The Anatomy of IoT Security

Satyajit Sinha
Research Analyst
IoT and Mobility
Mission

We help our partners make decisions with accurate data, delivered in timely manner.

Research Activities

- Connected devices, digital consumer goods, software & applications
- Emerging and disruptive technologies
- Internet of Things (IoT)
- Tailored research as well as syndicated reports
- Seminars and workshops
- Consulting and customized projects
Key IoT Denominators

1. One billion cellular-IoT connections by 2020

2. Four Pillars of security: Hardware, Software, Network and Cloud

3. Three major verticals under threat - Connected Car, Healthcare and Smart Cities

4. Understand: Cybercrime is a ‘Business’, not just a ‘System Glitch’
IoT Ecosystem and Evolution

Internet of Things

Intelligent Internet of Everything
Malware is Eating IoT World
Mirai: Turning point of IoT Security

Rise of Malware in M2M/IoT Devices
(number of Malware, in million)

- Gameover Zeus
- Malware Dominated By Ransomware
- Driven by Mirai
- Driven by Mirai 2.0 (OMG)

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Existed</th>
<th>New Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1Q2014</td>
<td>179</td>
<td>27</td>
</tr>
<tr>
<td>2Q2014</td>
<td>215</td>
<td>28</td>
</tr>
<tr>
<td>3Q2014</td>
<td>215</td>
<td>37</td>
</tr>
<tr>
<td>4Q2014</td>
<td>286</td>
<td>48</td>
</tr>
<tr>
<td>1Q2015</td>
<td>382</td>
<td>36</td>
</tr>
<tr>
<td>2Q2015</td>
<td>426</td>
<td>23</td>
</tr>
<tr>
<td>3Q2015</td>
<td>460</td>
<td>33</td>
</tr>
<tr>
<td>4Q2015</td>
<td>472</td>
<td>35</td>
</tr>
<tr>
<td>1Q2016</td>
<td>491</td>
<td>33</td>
</tr>
<tr>
<td>2Q2016</td>
<td>544</td>
<td>25</td>
</tr>
<tr>
<td>3Q2016</td>
<td>572</td>
<td>21</td>
</tr>
<tr>
<td>4Q2016</td>
<td>589</td>
<td>29</td>
</tr>
<tr>
<td>1Q2017</td>
<td>595</td>
<td>49</td>
</tr>
<tr>
<td>2Q2017</td>
<td>643</td>
<td>55</td>
</tr>
<tr>
<td>3Q2017</td>
<td>684</td>
<td>56</td>
</tr>
<tr>
<td>4Q2017</td>
<td>710</td>
<td>56</td>
</tr>
</tbody>
</table>

© 2018 Counterpoint
Malware attack not limited to online: BlueBorne Attacks via Bluetooth

According to Armis “In 2017, BlueBorne was estimated to potentially affect over 8.2 billion devices worldwide including laptops, smart cars, smartphones and wearable gadgets”
Ransomware: The latest Threat
Rise of Ransomware
(number of Malware, in million)

- **Ransom Denial of Service (RDoS)** made a significant comeback in Q3 2017
- A widespread wave of RDoS threats from the Phantom Squad hacker group kicked off in September 2017
End to End Security: Key to Secure IoT Data
End to End IoT Security and Threats

IoT Network Security
- Man in the Middle
- DDoS/RDoS
- Virus (Trojans)

IoT Hardware Security
- Low Cost Hardware Tampering
- Fake ADAS message sent V2V or V2X.
- Malicious data manipulation cause traffic outages

IoT Cloud Security
- Insecure APIs
- Service Traffic Hijacking
- Data Breach /Data Loss

IoT Software Security
- Buffer overflows
- Malware
Major Vendors and their Specialisation - 1

**IoT Hardware Security**
- SecureRF
- Sequitur Labs
- Rambus
- NXP
- Atmel
- Microchip
- arm
- ST

**IoT Software Security**
- Qadium
- 1010DATA
- Cockroach Labs
- accelerite

**IoT Network Security**
- Cloudflare
- keeze
- FILAMENT

**Embedded**
- avast
- baimos technologies
- Lookout
- Skycure
- Kaspersky
- Zimperium
- TRUSTiONIC

**Mobile**
- RedLock
- skyhigh
- afero
- evident.io

**Vehicles**
- Trillium
- CujoAI
- MOCANA
- ARGUS CYBER SECURITY
- Bayshore
- IoTium
- sentryo
- mPrest SYSTEMS LTD

**Database**
- Twistlock
- Attify
- aqua
- appthority
- A pareto
- TRUSTiONIC

**Application**
- Cylance
- Duo Security
- Morphisec
- Crowdstrike
- Webroot
- Bastille
- Mobilium

**Gateway/Router**
- Nozomi Networks
- SCADAfense

**End Point**
- Bastille
- Mobilium

**Network Visibility**
- Bastille
- Mobilium

© 2018 Counterpoint
### Perimeter and Network

<table>
<thead>
<tr>
<th>Firewall</th>
<th>NGFW</th>
<th>IDS</th>
<th>IPS</th>
<th>VAS</th>
<th>Antivirus</th>
<th>Malware</th>
</tr>
</thead>
</table>
| BROCADE | Check Point | KISMET + SOLUTIONS | WIRESHARK | Qualys | McAfee | VIX INTER 
| Barracuda | Juniper | SNORT | IBM | ALERT LOGIC | Symantec | VMRAY |
| Cyberoam | SURICATA | OSSEC | SNORT | Tenable | McAfee | 
| VAS | Antivirus | Malware | McAfee | Symantec | McAfee | 

### Application and Endpoint

<table>
<thead>
<tr>
<th>EDR</th>
<th>Certificate Manager</th>
<th>WAF</th>
<th>PT</th>
<th>Web Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee</td>
<td>zscaler</td>
<td>BROCADE</td>
<td>IMPERVA</td>
<td>Hewlett Packard</td>
</tr>
<tr>
<td>Symantec</td>
<td>OUTLIER</td>
<td>Barracuda</td>
<td>Trustwave</td>
<td>Enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>netsparker</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AppScan</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IBM Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>zscaler</td>
</tr>
</tbody>
</table>

### Data Security

<table>
<thead>
<tr>
<th>iDaas</th>
<th>FIM</th>
<th>DB VAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centrify</td>
<td>tripwire</td>
<td>GREEN SQL</td>
</tr>
<tr>
<td>onelogin</td>
<td></td>
<td>OSSEC</td>
</tr>
<tr>
<td>okta</td>
<td></td>
<td>IBM</td>
</tr>
</tbody>
</table>

### GRC and Audit

<table>
<thead>
<tr>
<th>GRC</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreadFix</td>
<td>OPTIV</td>
</tr>
<tr>
<td>RSA</td>
<td></td>
</tr>
<tr>
<td>MetricStream</td>
<td>Open-Audit</td>
</tr>
<tr>
<td>TRIPLE HELIX</td>
<td></td>
</tr>
</tbody>
</table>

### Security Orchestration

<table>
<thead>
<tr>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>netflexity</td>
</tr>
<tr>
<td>CloudPassage</td>
</tr>
<tr>
<td>AVANAN</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
</tbody>
</table>
Key Solution Against Threats
ARM Trust Zone + Platform Security Architecture

For: Ultra Low Power Processor

For: High Performance

Is Trust Platform Module Good Enough?

ARM Cortex®-M23

TrustZone for ARMv8-M

CPU

ARMv8-M Baseline

Memory Protection Unit

AHBS

ETM Trace

Fast I/O Port

Nested Vectored Interrupt Controller

Wake-up Interrupt Controller

Data Watchpoint

Breakpoint Unit

Serial Wire

ARM Cortex®-M33

TrustZone for ARMv8-M

CPU

ARMv8-M Mainline

Memory Protection Unit

DSP

FPU

2x AHBS

ITM Trace

Breakpoint Unit

Serial Wire

Coprocessor Interface

ETM Trace

MTB Trace

Analyse

Threat Models and Security Analysis.

Architect

Architecture specifications.

Implement

Source code (OSS) and Hardware IP.
Data Breaches Continue to Escalate

• The solution detects threats using analytics on a Hadoop based platform and correlates messages from multiprotocol signalling data. Real-time threat protection is available using firewalling at the interconnecting points.
• The one of the few vendors that initiated the adoption of artificial Intelligence and machine learning in network security.
Future of IoT Security
AI and Machine learning in Security: Plays important role on both sides

AI could go beyond monitoring and will provide a competitive edge to defenders that have primarily been absent from most cybersecurity technologies to date.

On the flip side, attackers may deploy AI that will initiate automated hacks that are able to study and learn about the systems they target, and identify vulnerabilities, on the fly.
Future of IoT Security: Blockchain

- In case of IoT, the blockchain will require infrastructure to manage device authentication, security and control layers, which is considerably more complex.
- **Asset tracking** – Chronicled A new pharmaceutical seal from Chronicled combines NFC chips with blockchain to track and secure prescription drugs.

Chronicled asset tracking blockchain concept showing single application Crypto Seal
The Upcoming Epidemic
Connected Car In-security:

- In 1Q2010, more than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control.
- On 20th Feb 2018, Tesla Cloud Servers Hacked By Cryptojackers. The hackers weren’t content just to steal the sensitive data they found, so they also installed some cryptocurrency mining clients.

Fast and Furious car hack stunt, may turn real
Security in IoT Healthcare: Major Breach

- The recall of the Abbot cardiac devices was the key moment in the evolution of connected medical devices.
- Although there have been no reports of actual harm to patients due to hackers exploiting the vulnerabilities in the devices, that number can go from zero to a lot of patients quickly if hackers decide to launch attacks.
1. Hacks to continue
   - Default credentials (the easiest path) used frequently
   - Evolution: Hackers will find other entry points
   - Malware is currently basic – But more professional and well-funded attackers in future

2. More collaborations like “Cyber Threat Alliance” with concerted offerings
   - Next gen offerings will fight malwares and botnets and learn/evolve on their own

3. AI, ML and Blockchain will open doors for Intelligent Internet of Everything (IIoE)
   - AI rewriting its own code to self-evolve and defend against ‘advance intelligent attacks’ in future