MALWARE

HARDWARE

SOFTWARE

HUMAN

NETWORK

CONTENTS
CYBER AWARENESS UPDATE

- Operation reveals several new malware variants in the wild
  - FBI took down password-protected, “vetted” hacking and cybercrime forum
  - 20 nations involved, 70 arrests
- Examples
  - Dendroid: affects Google Android phones
  - Facebook Spreader: infects Facebook users’ computers
  - Spam bots designed to target cellphone users
  - Butterfly bot: targets financial information
- Mitigation
  - Antivirus updates and safe computing

July 15: FBI announces that it has concluded the largest ever coordinated law enforcement effort against an online criminal forum. New vulnerabilities disclosed as a result.

Resources:
- ANTLabs InnGate: https://www.us-cert.gov/ncas/bulletins/SB15-194

HARDWARE

- Allows attacker to inject arbitrary code
- Attacker may obtain admin credentials
- Versions affected:
  - InnGate 3.01E
  - InnGate 3.10E
  - InnGate 3.10M
  - SG4
  - SSG 4
- Mitigation
  - Firmware update has been released
KEY POINTS

• Vulnerability allows remote attacker to execute arbitrary files
• Versions affected:
  ○ Samsung Galaxy S5
• Mitigation
  ○ Firmware update has been released

SOFTWARE
Oracle
Software developer best known for its Solaris operating system and database management systems. MySQL, the world’s most widely used open-source database management system, is in the world.

KEY POINTS

• Oracle released security fixes for 193 vulnerabilities
  ○ 63 products affected
  ○ Releases patches quarterly. This quarter’s release was on July 14
• Mitigation: Review and install security patches as needed

HARDWARE
Samsung Galaxy S5
Released by Samsung in April 2014.

Resources:
https://www.us-cert.gov/ncas/bulletins/SB15-194

Resources:

JULY 2015
https://www.us-cert.gov/ncas/bulletins/SB15-194

JULY 2015

JULY 2015

JULY 2015
Microsoft released security updates for multiple products:
- 14 vulnerabilities covering 84 software implementations
- Releasewas on July 14
- Mitigation: Review and install security patches as needed

Firefox - Vulnerable Versions before version 39.0
- Allow denial of service
- Possibly executing arbitrary code
- May allow attacker to obtain sensitive information from memory
- Mitigation: Update/Patch

Internet Explorer versions 6-11
- Allow denial of service
- Possibly executing arbitrary code
- Mitigation: Update/Patch
**KEY POINTS**

- **Multiple versions allow remote attackers to bypass protection and write to file system**
- **Vulnerable versions**
  - Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.180 on Windows and OS X and before 11.2.202.481 on Linux
  - Adobe AIR before 18.0.0.180
  - Adobe AIR SDK before 18.0.0.180
  - Adobe AIR SDK & Compiler before 18.0.0.180
- **Mitigation**
  - Update/patch

**SOFTWARE**

**Adobe Flash Player**

- Freeware software for using content created on the Adobe Flash platform, including streaming video and audio.
- Can run from a web browser as a browser plug-in or on supported mobile devices.

**Resources**


**KEY POINTS**

- Two related incidents:
  - April 2015: 4.2 million current and former federal employees impacted. Notifications were sent to those affected.
  - June 2015: OPM discovered an additional compromise affecting 21.5 million individuals. Notifications for this incident have not yet begun.
- Current and former federal employees, contractors, job candidates, spouses, and co-habitants and family members may be impacted.
- **Mitigation**
  - Currently, there is no record of misuse of data
  - Monitor credit, bank, and financial records
  - Be aware of phishing attempts
  - Think cybersecurity
  - Keep up to date: [https://www.opm.gov/cybersecurity/](https://www.opm.gov/cybersecurity/)

**OPM Cybersecurity Incidents**

- OPM recently announced two data breaches that may have involved personally identifiable information. The investigation is ongoing.
- [https://www.opm.gov/cybersecurity/](https://www.opm.gov/cybersecurity/)
KEY POINTS

- Attacker can upload and execute malicious scripts
  - Authentication is not required to exploit
- Vulnerable versions
  - Storage Manager
- Mitigation: Hotfix is available from the vendor

Develops enterprise-level infrastructure management software, particularly network monitoring software.

Resources:

https://www.us-cert.gov/ncas/bulletins/SB15-194

A network is information systems implemented with a collection of interconnect components. Such components may include routers, switches, cabling, telecommunication, controllers, key distribution centers and technical control devices.

KEY POINTS

- Multiple vulnerabilities in multiple products
  - Access server, web security system, wireless systems, etc.
  - Allows remote attacks, sessions hijacks, file uploads, script injection, denial of service, and other attacks.
- Vulnerable versions
  - Cisco Unified Communications Manager 10.5
  - Cisco Email Security Appliance 8.5.6-073, 8.5.6-074, and 9.0.0-461
  - Cisco WebEx Meeting Center
  - Cisco Unified Computing System software 1.5(3) and 1.6(0.16)
  - Multiple others
- Do you know hardware configuration? Does it impact you?
- Mitigation: Update
KEY POINTS
- Multiple vulnerabilities in multiple products
  - Allows remote attacks, session hijacks, file uploads, script injection, denial of service, and other attacks.
- Vulnerable versions
  - Juniper SRX Series gateways
  - Multiple versions Juniper OS
- Hardware/Software baseline, Configuration management.
- Mitigation: Update

Network is information systems implemented with a collection of interconnect components. Such components may include routers, nubs, cabling, telecommunication, controllers, key distribution centers and technical control devices.

“WHAT DO I NEED TO DO?”

Recommendations

1. Form a relationship/partnership with your IT and cybersecurity departments
2. Know what’s on your network (hardware and software)
3. Review/sign up for alerts through US CERT
4. Use CDSE resources, such as webinars, free eLearning courses, and more

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” – Bruce Schneier

CDSE: http://www.cdse.edu
US CERT Bulletins: https://www.us-cert.gov/ncas
Internet Crime Complaint Center: http://www.ic3.gov/default.aspx

QUESTIONS/COMMENTS:
CYBERSECURITY.TRAINING@DSS.MIL
THANKS FOR JOINING US!  
CHECK OUT OUR UPCOMING WEBINARS:

- RMF Steps 1-6 Course: July 2015
- Additional OBMS Job Aids and resources coming in August 2015