Cyber Threats to Transportation

Bruce Moran, TSA Information Assurance and Cybersecurity Division

Transportation Security Administration

TSA Environment

Internal TSA IT Infrastructure – Office of Information Technology

Headquarters & Field Office IT Systems

Passenger & Baggage Screening Equipment

TSA Network

Connectivity to Other Stakeholder Networks

- 65,000 users in CONUS/OCONUS locations
- Over 36,000 endpoints
- Over 70 unique systems supporting mission operations and public screening and vetting
- Two million passengers daily from 433 U.S. airports and 250 foreign airports with direct service to the U.S.
- Classified and unclassified environments to support threat identification
- Over 25M continuously vetted individuals allowing access to critical transportation infrastructure

Current Cyber Threat Environment

In the News

Cyber raises threat against America's energy backbone

Brussels attacks expose gaping hole in airport security nets

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Aviation industry's risk of cyber attack is on the rise

Gas industry says 'trust us' on tracking cyberthreats

Brussels airport closed for fear of terror attack and power failure

Slim TSA cyber staff takes on rising pipeline threat

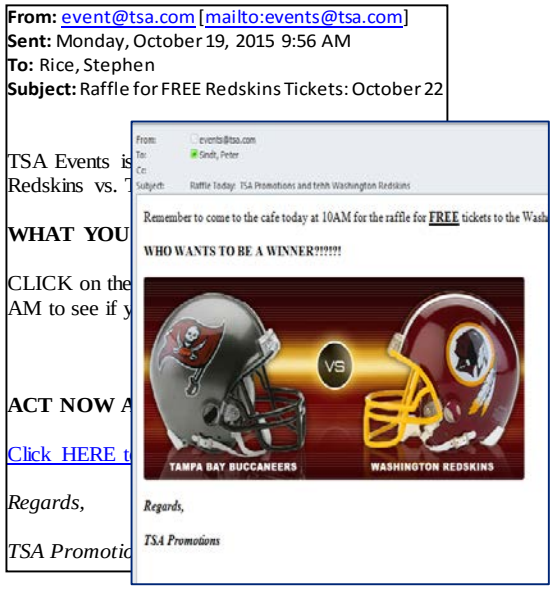
'Dirty bomb' threat shuts down Port of Charleston terminal

Man who drove through BWI airport fence made it onto airplane before being detained, police confirm

State of TSA Cybersecurity

TSA Internal Cybersecurity Statistics

- 8,456 total users targeted with phishing from Jan 2015 – Jun 2017
- ~16.5B events processed by security tools each month
- 294 cases requiring forensic analysis during 2016
- Performed reverse engineering on 8 custom pieces of malware in 2016
- Performed multiple Insider Threat assessments in 2016



Spearphishing testing for employees

IDENTIFY

- Entire enterprise scanned monthly
- Evaluation of all FISMA systems and designation of high value assets (HVAs)

PROTECT

- Monthly patching following DHS **Info Sec Vulnerability Management (ISVM)** program
- Dual factor authentication for privileged and unprivileged users

DETECT

- 24X7 **Security Operations Center (SOC)** monitoring and analysis with Security Information & Event Management tools
- SOC **team** gathers threat intelligence and tracks incidents

RESPOND

- TSA **Computer Security Incident Response Team (CSIRT)** fields security incidents 24x7
- **Focused Operations (FO)** team performs forensic investigations and impact assessments

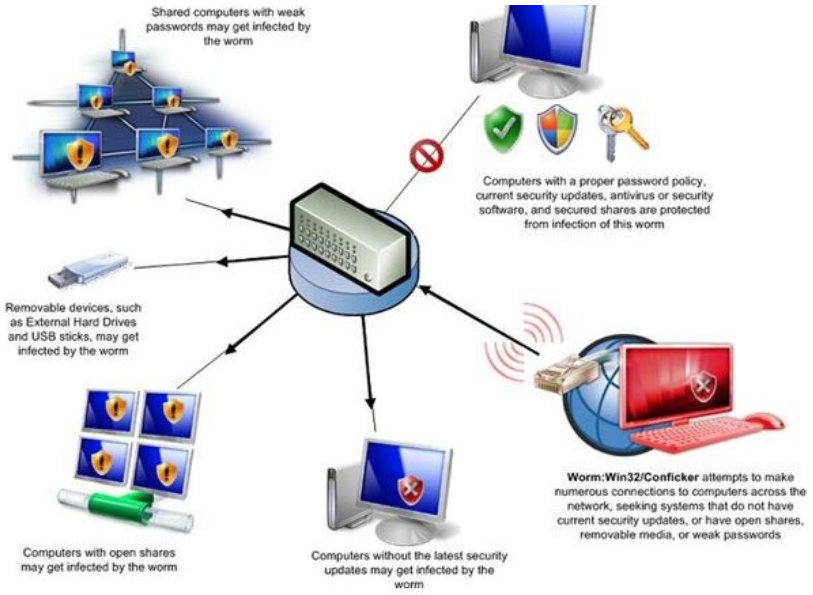
RECOVER

- Establishing OIT **Command Incident Center (CIC)** to enhance monitoring and response time
- OIT **Government Watch Officers (GWO)** coordinate and lead incident recovery efforts

The Threat is Real

Worm (Malware): Self-propagating program that spreads rapidly without user intervention

- Exploits unsecure systems, USB devices, or open network shares
- Usually has malicious payload attached (Worm is just the carrier)
- Can spread via Email, Chat, Web Servers, or network communication services
- Can be tailored to infect only when certain criteria met (i.e. Stuxnet – Targeted Iranian SCADA systems)



Ransomware: Malware that restricts access to the compromised systems until a ransom demand is satisfied

- WannaCry
- Petya