Computer security threats, vulnerabilities and attacks

Antonio Pérez Pérez
(CERN Computer Security Team)

CERN Security Lectures, May 23th 2012

OVERVIEW

- **Threats**
  - Overview of the major threats
- **Vulnerabilities**
  - Examples of different types of vulnerabilities
- **Motivations**
  - Examples of what do attackers go after
- **Attacks/Incidents**
  - Examples of major attacks and what we can learn from them

Attackers’ toolbox…

MAJOR THREATS

Stolen credentials

- One of the biggest threats
- Serves as entry point for other attacks
- PEBKAC: Good security practices are required
  - Use strong (and different) passwords
  - Change passwords periodically
  - Do not introduce passwords where not sure if legitimate
  - For extra security: use multi-factor authentication methods

Malware/Virus/Worms

- Common on Windows systems (affecting other platforms depending on their popularity)
- Infected PCs become zombies
- Zombies are included into a malicious network (botnet)
  - Triggered by the attacker to perform automated tasks
- Recent examples:
  - MAC – Flashback
  - Windows – win32.Ramnit

THE WORLD'S ONLY RELIABLE NEWSPAPER

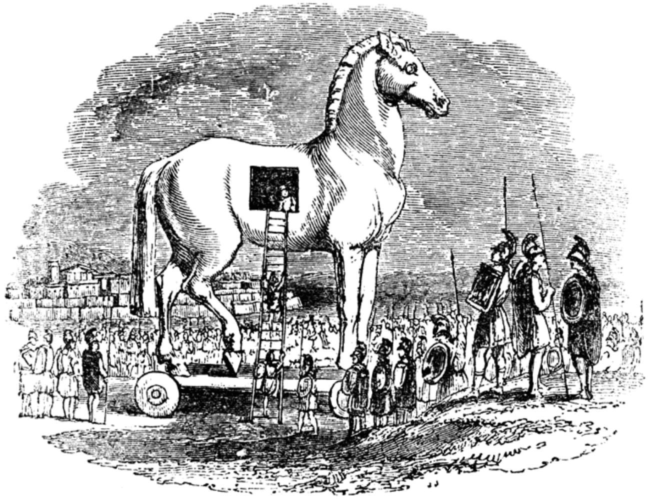
COMPUTER VIRUS SPREADS TO HUMANS!

BAR GLASSES HELP YOU SEE STRAIGHT WHEN YOU'RE DRUNK!

Rootkits/Trojans

- **Software that uses different techniques in order to open (and hide) a backdoor in a host/service**
  - May behave as malware

- **Commonly used for (major) targeted attacks**
  - Very sophisticated
  - Maintain access to the compromised hosts



Phishing/Spam

► Email that "behaves" as legitimate

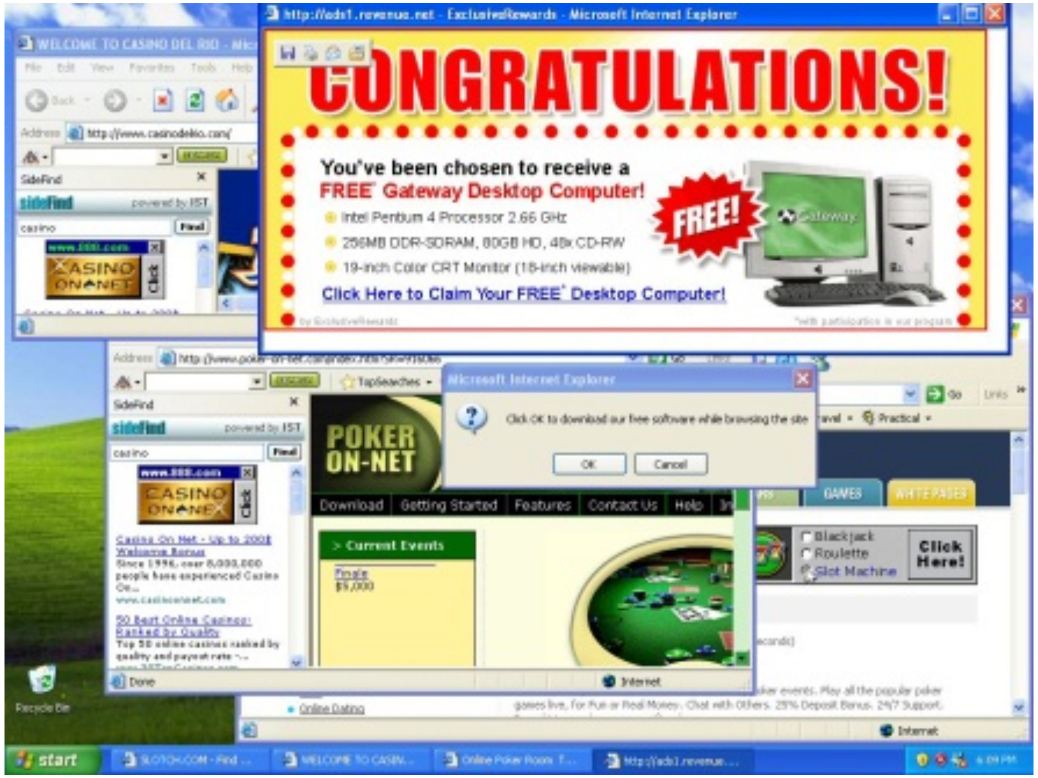
- ► **Spam**: usually refers to non-legitimate business offers
- ► **Phishing**: requires some action by the user to trigger a malicious behavior
  - Malicious URLs
  - Review credentials
  - Forms
  - Malicious attachments

Social Engineering

- ► Uses social skills to trick the victim(s)
- ► Always “effective”: no antivirus available for humans
- ► Commonly used for targeted attacks

Spyware/Adware

- ► Malicious software used to track user behaviour for non-ethical businesses plans
- ► Usually packaged with (free) applications



CONGRATULATIONS!

You've been chosen to receive a FREE Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

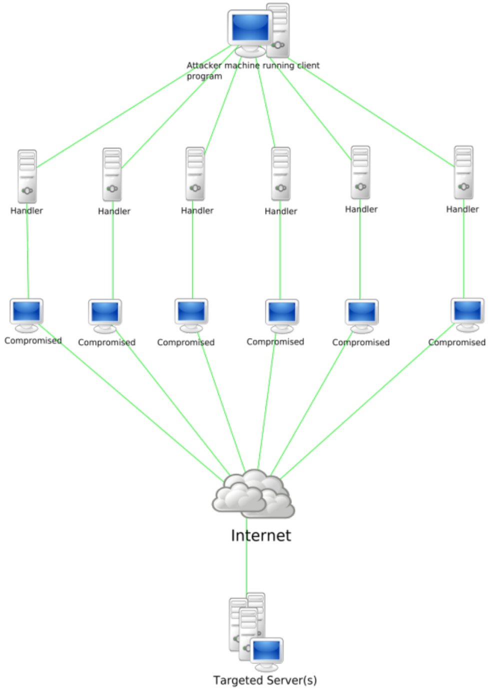
Click Here to Claim Your FREE Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

DOS/DDOS

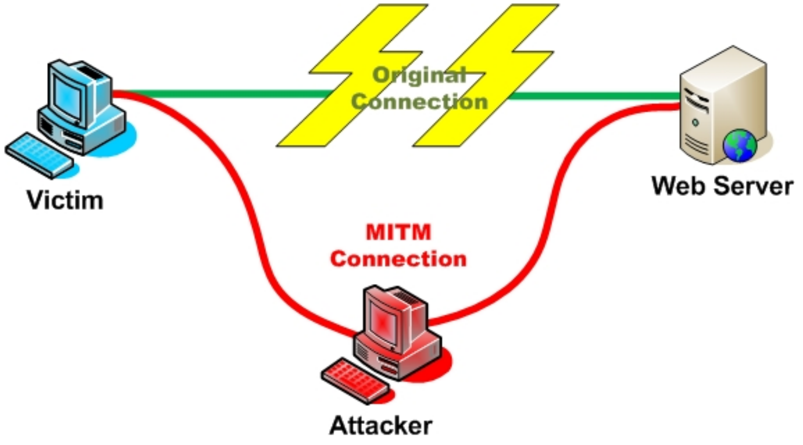
- (Distributed) Denial Of Service
- Used to disturb online (public) services
- Triggered on zombie PCs or through driven-by software
  - LOIC (Low Orbit Ion Cannon) software used by Anonymous



Rogue SSL certificates

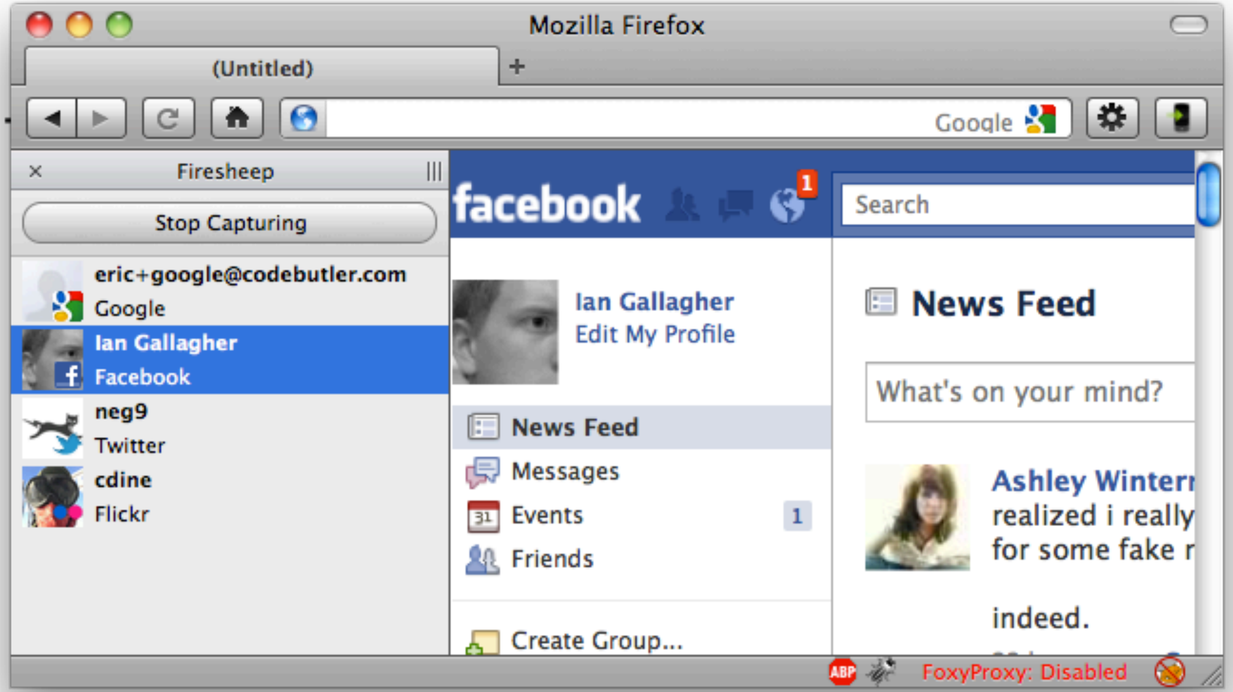
► Also known by "the DigiNotar scandal"

- ► Attackers issued false certificates by breaking into the systems of certification authority DigiNotar in the Netherlands
  - Other Certification Authorities (claimed as) hacked
    - Comodo CA
    - *GlobalSign, StartCom CA*
- ► Issued rogue *google.com* SSL certificate
- ► Targeted to spy on Iranian citizens (gmail traffic)
- ► Uses Man-In-The-Middle attacks to snoop on users traffic



Data sniffing

- ► May happen when using unsecured channels or protocols (no SSL!)
- ► Open WIFIs!


Mozilla Firefox

(Untitled)

Google

Firesheep

Stop Capturing

eric+google@codebutler.com
Google

Ian Gallagher
Facebook

neg9
Twitter

cdine
Flickr

facebook

Search

Ian Gallagher
Edit My Profile

News Feed

Messages

Events 1

Friends

Create Group...

News Feed

What's on your mind?

Ashley Winterr
realized i really
for some fake r

indeed.

FoxyProxy: Disabled

Web exploiting

▶ SQL injection

- ▶ Attack that uses non-sanitized/non-validated parameters to inject/ modify SQL queries
  - ▪ Direct access to the database

▶ XSS

- ▶ Attack that uses non-sanitized/non-validated parameters to inject html/ javascript code
  - ▪ Used to steal session cookies, elevate access-privileges or access any other information in behalf of the victim

It's just not about the threats. Some examples…

VULNERABILITIES

Operating Systems

Windows

- (CVE-2012-0002) RDP remote exploit
  - *The vulnerable RDP implementation does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending a sequence of specially crafted RDP packets to Port 3389/TCP*

Linux

- (CVE-2012-0056) Linux Local Privilege Escalation via SUID /proc/pid/mem Write
  - *The mem_write function in Linux kernel 2.6.39 and other versions, when ASLR is disabled, does not properly check permissions when writing to /proc/<pid>/mem, which allows local users to gain privileges by modifying process memory, as demonstrated by Mempodipper.*
- Bypass screensaver/locker program on Xorg 1.11 and up

MacOS

- Mac Lion update leaves passwords on clear text logs

Third-party software

► (CVE-2012-2329) PHP-cgi remote code execution vulnerability

- ► *The attackers are first sending a malicious query that includes the "-s" php-cgi flag to test if the targeted websites are vulnerable and then install a backdoor through a query with the "-d" flag*
  - http://facebook.com/?-s (was a fake page pointing to a security related job)

► (CVE-2012-1675) Oracle TNS Listener Poison attack

- ► *A remote user can exploit this vulnerability to impact the confidentiality, integrity and availability of systems that do not have recommended solution applied*

► Github

- ► *GitHub hacked, millions of projects at risk of being modified or deleted*

Or… what do attackers go after?

MOTIVATIONS

Reputation/Popularity

- ► **CMS website defacing**
  - ► … or how a misconfigured web service and an easy “exploiting” can lead to very bad publicity
- ► **Tink0de**
  - ► … or the need to claim that you have hacked many important organizations

Computing power and resources

- ## Bitcoin
  - … or how attackers can turn our servers into *ATMs*
  - Not really an incident, but used for stealing resources (using data centres and botnets)
  - In this case, computing power = money

- ## VoIP cracking
  - … or how attackers can use our resources to attack other sites

- ## DRFTPD
  - … or how grid infrastructure can be turned into a warez hosting

(Sensitive) data

- **Stuxnet**
  - … or how targeted attacks can go wild
  - Infected devices are just not “normal” devices
  - Attackers after nuclear research programs (governments?)

- **Credentials and other sensitive data found on google!**
  - … or why my data has been indexed by google (or other search engines)

Money

Hi,

I'm contacting you because I've found some vulnerabilities on cern.ch system.

I didn't get access to the databases it was a different attack. Was XSS. I hacked cern.ch with a xss attack .

Would like know if you're able to make a deal with me then I can send you all details, the link and also the string.

If you do not believe I can take a screenshot of the xss alert to prove it. How ever, first I'd like know if cern can reward me.

I'm waiting your reply ASAP,

Kind Regards!

Mix it all up!

INCIDENTS

These incidents are based on facts. Any similarity with fictitious events or characters was purely coincidental.

INCIDENTS: OVERVIEW

► PlayStation Network

- ► One of the largest data security breaches in history
- ► Big impact on the media
- ► Example of how to deal (or not) with users

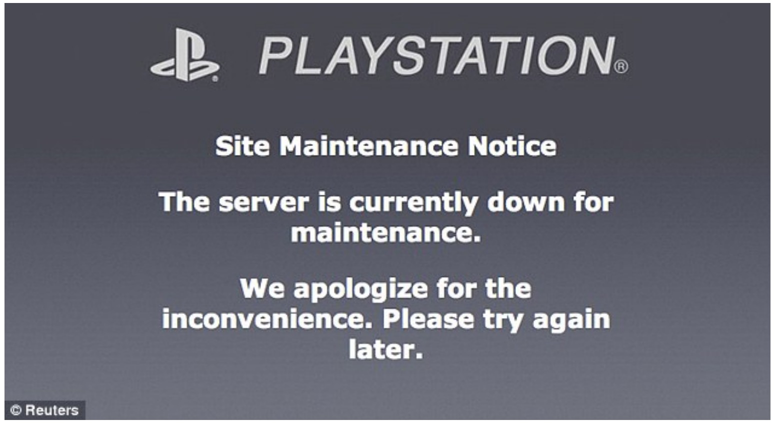
► HBGary Federal

- ► Security firm messing with the hacker community (Anonymous) gets backfired
- ► Several examples of bad practice
- ► Big exposure on the media

PlayStation Network

► Some context:

- ► Geohot bypasses the PS3 OtherOS' Hypervisor
- ► Sony removes OtherOS feature on the PS3
- ► PS3 security fail exposed by Fail0verflow
- ► PS3 jailbroken by geohot
- ► Sony persecutes geohot
- ► Sony attacked by DDOS (by Anonymous)
- ► April 2011:



Site Maintenance Notice

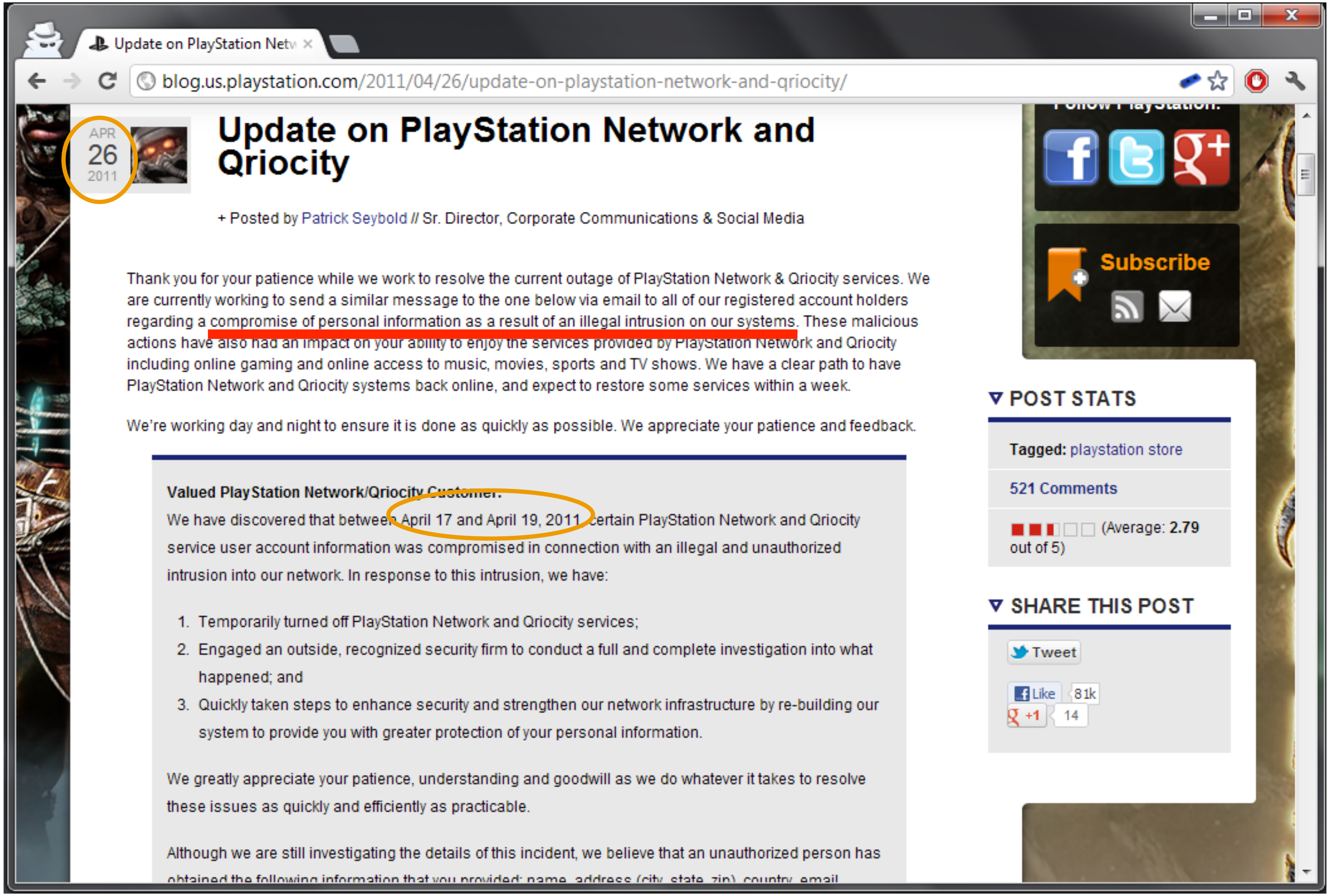
The server is currently down for maintenance.

We apologize for the inconvenience. Please try again later.

© Reuters

- ► "Just" a DDOS?

PSN: Officially acknowledged


Update on PlayStation Netw
blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/
APR
26
2011
Subscribe

Update on PlayStation Network and Qriocity

+ Posted by Patrick Seybold // Sr. Director, Corporate Communications & Social Media

Thank you for your patience while we work to resolve the current outage of PlayStation Network & Qriocity services. We are currently working to send a similar message to the one below via email to all of our registered account holders regarding a compromise of personal information as a result of an illegal intrusion on our systems. These malicious actions have also had an impact on your ability to enjoy the services provided by PlayStation Network and Qriocity including online gaming and online access to music, movies, sports and TV shows. We have a clear path to have PlayStation Network and Qriocity systems back online, and expect to restore some services within a week.

We're working day and night to ensure it is done as quickly as possible. We appreciate your patience and feedback.

Valued PlayStation Network/Qriocity Customer:

We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network. In response to this intrusion, we have:

1. Temporarily turned off PlayStation Network and Qriocity services;
2. Engaged an outside, recognized security firm to conduct a full and complete investigation into what happened; and
3. Quickly taken steps to enhance security and strengthen our network infrastructure by re-building our system to provide you with greater protection of your personal information.

We greatly appreciate your patience, understanding and goodwill as we do whatever it takes to resolve these issues as quickly and efficiently as practicable.

Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email

Follow PlayStation:

POST STATS

Tagged: playstation store

521 Comments

🟥🟥🟥□□ (Average: **2.79** out of 5)

SHARE THIS POST

Tweet

Like 81k

+1 14

PSN: What happened?

- ► **After 7 days of outage, Sony announces that the downtime was due to a massive hack**

- ► **All PSN users exposed**
  - ► personal data (names, birthdays, email addresses)
  - ► passwords (stored in plaintext)
  - ► security questions
  - ► and maybe* credit card details

77 million accounts

PSN: How did they get there?

- **SQL injection?**
  - It was used on many of the previous attacks from Anonymous

- **Hacked firmware for the PS3?**
  - Switched the console into a special developer mode
  - Gives trusted access to the private developer network
  - Ability to fake credit card details

PSN: Closure

- **Beginning May 2011, Sony restores the PSN**
  - Offered a “Welcome back” pack (2 downloadable games)
  - Changed the Terms of Service
    - Inability of suing Sony over any future security breaches

- **Huge negative impact on the media**
- **Sony stated that the costs of the outage were $171 million**

PSN: What we can learn

- ► To not trust our security on the idea of an unbreakable setup/system
- ► To quickly communicate users about sensitive data exposures
- ► Outages/hacks costs money… and (very) bad publicity

- ► No matter how big is an infrastructure: it can be hacked

HBGary Federal

► Some context:

- ► Chief executive of the security firm HBGary Federal, announces that his firm has successfully infiltrated the Anonymous group

- ► HBGary Federal website hacked by Anonymous members
- ► Corporate e-mails and sensitive data exposed
- ► Phone system taken down
- ► CEO’s twitter account hacked

HBGary: What happened?

- **Website (powered by a Content Management System) compromised by SQL injection**
  - Gained access to the user table on the database (usernames, e-mail addresses, passwords)
    - Passwords hashed with MD5
- **Cracked (weak) MD5 passwords using Rainbow Tables**
- **Same passwords also used on other services**
  - Linux box with ssh access
  - CEO’s email (and administrator rights), Twitter and LinkedIn

HBGary: What happened next?

- **Linux box hacked (exploiting a known vulnerability)**
  - Research, backups and sensitive data exposed
- **CEO’s Google Apps administrator password**
  - Access to his email
  - Reset other mailboxes passwords
- **Resetting one of the user passwords, played some social engineering**

HBGary: Social Engineering

Subject: Need ssh into server

yup im logged in thanks ill email you in a few, im backed up

thanks

HBGary: Summarizing

- **Gained root access to another server (rootkit.com)**
  - Got the user database with passwords and emails
  - Cracked the weak MD5 passwords

- **Analysis of the passwords leaked from rootkit.com shows that password re-use is extremely widespread**
  - ~30% of users re-using their passwords

- **As a security firm, they (supposedly) knew about best practices**
  - They just didn't use them

HBGary: What we can learn

- ► To always use standard and good security practices
- ► To not reuse passwords
- ► To not handle over user credentials by email or other unsecure/untrusted channels
- ► To maintain our systems updated
- ► To sanitize inputs and protect from SQL injections

- ► To not mess with people with (almost) infinite time and resources/manpower

CONCLUSIONS

Good practice/Recommendations

- **Apply common sense:**
  - Keep your software updated
    - Keep your antivirus and malware detection software up-to-date
  - Do not reuse passwords
  - Use strong passwords
  - In case of developing software, sanitize inputs
  - Do not run unnecessary services

- **DO NOT TRUST THE INTERNET!**

Using CERN standards

- **Follow CERN procedures and recommendations**
  - They are there for a reason
  - It will make our lives much easier in case of an incident

- **Report strange behaviours**

- **In case of doubt, feel free to ask us ☺**

Computer.Security@cern.ch

THANKS FOR COMING!

QUESTIONS?