IBM Security
Intelligence. Integration. Expertise.

IBM

Real stories from real security incidents, security testing, and things that go bump in the net…

Martin Overton
ERS Team Lead, Security Consultant, Ethical Hacker, Malware Specialist, Forensics, etc.
IBM ERS, CSAR

Background

- Sun Alliance / Royal and SunAlliance
  - Joined 1988
  - Commissioning PCs, Strategy (hardware and software)
  - Responsible for Malware Research/Prevention (10 years)
  - Ethical Hacker (2.5 years)
  - Helped set up Independent ISS UK User Group
  - WildList reporter, Charter member of AVIEN
- Outsourced April 2002
  - Joined EMEA IGS Security June 2002 as Malware/Anti-Malware SME
  - Moved to MSSD (EMEA) June 2004 to set up EMEA Virus CERT
  - Member of Global Virus CERT
  - Moved to ISS X-Force Professional Security Services April 2008
  - Also doing ethical hacking, computer forensics and application assessments as well as malware related work.
  - Currently ERS Team Lead for IBM EMEA
- 27+ Years of knowledge on malware and related security threats.

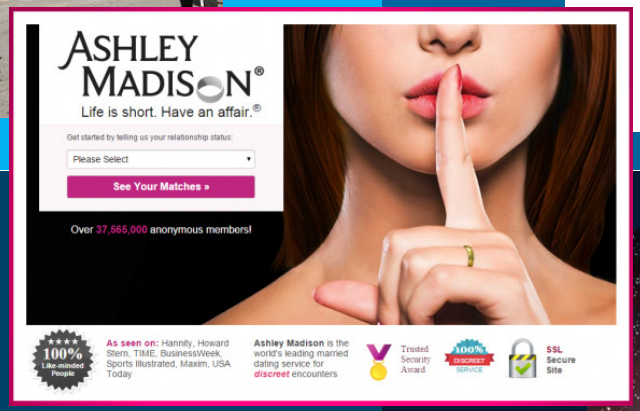
What Managing Security is Like in MOST Organisations….

SECURITY IS A BOARDROOM DISCUSSION

CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Increasingly, companies are appointing CROs and CISOs with a direct line to the Audit Committee

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

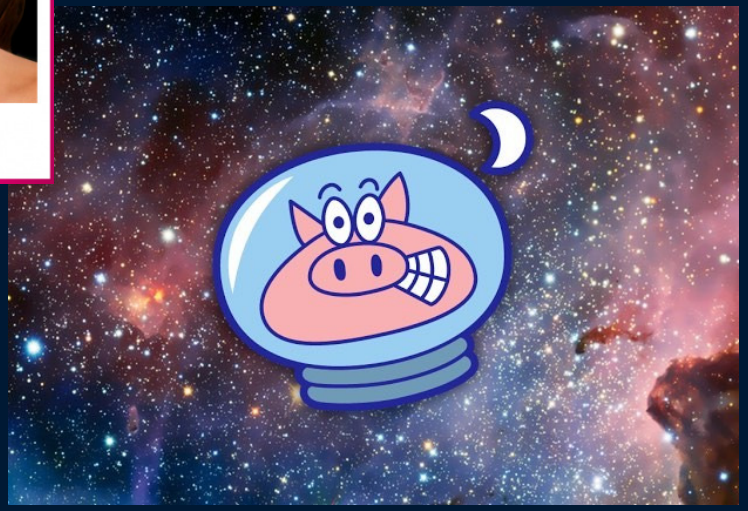


mumsnet

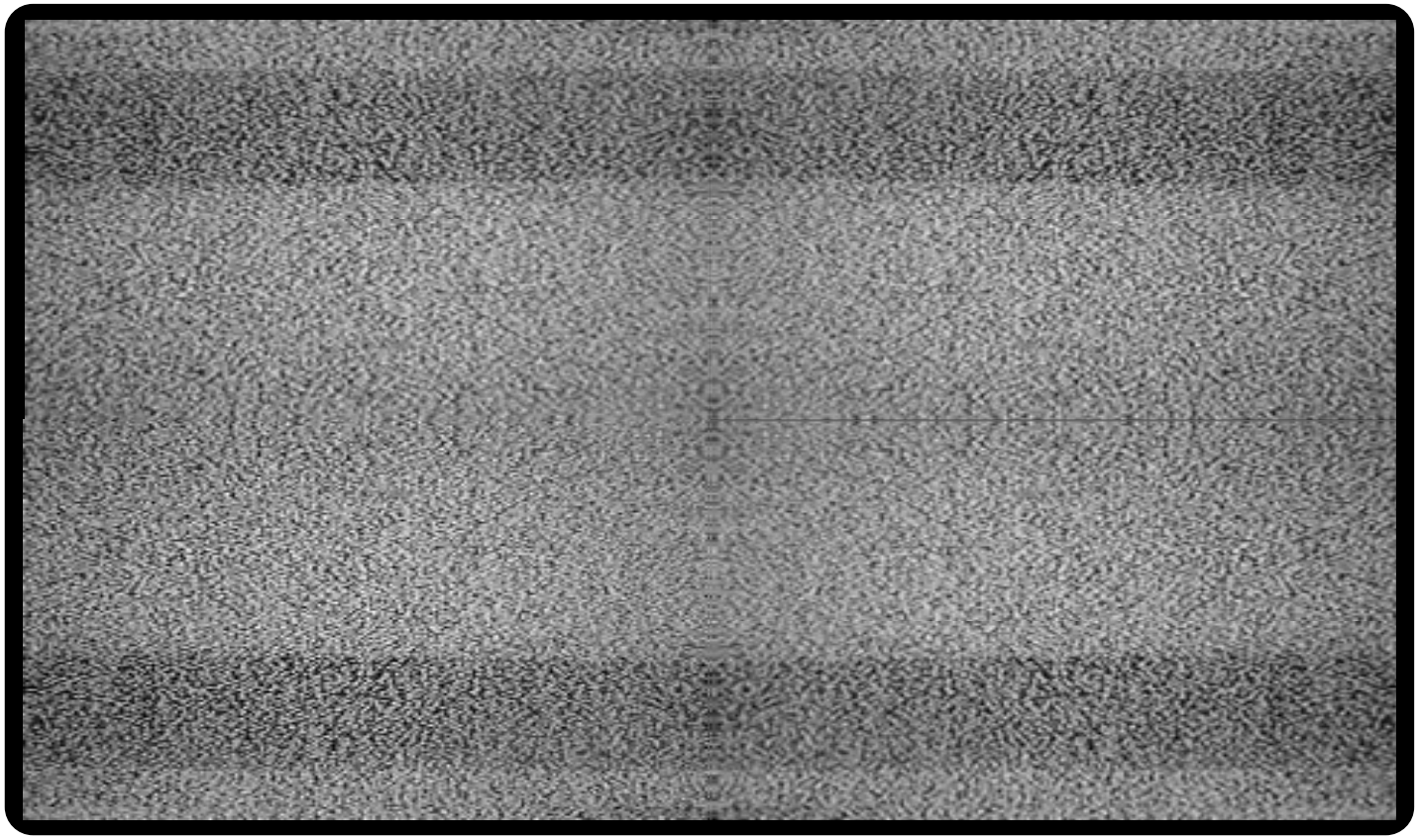
TARGET

HackingTeam

— WALL STREET JOURNAL



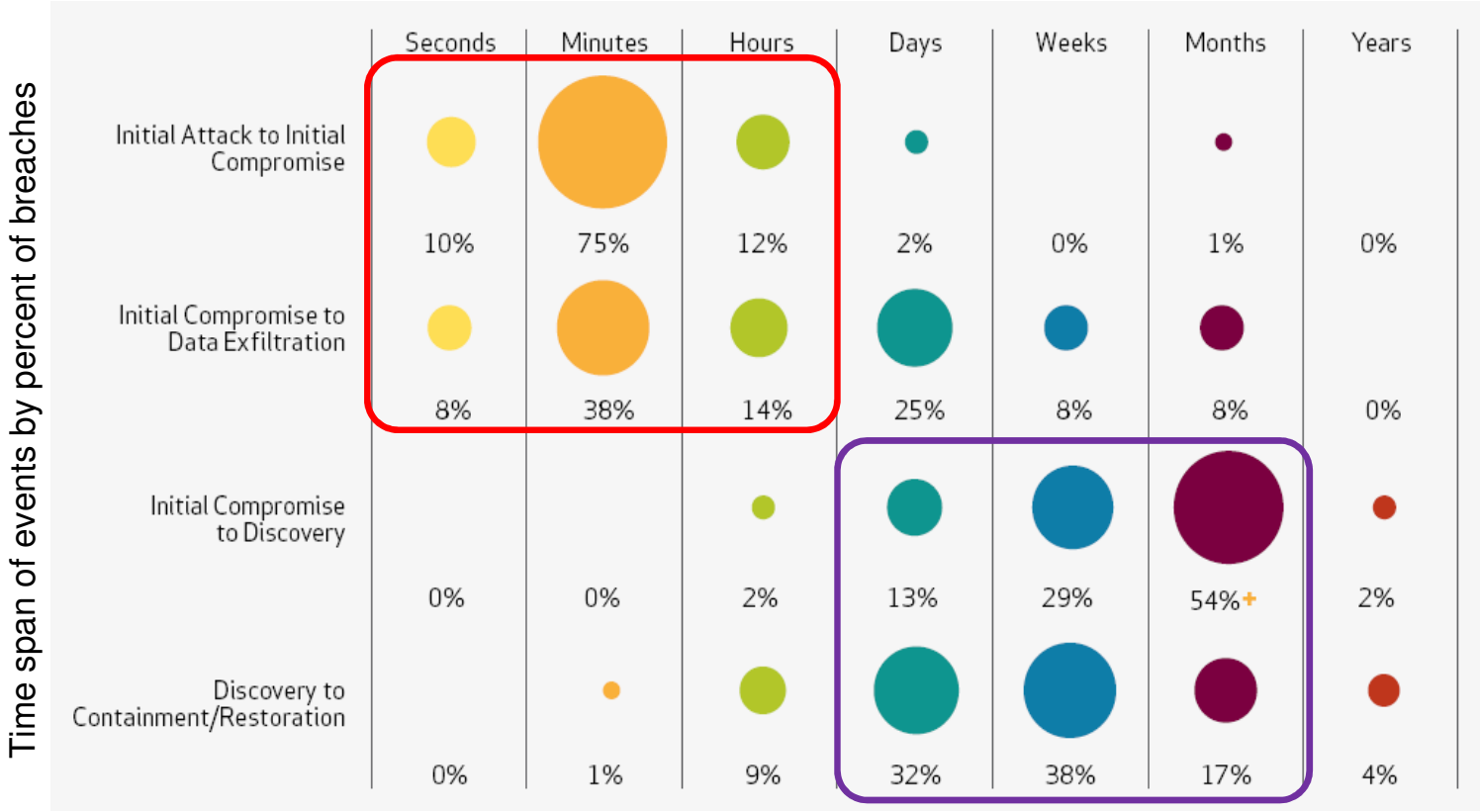
Typical company security team sees noise…



If they monitor and log at all…

Early detection and **rapid response** are the best defense against rising cyber threats and sophisticated attacks

Compromises take days or more to discover in 96% of cases; and over 91% weeks or more to contain



http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z038

Harsh realities for many enterprise network CISOs

Attackers spend an estimated **243 days on a victim's network** before being discovered

In 2013, it took organizations **32 days** on average **to resolve a cyber-attack**

In 2012, **38%** of targets were **attacked again** once the original incident was remediated.

Up to 85% of attack targets only discover compromise **when warned by 'Third Parties'**

An Overview of the changes… So many ways in…

Crumbling Logical and Physical Perimeter

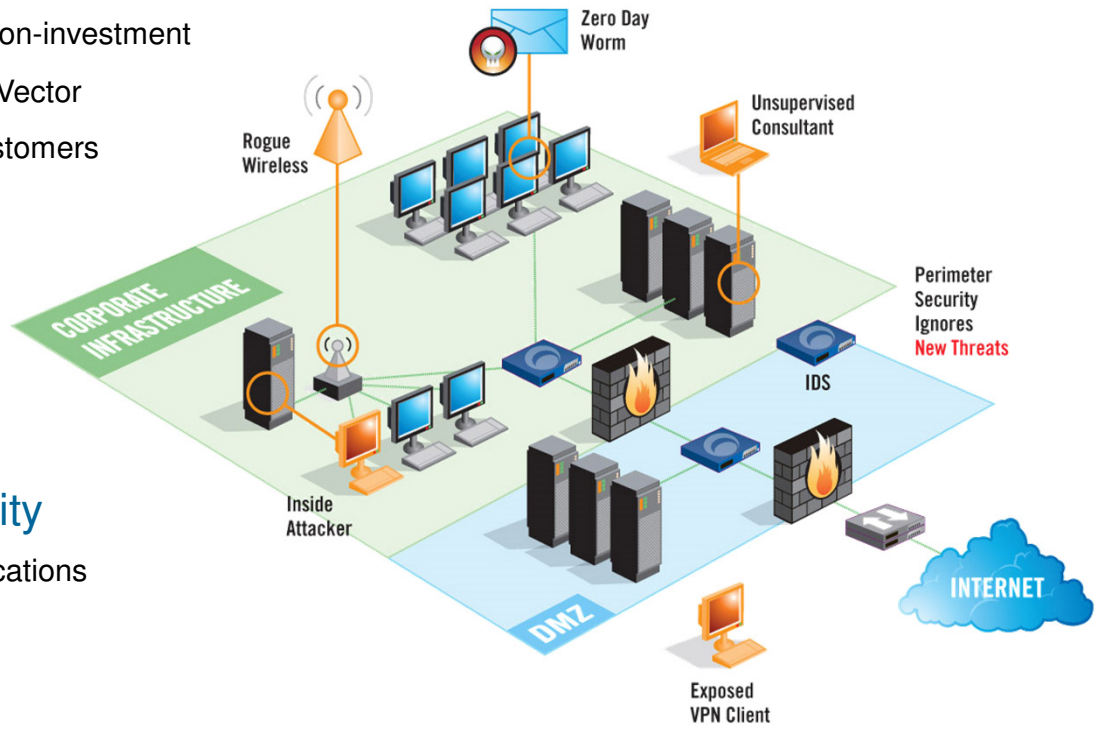
- Legacy business model non-investment
- VPNs, Wireless, Walk-In Vector
- Contractors, partners, customers

Evolving Threats

- Automated attacks, zero-day worms
- Organized Cyber Crime

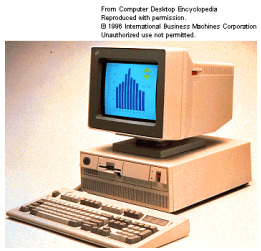
Operational Complexity

- New business, new applications
- Mergers and acquisitions



My, How Times Have Changed!

- **1980's - 2004**
  - Hackers were the good guys and the bad guys were called Crackers…
  - Most malware authors created malware for the challenge, peer acclaim, etc.
  - Most attacks (malware or hacks) were very 'noisy' and obvious…PC malware started in 1986!
  - Most malware and hacking tools written by "amateurs" and "hobbyists" (mainly teenage boys)
  - Mainly simple attacks, easily identified an blocked…
  - Defences were mainly perimeter based…

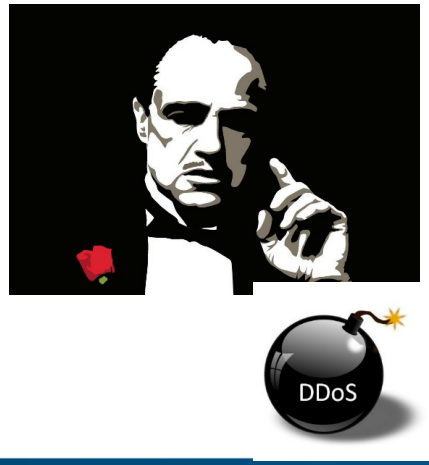


My, How Times Have Changed!

- **2005 - 2010**
  - Cyber-crime starts to take over…the bad guys are called hackers…
    Malware and hacking tools start to be written by professional programmers…by contract
  - Botnets are the main tool of choice for attacks and remote control of zombie armies (mainly PCs)
  - Increase in sophistication and complexity…
  - The perimeter defence model is dead! End-point protection is the new king…

My, How Times Have Changed!

- **2011 - Today…**
  - Cyber-crime is king…real criminal gangs heavily involved (and also nation states)
  - Botnets and Backdoors are the main weapons, often served up by Phishing attacks…
  - Hacktivists are a major pain…
  - DDoS attacks are a key disruption tool and often used as a smokescreen (diversion)
  - It is all about the money; stealing data, services and bandwidth…
  - APT is the latest buzzword, but it is nothing new!
  - Very sophisticated…
  - Defences today need to be data-centric; focus on protecting your “Crown Jewels”…



Top Reasons WHY Compromises Occur

end users/endpoints

Double-clicking "on anything"
Disabling endpoint security settings
Using vulnerable, legacy software and hardware
Failing to install security patches
Failing to install anti-virus
Failing to report lost/stolen device
Connecting endpoint to a network from an insecure access point (i.e., Starbucks)
Using a second access point (i.e., AirCard) creating a bypass
Using weak/default passwords and/or using business passwords for personal use
Giving passwords over the phone
Opening PDFs, Office Documents, etc.

80-90% of all security incidents can be easily avoided!

infrastructure

Connecting systems/virtual images to the Internet before hardening them

Connecting test systems to the Internet with default accounts/passwords

Failing to update or patch systems/applications on a timely basis.

Failing to implement or update virus detection software

Using legacy/EOLed software and hardware

Running unnecessary services

Using insecure back end management software

Failing to remove old or unused accounts end user accounts.

Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing.

Failing to segment network and/or adequately monitor/block malicious traffic with IDS/IPS

VIRUSES AND OTHER MALWARE

History, Why it IS Important!

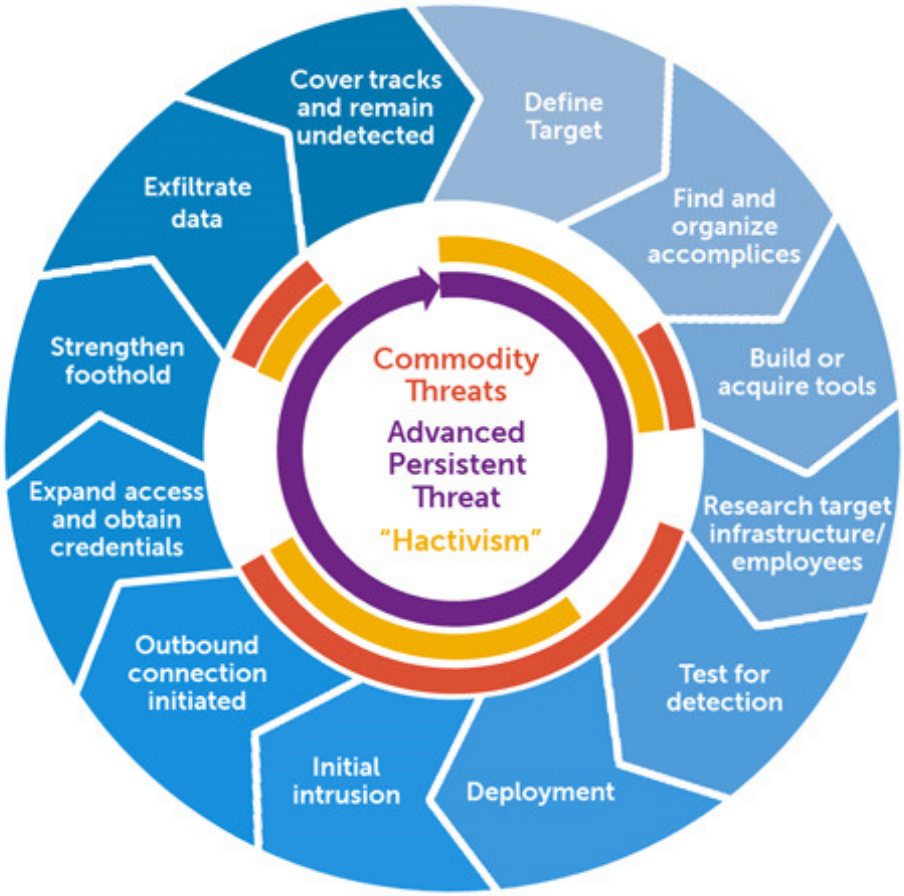
Definition - APT:

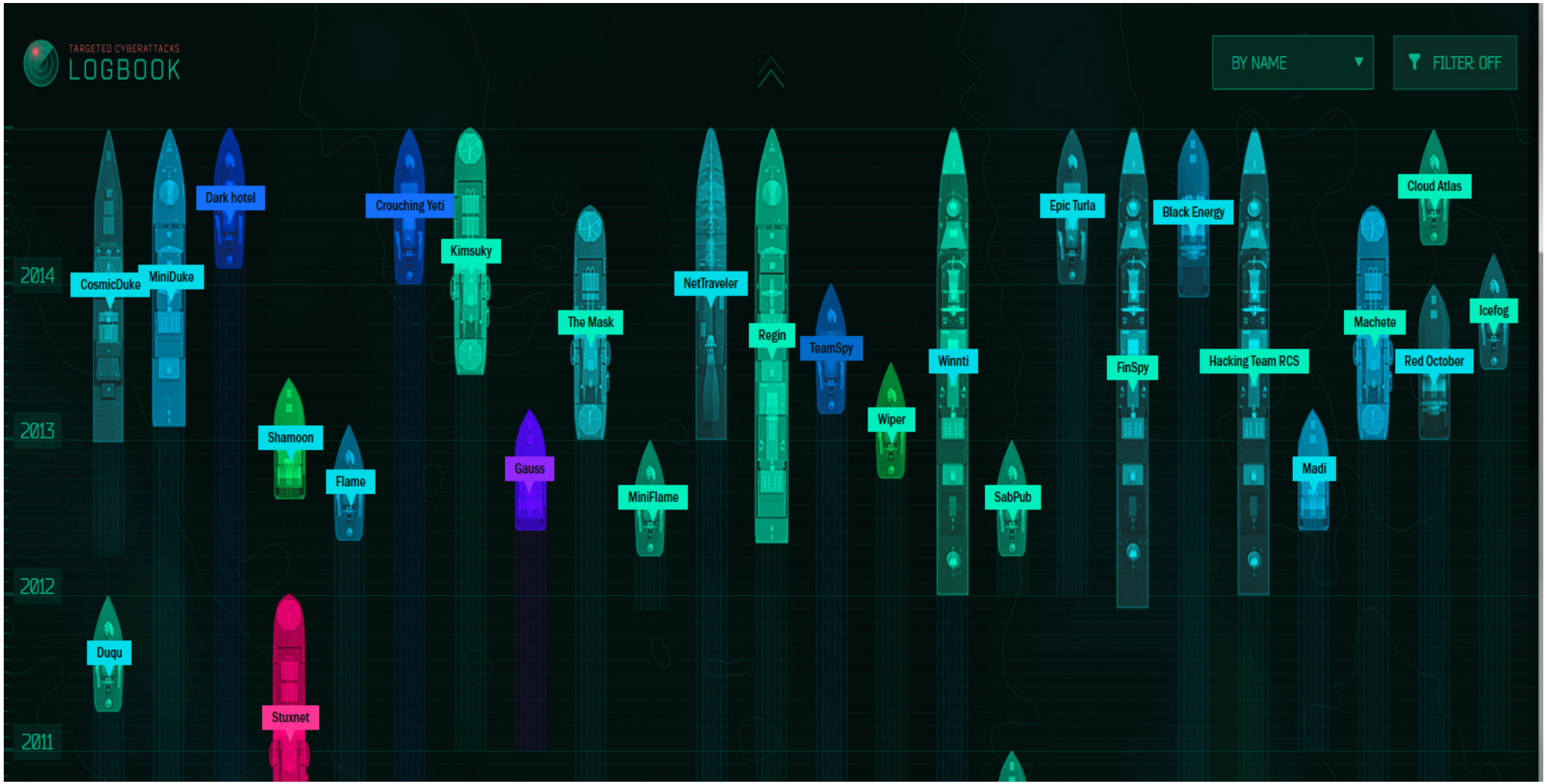
- APT:- Advanced Persistent Threat also known as a Targeted Attack.

  The attackers use a mixture of tools and methodologies to gain access to a specific organisation's infrastructure. This may be via simple hacking, spear-phishing or other social engineering attacks; this may include customised malware.

  – Think of an APT attack as a persistent Penetration Test, without your approval or knowledge…utilising:

    - Hacking
    - Social engineering
    - Malcode/malware.





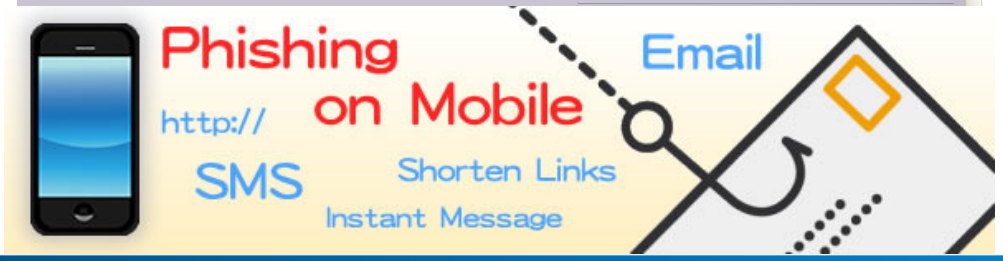
ERS - An international defence contractor…

- **Business challenge:**
  - The FBI contacted the customer to inform them that they had been hacked and that the attackers were stealing data from them as well as “bugging” key executives laptops. They also suggested that they get help in finding and removing the malcode.
- **Solution:**
  - IBM identified the new malware (unknown to all anti-malware solutions) installed (and how it was hidden)
  - IBM identified how and to which remote systems the data was being “exfiltrated” to so that network traffic to/from those systems could be blocked. Cutting off remote control and data leakage.
- **Benefits:**
  - IBM identified the new malware and identified how it installed, what it did, etc.
  - IBM created a “bespoke” detection and removal script for the customer. This “killed” the malware in memory and then deleted the malware from the system. It also sent reports of infections found and cleaned to the security manager.
  - Client was delighted with our speed of action and the complete removal of the malware.

APT was found that allowed attackers to get access to confidential data including weapons systems code and blueprints as well as record executive meetings!

Phishing – it's not just about banks

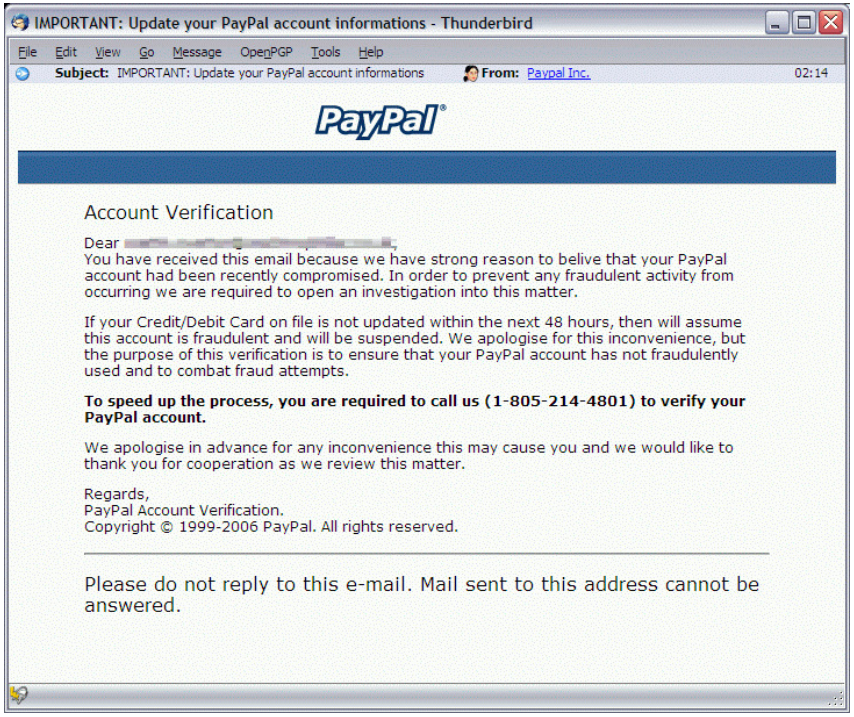
- Phishing – deception designed to steal personal data such as banking details, credit card information or logon information (e.g. amazon, itunes, facebook)
- Targets include email, instant messaging, mobile devices, fake web sites
- Has been around for a number of years. Phishers using more innovative ways to bypass filters and deceive users
- Use social engineering to entice victims (e.g. you've won a competition, get free stuff, you've been compromised)
- They are VERY realistic



Vishing

- Phishing via VOIP
  - Works like this
  - You receive an e-mail message stating:

    "To verify your details please call 1-800-214-4801"
  - You call the number and are asked to leave your credit card information by a recorded message



IMPORTANT: Update your PayPal account informations - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: IMPORTANT: Update your PayPal account informations **From:** Paypal Inc. 02:14

PayPal

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

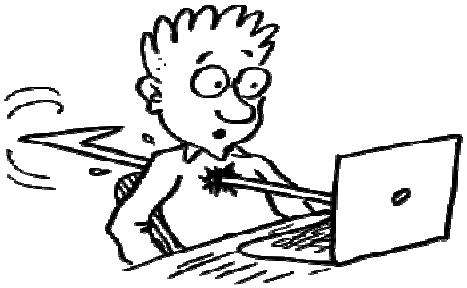
Please do not reply to this e-mail. Mail sent to this address cannot be answered.

SMiShing

- Phishing via SMS
  - Works like this
  - You receive an SMS message stating:
    - "**We're confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order: www.smishingurl.com**".
  - You visit the link using your PC's Web browser and get infected with malware

Spear Phishing

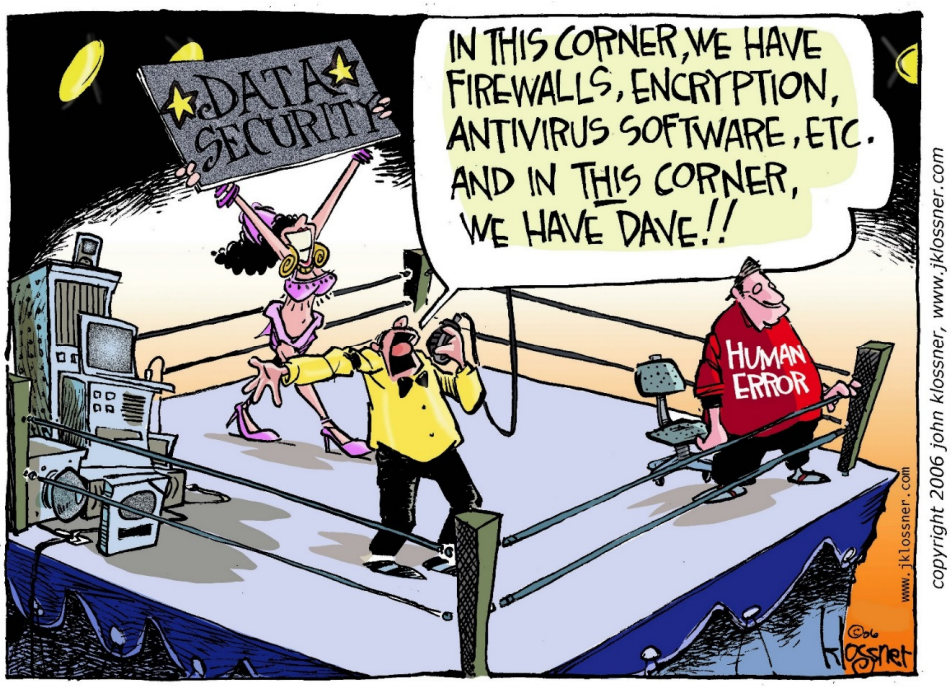
- Phishing scam targeting a single company or organisation
  - **If your users received an email from "H.R." asking them to confirm their username/password how many would?**



- **Attacks have a specific aim - to gain access to your internal systems**

- **Many so-called APT* or Targeted attacks use this as one of their main attack vectors.**

- **This is made easier by the vast amount of data most people give away via social media sites and services…**



Advanced Persistent Threat

Penetration Testing Win Story:
A Payroll Services Company

- **Business Challenge:**
  - The customer wanted IBM to test the security of their network, externally and internally as well as carrying out social engineering tests to check that their in-house education was working, or not...
- **What We Did:**
  - Dropped USB sticks in the foyer and office areas that contained auto-running payloads (when inserted) and also `sensitive` files; also booby-trapped.
  - Carried out Phishing attacks, via email, the web and over the phone.
  - Performed a full external and internal penetration test of their infrastructure.
  - Despite being well trained in spotting phishing attacks we managed to get a key individual to disclose credentials!
- **Benefits:**
  - Customer was delighted with the results, although somewhat surprised that someone had fallen for our phishing email and website, disclosing credentials for an account that contained many Millions of Pounds.
  - The final report included a number of recommendation to deal with the issues (not just the social engineering) identified as part of the engagement.

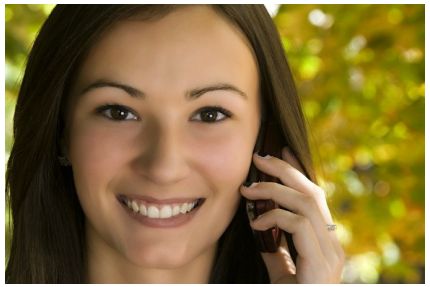
IBM socially-engineered a key staff member that had direct access to a bank account that contained Millions of Pounds of Payroll for their customers. This was done via a Phishing email and Fake Bank website that IBM created for the customer to test their staff education.

HACKING

The Internet of Things!

Penetration Testing Win Story:
An International Technology Company

- **Business Challenge:**
  - The customer wanted IBM to test the security of their mobile devices running a customised version of Android, including drivers, kernel, etc. They wanted IBM to identify any areas of weakness that needed to be addressed
- **What We Did:**
  - Fuzzing and reverse-enginering of the kernel and drivers used was undertaken with numerours issues identified, including:
    - Denial of Service
    - Buffer Overflows
    - Privilige Escalation
    - Code Injection
- **Benefits:**
  - A report containing details of how we tested and compromised the devices along with remediation details and longer term recommendations was supplied to the customer.



IBM tested the mobile devices at the lowest possible level, by using fuzzing and reverse engineering to identify security flaws in the kernel and drivers which could have led to the devices being compromised by an attacker.

And it Isn't Just Servers and Desktop Computers or Laptops Organisations and You Need to Worry About…

COMPUTERWORLD

White Papers | Webcasts | Newsletters

Topics | News | In Depth | Reviews | Blogs | Opinion

Security | Application Security | Cybercrime and Hacking | Cyberwarfare | Dat
Malware and Vulnerabilities | Mobile Security | Privacy

Home > Security > Malware and Vulnerabilities

News

Printers, routers used as bots in DDoS attacks

Network-connected devices have vulner
be easily manipulated, Prolexic says

By Jaikumar Vijayan
May 1, 2013 04:05 PM ET

More

Computerworld - Printers, routers, IP came
connected devices are increasingly used t
service attacks, security firm Prolexic warr

Attackers are taking advantage of inherent
network protocols used by these devices t
Prolexic said.

INTERNATIONAL BUSINESS TIMES

FRIDAY, AUGUST 09, 2013 AS OF 10:30 AM EDT

Home | Politics | Economy | Markets / Finance | Companies | Tech / Sci | Media &

TECH / SCI | INTERNET

Toilets And TVs: Hackers Find New Ways To Invade Your Personal Life

By Ryan W. Neal
on August 05 2013 3:15 PM

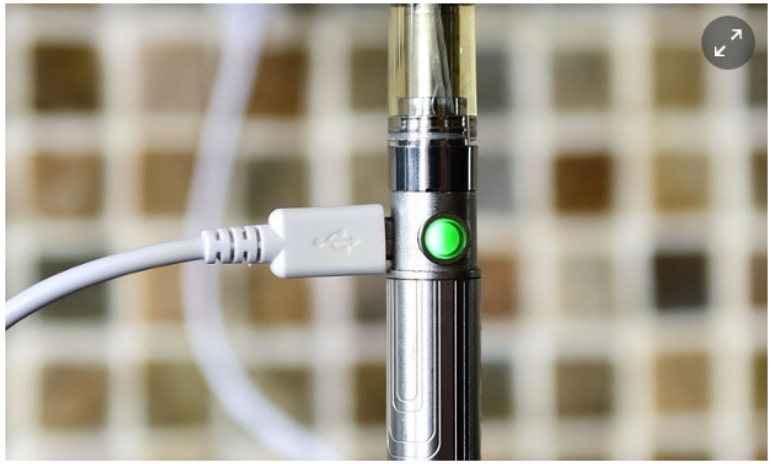
0 | 0 | 0 | Ć | p more

If you didn't have enough to worry about with the NSA tracking everything you do online and hackers extracting personal data from your smartphone, now you can worry about cybercriminals invading your bathroom and living room. With the advent of Smart TVs and even a Smart Toilet, even your most private moments are vulnerable to prying eyes.

LAXIL, a Japanese toilet manufacturer, introduced the Satis, a toilet with deodorizing capabilities, an automatic seat, a dual-nozzel bidet and Bluetooth capabilities to control the porcelain throne with an Android app. But it appears Satis gave every toilet

Now e-cigarettes can give you malware

Better for your lungs, worse for your hard drives, e-cigarettes can potentially infect a computer if plugged in to charge

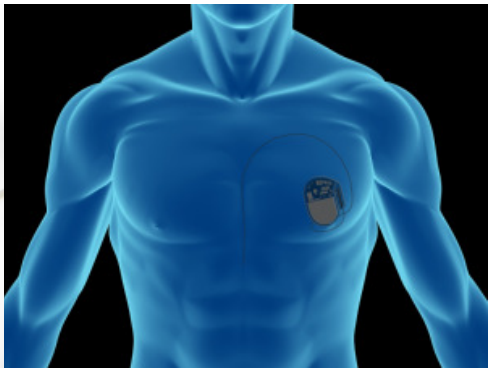


E-cigarette can either be charged from the wall or by plugging the cigarette itself into a USB port. Photograph: Ian West/PA

E-cigarettes may be better for your health than normal ones, but spare a thought for your poor computer - electronic cigarettes have become the latest vector for malicious software, according to online reports.

Healthcare

- ICS-CERT reported that around 300 machines from 40 vendors have hard coded passwords…These include:
  - Pacemakers
  - Surgical and anesthesia devices
  - Ventilators
  - Drug infusion pumps
  - External defibrillators
  - Patient monitors
  - Laboratory and analysis equipment
  - Drug control systems
  - Patient records
  - Surgery robots (teleoperated)



"In 2007, then-U.S. Vice President Dick Cheney ordered some of the wireless features to be disabled on his defibrillator due to security concerns."

Critical Infrastructure - Airplanes

- ACARS Systems for sale on eBay
- On-board systems only separated by a firewall
- Can in theory be hacked via on-board WiFi
- Government Accountability Office confirmed risk

SC Staff

February 13, 2015

Demo hack shows how to crash a plane; air cyber-security being improved

Share this article:

In separate developments, a demo hack in Amsterdam shows how to crash a plane, while the US Federal Aviation Administration seeks to improve air cyber-security.

Hacking an aircraft is just an app away and modern aircraft with in-flight connectivity are particularly susceptible, as a demo this week (see below) demonstrated.

Separately, the US Federal Aviation Administration is setting up an industry working group on how to improve aircraft cyber-security.

Cyber-security vulnerabilities for aircraft operating in the US National Airspace System are not specifically addressed, and the FAA says that as a result vulnerabilities "may not be identified and mitigated, thus increasing exposure times to security threats".

Threats include hackers gaining unauthorised access to aircraft systems and networks which "could result in the malicious use of networks, and loss or corruption of data (eg, software applications, databases, and configuration files) brought about by software worms, viruses, or other malicious entities".

The FAA also says that a lack of cyber-security regulations, policy, and guidance "could result in security-related certification criteria that are not standardised and harmonis

"Modern communications technologies, including IP connectivity, are increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems"

Penetration Testing - An International Airport

- **Business Challenge:**
  - The airport wanted IBM to test the security both externally (from the Internet) and internally (on-site) to ensure that they were secure from being hacked and to identify any areas of weakness that needed to be addressed
- **What We Did:**
  - An external webserver was found to be vulnerable to attack (weak password and default admin user id).
  - Once compromised IBM gained Domain Admin privileges to the DMZ Domain Contollers, and so could access all files regardless of who owned them or how they were secured. IBM also could do the same attack against the internal Domain Controllers.
  - We also had access to power controls, emails, pay slips, phone calls...
- **Benefits:**
  - The customer was shocked at how far we managed to penetrate their networks. They were delighted in the level of detail in our report and welcomed the remediation advice and recommendations on how to seriously improve their security posture.

IBM compromised an Internet facing web server. IBM acquired Domain admin for the DMZ Domain.
This means we own all Windows systems in the DMZ domain, and all data on the Windows systems! We could also add ourselves to the INTERNAL Domain Controllers as Domain Admin…all from the Internet!

Intellectual Property Theft

- Gemalto – SIM card keys stolen – Nation State Actors
- Diginotar – Fake SSL Certificates created – Nation State Actors
- SONY – Lots of attacks and theft of material
- RSA – Compromised via business partner
- Defence Contractors – Weapons controls/guidance systems and blueprints stolen
- Drug Companies – Patented and un-patented drug details
- Engineering Firms
- Retailers, Hoteliers, Insurers, Banks, Credit/Loan companies, etc.

"Information is the new worldwide currency. Every piece of data is valuable to someone, somewhere, somehow"

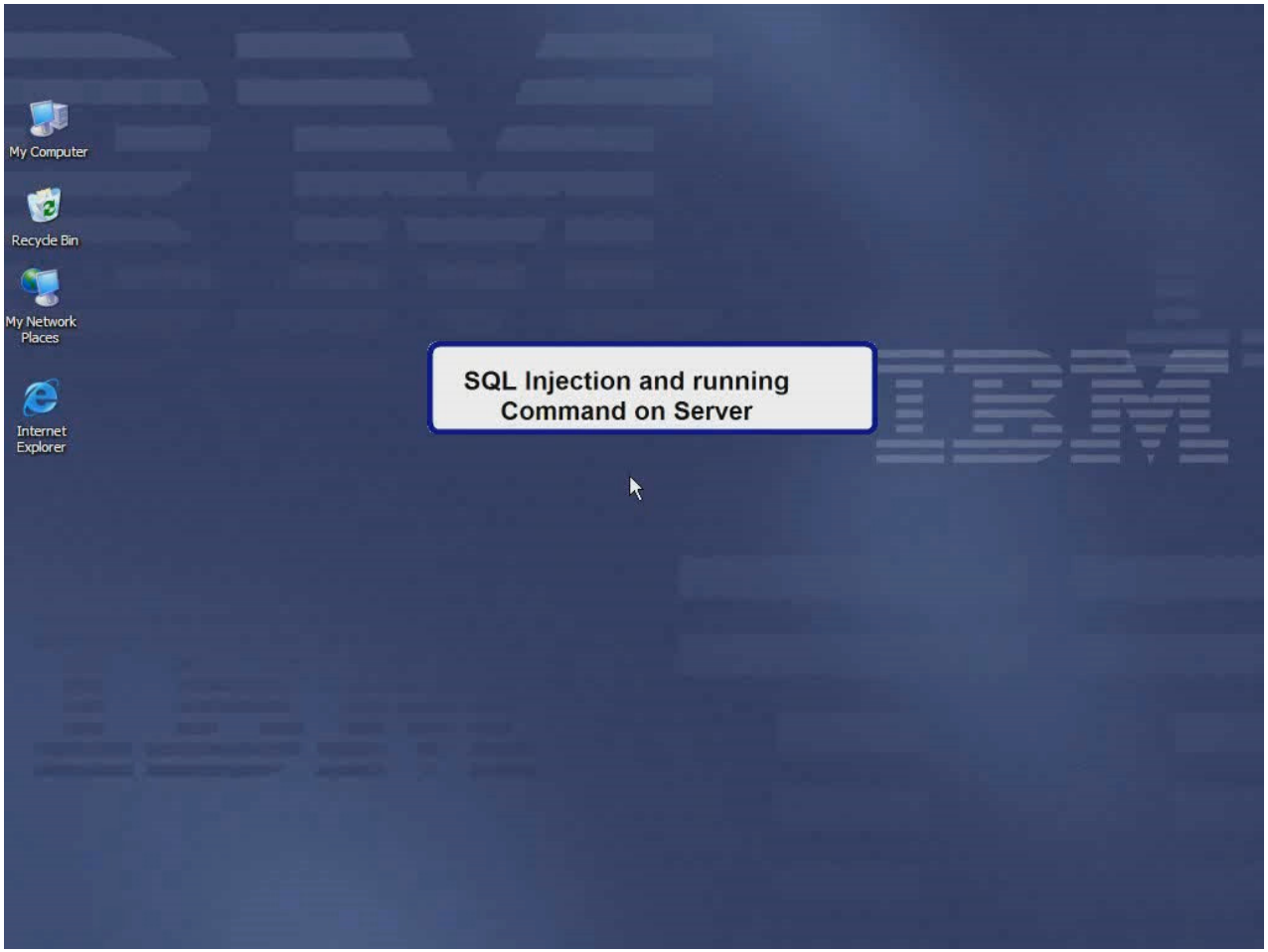
(IDC, Worldwide and U.S. Security Services Threat Intelligence 2011-2014 Forecast)

Penetration Testing Win Story:
A High-Street Retail Company

- **Business Challenge:**
  - The customer wanted IBM to test the security of their branches and whether we could hack them and if we could gain access to the data center and sensitive data held. We were only allowed to hack them via WiFi...
- **What We Did:**
  - Sat in the Cafe next door and quickly compromised the branch WiFi network, also took control of the PoS systems.
  - From there we found we could gain access back to the data center.
  - On the data center network we managed to find and access details of over 5 million credit card transactions, all un-encrypted.
- **Benefits:**
  - Customer was very shocked to find out how easily we hacked them and the data we had access to.
  - A detailed step-by-step account of how we hacked them was included in the final report to the customer (as usual) as well as detailed remediation instructions and recommendations on how to improve their overall security.

IBM cracked the branch WiFi network and gained access to the tills and other PoS systems before quickly moving on to the data center (over the branch WiFi) and gaining access to over 5 Million credit card transactions (including card details) found un-encrypted on their servers.

So Just How Easy is it to Hack a Website?



ERS - An international insurance company….

- **Business challenge:**
  - The customer contacted IBM to investigate a hack on their management server for all their iDevices. The hacker got in to the management portal and requested that all devices were [illegible] to attempt to cover their tracks.
- **Solution:**
  - IBM confirmed that the integrity [illegible]
  - IBM confirmed that the data ac[illegible] the management portal administra[illegible]
  - IBM confirmed that no other da[illegible] at the second server had not been co[illegible]
  - We managed to create a full ti[illegible] e attacker, despite their attempt [illegible] ver back to factory defaults.
- **Benefits:**
  - IBM performed a thorough ass[illegible] ervers, providing the customer with a list of critical areas/issues that should be reviewed/addressed by the hosting provider before bringing the servers back on-line.
  - The final report also included a set of medium and longer term recommendations on remediating migration procedures and security best practices that had not been followed by the hosting provider.

Hacker accessed the customers management console for managing iDevices (iPhone, iPad, ec.) in use in their company.
We identified what the attacker had accessed (despite their attempt to destroy evidence) and that the root cause for the data leakage was the outsourcer's improper security procedures

ERS - International Manufacturing Company

- **Business challenge:**
  - The customer contacted IBM as several public-facing websites on one of their servers had been defaced.
- **Issues found:**
  - IBM quickly identified that the web defacers had got in via a combination of an insecure Application and WebDav being enabled on the web server.
  - Further analysis of the system uncovered activities by a second group of hackers that had been active on DMZ systems for more than 2 months.
  - The source of the attack was found in an un-patched SAP system. The vulnerability allowed remote command execution on the SAP server.
  - Within a month from the start of the attack, attackers managed to:
    - Install unknown malware on several systems (both internal and DMZ)
    - Install 5 different types of backdoors on several DMZ systems
    - Open Remote Desktop connections to the DMZ systems by tunneling it over the HTTP port
- Get access to the domain controllers on the intranet
    - Steal (and use) lots and lots of domain credentials
    - **Basically, they owned the network without being detected!!**

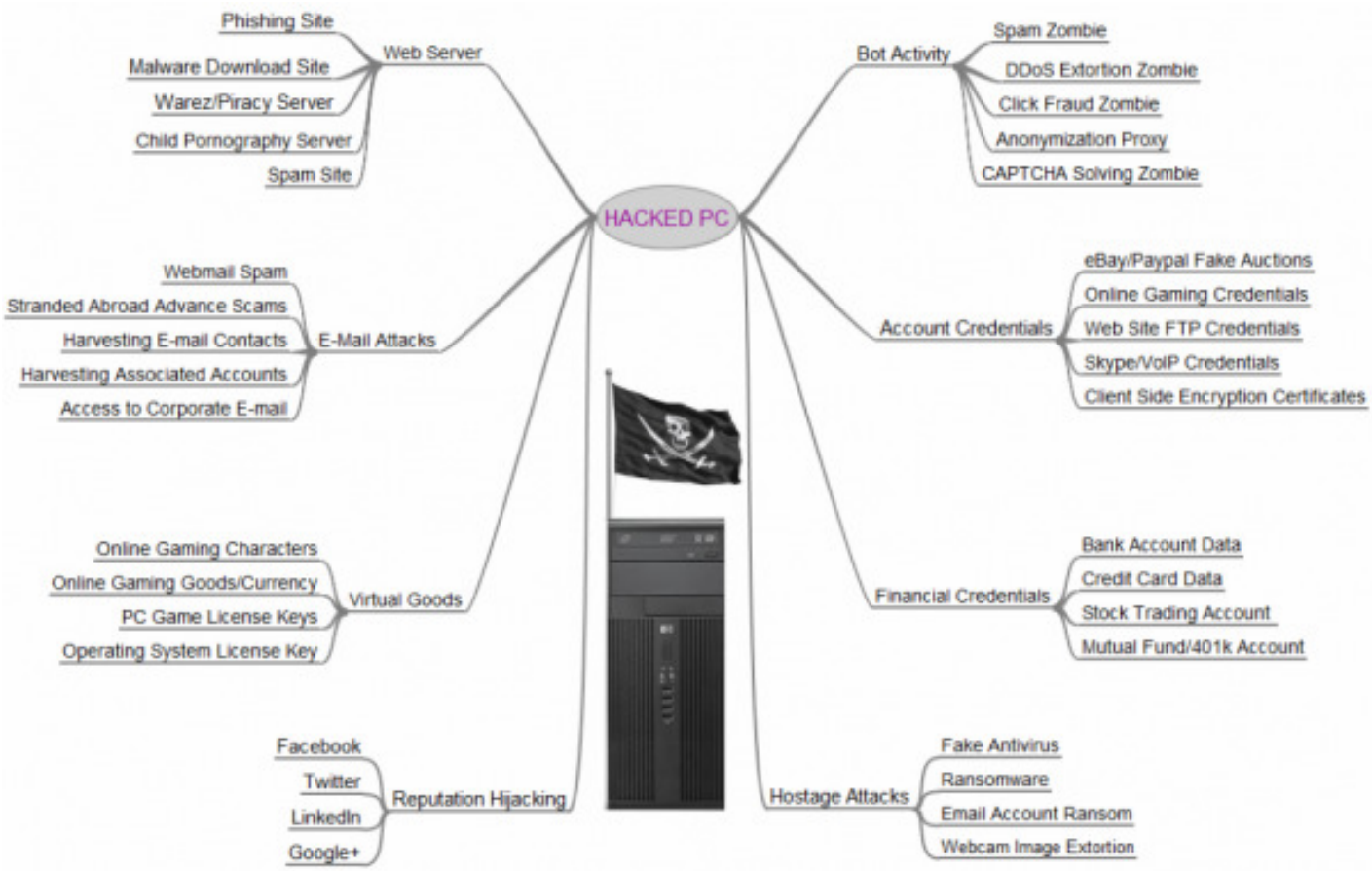
Remote access tools and unknown strains of malware were discovered and removed.

A full timeline of events from the time of the breach until the issue was identified was created.

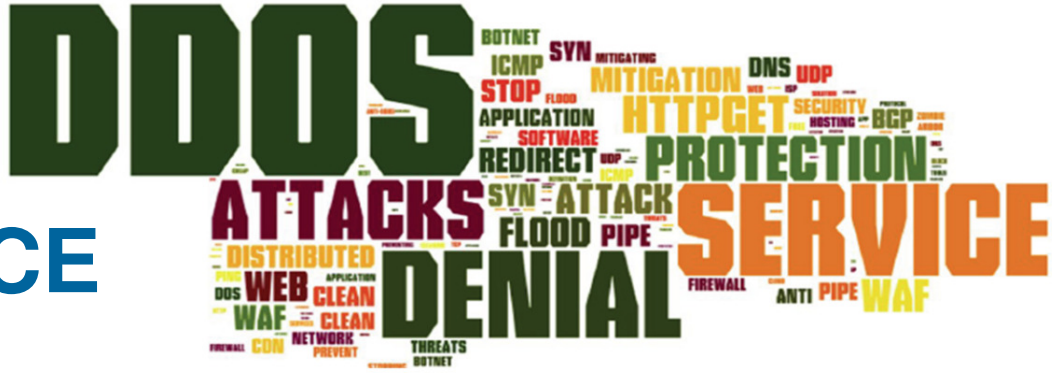
Remediation steps were provided to customer.

Sad day when you have to be “thankful” for a Web defacement!

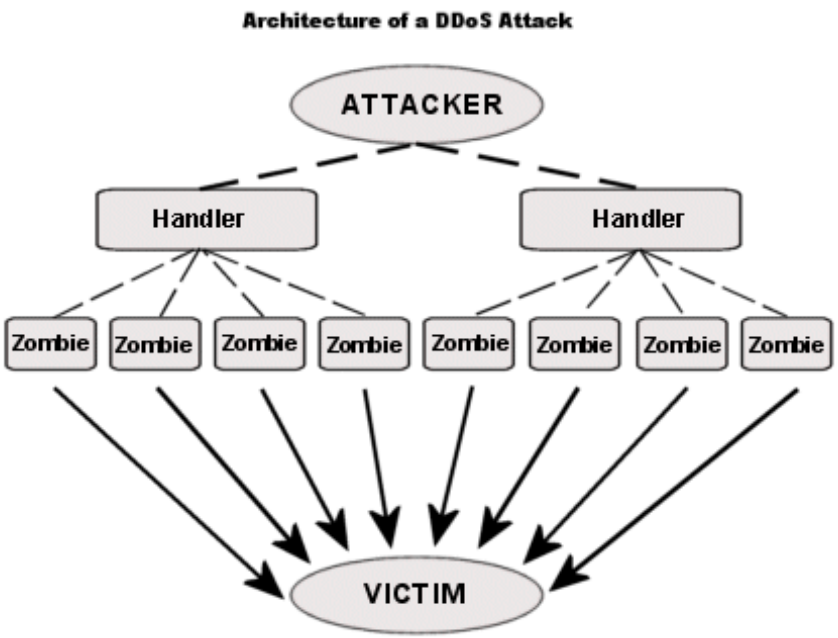
The “Value” of a Hacked System…



DENIAL OF SERVICE



Distributed Denial of Service (DDoS)



- ICMP (Ping Flood) aka “Smurf Attack”
- Lots of other DoS and DDoS methods
- Easy and cheap to carry out, just need willing volunteers or a Botnet…

- TCP (SYN, Connect) Flood, and others
- UDP Flood (Fraggle Attack) amongst others

DoS/DDoS attacks

- Network (L4 attacks)
  - Floods (TCP/UDP/ICMP)
  - Fragmentation attacks (Teardrop, Nestea, etc)
- Application (L7 attacks)
  - HTTP
  - HTTPS
- Newer attacks
  - NTP
  - SNMP
  - SSDP
  - DNS
  - WordPress Pingbacks/Trackbacks

"***From a philosophical perspective, if the attacker's pipe is bigger than the defender's pipe, the attacker can always knock out the defender***"

- Bruce Schneier

DDoS as smokescreen to masquerade other fraudulent activities

"*After the [bank] accounts are compromised, the perpetrators conduct a Distributed Denial of Service (DDoS) attack on the financial institution. The belief is the DDoS is used to deflect attention from the wire transfers as well to make them unable to reverse the transactions"*

Sources:

- FBI Denver Cyber Squad Advises Citizens to be Aware of a New Phishing Campaign
- DDoS Attack on Bank Hid $900,000 Cyberheist

KrebsonSecurity

In-depth security news and investigation

BLOG ADVERTISING

19 DDoS Attack on Bank Hid $900,000 Cyberheist

FEB 13

A Christmas Eve cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than $900,000.

At approximately midday on December 24, 2012, organized cyber crooks began moving money out of corporate accounts belonging to **Ascent Builders**, a construction firm based in Sacramento, Calif. In short order, the company's financial institution – San Francisco-based **Bank of the West** –

Recent Posts

DHS: 'OpUSA' M
Than Bite
Wash. Hospital
Million Cyberhe
Dutchman Arres
DDoS
How Not to Inst
Skimmer
Sources: Tea Le

At IBM, the world is our security lab

6,000+ IBM researchers, developers, and subject matter experts focused on security

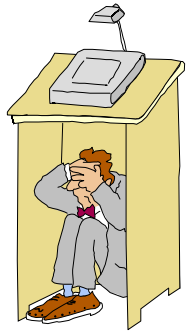
3,000+ IBM security patents

Conclusions

- **You DON'T have to make the same mistakes. It is not compulsory ;-)**
- **It isn't IF you get compromised, it is when, as it will happen!**
- **Have an Incident Response Plan and test it (regularly)**
- **Carry out regular penetration tests, or at least vulnerability scans (they are NOT the same thing!)**
- **Follow industry best practice, patch as quickly as you can**
- **Make sure that passwords are changed regularly**
- **Ensure that staff are adequately trained**
- **Encrypt data wherever possible to help minimise the risk if it does get stolen.**
- **Baseline your "normal" network traffic**

- **Be risk aware and get actionable security intelligence to help you keep ahead of the threat!**

Questions?



Contact Details:

Martin Overton

Phone: +44 (0)2392 563442

Email: overtonm@uk.ibm.com

Twitter: martin_sec

also on LinkedIn, FaceBook, Xing

Lots of conference papers here: http://momusings.com/papers

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.

Consulting & Systems Integration | Cloud Security Services

IBM Cybersecurity Assessment and Response Services help prepare and more quickly respond to security threats and incidents

IBM Cybersecurity Assessment and Response Services

Offering descriptions

Emergency Response Services	Helps manage incident response across multiple stages including prevention, intelligence gathering, containment, eradication, recovery, and compliance management
Incident Response Planning	Determines the right process, tools, and resources to respond to and help reduce the impact of a cyber attack
Active Threat Assessment	Examines a client's infrastructure to uncover indicators of a compromise and/or hidden threats
Penetration Testing	Performs controlled attacks to identify vulnerable systems and provides detailed security roadmap to help prevent network compromise and better manage compliance
Smart and Embedded Device Security	Helps manufacturers improve their products by identifying and fixing security vulnerabilities to support increased integrity, stability, and availability of devices while helping to prevent hackers from gaining access
APT Survival Kit	Helps you better prepare for, prevent, detect and remediate attacks, reducing the timeline for potential impact by providing end-to-end cyber breach preparedness and recovery solutions
Security Awareness Training	A low cost, cloud-based training regiment designed to enable end-users, to defend themselves against common online crime.

24x7

The (cyber)storm is coming. ARE YOU READY?

Help is just one click away.
Or call us at: (US) 1-888-241-9812 | (WW) +1-312-212-8034
Get ahead of the storm with a penetration test & incident response planning