Industry Analysis – 2014 Data Breaches - Ponemon

- Probability of data breach involving 10,000 or more records within the next 24 months

Ponemon 2014 Data Breach Report
## Industry Analysis – 2014 Data Breaches - Mandiant

### Across the Cyber Threat Landscape

<table>
<thead>
<tr>
<th>Objective</th>
<th>NUISANCE</th>
<th>DATA THEFT</th>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
<th>NETWORK ATTACK</th>
</tr>
</thead>
</table>

### How Compromises Are Detected

- **33%** of victims discovered the breach internally (Down from 37% in 2012)
- **67%** of victims were notified by an external entity

### Time from Earliest Evidence of Compromise to Discovery of Compromise

- 229 days
- Median number of days that threat groups were present on a victim’s network before detection
- 14 days less than 2012
- Longest Presence: 2,287 days

### IRAN-BASED vs. CHINA-BASED

<table>
<thead>
<tr>
<th>Category</th>
<th>IRAN-BASED</th>
<th>CHINA-BASED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industries Targeted</td>
<td>Energy, state government agencies</td>
<td>Most industry sectors</td>
</tr>
<tr>
<td>Victim Selection</td>
<td>Limited based on vulnerabilities</td>
<td>Varied and independent of vulnerabilities</td>
</tr>
<tr>
<td>Available Tools</td>
<td>Publicly available</td>
<td>Specially created, customized, publicly available</td>
</tr>
<tr>
<td>Date of Initial Mandiant Observation</td>
<td>2012</td>
<td>At least 2006</td>
</tr>
<tr>
<td>Detected by Victim</td>
<td>75%</td>
<td>33%</td>
</tr>
<tr>
<td>Average Time Spent in a Victim Organization</td>
<td>28 days</td>
<td>243 days</td>
</tr>
<tr>
<td>Re-Compromise After the Initial Security Incident</td>
<td>Not witnessed</td>
<td>40% of cases</td>
</tr>
</tbody>
</table>

### Phishing Email Trends

- **44%** of observed phishing emails were IT related, often attempting to impersonate the targeted company’s IT department
- 93% of phishing emails were sent on weekdays
Major Financial Institutions Cyber

- Anthem
- Morgan Stanley
- Phishing
- United States
- J.P. Morgan Chase & Co.
- Insurance
- Federal Bureau of Investigation
- Experian
- Other

Colors:
- Anthem
- Morgan Stanley
- Phishing
- United States
- J.P. Morgan Chase & Co.
- Insurance
- Federal Bureau of Investigation
- Experian
- Other

Event Marker Size:
- 1 reference
- 4,728 references


Equifax, Experian and TransUnion are honing their focus to better handle disputes with consumers and to help victims of identity theft and fraud.
Industry Analysis - Healthcare

Healthcare or Healthcare Providers or "Healthcare" Cyber

National EMS attorney and course co-developer Ryan Stark remarked that “the data breaches in the news recently underscore how susceptible our information systems are, and the FBI specifically warned healthcare providers that hackers are targeting medical information.

The Federal Trade Commission received permission to proceed with its enforcement action against LabMD for an alleged healthcare privacy breach, according to a National Law Review report.

News that Community Health Systems suffered a breach by a purported “advanced persistent threat group originating from China” that affected 4.5 million patients illustrates yet again the healthcare sector’s vulnerability.

“Data breaches in retail, healthcare, financial services and other industries cause considerable economic damage, costing jobs, reputations and financial losses,” said Nat Kausik, CEO of Bitglass.

Former US Vice President Dick Cheney actually disabled the remote management on his pacemaker for fear of someone hacking into his healthcare provide and turning it off.

@bynd_news bynd_news: RedTapeChron: RT @wstein: PHI of 485K swiped in USPS data breach | Healthcare IT News http://t.co/IDOZ49vMIH.
Industry Analysis - Retail

Imagine you’re the CEO of a thriving company and you’ve been horrified by the news of the Sony hack, the Target breach and the litany of security issues that have plagued big companies in recent years.

@byod_news Westerangetap: Staples reveals consumer data breach at six nj locations - http://t.co/naf77Cylkz.

@id911 Texas banks confirm retail data breach, reissue thousands of cards http://t.co/3OgygNjU49.

'Sears' was also the victim of a suspected attack by cyber criminals.

Related posts: Walmart Warns of Phishing Scam The corporate giant has made a special effort to... Ransomware Decryption Scam Be on the lookout for scams offering 'cryptolocker decryption [...].
Different Cells
New Groups Emerging
Tools of the Trade

Usage example:
```
python sqlmap.py -u 'http://target/vuln.php?id=1' --batch
```

Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

Starting at 15:02:07:
```
[15:02:07] [INFO] testing connection to the target URL.
[15:02:07] [INFO] heuristics detected web page charset 'ascii'.
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of seconds.
[15:02:07] [INFO] Target URL is stable.
[15:02:07] [INFO] Testing if GET parameter 'id' is dynamic.
[15:02:07] [INFO] Confirming that GET parameter 'id' is dynamic.
[15:02:07] [INFO] Confirming that GET parameter 'id' is dynamic.
```
Black Shades RAT
Underground Economy

- **Drop Sites**
  - Phishing
  - Keyloggers

- **Botnet Service**
  - Botnet Owners
  - Spammers

- **Malware Distribution Service**
- **Data Acquisition Service**
- **Data Mining & Enrichment**

- **Data Sales**
- **Cashing**

- **Payment Gateways**
- **Validation Service (Card Checkers)**
- **eCommerce Sites**
- **ICQ**
- **Carding Forums**

- **eCurrency**
- **Bank**
- **Retailers**
- **Drop Service**
- **Gambling**
- **Wire Transfer**

- **Malware Writers**
- **Identity Collectors**
- **Credit Card Users**
- **Master Criminals**
HOW DO WE DEFEND AGAINST THESE ATTACKS
http://aws.amazon.com/security/security-resources/
Data Correlation is the Key
SIEM Operations

8.2 Million Per Day

40,000 Per Month
Enterprise Cyber Security Teams

- Monitor and Maintain non-managed hardware deployment uptime
- Collect and Maintain content for all non-managed devices
- Operational Implementation of all security infrastructure
- Network and Application Penetration Testing and Audit Team
- Cyber Security Awareness Program
- Incident Response Team

Process
- Response & process SLAs
- Change management
- Quality control

People
- Technical expertise
- Security training
- Management

Technology
- Client Security Portal
- Risk-based event correlation model
24x7 Security Operations Center

- Monitor intrusion detection and vulnerability scan activity
- Respond to incidents and provide ongoing tuning services as new threats appear
- Provide guidance on remediation when incidents are identified
- Detect Zero-Day and APT attacks
- Proactively monitor web application firewall
- Analyze incidents and escalate according to custom requirements
- Identify and implement required policy changes

Alert Logic
THREAT INTELLIGENCE
Honeypot Findings

• Highest volume of attacks occurred in Europe
• Attacks against Microsoft DS accounted for over 51% of the overall attack vectors
• Database services have been a consistent target
• 14% of the malware loaded on the Honeypots was considered undetectable by AV
• Underscores the importance of a defense in depth strategy for the need to secure your enterprise and cloud infrastructure
Samples of Malware detected

If an attacker were using the collected malware to launch an attack against an individual or an enterprise it would be theoretically run in this order.

1. Ping Sweep
2. Port Reconnaissance
3. Exploit a Vulnerability
4. Check for Shares or Networked Drives
5. Load Malware
6. Load Worm
7. Load Remote Access Trojan for full Control
Partnering with other Researchers
Open/Closed Source Intelligence

Attackers using Havex

Jan 2014: "In January of this year, the cyber security firm CrowdStrike...Havex Trojan From Russia?"

Mar 2014: "Since March 2014 the group has targeted the energy grid, major electricity firms and petroleum pipeline operators using a number of attack vectors, including the Havex Trojan which has infected industrial control systems, according to a report by Symantec Corp."

Jun 2014: "The department said last week it was investigating whether the Havex Trojan software had been involved in previous compromises of energy infrastructure."
Monitoring the Social Media Accounts
Following IRC and Forums

**Athena IRC Bot**

An IRC (Internet Relay Chat) bot that could steal file information, flood your network (DDOS) or any target sites with your zombie bots. The amount of Athena IRC bot is around $100 pre-configured bot per customer's request. $10 for rebuild and another $15 IRC setup via TeamViewer, join.me and PuTTY. In addition to that the bin settings has a capability or has a tool that could convert the encrypting the actual IP. The ability to download binaries (hosted elsewhere) and take over a target client to gain access/privileges.

The following PCAP sample triggered our IDS system to one of our customers.

```
JOIN #chatroom
_MODE #chatroom
+rt1vCvs...

NICK n[USA]/[M]
IN7p8b2c/0/zwuw
X[btm.

n[USA]/[M][WIN7]
x86[2c/0/zwuw0m!
rrrommmnj@brama.g
ongle.com J01
N #chatroom...
irc.private-life.biz 353 n[USA]/
DJWIN7/x86/2c/bz
zwuw0m @ #chatro
on:n[USA]...

e1ggyvvv@brama.g
ongle.com J01
N #chatroom:
irc.private-life,
biz 353 ...

What was identified:
- JOIN (command use to join a channel)
- #chatroom (existing chatroom)
- n[USA]/[M][WIN7]x86/2c/0/zwuw0m!rrrommmnj@brama.google.com (a possible target brute-forcing its way to the machine)
```
Tracking and Predicting the Next Move

- He is a guy from a European country/ (Russia)
- His handle or nick is madd3
- Using ICQ 416417 as a tool of communication (illegal transaction)
- A simple /whois command to the nick provided us with good information
- 85.17.139.13 (Leaseweb)
- ircname : John Smith
- channels : #chatroom
- server : irc.private-life.biz [Life Server]
- Check this out user has another room. #attackroom4
- We can confirm that Athena version 2.3.5 is being use to attack other sites.
- 2,300 infected Users
- Cracked Software is available in forums
- As of today 1 BTC to $618.00 or £361.66
Forums to Follow – Exploit.in

A US court on Friday sentenced a hacker from Estonia Sergey Churikov to imprisonment for 11 years for breaking into RBS WorldPay. Churikov convicted of cyber fraud and stealing $8.4 million from a bank branch Royal Bank of Scotland in Atlanta in 2008. Churikov sentenced to 11 years in prison and ordered to pay $8.4 million. The Government of Estonia in early May 2010 decided to give Churikova US authorities. In co-operation of the State Prosecutor’s Office and the Estonian Central Criminal Police, US law enforcement May 6, 2009 were arrested members of a group of international computer fraud. As found out a consequence, Churikov in early November 2008 hacked into the database of the company-operator debit cards RBS WorldPay one of the US banks. These data Churikov gave his partner Igor Grudiev, whose task was to record dumps resulting from burglary, on cards and then cash them in ATMs. Just for one day Ronald and Evelyn Choi, and Michael Evgenov removed from the accounts of different persons over 3.5 million CZK 10 000 Estonian kroner at a time in Tallinn. In the future, money from ATMs worldwide and received numerous other hired drops. Correspondent resident of Tallinn, while 35-year-old Sergey Churikov, a resident of St. Petersburg Victor Plescu and resident Oleg ovelline Chiasnau. The fourth key figure of the group took place on court documents as “Hecker 3”. Igor chest was accused of repeated forgery of means of payment for the purpose of use, the use of counterfeit payment instruments and computer fraud. He is sentenced to 5 years imprisonment with a probation period of 5 years. Eugene and Evelyn Choi charged with computer fraud and fraudulent use of payment instruments in large scales, Evelyn Choi was sentenced to 3 years imprisonment with a probation period of 3 years. Eugene - 2 years imprisonment with a probation period of 2 years. In November 2008, 12 hours more than 2100 ATMs in 280 cities around the world were received US $ 9 million. Crime seized the US, Estonia, Russia, Ukraine, Italy, Hong Kong, Japan and Canada. Withdraw money previously hired drops.

According to the company Damballa, the number of computers infected with malicious software Backoff, increased rapidly in North America. This malicious software used to steal information about credit cards. In Damballa observed 57% increase in activity in the period between August and September 2014. Backoff is used to scan memory and retrieval of data on credit cards. This was stated by the technical director Damballa Brian Foster (Brian Foster). Data are based on information collected from customers, businesses and Internet service providers, who use Damballa products to detect malicious software. "We take the domain names and IP-addresses that are looking for malicious software to calculate risk. The company monitors the number and characteristics of domain names associated with Backoff. Number of requests indicates growth of infected PC "-, said Brian Foster. - About 55% of the traffic, including DNS-queries, comes from North America. To preserve the privacy company is not interested in IP-addresses of most of these computers. Hadoop-cluster at
Stay Informed of the Latest Vulnerabilities

• Websites to follow
  – http://www.securityfocus.com
  – http://www.exploit-db.com
  – http://seclists.org/fulldisclosure/
  – http://www.securitybloggersnetwork.com/
  – http://nvd.nist.gov/
  – http://cve.mitre.org/
To Follow our Research

• Twitter:
  – @AlertLogic
  – @StephenCoty

• Blog:
  – https://www.alertlogic.com/resources/blog

• Cloud Security Report

• Zero Day Magazine
  – http://www.alertlogic.com/zerodaymagazine/
Thank you.