More Malcode & Responses

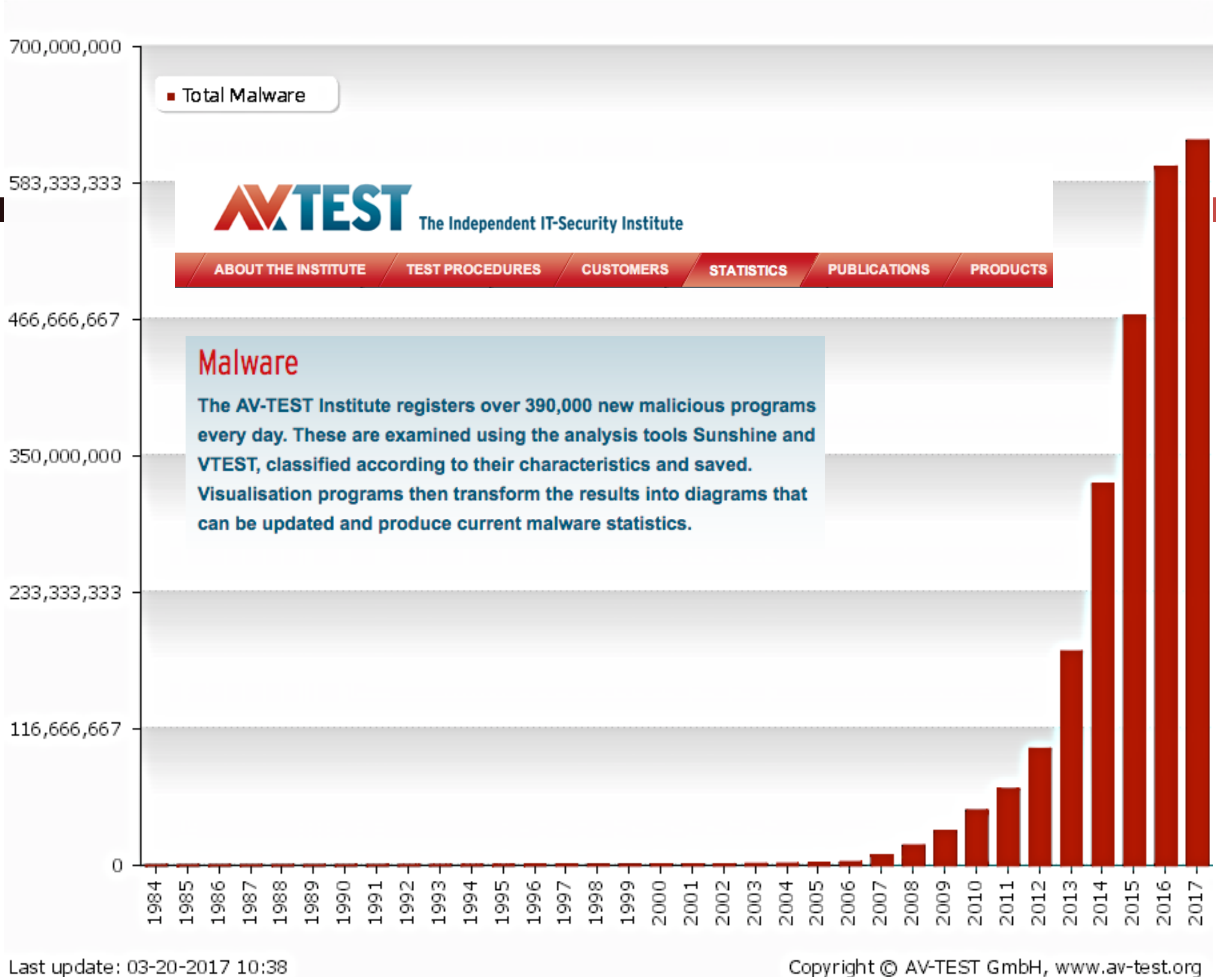
"I've been working day and night trying to secure the Internet of Things.
I finally made a breakthrough and it's called:
VLAN of Thing."
- Taylor Swift

End of Term Logistics...

- Check glookup! Make sure everything is in already
- Reminder, Project 2 is due Monday
- Homework 4 will be due Monday the 4th
- Final is the 15th, locations still TBD
- There ***will*** be review sessions during the class timeslot during dead week
- Today: Malcode
- Monday: ??? (What do you want) + HKN course evaluations
- Wednesday: Guest Lecture from Lea Kissner, Product Privacy Lead and Principal Engineer @ Google. Please come in person!
  - Privacy and User Respect in a Complex World

How Much Malware Is Out There?

- A final consideration re polymorphism and metamorphism:
  - Presence can lead to mis-counting a single virus outbreak as instead reflecting 1,000s of seemingly different viruses
- Thus take care in interpreting vendor statistics on malcode varieties
  - (Also note: public perception that huge malware populations exist is in the vendors' own interest)



Malware

The AV-TEST Institute registers over 390,000 new malicious programs every day. These are examined using the analysis tools Sunshine and VTEST, classified according to their characteristics and saved. Visualisation programs then transform the results into diagrams that can be updated and produce current malware statistics.

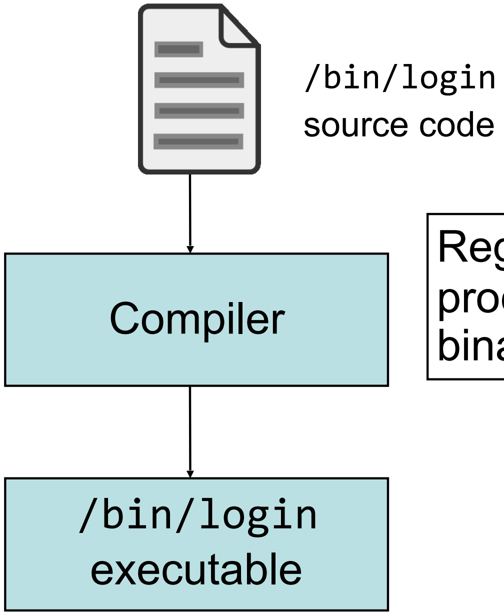
Last update: 03-20-2017 10:38

Infection Cleanup

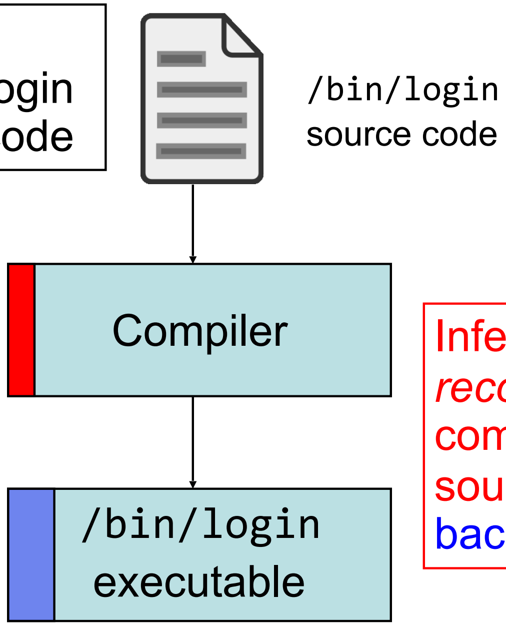
- Once malware detected on a system, how do we get rid of it?
- May require restoring/repairing many files
  - This is part of what AV companies sell: per-specimen disinfection procedures
- What about if malware executed with adminstrator privileges?
  - "Game over man, Game Over!"
  - “Dust off and nuke the entire site from orbit. It’s the only way to be sure”- Aliens
  - i.e., rebuild system from original media + data backups
- Malware may include a rootkit: kernel patches to hide its presence (its existence on disk, processes)

Infection Cleanup, con’t

- If we have complete source code for system, we could rebuild from that instead, couldn’t we?
- No!
- Suppose forensic analysis shows that virus introduced a backdoor in /bin/login executable
  - (Note: this threat isn’t specific to viruses; applies to any malware)
- Cleanup procedure: rebuild /bin/login from source …

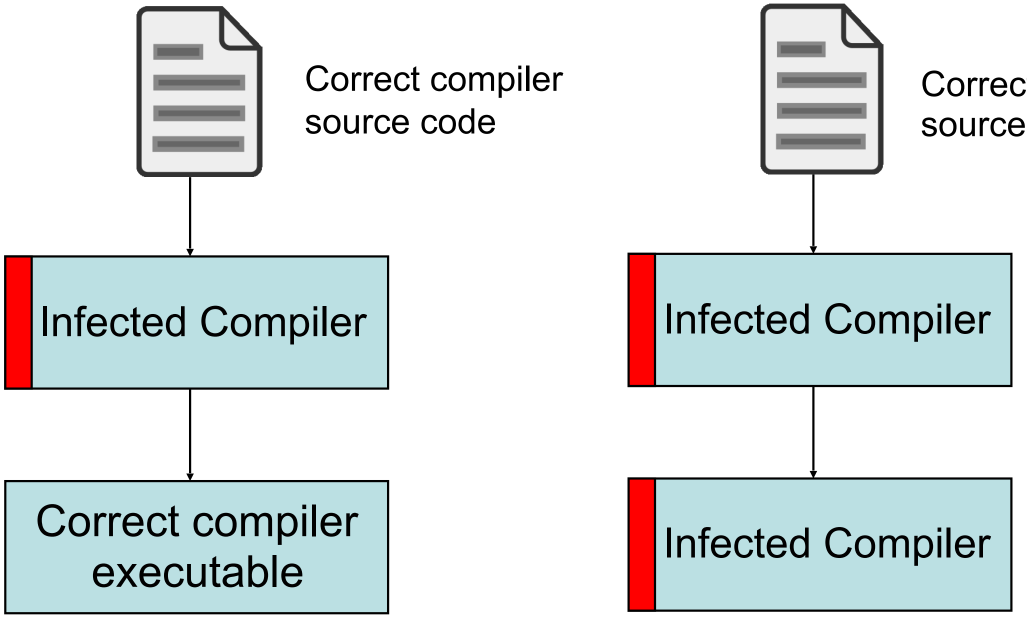


Regular compilation process of building login binary from source code



Infected **compiler** *recognizes* when it's compiling /bin/login source and inserts extra back door when seen

~~No problem: first step, rebuild the compiler so it's uninfected~~


Correct compiler source code
Infected Compiler
Correct compiler executable
Correct compiler source code
Infected Compiler
Infected Compiler

Oops - infected compiler recognizes when it's compiling its own source and inserts the infection!

No amount of careful source-code scrutiny can prevent this problem.
And if the *hardware* has a back door …

Reflections on Trusting Trust
Turing-Award Lecture, Ken Thompson, 1983

Forensics

- Vital complement to detecting attacks: figuring out what happened in wake of successful attack
- Doing so requires access to rich/extensive logs
    - Plus tools for analyzing/understanding them
- It also entails looking for patterns and understanding the implications of structure seen in activity
    - An iterative process ("peeling the onion")
- Consider these actual emails from operational security …

Emails omitted from on-line slides

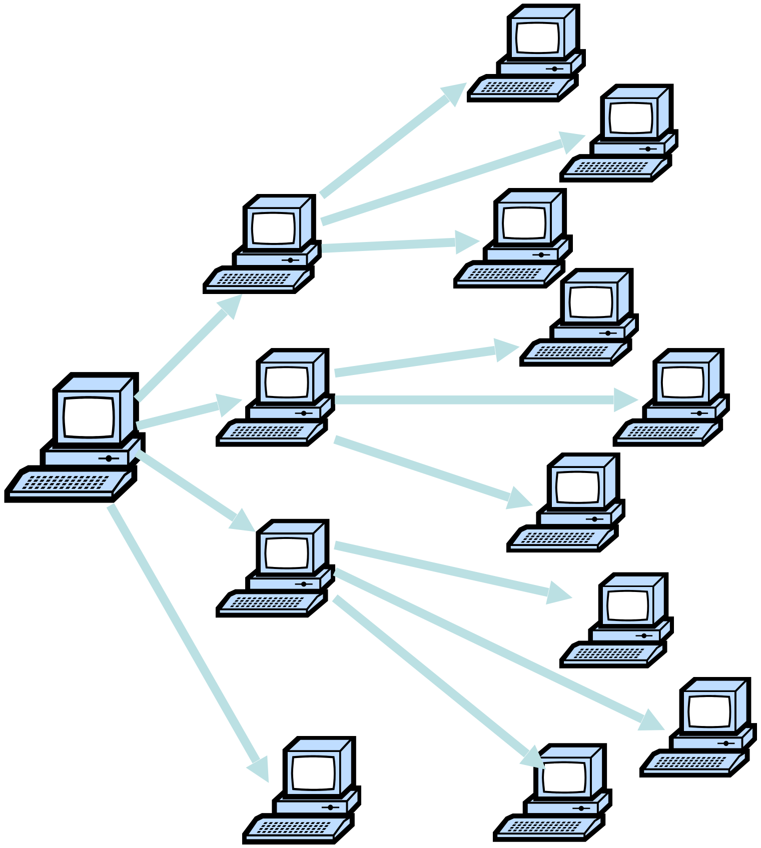
Large-Scale Malware

- Worm = code that self-propagates/replicates across systems by arranging to have itself immediately executed
  - Generally infects by altering running code
  - No user intervention required
- Propagation includes notions of targeting & exploit
  - How does the worm find new prospective victims?
  - How does worm get code to automatically run?
- Botnet = set of compromised machines ("bots") under a common command-and-control (C&C)
  - Attacker might use a worm to get the bots, or other techniques; orthogonal to bot's use in botnet

Rapid Propagation

Worms can potentially spread quickly because they **parallelize** the process of propagating/ replicating.

Same holds for viruses, but they often spread more slowly since require some sort of user action to trigger each propagation.



Worms

- Worm = code that self-propagates/replicates across systems by arranging to have itself immediately executed
  - Generally infects by altering running code
  - No user intervention required
- Propagation includes notions of targeting & exploit
  - How does the worm find new prospective victims?
    - One common approach: random scanning of 32-bit IP address space
      - Generate pseudo-random 32-bit number; try connecting to it; if successful, try infecting it; repeat
    - But for example "search worms" use Google results to find victims
  - How does worm get code to automatically run?
    - One common approach: buffer overflow ⇒ code injection
    - But for example a web worm might propagate using XSS

The Arrival of Internet Worms

- Worms date to Nov 2, 1988 - the *Morris Worm*
- ***Way*** ahead of its time
- Employed whole suite of tricks to infect systems …
  - *Multiple* buffer overflows
  - Guessable passwords
  - “Debug” configuration option that provided shell access
  - Common user accounts across multiple machines
- … and of tricks to find victims
  - Scan local subnet
  - Machines listed in system’s network config
  - Look through user files for mention of remote hosts

Arrival of Internet Worms, con't

- Modern Era began Jul 13, 2001 with release of initial version of Code Red
- Exploited known buffer overflow in Microsoft IIS Web servers
  - *On by default* in many systems
  - Vulnerability & fix announced previous month
- Payload part 1: web site defacement
  - `HELLO! Welcome to http://www.worm.com! Hacked By Chinese!`
  - Only done if language setting = English

Code Red of Jul 13 2001, con't

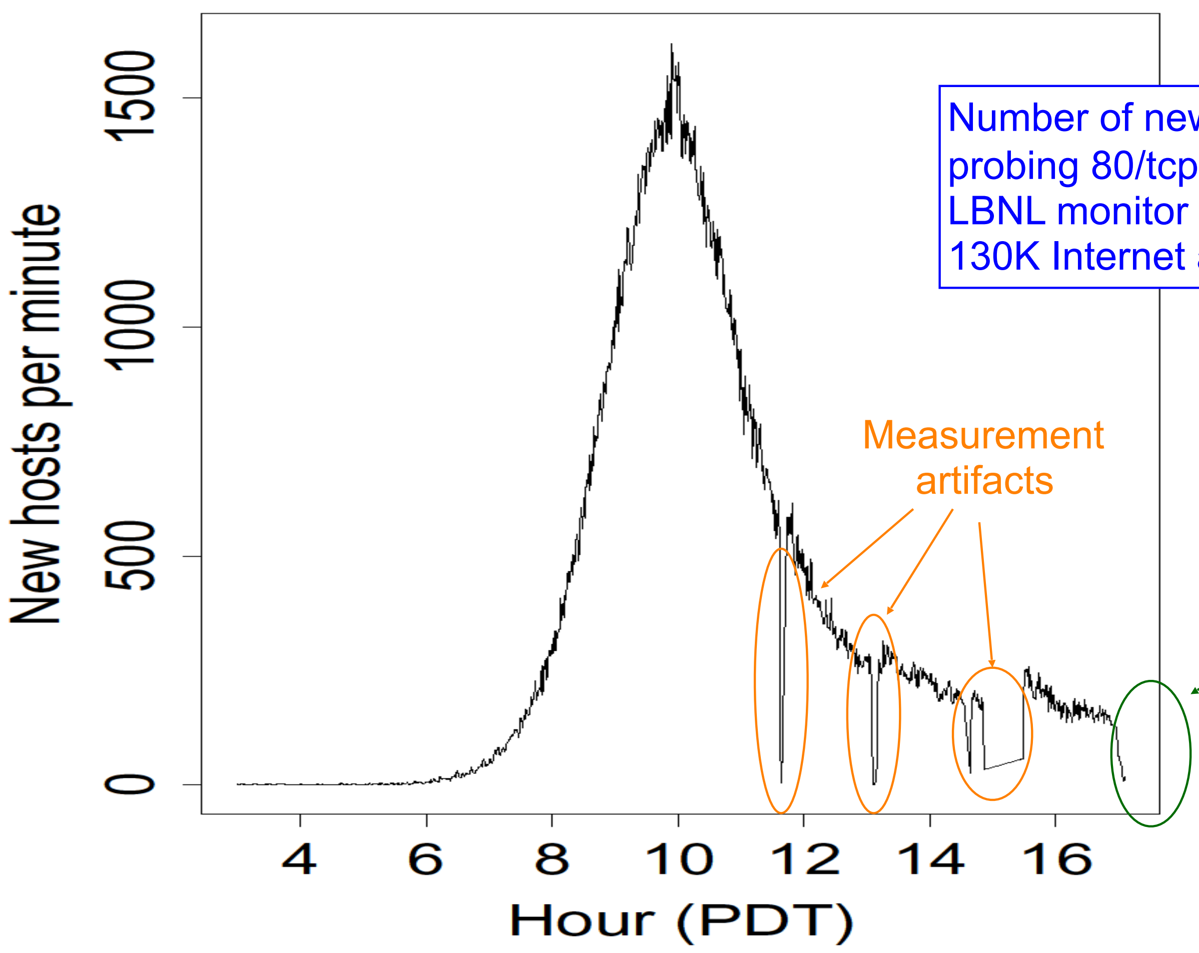
- Payload part 2: check day-of-the-month and …
  - … 1st through 20th of each month: spread
  - … 20th through end of each month: attack
    - Flooding attack against 198.137.240.91 …
    - … i.e., *www.whitehouse.gov*
- Spread: via *random scanning* of 32-bit IP address space
  - Generate pseudo-random 32-bit number; try connecting to it; if successful, try infecting it; repeat
  - Very common (but not fundamental) worm technique
- Each instance used same random number seed
  - How well does the worm spread?

Linear growth rate

Code Red, con’t

- Revision released July 19, 2001.
- White House responds to threat of flooding attack by changing the address of *www.whitehouse.gov*
- Causes Code Red to die for date ≥ 20th of the month due to failure of TCP connection to establish.
  - Author didn’t carefully test their code - buggy!
- But: this time random number generator correctly seeded. Bingo!

Growth of Code Red Worm



Number of new hosts probing 80/tcp as seen at LBNL monitor of 130K Internet addresses

Measurement artifacts

The worm dies off globally!

Nick's Reaction to Code Red

Surely Squigler.com is not vulnerable to XSS worms, right?

Yes, "Squiggler.com" was taken.

A Self Propagating Squig...

```
<div id="infection">
<marquee style="font-size: 200%; color: red; text-shadow:
                gold 0 0 10px;">
Dilbert is my hero.
</marquee>
<script>
// Copy the infection text out of the DOM.
var squig =
           document.getElementById("infection").outerHTML;
// Create and send a do_squig request.
var req = new XMLHttpRequest();
req.open("GET", "/do_squig?squig=" +
                encodeURIComponent(squig));
req.send();
</script>
</div>
```

(not quite a true worm as it requires a user to view it, but turns csrf into self propagating attack)

Modeling Worm Spread

- Worm-spread often well described as infectious epidemic
  - Classic SI model: homogeneous random contacts
    - SI = Susceptible-Infectible
- Model parameters:
  - N: population size
  - S(t): susceptible hosts at time t.
  - I(t): infected hosts at time t.
  - β: contact rate
    - How many population members each infected host communicates with per unit time
    - E.g., if each infected host scans 250 Internet addresses per unit time, and 2% of Internet addresses run a vulnerable (maybe already infected) server ⇒ β = 5
    - For scanning worms, larger (= denser) vulnerable pop. ⇒ higher β ⇒ faster worm!

$$\boxed{\begin{array}{c} N = S(t) + I(t) \\ S(0) = I(0) = N/2 \end{array}}$$

- Normalized versions reflecting relative proportion of infected/susceptible hosts
  - $s(t) = S(t)/N \quad i(t) = I(t)/N \quad s(t) + i(t) = 1$

Computing How An Epidemic Progresses

- In continuous time:

Increase in # infectibles per unit time

$$\frac{dI}{dt} = \beta \cdot I \cdot \frac{S}{N}$$

Proportion of contacts expected to succeed

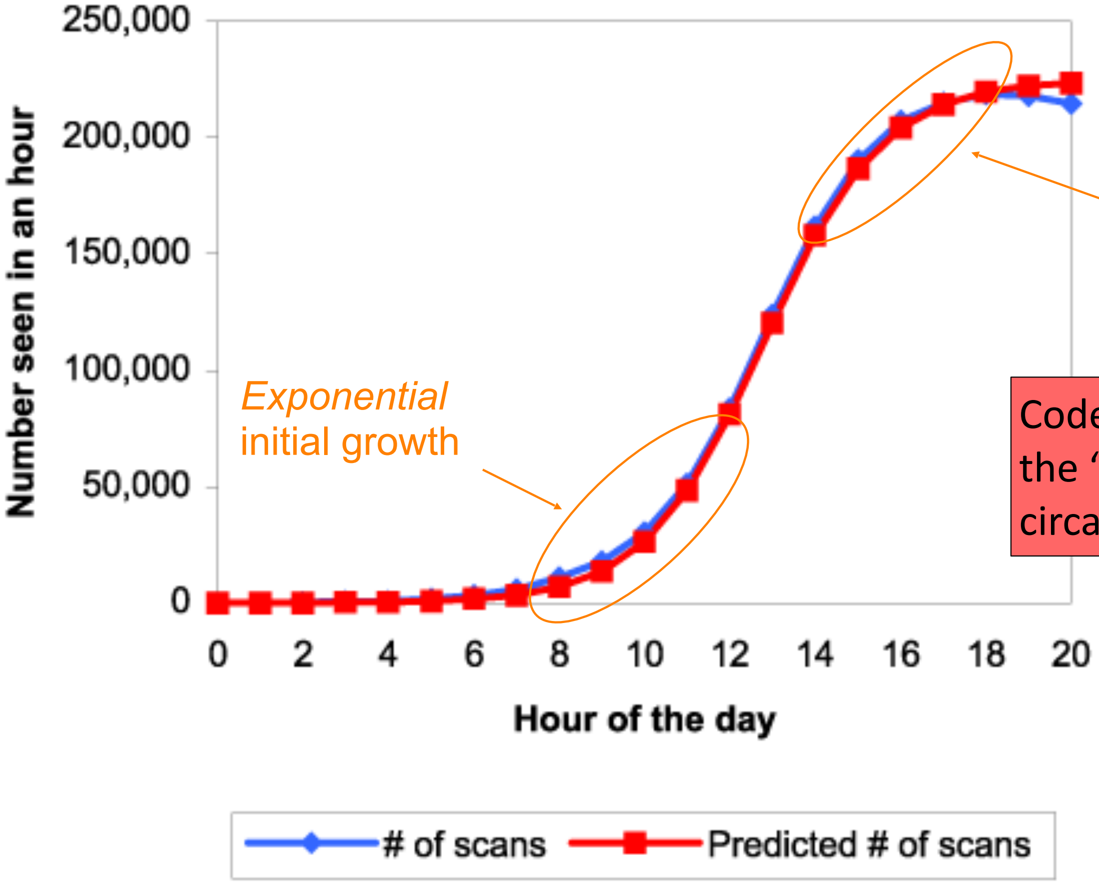
Total attempted contacts per unit time

- Rewriting by using i(t) = I(t)/N, S = N - I:

$$\frac{di}{dt} = \beta\, i(1 - i) \quad \Longrightarrow \quad i(t) = \frac{e^{\beta t}}{1 + e^{\beta t}}$$

Fraction infected grows as a *logistic*

Fitting the Model to “Code Red”

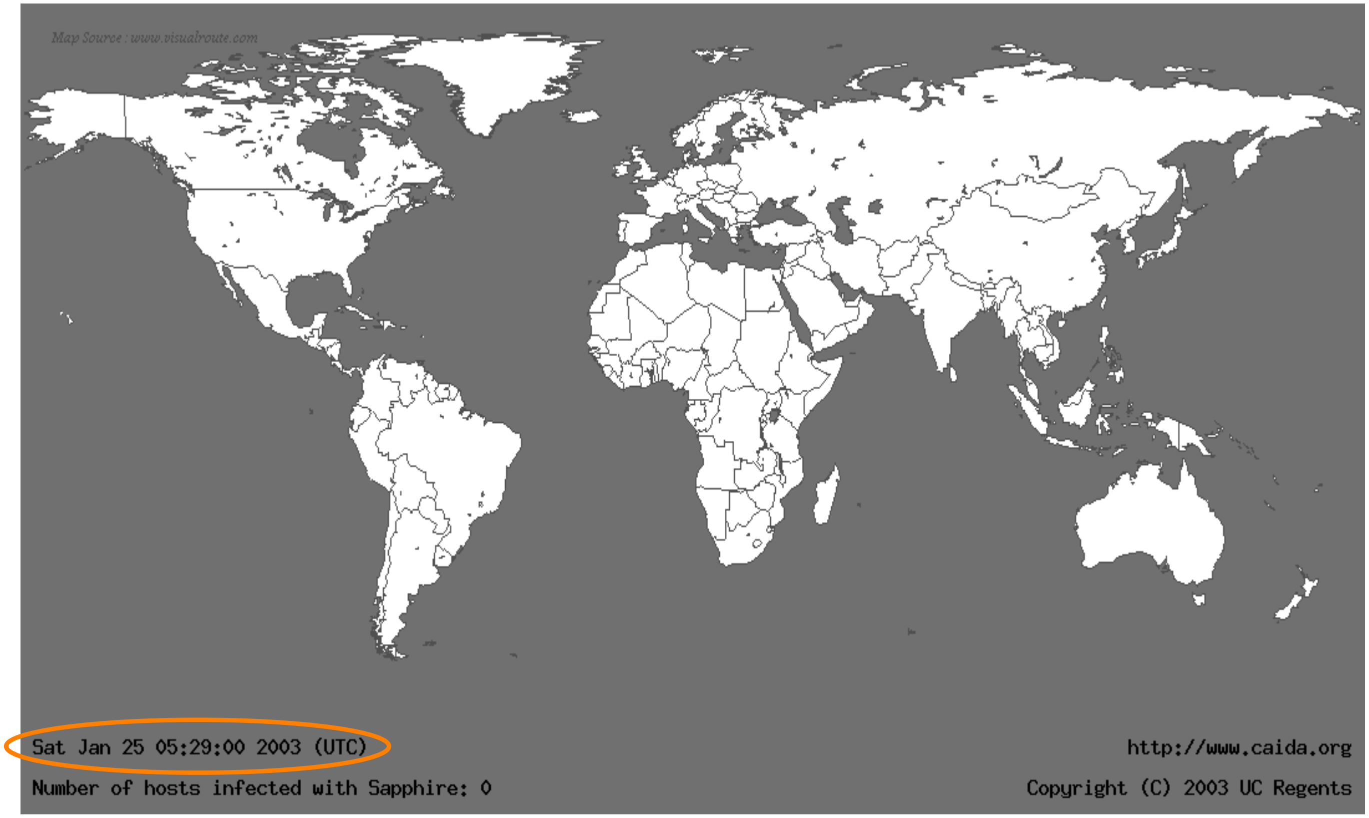


Exponential initial growth

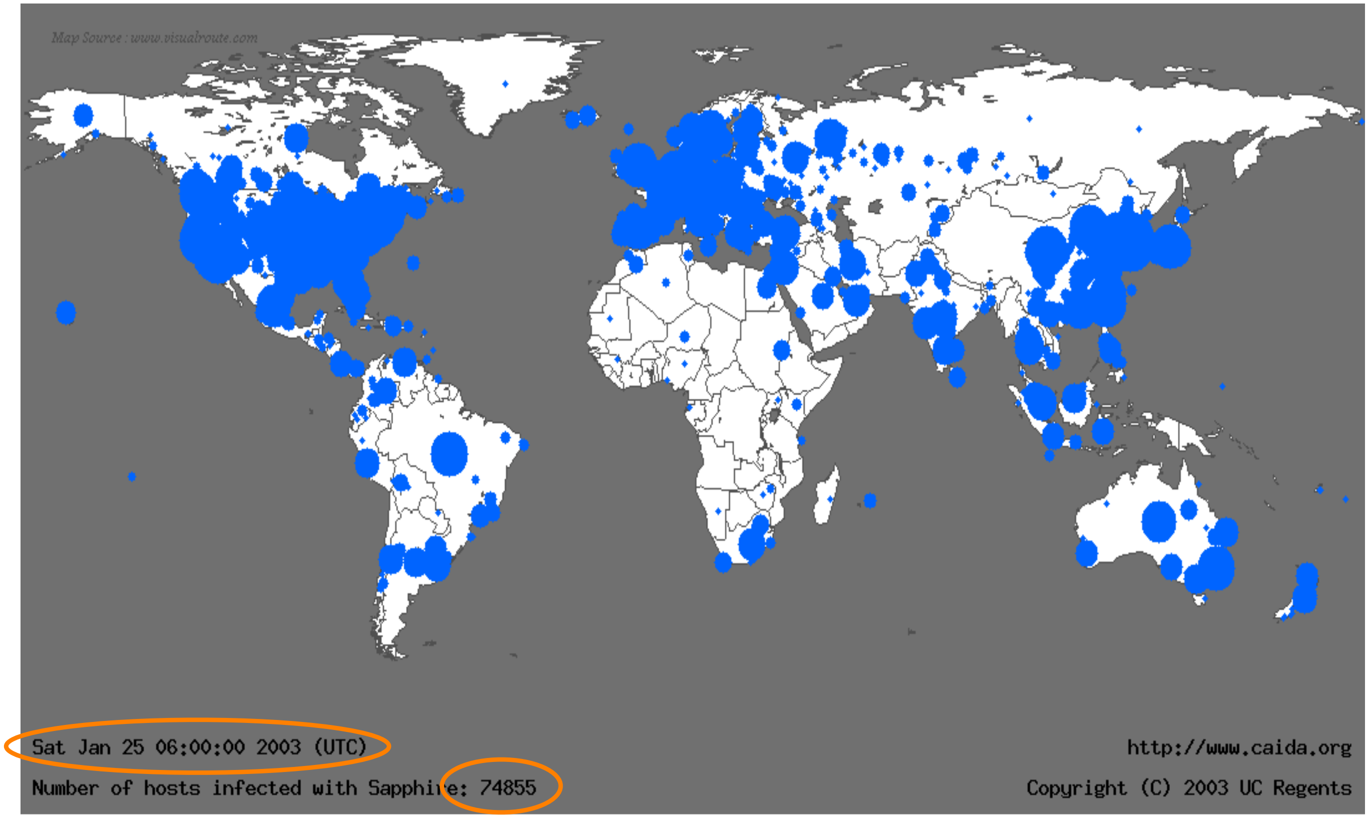
Growth slows as it becomes harder to find new victims!

Code Red = first worm of the “Modern Worm Era”, circa 2001.

Life Just Before Slammer


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

Life 10 Minutes After Slammer



Map Source : www.visualroute.com

Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

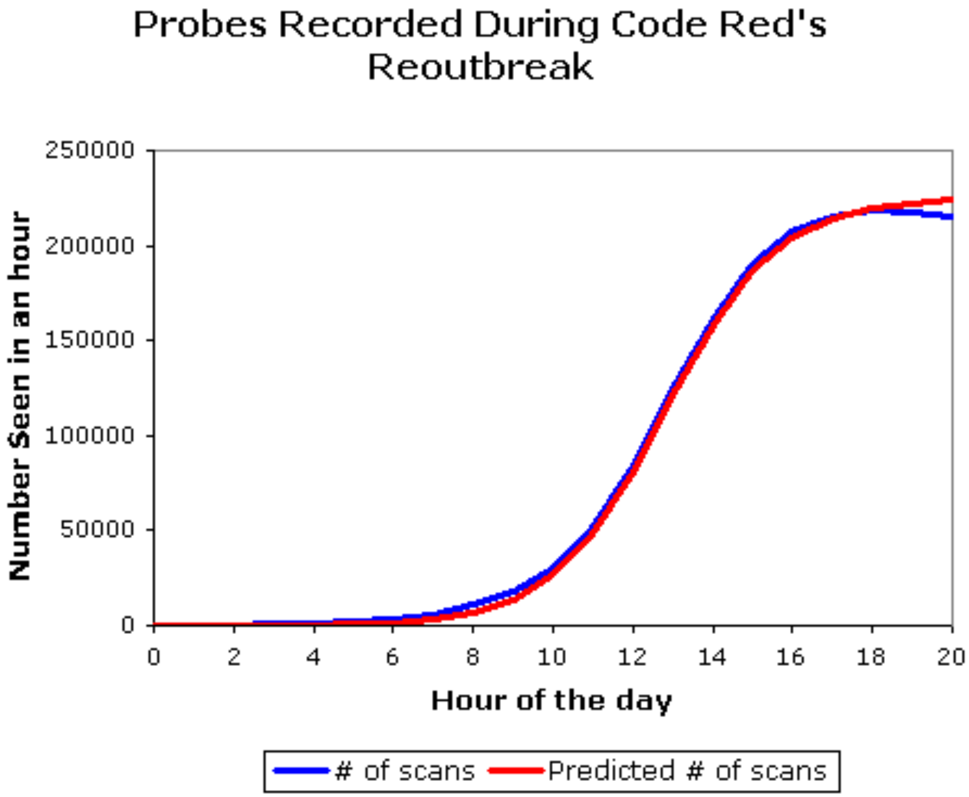
http://www.caida.org

Going Fast: Slammer

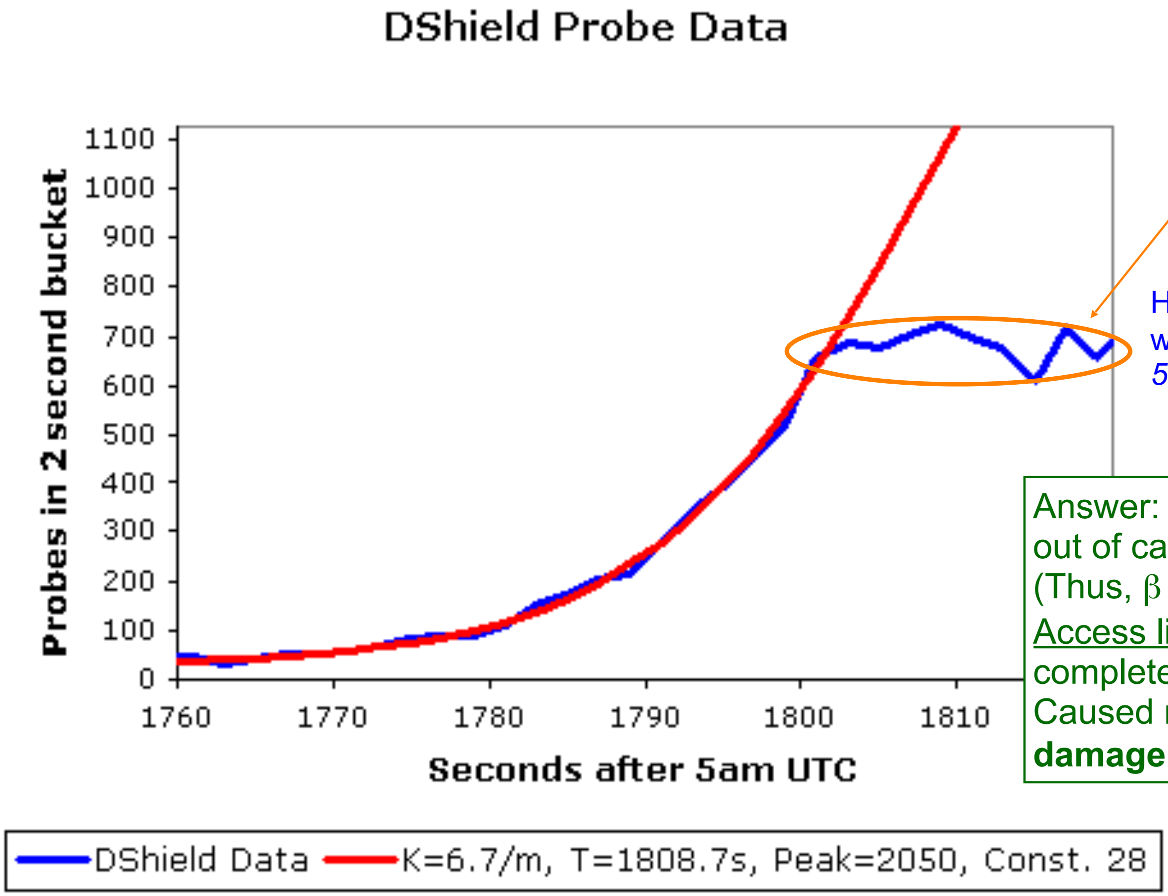
- Slammer exploited connectionless UDP service, rather than connection-oriented TCP
- Entire worm fit in a single packet!
- ⇒ When scanning, worm could “fire and forget”

  Stateless!
- Worm infected 75,000+ hosts in << 10 minutes
- At its peak, doubled every 8.5 seconds

The Usual Logistic Growth



Slammer’s Growth



What could have caused growth to deviate from the model?

Hint: at this point the worm is generating *55,000,000 scans/sec*

Answer: the Internet ran out of carrying capacity! (Thus, β decreased.) Access links used by worm completely clogged. Caused **major collateral damage**.

Witty...

- A worm like Slammer but with a twist...
  - Targeted network intrusion detection sensors!
  - Released ~36 hours after vulnerability disclosure and patch availability!
- Payload wasn't just spreading, however...

  -
    ```
    while true {
      for i := range(20000){
        send self to random target;
      }
      select random disk (0-7)
      if disk exists {
         select random block, erase it;
      }}
    ```

Stuxnet

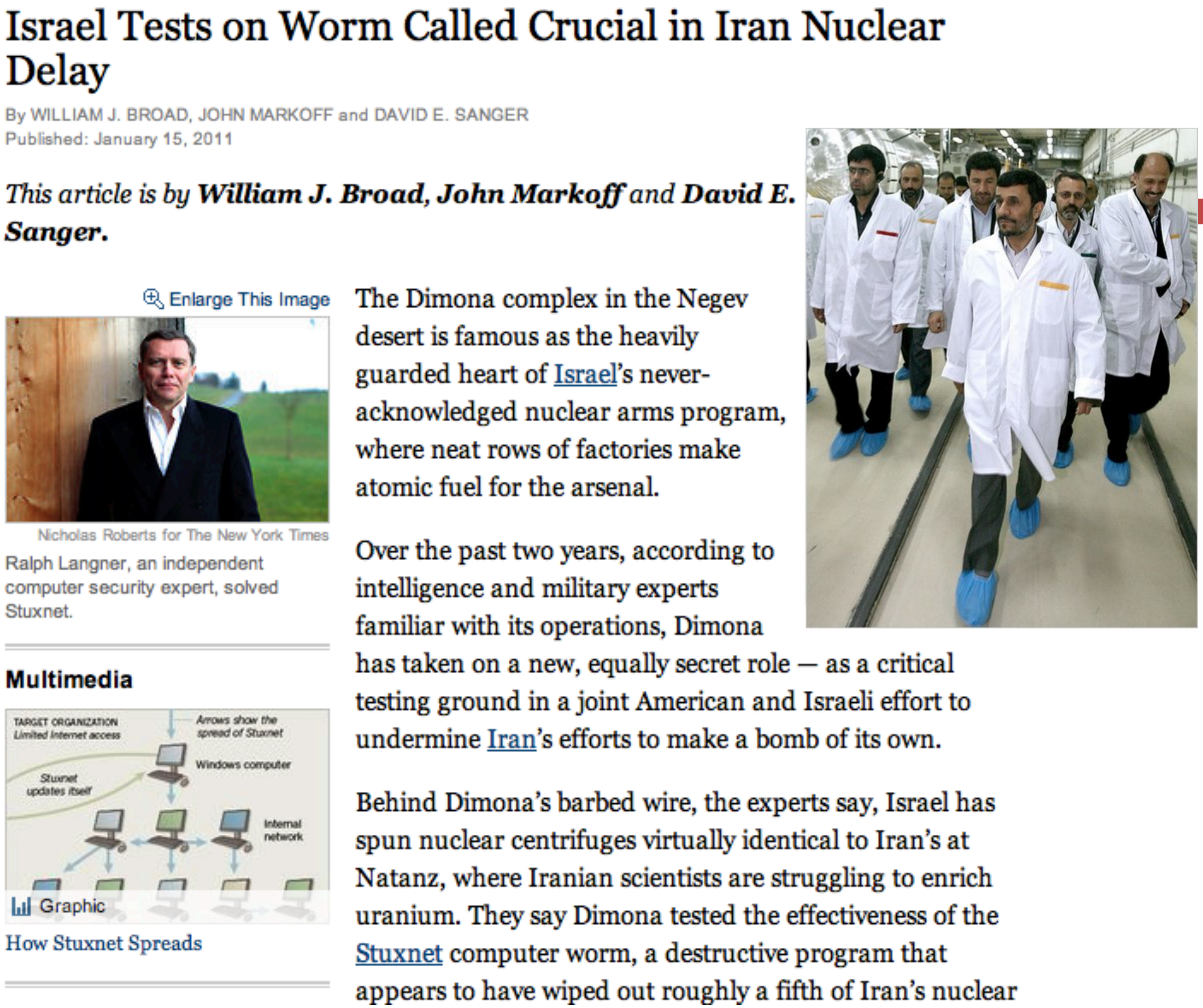
- Discovered July 2010. (Released: Mar 2010?)
- Multi-mode spreading:
  - Initially spreads via USB (virus-like)
  - Once inside a network, quickly spreads internally using Windows RPC scanning
- Kill switch: programmed to die June 24, 2012
- Targeted SCADA systems
  - Used for industrial control systems, like manufacturing, power plants
- Symantec: infections geographically clustered
  - Iran: 59%; Indonesia: 18%; India: 8%

Stuxnet, con’t

- Used four Zero Days
  - Unprecedented expense on the part of the author
- “Rootkit” for hiding infection based on installing Windows drivers with valid digital signatures
  - Attacker stole private keys for certificates from two companies in Taiwan
- Payload: do nothing …
  - … unless attached to particular models of frequency converter drives operating at 807-1210Hz
  - … like those made in Iran (and Finland) …
  - … and used to operate centrifuges for producing enriched uranium for nuclear weapons

Stuxnet, con’t

- Payload: do nothing …
  - … unless attached to particular models of frequency converter drives operating at 807-1210Hz
  - … like those made in Iran (and Finland) …
  - … and used to operate centrifuges for producing enriched uranium for nuclear weapons
- For these, worm would slowly increase drive frequency to 1410Hz
  - … enough to cause centrifuge to fly apart …
  - … while sending out fake readings from control system indicating everything was okay …
- … and then drop it back to normal range



Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

*This article is by **William J. Broad, John Markoff** and **David E. Sanger.***

Enlarge This Image

Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

Multimedia

How Stuxnet Spreads

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear

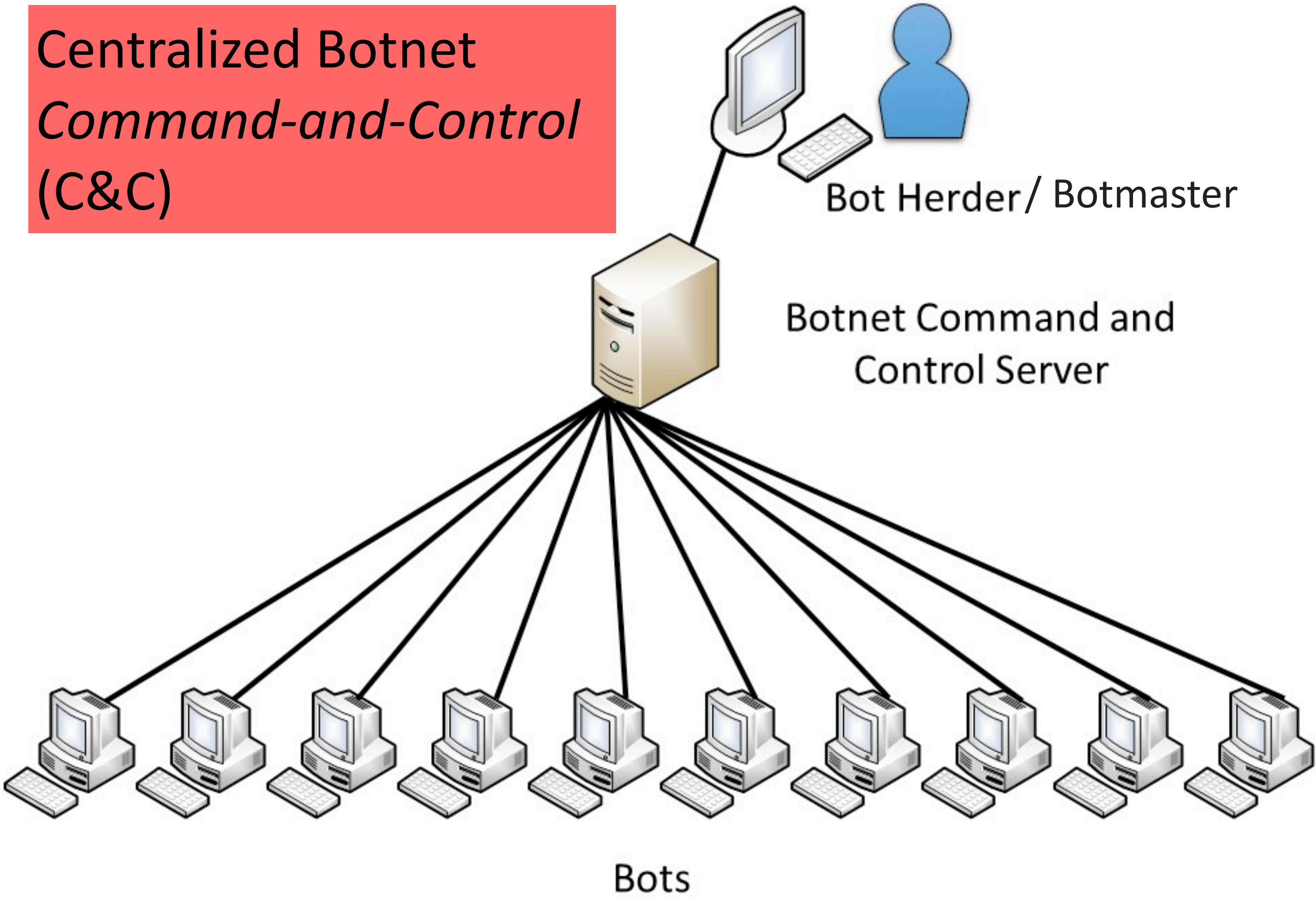
The "Toddler" Attack Payload...

- Stuxnet was very carefully engineered...
  - Designed to only go off under ***very specific*** circumstances
- But industrial control systems are inherently vulnerable
  - They consist of sensors and actuators
  - And safety is a ***global*** property
- Generic Boom:
  - At zero hour, the payload sees that it is on control system:
    map the sensors and actuators, see which ones are low speed vs high speed
  - T+30 minutes: Start replaying sensor data, switch actuators in low-speed system
  - T+60 minutes: Switch all actuators at high speed...
- This ***has been done***:
  A presumably Russian test attack on the Ukranian power grid! ("CrashOverride" attack)

Botnets

- Collection of compromised machines (bots) under (unified) control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm / virus / drive-by infection / etc.
  - (Or just buy the access – discussed later)
- Upon infection, new bot “phones home” to rendezvous w/ botnet command-and-control (C&C)
- Botmaster uses C&C to push out commands and updates
- Lots of ways to architect C&C:
  - Star topology; hierarchical; peer-to-peer
  - Encrypted/stealthy communication

Centralized Botnet *Command-and-Control* (C&C)



Example of C&C Messages

1. Activation (report from bot to botmaster)
2. Email address harvests
3. Spamming instructions
4. Delivery reports
5. DDoS instructions
6. *FastFlux* instructions (rapidly changing DNS)
7. HTTP proxy instructions
8. Sniffed passwords report
9. IFRAME injection/report

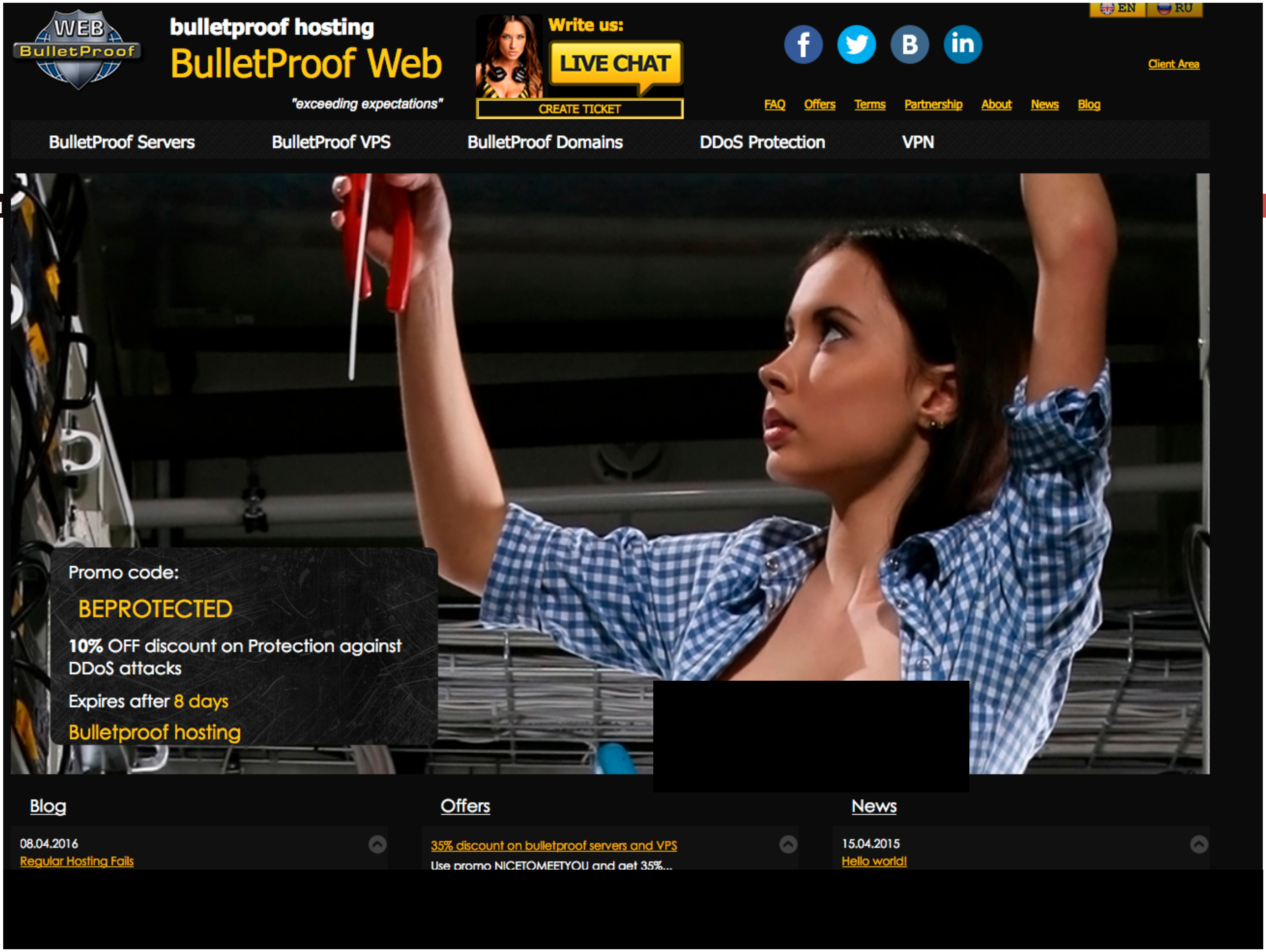
From the "Storm" botnet circa 2008

Fighting Bots / Botnets

- How can we defend against bots / botnets?
- Approach #1: prevent the initial bot infection
  - Equivalent to preventing malware infections in general …. HARD
- Approach #2: Take down the C&C master server
  - Find its IP address, get associated ISP to pull plug

Fighting Bots / Botnets

- How can we defend against bots / botnets?
- Approach #1: prevent the initial bot infection
  - Equivalent to preventing malware infections in general …. HARD
- Approach #2: Take down the C&C master server
  - Find its IP address, get associated ISP to pull plug
- Botmaster countermeasures?
  - Counter #1: keep moving around the master server
    - Bots resolve a domain name to find it (e.g. c-and-c.evil.com)
    - Rapidly alter address associated w/ name (“fast flux”)
  - Counter #2: buy off the ISP … (“bullet-proof hosting”)



Promo code:

BEPROTECTED

10% OFF discount on Protection against DDoS attacks

Expires after 8 days

Bulletproof hosting

[redacted]

Blog

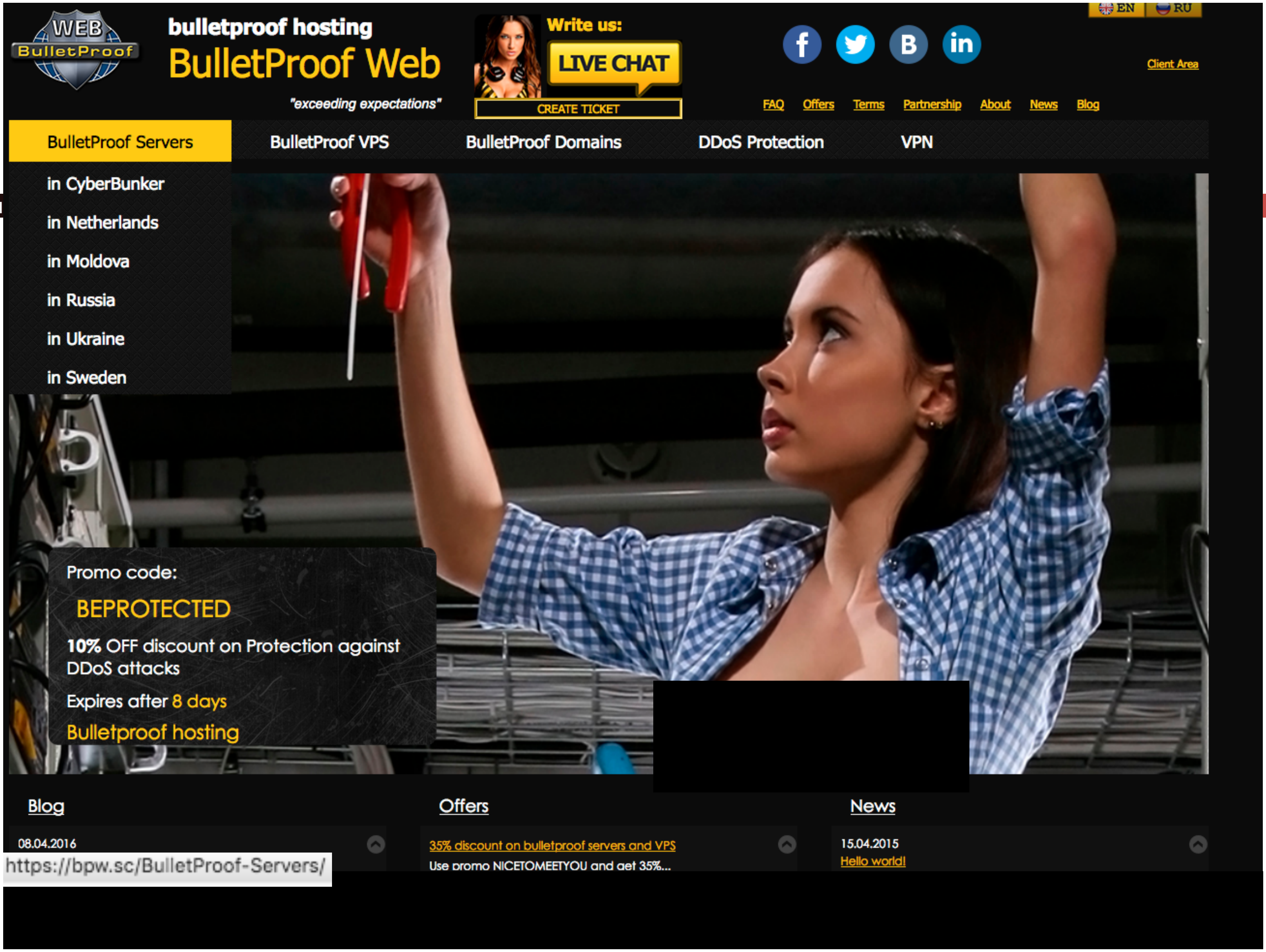
08.04.2016
Regular Hosting Fails

Offers

35% discount on bulletproof servers and VPS
Use promo NICETOMEETYOU and get 35%...

News

15.04.2015
Hello world!



EN RU

bulletproof hosting

BulletProof Web

"exceeding expectations"

Write us:

LIVE CHAT

CREATE TICKET

Client Area

FAQ Offers Terms Partnership About News Blog

BulletProof Servers | BulletProof VPS | BulletProof Domains | DDoS Protection | VPN

- in CyberBunker
- in Netherlands
- in Moldova
- in Russia
- in Ukraine
- in Sweden

Promo code:

BEPROTECTED

10% OFF discount on Protection against DDoS attacks

Expires after 8 days

Bulletproof hosting

[redacted]

Blog

08.04.2016

Offers

35% discount on bulletproof servers and VPS

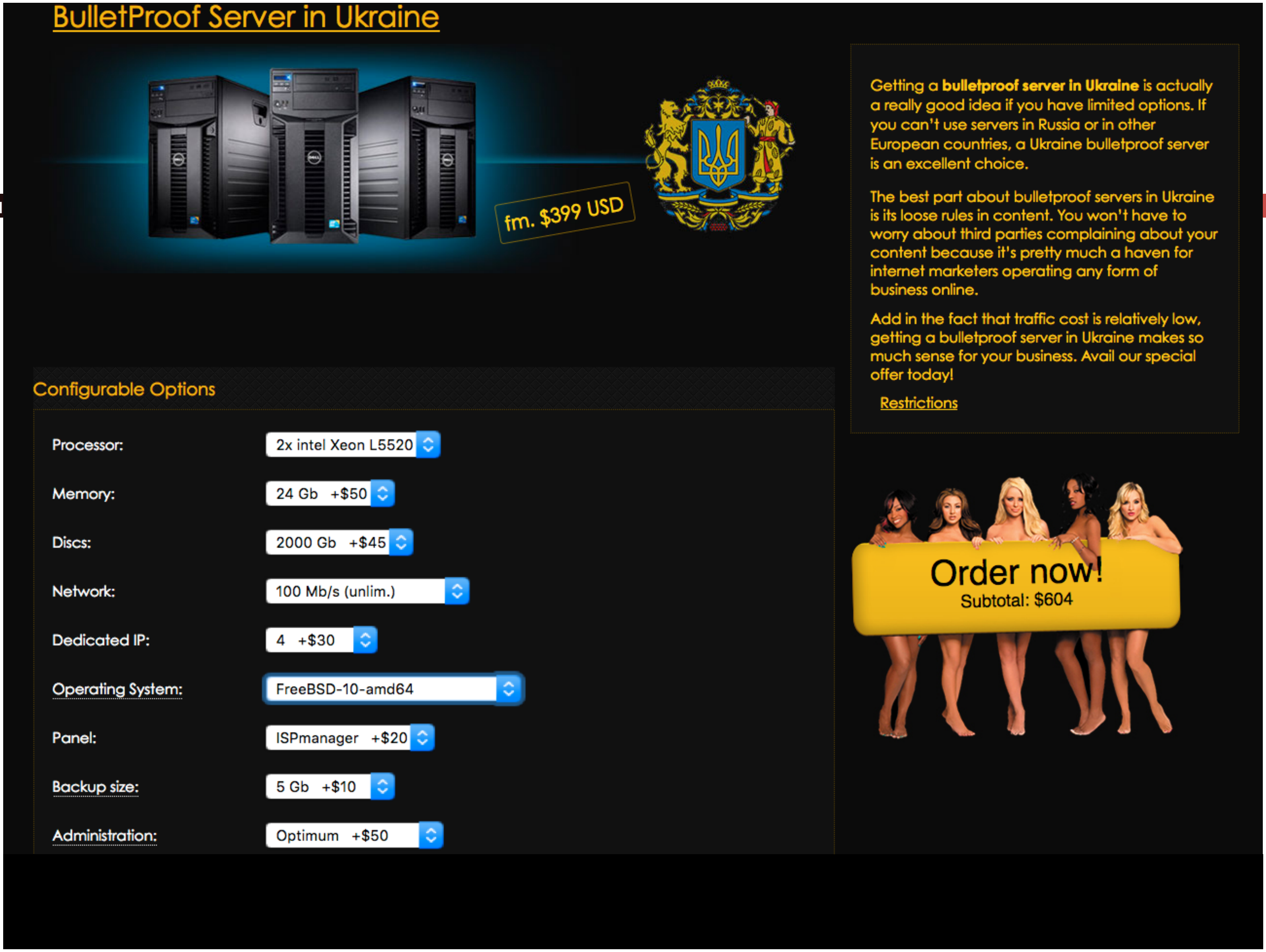
Use promo NICETOMEETYOU and get 35%...

News

15.04.2015

Hello world!

https://bpw.sc/BulletProof-Servers/



BulletProof Server in Ukraine

Getting a **bulletproof server in Ukraine** is actually a really good idea if you have limited options. If you can't use servers in Russia or in other European countries, a Ukraine bulletproof server is an excellent choice.

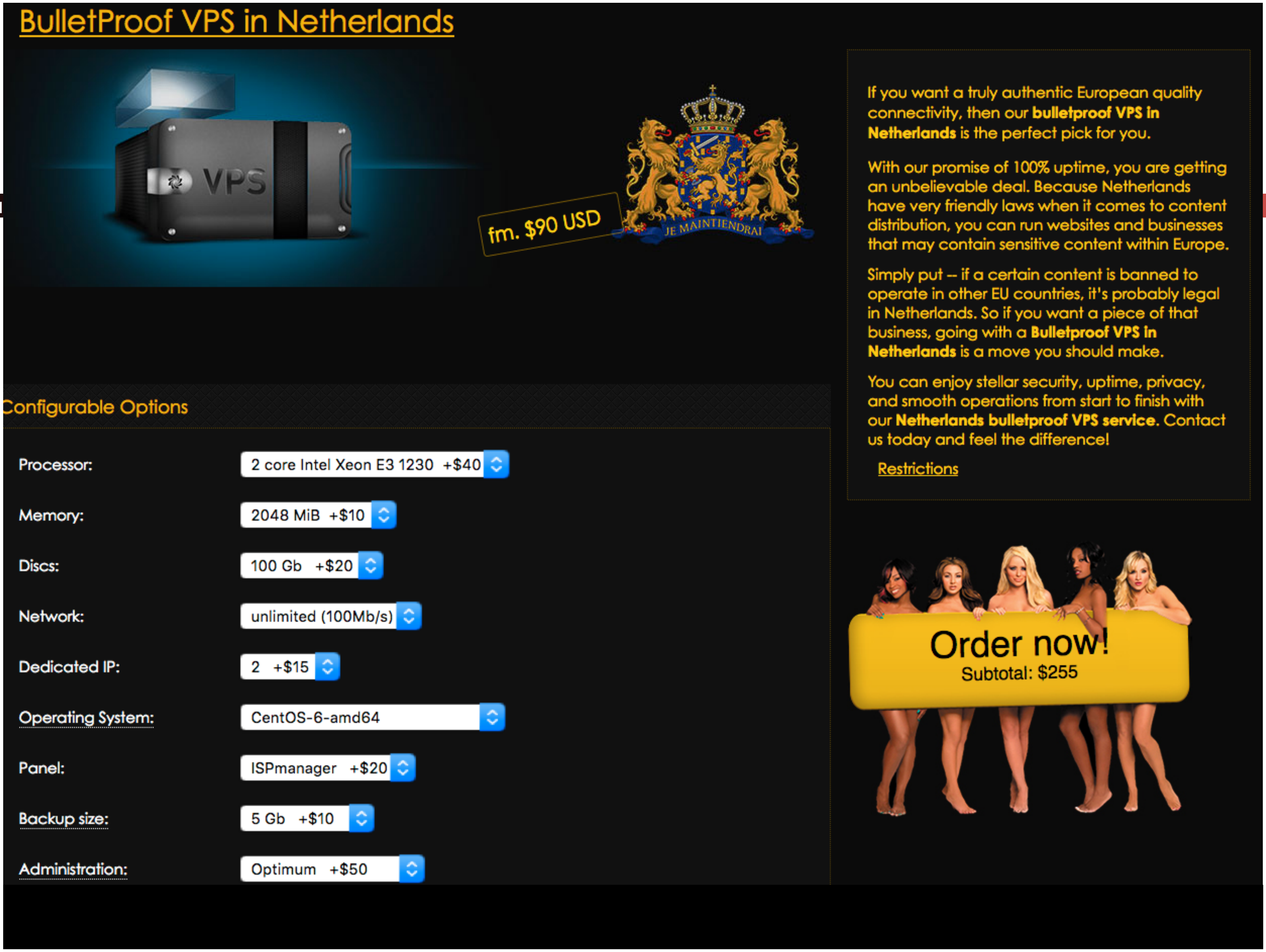
The best part about bulletproof servers in Ukraine is its loose rules in content. You won't have to worry about third parties complaining about your content because it's pretty much a haven for internet marketers operating any form of business online.

Add in the fact that traffic cost is relatively low, getting a bulletproof server in Ukraine makes so much sense for your business. Avail our special offer today!

Restrictions

Configurable Options

Processor:	2x intel Xeon L5520
Memory:	24 Gb +$50
Discs:	2000 Gb +$45
Network:	100 Mb/s (unlim.)
Dedicated IP:	4 +$30
Operating System:	FreeBSD-10-amd64
Panel:	ISPmanager +$20
Backup size:	5 Gb +$10
Administration:	Optimum +$50



BulletProof VPS in Netherlands

If you want a truly authentic European quality connectivity, then our **bulletproof VPS in Netherlands** is the perfect pick for you.

With our promise of 100% uptime, you are getting an unbelievable deal. Because Netherlands have very friendly laws when it comes to content distribution, you can run websites and businesses that may contain sensitive content within Europe.

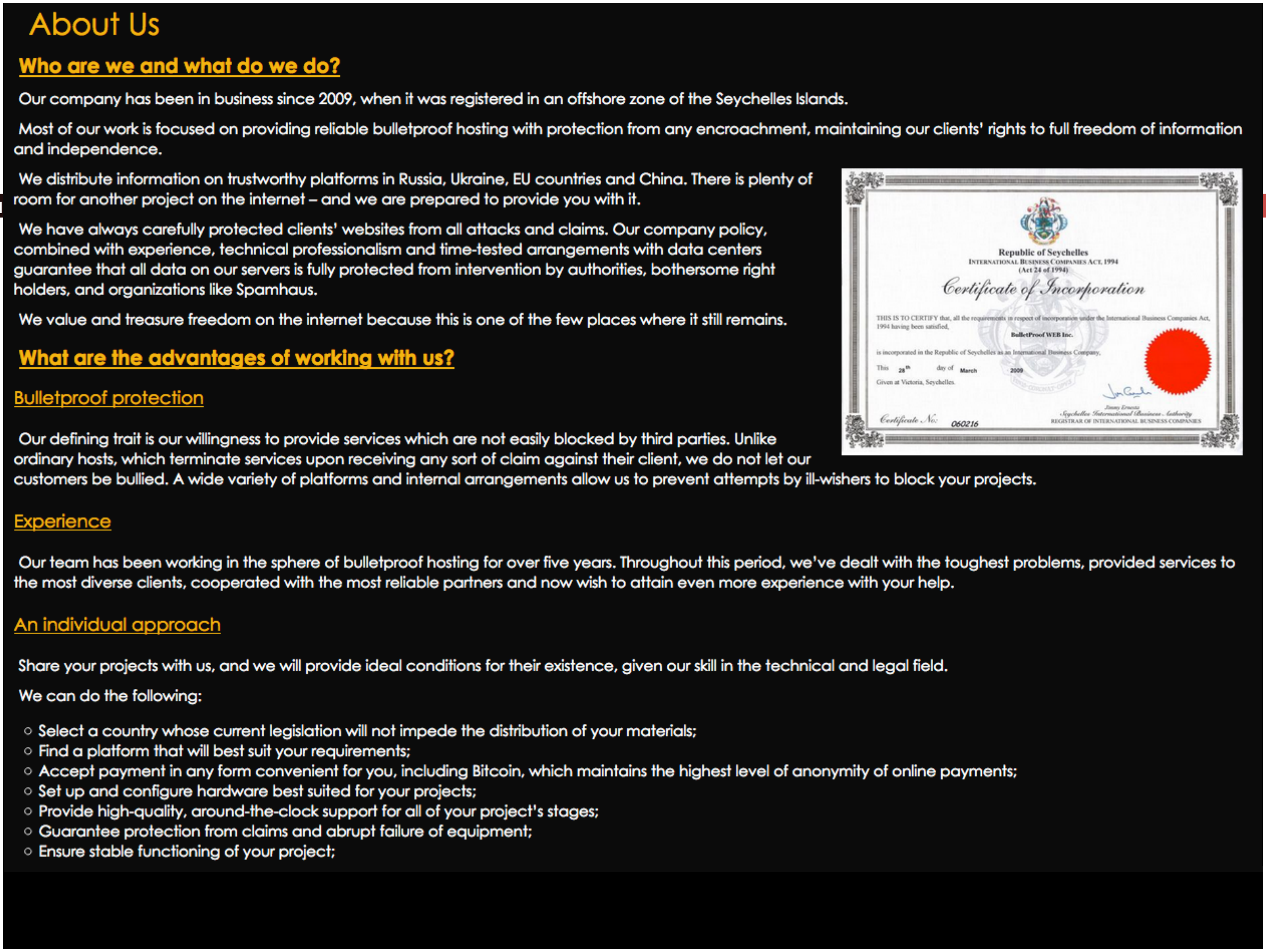
Simply put – if a certain content is banned to operate in other EU countries, it's probably legal in Netherlands. So if you want a piece of that business, going with a **Bulletproof VPS in Netherlands** is a move you should make.

You can enjoy stellar security, uptime, privacy, and smooth operations from start to finish with our **Netherlands bulletproof VPS service**. Contact us today and feel the difference!

Restrictions

Configurable Options

Processor:	2 core Intel Xeon E3 1230 +$40
Memory:	2048 MiB +$10
Discs:	100 Gb +$20
Network:	unlimited (100Mb/s)
Dedicated IP:	2 +$15
Operating System:	CentOS-6-amd64
Panel:	ISPmanager +$20
Backup size:	5 Gb +$10
Administration:	Optimum +$50



About Us

Who are we and what do we do?

Our company has been in business since 2009, when it was registered in an offshore zone of the Seychelles Islands.

Most of our work is focused on providing reliable bulletproof hosting with protection from any encroachment, maintaining our clients' rights to full freedom of information and independence.

We distribute information on trustworthy platforms in Russia, Ukraine, EU countries and China. There is plenty of room for another project on the internet – and we are prepared to provide you with it.

We have always carefully protected clients' websites from all attacks and claims. Our company policy, combined with experience, technical professionalism and time-tested arrangements with data centers guarantee that all data on our servers is fully protected from intervention by authorities, bothersome right holders, and organizations like Spamhaus.

We value and treasure freedom on the internet because this is one of the few places where it still remains.

What are the advantages of working with us?

Bulletproof protection

Our defining trait is our willingness to provide services which are not easily blocked by third parties. Unlike ordinary hosts, which terminate services upon receiving any sort of claim against their client, we do not let our customers be bullied. A wide variety of platforms and internal arrangements allow us to prevent attempts by ill-wishers to block your projects.

Republic of Seychelles
INTERNATIONAL BUSINESS COMPANIES ACT, 1994
(Act 24 of 1994)

Certificate of Incorporation

THIS IS TO CERTIFY that, all the requirements in respect of incorporation under the International Business Companies Act, 1994 having been satisfied,

BulletProof WEB Inc.

is incorporated in the Republic of Seychelles as an International Business Company,

This 28th day of March 2009

Given at Victoria, Seychelles.

Jimmy Ernesta
Seychelles International Business Authority
REGISTRAR OF INTERNATIONAL BUSINESS COMPANIES

Certificate No: 060216

Experience

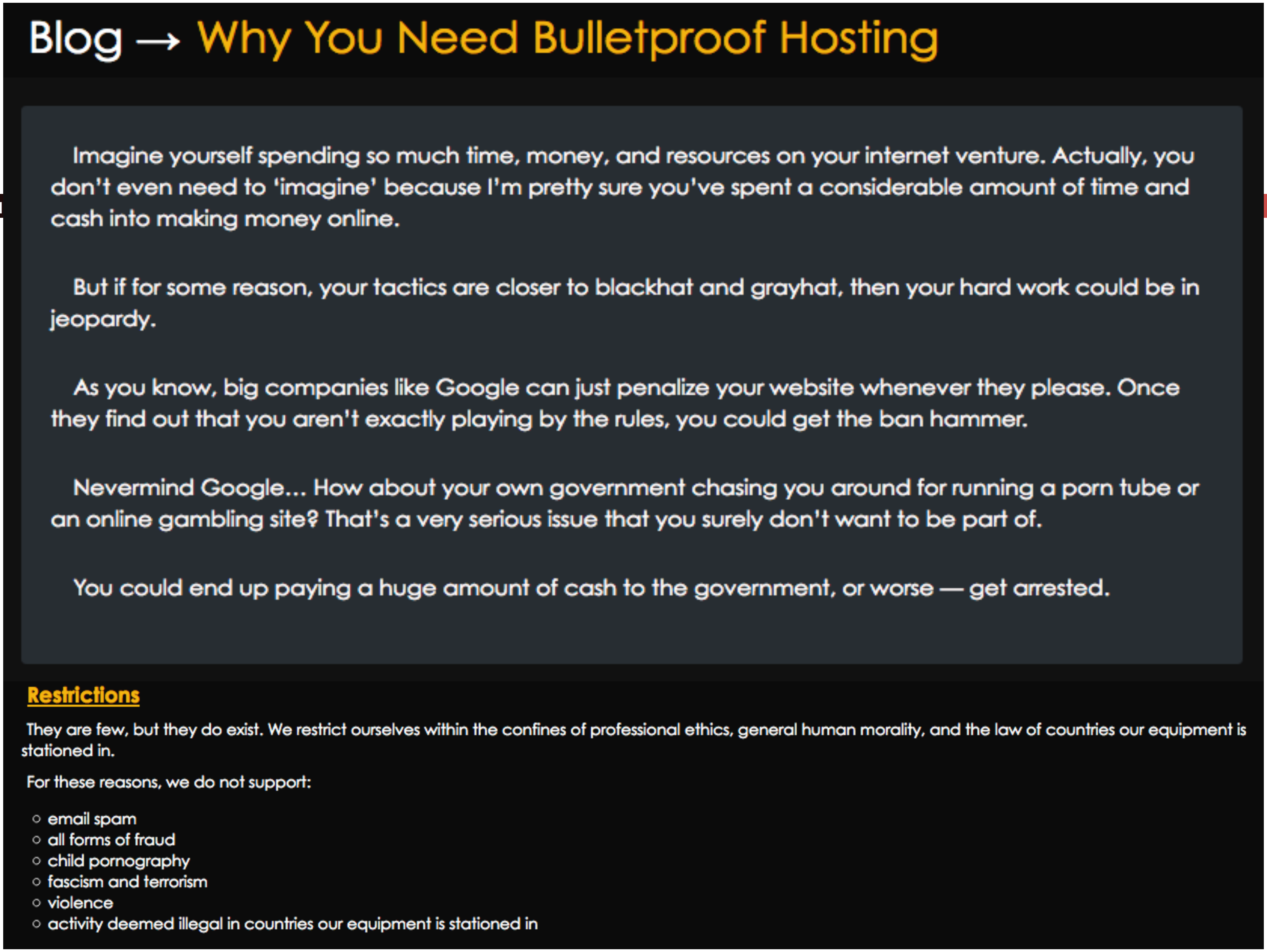
Our team has been working in the sphere of bulletproof hosting for over five years. Throughout this period, we've dealt with the toughest problems, provided services to the most diverse clients, cooperated with the most reliable partners and now wish to attain even more experience with your help.

An individual approach

Share your projects with us, and we will provide ideal conditions for their existence, given our skill in the technical and legal field.

We can do the following:

- Select a country whose current legislation will not impede the distribution of your materials;
- Find a platform that will best suit your requirements;
- Accept payment in any form convenient for you, including Bitcoin, which maintains the highest level of anonymity of online payments;
- Set up and configure hardware best suited for your projects;
- Provide high-quality, around-the-clock support for all of your project's stages;
- Guarantee protection from claims and abrupt failure of equipment;
- Ensure stable functioning of your project;



Blog → Why You Need Bulletproof Hosting

Imagine yourself spending so much time, money, and resources on your internet venture. Actually, you don't even need to 'imagine' because I'm pretty sure you've spent a considerable amount of time and cash into making money online.

But if for some reason, your tactics are closer to blackhat and grayhat, then your hard work could be in jeopardy.

As you know, big companies like Google can just penalize your website whenever they please. Once they find out that you aren't exactly playing by the rules, you could get the ban hammer.

Nevermind Google... How about your own government chasing you around for running a porn tube or an online gambling site? That's a very serious issue that you surely don't want to be part of.

You could end up paying a huge amount of cash to the government, or worse — get arrested.

Restrictions

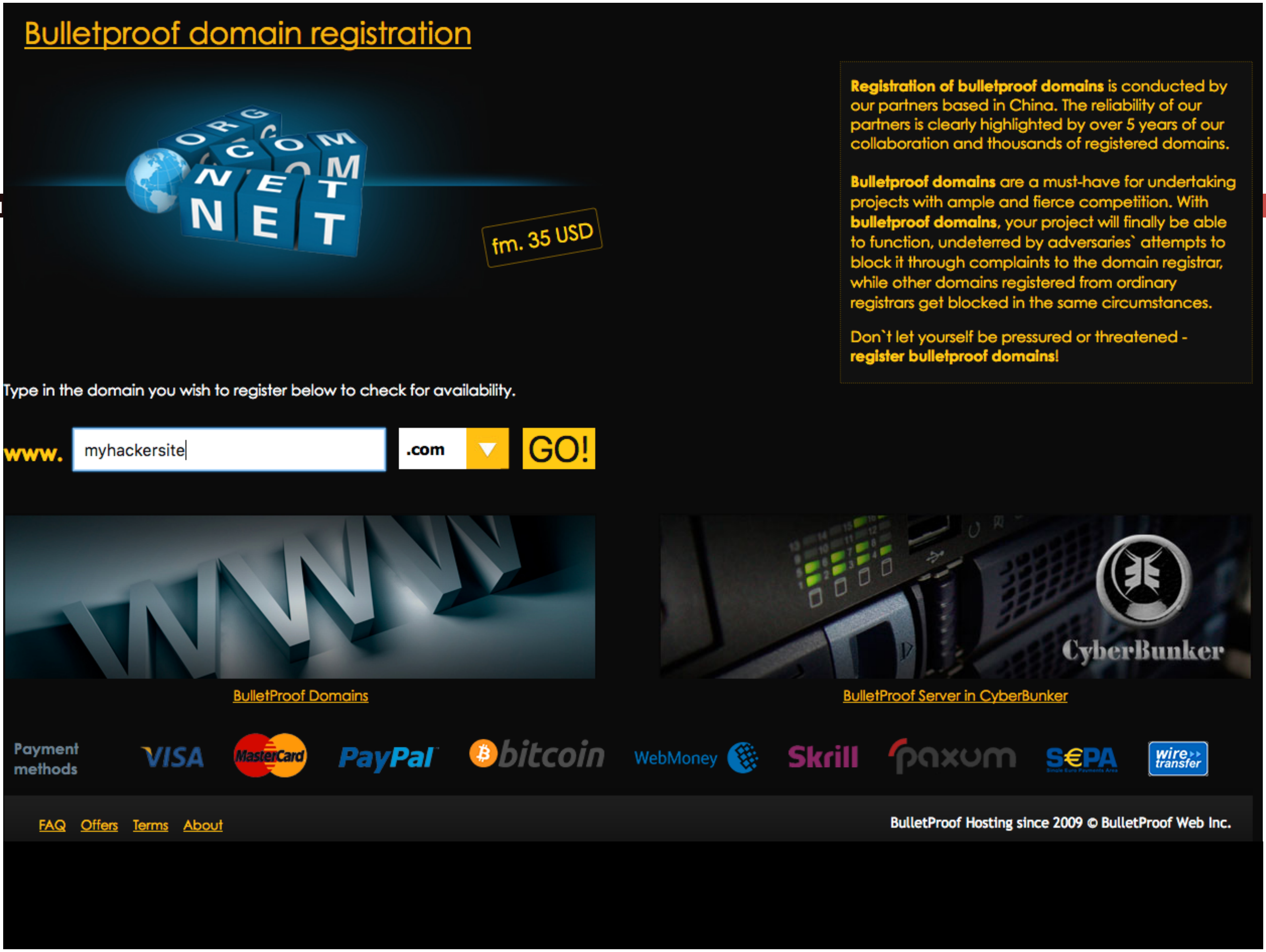
They are few, but they do exist. We restrict ourselves within the confines of professional ethics, general human morality, and the law of countries our equipment is stationed in.

For these reasons, we do not support:

- email spam
- all forms of fraud
- child pornography
- fascism and terrorism
- violence
- activity deemed illegal in countries our equipment is stationed in

Fighting Bots / Botnets, con’t

- Approach #3: seize the domain name used for C&C
- … Botmaster counter-measure?
- Business counter-measure: bullet-proof domains



Bulletproof domain registration

Registration of bulletproof domains is conducted by our partners based in China. The reliability of our partners is clearly highlighted by over 5 years of our collaboration and thousands of registered domains.

Bulletproof domains are a must-have for undertaking projects with ample and fierce competition. With **bulletproof domains**, your project will finally be able to function, undeterred by adversaries` attempts to block it through complaints to the domain registrar, while other domains registered from ordinary registrars get blocked in the same circumstances.

Don`t let yourself be pressured or threatened - **register bulletproof domains!**

Type in the domain you wish to register below to check for availability.

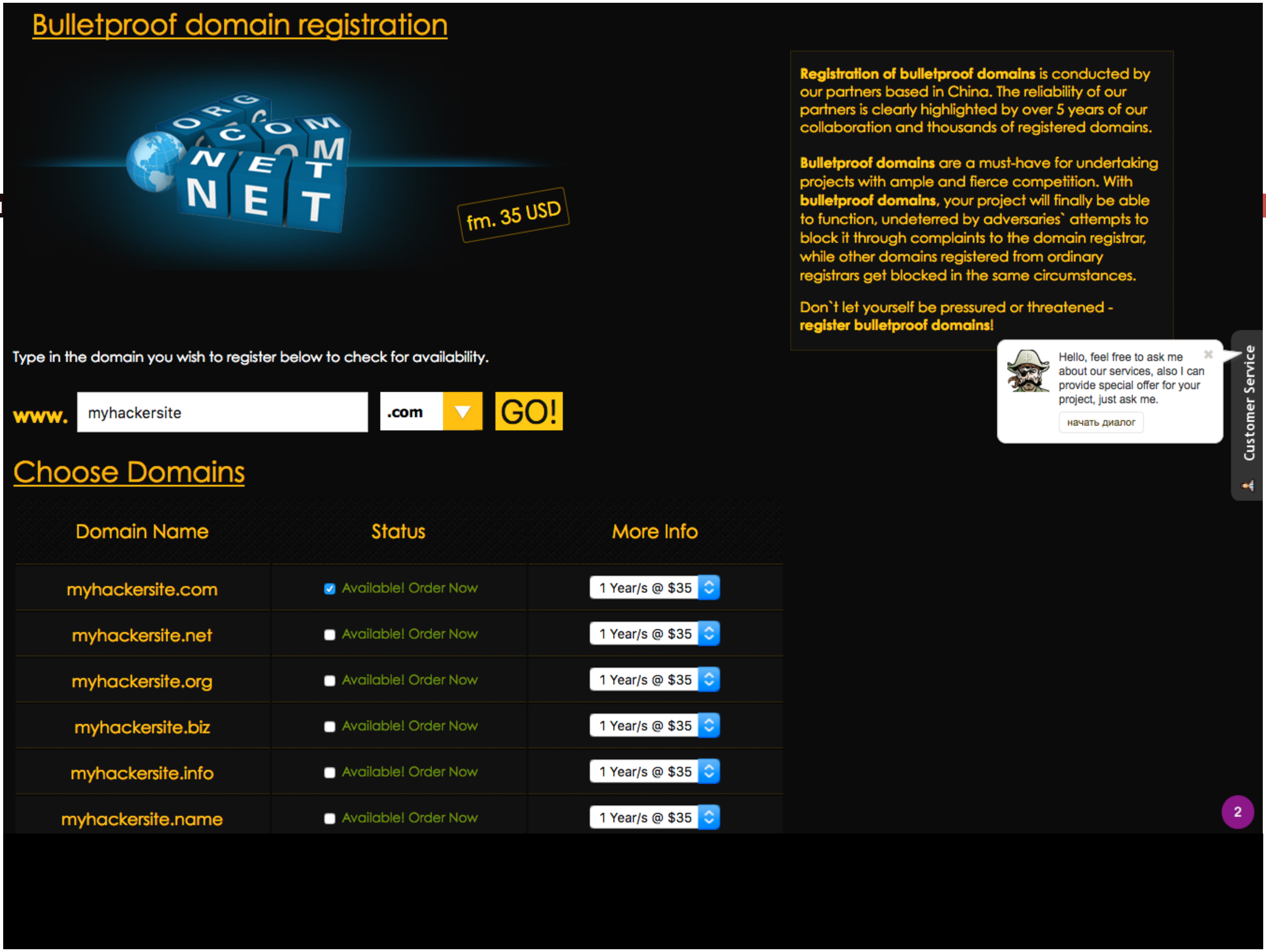
www. myhackersite .com GO!

BulletProof Domains

BulletProof Server in CyberBunker

FAQ Offers Terms About

BulletProof Hosting since 2009 © BulletProof Web Inc.



Bulletproof domain registration

Registration of bulletproof domains is conducted by our partners based in China. The reliability of our partners is clearly highlighted by over 5 years of our collaboration and thousands of registered domains.

Bulletproof domains are a must-have for undertaking projects with ample and fierce competition. With **bulletproof domains**, your project will finally be able to function, undeterred by adversaries` attempts to block it through complaints to the domain registrar, while other domains registered from ordinary registrars get blocked in the same circumstances.

Don`t let yourself be pressured or threatened - **register bulletproof domains!**

Type in the domain you wish to register below to check for availability.

www. myhackersite .com GO!

Hello, feel free to ask me about our services, also I can provide special offer for your project, just ask me.

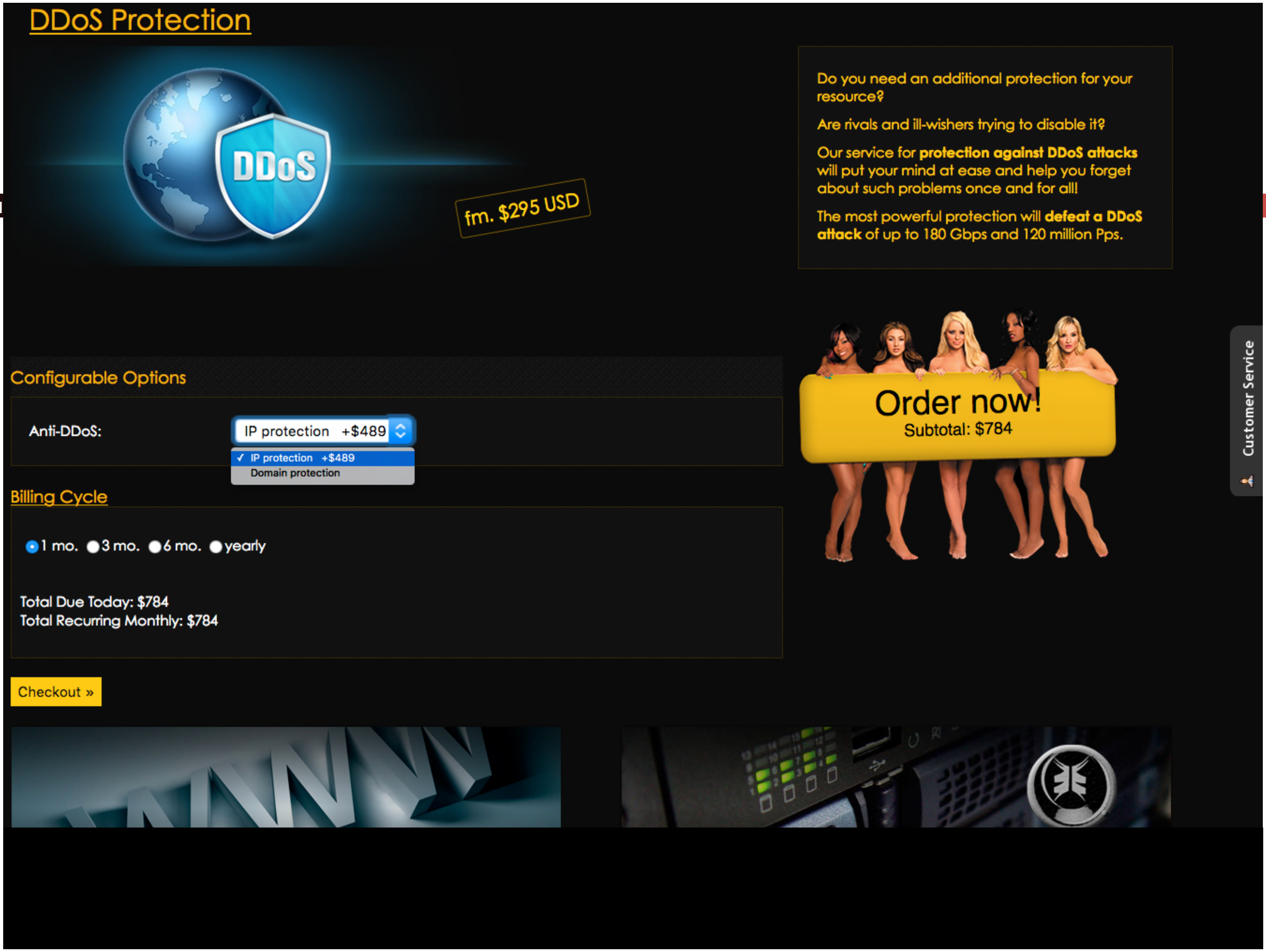
начать диалог

Customer Service

Choose Domains

Domain Name	Status	More Info
myhackersite.com	☑ Available! Order Now	1 Year/s @ $35
myhackersite.net	☐ Available! Order Now	1 Year/s @ $35
myhackersite.org	☐ Available! Order Now	1 Year/s @ $35
myhackersite.biz	☐ Available! Order Now	1 Year/s @ $35
myhackersite.info	☐ Available! Order Now	1 Year/s @ $35
myhackersite.name	☐ Available! Order Now	1 Year/s @ $35

2



DDoS Protection

fm. $295 USD

Do you need an additional protection for your resource?

Are rivals and ill-wishers trying to disable it?

Our service for **protection against DDoS attacks** will put your mind at ease and help you forget about such problems once and for all!

The most powerful protection will **defeat a DDoS attack** of up to 180 Gbps and 120 million Pps.

Order now!
Subtotal: $784

Configurable Options

Anti-DDoS: IP protection +$489

✓ IP protection +$489
Domain protection

Billing Cycle

● 1 mo. ○ 3 mo. ○ 6 mo. ○ yearly

Total Due Today: $784
Total Recurring Monthly: $784

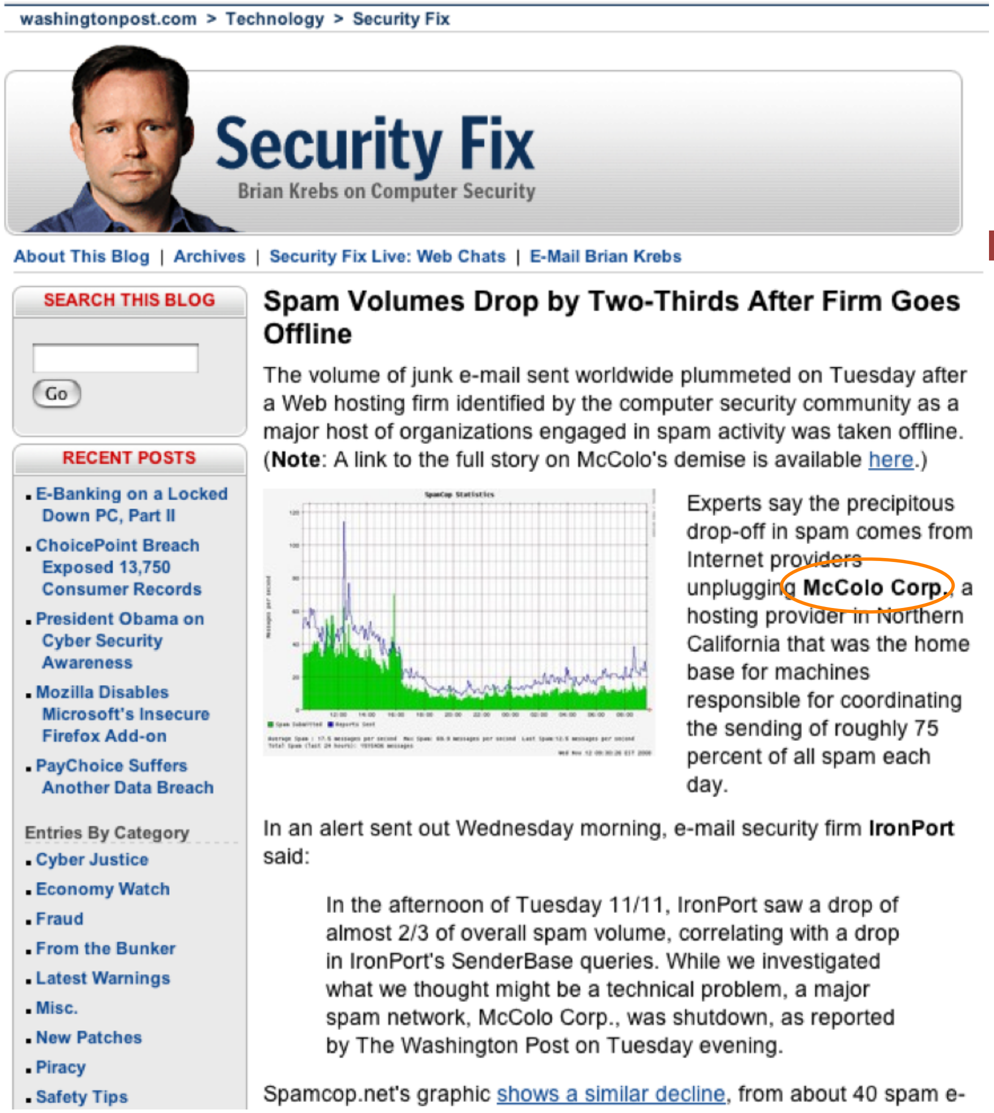
Checkout »

Fighting Bots / Botnets, con’t

- Approach #3: seize the domain name used for C&C
- … Botmaster counter-measure?
- Business counter-measure: bullet-proof domains
- Technical counter-measure: DGAs
  - Each day (say), bots generate large list of possible domain names using a Domain Generation Algorithm
    - Large = 50K, in some cases
    - E.g.: eqxowsn.info, ggegtugh.info, hquterpacw.net, oumaac.com, qfiadxb.net, rwyoehbkhdhb.info, rzziyf.info, vmlbhdvtjrn.org, yeiesmomgeso.org, yeuqik.com, yfewtvnpdk.info, zffezlkgfnox.net
  - Bots then try a random subset looking for a C&C server
    - Server signs its replies, so bot can’t be duped
    - Attacker just needs to register & hang onto a small portion of names to retain control over botnet

Fighting Bots / Botnets, con’t

- Approach #4: rally the community to sever bullet-proof hosting service’s connectivity



washingtonpost.com > Technology > Security Fix

Security Fix

Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

RECENT POSTS

- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

Entries By Category

- Cyber Justice
- Economy Watch
- Fraud
- From the Bunker
- Latest Warnings
- Misc.
- New Patches
- Piracy
- Safety Tips

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)

Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

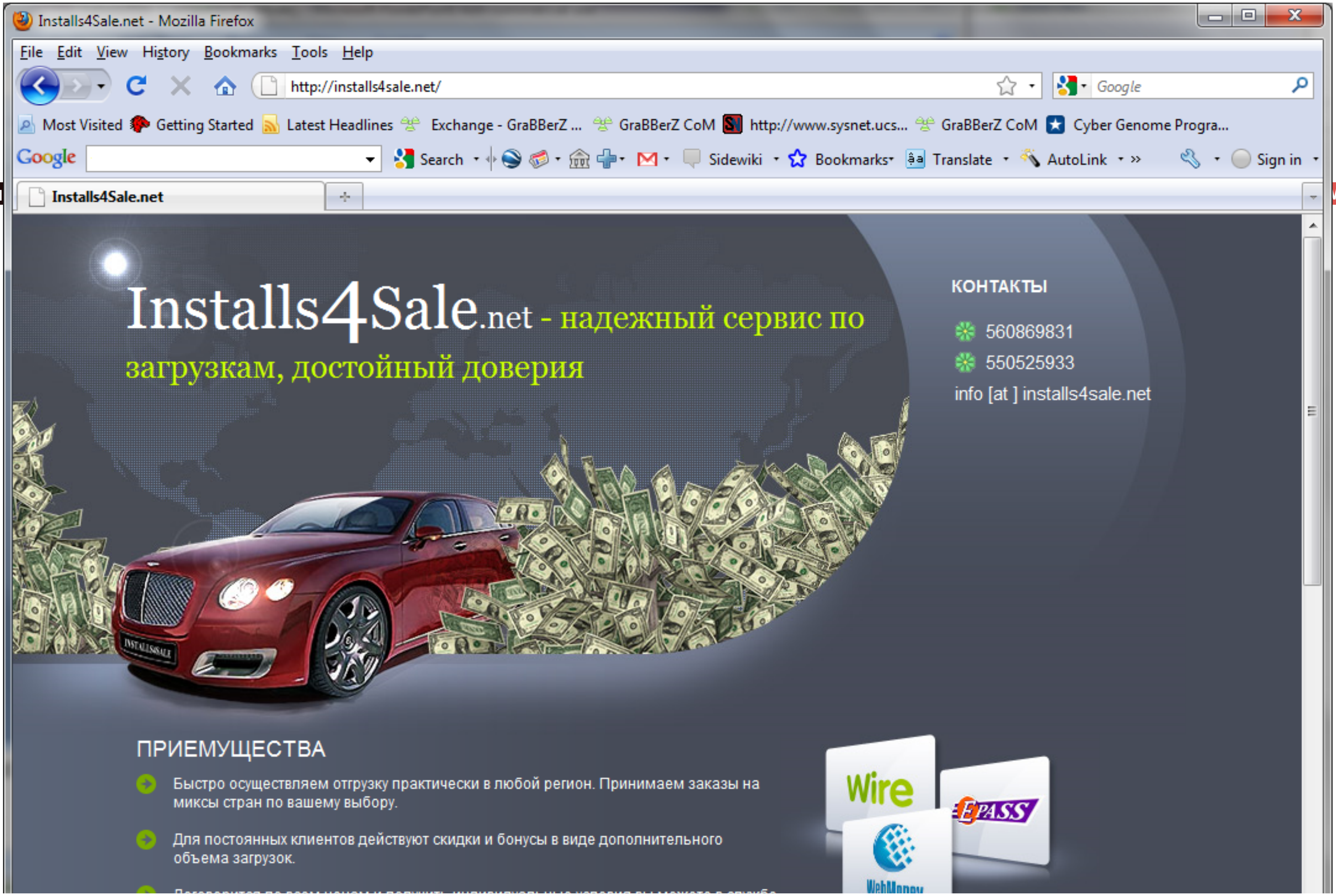
> In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

Fighting Bots / Botnets, con’t

- Approach #4: rally the community to sever bullet-proof hosting service’s connectivity
- Botmaster countermeasure?
- Who needs to run a bot when you can buy just-in-time bots … !

The Malware
“Pay Per Install” (PPI) Ecosystem



Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

КОНТАКТЫ

560869831

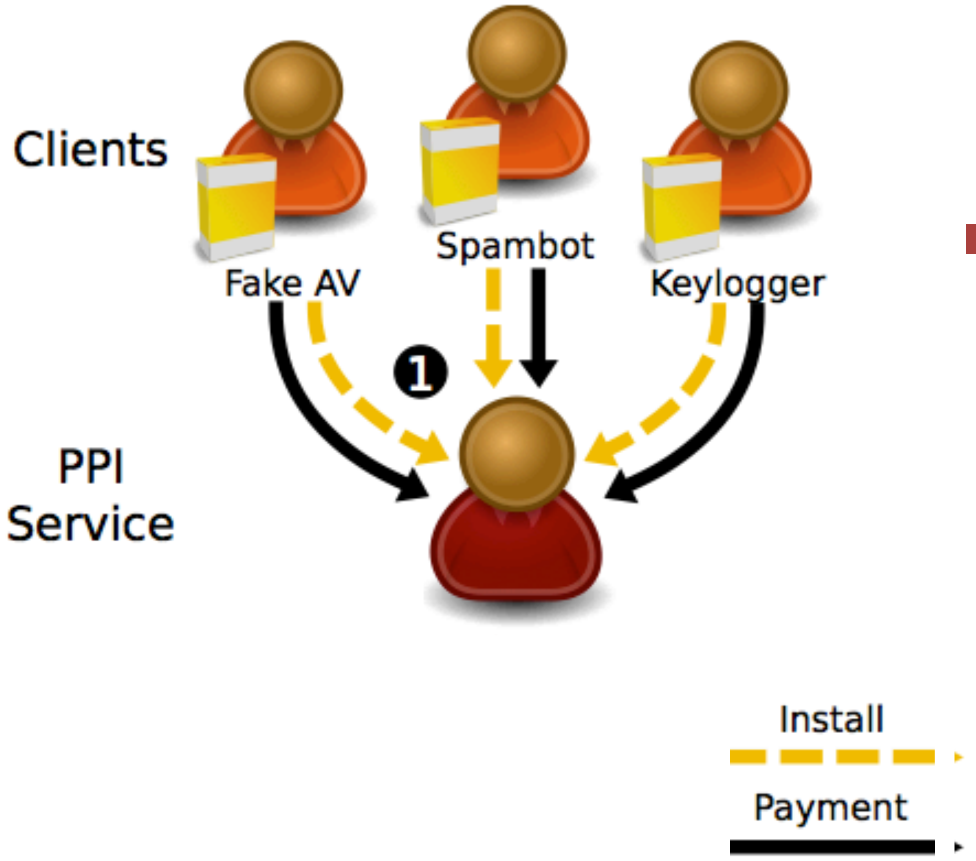
550525933

info [at] installs4sale.net

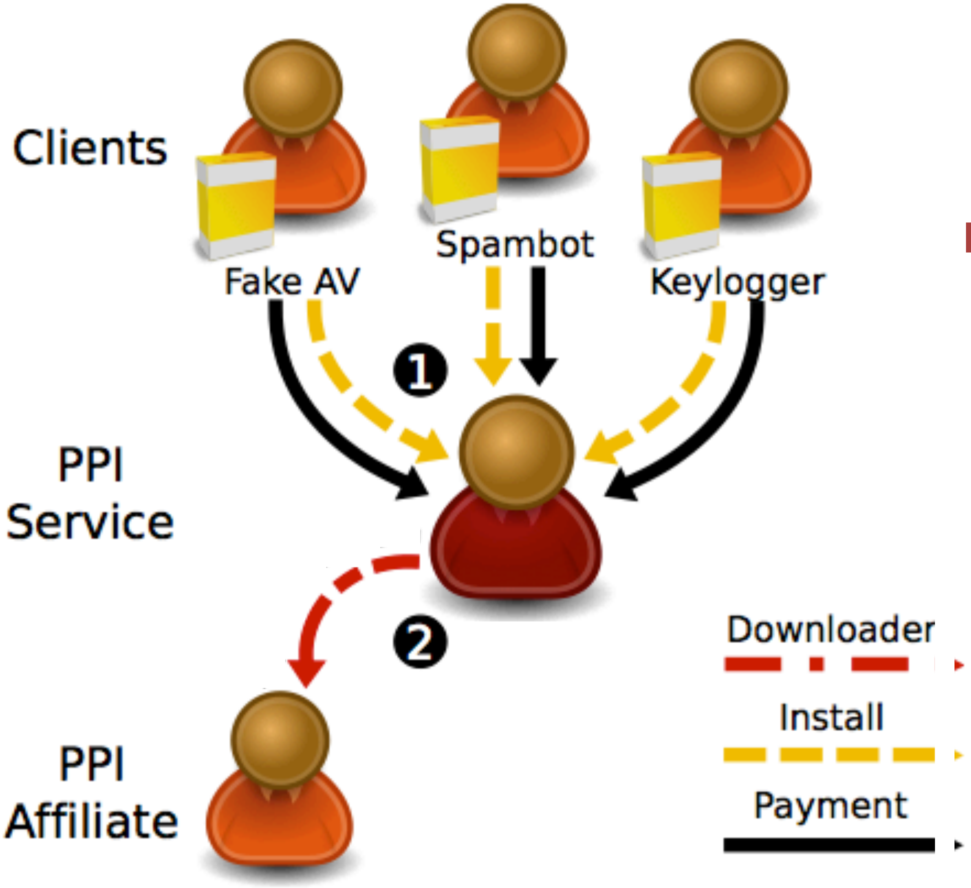
ПРИЕМУЩЕСТВА

- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договорится по всем ценам и получить индивидуальные условия вы можете в службе

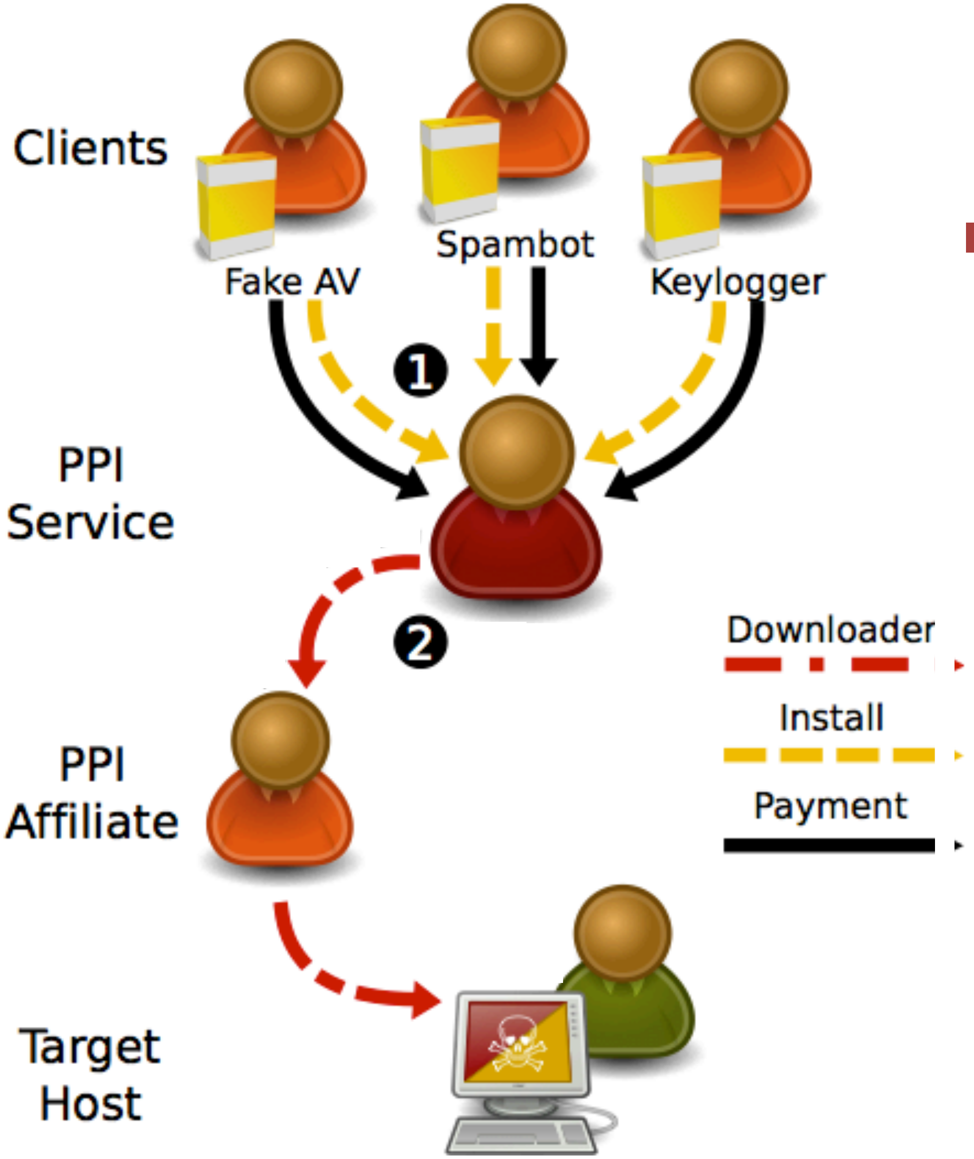
The PPI Eco-system



The PPI Eco-system



The PPI Eco-system



Clients

Fake AV

Spambot

Keylogger

1

PPI Service

2

PPI Affiliate

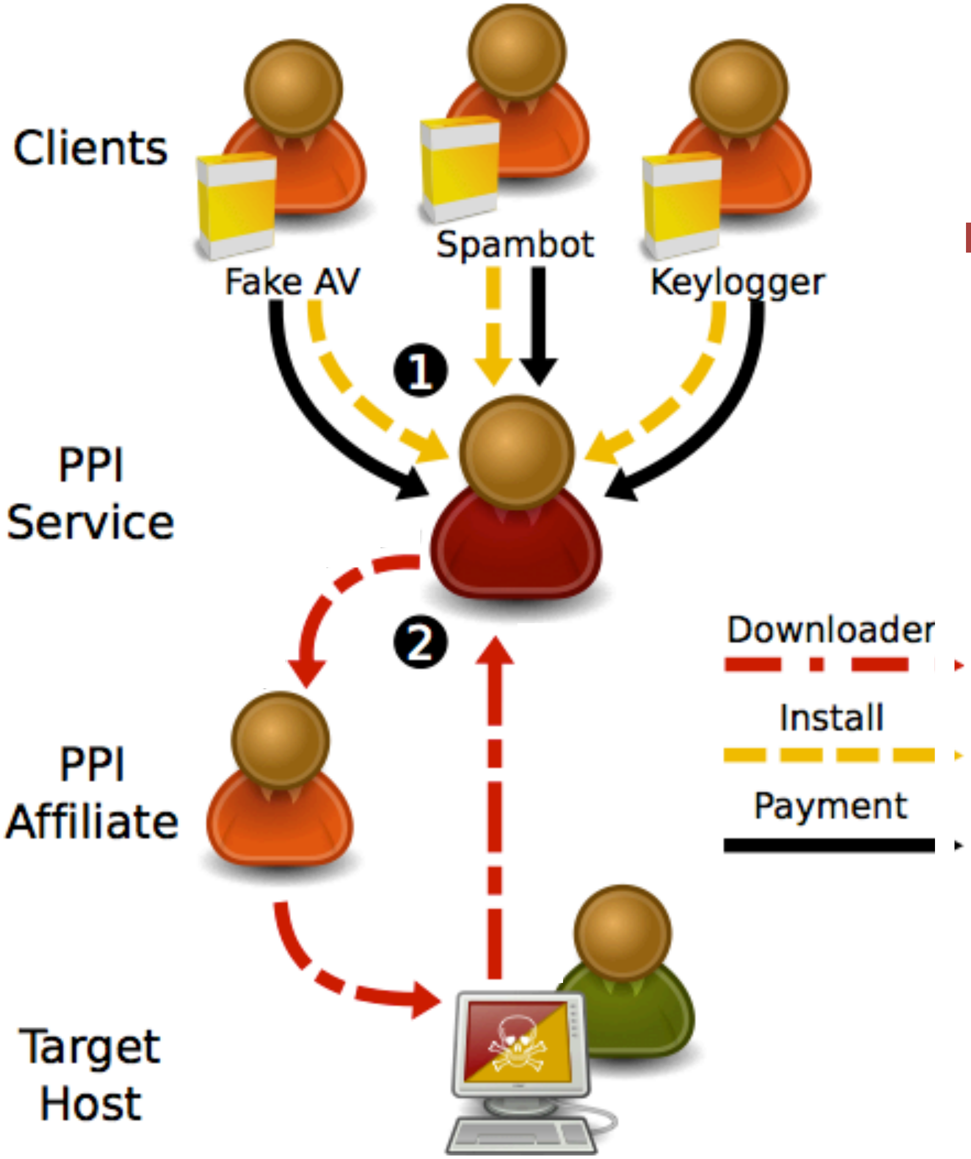
Target Host

Downloader

Install

Payment

The PPI Eco-system



Clients

Fake AV

Spambot

Keylogger

1

PPI Service

2

PPI Affiliate

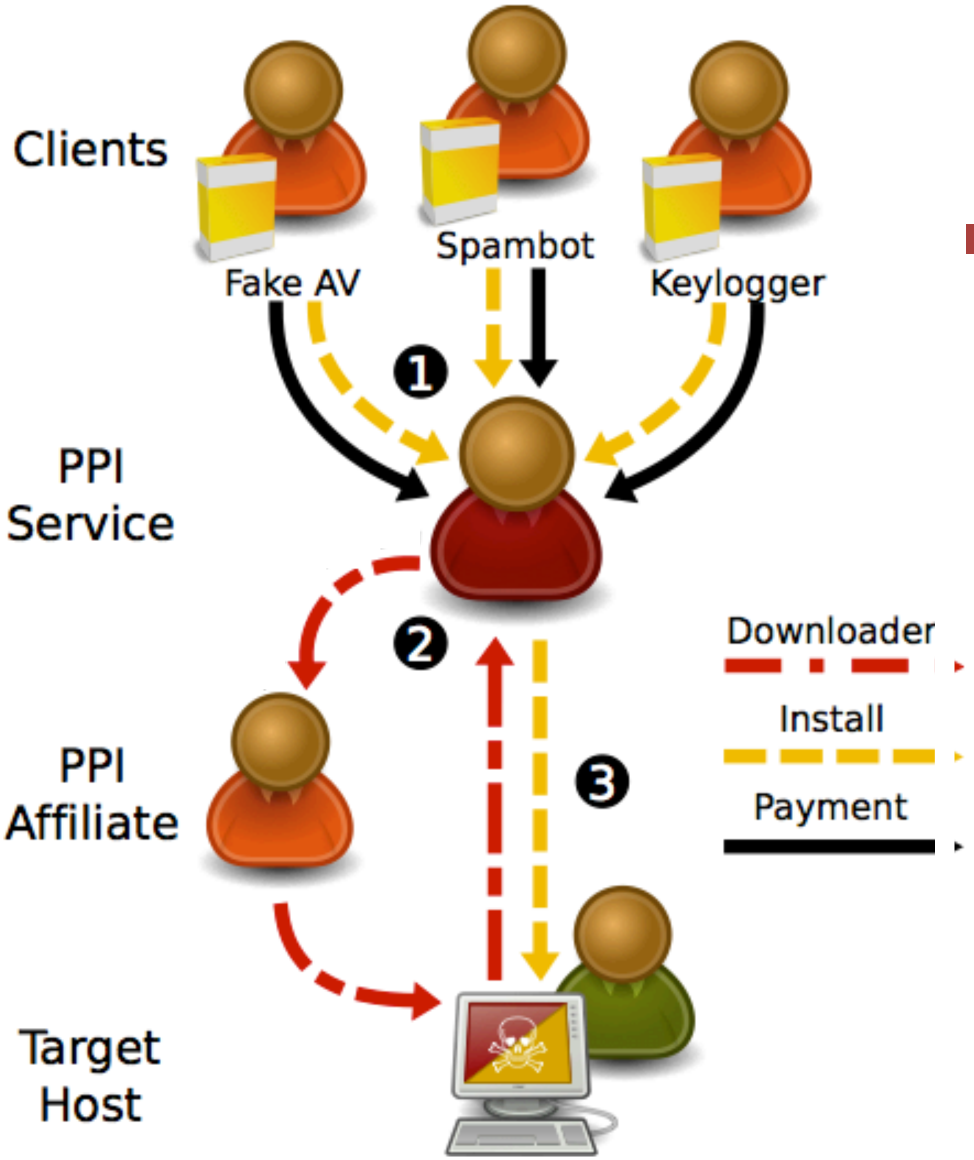
Target Host

Downloader

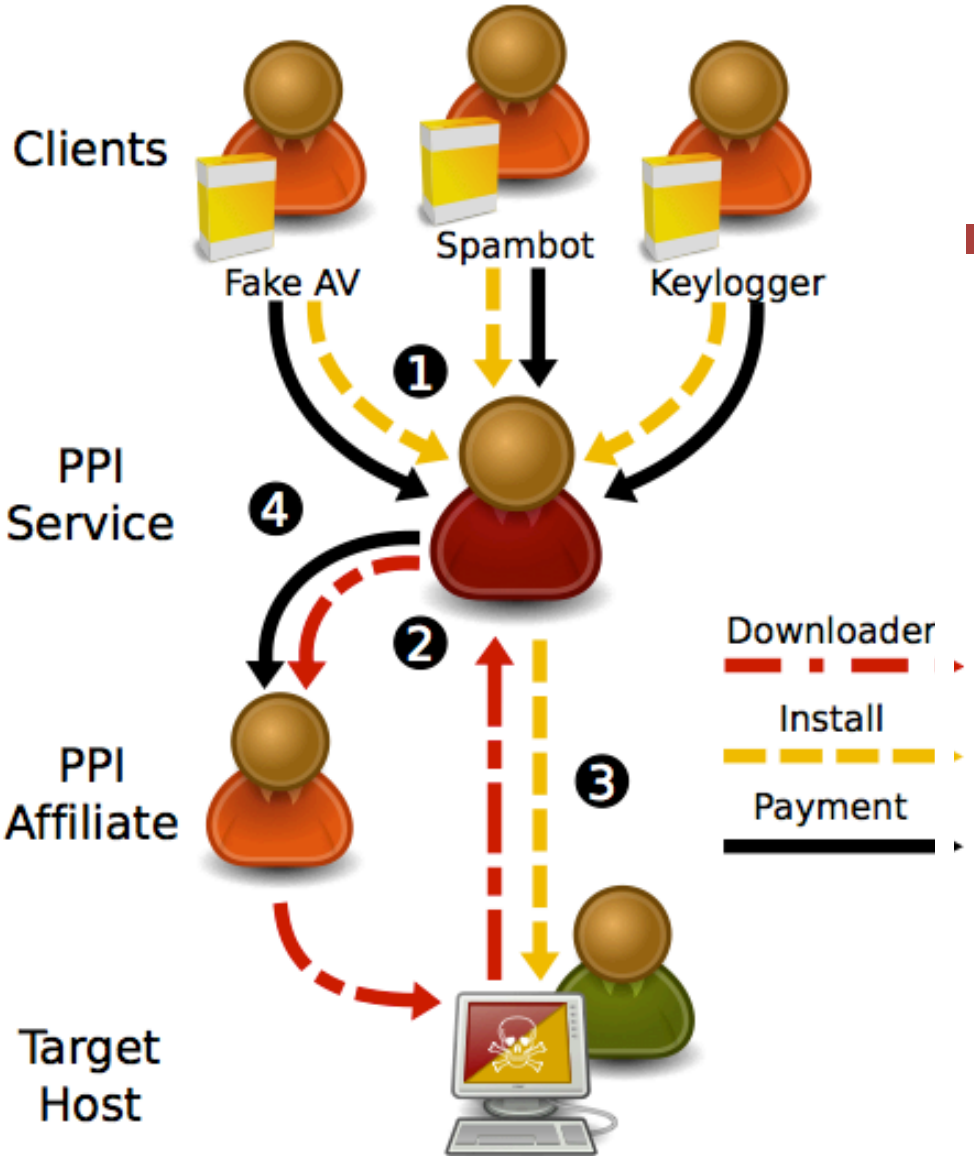
Install

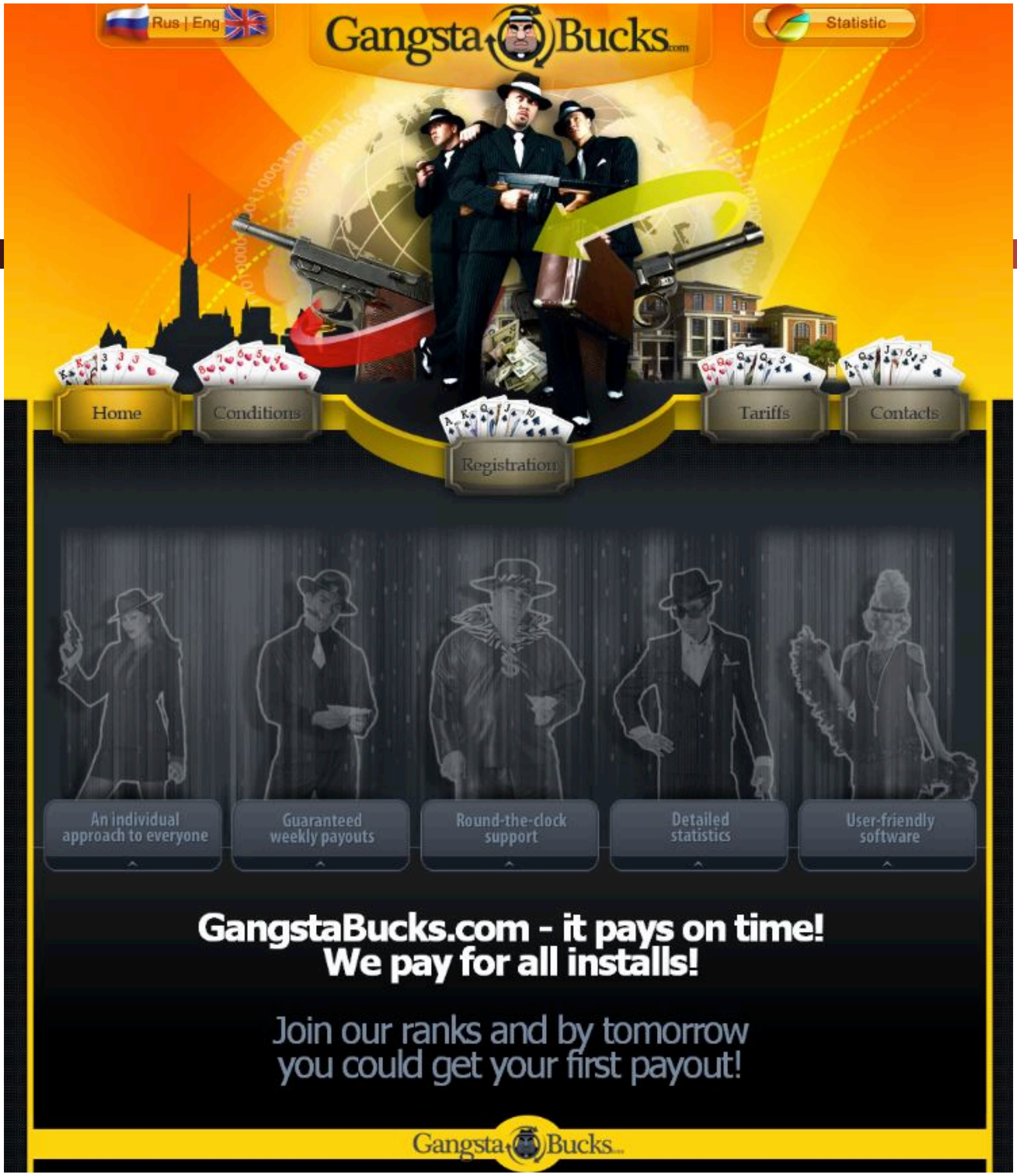
Payment

The PPI Eco-system



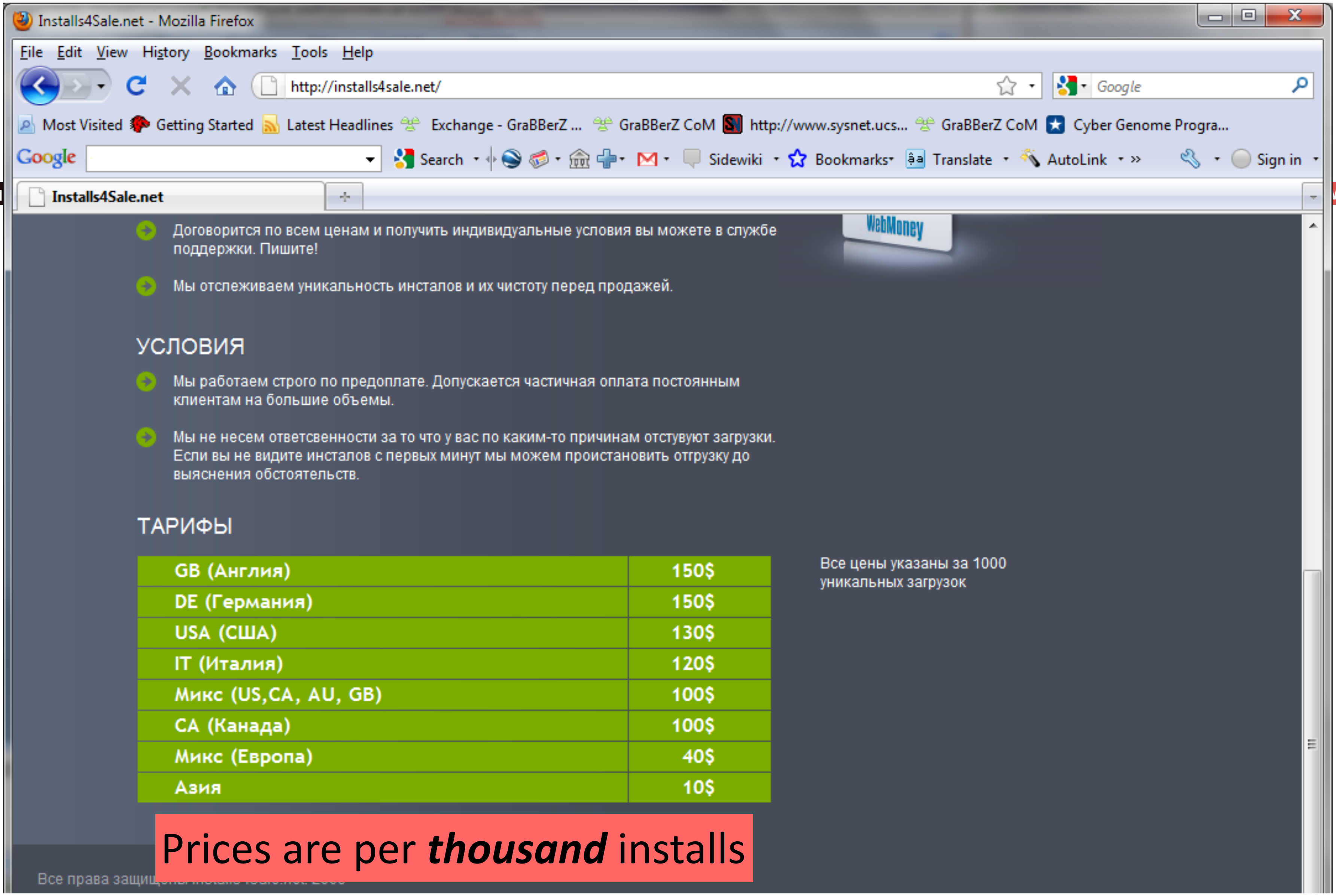
The PPI Eco-system





GangstaBucks.com - it pays on time!
We pay for all installs!

Join our ranks and by tomorrow
you could get your first payout!



- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
- Мы отслеживаем уникальность инсталов и их чистоту перед продажей.

УСЛОВИЯ

- Мы работаем строго по предоплате. Допускается частичная оплата постоянным клиентам на большие объемы.
- Мы не несем ответсвенности за то что у вас по каким-то причинам отстувуют загрузки. Если вы не видите инсталов с первых минут мы можем приостановить отгрузку до выяснения обстоятельств.

ТАРИФЫ

GB (Англия)	150$
DE (Германия)	150$
USA (США)	130$
IT (Италия)	120$
Микс (US,CA, AU, GB)	100$
CA (Канада)	100$
Микс (Европа)	40$
Азия	10$

Все цены указаны за 1000 уникальных загрузок

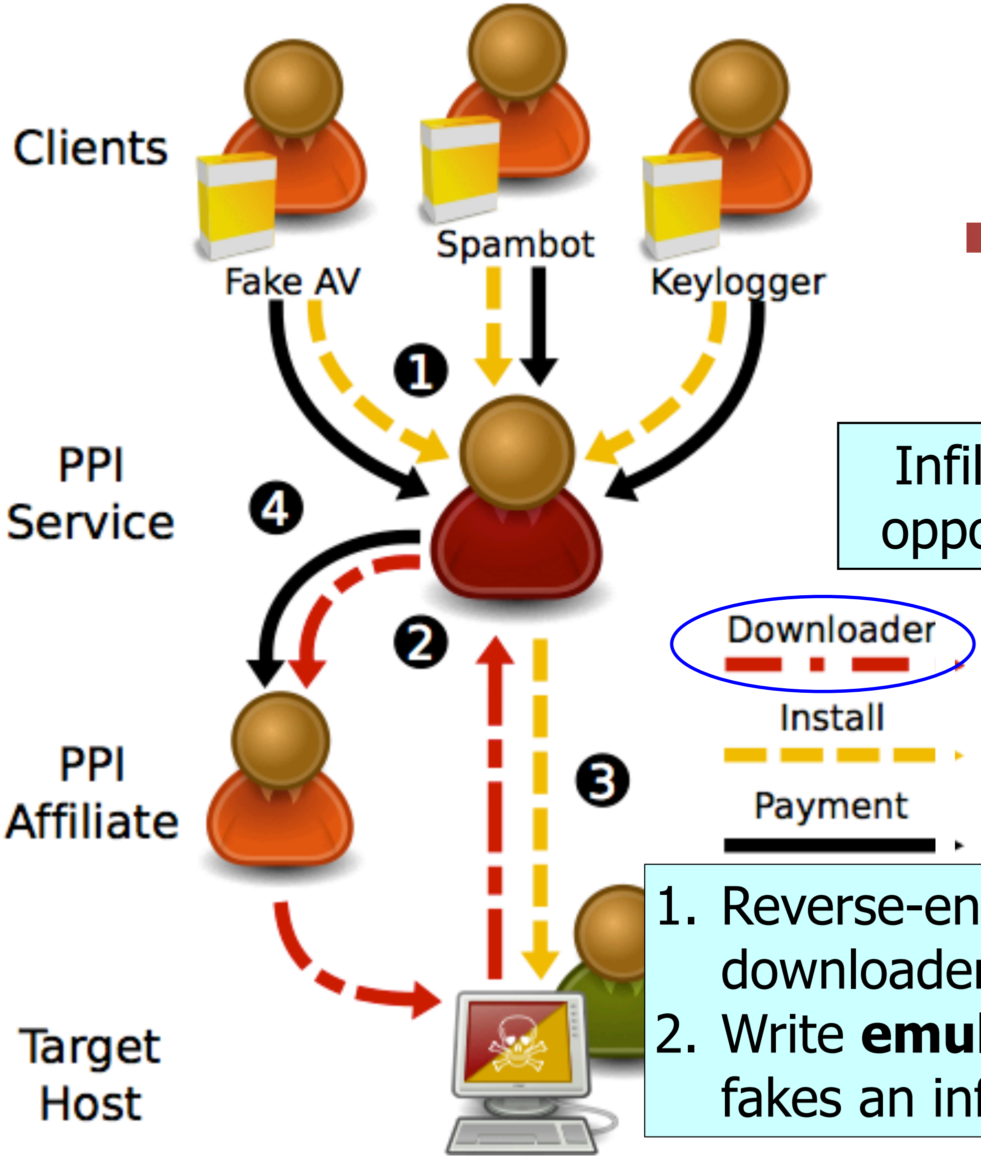
Все права защищ

Prices are per ***thousand*** installs

Fighting Bots / Botnets, con't

- Approach #4: rally the community to sever bullet-proof hosting service's connectivity
- Botmaster countermeasure?
- Who needs to run a bot when you can buy just-in-time bots ... !
- Approach #5: use the complexity of the malware infrastructure to undermine it ...

The PPI Eco-system

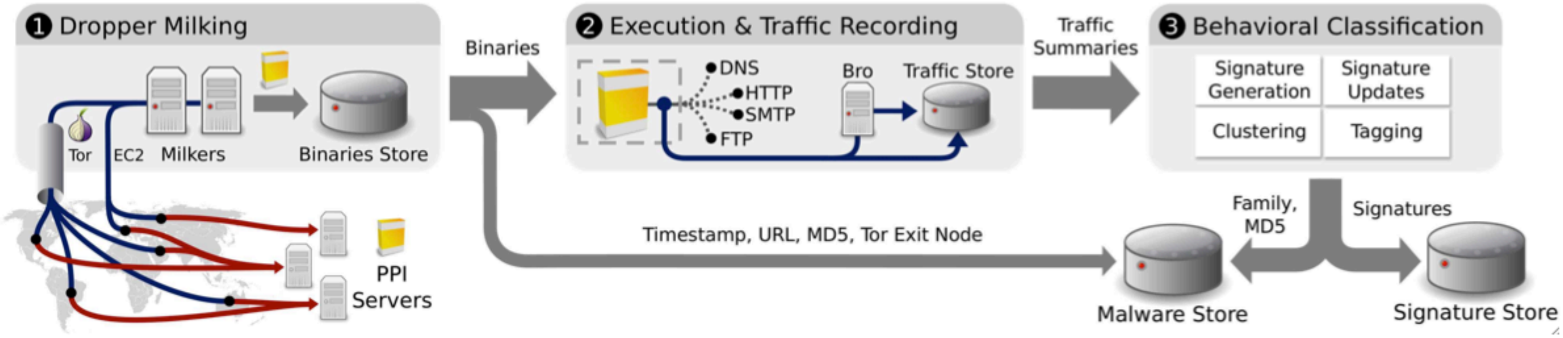


Infiltration opportunity

1. Reverse-engineer downloader protocol
2. Write **emulator** that fakes an infection

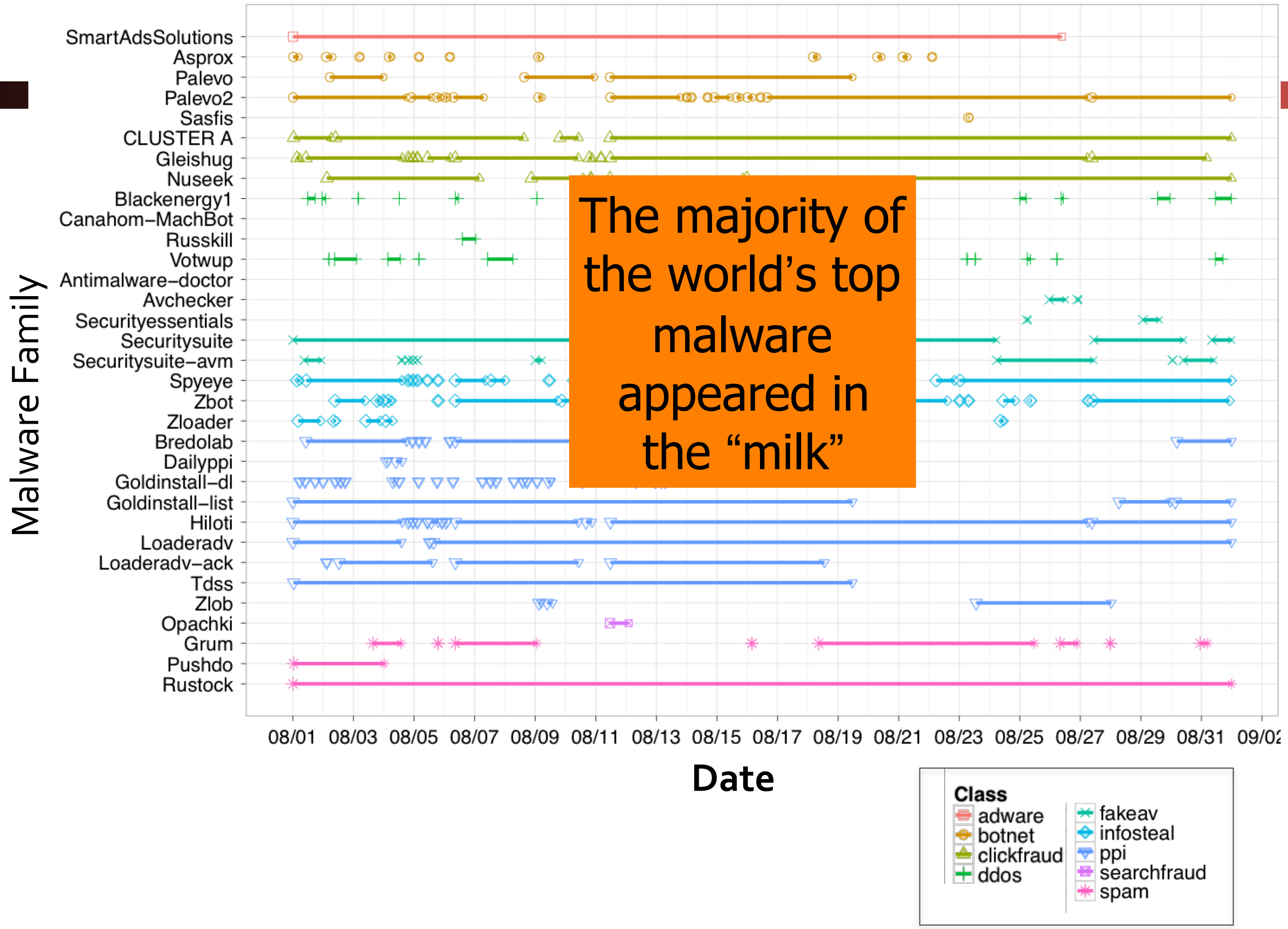
Intelligence via Infiltration...

"Milking" = mimic downloader, repeatedly ask PPI service for next program to install



Running for five months, Berkeley & UCSD researchers downloaded ("milked") > 1M binaries (9K distinct) from 4 different affiliate programs

Malware Extracted via “Milking”



The majority of the world’s top malware appeared in the “milk”

Addressing The Botnet Problem

- What are our prospects for securing the Internet from the threat of botnets? What angles can we pursue?
- Angle #1: detection/cleanup
  - Detecting infection of individual bots hard as it’s the defend-against-general-malware problem
  - Detecting bot doing C&C likely a losing battle as attackers improve their sneakiness & crypto
  - Cleanup today lacks oomph:
    - Who’s responsible? … and do they care? (externalities)
    - Landscape could greatly change with different model of liability
- Angle #2: go after the C&C systems / botmasters
  - Difficult due to ease of Internet anonymity & complexities of international law
    - But: a number of successes in this regard
    - Including some via peer pressure rather than law enforcement (McColo)
  - One potential angle: policing domain name registrations

Addressing The Problem, con’t

- Angle #3: prevention
  - Bots require installing new executables or modifying existing ones
  - Perhaps via infection …
    - … or perhaps just via user being fooled / imprudent
- Better models?
- We could lock down systems so OS prohibits user from changing configuration
  - Sacrifices flexibility
  - How does this work for home users?
  - Can we leverage trusted kernels + white lists / code signing?
- Or: structure OS/browser so code runs with Least Privilege
  - Does this solve the problem?
  - Depends on how granular the privileges are … and how the decision is made regarding just what privileges are “least”
    - E.g., iTunes App Store model (vetting), Android model (user confirmation)

Or Forget Fighting Botnets...

- Fight the ***business models!***
  - If bad guys can't make money, they stop doing it
- Managed to do this reasonably well for Viagra spam...
- But can we do this for other areas?

Worm Take-Aways

- Potentially enormous reach/damage
  - Weapon
- Hard to get right
- Emergent behavior / surprising dynamics
- Remanence: worms stick around
  - E.g. Slammer still seen in 2013!
- Propagation faster than human response