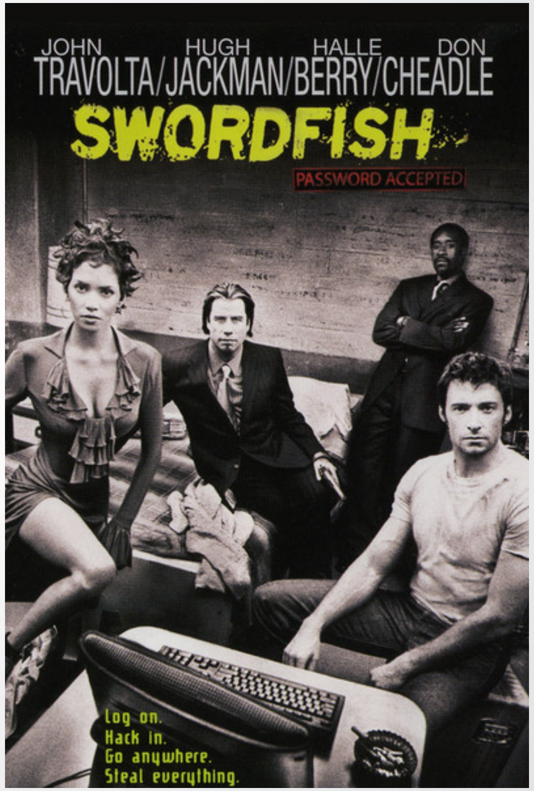
The economics of hacking have turned a corner!

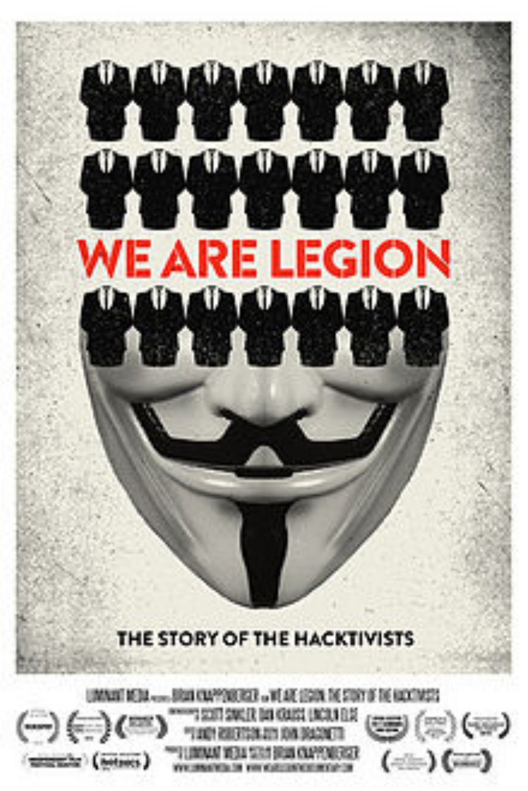
Modern Economics of Cyber Attacks and Hacking

Do You Romanticize Hackers?


ROBERT REDFORD
DAN AYKROYD
BEN KINGSLEY
MARY McDONNELL
RIVER PHOENIX
SIDNEY POITIER
DAVID STRATHAIRN
SNEAKERS
A burglar, a spy, a fugitive, a delinquent, a hacker, and a piano teacher...
and these are the good guys.







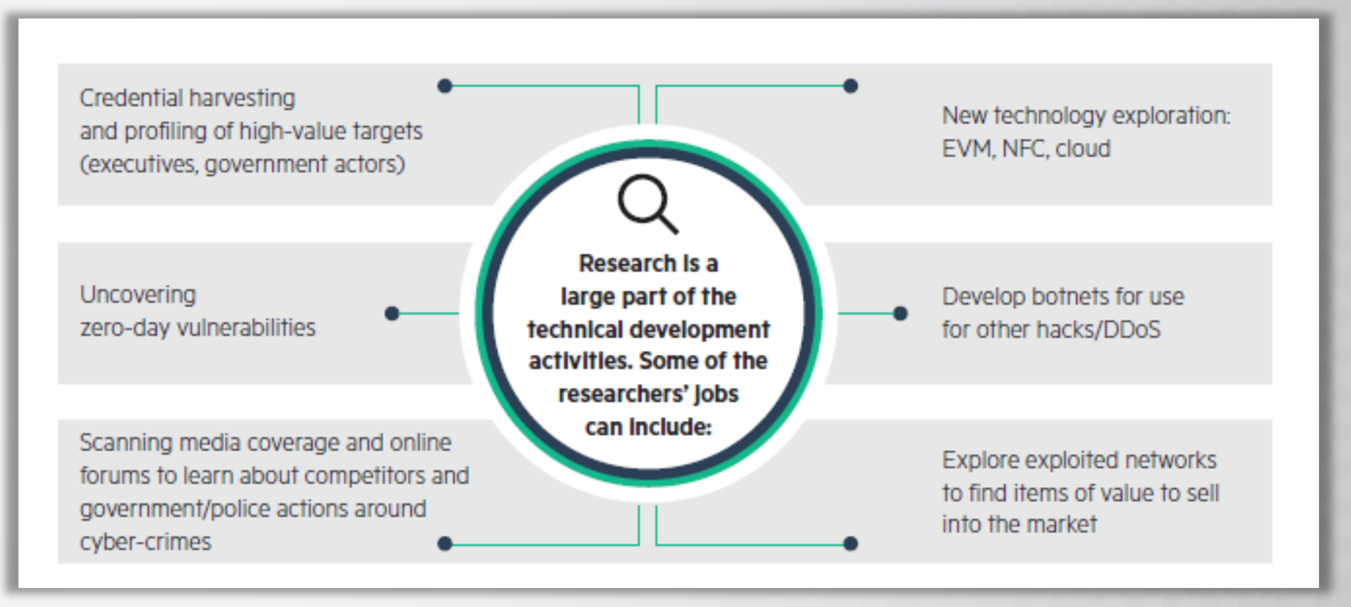
Reality of Today’s Hackers

May look more like this . . .

. . . than like this

Today's Adversary: Not always the Lone Wolf

- Structured organization with roles, focus
- Premeditated plan for targeting, exfiltration, monetization of data/assets
- Multi-layered trading networks for distribution, obfuscation



Research is a large part of the technical development activities. Some of the researchers' jobs can include:

Credential harvesting and profiling of high-value targets (executives, government actors)

Uncovering zero-day vulnerabilities

Scanning media coverage and online forums to learn about competitors and government/police actions around cyber-crimes

New technology exploration: EVM, NFC, cloud

Develop botnets for use for other hacks/DDoS

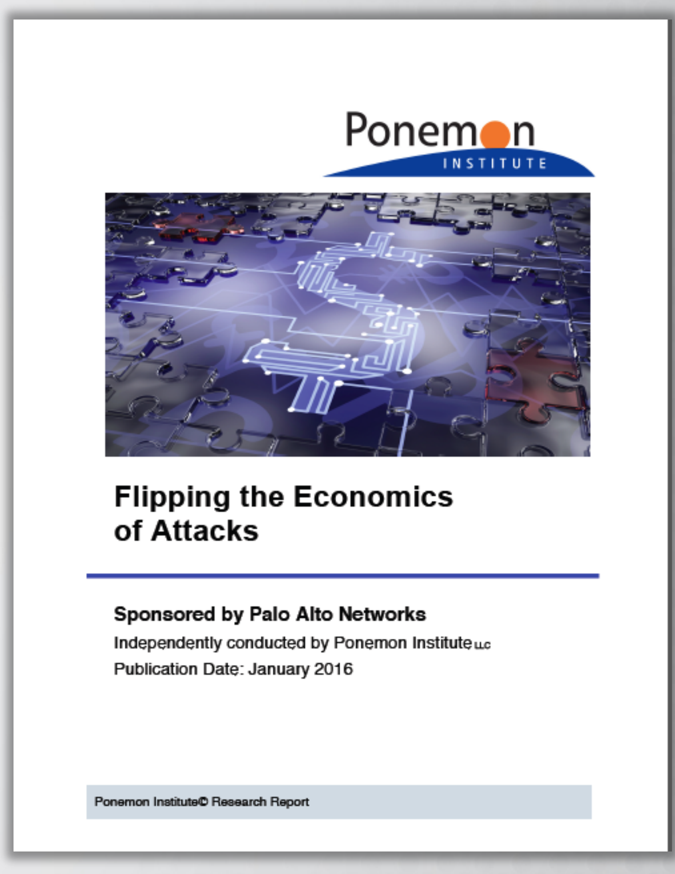
Explore exploited networks to find items of value to sell into the market

Source: HPE: the business of hacking

Why? Because increasingly, CRIME PAYS!

Or Does It?

- The average attacker earns approximately ¼ of the salary of an average IT employee
- The cost and time to plan attacks has decreased
- Better access to better tools makes attacks easier
- Remember: Nobody is trying to be "average"



Ponemon INSTITUTE

Flipping the Economics of Attacks

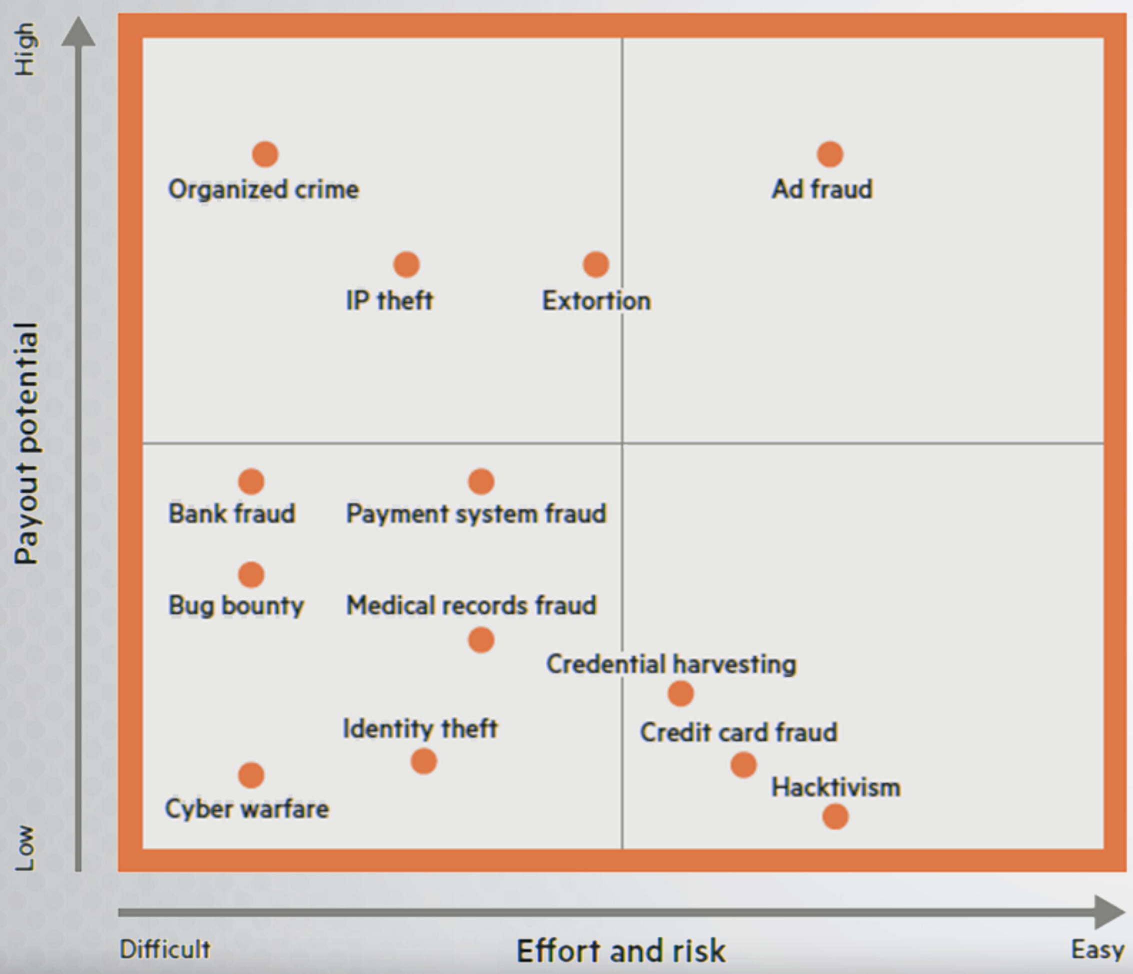
Sponsored by Palo Alto Networks

Independently conducted by Ponemon Institute LLC

Publication Date: January 2016

Ponemon Institute© Research Report

Sophisticated Understanding of Value



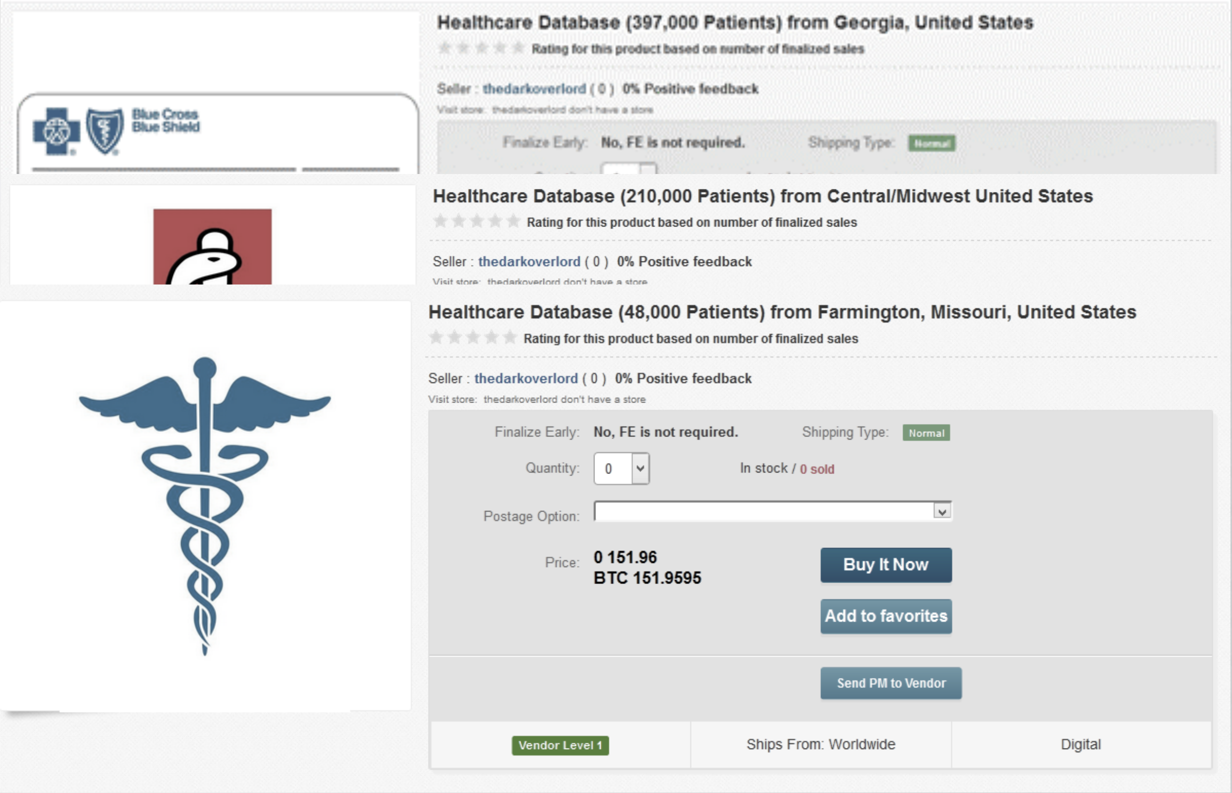
Monetizable criminal enterprise

- ▼ Credit Cards
- ▲ Medical Records
- ▲ Intellectual Property
- ▶ Credentials
- ▼ Vulnerabilities
- ▲ Exploits

The Economics of Web Attacks

Hacker steals US healthcare records

- 397,000 records from Georgia
  - 607.84 BTC / about $350,000
- 210,000 records from Central / Midwest US
  - 303.92 BTC / about $175,000
- 48,000 records from Missouri
  - 151.96 BTC / about $87,000



Healthcare Database (397,000 Patients) from Georgia, United States

Rating for this product based on number of finalized sales

Seller : thedarkoverlord (0) 0% Positive feedback

Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: Normal

Healthcare Database (210,000 Patients) from Central/Midwest United States

Rating for this product based on number of finalized sales

Seller : thedarkoverlord (0) 0% Positive feedback

Visit store: thedarkoverlord don't have a store

Healthcare Database (48,000 Patients) from Farmington, Missouri, United States

Rating for this product based on number of finalized sales

Seller : thedarkoverlord (0) 0% Positive feedback

Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: Normal

Quantity: 0 In stock / 0 sold

Postage Option:

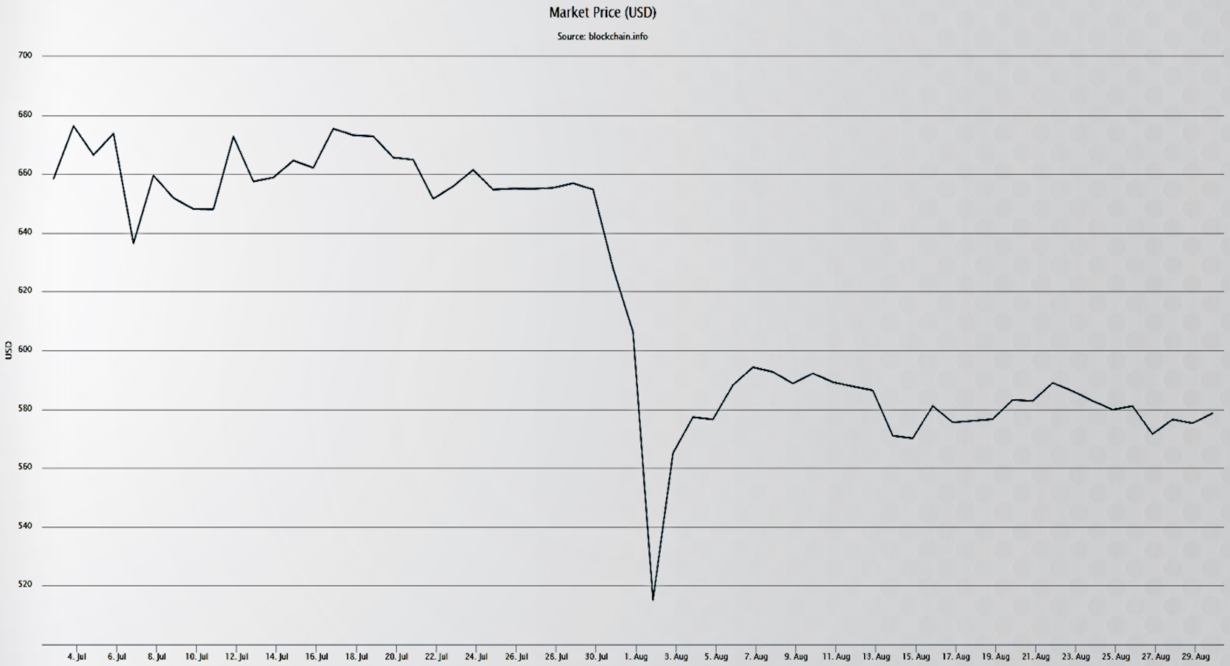
Price: 0 151.96
BTC 151.9595

Image Source: https://www.deepdotweb.com/2016/06/26/655000-healthcare-records-patients-being-sold/

The Economics of Web Attacks

Hacker steals $72M in BTC

- Bitfinex is the 3rd largest Bitcoin exchange
- Hacker stole 119,756 BTC / $72M by breaching the exchange
- Breach caused a 20% decrease in trading value of BTC
- $3.5M reward for info leading to recovery


Market Price (USD)

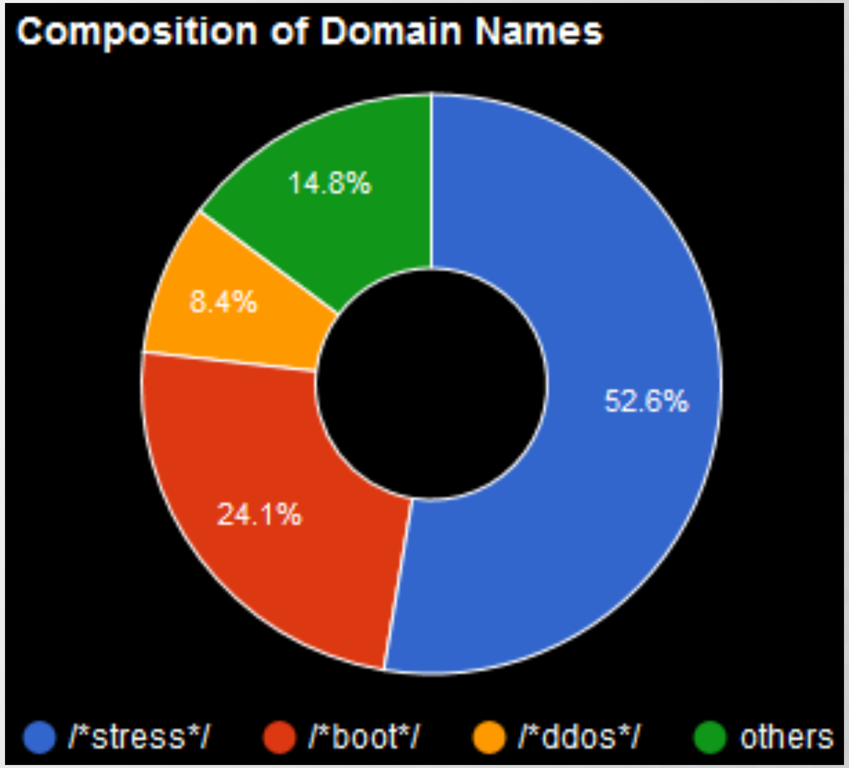
Source: blockchain.info

Image Source: http://blockchain.info

The Economics of DDoS

Commercial DDoS Services

- Recent study found over 430 booter and stresser websites on the Clearnet
- For as little as $6, people can anonymously order a 5-10 Gbps DDoS attack lasting 10 minutes or more

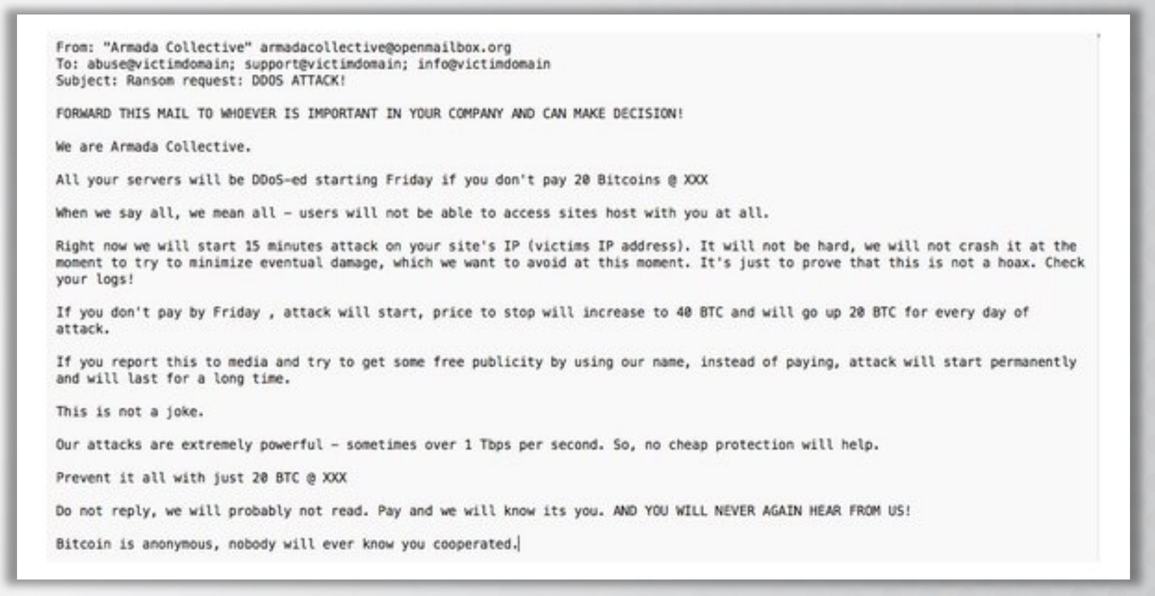


Source: http://booterblacklist.com/
Related Work:J. J. Santanna, R. de O. Schmidt, D. Tuncer, J. de Vries, L. Granville, and A. Pras. "Booter Blacklist: Unveiling DDoS-for-hire Websites"
International Conference on Network and Service Management (CNSM). 2016.

The Economics of RDoS

Ransom attacks pay!

- In Radware’s recent report, 1 in 7 say they’ve had ransom attacks in the past year
- In US, the average ransom paid was $7,520
- In UK, the average ransom paid was £22,218

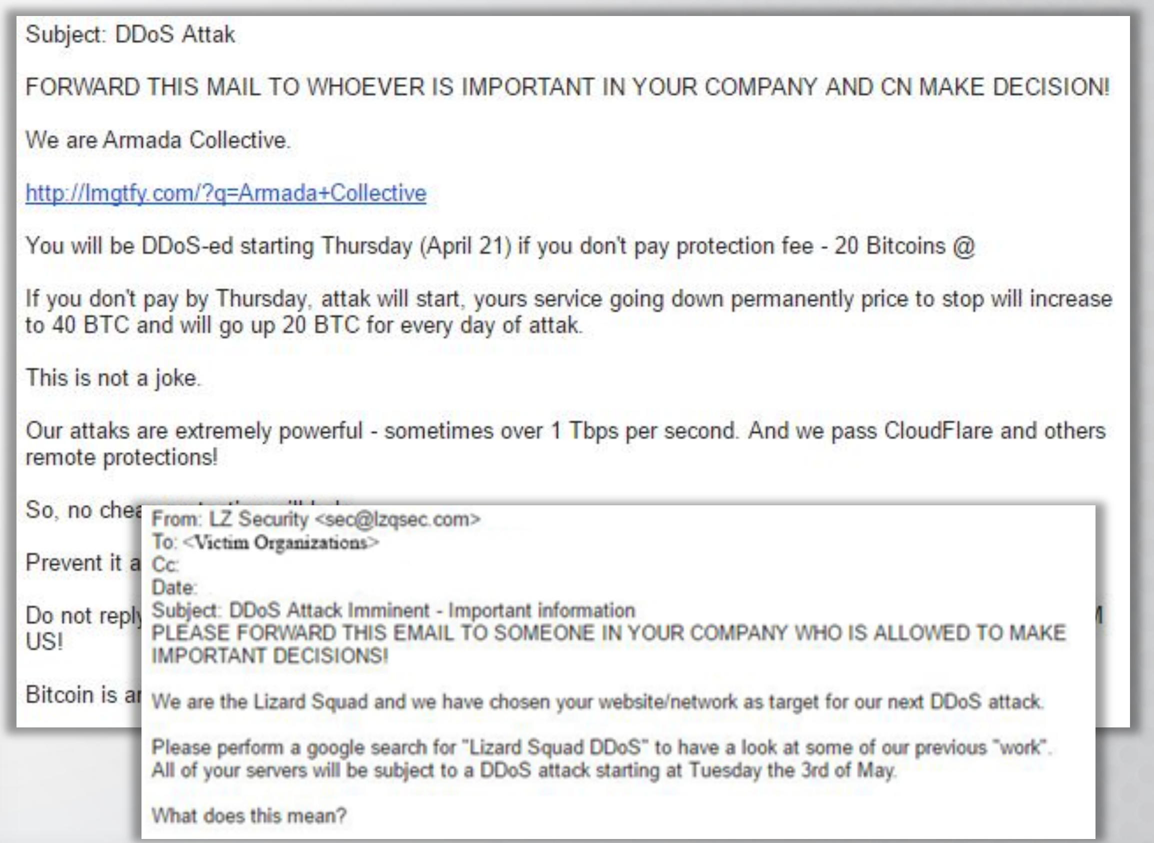


```
From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the
moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check
your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of
attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently
and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.
```

The Economics of RDoS

Fake ransom attacks also pay!

- Armada Collective and Lizard Squad impersonators send ransom emails
- Warning shots particularly useful
- They reportedly earned $100,000 with this wave of ransom letters



Subject: DDoS Attak

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CN MAKE DECISION!

We are Armada Collective.

http://lmgtfy.com/?q=Armada+Collective

You will be DDoS-ed starting Thursday (April 21) if you don't pay protection fee - 20 Bitcoins @

If you don't pay by Thursday, attak will start, yours service going down permanently price to stop will increase to 40 BTC and will go up 20 BTC for every day of attak.

This is not a joke.

Our attaks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections!

So, no chea

Prevent it a

Do not reply M
US!

Bitcoin is a

From: LZ Security <sec@lzqsec.com>
To: <Victim Organizations>
Cc:
Date:
Subject: DDoS Attack Imminent - Important information
PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack.

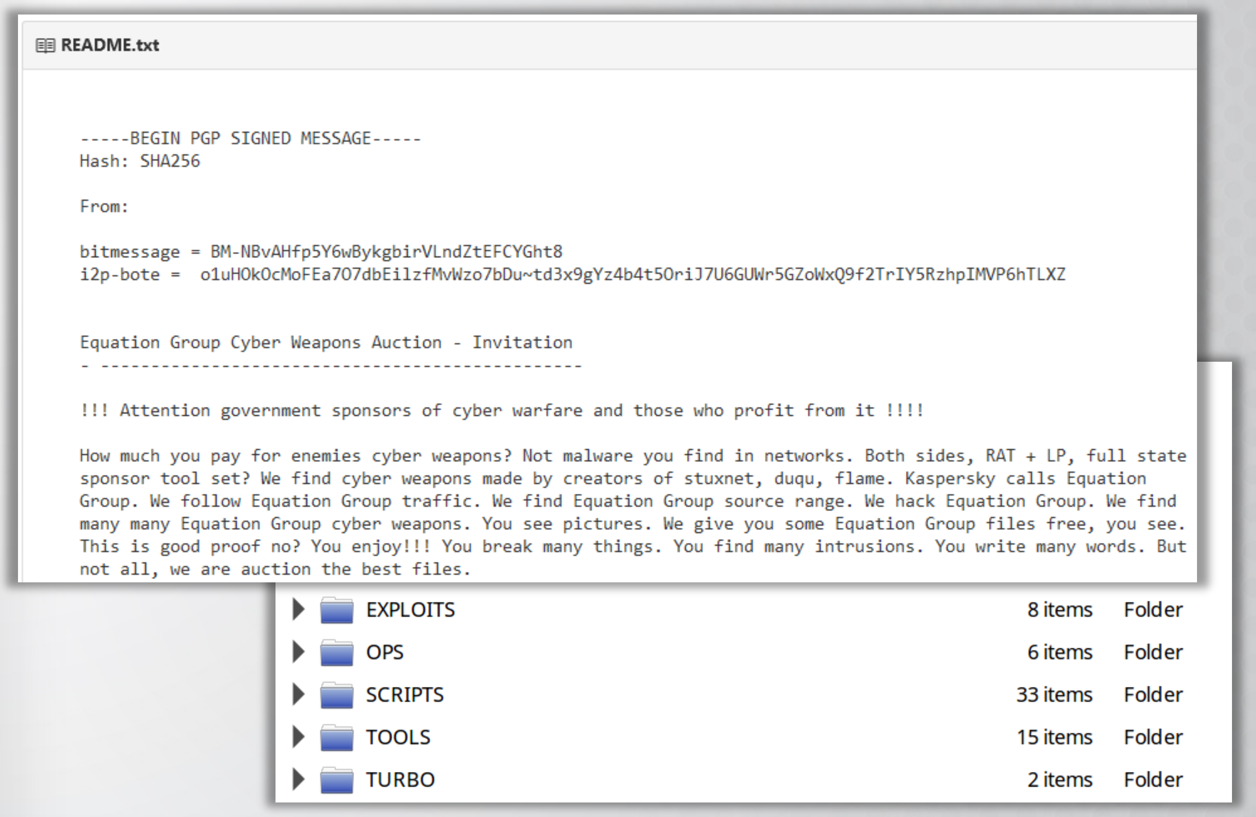
Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous "work". All of your servers will be subject to a DDoS attack starting at Tuesday the 3rd of May.

What does this mean?

Global Impact: Cyberwar and Espionage

NSA Hack

- “The Shadow Brokers” hack the NSA’s hacking team “Equation Group”
- Highest bidder gets the tools but all other bidders “lose lose”
- If 1M Bitcoins are raised, the entire kit will be released publically (~ $572.4M)



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

From:

bitmessage = BM-NBvAHfp5Y6wBykgbirVLndZtEFCYGht8
i2p-bote =  o1uHOkOcMoFEa7O7dbEilzfMvWzo7bDu~td3x9gYz4b4t5OriJ7U6GUWr5GZoWxQ9f2TrIY5RzhpIMVP6hTLXZ


Equation Group Cyber Weapons Auction - Invitation
- ------------------------------------------------

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state
sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation
Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find
many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see.
This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But
not all, we are auction the best files.
```

EXPLOITS	8 items	Folder
OPS	6 items	Folder
SCRIPTS	33 items	Folder
TOOLS	15 items	Folder
TURBO	2 items	Folder

Global Impact: Cyberwar and Espionage

Negative Impacts

- NSA’s PRISM project leaked by Snowden
- Companies avoiding US providers to avoid spying
- ITIF study estimated a $35B loss to US companies from lost business
- Forrester estimated it at $180B!

The Cyber Attack Marketplace

What is the Cyber Attack Marketplace?

- E-Commerce for criminals
- Mainly found on the Darknet
- Most markets are available to the public
  - Some require you to commit a crime for membership
- Currency of choice: Bitcoin

Why is it Attractive to Hackers?

Accessible

Full marketplace
Readily available

Easy to Use

As-a-Service
options

Everything You Need

Variety of vectors,
tools, lists and
customized solutions

Why is it Attractive to Hackers?

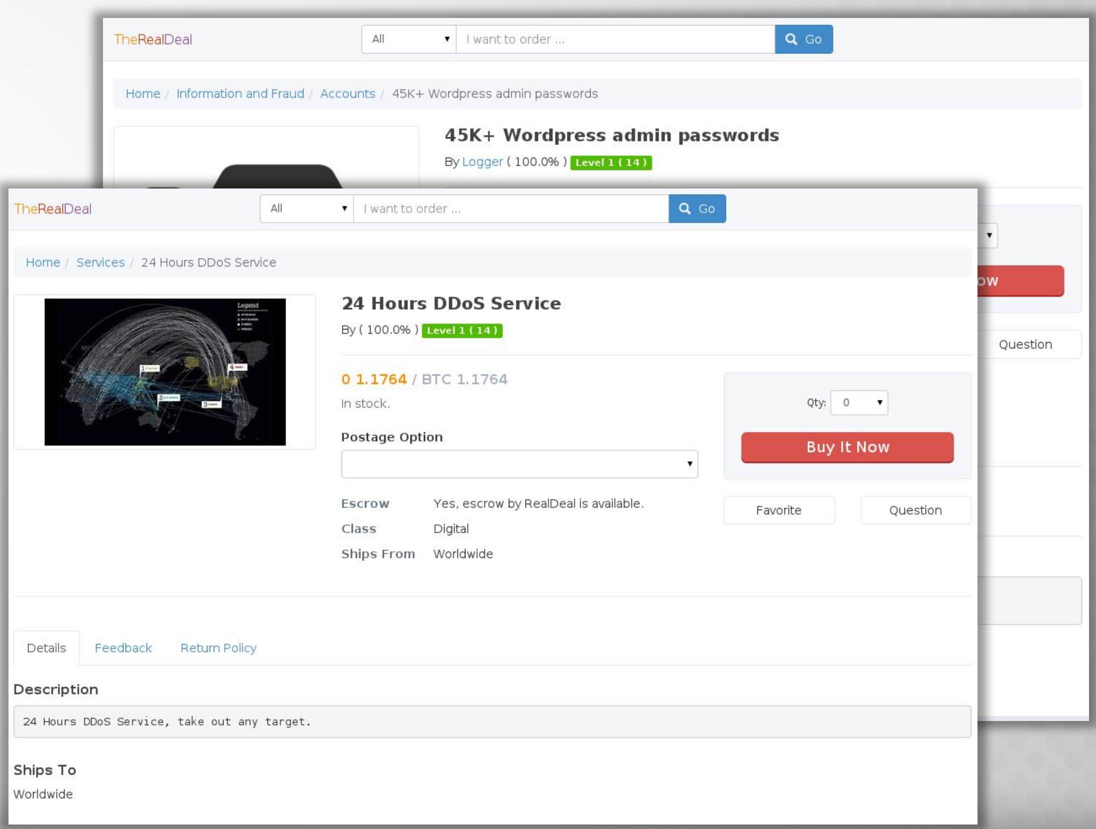
Accessible
Full marketplace
Readily available

Easy to Use
As-a-Service
options

Everything You Need
Variety of vectors,
tools, lists and
customized solutions

Your Marketplace of Choice

- Variety of marketplaces available on Darknet:
  - HELL
  - Alphabay
  - Valhalla
  - Hansa
  - The Real Deal
- One click shopping experience for
  - DDoS services, Tools, PII lists



TheRealDeal

Home / Information and Fraud / Accounts / 45K+ Wordpress admin passwords

45K+ Wordpress admin passwords

By Logger (100.0%) Level 1 (14)

TheRealDeal

Home / Services / 24 Hours DDoS Service

24 Hours DDoS Service

By (100.0%) Level 1 (14)

0 1.1764 / BTC 1.1764

In stock.

Postage Option

Qty: 0

Escrow: Yes, escrow by RealDeal is available.

Class: Digital

Ships From: Worldwide

Description

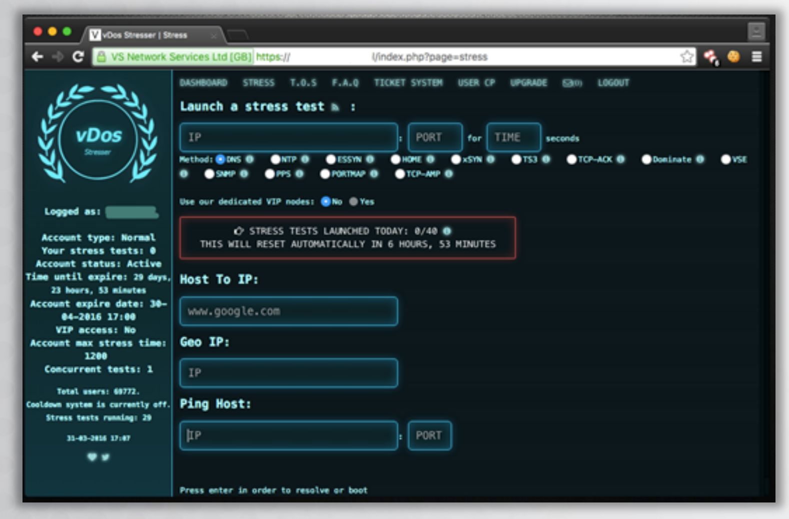
24 Hours DDoS Service, take out any target.

Ships To

Worldwide

You Don`t Need to Look Far

Services on Clearnet



vDos Stresser | Stress

VS Network Services Ltd [GB] https://[redacted]/index.php?page=stress

vDos
Stresser
DASHBOARD STRESS T.O.S F.A.Q TICKET SYSTEM USER CP UPGRADE LOGOUT

Launch a stress test :

IP : PORT for TIME seconds

Method: ● DNS ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ TS3 ○ TCP-ACK ○ Dominate ○ VSE ○ SNMP ○ PPS ○ PORTMAP ○ TCP-AMP

Use our dedicated VIP nodes: ● No ○ Yes

STRESS TESTS LAUNCHED TODAY: 0/40
THIS WILL RESET AUTOMATICALLY IN 6 HOURS, 53 MINUTES

Host To IP:

www.google.com

Geo IP:

IP

Ping Host:

IP : PORT

Press enter in order to resolve or boot

Logged as: [redacted]

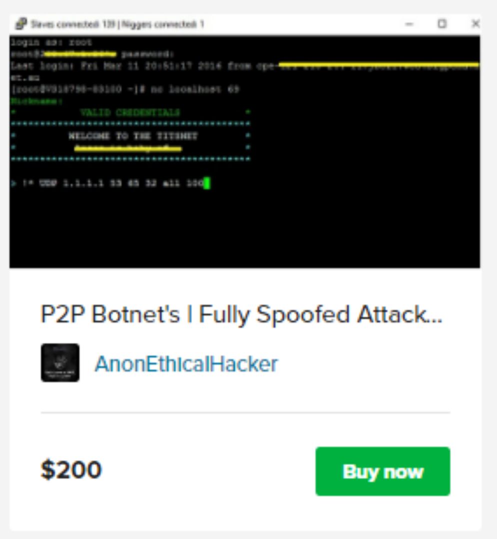
Account type: Normal
Your stress tests: 0
Account status: Active
Time until expire: 29 days, 23 hours, 53 minutes
Account expire date: 30-04-2016 17:00
VIP access: No
Account max stress time: 1200
Concurrent tests: 1

Total users: 69772.
Cooldown system is currently off.
Stress tests running: 29

31-03-2016 17:07

Shenron, vDos, Bangstresser

Hidden in legitimate e-commerce sites



Slaves connected: 139 | Niggers connected: 1

```
login as: root
root@[redacted] password:
Last login: Fri Mar 11 20:51:17 2016 from cpe-[redacted]
et.au
[root@V918798-89100 ~]# nc localhost 69
Nickname:
*          VALID CREDENTIALS          *
***************************************
*        WELCOME TO THE TITSNET       *
*        [redacted]                   *
***************************************

> !* UDP 1.1.1.1 53 65 32 all 100
```

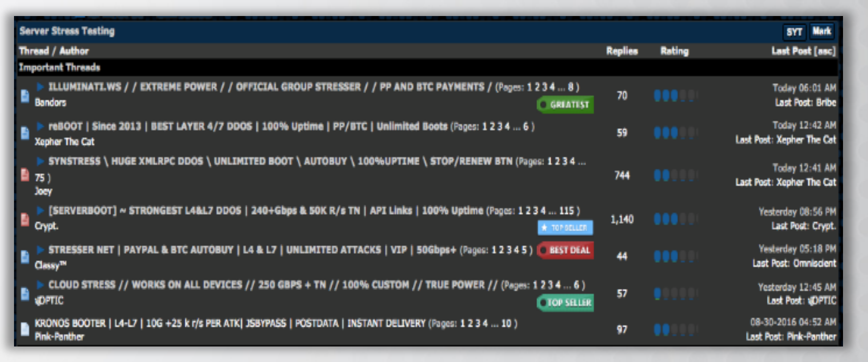
P2P Botnet's I Fully Spoofed Attack...

AnonEthicalHacker

$200

IRC setup, Preloaded VPS, Botnet

Vendor area in hacker forums



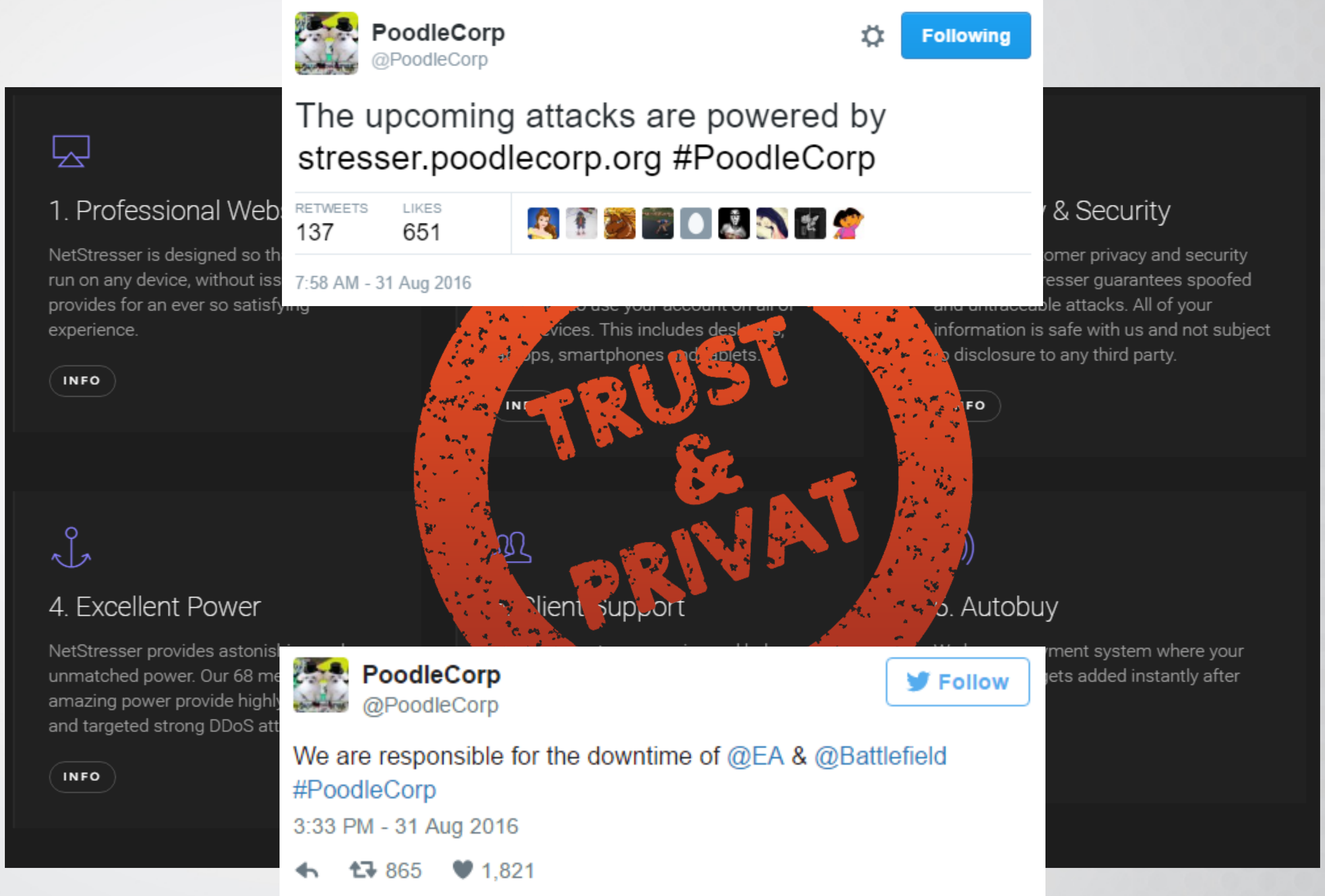
Server Stress Testing

Thread / Author	Replies	Rating	Last Post [asc]
Important Threads			
ILLUMINATI.WS / / EXTREME POWER / / OFFICIAL GROUP STRESSER / / PP AND BTC PAYMENTS / (Pages: 1 2 3 4 ... 8) Bandors GREATEST	70	●●●○○	Today 06:01 AM Last Post: Bribe
reBOOT | Since 2013 | BEST LAYER 4/7 DDOS | 100% Uptime | PP/BTC | Unlimited Boots (Pages: 1 2 3 4 ... 6) Xepher The Cat	59	●●●○○	Today 12:42 AM Last Post: Xepher The Cat
SYNSTRESS \ HUGE XMLRPC DDOS \ UNLIMITED BOOT \ AUTOBUY \ 100%UPTIME \ STOP/RENEW BTN (Pages: 1 2 3 4 ... 75) Joey	744	●●○○○	Today 12:41 AM Last Post: Xepher The Cat
[SERVERBOOT] ~ STRONGEST L4&L7 DDOS | 240+Gbps & 50K R/s TN | API Links | 100% Uptime (Pages: 1 2 3 4 ... 115) Crypt. ★ TOP SELLER	1,140	●●●○○	Yesterday 08:56 PM Last Post: Crypt.
STRESSER NET | PAYPAL & BTC AUTOBUY | L4 & L7 | UNLIMITED ATTACKS | VIP | 50Gbps+ (Pages: 1 2 3 4 5) BEST DEAL Classy™	44	●●●○○	Yesterday 05:18 PM Last Post: Omniscient
CLOUD STRESS // WORKS ON ALL DEVICES // 250 GBPS + TN // 100% CUSTOM // TRUE POWER // (Pages: 1 2 3 4 ... 6) ɖOPTIC TOP SELLER	57	●○○○○	Yesterday 12:45 AM Last Post: ɖOPTIC
KRONOS BOOTER | L4-L7 | 10G +25 k r/s PER ATK| JSBYPASS | POSTDATA | INSTANT DELIVERY (Pages: 1 2 3 4 ... 10) Pink-Panther	97	●●○○○	08-30-2016 04:52 AM Last Post: Pink-Panther

Attack scripts, Amp lists, Hijacked accounts

And Vendors Market their Services

- Stunt hacking
- Social media
- Forums
- Customer service
- Private offerings



PoodleCorp
@PoodleCorp

The upcoming attacks are powered by stresser.poodlecorp.org #PoodleCorp

RETWEETS 137 LIKES 651

7:58 AM - 31 Aug 2016

1. Professional Web

NetStresser is designed so th run on any device, without iss provides for an ever so satisfying experience.

o use your account on all of vices. This includes desk ops, smartphones and tablets.

& Security

omer privacy and security esser guarantees spoofed and untraceable attacks. All of your information is safe with us and not subject to disclosure to any third party.

TRUST & PRIVAT

4. Excellent Power

NetStresser provides astonis unmatched power. Our 68 me amazing power provide highly and targeted strong DDoS att

Client support

5. Autobuy

ment system where your ets added instantly after

PoodleCorp
@PoodleCorp

We are responsible for the downtime of @EA & @Battlefield #PoodleCorp

3:33 PM - 31 Aug 2016

865 1,821

Why is it Attractive to Hackers?

Accessible
Full marketplace
Readily available

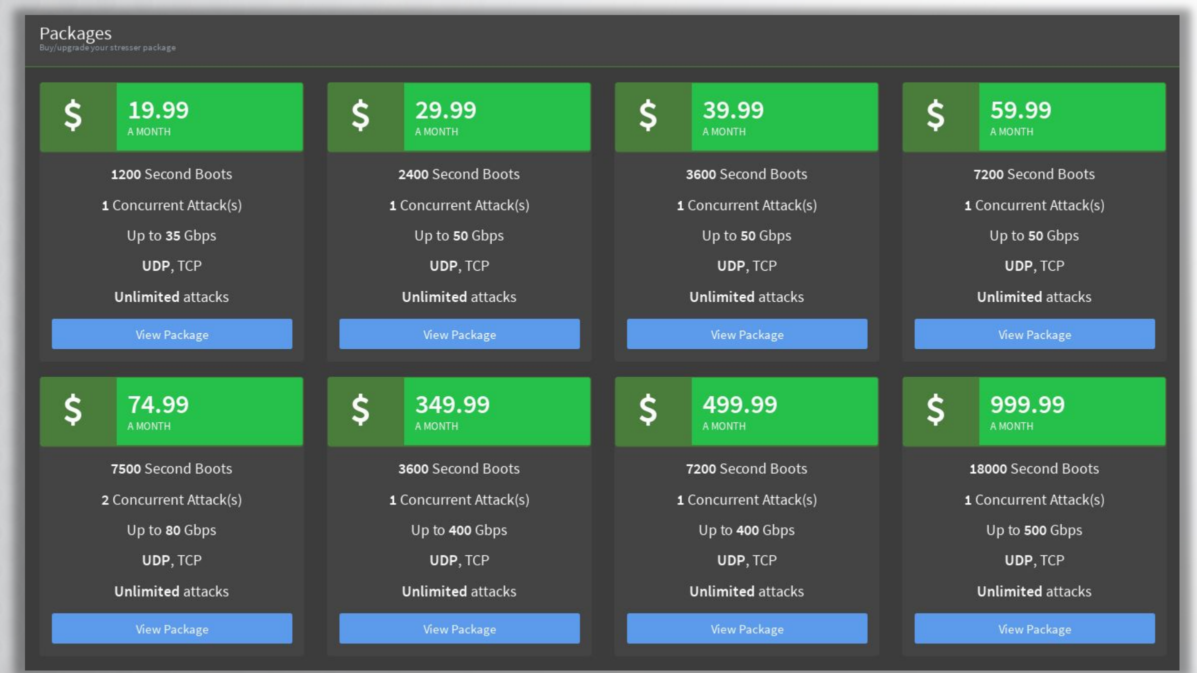
Easy to Use
As-a-Service
options

Everything You Need
Variety of vectors,
tools, lists and
customized solutions

As A Service - Shenron Attack Tool

BUSTED BUSTED BUSTED

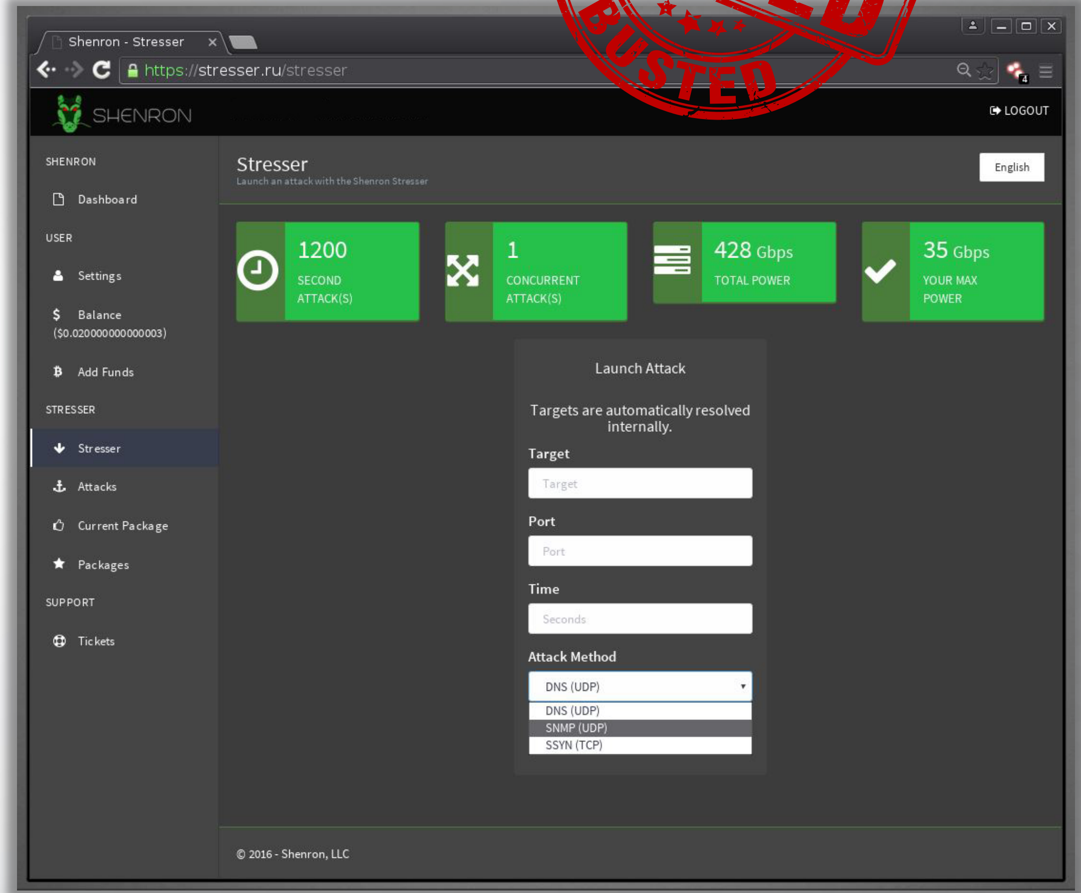
- Lizard Squad‘s public stresser services
- $19.99 => 15Gb attack for 1200 seconds



Packages
Buy/upgrade your stresser package

$	19.99 A MONTH	29.99 A MONTH	39.99 A MONTH	59.99 A MONTH
	1200 Second Boots	**2400** Second Boots	**3600** Second Boots	**7200** Second Boots
	1 Concurrent Attack(s)	**1** Concurrent Attack(s)	**1** Concurrent Attack(s)	**1** Concurrent Attack(s)
	Up to **35** Gbps	Up to **50** Gbps	Up to **50** Gbps	Up to **50** Gbps
	UDP, TCP	**UDP**, TCP	**UDP**, TCP	**UDP**, TCP
	Unlimited attacks	**Unlimited** attacks	**Unlimited** attacks	**Unlimited** attacks
	View Package	View Package	View Package	View Package

$	74.99 A MONTH	349.99 A MONTH	499.99 A MONTH	999.99 A MONTH
	7500 Second Boots	**3600** Second Boots	**7200** Second Boots	**18000** Second Boots
	2 Concurrent Attack(s)	**1** Concurrent Attack(s)	**1** Concurrent Attack(s)	**1** Concurrent Attack(s)
	Up to **80** Gbps	Up to **400** Gbps	Up to **400** Gbps	Up to **500** Gbps
	UDP, TCP	**UDP**, TCP	**UDP**, TCP	**UDP**, TCP
	Unlimited attacks	**Unlimited** attacks	**Unlimited** attacks	**Unlimited** attacks
	View Package	View Package	View Package	View Package



Shenron - Stresser
https://stresser.ru/stresser

SHENRON
LOGOUT

Stresser
Launch an attack with the Shenron Stresser

English

1200 SECOND ATTACK(S)

1 CONCURRENT ATTACK(S)

428 Gbps TOTAL POWER

35 Gbps YOUR MAX POWER

Launch Attack

Targets are automatically resolved internally.

Target: Target

Port: Port

Time: Seconds

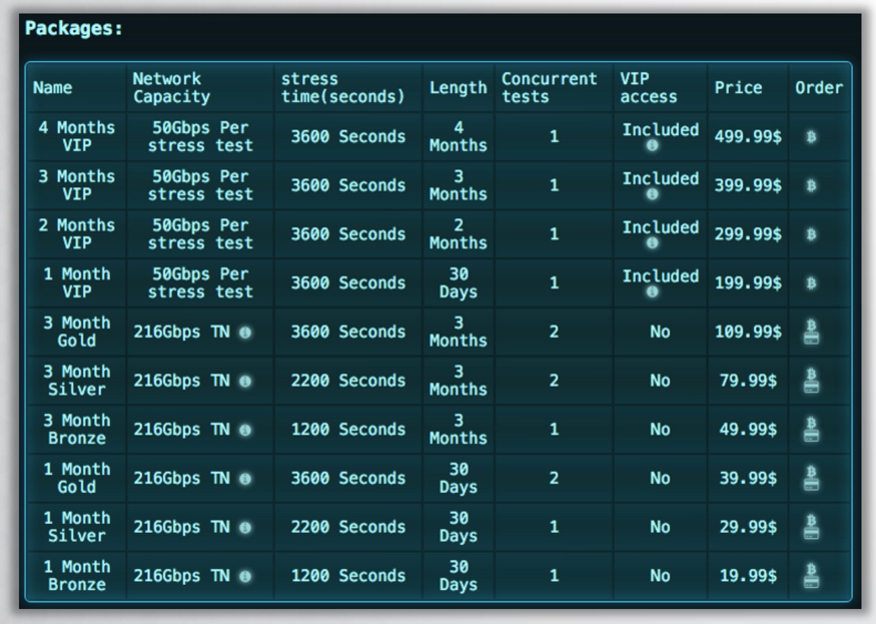
Attack Method: DNS (UDP)

© 2016 - Shenron, LLC

As A Service - vDos Attack Tool

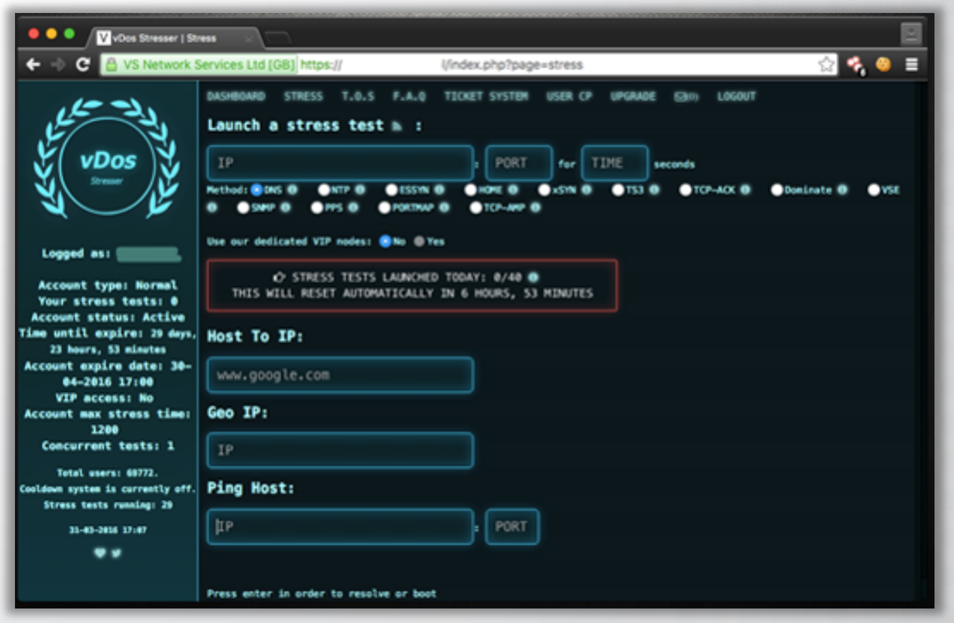
BUSTED
★★★★
BUSTED
★★★★
BUSTED

- Was one of the most popular tools
- $19.99 would gain access to 216 Gbps Attack Network (Shared)
- Thirteen different vectors available



Packages:

Name	Network Capacity	stress time(seconds)	Length	Concurrent tests	VIP access	Price	Order
4 Months VIP	50Gbps Per stress test	3600 Seconds	4 Months	1	Included	499.99$	฿
3 Months VIP	50Gbps Per stress test	3600 Seconds	3 Months	1	Included	399.99$	฿
2 Months VIP	50Gbps Per stress test	3600 Seconds	2 Months	1	Included	299.99$	฿
1 Month VIP	50Gbps Per stress test	3600 Seconds	30 Days	1	Included	199.99$	฿
3 Month Gold	216Gbps TN	3600 Seconds	3 Months	2	No	109.99$	฿
3 Month Silver	216Gbps TN	2200 Seconds	3 Months	2	No	79.99$	฿
3 Month Bronze	216Gbps TN	1200 Seconds	3 Months	1	No	49.99$	฿
1 Month Gold	216Gbps TN	3600 Seconds	30 Days	2	No	39.99$	฿
1 Month Silver	216Gbps TN	2200 Seconds	30 Days	1	No	29.99$	฿
1 Month Bronze	216Gbps TN	1200 Seconds	30 Days	1	No	19.99$	฿



Launch a stress test :

IP : PORT for TIME seconds

Method: ● DNS ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ TS3 ○ TCP-ACK ○ Dominate ○ VSE ○ SNMP ○ PPS ○ PORTMAP ○ TCP-AMP

Use our dedicated VIP nodes: ● No ○ Yes

STRESS TESTS LAUNCHED TODAY: 0/40
THIS WILL RESET AUTOMATICALLY IN 6 HOURS, 53 MINUTES

Host To IP:

www.google.com

Geo IP:

IP

Ping Host:

IP : PORT

Press enter in order to resolve or boot

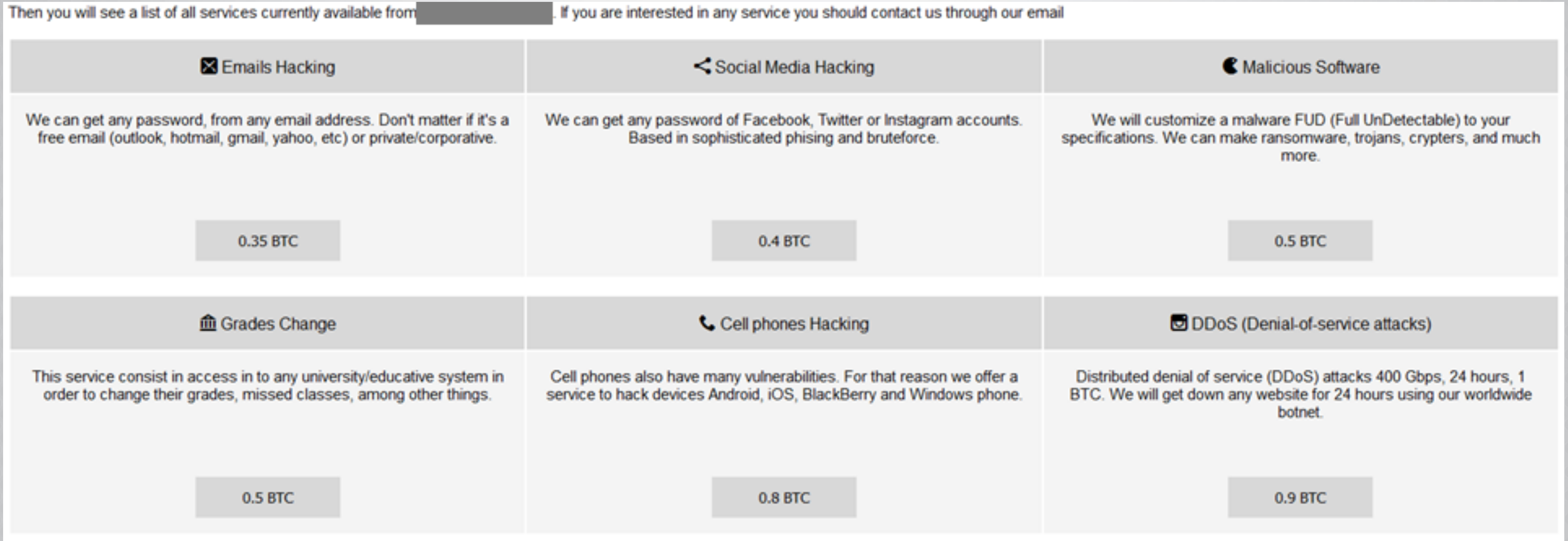
Logged as: [redacted]

Account type: Normal
Your stress tests: 0
Account status: Active
Time until expire: 29 days, 23 hours, 53 minutes
Account expire date: 30-04-2016 17:00
VIP access: No
Account max stress time: 1200
Concurrent tests: 1

Total users: 69772.
Cooldown system is currently off.
Stress tests running: 29

31-03-2016 17:07

Custom Services



Then you will see a list of all services currently available from [redacted]. If you are interested in any service you should contact us through our email

Emails Hacking

We can get any password, from any email address. Don't matter if it's a free email (outlook, hotmail, gmail, yahoo, etc) or private/corporative.

0.35 BTC

Social Media Hacking

We can get any password of Facebook, Twitter or Instagram accounts. Based in sophisticated phising and bruteforce.

0.4 BTC

Malicious Software

We will customize a malware FUD (Full UnDetectable) to your specifications. We can make ransomware, trojans, crypters, and much more.

0.5 BTC

Grades Change

This service consist in access in to any university/educative system in order to change their grades, missed classes, among other things.

0.5 BTC

Cell phones Hacking

Cell phones also have many vulnerabilities. For that reason we offer a service to hack devices Android, iOS, BlackBerry and Windows phone.

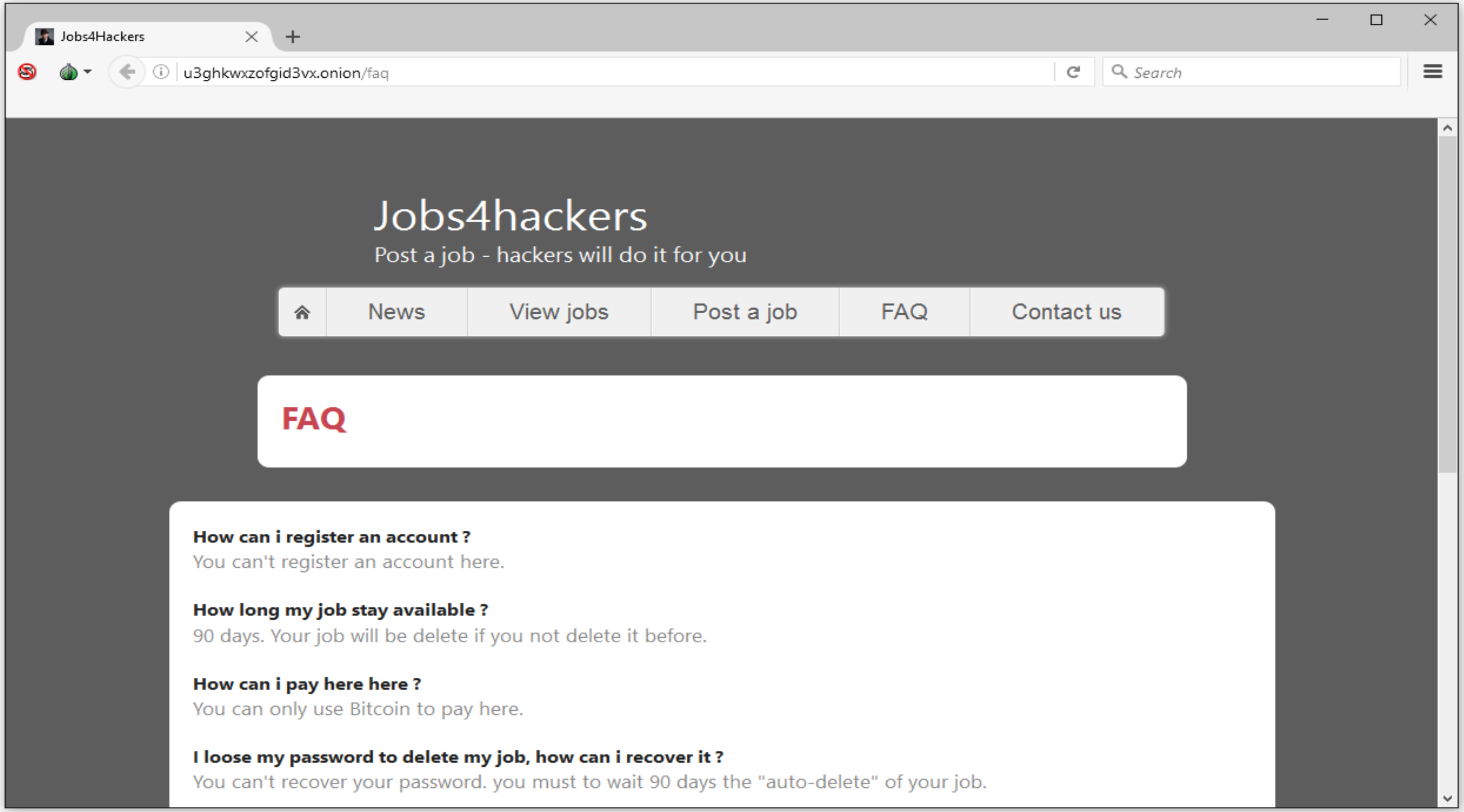
0.8 BTC

DDoS (Denial-of-service attacks)

Distributed denial of service (DDoS) attacks 400 Gbps, 24 hours, 1 BTC. We will get down any website for 24 hours using our worldwide botnet.

0.9 BTC

There Are Even Job Boards



Jobs4hackers

Post a job - hackers will do it for you

FAQ

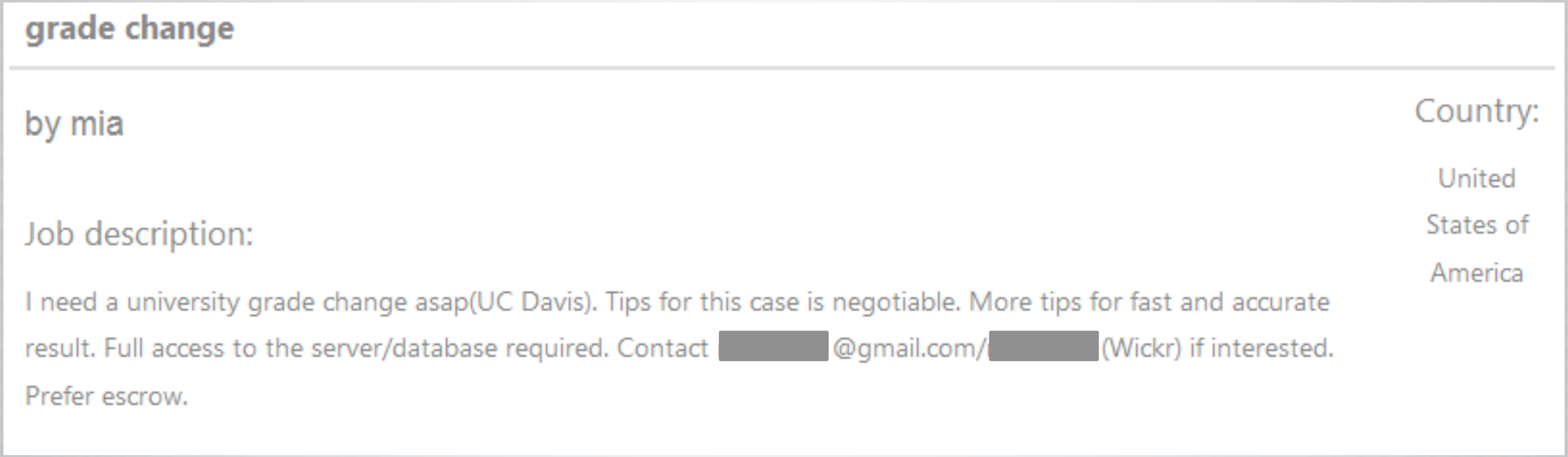
How can i register an account ?
You can't register an account here.

How long my job stay available ?
90 days. Your job will be delete if you not delete it before.

How can i pay here here ?
You can only use Bitcoin to pay here.

I loose my password to delete my job, how can i recover it ?
You can't recover your password. you must to wait 90 days the "auto-delete" of your job.

…Where You Can Request Services



grade change

by mia

Country:

United States of America

Job description:

I need a university grade change asap(UC Davis). Tips for this case is negotiable. More tips for fast and accurate result. Full access to the server/database required. Contact [redacted]@gmail.com/[redacted](Wickr) if interested. Prefer escrow.

Why is it Attractive to Hackers?

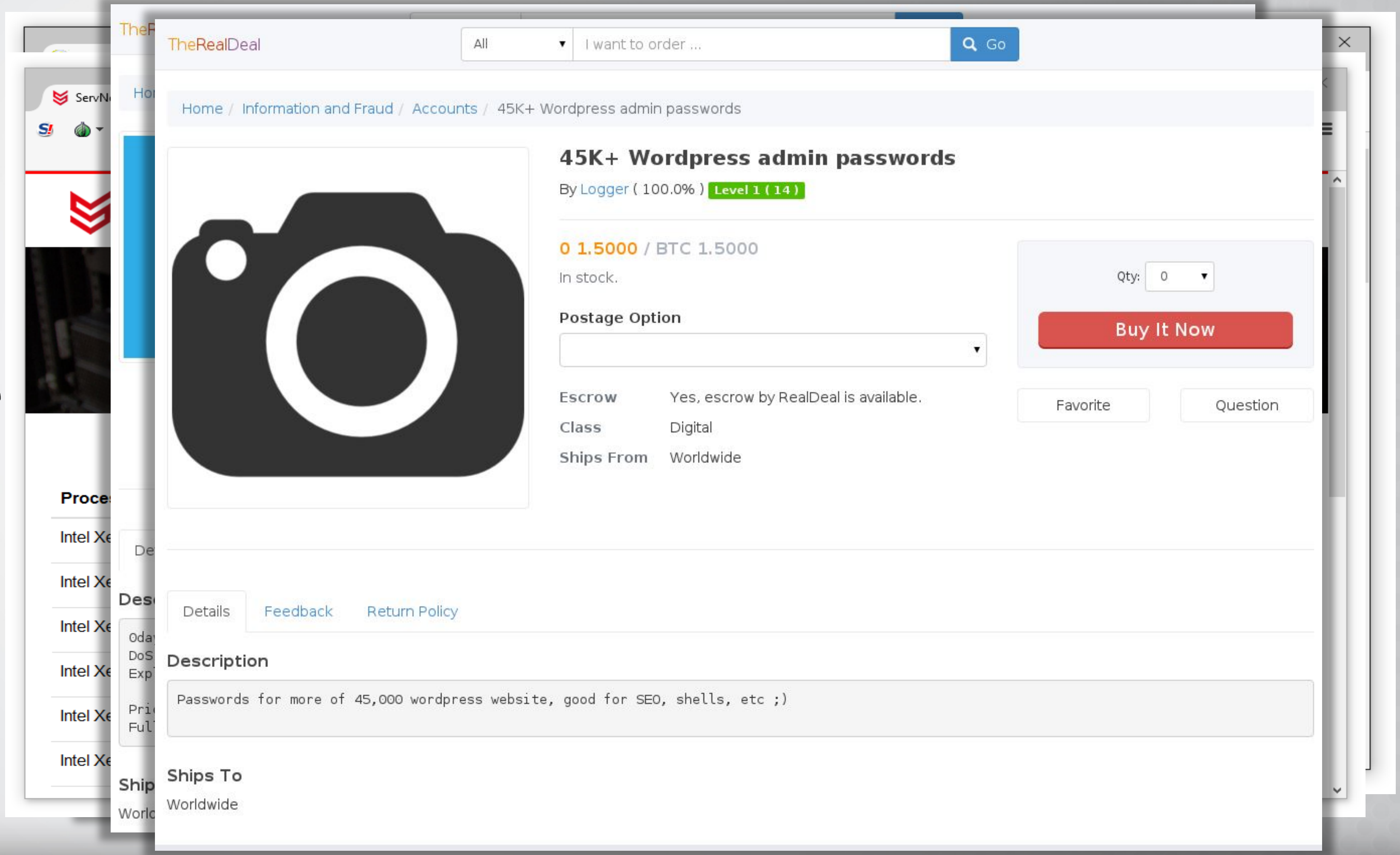
Accessible
Full marketplace
Readily available

Easy to Use
As-a-Service
options

Everything You Need
Variety of vectors,
tools, lists and
customized solutions

Variety on the Darknet

- DDoS as a Service
- Botnet Rental
- Malware/Ransomware
- Security/Hosting
- Undisclosed Exploits
- Leaked Data/Fraud



Home / Information and Fraud / Accounts / 45K+ Wordpress admin passwords

45K+ Wordpress admin passwords

By Logger (100.0%) Level 1 (14)

0 1.5000 / BTC 1.5000

In stock.

Postage Option

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

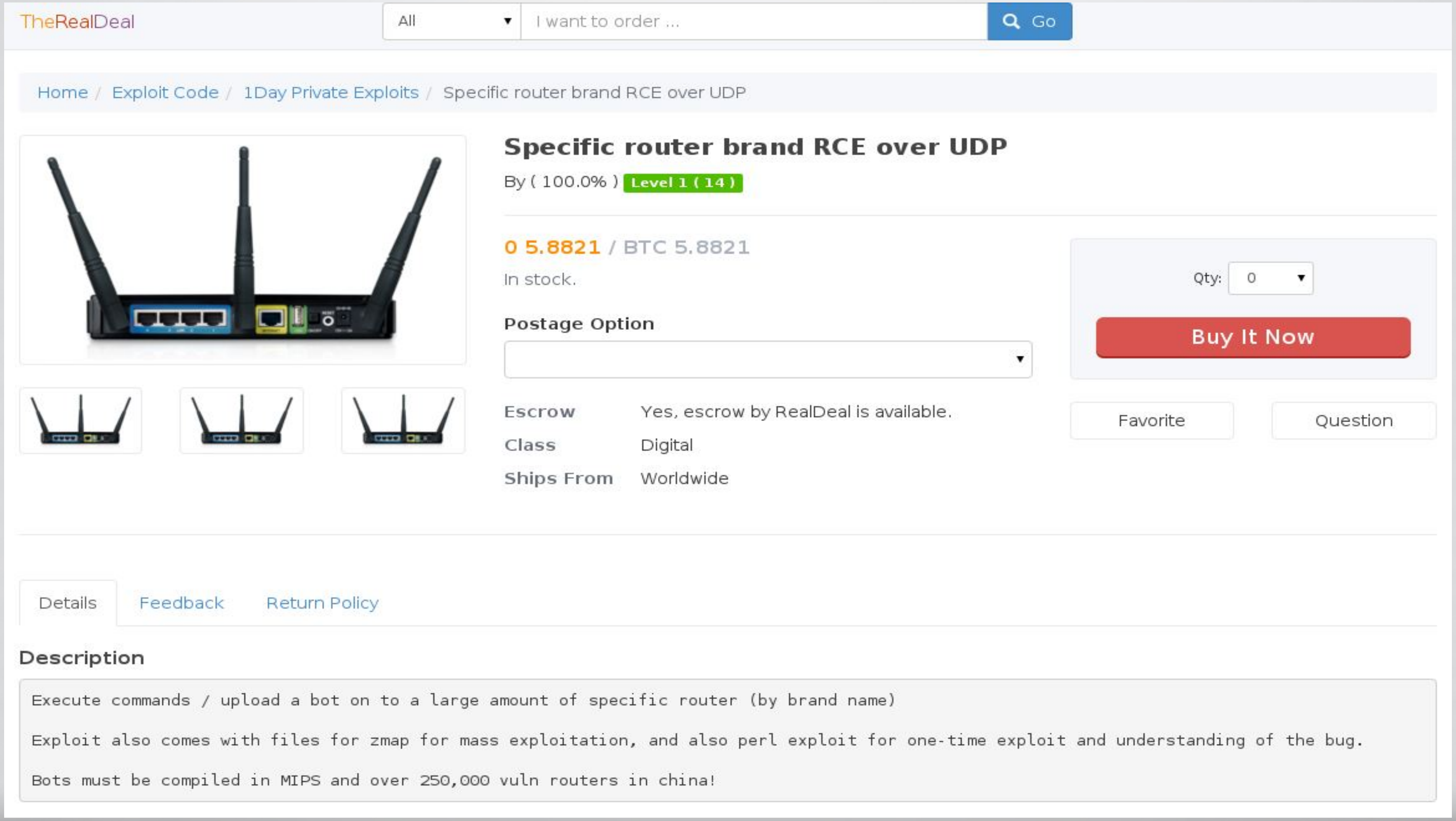
Description

```
Passwords for more of 45,000 wordpress website, good for SEO, shells, etc ;)
```

Ships To

Worldwide

Here‛s an interesting one…



Home / Exploit Code / 1Day Private Exploits / Specific router brand RCE over UDP

Specific router brand RCE over UDP

By (100.0%) Level 1 (14)

0 5.8821 / BTC 5.8821

In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.

Class Digital

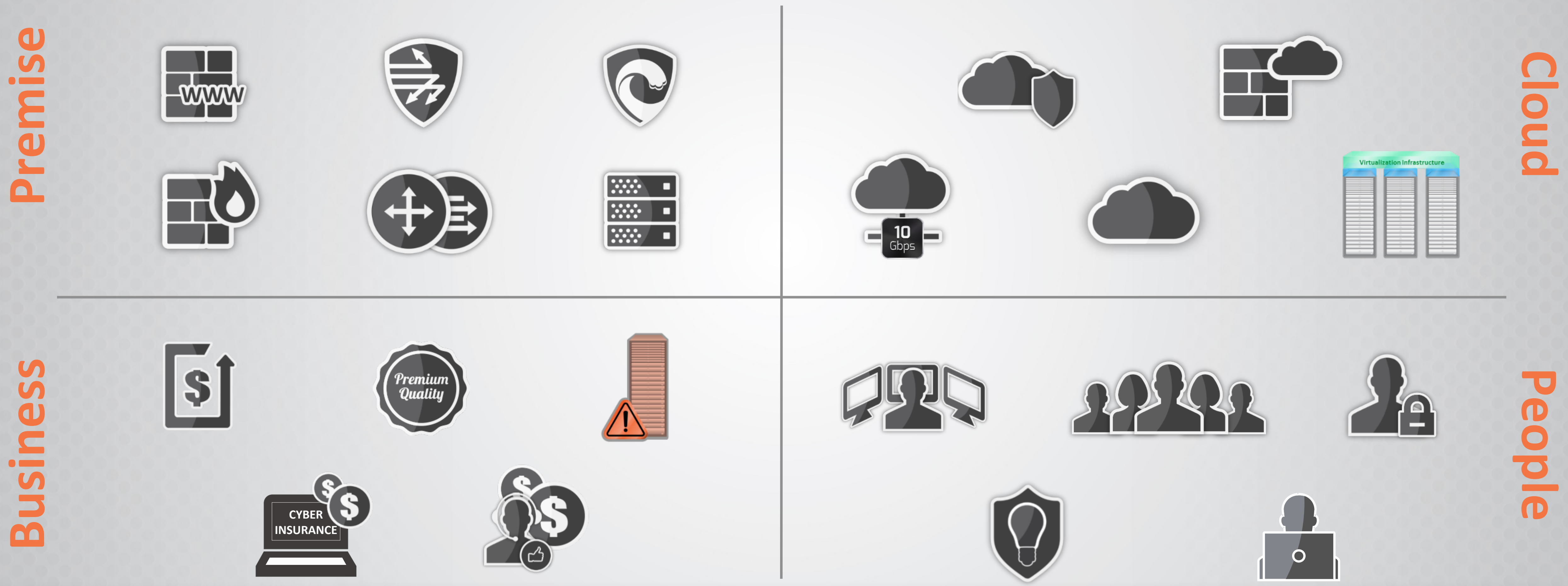
Ships From Worldwide

Description

```
Execute commands / upload a bot on to a large amount of specific router (by brand name)

Exploit also comes with files for zmap for mass exploitation, and also perl exploit for one-time exploit and understanding of the bug.

Bots must be compiled in MIPS and over 250,000 vuln routers in china!
```

Economics of Defense: Reality Check and Path Forward

The Economics of DDoS on our Businesses



Premise

Cloud

Business

People

Security ROI: IT's Holy Grail

Obstacles Have Stood in the Way

- Definition of "Return" can vary greatly by role
- Poor visibility into actual attack activity until it's too late . . . i.e., breach or takedown
- A lack of understanding of whether or not they fit the attackers' profile
- Overlooking the actual costs of manual security solutions
- Underestimating (or ignoring) the hidden costs of processing attack traffic

How We Define "Return" May Depend on Role

Business Manager	Revenue per hour x hours of downtime per attack x number of attacks
Risk Manager	ALE (loss expectancy x number of attacks x likelihood of attack)
Compliance Officer	Cost of Penalties/Cost of Compliance (check box approach)
IT/Security Teams	Job security balancing act (need attacks to stay relevant/downtime and breach cost me my job)

Tipping the Scales, Shifting the ROI Equation

Return

Reduced Opportunity Cost of Manual Mitigation

Improved Efficiency of Net/App Infrastructure

Compliance
Revenue/Brand
Assurance
Job Security

Security Budget
Staff/Management
Operational Risk

Investment/Cost

Tipping the Scale in Favor of Security

Reduced Opportunity Cost of Manual Mitigation

Manual Signatures

UP TO 30 MINUTES

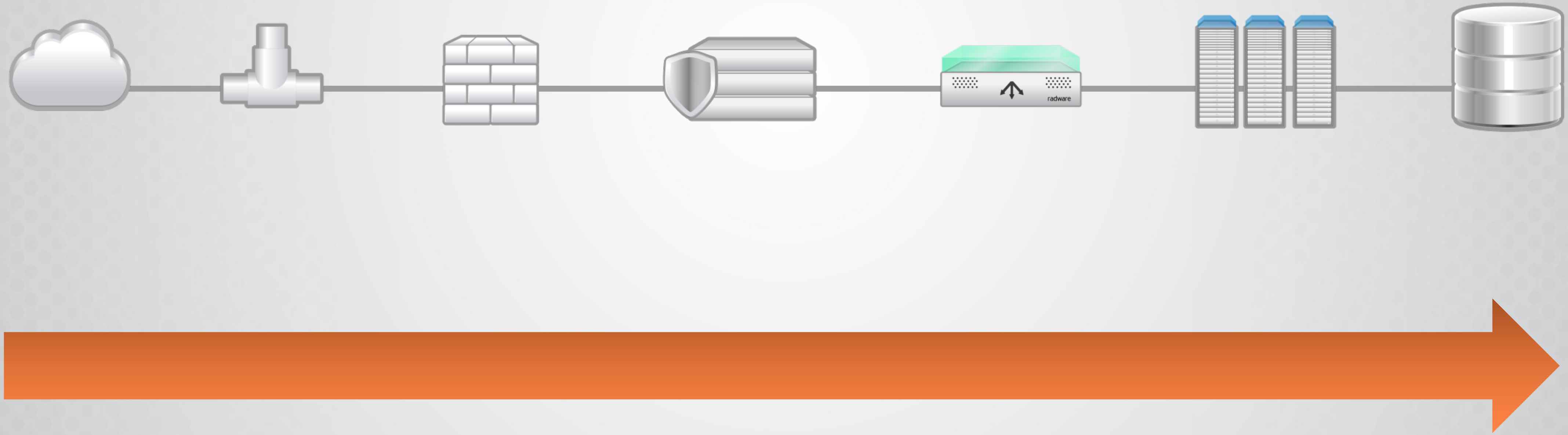
Automated Signatures

WITHIN SECONDS

Automation can learn the anomaly and react faster than a human

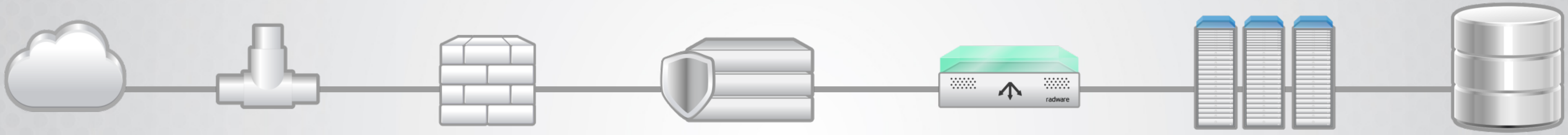
More Efficient Net/App Infrastructure

How much do you spend over-provisioning for bad traffic?

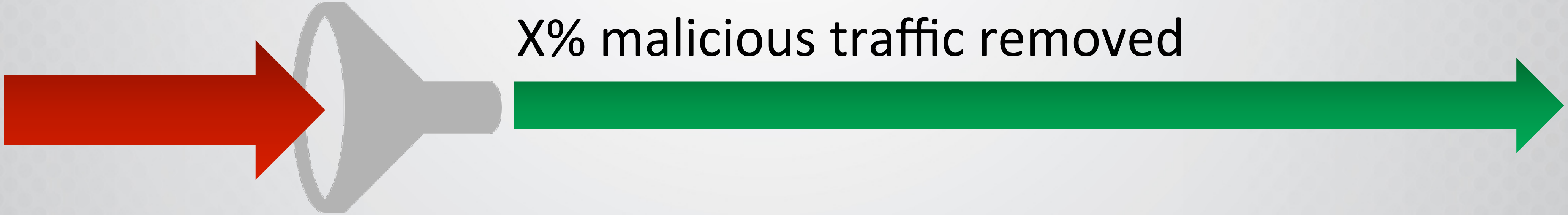


Efficient Nets/Apps: Some Quick Math

How much would effective filtering save you in over-provisioning?



X% decrease in malicious traffic = X% reduction in infrastructure over-investment



X% malicious traffic removed

Bringing it home…

History Repeating?

Cyber Security Reaching a Tipping Point

More Resources

More Targets

More Mature

- Investment in Automated, Adaptive Security Protections
- Reduced Opportunity Cost of Manual Mitigation
- Improved Efficiency of Network/Application Infrastructure

Stay Focused. Be Prepared.

Build your protection strategy. Develop an incident response plan.

Consider Automation.

It has become necessary to fight automated threats with automation technology.

Cover the Blind Spot.

Choose a solution with the widest coverage to protect from multi-vector attacks.

Simplify with Services.

Fully managed services will provide the resources and expertise needed to combat today's attacks.

Have Visibility.

There are many tools (free and commercial) that will give you insightful data to attacks in your network.

radware

Every second counts