Defending Airports Against Emerging Ransomware Attacks

Ayed Al Qartah
Security Technical Solutions Architect
Cisco Systems
Attack landscape constantly evolving

Advanced Persistent Threats
Supply chain attacks

Unpatched Software
Ransomware

Spyware/Malware
Data/IP Theft

Wiper Attacks
Malvertising

Phishing
Drive by Downloads

Man in the Middle
Rogue Software

DDoS
Botnets

Cryptomining
Credential compromise
Cleveland Hopkins Airport affected by ransomware attack

Cleveland Hopkins International Airport has been target of more cyber attacks, but security upgrades blocked them

Cyber attack led to Bristol Airport blank screens

Louisville Regional Airport Authority grounded by ransomware attack

Airports are ill-equipped to deal with a major cyber attack, says consultancy firm

The World’s Busiest Airport Shuts off Wi-Fi Amid a Ransomware Attack

Kolkata: 4,000 flyers stranded as cyber attack led to delay of 30 flights

Ukraine govt, banks & airports hit by mass ransomware attack

Ukraine says to review cyber defences after airport targeted from Russia
Aviation Cybersecurity: Major Challenges
Key assets supporting the daily airport operation

- **IT and Communications including internal and external infrastructure:**
  - Internal: Lan, VPN, IT equipment, Mobile network and apps, passenger WIFI, SOC, Flight Display Systems.
  - GPS, cloud-based data, Network Security Management, WAN, Air to satellite communication systems, GIS, etc.

- **Airline / Airside Operations:** including among others – air traffic management, flight tracking systems, departure control systems, airfield lighting and runway control and monitoring, cargo processing, aircraft re-fuelling, etc.

- **Landside Operations:** including the landside operations systems control center, fuel management, lighting detection systems, parking management systems, etc.

- **Safety and Security:** access control systems, authentication systems, baggage screening and handling systems, surveillance systems, passenger screening, perimeter intrusion detection, emergency response, firefighting, etc.
Key assets supporting the daily airport operation – cont.

- **Customer Ancillary Services:** Cashpoint terminals, mobile payments, point of sales (PoS), duty free, catering, etc.

- **Facilities and Maintenance:** airport vehicle maintenance, building management and control systems, energy management systems, lifts and escalators, SCADA (utilities, roads, ancillary areas), environmental management systems, etc.

- **Passenger Management Systems:** kiosk devices, e-ticketing, electronic visual information display systems, passenger check-in and boarding, central reservation systems, etc.

- **Staff Management:** staff records management, authentication systems, mobility-enabled applications.
Taxonomy of threats to the cyber security of Smart airports

**Human Errors**
- Configuration errors
- Operator/user errors
- Loss of hardware
- Non compliance with policies or procedures

**Third Party Failures**
- Internet service provider
- Cloud service provider (IaaS / PaaS / SaaS)
- Utilities (power / gas / water)
- Remote maintenance provider
- Security testing companies

**Malicious Actions**
- Denial of Service attacks
- Exploitation of (known or unknown) software vulnerabilities
- Misuse of authority / authorisation
- Network/interception attacks
- Social attacks
- Tampering with devices
- Breach of physical access controls / administrative controls
- Malicious software on IT assets (including passenger and staff devices)
- Physical attacks on airport assets

**System Failures**
- Failures of devices or systems
- Failures or disruptions of communication links (communication networks)
- Failures of parts of devices
- Failures or disruptions of main supply
- Failures or disruptions of the power supply
- Malfunctions of parts of devices
- Malfunctions of devices or systems
- Failures of hardware
- Software bugs

**Natural Phenomena**
- Earthquakes
- Floods
- Solar flare
- Volcano explosion
- Nuclear incident
- Pandemic (e.g. ebola)
- Industrial actions (e.g. strikes)
- Fires
- Shortage of fuel
- Space debris & meteorites
- Dangerous chemical incidents
Ransomware

Malicious Software

Encrypts Critical Data

Demands Payment
Ransomware

• Ransomware is the most profitable type of malware in history.

• Ransomware has changed the game from stealthy undetected access to extortion.

• Ransomware uses traditional malware attack vectors such as phishing emails, known vulnerabilities, and exploit kits to deliver the ransomware to a desktop.

• Ransomware communications include command and control (C2) callback methods for obtaining encryption keys and payment messaging are mostly using DNS.
The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.
Ransomware Email and Web Delivery

Web Server
- Compromised Site or Malvertising

Web Link
- Email Attachment

Email
- Phishing or Spam

Web Redirect

Exploit Kit Domains

Encryption Key Infrastructure

C2

File drop

Malicious Infrastructure

Ransomware Payload
# Ransomware and DNS

<table>
<thead>
<tr>
<th>NAME*</th>
<th>DNS</th>
<th>IP</th>
<th>NO C2</th>
<th>TOR</th>
<th>PAYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locky</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>SamSam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>TeslaCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>CryptoWall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>TorrentLocker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>PadCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>CTB-Locker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>FAKBEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>PayCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>KeyRanger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
</tbody>
</table>

## Encryption Key

- **VPN**: No specific entry for VPN in the table.

## Payment MSG

- **VPN**: No specific entry for VPN in the table.
Dear customer,

We want to use this opportunity to first say “Thank you very much for your purchase!”

Attached to this email you will find your invoice.

Kindest of regards,
your Amazon Marketplace

G

[commMgrHndTokenGJARWGBKBYKON]

---------- End message ----------

P

For Your Information: To help arbitrate disputes and preserve trust and safety, we retain all messages buyers and sellers send through Amazon.com. This includes your response to the message below. For your protection we recommend that you only communicate with buyers and sellers using this method.

Important: Amazon.com’s A-to-z Guarantee only covers third-party purchases paid for through our Amazon Payments system via our Shopping Cart or 1-Click. Our Guarantee does not cover any payments that occur off Amazon.com including wire transfers, money orders, cash, check, or off-site credit card transactions.

Rc

[commMgrTokiGJARWGBKBYKON]
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7XXXXXXXXX BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   NjjXXXXXXXXX P5

If you already purchased your key, please enter it below.

Key:
Bristol Airport Ransomware Incident – Sept 2018
Capabilities needed to break the kill chain

- Threat intelligence – Knowledge of existing Ransomware and communication vectors
- E-mail security – Block Ransomware attachments and links
- Web Security – Block web communication to infected sites and files
- DNS Security - Break the Command & Control call back
- Client Security – Inspect files for Ransomware and Virus’s, quarantine and remove
- Segment infrastructure – Authenticate access, separate traffic based on role and policy
- Intrusion Prevention - Block attacks, exploitation and intelligence gathering
- Monitor Infrastructure communications – Identify and alert on abnormal traffic flows
Capability Defense against the “Kill Chain”
Final thoughts

- Commercial airlines and other transportation providers present a tempting target for cybercriminals.

- As technology adoption evolves in the civil aviation industry, it will have to invest in smarter, safer digital infrastructure that leverages machine learning, integrated cyber security architecture, and threat intelligence to thwart attacks and ensure that its critical systems are protected and always available.
Questions?
North American
Central American
and Caribbean
(NAAC) Office
Mexico City

South American
(SAM) Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
(WACAF) Office
Dakar

European and
North Atlantic
(EUR/NAT) Office
Paris

Middle East
(MID) Office
Cairo

Eastern and
Southern African
(ESAF) Office
Nairobi

Asia and Pacific
(APAC) Sub-office
Beijing

Asia and Pacific
(APAC) Office
Bangkok

THANK YOU