P2P as a corporate *persona non grata*

LOCKHEED MARTIN

John Alexander
Anti-Virus Technical Lead
Endpoint Data Protection
Lockheed Martin

Breaking News

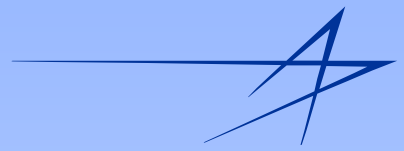
- **Presidential Helicopter – Marine One**
- **A security company discovered a breach involving the transfer of military information to an Iranian IP address.**
- **A defense contractor in Bethesda, MD had a file-sharing program on a system that contained planned engineering blueprints, upgrades, avionic schematics, and computer network information for Marine One.**

LOCKHEED MARTIN

Not Involved

Image: http://en.wikipedia.org/wiki/File:VH-60_Marine_One.jpg

P2P Key Points



- Decentralized
- Chunked Data
- Searchable
- Very Popular
- Widely Available
- Many Versions
- Many Vectors
- User Driven Content
- Accountability?
- Anonymous?
- Encrypted?
- Private?

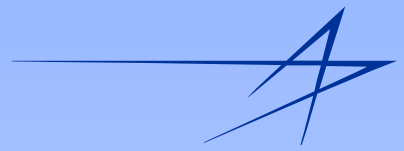
Risk Categories

- Confidentiality
  - Required Sharing
  - Encryption
  - Identity
- Integrity
  - Vulnerabilities
  - Backdoors
  - Malware Seeding
- Availability
  - Bandwidth
  - Copyrighted Material
  - Unlicensed Software

Risk Level Assessment Model

Criteria	Low	Medium	High
P2P Installed	No	Yes	Yes
P2P Running	No	No	Yes
Data Exposure	No	Limited	Yes
Repeat Offender	1st	1st	2nd +
Data Classification	N/A	Public Limited	Classified Sensitive
Malware Detected	No	No	Yes

Controls



- Confidence
  - Unknown
  - Low
  - High
  - False Positives
- Theme
  - Information Reuse
- Objectives
  - Clients
  - Communication
  - Content
- Types
  - Enforced
  - Informational
  - Ad Hoc
  - Other

Challenges

- Management
- Policy
- Technical
- Human
- Vendor

Management Challenges

- Terminology
  - P2P vs LMP2P
- Reporting
  - Centralize
- Sharing Success
  - Not P2P
  - But Still Unwanted

Policy Challenges

- **Banning P2P**
  - **Define P2P**
  - **Not Malware**
- **Information Assurance**
  - **Information Classifications**
  - **Defining Risk**

Technical Challenges

- Sources
- False Positives
  - 3 Strikes
- Detection
  - Darknets
  - Enabling Technologies
- Tool Limitations
  - Capabilities
  - Control Interactions
  - Not Enforceable
  - Latency in Reporting
  - Tagging

Human Challenges

- User Cooperation
- Recidivism
- Communication
- Education

Vendor Challenges

- P2P Categories
- Terminology
  - Threat Naming

Recommendations

- **Risk Assessment**
- **Controls**
- **Other**

Risk Assessment Recommendations

- Centralized Reporting
- Levels of Risk
- Defining Risky Software
- Control Confidence

Control Recommendations

- Network Scanners
  - Software Inventory
  - Vulnerability
  - Intrusion Detection
- Malware Detections
  - Hitchhikers
  - Squeaky Wheels
  - Mobile & Remote Stroage
- Files
  - File Names
  - Name Space Collisions
  - Wild Cards
  - File Types
  - Key Words
  - Identifiable Information

Control Recommendations

- Web Proxies
  - Content Categories
  - User Agent Strings
  - Data Mining
  - Authentication
- Email Gateways
- Remediation
  - Forensic Analysis
  - User Interviews

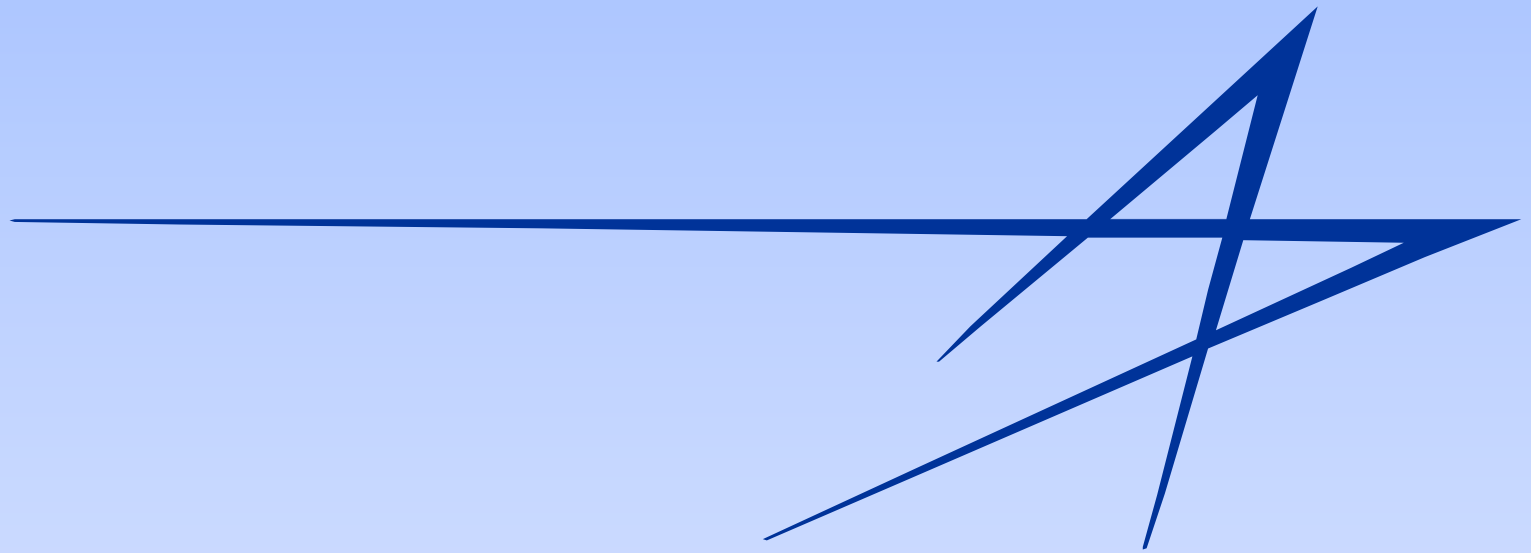
Other Recommendations

- Repeat Offenders
- Communication
- Product Development
  - P2P PUP

Conclusion

- Management Support
- Clear Policies
- Risk Benefit Analysis
- Protect Your Data

Questions?



Thank You

- Rick Genesi
- Andrew Maguhn
- Chad Anderson
- James M Wolfe
- Ken Bechtel
- Greg Edwards
- Joseph Howell