

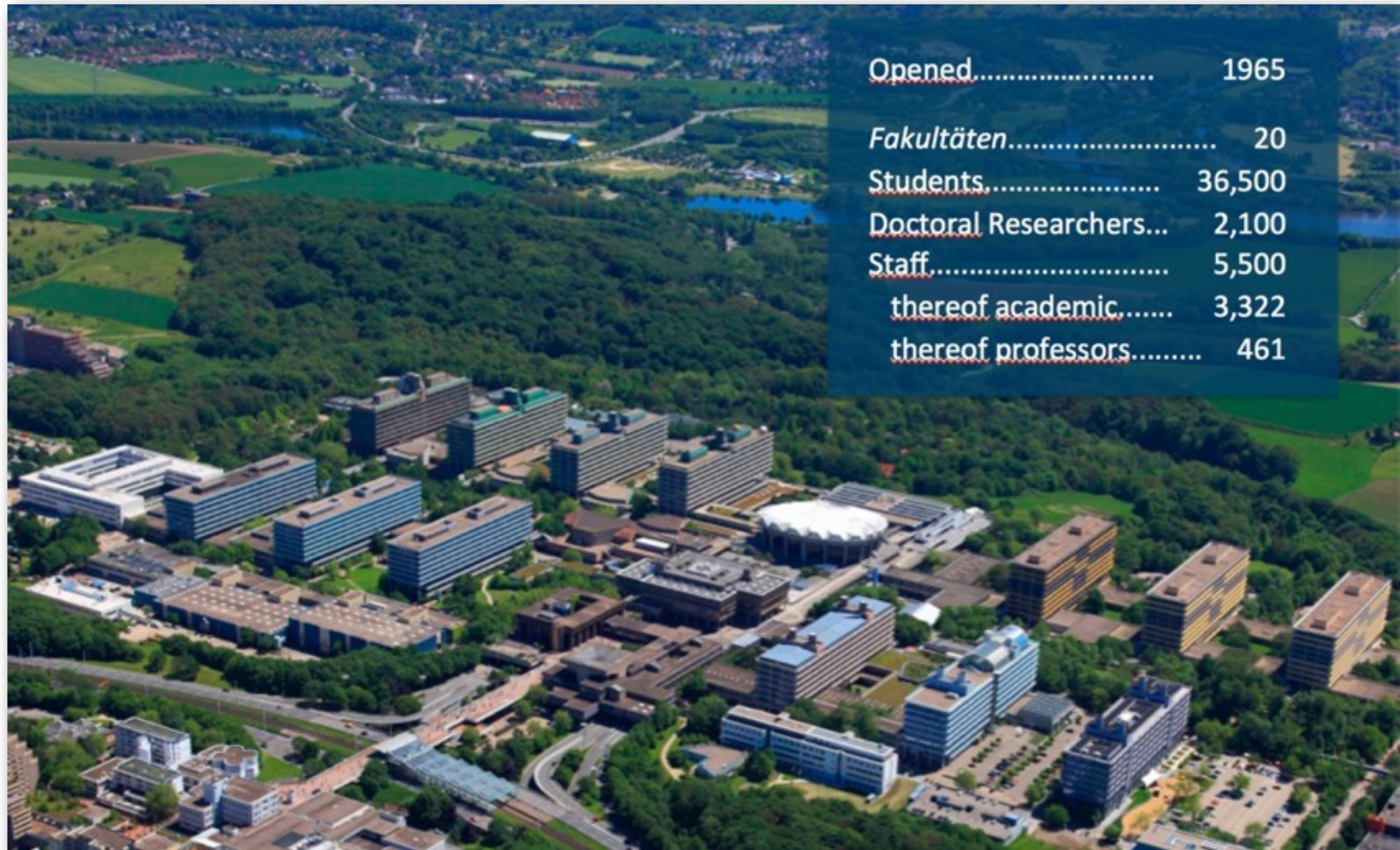
An Overview of Modern Security Threats

Thorsten Holz
Ruhr-University Bochum

November 30, 2012
University of Potsdam

RUB / HGI

Systems Security
Ruhr-University Bochum



Horst Görtz Institut für IT-Sicherheit (HGI)

Elektrotechnik und Informationstechnik

Prof. Tim Güneysu
Prof. Thorsten Holz
Prof. Dorothea Kolossa
Prof. Christof Paar
Prof. Jörg Schwenk

Mathematik

Prof. Holger Dette
Prof. Eike Kiltz
Prof. Alexander May
Prof. Hans Simon
Dr. Christopher Wolf

Wirtschaftswissenschaften

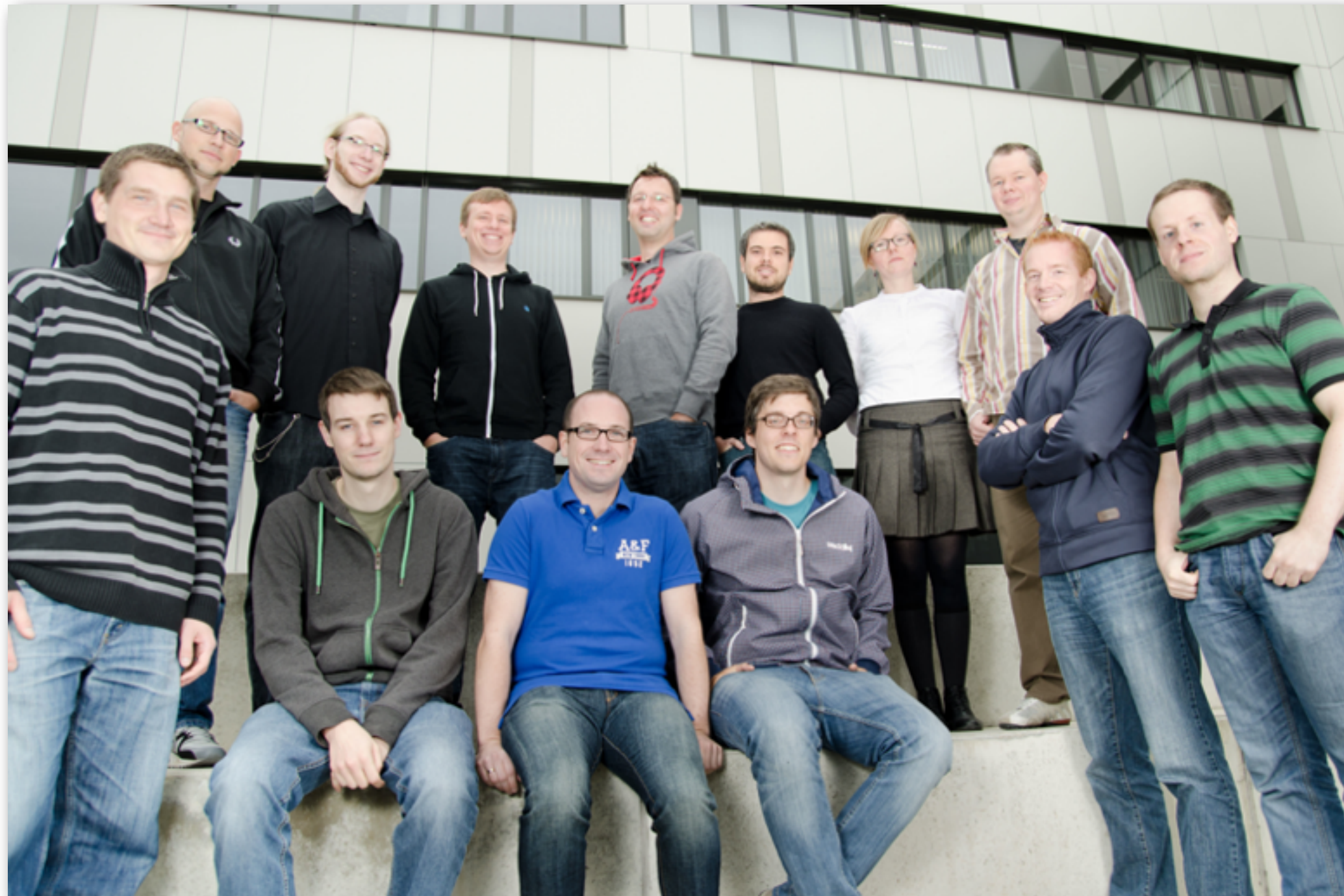
Prof. Roland Gabriel
Prof. Brigitte Werners

Jura

Prof. Georg Borges

Chair for Systems Security

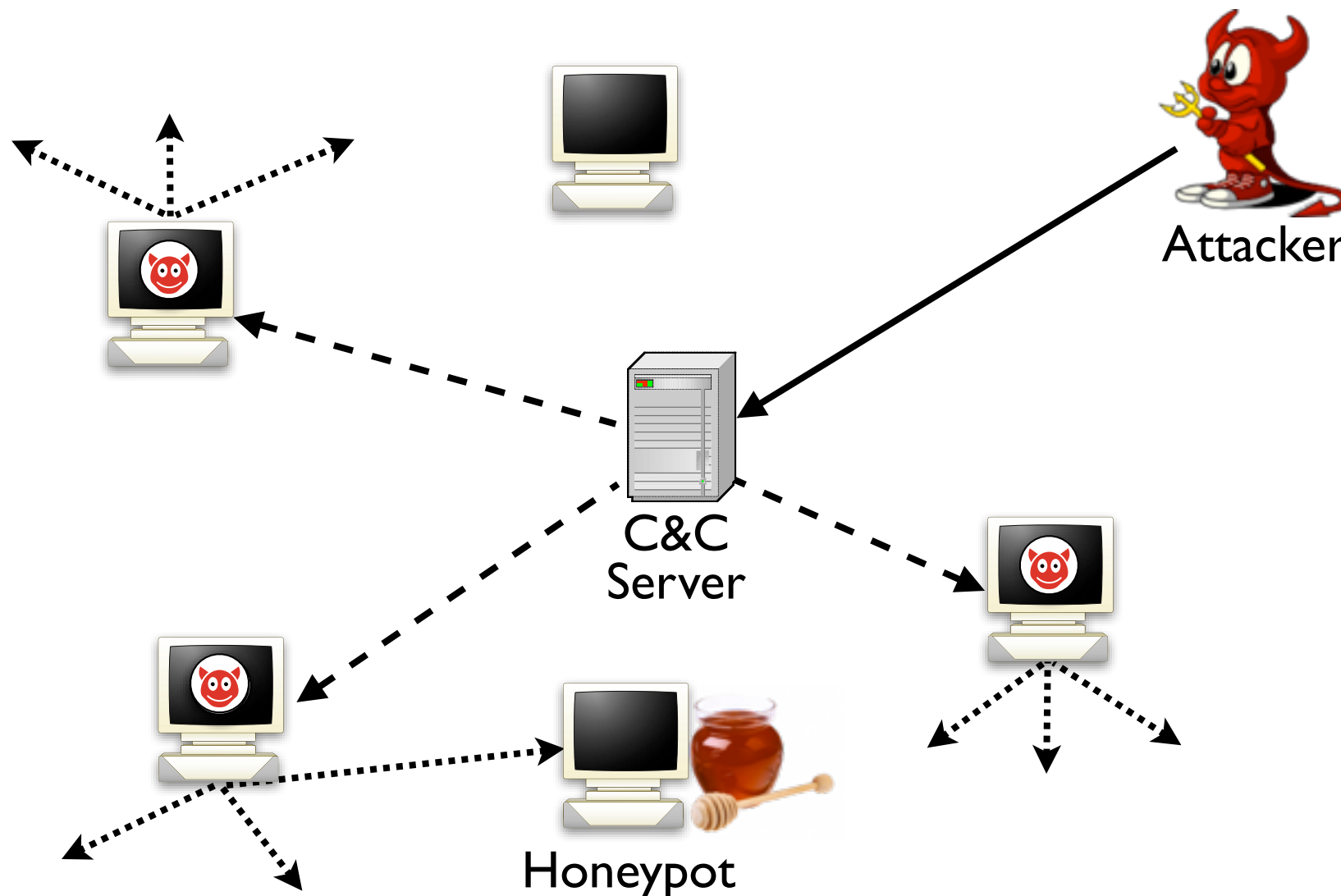
Systems Security
Ruhr-University Bochum



Research Topics

Systems Security
Ruhr-University Bochum

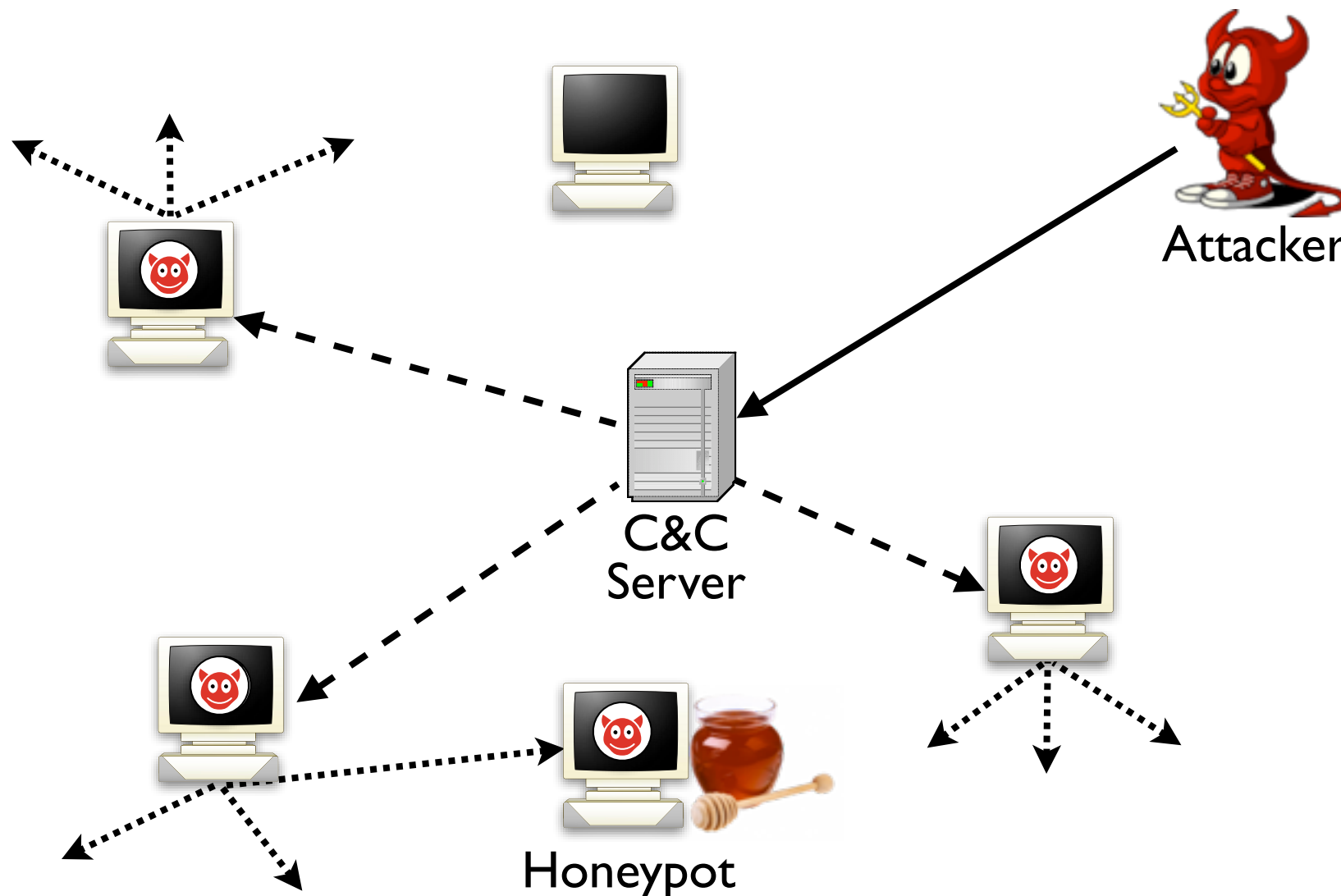
Research focus on *systems security* (botnets, honeypots, malware analysis, security of social networks, ...)



Research Topics

Systems Security
Ruhr-University Bochum

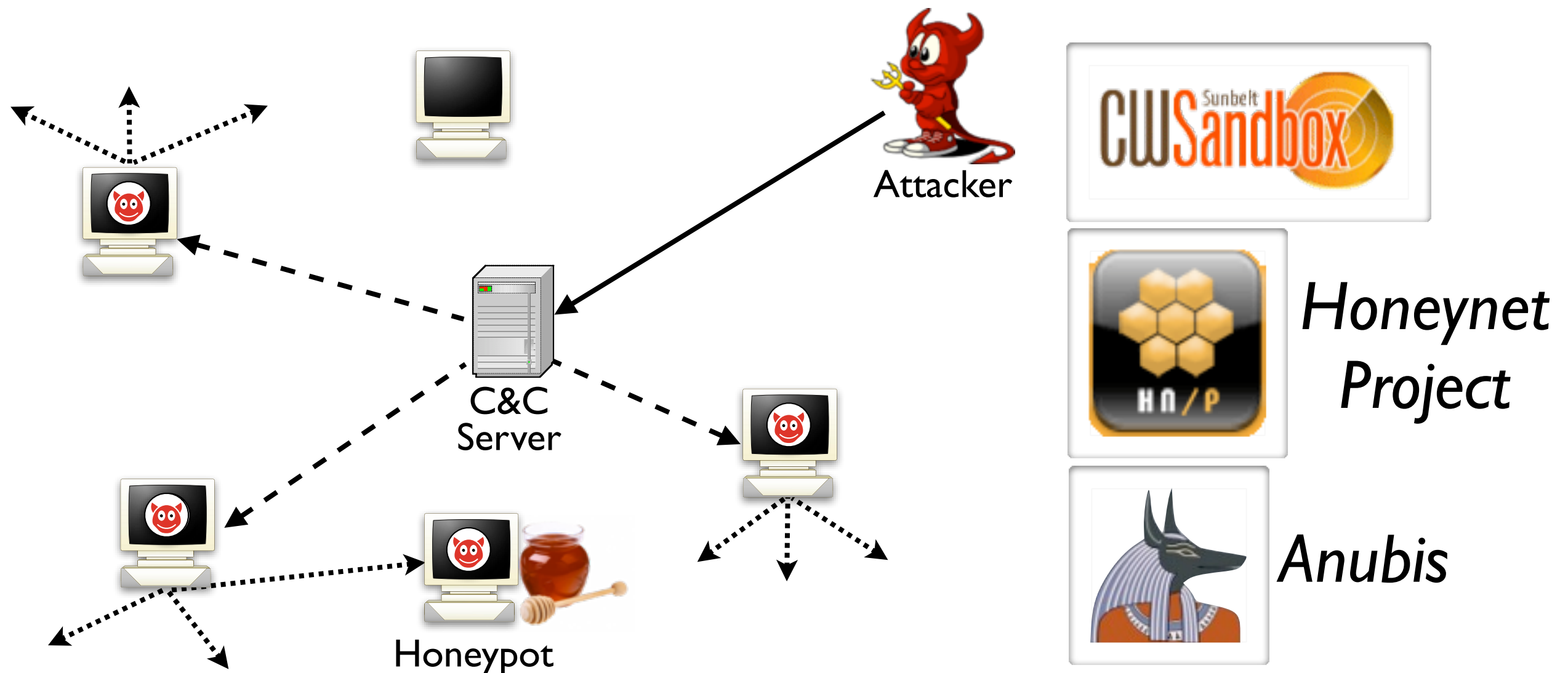
Research focus on *systems security* (botnets, honeypots, malware analysis, security of social networks, ...)



Research Topics

Systems Security
Ruhr-University Bochum

Research focus on *systems security* (botnets, honeypots, malware analysis, security of social networks, ...)



APT and More?

Operation Aurora

<http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>



Insights from Googlers into our products, technology, and the Google culture.

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors—have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.



RSA Compromise

Home > Programs

Open Letter to RSA Customers



Arthur W. Coviello,
Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Source: <http://www.rsa.com/node.aspx?id=3872>



RSA Compromise

Home > Programs

Open Letter to RSA Customers



Arthur W. Coviello,
Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the information being extracted from our products is specifically related to RSA SecurID products. While at this time we are confident that the attack on any of our RSA SecurID products will not reduce the effectiveness of a current implementation as part of a broader attack. We are very actively providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.



Source: <http://www.rsa.com/node.aspx?id=3872>



RSA Aftermath:



Systems Security
University Bochum

Source: <http://www.nytimes.com/2011/06/04/technology/04security.html>

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times **Business Day**
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search Technology Go

Inside Technology | Internet | Start-Ups | Business Computing | Companies | Bits Blog

Stolen Data Is Tracked to Hacking at Lockheed

By CHRISTOPHER DREW
Published: June 3, 2011

[Lockheed Martin](#) said Friday that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users.



Lockheed's finding confirmed the fears of security experts about the safety of the SecurID tokens and heightened concerns that other companies or government agencies could be vulnerable to hacking attacks.

The tokens, which are used to protect remote access to computer networks, are sold by the RSA Security Division of the EMC Corporation. RSA officials said Friday that they accepted Lockheed's findings and were working with customers to offset the risks through other measures.

- RECOMMEND
- TWITTER
- LINKEDIN
- SIGN IN TO E-MAIL
- PRINT
- REPRINTS
- SHARE

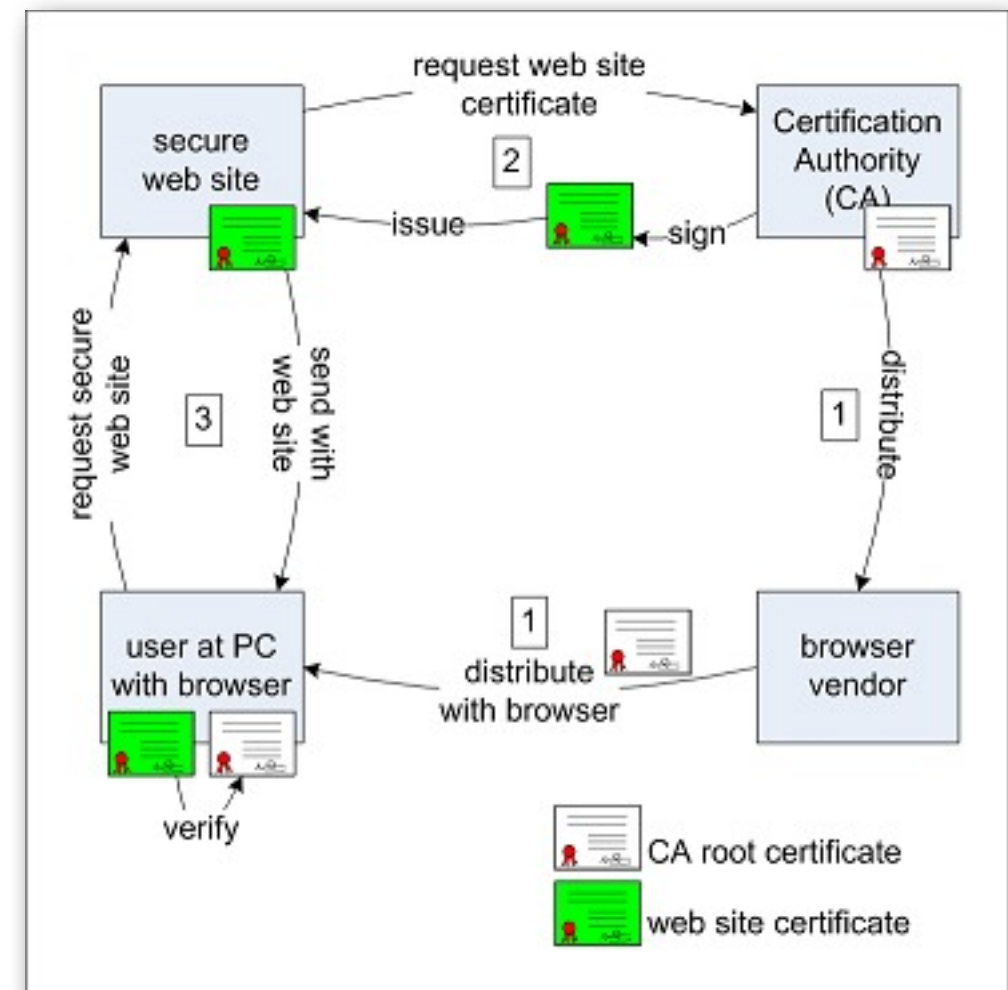


APT == Botnets?

- The sophistication of *Advanced Persistent Threats* is often limited
- Sometimes zero-day attacks, but often against older software versions
- Remote access tools are often standard malware
- It often takes weeks or even months until such attacks are detected
- Why are attackers successful? What can we do?

SSL Certificates

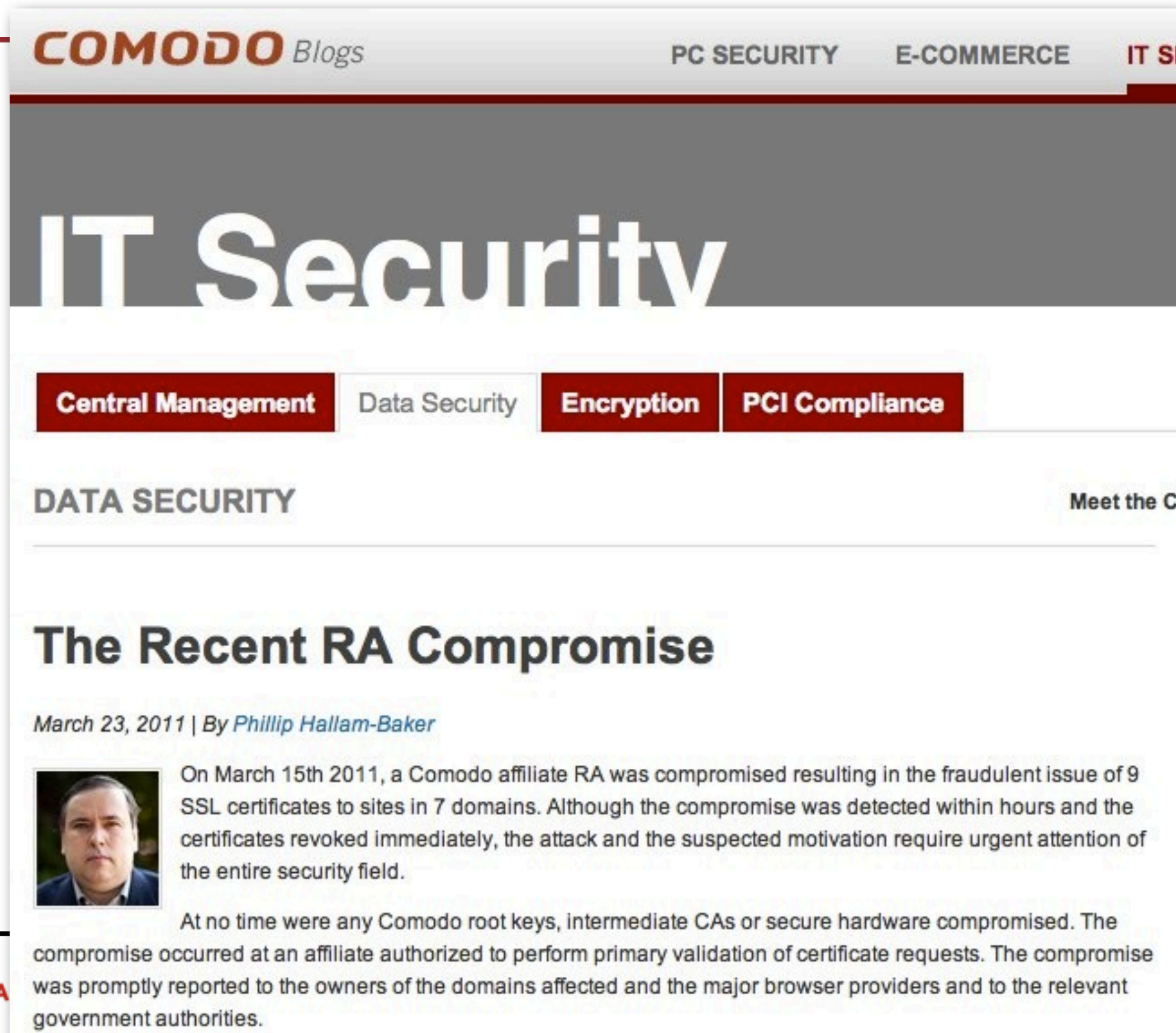
- SSL certificates are one of the “roots of trust” on the Internet
- A so called *Certification Authority (CA)* issues these certificates (e.g., Verisign or Comodo)
- Browser vendors distribute CA root certificates such that browsers can check validity



Source: <http://www.win.tue.nl/hashclash/rogue-ca/>

Comodo Compromise

<http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/>



The screenshot shows a blog post on the Comodo website. The header includes the Comodo logo and navigation links for 'PC SECURITY', 'E-COMMERCE', and 'IT SECURITY'. The main heading is 'IT Security'. Below this are four navigation buttons: 'Central Management', 'Data Security', 'Encryption', and 'PCI Compliance'. The article is categorized under 'DATA SECURITY' and features a sub-header 'The Recent RA Compromise' by Phillip Hallam-Baker, dated March 23, 2011. The article text describes a security incident where a Comodo affiliate RA was compromised, leading to the fraudulent issuance of 9 SSL certificates across 7 domains. It notes that the compromise was detected quickly and certificates were revoked, but the event is significant for the security community. A photo of Phillip Hallam-Baker is included. The article concludes by stating that Comodo's root keys and hardware were not affected, and the incident was reported to domain owners, browser providers, and government authorities.

ity
ochum



Comodo Compromise

<http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/>

COMODO Blogs

PC SECURITY

E-COMMERCE

IT S

ity
ochum

Several other CAs were compromised, too!

Central Management

Data Security

Encryption

PCI Compliance

DATA SECURITY

Meet the C

The Recent RA Compromise

March 23, 2011 | By Phillip Hallam-Baker



On March 15th 2011, a Comodo affiliate RA was compromised resulting in the fraudulent issue of 9 SSL certificates to sites in 7 domains. Although the compromise was detected within hours and the certificates revoked immediately, the attack and the suspected motivation require urgent attention of the entire security field.

At no time were any Comodo root keys, intermediate CAs or secure hardware compromised. The compromise occurred at an affiliate authorized to perform primary validation of certificate requests. The compromise was promptly reported to the owners of the domains affected and the major browser providers and to the relevant government authorities.



Stuxnet

- Highlights attacks against control systems
- Attackers do not target only PCs
- Other embedded systems are vulnerable to this kind of attacks as well
- Highly sophisticated attack
 - *Advanced persistent threat (APT)*
 - State-sponsored attack?



A Look Behind the Malware Business



Spam

- One of the major problems we need to deal with
 - ~90% of worldwide email traffic is spam
 - ~85% of spam is sent with the help of *botnets*
 - Advertise cheap pharmaceutical drugs, distribute malware, perform scams, ...



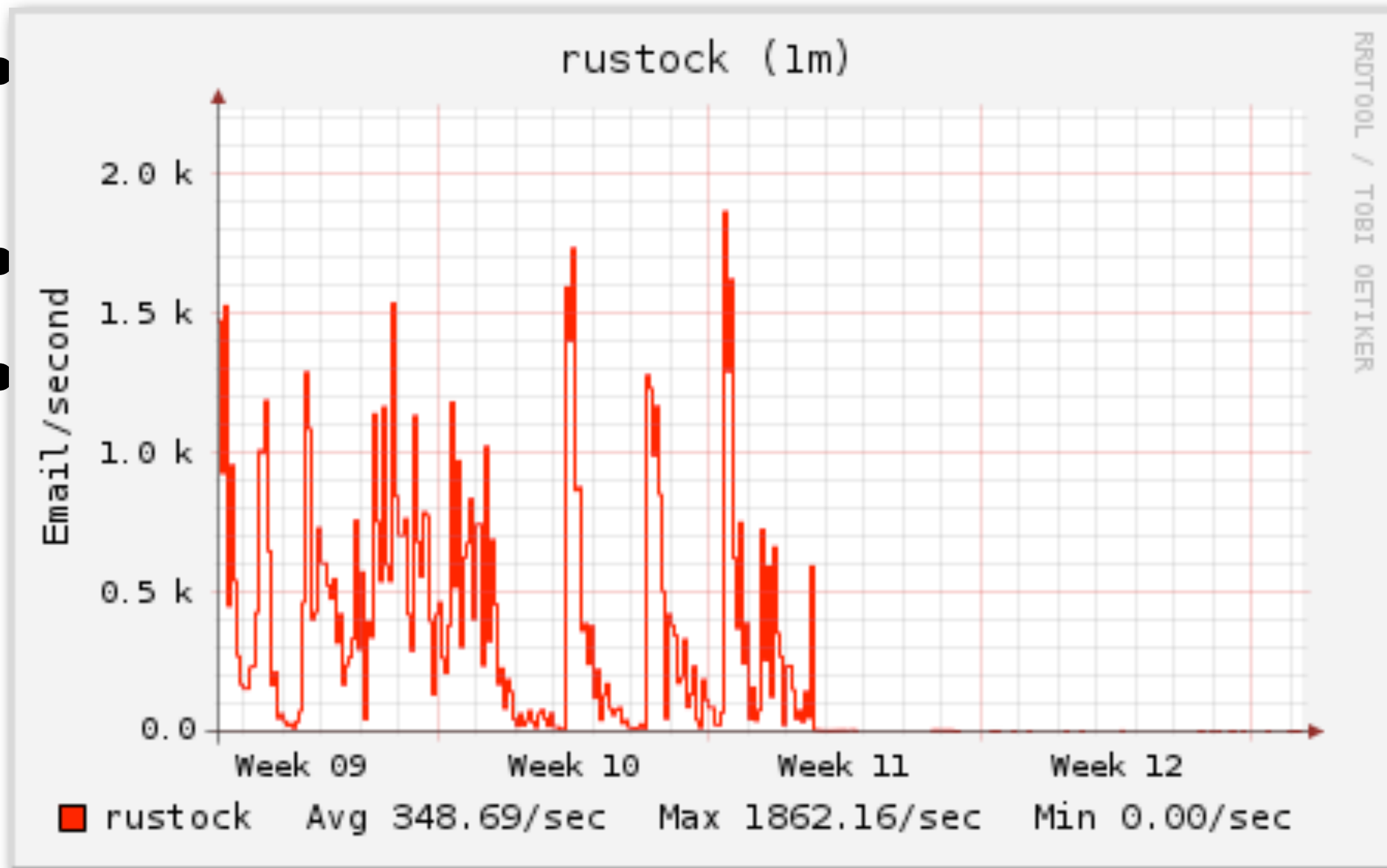
Spam

- One of the major problems we need to deal with
 - ~90% of worldwide email traffic is spam
 - ~85% of spam is sent with the help of *botnets*
 - Advertise cheap pharmaceutical drugs, distribute malware, perform scams, ...
- Two interesting incidents in 2011
 - Takedown of Rustock botnet
 - Takedown of Pushdo/Cutwail botnet

Rustock

- Rustock was largest spam botnet, responsible for ~30% of e-mail spam traffic on the Internet
- Takedown in March 2011
- Operation **b107**, lead by Microsoft
- Second instance of Project MARS (*Microsoft Active Response for Security*)
- First was Operation **b49** (Waledac takedown)
- Last one was Operation **b70** (Nitol takedown)

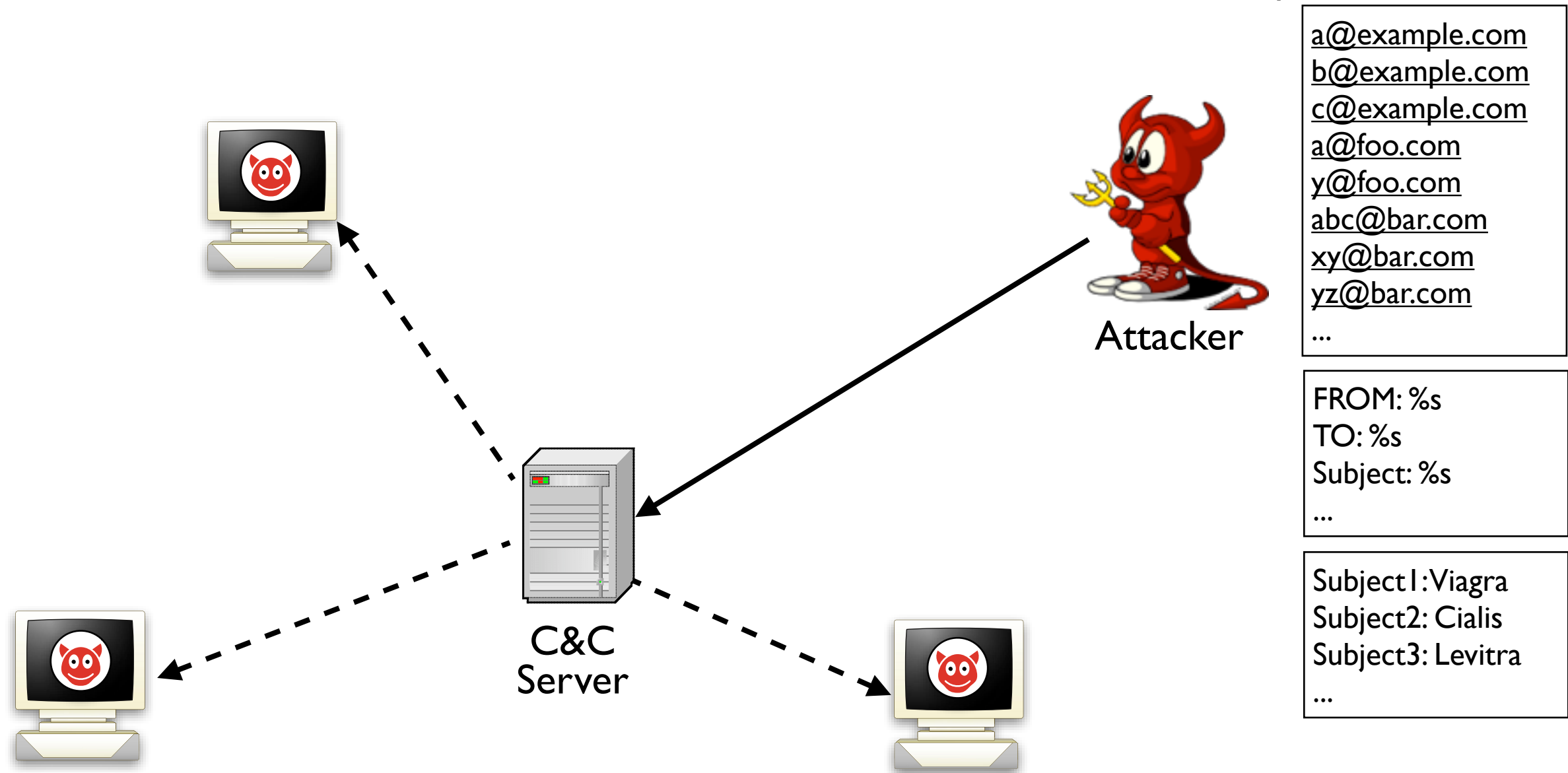
Rustock



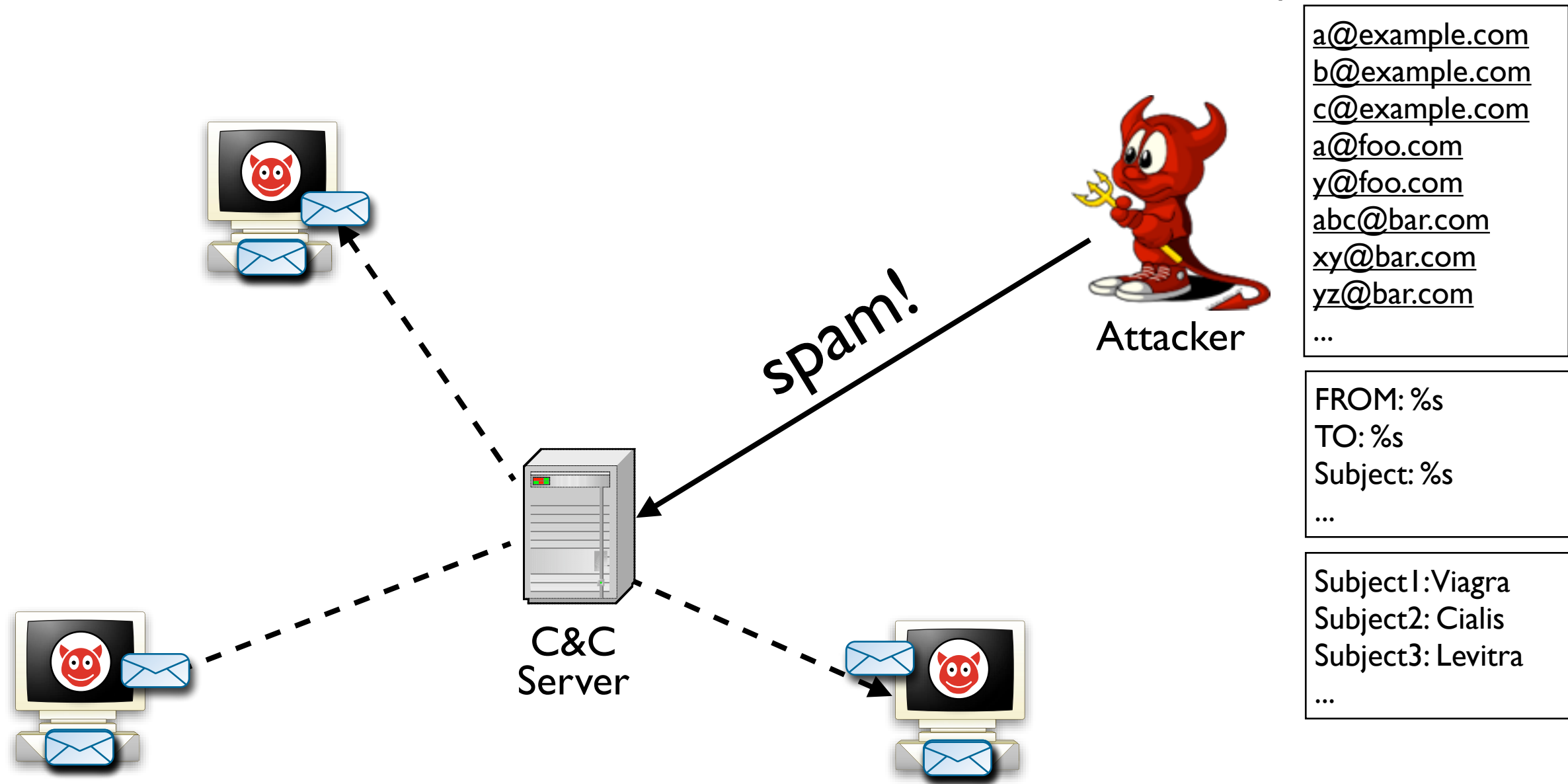
Rustock

- Rustock was largest spam botnet, responsible for ~30% of e-mail spam traffic on the Internet
- Takedown in March 2011
- Operation **b107**, lead by Microsoft
- Second instance of Project MARS (*Microsoft Active Response for Security*)
- First was Operation **b49** (Waledac takedown)
- Last one was Operation **b70** (Nitol takedown)

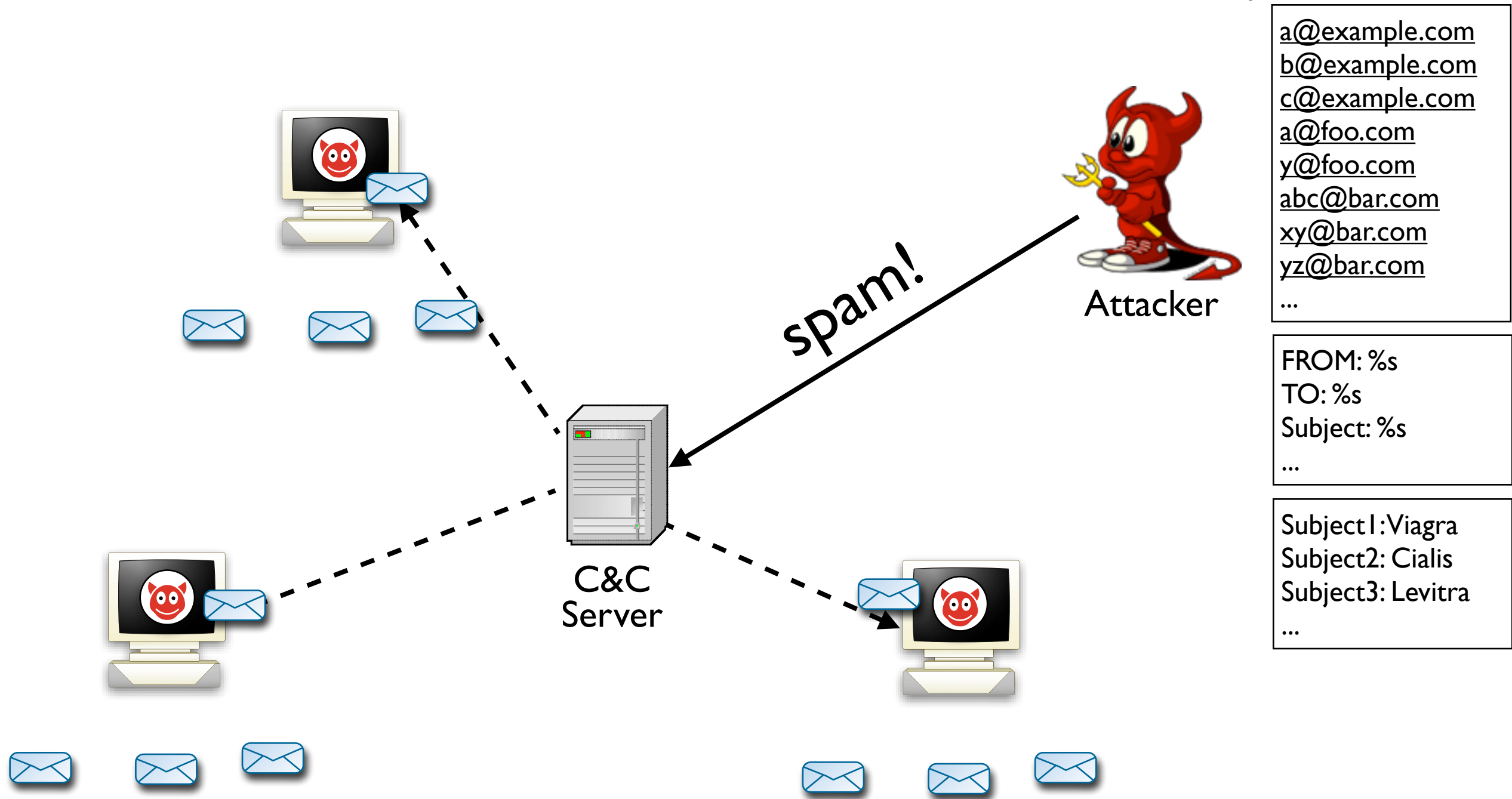
Spam Botnets



Spam Botnets



Spam Botnets



```
a@example.com  
b@example.com  
c@example.com  
a@foo.com  
y@foo.com  
abc@bar.com  
xy@bar.com  
yz@bar.com  
...
```

```
FROM: %s  
TO: %s  
Subject: %s  
...
```

```
Subject1:Viagra  
Subject2: Cialis  
Subject3: Levitra  
...
```

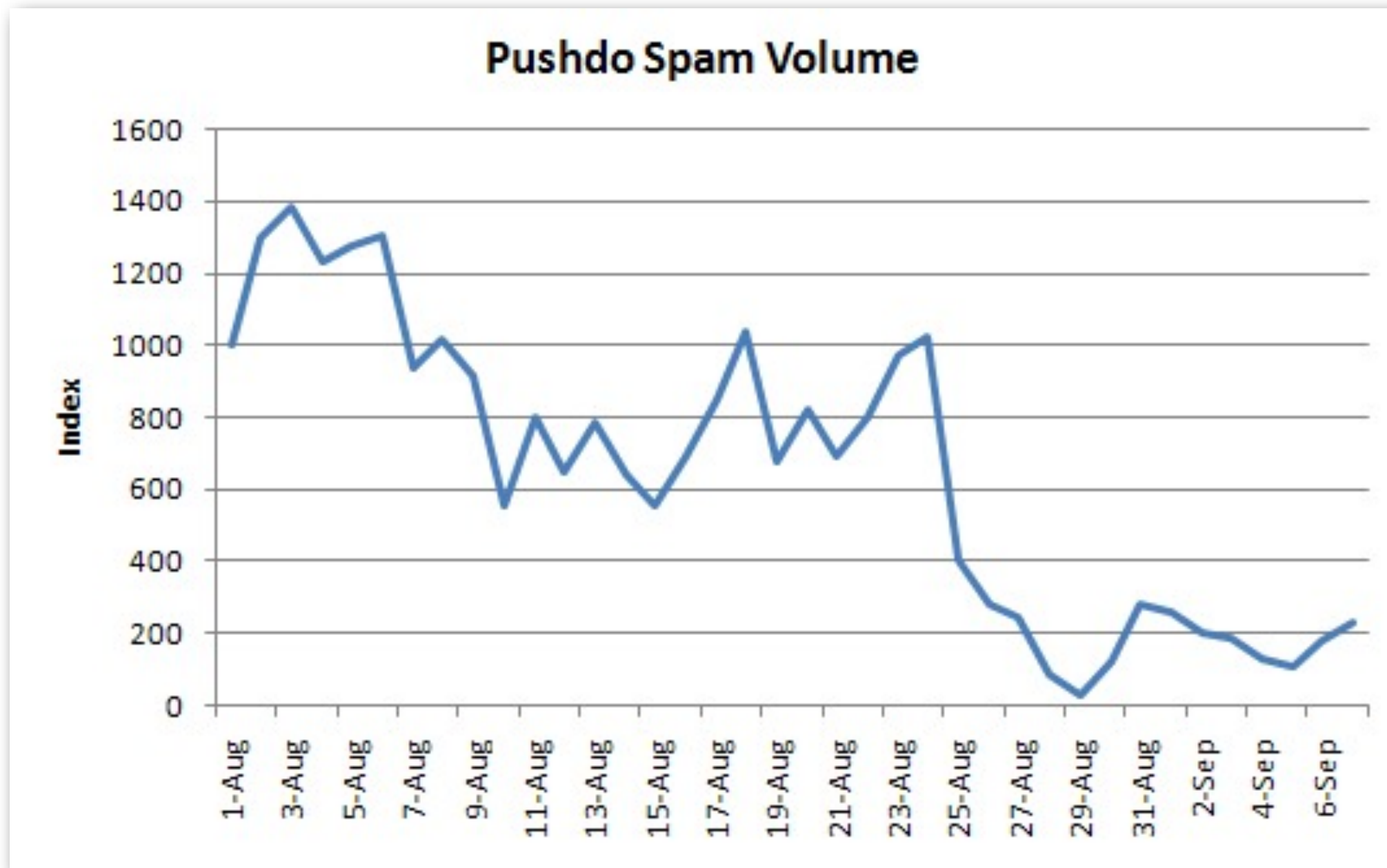

Pushdo/Cutwail

- In-depth study of Pushdo/Cutwail botnet
- Collaboration with Brett Stone-Gross, Gianluca Stringhini and Giovanni Vigna (UCSB), paper published at USENIX LEET'11
- Has been used by some of the most prolific spammers
- Also interesting from a technical perspective
 - Encrypted communication protocol
 - Automated, template-based spamming system

Takedown

- Identified 30 Cutwail C&C servers
- 20 servers shut down, obtained access to 16 servers
- More than 2.35 TB of data
- 24 databases with detailed statistics about infected machines and overall spam operations
- Spam templates and billions of target email addresses for spam campaigns
- Botnet's source code and instruction manual

Takedown Effects

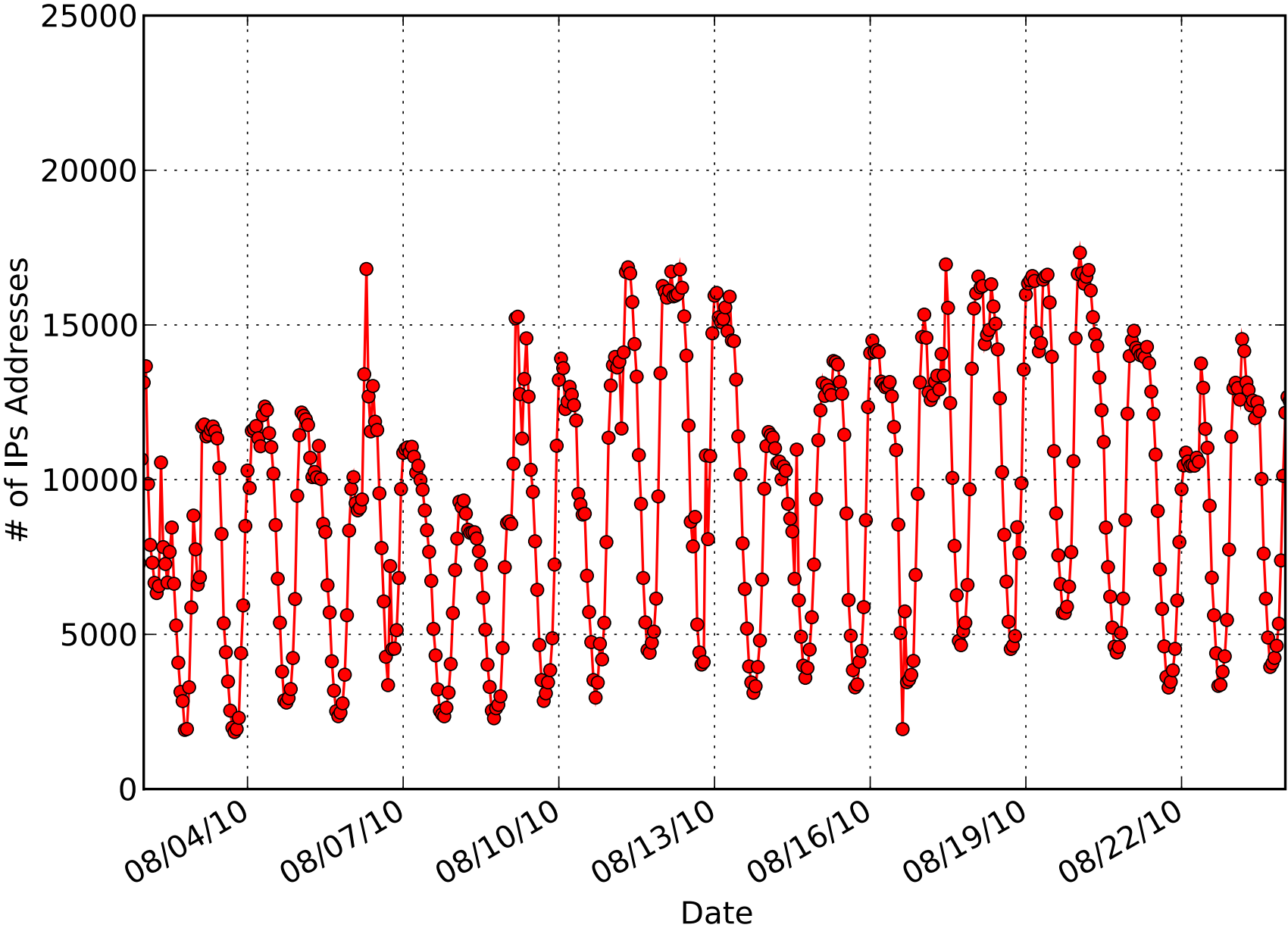


Source: M86Security

Cutwail Size

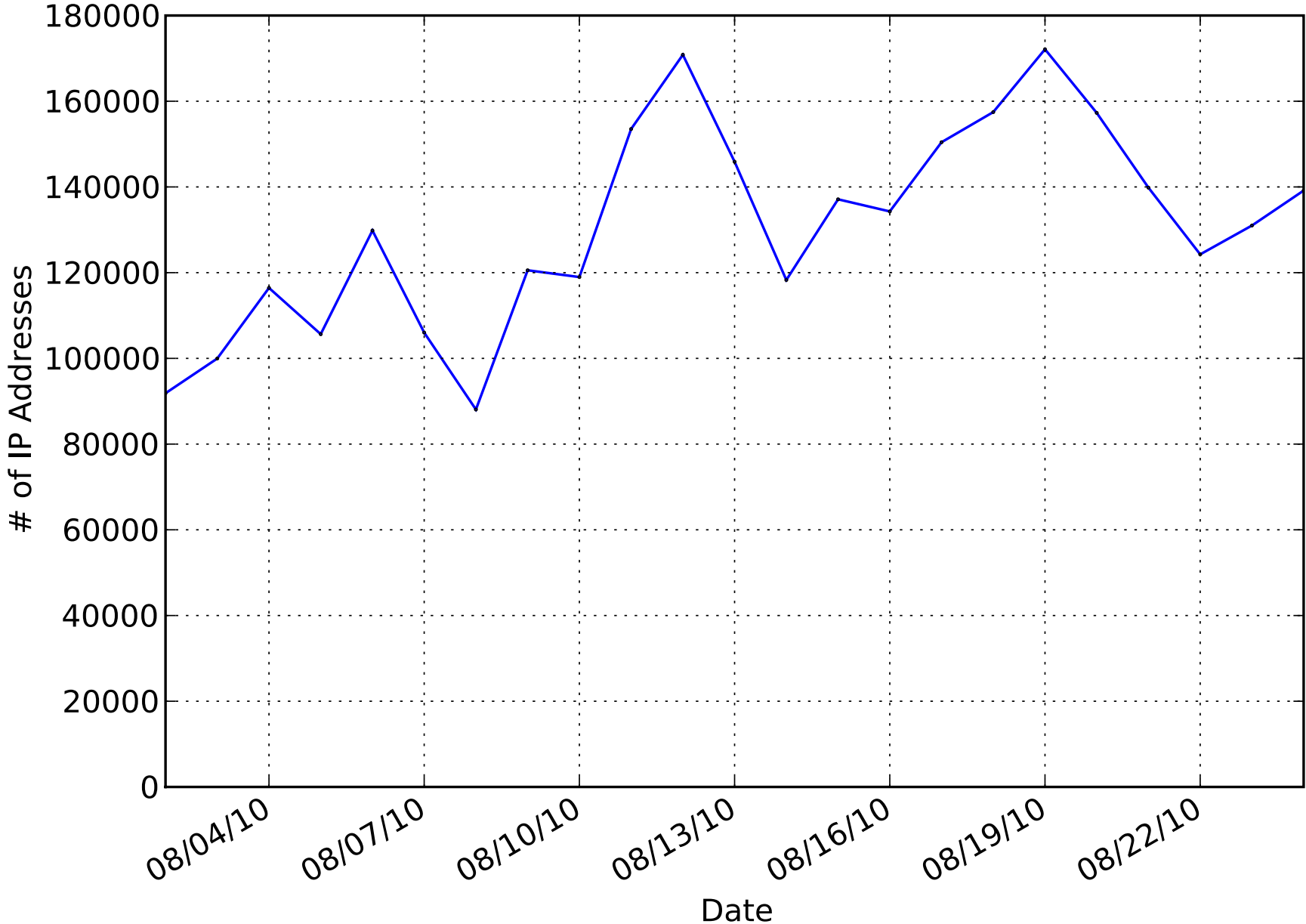
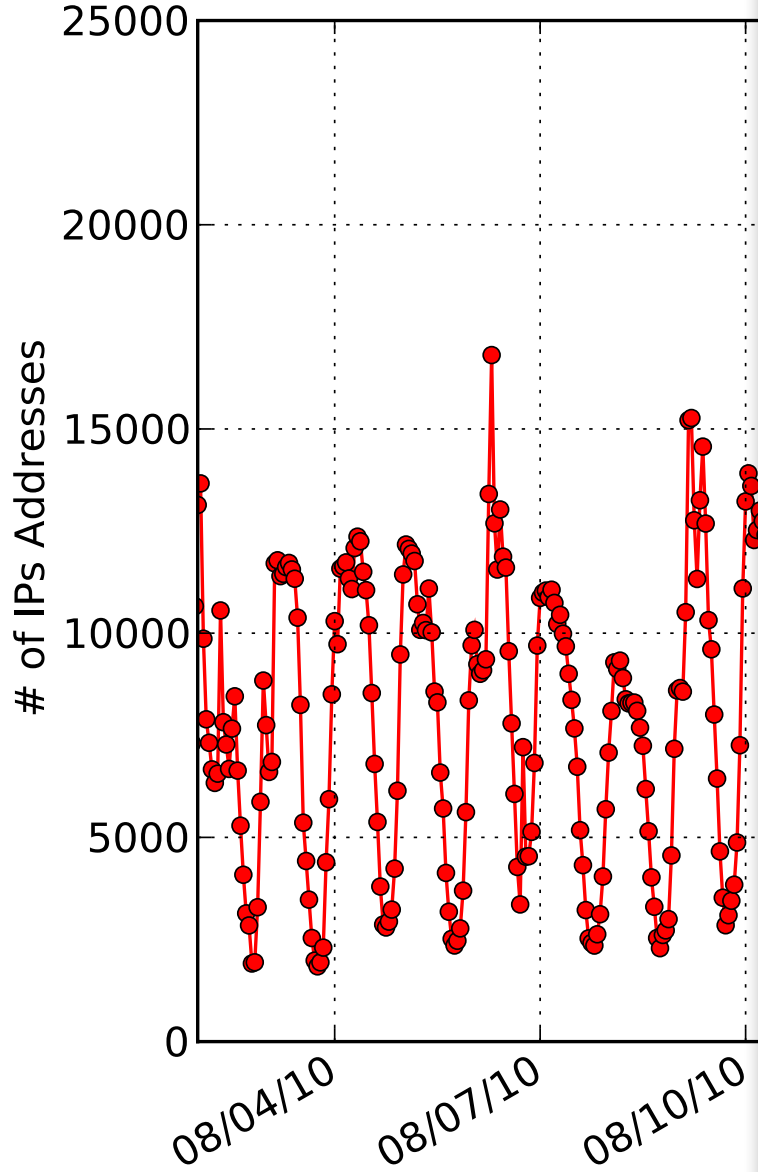
- Size of a botnet is an important metric
- Unfortunately, no unique identifier per bot
- Estimate for size: *number of unique IP addresses on an hourly basis*
- 121,336 unique IPs online per day
- 2,536,934 total IPs observed

Cutwail Size



bot
Addresses on an

Cutwail Size



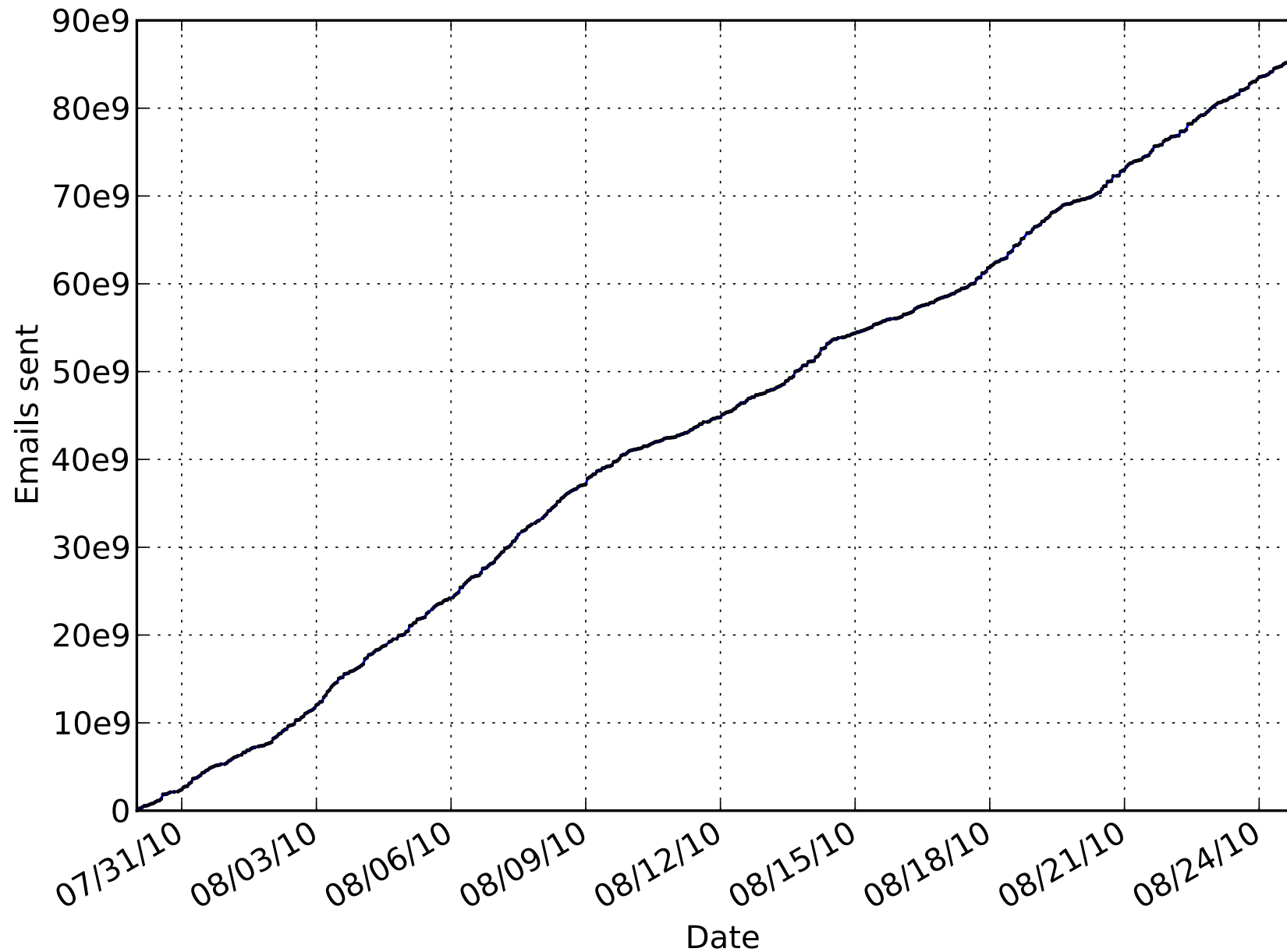
Spam Campaign Dynamics

- Databases contain meticulous records for each bot
- Only 30.3% of the mails were actually delivered to target mail server, many causes of errors
 - Invalid email address (53.3%)
 - SMTP blacklisting (16.9%)
 - Misc. SMTP error (11.8%)
 - Connection timeout (11.3%)

Spam Campaign Volume

- Volume is immense
- **87.7 billion** emails sent between July 30 and August 25, 2010
- Sum of all reports on all C&Cs: 516,852,678,718 messages were accepted for delivery out of a total of 1,708,054,952,020 attempts
- ... and this is only based on an analysis of only about half of the C&Cs of one particular spam botnet

Spam Campaign Volume



18
total

out

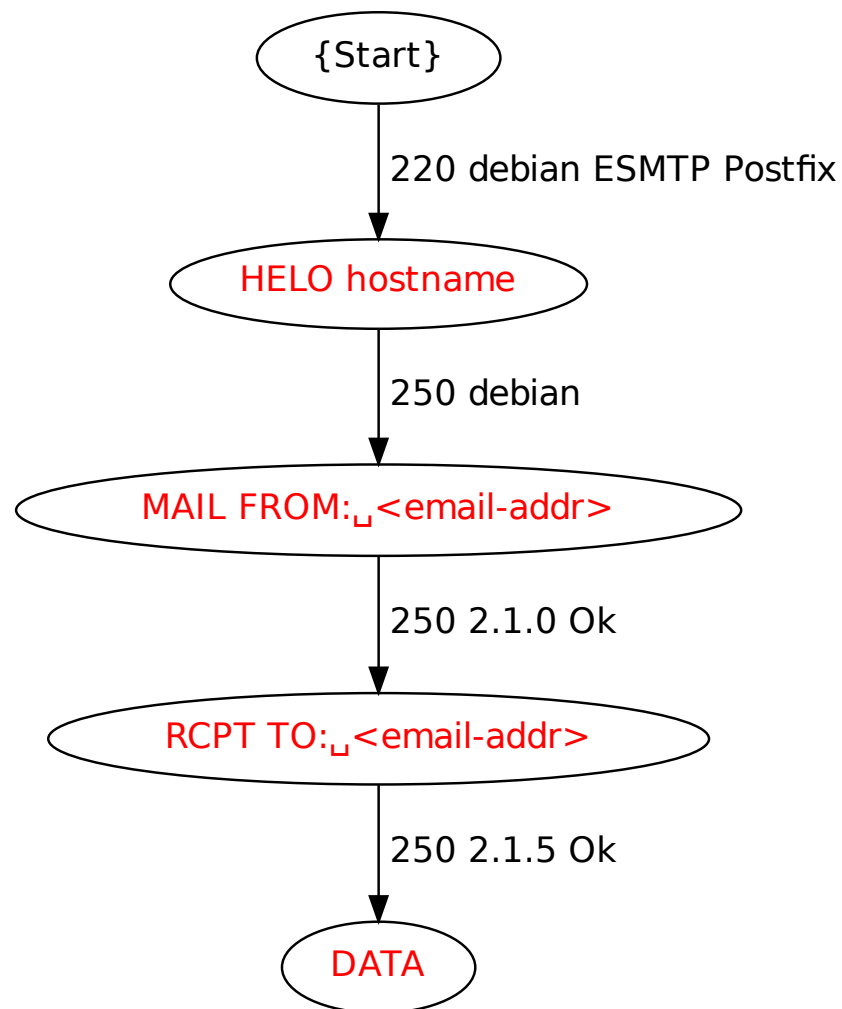
Spam Operations

Systems Security
Ruhr-University Bochum

Client (ID)	Instances (#)	Unique Bot IPs (#)	Avg. Lifespan (Days)	Mails Sent (#)	Average Mails/Active Bot (Per Day)	Campaign Type
1	8	2,251,156	17	98,401,907,545	2,571	Phishing, Malware
2	2	40,924	168	45,555,535,375	6,626	Phishing
3	2	56,733	54	155,098,090,946	50,626	Diplomas
4	2	34,742	22	17,941,545,204	23,473	Phishing, Pharm.
5	1	21,993	8	60,169,427,197	341,980	Money Mule
6	1	29,471	13	4,309,066,448	11,247	Pharmaceuticals
7	1	27,658	55	9,408,910,232	6,185	Phishing
8	1	30,503	135	12,485,832,067	3,032	Phishing
9	1	29,415	18	2,365,652,828	4,467	Real Estate

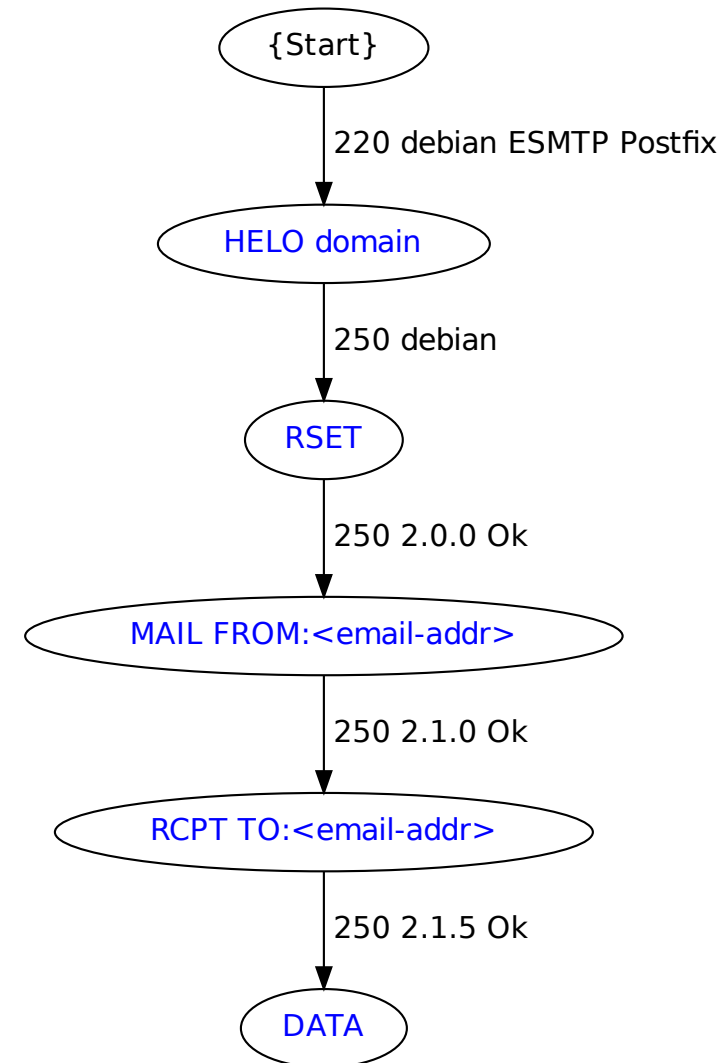
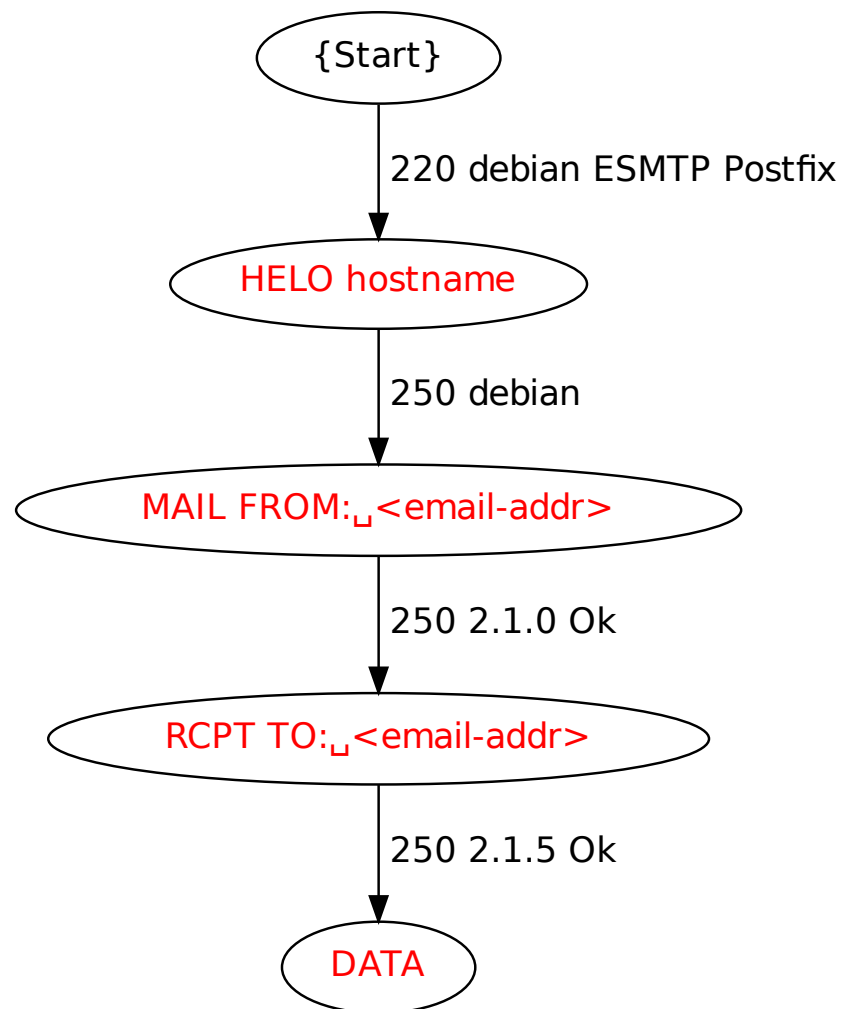
- Spam-as-a-Service can be purchased for ~\$100–\$500 per million emails sent
- Larger campaigns: 100 million emails per day for \$10,000 per month

Spam Analysis



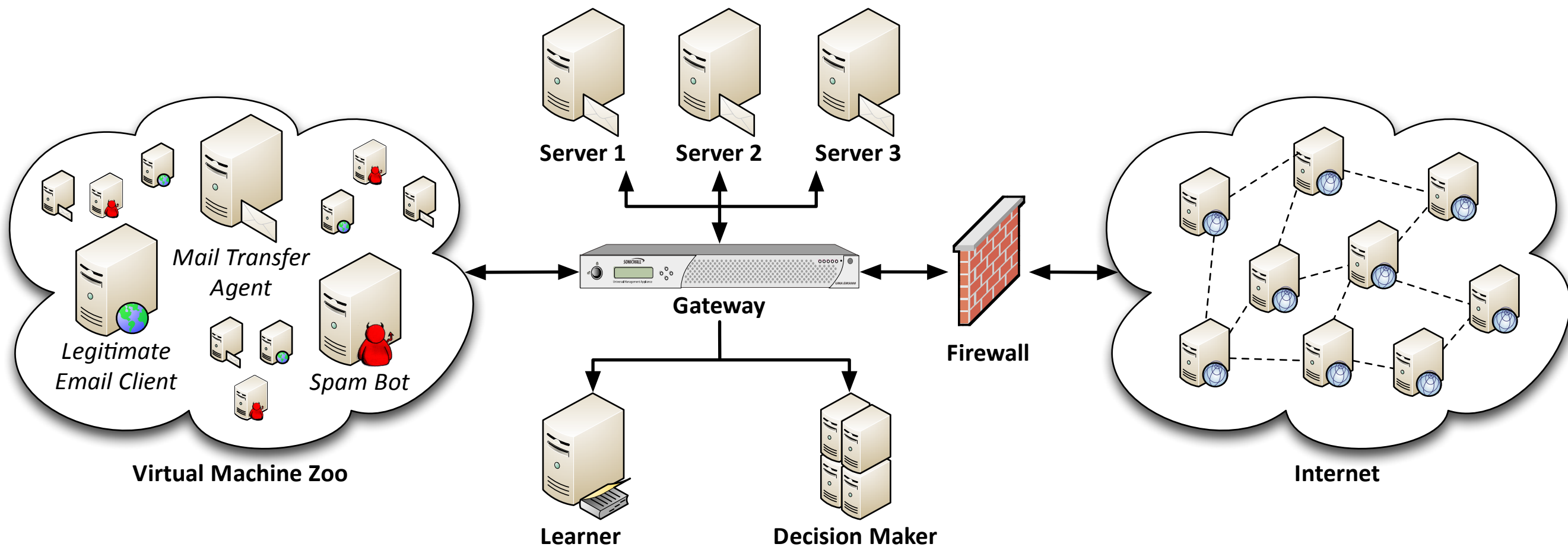
“B@bel: Leveraging Email Delivery for Spam Mitigation”
by Stringhini et al., Usenix Security’12

Spam Analysis



“B@bel: Leveraging Email Delivery for Spam Mitigation”
by Stringhini et al., Usenix Security’12

Spam Analysis



“B@bel: Leveraging Email Delivery for Spam Mitigation”
by Stringhini et al., Usenix Security’12

Other Projects

Systems Security
Ruhr-University Bochum



GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung



Gefördert durch:



Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages



GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

SASER

Summary I

- We saw quite a lot of successful attacks recently
- *Advanced Persistent Threat (APT)* pose a risk to many companies, but the term is often overhyped
- Do we need more ways to retrofit security to deployed systems?
- Better detection techniques?
- Better malware analysis techniques?
- More approaches to stop root cause behind spam?

Summary II

- We saw SSL certificates failing several times in 2011
- We need to come up with something better
- There are some ideas, but none is convincing
- Attacks are very lucrative, what can we do about this?
 - Economic aspects are interesting
 - *Workshop on the Economics of Security (WEIS)*

Questions?

Systems Security
Ruhr-University Bochum

Contact:

Thorsten Holz

thorsten.holz@rub.de

@thorstenholz on Twitter



More info:

<http://syssec.rub.de>