Security Update

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

Don Hewatt CISSP
Security Engineering
Government Markets

verizonbusiness

Threats

- **Threats are growing in complexity and their ability to target specific assets**
- **Organized crime has created business out of Hacking**
  - Multi tiered fraud rings
  - Lucrative business – Bank robbery = Avg. $3K, Admin for bot network - $5K/week
  - Advanced software and network design dedicated to fraudulent means
- **National Security**
  - Nation sponsored hacks at the Federal level are just now starting to hit the media
  - US Government is enacting multiple efforts to address threat
- **State Governments are rich targets**
  - Data stored
  - Economy
  - Public facing entity
  - Hacker organizations are opportunistic – go where the money/profit is

***Much of data in this report is based on 2009 Data Breach Investigation Report**

verizon business

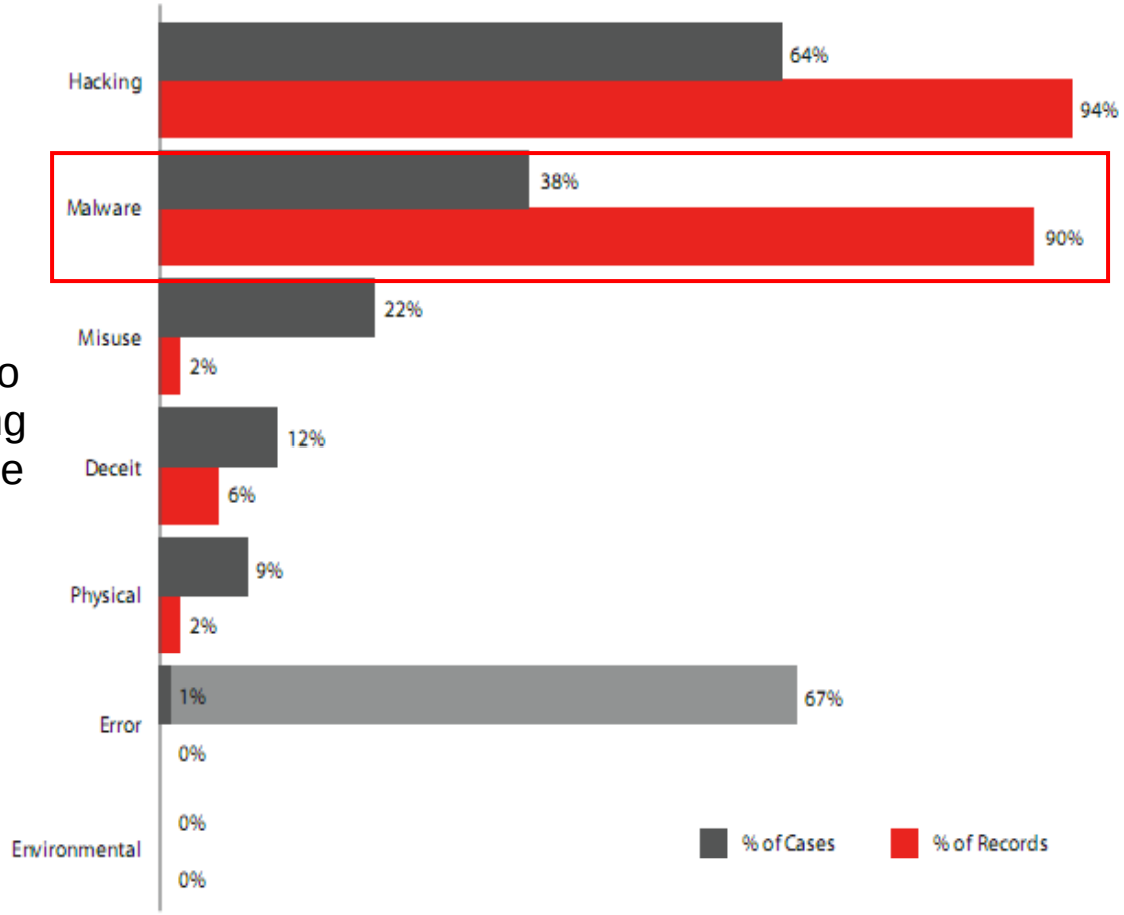
Investigative Findings – 2009 Breach Report

- In 2008 alone, Verizon Business investigated 285 million records that were compromised totaling more compromised records than in the previous four years combined.
- Most data breaches investigated were caused by external sources.
- Most breaches resulted from a combination of events rather than a single action.
- In almost 70% of the cases, the breach was discovered by third parties.
- Nearly all records compromised in 2008 were from online assets.
- About 20% of the cases involved more than one breach.
- Being PCI-compliant is critically important.
- Nearly 9 out of 10 breaches were considered avoidable if security basics had been followed.

verizon business

Malware

- **Typical purpose is to gather intelligence and provide distribution method for other malicious efforts**
- **Result**
  - massive remediation efforts due to lack of proper preparation planning
  - Critical systems being taken offline
  - Public disclosure causing PR challenge
- **Last years investigations indicated 38% of cases were hacks with 90% of 285 million records breached as a result***



verizon business

MS08-067 Timeline – Conficker exploit

- Oct 22nd, 2008 – Out of cycle Patch released by Microsoft (MS08-067)
- Oct 24th, 2008 – Gimmiv released
- Oct 28th, 2008 – Initial Metasploit exploit released (Conficker authors used it in their worm)
- Nov 21st, 2008 – Large port 445/TCP port spikes observed
- Nov 21st, 2008 – Downadup.A released (quickly spread to 500k+ machines mostly in China and Argentina)
- Nov 25th, 2008 – Symantec warns of MS08-067 exploitation in the wild
- Dec 31st, 2008 – Downadup.B released (2 – 8 million+ by Jan 9th)
- Jan 28th, 2009 - Conficker still growing (perhaps 1.14% per day or 8% over the last week)
- Feb 1st, 2009 – Daily sources exceeds 10million (.A = 40%, .B = 60%)
- Mar 16th, 2009 - Many Conficker.B machines updated to new .C variant
- Apr 7th, 2009 - Conficker.E variant discovered in the wild with new features
- May 11th, 2009 - Conficker variants continue to propagate. Conficker remains a significant threat.

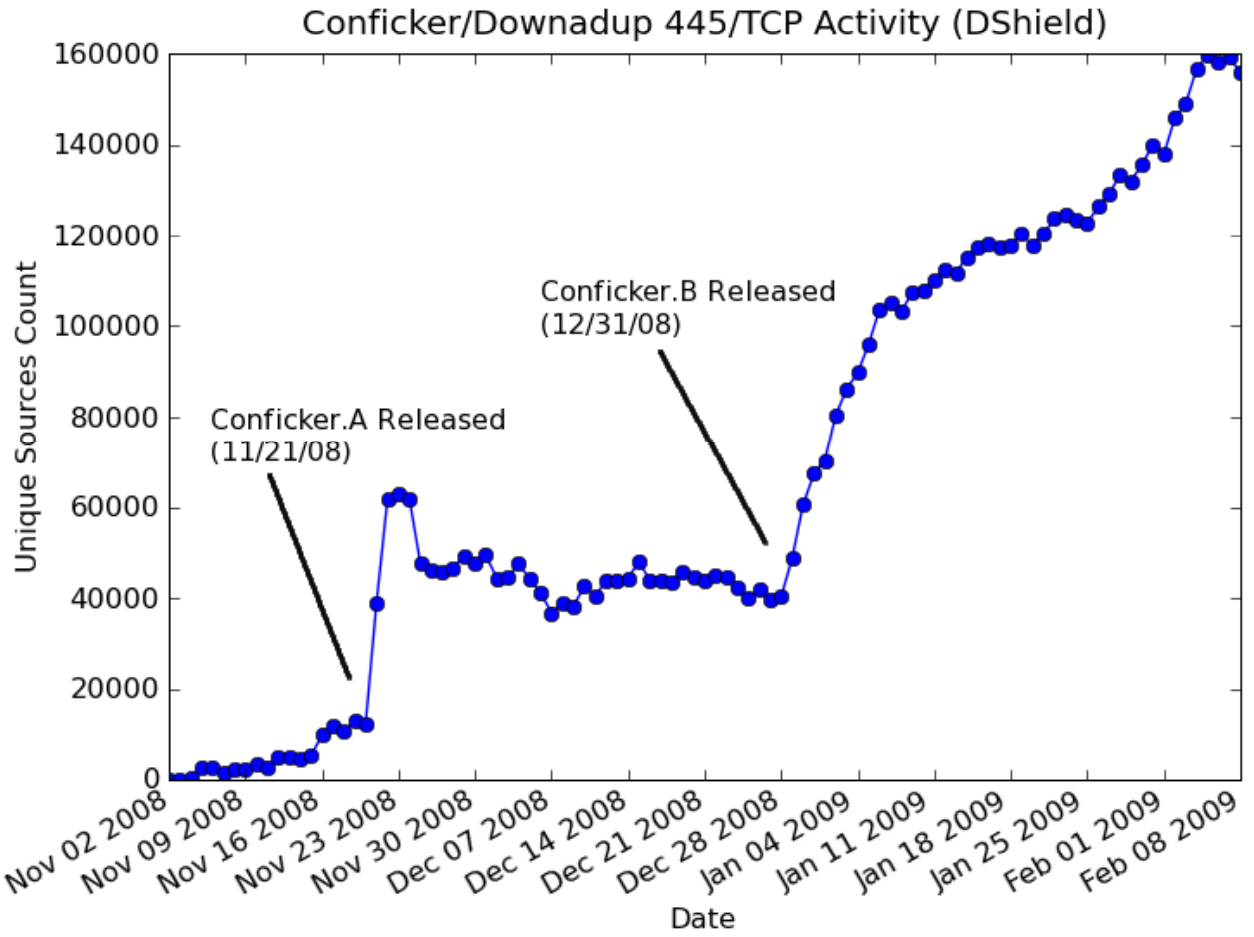
verizon business

Growth
(Uniq Sources/Day exceeds 10 million on 2/2/09)

Top Countries (Source IP 445/TCP) at P

- **Russian Federation (13%)**
- **China (12%)**
- **Taiwan (7%)**
- **Italy (7%)**
- **Brazil (7%)**
- **India (4%)**
- **United States (3%)**
- **Germany (3%)**
- **Ukraine (3%)**
- **Argentina (3%)**

156 Other Countries (38%)



verizon business

Conficker Outbreak

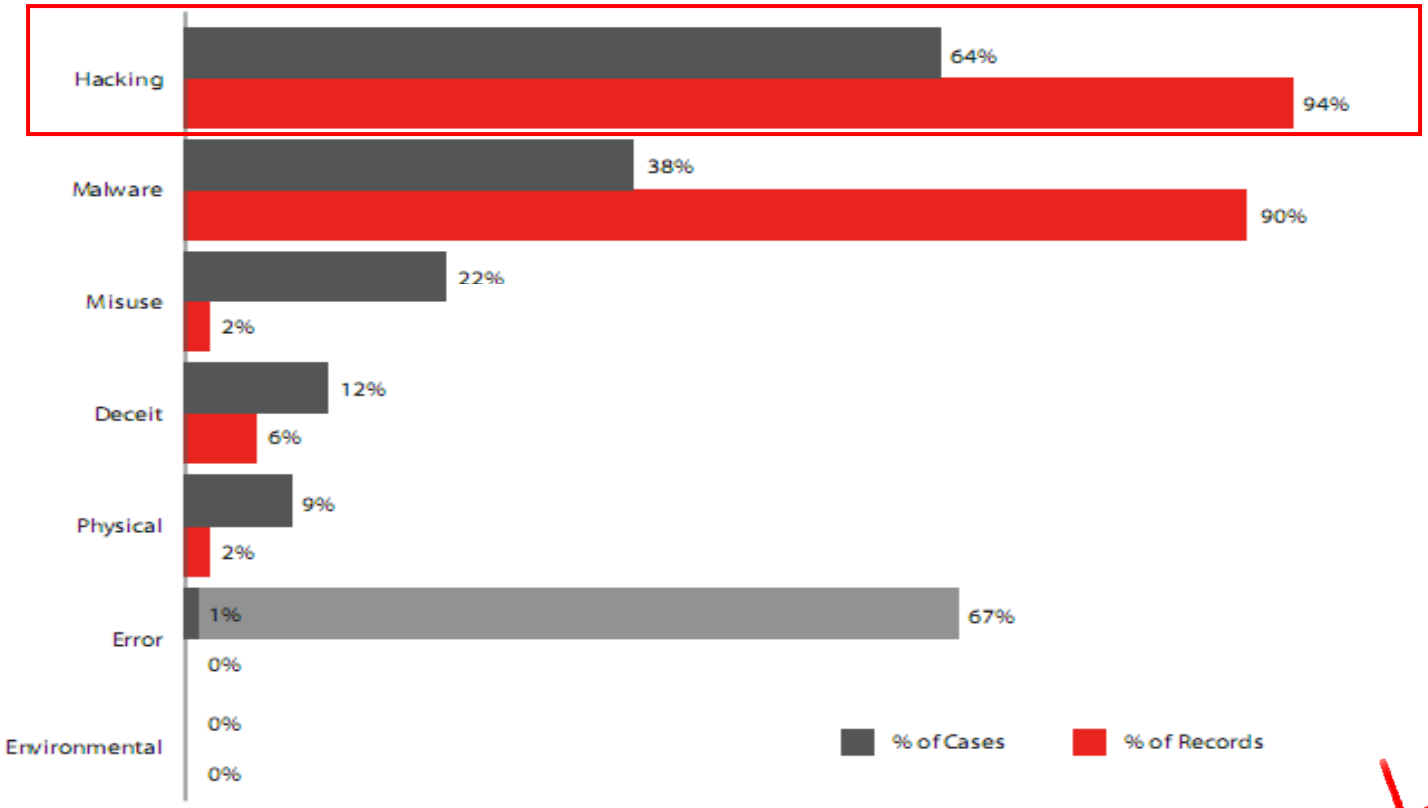
- **Damage in US was controlled due to target selection (US is typically top 3)**
- **The US was impacted far less than other countries. Removable USB devices remain a threat.**
- **Arms race: Conficker flaw enabled remote scanning with tools such as Nmap, Nessus,etc.**
- **Conficker authors patched the flaw within 8 days. Scanning tools authors had to develop new methods, etc., etc.**

- **Impacted large agency within state government**
  - Malcode introduced via thumb drive
  - 6000-7000 PCs infected within 48 hours
  - Had to disconnect Internet connectivity to reduce outside connections and updates

verizon business

Hacking

- **Last years investigations indicated 64% of cases were hacks with 94% of 285 million records breached as a result ***



verizon business

Hacking by the numbers

- **Based on investigated breaches ***

Figure 15. Types of hacking by number of breaches (black) and percent of records (red)

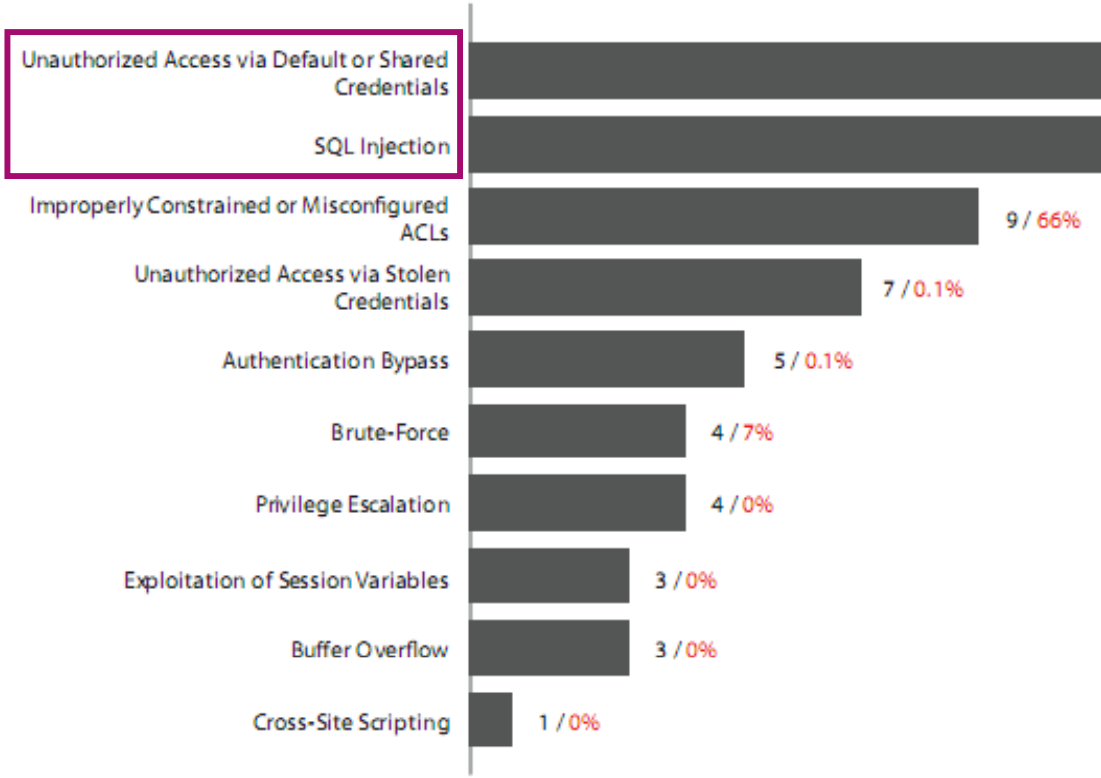


Table 2. Patch availability at time of breach

Less than 1 month	0
1 to 3 months	0
3 to 6 months	0
6 to 12 months	1
More than 1 year	5

verizonbusiness

Virginia's Prescription Drug Monitoring Program (PDMP)

- Established in 2006 to prevent prescription drug fraud
- 8 million patient record and 35 million prescription records claimed to have been breached
- More than 38 states have similar monitoring program
- Whether records were actually taken or not, damage to the program is extensive
- Ransom note:

> ATTENTION VIRGINIA I have your s***! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(
>
> For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I'll go ahead and put this baby out on the market and accept the highest bid. Now I don't know what all this sh** is worth or who would pay for it, but I'm bettin' someone will. Hell, if I can't move the prescription data at the very least I can find a buyer for the personal data (name,age,address,social security #, driver's license #)…….

verizon business

Preparation and Remediation in State and Local Gov

- **Technology is not always the answer** (In many cases it is the problem)
  - Product tends to be used as a replacement for process
  - Capital expenditures may be easier to come by than operational expenses
  - Always a better widget to be had

- **Lack of understanding and control**
  - Unknown data accounts for 2/3 of compromised records and over a third of the breaches*
  - Unknown assets, connections and privileges
  - Organizations have trouble controlling procurement and asset on boarding
  - Proper data classification does not exist
  - Access auditing and control down to the actual user is expensive and difficult

- **Internal resource expertise are becoming scarce**
  - Employees are multi tasked
  - Skills are in high demand where salaries are higher in private sector
  - Many states can not afford a resource ‘bench’ to activate during large breaches

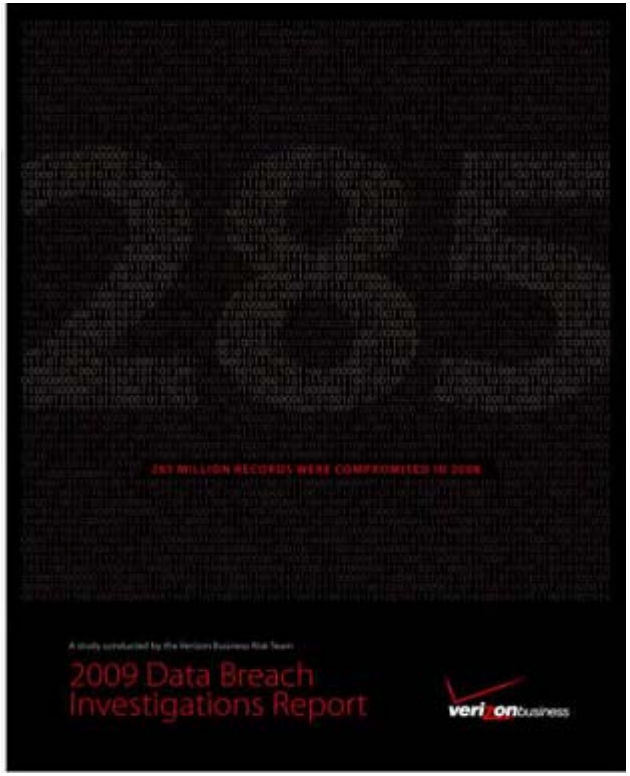
verizon business

Focus efforts on what matters

- **Ensure essential controls are met**
  - Stop trying to boil the ocean
- **Find, track, and assess data.**
  - Eliminate unknown unknowns as much as possible
- **Collect and monitor event logs**
  - Establish procedure to ensure data is reviewed on an ongoing basis
- **Audit user accounts and credentials**
  - Ensure you have a process to properly assign and revoke credentials
- **Test and review web applications**
  - Most common vector of record breaches

verizon business

Data Breach Investigation Report Event Info



Sacramento CA Session
June 17, 2009
1:00 PM – 3:00 PM
Department of Health,
1500 Capital Avenue,
Sacramento, CA
Host by Dr. Tippett

Register at:
http://www.verizonbusiness.com/us/about/events/2009databreach/goved/

verizonbusiness

Thank you

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

verizon business