Security in Computing & Information Technology

Lecture 12

Internet Banking

Crimeware

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

- Credit cards on the Internet
- Mobile banking
- Crimeware

Quote(s) of the day

- "So now, when we face a choice between adding features and resolving security issues, we need to choose security."
- -***Bill Gates***

The user's going to pick dancing pigs over security every time.
-***Bruce Schneier***

Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench.
-***Gene Spafford***

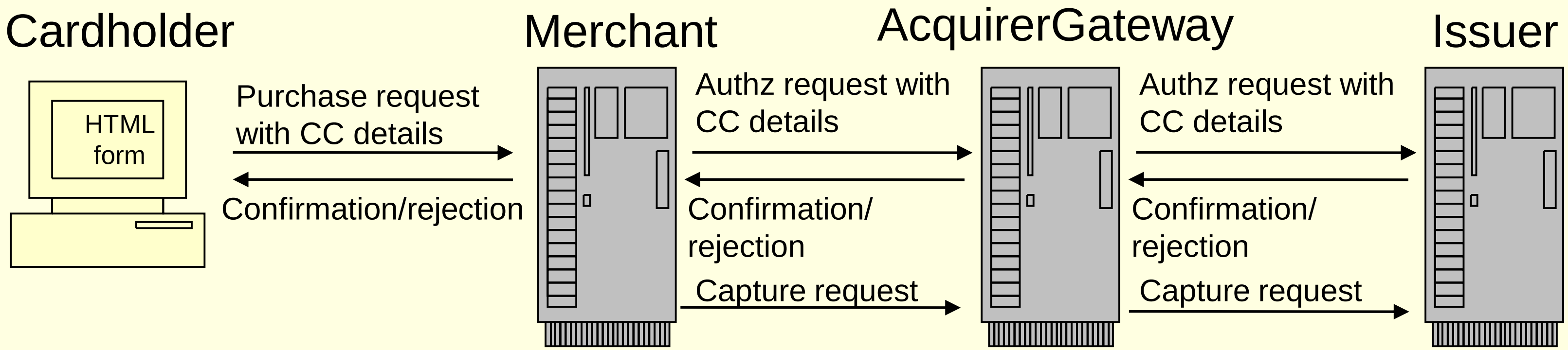
If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
-***Bruce Schneier***

Credit Card Payments

- Credit cards have been around for decades
- Still accounts for around 95% of all online sales.
- Existing credit card information is sent over the Internet in encrypted form.
- To make a purchase,
  - consumer sends encrypted card information to merchant
  - merchant passes card info to bank for payment processing

Credit Card Transactions – Entities

Issuer:	provides the CC to the customer
Cardholder:	makes the payment
Merchant:	receives the payment
Acquirer:	processes the payment
Gateway:	bridge to CC network



Cardholder

Merchant

AcquirerGateway

Issuer

HTML form

Purchase request with CC details

Confirmation/rejection

Authz request with CC details

Confirmation/ rejection

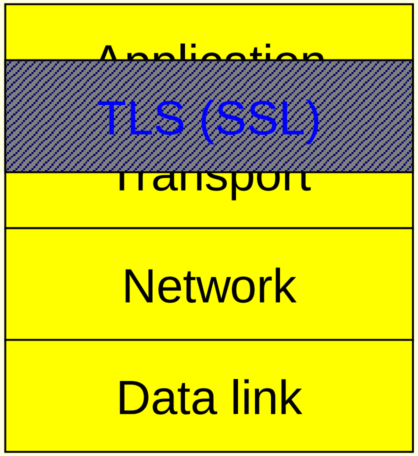
Capture request

Authz request with CC details

Confirmation/ rejection

Capture request

Protecting Credit Card Content



Application

TLS (SSL)

Transport

Network

Data link

- Technical aspects
  - TCP/IP is not secure.
  - Communications is protected
    - TLS (SSL) sits between the transport and application layer, and supports:
      - Integrity, Confidentiality
      - Server & (optional) Client auth
- Trusted actors are needed
  - Eg: PayPal - 'trust and safety' is their priority

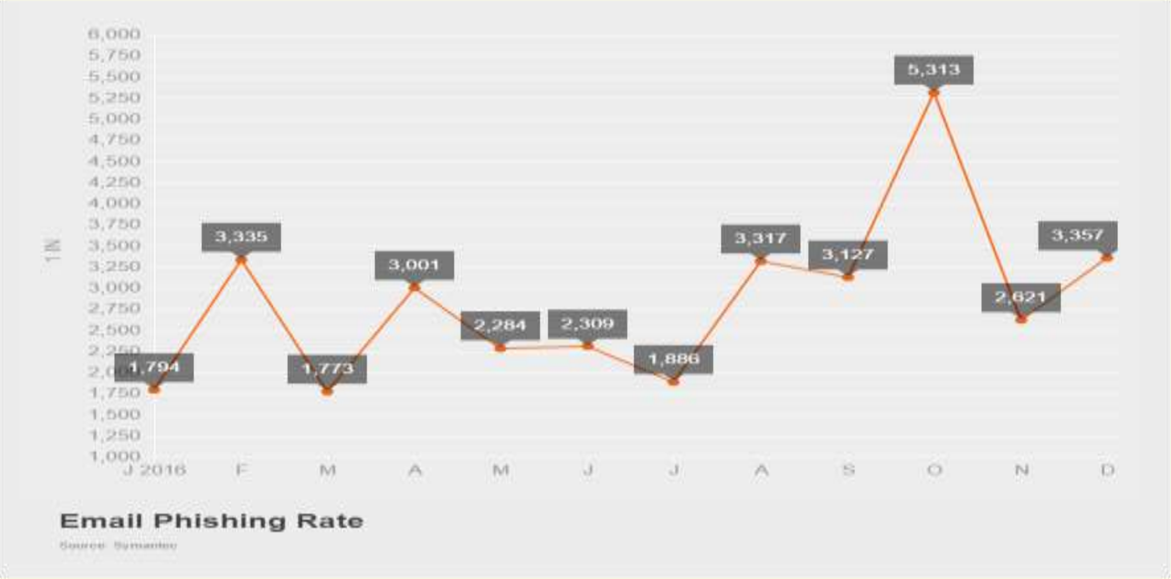
    ~200million users (Q4 2016), ~100billion US$ (2016),

    Large percentage of staff dealing with security

Internet Banking Attacks

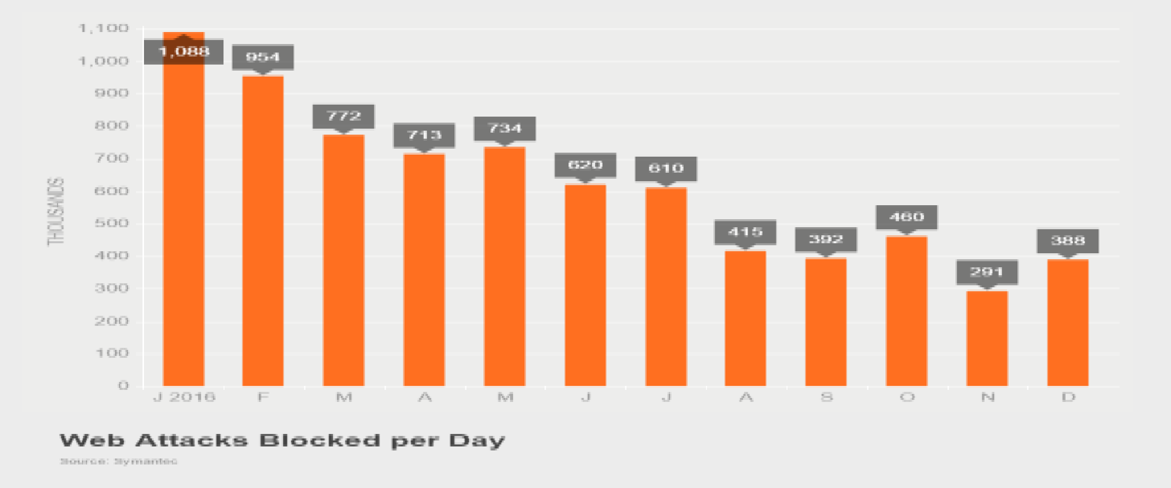
- Phishing
  - Fraudulent websites to capture sensitive customer details
  - Spear Phishing / Whaling
    - Targeted phishing, eg to senior executives
  - Vishing
    - Phone (eg VoIP) phishing (eg fake call centre)
- Pharming
  - Attacker redirects website traffic to another fraudulent site (eg DNS redirects)
- Search Engine Optimisation (SEO)
- Advanced Persistent Threats (APT)

Attack Statistics



Email Phishing Rate

Source: Symantec



Web Attacks Blocked per Day

Source: Symantec

Image source: https://www.symantec.com/security_response/publications/monthlythreatreport.jsp

Common Phishing Attack Methodology

From: admin@hackme.com
Subject: Security Alert

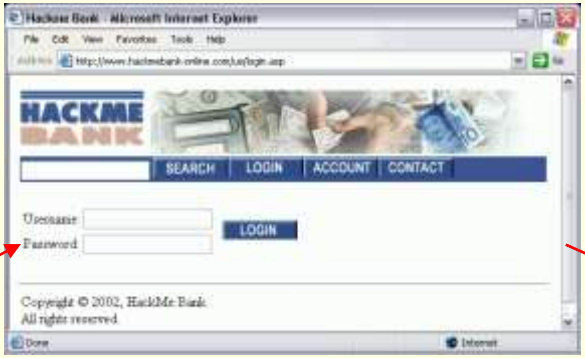
Dear HackMe Bank Client,

We are performing system maintenance, wich may interfere with access to your Online Services. Due to these technical updates your online account has been deactivated.

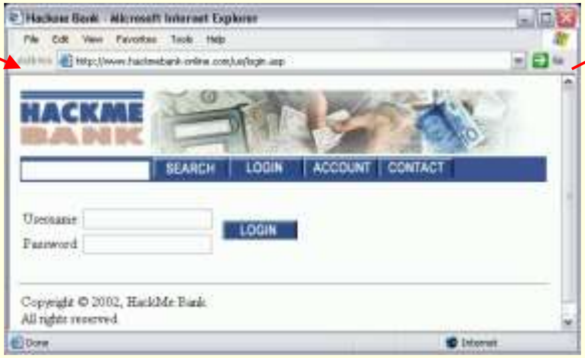
Click here to reactivate:

http://www.hackmebank.com/us/login.asp

Real Site


Hackme Bank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
http://www.hackmebank-online.com/us/login.asp
HACKME BANK
SEARCH
LOGIN
ACCOUNT
CONTACT
Username
Password
LOGIN
Copyright © 2002, HackMe Bank
All rights reserved
Done
Internet

Fake Site


Hackme Bank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
http://www.hackmebank-online.com/us/login.asp
HACKME BANK
SEARCH
LOGIN
ACCOUNT
CONTACT
Username
Password
LOGIN
Copyright © 2002, HackMe Bank
All rights reserved
Done
Internet

Attacker Data Collection

Name: John Doe
Address: 15 Broadway Ave
SSN: 123 45 6789
CC: 4388 1234 1234 1234
Username: jdoe
Password: password

Name: Jane Doe
Address: 15 7th Ave
SSN: 123 45 6798
CC: 4388 1234 1234 4321
Username: jane.doe
Password: password

Source: http://www.owasp.org/images/5/5c/AppSec2005DC-Danny_Allan-Identity_Theft_Phishing_and_Pharming.ppt

Phishing: Prevention (1)

- Technology
  - Web application security
    - Restrict Track / Trace HTTP methods
    - Output Encoding
    - Use “httpOnly” & “secure” cookie flags
    - Break out of frames
      - if (self != top) top.location = self.location;
  - Web application firewalls
    - XSS detection
    - Content referrer restrictions

Source: http://www.owasp.org/images/5/5c/AppSec2005DC-Danny_Allan-Identity_Theft_Phishing_and_Pharming.ppt

Phishing: Prevention (2)

- Operational
  - Customer Education
    - Describe how you will interact with them
    - Possible ID theft techniques & safeguards
  - Email Communication
    - Be consistent with all customer communication
    - Do not ask for personal information
  - Web
    - Blanket SSL
    - Two factor authentication
    - Domain name consistency

Source: http://www.owasp.org/images/5/5c/AppSec2005DC-Danny_Allan-Identity_Theft_Phishing_and_Pharming.ppt

Authenticating E-mail

- It is easy to spoof email
  The Simple Mail Transfer Protocol (SMTP) has no built-in protection
- Spoofed source is commonly used for spam and attack emails
- Additional methods are used for verification of source and intermediate nodes
  - Publishing the identity of servers
    Sender Policy Framework (SPF)
  - Digitally signing emails
    Domain Key Identified Mail (DKIM)

Sender Policy Framework (SPF)

- Participating domains publish the features of mail originating from them
  - Method: an SPF resource record (SPFRR) is registered at the sender's domain name server (DNS)
  - Most frequently used feature: IP addresses of computers authorised to send email
- Receivers check those features by retrieving the SPFRR from the sender's domain
- SenderID: a (slightly) improved version of SPF

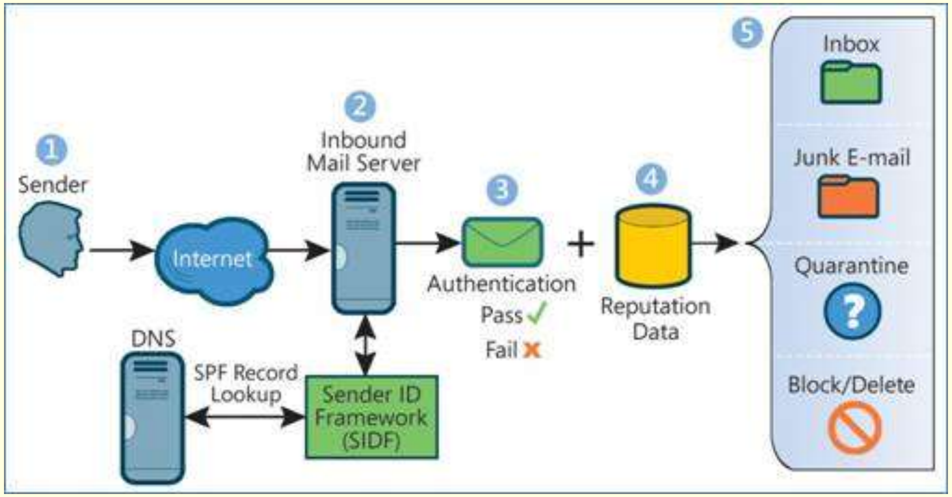


Image source: http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/

Domain Keys Identified Mail (DKIM)

- The sender domain
  - Digitally signs the email
  - Inserts the signature into the email (in the DKIM-Signature field)
- Receiver retrieves the domain's public key from the sender's DNS and verifies the signature
- Becoming more popular than SPF
- Very useful but not foolproof method

Card Types

- Smart Cards
  - Smarter than traditional magnetic strip card.
  - Have the potential for storing value, plus a wide range of personal information on a chip.
  - Think e-tag, Myki, ...
- PayWave, PayPass
  - Near-field communication (NFC)
    - Technology exists to copy (steal) data from an RFID chip
      - Complex attack, no report of its use in finance (yet)
      - Easier to rack up many transactions under $100

Mobile Banking

- Mobile Phones
  - Thick clients / mini-browsers for iPhone, Windows Mobile, etc
  - SMS authentication
  - Peer to peer payments
- EftPOS
  - Debit-card transaction processing
  - Wireless terminals now common-place
- ATMs
  - Mag-stripe or chip-and-pin bank cards
  - PIN numbers (3-DES) read by encrypting PIN PAD (EPP) and secure crypto-processor
  - Common attacks include card skimming, pin-hole cameras, ram-raids

Digital Currencies

- Electronic money schemes
  - Use traditional currency with legal foundation
- Virtual currency schemes
  - Cryptocurrencies: use crytpographic solutions to secure transactions and control the creation of units (more than 740 cryptocurrencies exist in total – according to Wikipedia)
  - Convertible to real money
  - Best known: Bitcoin
    - Non-traceable, favourite of the black market

□ Market Order (buy/sell at market price) This order either gets executed immediately or cancelled.

GBP in your account: £0.00000 (add more) | Lowest Ask Price: £91.50000

Amount of BTC to BUY: Enter amount X Price per coin in GBP: 91.5 = Total to spend in GBP: 0

Image source: http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf/

Digital Currency-Related Attacks

- Bitcoin mining
  - Websites can use their visitors for calculations in background scripts (Web Workers)
  - Botnets used for mining
- Attacking Bitcoin exchange

Image source: http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf/

Regulatory Compliance – PCI DSS

- Payment Card Industry Data Security Standards
- Merchants that conduct credit card transactions online must comply with PCI-DSS
- Compliance is performed as follows:
  - vulnerability assessment (VA) scanning by a PCI-approved security vendor (ASV)
  - controls assessment by PCI-approved Qualified Security Assessor (QSA)

PCI DSS Requirements

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Financial Incident Timeline

- Statistics of 2016 data

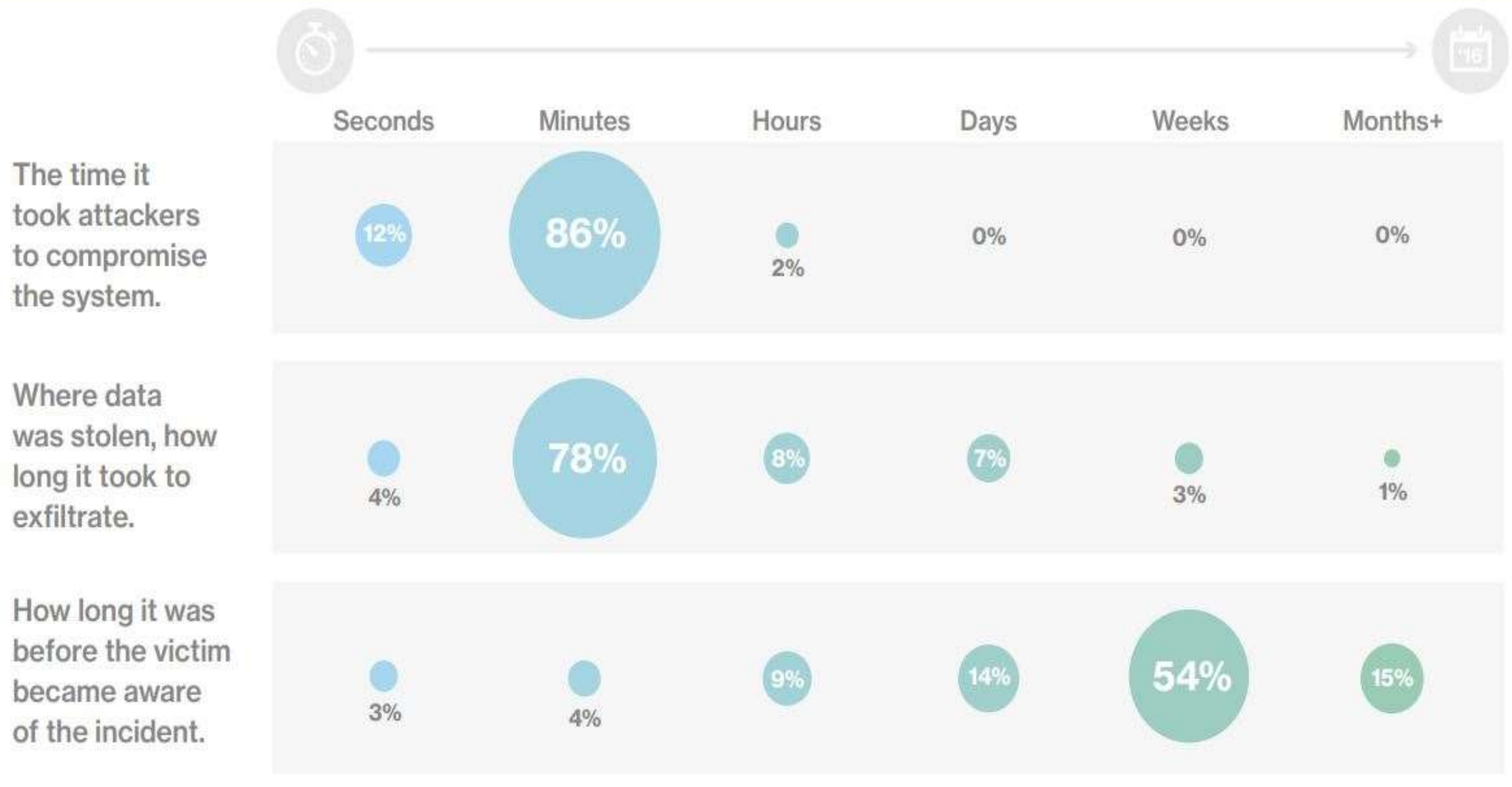
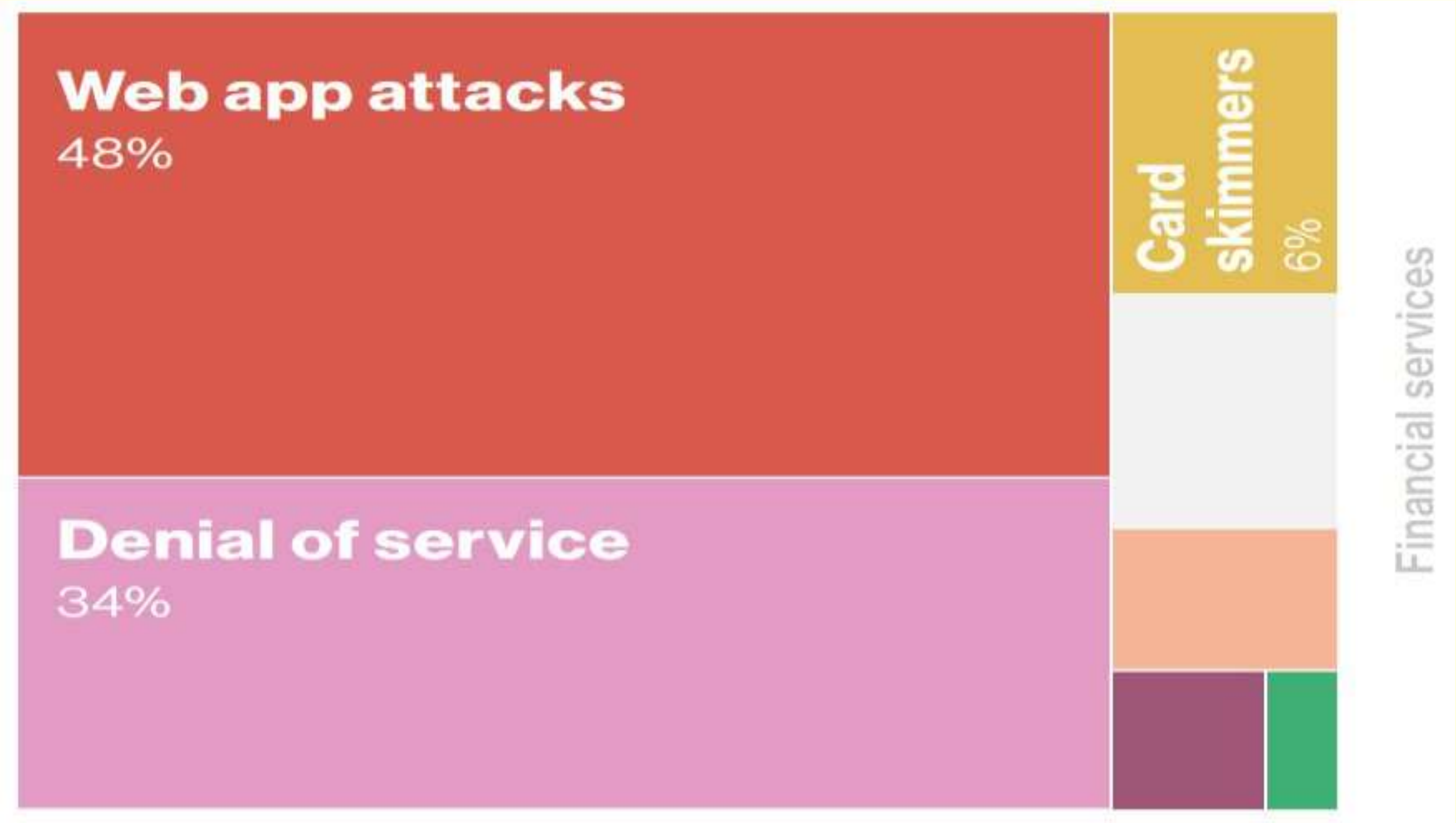


Image source: http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Financial-Data-Security_en_xg.pdf

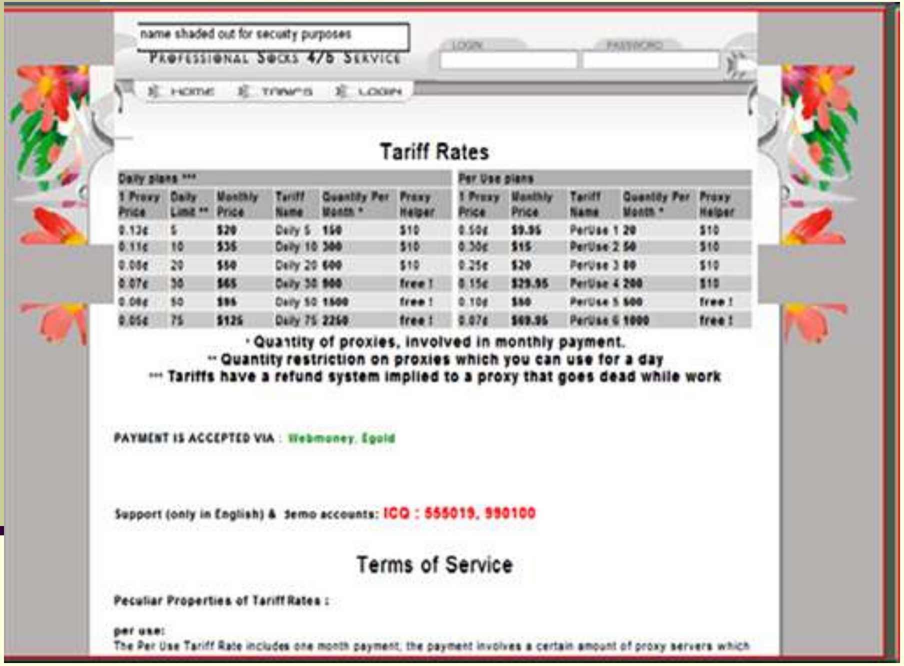
Financial Service Attack Types

- Statistics of 2016 data



Cybercrime Trends – Crimeware

Crimeware as a service:
Botnet for rent



name shaded out for secuity purposes

PROFESSIONAL SOCKS 4/5 SERVICE

Tariff Rates

Daily plans ***					
1 Proxy Price	Daily Limit **	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper
0.13¢	5	$20	Daily 5	150	$10
0.11¢	10	$35	Daily 10	300	$10
0.08¢	20	$50	Daily 20	600	$10
0.07¢	30	$65	Daily 30	900	free !
0.06¢	50	$95	Daily 50	1500	free !
0.05¢	75	$125	Daily 75	2250	free !

Per Use plans				
1 Proxy Price	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper
0.50¢	$9.95	PerUse 1	20	$10
0.30¢	$15	PerUse 2	50	$10
0.25¢	$20	PerUse 3	80	$10
0.15¢	$29.95	PerUse 4	200	$10
0.10¢	$50	PerUse 5	500	free !
0.07¢	$69.95	PerUse 6	1000	free !

* Quantity of proxies, involved in monthly payment.
** Quantity restriction on proxies which you can use for a day
*** Tariffs have a refund system implied to a proxy that goes dead while work

PAYMENT IS ACCEPTED VIA : Webmoney, Egold

Support (only in English) & demo accounts: ICQ : 555019, 990100

Terms of Service

Peculiar Properties of Tariff Rates :

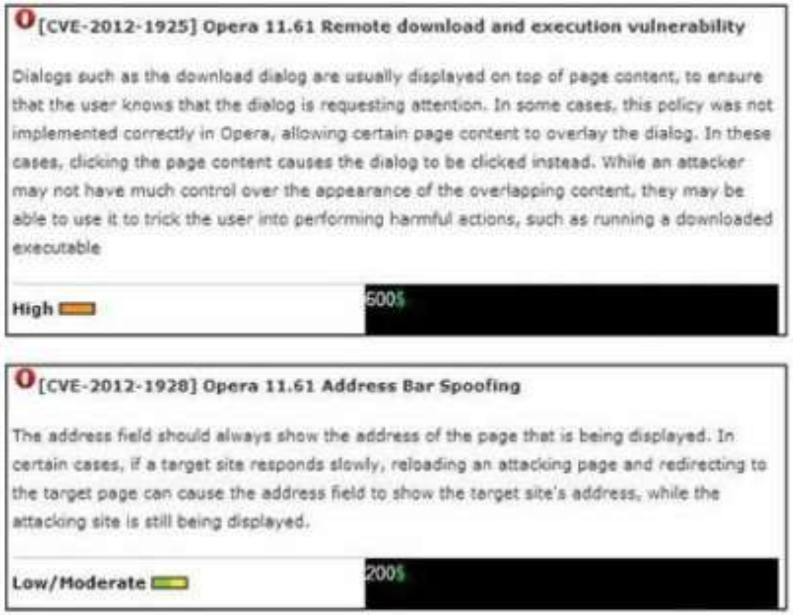
per use:
The Per Use Tariff Rate includes one month payment; the payment involves a certain amount of proxy servers which

- In 2008, the Australian Prime Minister listed CyberCrime as a national Top 10 priority
- $400 to set up your own botnet
  - Can be rented out
- GeoIP to serve dynamic, localised content
- Criminals using device and network encryption (eg Tor, Truecrypt) constantly rising.
- Telcos taking more responsibility on botnets –more pro-active profiling needed (similar to how bank calls when suspicious transactions detected)

Image source: http://deepcontentinspection.com/page/2/

Marketplace for Cybercrime

- Cybercirme as a service
  - Commercial companies selling zero-day vulnerabilities
  - Identification and development of exploits for special operations
  - Hacking as a service
- Marketplaces for stolen information (e.g. payment cards)



[CVE-2012-1925] Opera 11.61 Remote download and execution vulnerability

Dialogs such as the download dialog are usually displayed on top of page content, to ensure that the user knows that the dialog is requesting attention. In some cases, this policy was not implemented correctly in Opera, allowing certain page content to overlay the dialog. In these cases, clicking the page content causes the dialog to be clicked instead. While an attacker may not have much control over the appearance of the overlapping content, they may be able to use it to trick the user into performing harmful actions, such as running a downloaded executable

High 🟧 500$

[CVE-2012-1928] Opera 11.61 Address Bar Spoofing

The address field should always show the address of the page that is being displayed. In certain cases, if a target site responds slowly, reloading an attacking page and redirecting to the target page can cause the address field to show the target site's address, while the attacking site is still being displayed.

Low/Moderate 🟩 200$

The higher the impact the higher the price

Image source: http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf

Underground Markets

- Darknet
  - Overlay network
  - Accessible with special software only
  - Main types
    - Friend-to-friend
    - Anonymity networks
- Darknet market (cryptomarket) for illicit (and legal) goods

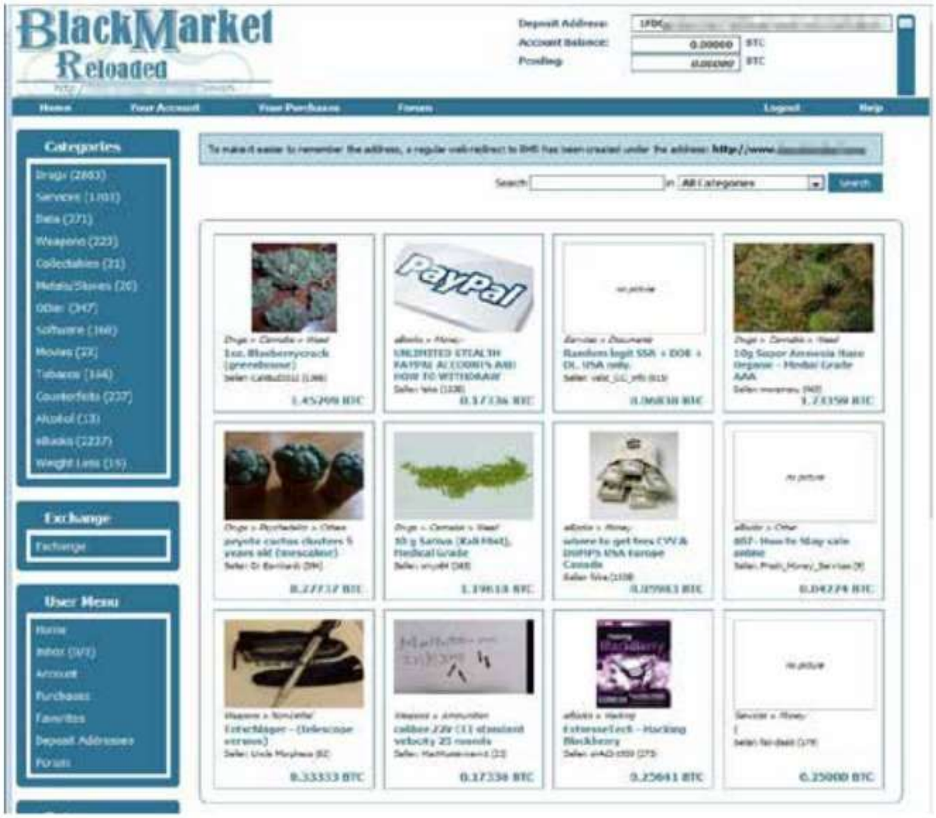
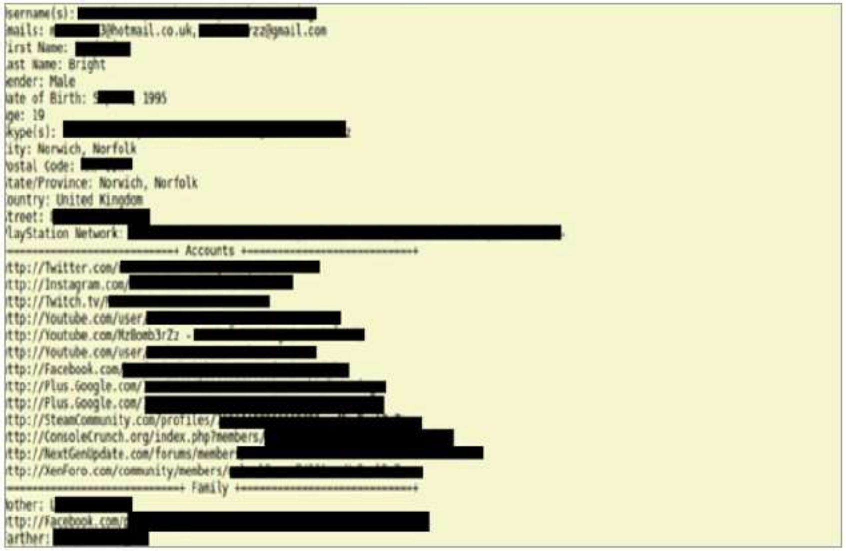


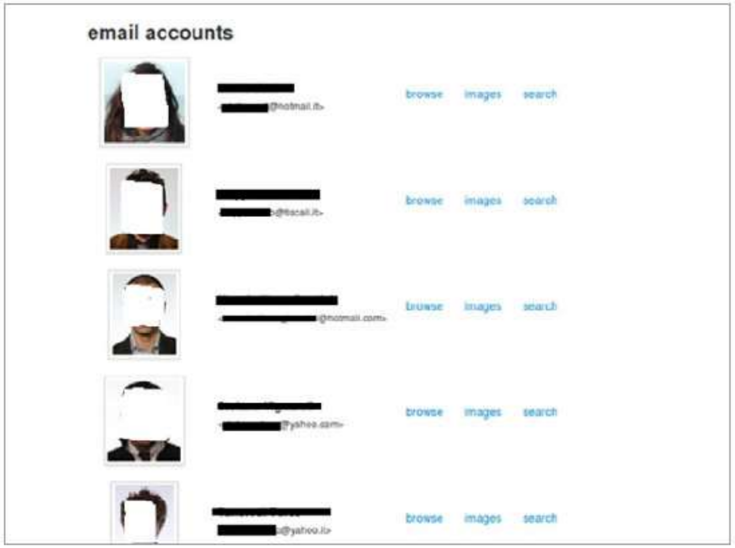
Image source: http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

Items on the Black Market (1)

- On-line accounts
  - E.g. entertainment services/media streaming, loyalty programs
- Identities
  - Personal data, email accounts, medical history



```
sername(s): [redacted]
mails: [redacted]3@hotmail.co.uk, [redacted]zz@gmail.com
irst Name: [redacted]
ast Name: Bright
ender: Male
ate of Birth: [redacted] 1995
ge: 19
kype(s): [redacted]
ity: Norwich, Norfolk
ostal Code: [redacted]
tate/Province: Norwich, Norfolk
ountry: United Kingdom
treet: [redacted]
layStation Network: [redacted]
----------------------------+ Accounts +------------------------------+
ttp://Twitter.com/[redacted]
ttp://Instagram.com/[redacted]
ttp://Twitch.tv/[redacted]
ttp://Youtube.com/user/[redacted]
ttp://Youtube.com/MrBomb3rZz - [redacted]
ttp://Youtube.com/user/[redacted]
ttp://Facebook.com/[redacted]
ttp://Plus.Google.com/[redacted]
ttp://Plus.Google.com/[redacted]
ttp://SteamCommunity.com/profiles/[redacted]
ttp://ConsoleCrunch.org/index.php?members/[redacted]
ttp://NextGenUpdate.com/forums/member[redacted]
ttp://XenForo.com/community/members/[redacted]
----------------------------+ Family +--------------------------------+
other: [redacted]
ttp://Facebook.com/[redacted]
arther: [redacted]
```



email accounts

[redacted]
<[redacted]@hotmail.it>
browse images search

[redacted]
<[redacted]@tiscali.it>
browse images search

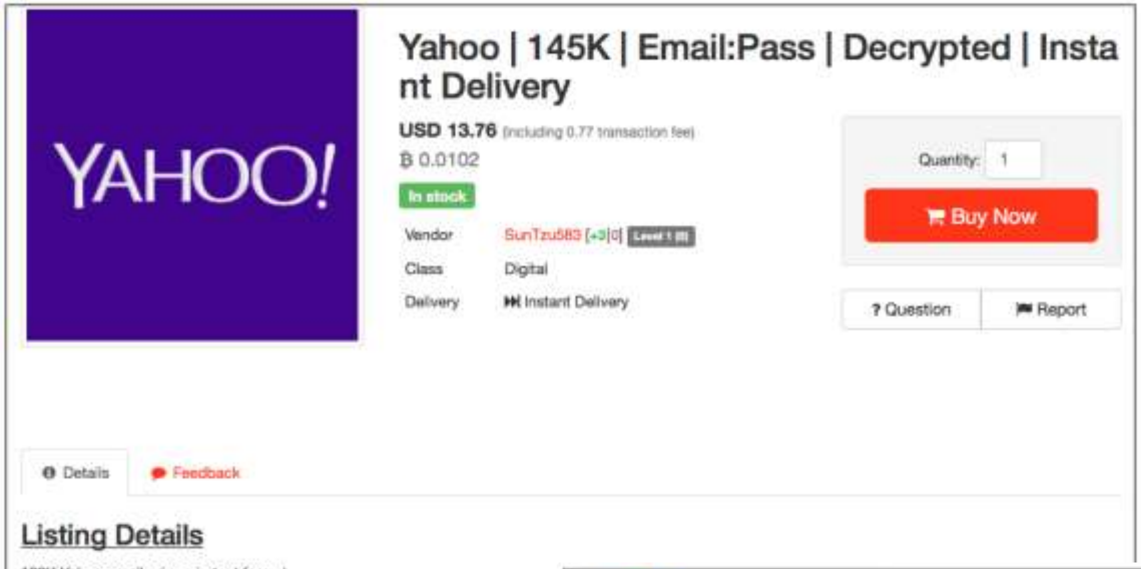
[redacted]
<[redacted]@hotmail.com>
browse images search

[redacted]
<[redacted]@yahoo.com>
browse images search

[redacted]
[redacted]@yahoo.it>
browse images search

Image source: http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf

Items on the Black Market (2)



Yahoo | 145K | Email:Pass | Decrypted | Instant Delivery

USD 13.76 (including 0.77 transaction fee)

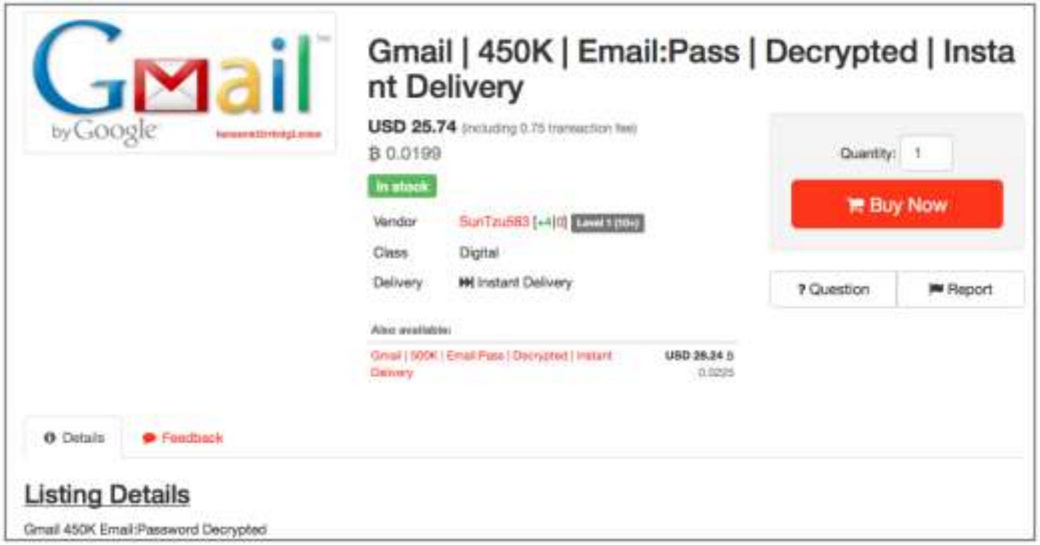
Ƀ 0.0102

In stock

Vendor	SunTzu583 [+3|0] Level 1 (0)
Class	Digital
Delivery	⏭ Instant Delivery

Listing Details

100K Yahoo email:adress in text format.



Gmail | 450K | Email:Pass | Decrypted | Instant Delivery

USD 25.74 (including 0.75 transaction fee)

Ƀ 0.0199

In stock

Vendor	SunTzu583 [+4|0] Level 1 (10+)
Class	Digital
Delivery	⏭ Instant Delivery

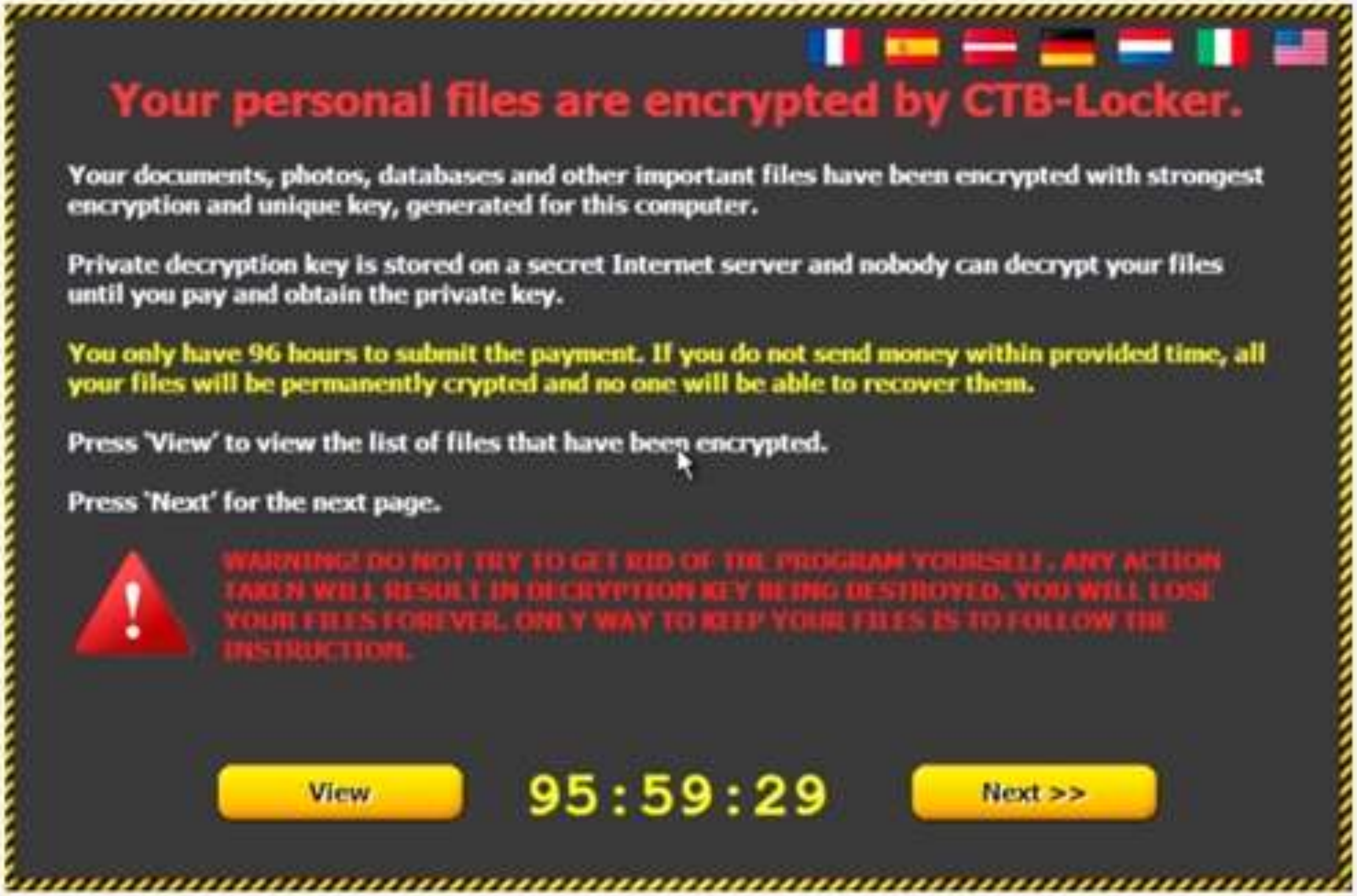
Also available:

Gmail | 500K | Email:Pass | Decrypted | Instant Delivery	USD 28.24 Ƀ 0.0225

Listing Details

Gmail 450K Email:Password Decrypted

Ransomware



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

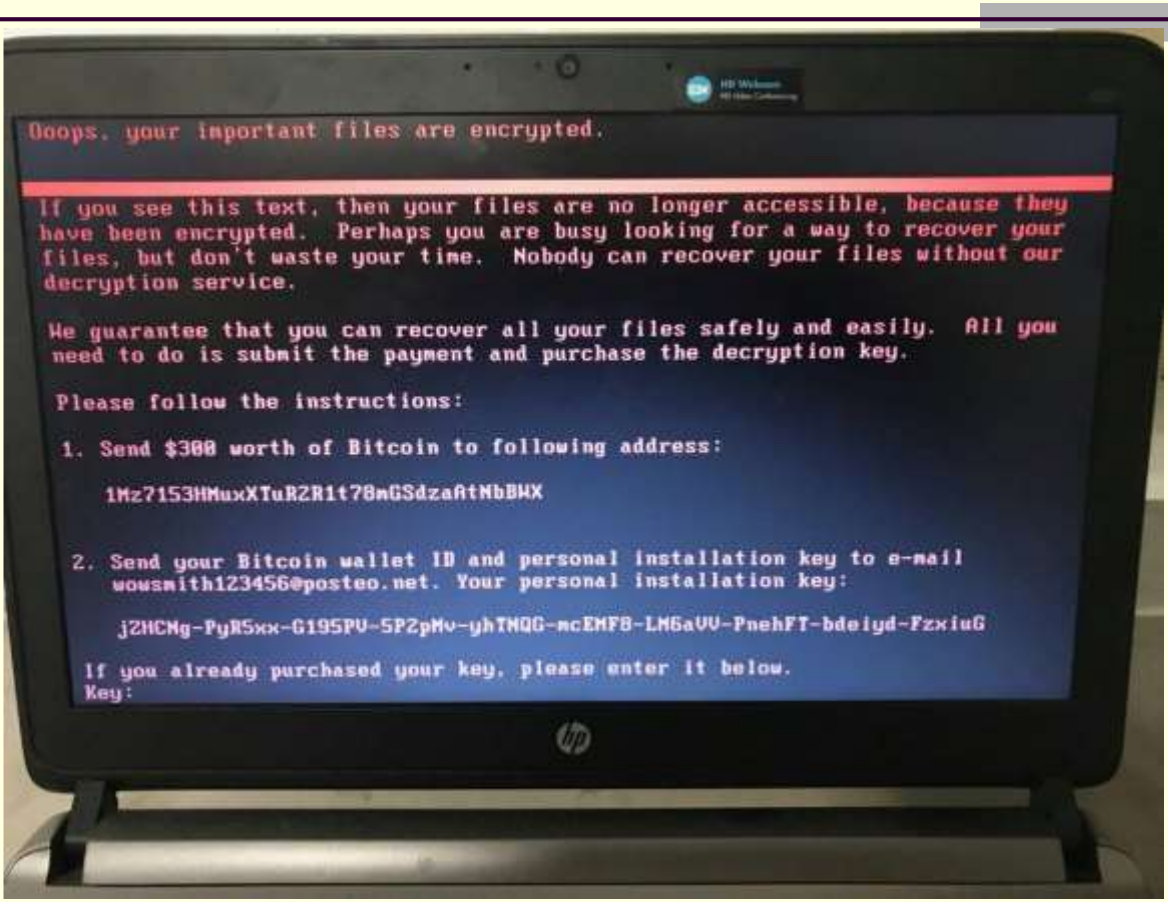
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Ransomware

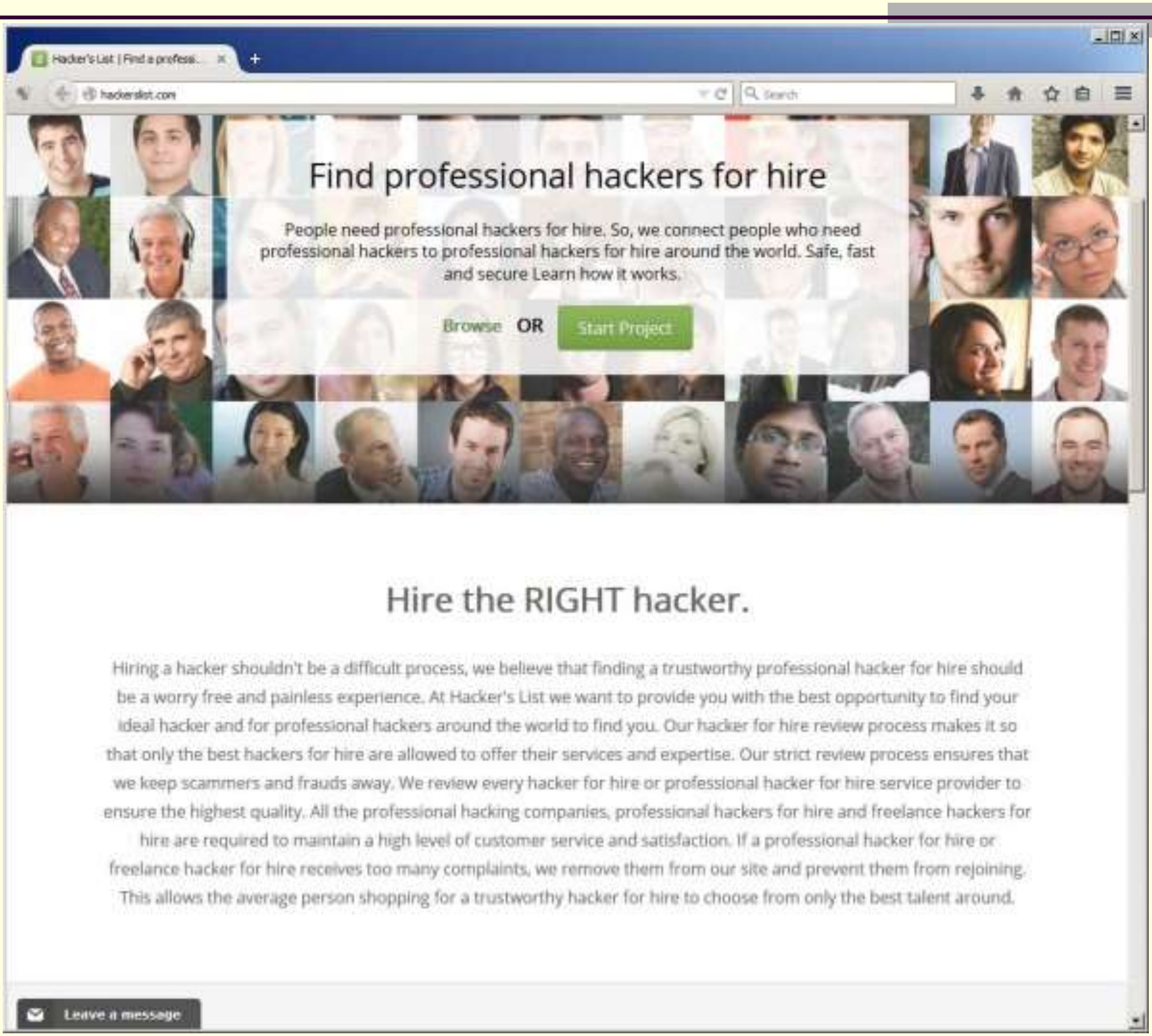


```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   jZHCMg-PyR5xx-G195PV-5P2pMv-yhTNQG-mcEMF8-LM6aVV-PnehFT-bdeiyd-FzxiuG

If you already purchased your key, please enter it below.
Key:
```

Malware can

- overwrite Master Boot Record (MBR)
- encrypt files
- …

The Hacking Business



Find professional hackers for hire

People need professional hackers for hire. So, we connect people who need professional hackers to professional hackers for hire around the world. Safe, fast and secure Learn how it works.

Hire the RIGHT hacker.

Hiring a hacker shouldn't be a difficult process, we believe that finding a trustworthy professional hacker for hire should be a worry free and painless experience. At Hacker's List we want to provide you with the best opportunity to find your ideal hacker and for professional hackers around the world to find you. Our hacker for hire review process makes it so that only the best hackers for hire are allowed to offer their services and expertise. Our strict review process ensures that we keep scammers and frauds away. We review every hacker for hire or professional hacker for hire service provider to ensure the highest quality. All the professional hacking companies, professional hackers for hire and freelance hackers for hire are required to maintain a high level of customer service and satisfaction. If a professional hacker for hire or freelance hacker for hire receives too many complaints, we remove them from our site and prevent them from rejoining. This allows the average person shopping for a trustworthy hacker for hire to choose from only the best talent around.

From the Past: "Blaster" Trojan

- RPC buffer overrun (in RPCSS) – circa 2003:

  (http://support.microsoft.com/kb/824146)

  Vulnerable code:

```
while (*pwszTemp != L’\\’)
    *pwszServerName++ = *pwszTemp++;
```

- ~6m infected computers, 3.37m service calls

  Should have been

```
while ( (*pwszTemp != L'\\') &&
       ((*pwszTemp != L'\0')) &&
       (pwszServerName < end_addr) )
    *pwszServerName++ = *pwszTemp++;
```

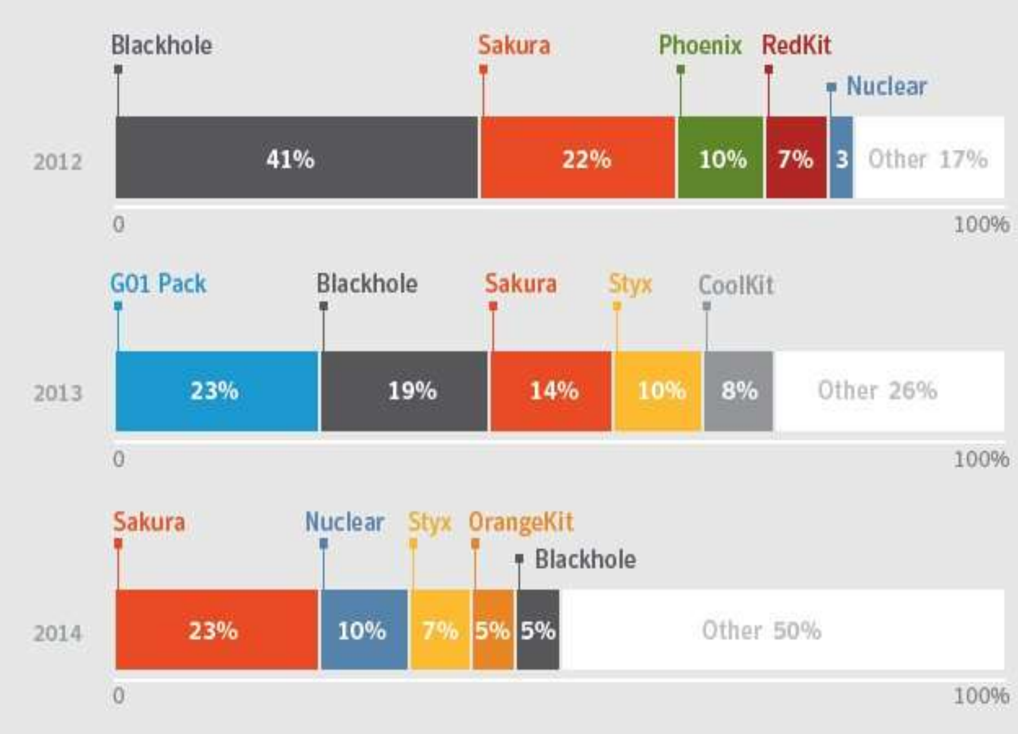
- The Gates memo:
  - "When we face a choice between adding features and resolving security issues, we need to choose security,“
  - "Our products should emphasize security right out of the box."

Recent: Blackhole Exploit Kit

- Malware kits
  - Tools for criminals to create and distribute malware
  - Systems to manage networks of infected machines

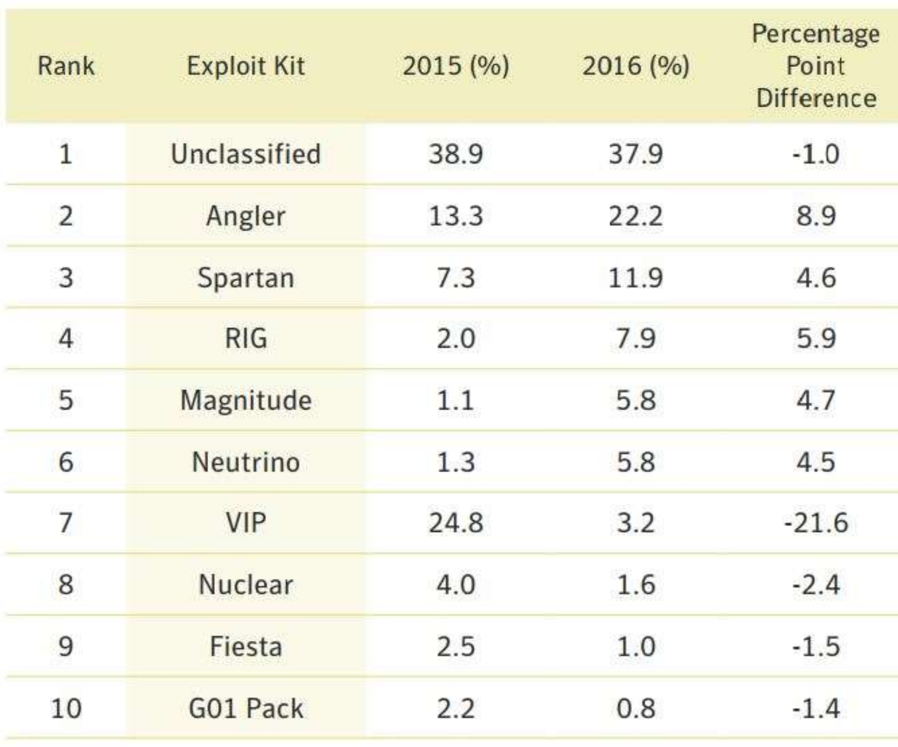
- Blackhole first version in late 2010
  - Spreads via web pages compromised by injected Javascript
  - Targets a variety of vulnerabilities
  - Code obfuscated with commercial tools
    - Consists of encrypted PHP scripts (ionCube)
  - Typical payload: polymorphic malware encrypted with custom tools to evade detection
    - E.g. Zeus, fake AV (scareware), Ransomware
  - Provides management services
    - Configuration options, statistical summary of infections, blacklisting/blocking of IP addresses
  - Autoupdate
  - At the end of 2013, Russian authorities arrested the alleged author of Blackhole

Web Attack Toolkits



Top 5 Web Attack Toolkits, 2012–2014

Source: Symantec



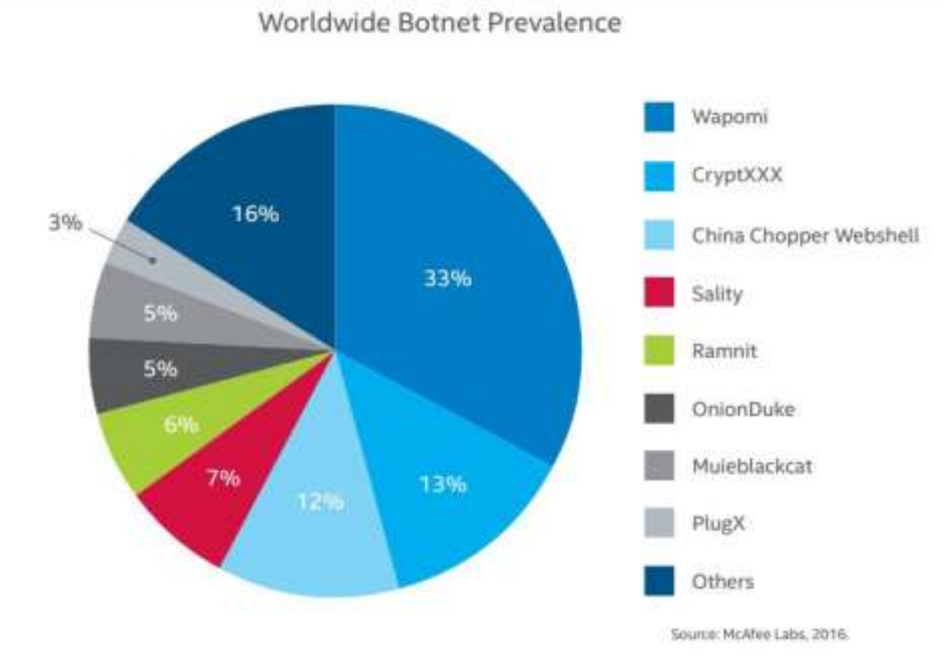
Rank	Exploit Kit	2015 (%)	2016 (%)	Percentage Point Difference
1	Unclassified	38.9	37.9	-1.0
2	Angler	13.3	22.2	8.9
3	Spartan	7.3	11.9	4.6
4	RIG	2.0	7.9	5.9
5	Magnitude	1.1	5.8	4.7
6	Neutrino	1.3	5.8	4.5
7	VIP	24.8	3.2	-21.6
8	Nuclear	4.0	1.6	-2.4
9	Fiesta	2.5	1.0	-1.5
10	G01 Pack	2.2	0.8	-1.4

Image source: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

Cybercrime – Botnets

- Prevalent tool for massive attacks
  - E.g. ransomware-as-a-service

    Bridges: PHP scripts that store client IP addresses, encryption keys, ransom values, verify payment status



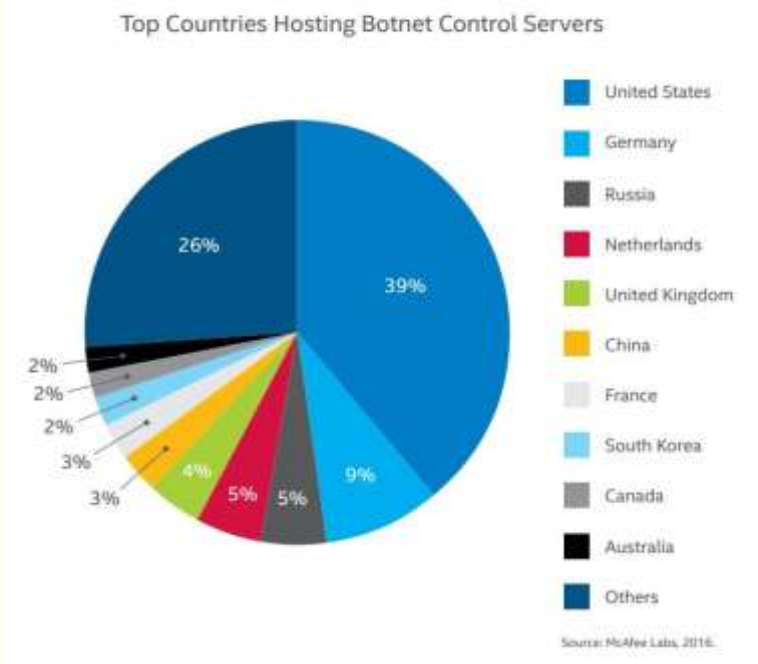


Image source: http://www.mcafee.com/au/resources/reports/rp-quarterly-threats-dec-2016.pdf

Botnet from the Past: Zeus Bot

- Analysed by:
  - Creating dummy customer records and seeding into botnets
  - Fingerprints in HTTP requests / responses …
- Professionally developed: feature-rich, user friendly and scalable
- New features - WebInjects and Jabber IM
- Total pkg can cost $8k. Hardwired protection to keep bot creator’s revenue stream wall-gardened

Zeus Botnet Overview

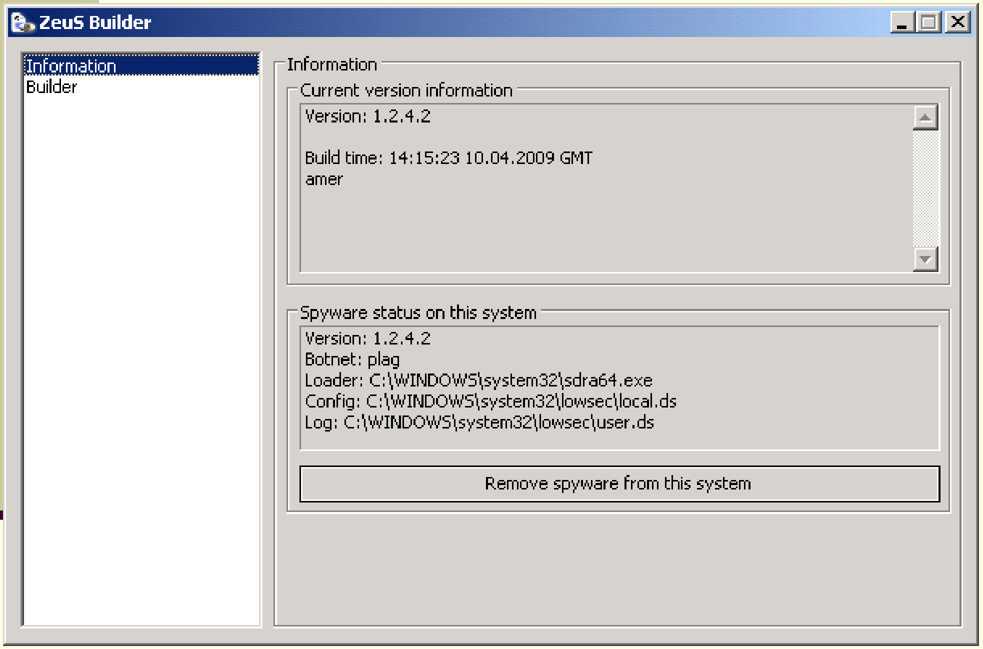
- It is a toolkit
  - There are many Zeus botnets
- Components
  - Distribution

    Via spam (attachment or link)

    Not self-propagating
  - Automatic installation
  - Configuration
    - Static: Sets the basic parameters (owner, URLs for botnet administration, etc)
    - Dynamic: Used for changing the botnet's behaviour

Zeus Botnet Screenshots

Zeus Builder



Information

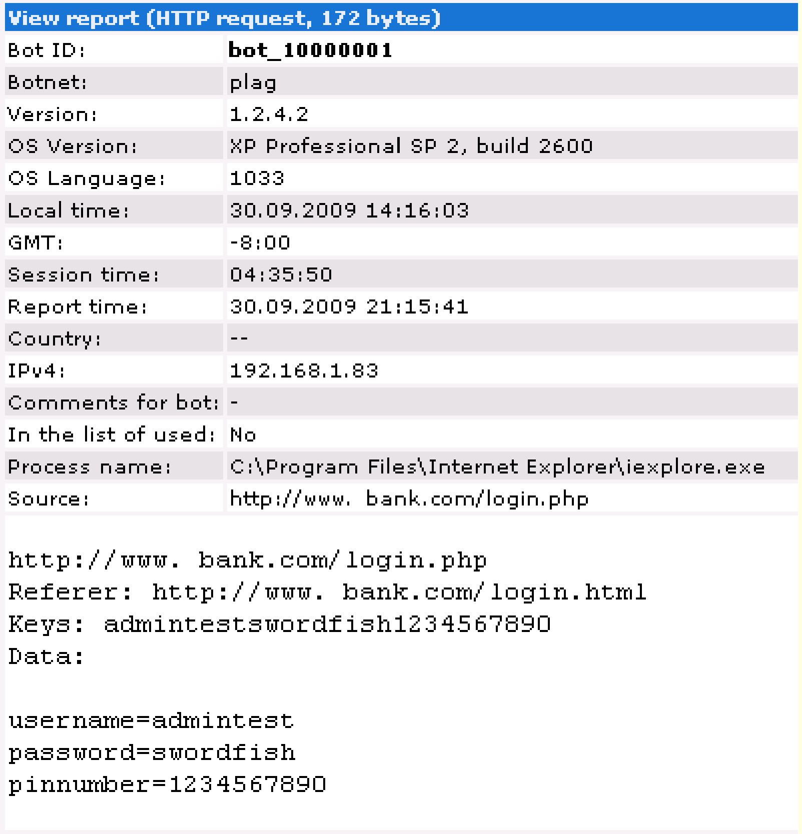
Current version information

```
Version: 1.2.4.2

Build time: 14:15:23 10.04.2009 GMT
amer
```

Spyware status on this system

```
Version: 1.2.4.2
Botnet: plag
Loader: C:\WINDOWS\system32\sdra64.exe
Config: C:\WINDOWS\system32\lowsec\local.ds
Log: C:\WINDOWS\system32\lowsec\user.ds
```

Password capture



View report (HTTP request, 172 bytes)	
Bot ID:	**bot_10000001**
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	30.09.2009 14:16:03
GMT:	-8:00
Session time:	04:35:50
Report time:	30.09.2009 21:15:41
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	http://www. bank.com/login.php

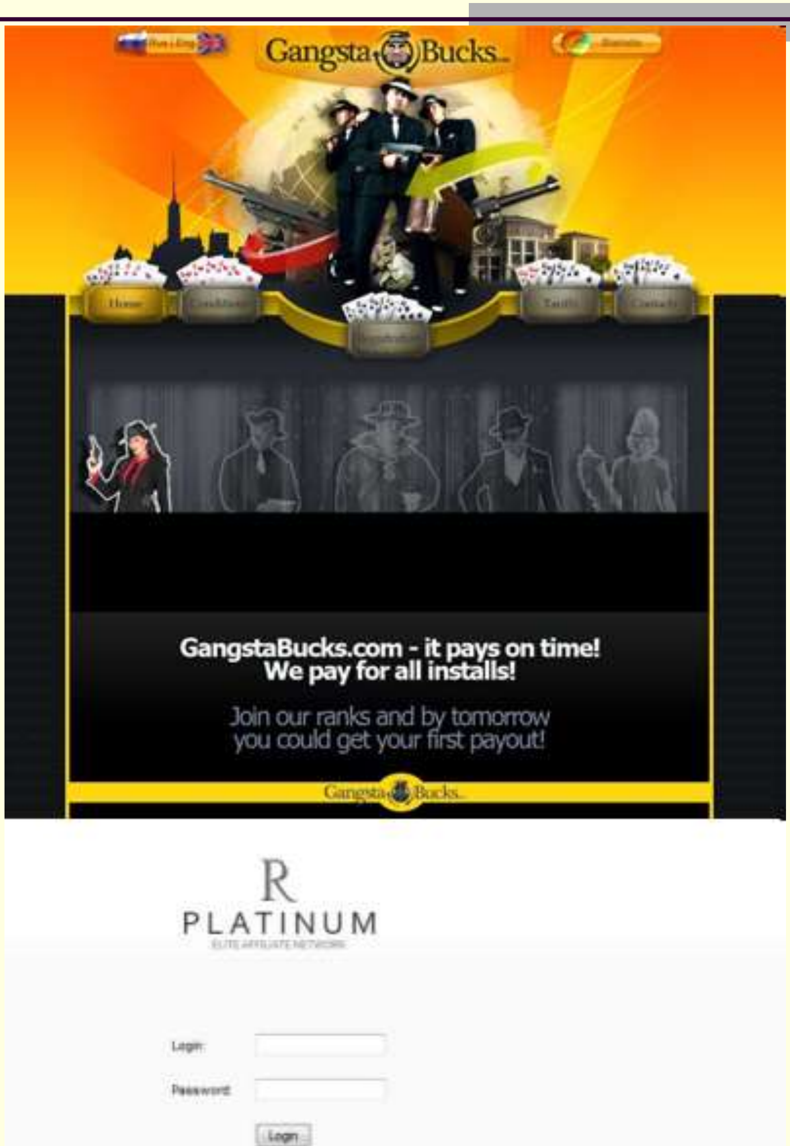
```
http://www. bank.com/login.php
Referer: http://www. bank.com/login.html
Keys: admintestswordfish1234567890
Data:

username=admintest
password=swordfish
pinnumber=1234567890
```

Image source: http://www.fortiguard.com/legacy/analysis/zeusanalysis.html

The Botnet Industry
TDL 4 – The Indestructible Botnet

- Has been evolving since 2008
- Prolific
  - ~4.5 million infected computers (with a rootkit in the Master Boot Record)
  - Affiliates get $20-$200 for every 1000 infections
- Uses sophisticated technology
  - advanced encryption
  - public peer-to-peer network (Kad) for communication
- Launchpad for other malware

  Downloads associated malware and deletes others (e.g. Zeus)



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

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

Login:

Password:

Summary

- Banking has always been an attractive target for criminals
- There are security standards for the payment card industry
- Data protection is
  - strong when data is in transit
  - critical at the endpoints
    - user gullibility
    - payment processing sites are high-yield targets for criminals

Preparing for the Exam

- Read the material and prepare your notes
- Check your knowledge by going through the revision questions
- Write down your answers, writing is different from thinking them through
- Once finished writing, evaluate your answers by using the lecture/tute/lab notes

Expectations at the Exam

You should be able to

- Explain basic security related terms
- Describe the basics of most common attack methods
  - Their aims
  - The way they work
- Explain key security concepts
- Explain basic security mechanisms
  - What they protect
  - The principle of operation
  - Their components (where applicable)
- Analyse and evaluate a system from the security perspective
- Apply your security knowledge to simple scenarios

After the Exam