Malware: Worms and Botnets

CS 161: Computer Security

Prof. Vern Paxson

TAs: Paul Bramsen, Apoorva Dornadula,
David Fifield, Mia Gil Epner, David Hahn, Warren He,
Grant Ho, Frank Li, Nathan Malkin, Mitar Milutinovic,
Rishabh Poddar, Rebecca Portnoff, Nate Wang

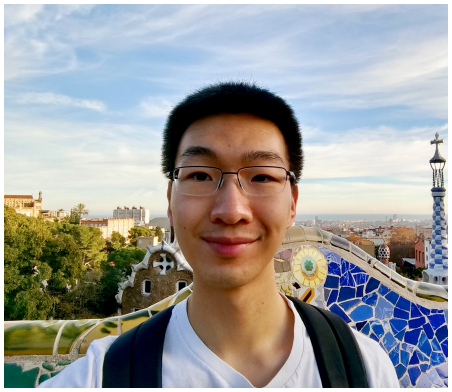
https://inst.eecs.berkeley.edu/~cs161/

April 25, 2017

CS 161 End Game

- Thursday's lecture (EECS faculty retreat):
  - Side channels, Bitcoin blockchain, user authentication, trusted hardware
    - Plus some associated research activities (not in scope)
  - Presented by Frank/Rebecca/Grant/Rishabh:






- RRR:
  - no section, see Piazza for office hours
  - Final review: regular class slots Tu/Th (+ webcast), conducted by TAs

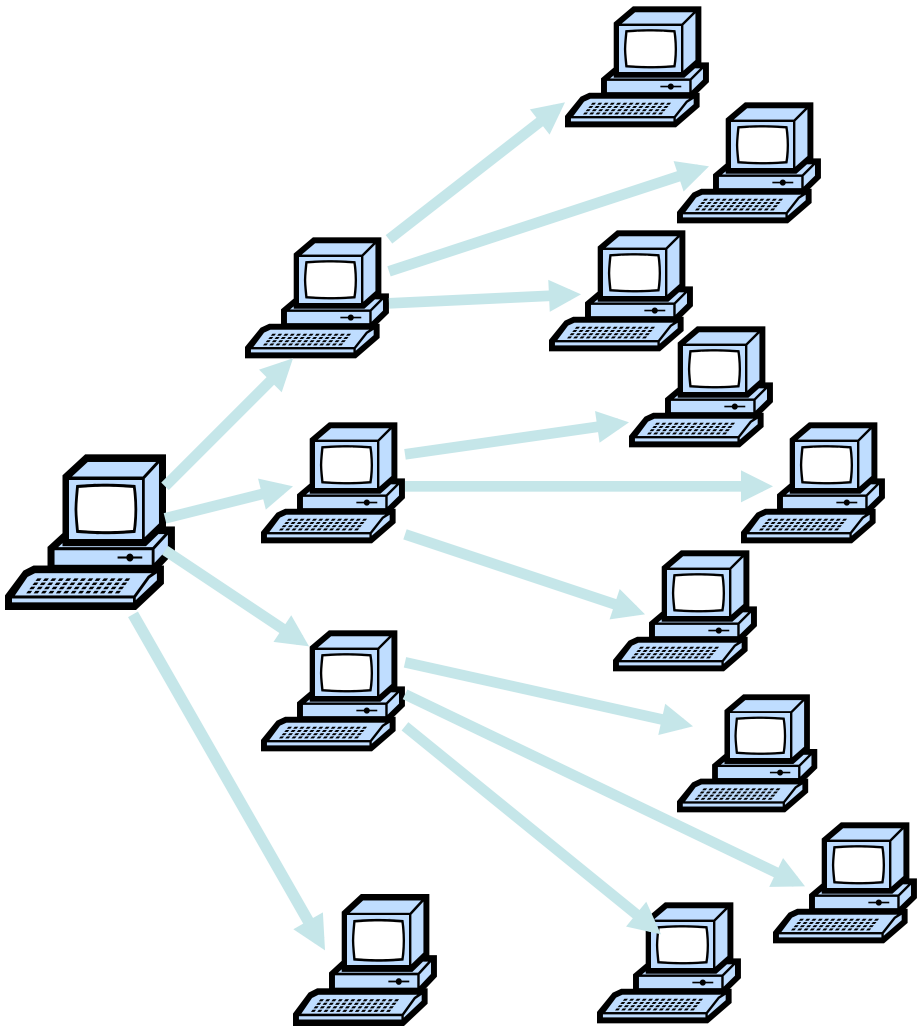
Worms

- 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

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

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

Yes, "Squiggler.com" was taken.

Squig that self-propagates upon viewing

```
<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)

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 $\Rightarrow \beta = 5$
    - For scanning worms, larger (= denser) vulnerable pop. $\Rightarrow$ higher $\beta \Rightarrow$ faster worm!

$$N = S(t) + I(t)$$
$$S(0) = I(0) = N/2$$

- 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:

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

Increase in # infectibles per unit time

Total attempted contacts per unit time

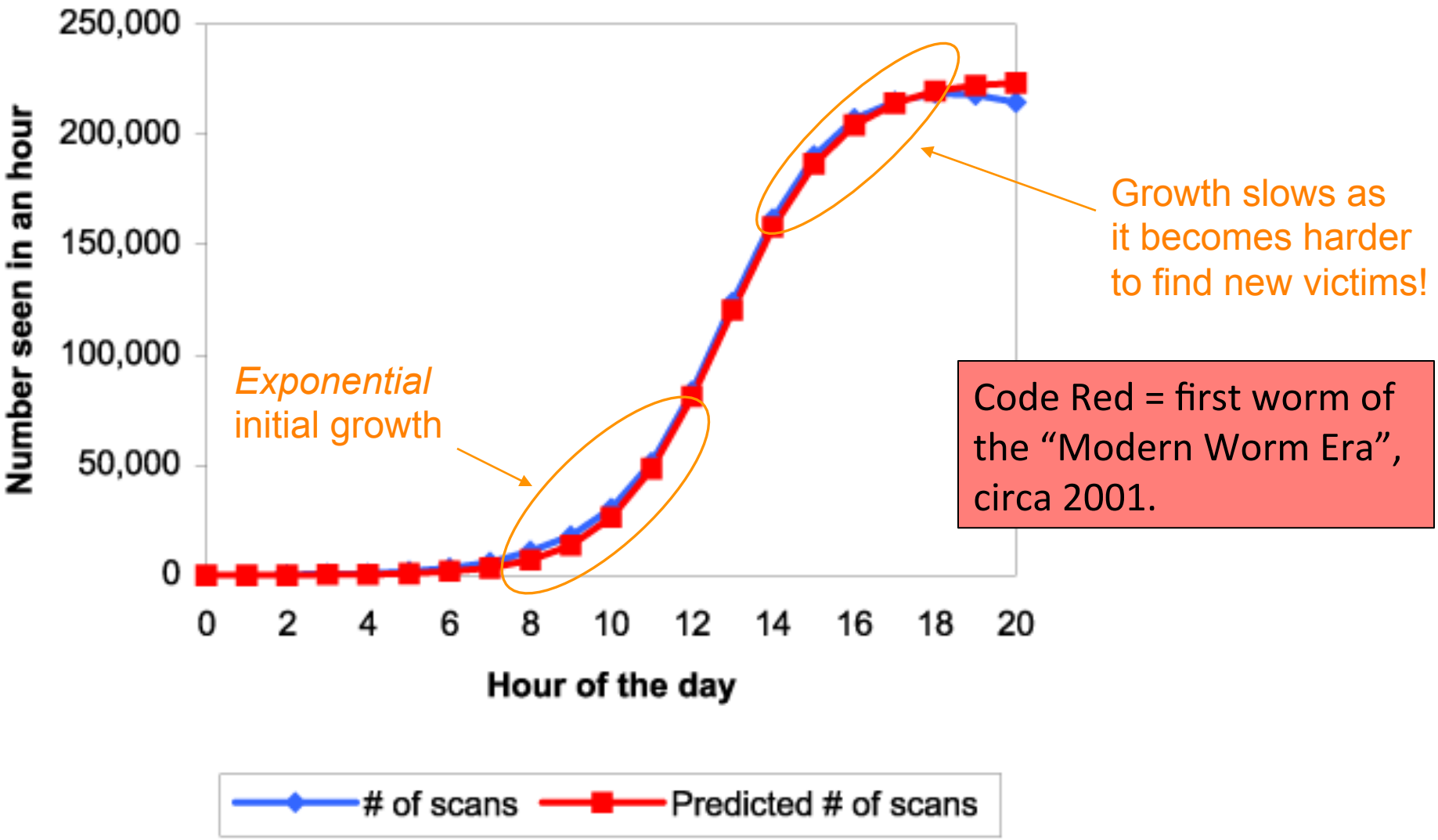
Proportion of contacts expected to succeed

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

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

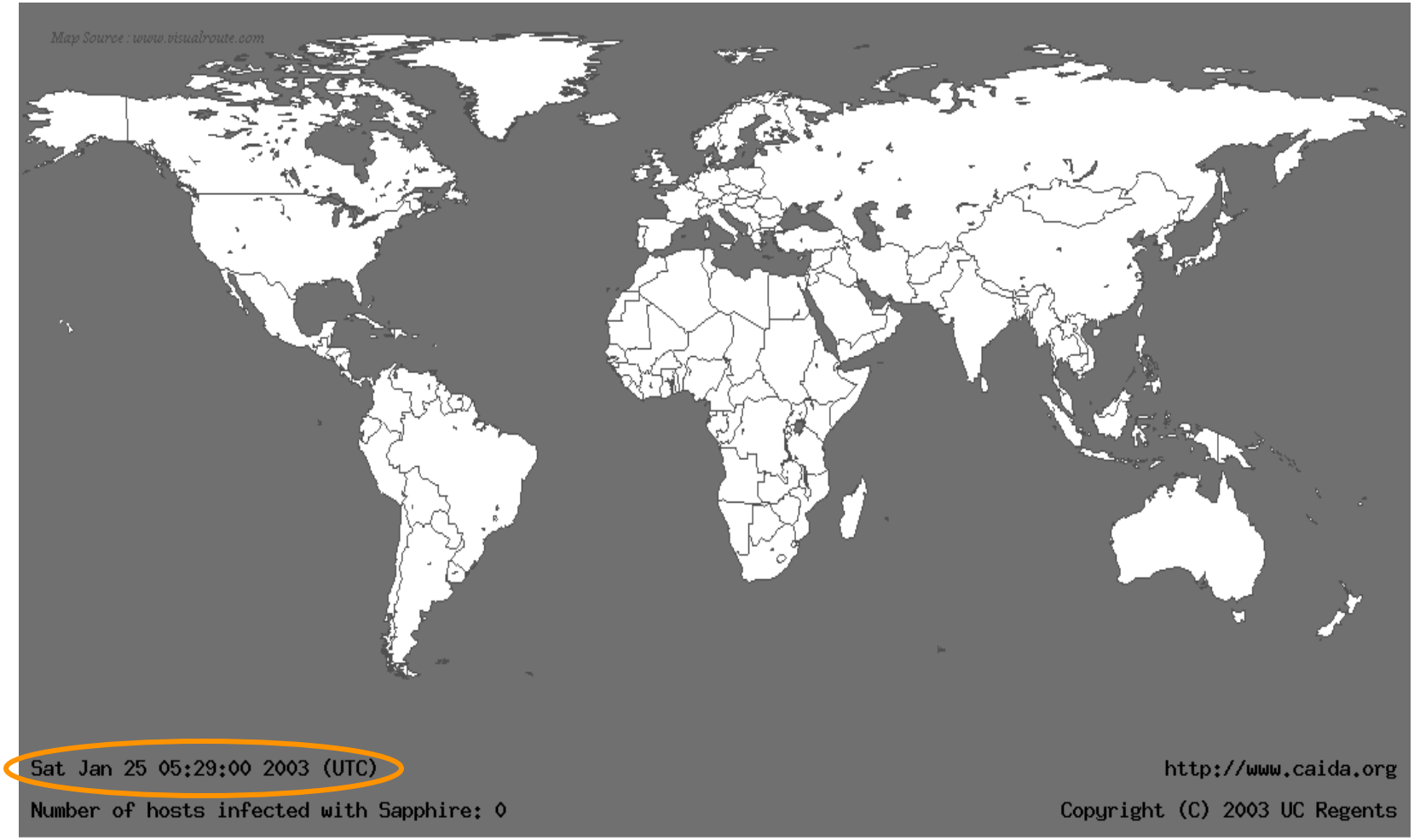
Fraction infected grows as a *logistic*

Fitting the Model to "Code Red"

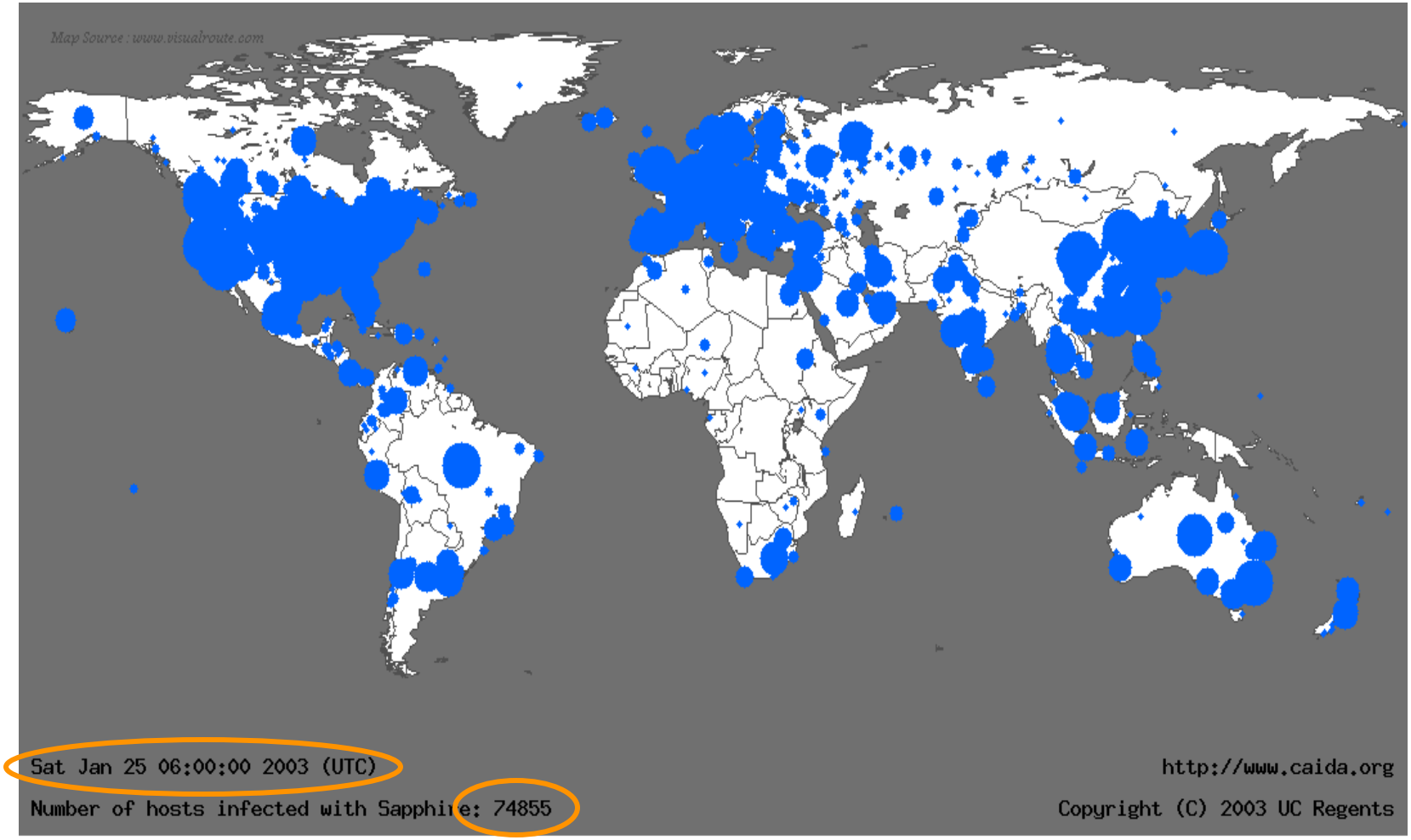


Code Red = first worm of the "Modern Worm Era", circa 2001.

Life Just Before Slammer



Life 10 Minutes After Slammer



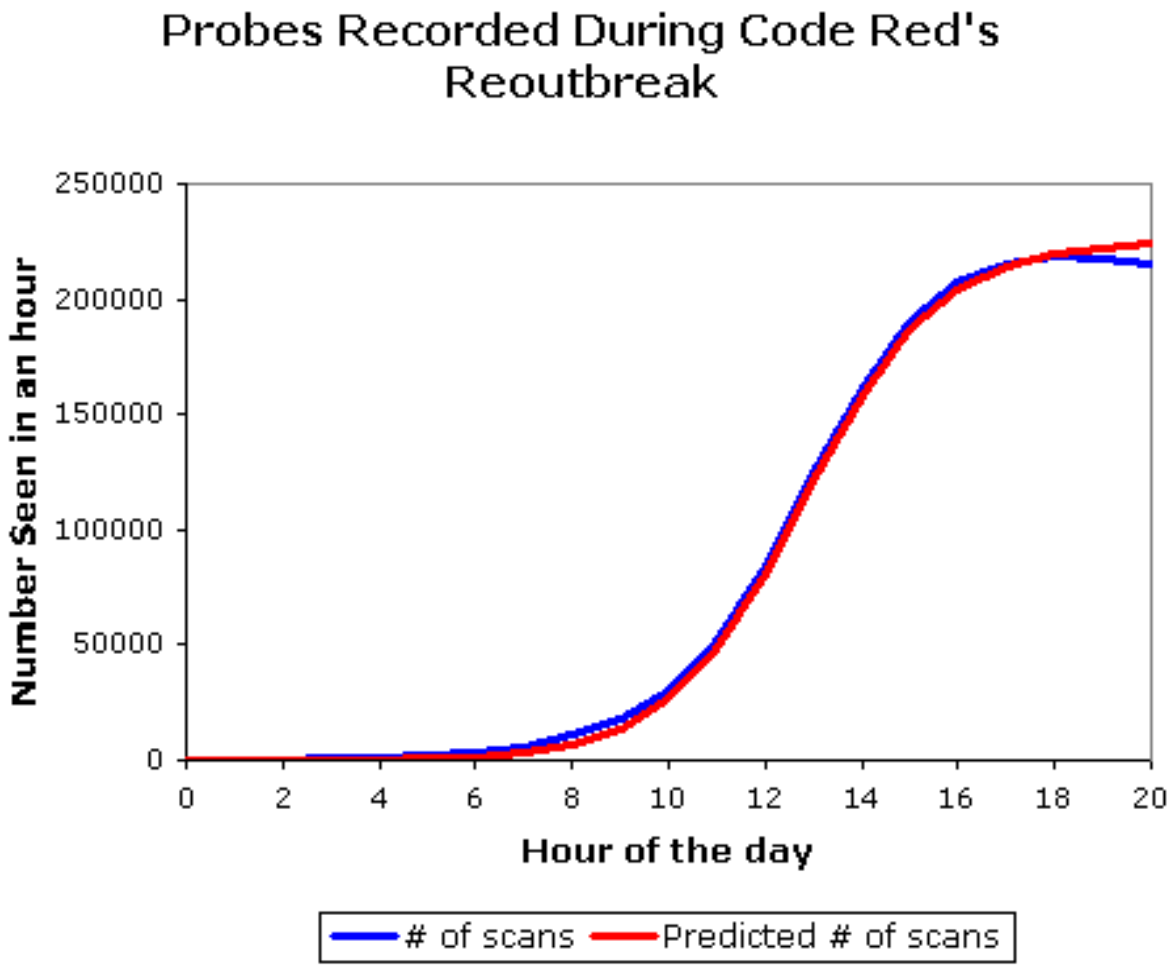
Going Fast: *Slammer*

- Slammer exploited connectionless UDP service, rather than connection-oriented TCP
- *Entire worm* fit in a single packet!

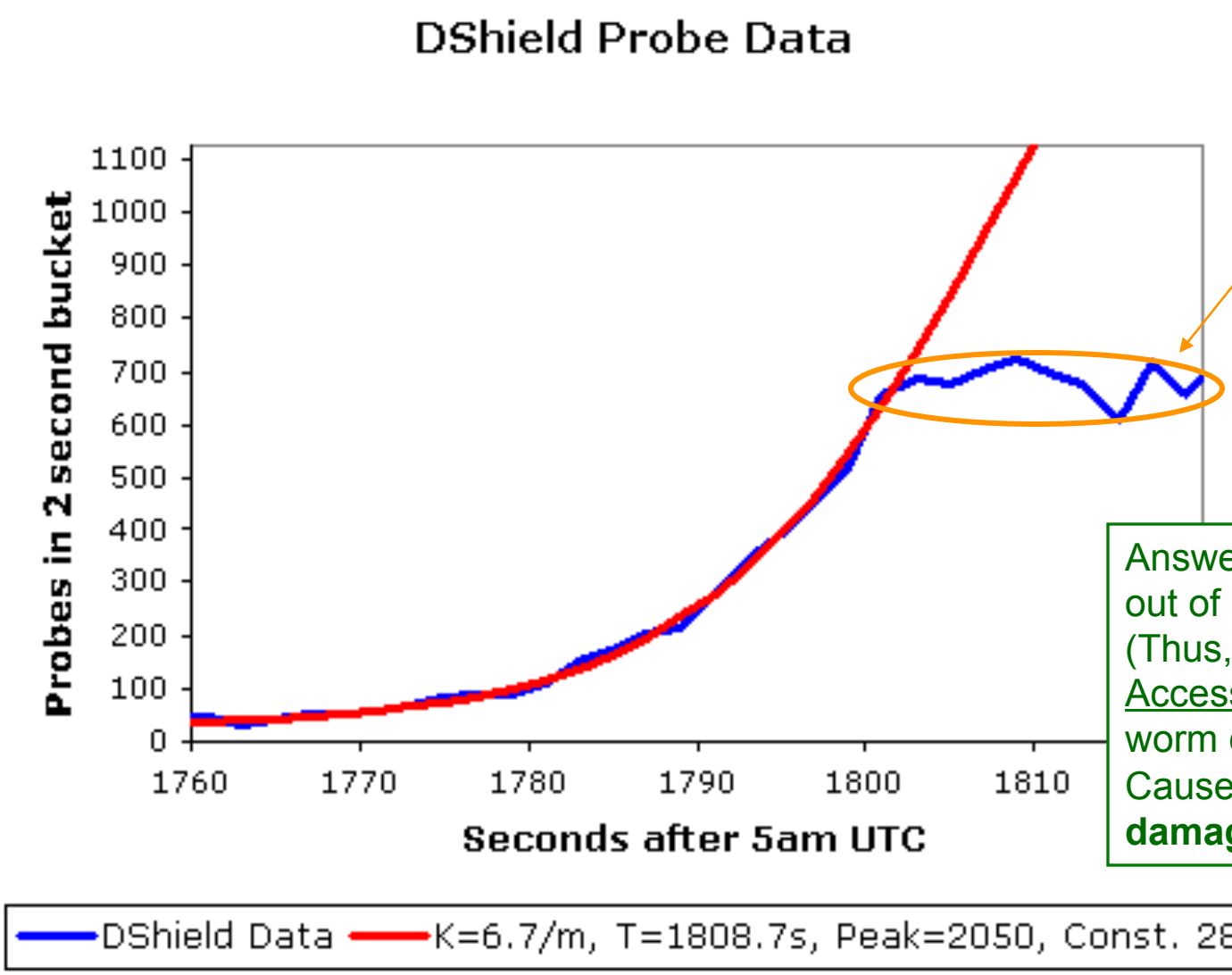
⇒ When scanning, worm could "fire and forget"
Stateless!

- Worm infected 75,000+ hosts in *<< 10 minutes*
- At its peak, **doubled every <u>8.5 seconds</u>**

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**.

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

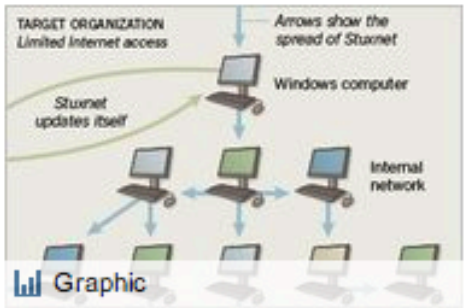
*This article is by **William J. Broad, John Markoff** and **David E. Sanger.***

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

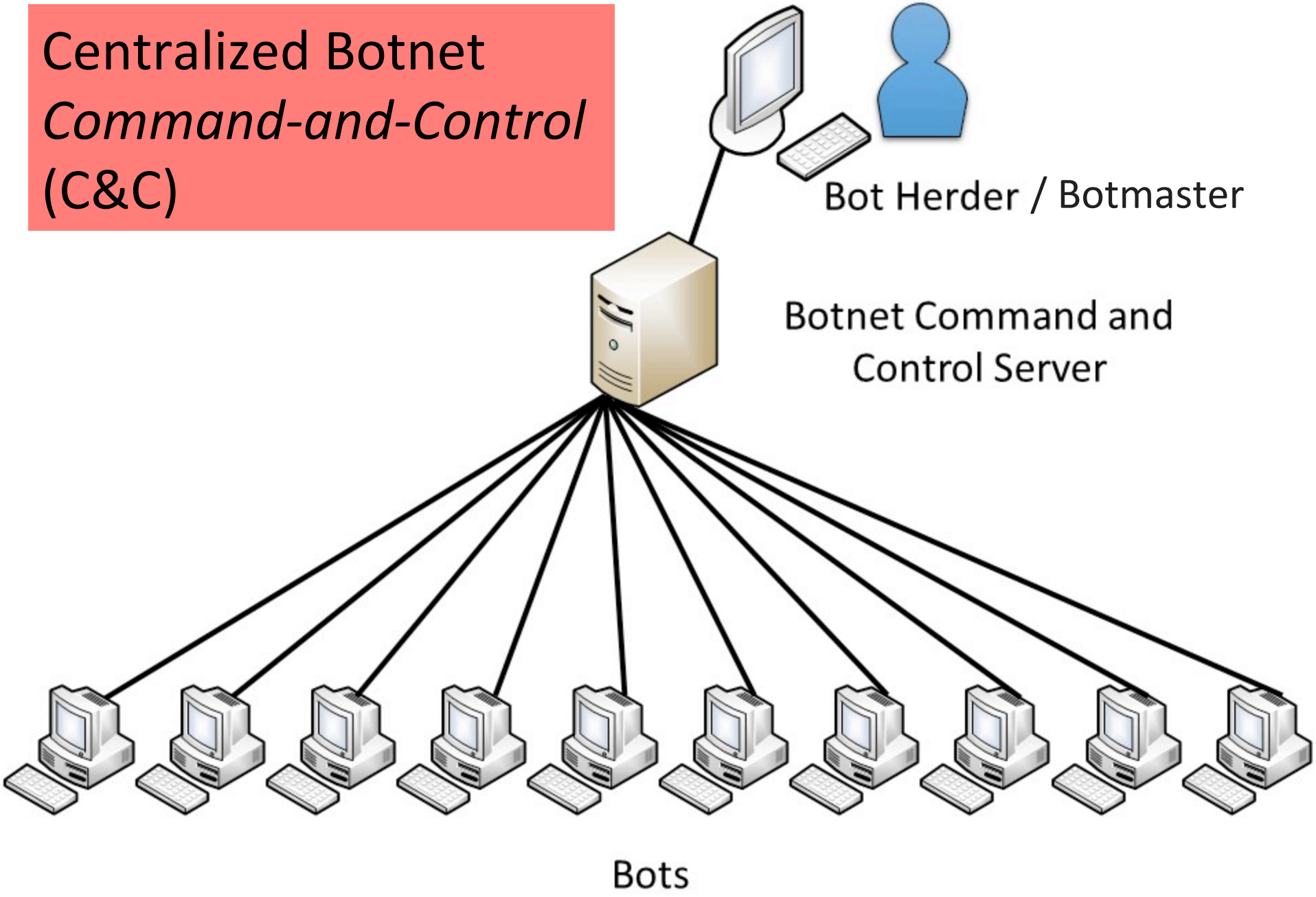
5 Minute Break

Questions Before We Proceed?

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")


WEB BulletProof
bulletproof hosting
BulletProof Web
"exceeding expectations"
Write us:
LIVE CHAT
CREATE TICKET
EN
RU
Client Area
FAQ
Offers
Terms
Partnership
About
News
Blog
BulletProof Servers
BulletProof VPS
BulletProof Domains
DDoS Protection
VPN
Promo code:
BEPROTECTED
10% OFF discount on Protection against DDoS attacks
Expires after 8 days
Bulletproof hosting
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!


WEB BulletProof
bulletproof hosting
BulletProof Web
"exceeding expectations"
Write us:
LIVE CHAT
CREATE TICKET
EN
RU
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
Blog
08.04.2016
https://bpw.sc/BulletProof-Servers/
Offers
35% discount on bulletproof servers and VPS
Use promo NICETOMEETYOU and get 35%...
News
15.04.2015
Hello world!

BulletProof Server in Ukraine

fm. $399 USD

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

fm. $90 USD

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.

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.

Certificate No: 060216

Jimmy Ernesta
Seychelles International Business Authority
REGISTRAR OF INTERNATIONAL BUSINESS COMPANIES

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.

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

Payment methods VISA MasterCard PayPal bitcoin WebMoney Skrill paxum SEPA wire transfer

FAQ Offers Terms About

Bulletproof domain registration

fm. 35 USD

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

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.

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 »

Customer Service

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

Security Fix

Brian Krebs on Computer Security

SEARCH THIS BLOG

Go

RECENT POSTS

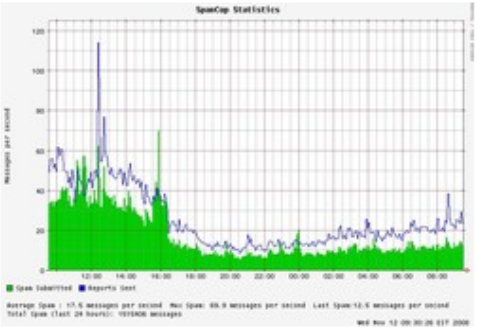
- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

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 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://installs4sale.net/

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr

Google Search Sidewiki Bookmarks Translate AutoLink

Installs4Sale.net

Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

КОНТАКТЫ

560869831

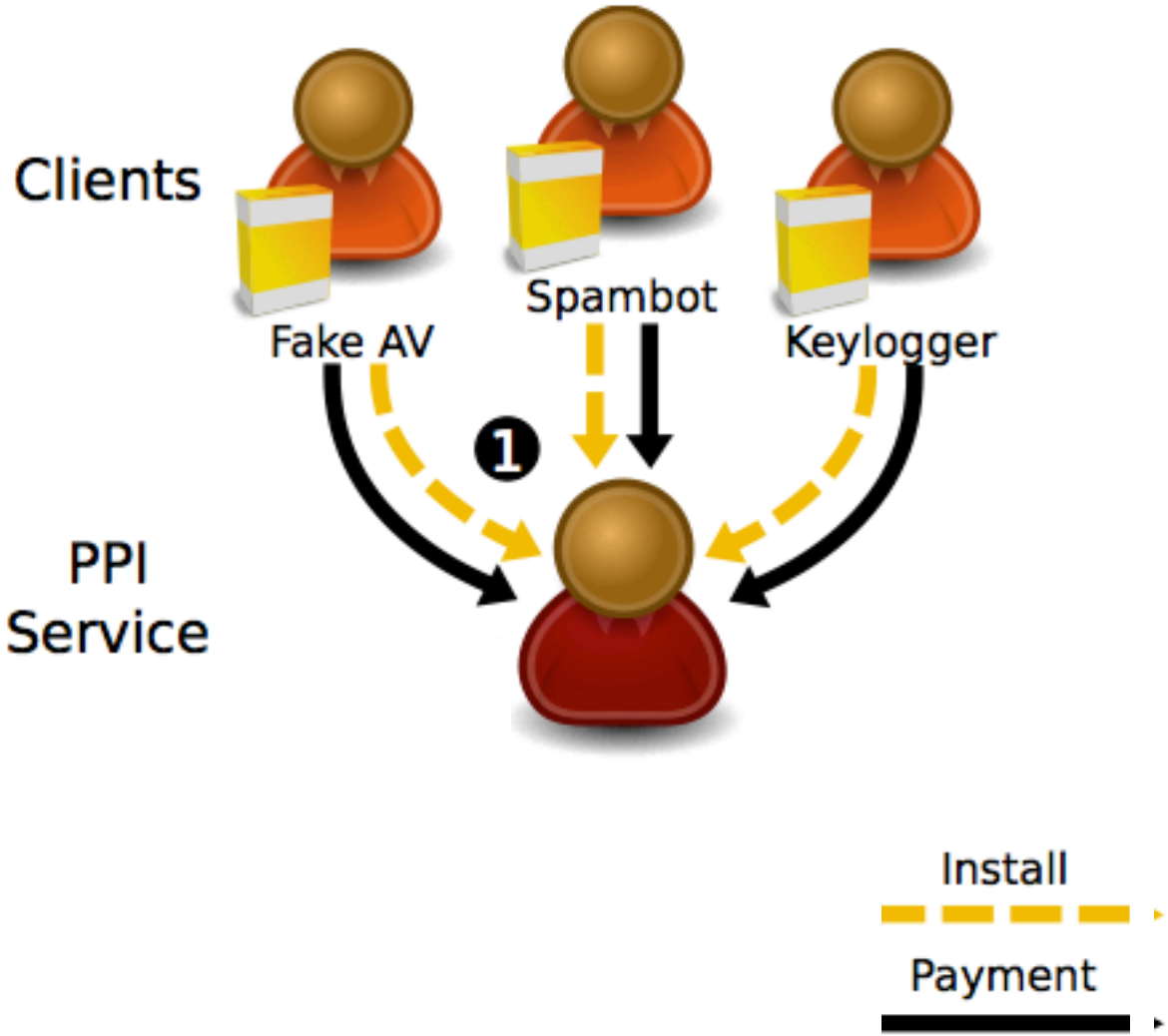
550525933

info [at] installs4sale.net

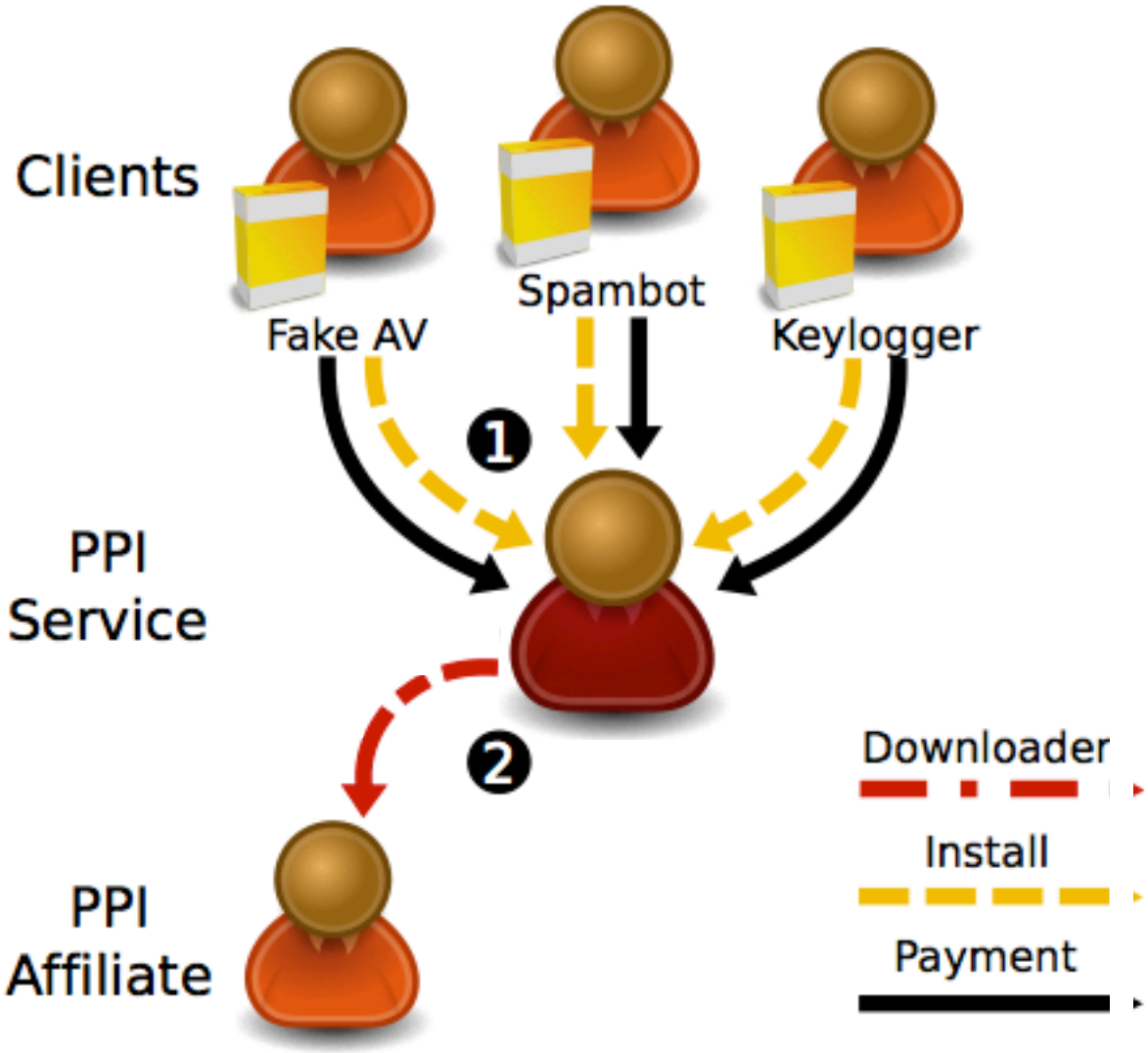
ПРИЕМУЩЕСТВА

- 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.

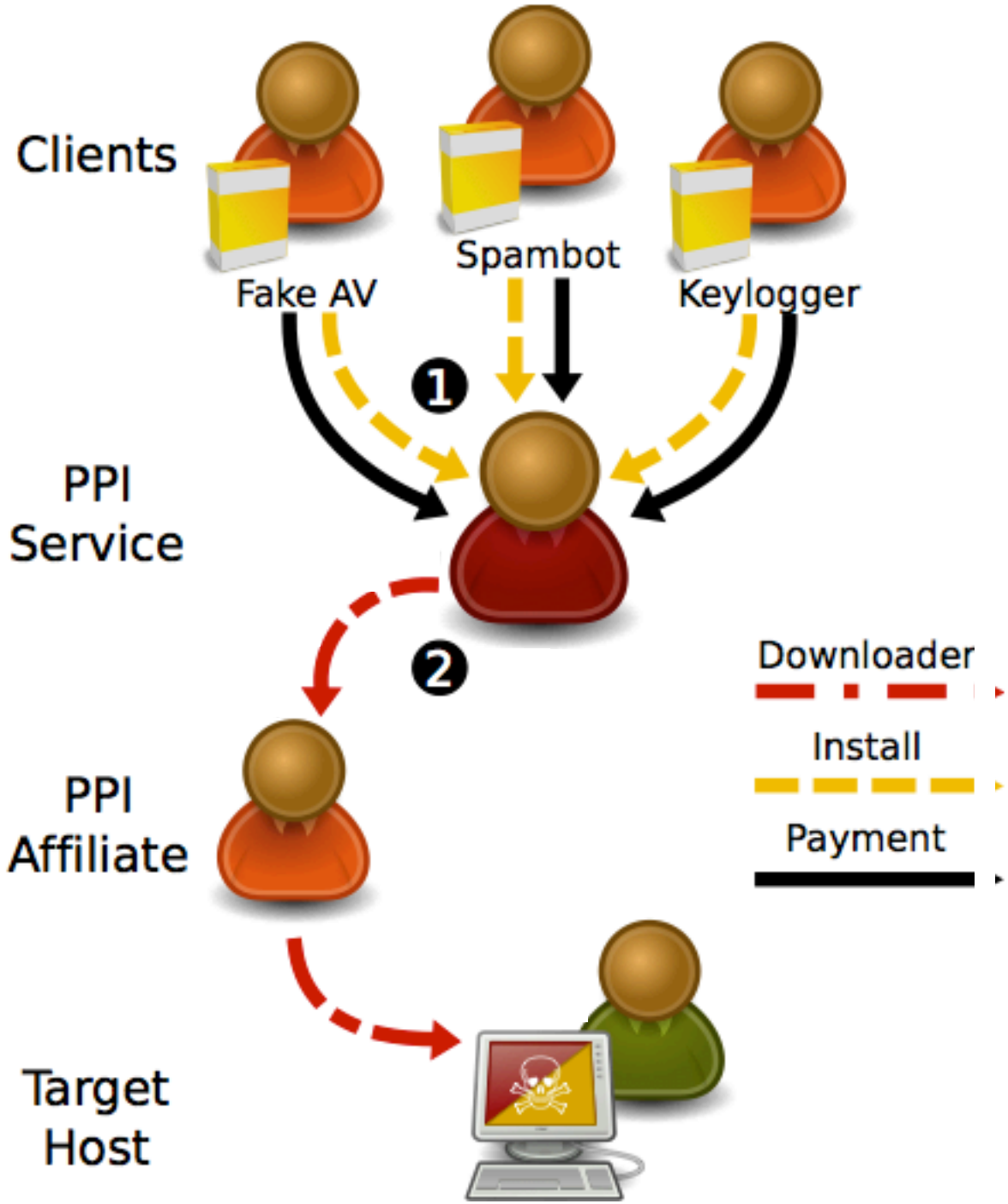
The PPI Eco-system



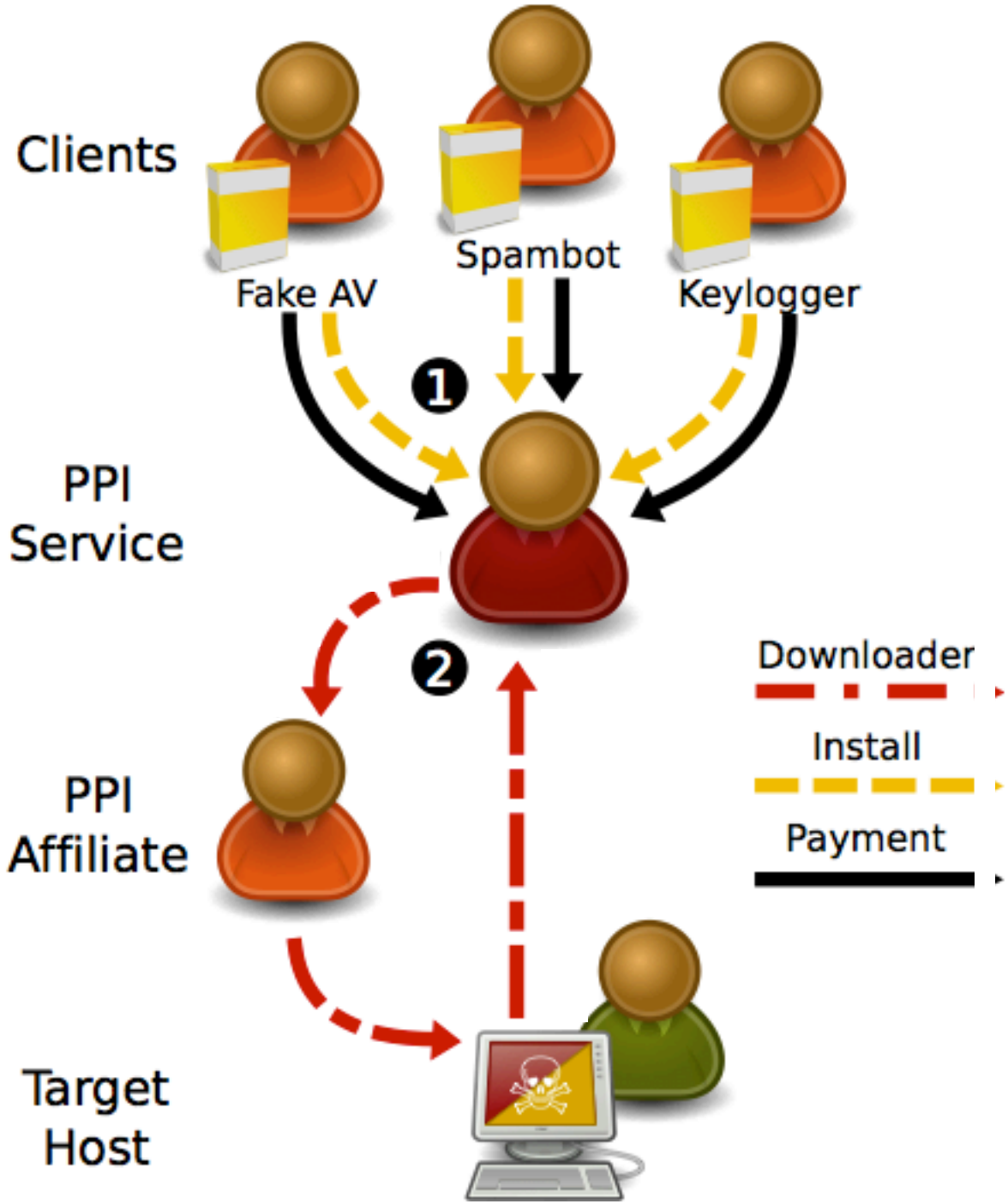
The PPI Eco-system



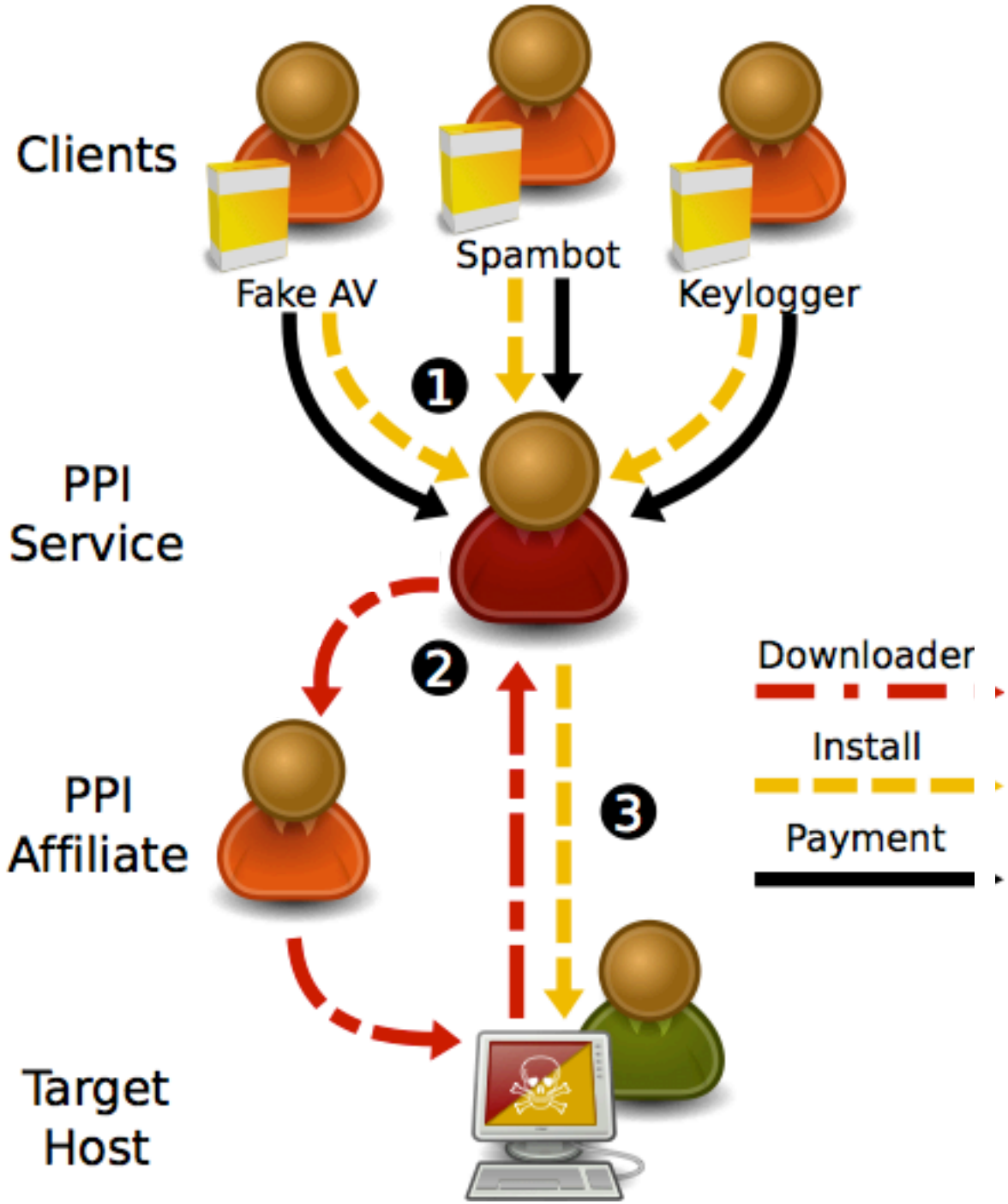
The PPI Eco-system



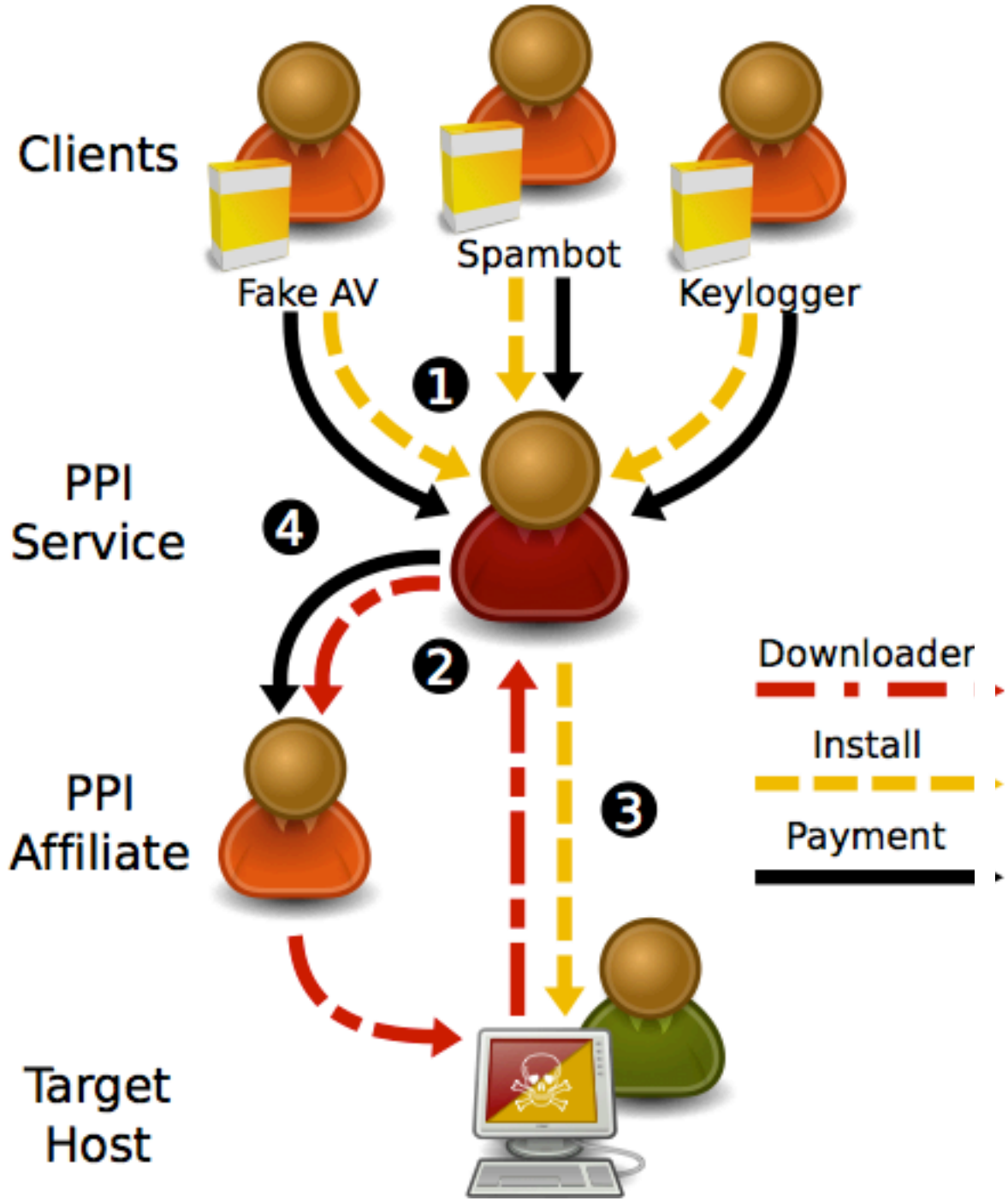
The PPI Eco-system



The PPI Eco-system



The PPI Eco-system




Rus | Eng
GangstaBucks.com
Statistic
Home
Conditions
Registration
Tariffs
Contacts
An individual approach to everyone
Guaranteed weekly payouts
Round-the-clock support
Detailed statistics
User-friendly software
GangstaBucks.com - it pays on time!
We pay for all installs!
Join our ranks and by tomorrow you could get your first payout!
GangstaBucks.com

Installs4Sale.net - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://installs4sale.net/

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr

Google Search Sidewiki Bookmarks Translate AutoLink

Installs4Sale.net

WebMoney

- 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 проистановить 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

Prices are per ***thousand*** installs

Все права защ