Cyber attacks against enterprises

What is the security posture of enterprises?
Does the investment pays off?

Equifax breach: basic security

Verizon partner data breach exposes millions of customer records
Accessed through an unprotected Amazon S3 storage server

City of Atlanta
$2.6M to recover from SamSam ransomware
Vulnerabilities and Malware

What is the patching behavior of enterprise client and server software?

What are the malware encounters?
Prior Work

Consumers

1 enterprise
85K hosts
4 months

[Nappa et al ‘15]

Servers

28K Enterprises
82M hosts
~3 years

[Yen et al ‘14]

[Rescorla ’03]
[Yilek ’09]
[Durumeric et al ‘14]
In this work

Malware Encounters

Patching Behavior

Internal

External
Symantec Datasets – Internal View

- 28K Enterprises
- 82M Hosts
- 67 Sectors
- 137 Countries
- ~3 years (Apr15 - Dec17)
Public Datasets

Outside View

- **Censys**
  - IPv4 scans
  - (Oct15 – Nov17)

- **38 Blacklists**
  - (Jul15 – Dec17)
  - Spam, Botnet infections, C&C

Other

- **NVD**
  - (Apr15 – Dec17)

- **VirusTotal**
Road Map – Malware Encounters

Malware Encounters

Internal

External

Patching Behavior
Only 27% of our queried hashes were found in VirusTotal

57% no AVClass families
## Family Classification – Winactivator

<table>
<thead>
<tr>
<th>Family</th>
<th>Type</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>opencandy</td>
<td>pup</td>
<td>1.1M</td>
</tr>
<tr>
<td>winactivator</td>
<td>malware</td>
<td>470.8K</td>
</tr>
<tr>
<td>installcore</td>
<td>pup</td>
<td>453.4K</td>
</tr>
<tr>
<td>autoit</td>
<td>malware</td>
<td>398.4K</td>
</tr>
<tr>
<td>remoteadmin</td>
<td>pup</td>
<td>333K</td>
</tr>
<tr>
<td>sogou</td>
<td>pup</td>
<td>282.8K</td>
</tr>
<tr>
<td>mictraylog</td>
<td>pup</td>
<td>264K</td>
</tr>
<tr>
<td>asparnet</td>
<td>pup</td>
<td>232.8K</td>
</tr>
<tr>
<td>elex</td>
<td>pup</td>
<td>218K</td>
</tr>
<tr>
<td>donex</td>
<td>pup</td>
<td>142.3K</td>
</tr>
<tr>
<td>dealply</td>
<td>pup</td>
<td>176.5K</td>
</tr>
<tr>
<td>nssm</td>
<td>malware</td>
<td>171.2K</td>
</tr>
<tr>
<td>ramnit</td>
<td>malware</td>
<td>142.3K</td>
</tr>
</tbody>
</table>

34% (9.4K) Enterprises

470K Hosts
Almost all enterprises will suffer at least one encounter in 3 years
Enterprises encounter malware much more often than PUP

PUP is less prevalent in enterprise than in consumer hosts

[Kotzias et al ‘16]
## Industry prevalence – Malware and PUP

### Industry Hosts

<table>
<thead>
<tr>
<th>Industry</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical Equipment</td>
<td>76.4%</td>
</tr>
<tr>
<td>Automobiles</td>
<td>75.5%</td>
</tr>
<tr>
<td>Construction Materials</td>
<td>74.4%</td>
</tr>
<tr>
<td>Marine</td>
<td>74.3%</td>
</tr>
<tr>
<td>Banks</td>
<td>15.7%</td>
</tr>
<tr>
<td>Consumer Finance</td>
<td>15.9%</td>
</tr>
<tr>
<td>Biotechnology</td>
<td>20.5%</td>
</tr>
<tr>
<td>Wireless Telecommunication</td>
<td>28.6%</td>
</tr>
</tbody>
</table>

Some industries are doing much better than others

4/10 least affected industries are finance-related
### Ransomware Case Study – Modest prevalence

- **Wannacry (worm/ransomware):**
  - Eternal Blue SMB patched in Windows 7
  - Enterprises with Windows XP affected

<table>
<thead>
<tr>
<th>Family</th>
<th>Hosts</th>
<th>Enterprises</th>
</tr>
</thead>
<tbody>
<tr>
<td>wannacry</td>
<td>30.1K</td>
<td>872</td>
</tr>
<tr>
<td>locky</td>
<td>20.3K</td>
<td>5.2K</td>
</tr>
<tr>
<td>petya</td>
<td>11.2K</td>
<td>155</td>
</tr>
<tr>
<td>ransomkd</td>
<td>10.2K</td>
<td>1.1K</td>
</tr>
<tr>
<td>teslacrypt</td>
<td>9.4K</td>
<td>2.9K</td>
</tr>
<tr>
<td>cryptolocker</td>
<td>8.7K</td>
<td>1.7K</td>
</tr>
<tr>
<td>cerber</td>
<td>6.1K</td>
<td>2.2K</td>
</tr>
<tr>
<td>cryptowall</td>
<td>2.6K</td>
<td>1.4K</td>
</tr>
<tr>
<td>dcryptor</td>
<td>2.0K</td>
<td>468</td>
</tr>
<tr>
<td>torrentlocker</td>
<td>785</td>
<td>443</td>
</tr>
</tbody>
</table>
Outside-in Perspective

Blacklists serve only for high-level perspective of the threat landscape

- Weekly basis
- IP blocks owned & cloud servers rented

IT Services sector

16 times more encounters from internal view
Road Map – Patching Behavior

Malware Encounters

Patching Behavior

Internal

External
Identifying Vulnerable client applications

12 applications

Google
Mozilla
Microsoft
Adobe
Oracle

Symantec

Identify application in File Appearance Logs

firefox.exe
2.1.3
10/02/2017

CVE-2009-0162: Apple Safari (safari.exe)

Kaplan-Meier Estimate for Vulnerability Decay

Time in Days
Survival Probability

Survival Analysis

National Vulnerability Database
Identifying Vulnerable Server Applications

112 applications (6 services)

Apache HTTPD
2.1.3
10/02/2017

Identify application in Protocol Baners

Survival Analysis

National Vulnerability Database

CVE

− 2009
− 0162 : Apple Safari (safari.exe)

Kaplan−Meier Estimate for Vulnerability Decay

Time in Days
Survival Probability
Vulnerability Lifecycle

- Application version released
- Vulnerability disclosed
- Patch deployment starts
- $t_v$
- $t_0$
- $t_p$
- $t_{50\%}$
- $t_{90\%}$
- 50% hosts patched
- Most hosts patched
**Client Side Vulnerabilities – 12 Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>90% Patched (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>72</td>
</tr>
<tr>
<td>Skype</td>
<td>89</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>234</td>
</tr>
<tr>
<td>Media Player</td>
<td>314</td>
</tr>
</tbody>
</table>

Over **6 months** on average to patch 90% of vulnerable population across all applications

Compare with consumer hosts

[Nappa et al. ‘15]

**Enterprises are slightly faster than consumers to patch applications**
Server Side Vulnerabilities – Patching behavior

Patching of enterprise clients better than enterprise servers

233 to 575 days for patching 90% of vulnerable hosts

216 to 287 days for patching 90% of vulnerable hosts

282 days for patching 90% of vulnerable hosts

200 days for patching 90% of vulnerable hosts

112 applications
Key Takeaways

Malware Encounters

- Almost all enterprises should expect a malicious appearance in 3 years
- Significant differences among industries

Patching Behavior

- Enterprise client patching better than consumers but still slow
- Server patching is worse than client patching
Mind your Own Business: A Longitudinal Study of Threats and Vulnerabilities

Platon Kotzias, Leyla Bilge, Pierre-Antoine Vervier, Juan Caballero
Survival Analysis

Survival Function

\[ S(t) = \Pr[T < t] = 1 - F(t) \]

Patching Milestones

\[ t_a = S^{-1}(1 - a) \]

Calculated from the inverse of the survival function

\[ t_{90\%} = S^{-1}(0.1) \]

OS upgrade behavior

43% of enterprises with at least one Windows XP machine in 2017
Client Side Vulnerabilities – By Industry

- Using the 5 most prevalent applications (IE, Chrome, Adobe Reader, Firefox, JRE)

<table>
<thead>
<tr>
<th>Industry</th>
<th>90% Patched</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunication Services</td>
<td>141</td>
</tr>
<tr>
<td>Consumer Finance</td>
<td>152</td>
</tr>
<tr>
<td>Communications Equipment</td>
<td>152</td>
</tr>
<tr>
<td>Multiline Retail</td>
<td>193</td>
</tr>
<tr>
<td>Construction Materials</td>
<td>187</td>
</tr>
<tr>
<td>Gas Utilities</td>
<td>197</td>
</tr>
</tbody>
</table>

- Finance, Software and Communications are faster
- Invest more in cyber security products
- Some industries are worse than consumer hosts
Ransomware over time

Locky

Wannacry and Petya

Hosts

Enterprise
Client Side Vulnerabilities - Best and worst

- Compare patching time among enterprises with more than 1K hosts

**TOP 10**

Patch 90% of machines in < 10 days

Most in Financial and Insurance industry

Best patcher from the Hotels, Restaurants and Leisure industry

**Bottom 10**

Patch 90% of machines in 500 days

Spread in multiple industries: Media, Healthcare etc.

Worst patcher from the Capital Market industry

Best patchers have less malware encounters than worst patchers
## Industry Sector Coverage – Top 15 Industries

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>Enterprises</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>1.1K</td>
<td>16.6M</td>
</tr>
<tr>
<td>IT Services</td>
<td>1.0K</td>
<td>7.5M</td>
</tr>
<tr>
<td>Healthcare Services</td>
<td>1.1K</td>
<td>6.5M</td>
</tr>
<tr>
<td>Professional Services</td>
<td>875</td>
<td>3.8M</td>
</tr>
<tr>
<td>Commercial Services</td>
<td>1.2K</td>
<td>3.2M</td>
</tr>
<tr>
<td>Insurance</td>
<td>597</td>
<td>3.2M</td>
</tr>
<tr>
<td>Capital Markets</td>
<td>851</td>
<td>2.0M</td>
</tr>
<tr>
<td>Software</td>
<td>832</td>
<td>2.0M</td>
</tr>
<tr>
<td>Electronic Equipment</td>
<td>1.0K</td>
<td>1.7M</td>
</tr>
<tr>
<td>Machinery</td>
<td>1.4K</td>
<td>1.5M</td>
</tr>
<tr>
<td>Specialty Retail</td>
<td>601</td>
<td>1.5M</td>
</tr>
<tr>
<td>Constructions &amp; Engineering</td>
<td>1.3K</td>
<td>1.1M</td>
</tr>
<tr>
<td>Media</td>
<td>971</td>
<td>1.5M</td>
</tr>
<tr>
<td>Chemicals</td>
<td>850</td>
<td>1.0M</td>
</tr>
<tr>
<td>Food Products</td>
<td>846</td>
<td>872K</td>
</tr>
</tbody>
</table>