A fairly new ransomware variant has been making the rounds lately:

- Computers become infected by clicking on links in malicious emails that appear to be from legitimate businesses and through compromised advertisements on popular websites.
- Directs user to a personalized victim's ransom page.

Examples:
- CryptoWall
- CryptoWall 2.0 (its newer version)

Mitigation:
- Recognize ransomware
- Back up and securely store data.

Resources:
CYBER AWARENESS UPDATE

• QR Codes have multiple functions, often transparent to the user
  - Launch websites, download files, initiate Skype calls, alter OS files and settings and more.
  - No standard way to tell 'safe' from 'unsafe' codes

• Examples
  - Heinz Ketchup
  - Google Glass

• Mitigation
  - Only scan QR codes from trusted sources
  - Use a QR reader that lets you preview the action before launching it

Quick Response (QR) code: a matrix barcode that can store a large amount of data, which can be processed by a reader.

MALWARE

QR Code Vulnerabilities

KEY POINTS

- QR Codes have multiple functions, often transparent to the user
  - Launch websites, download files, initiate Skype calls, alter OS files and settings and more.
  - No standard way to tell 'safe' from 'unsafe' codes

- Examples
  - Heinz Ketchup
  - Google Glass

- Mitigation
  - Only scan QR codes from trusted sources
  - Use a QR reader that lets you preview the action before launching it

HARDWARE

Apple iPhone

Weaknesses likely introduced during code development, including specification, design, and implementation.

Resources

http://money.cnn.com/2015/06/19/news/companies/heinz-ketchup-porn/

Crafted text message causes denial of service (reboot/message disruption)

- Versions affected
  - iOS 8.x through 8.3

- Mitigation
  - Update/pats.h (when available)
HARDWARE

Barracuda Web Filter

Man-in-the-middle attack is an attack in which an attacker intercepts and alters data traveling between two parties.

KEY POINTS
- Uses default certificates, enabling man-in-the-middle (MITM) attacks
  - Loss of sensitive information.
  - Does not properly verify certificates.
- Vulnerable versions between 1 and 8.1.005.
- Mitigation
  - Update/Patch

HARDWARE

Rockwell Automation

Rockwell Software RSView 32 is a component-based human machine interface (HMI) for monitoring and controlling automation machines and processes.

KEY POINTS
- Does not properly encrypt credentials; allows local users to obtain sensitive information
  - Vulnerable versions: RSView32 7.60.00 (aka CPR9 SHA) and earlier
  - Mitigation
  - Update/Patch

SOFTWARE
A web browser, or simply “browser,” is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

KEY POINTS
- Multiple vulnerabilities in web browsers
  - Google Chrome - Vulnerable versions before 43.0.2357.6
    - Denial of service
    - Unspecified impact
    - Execute tasks
  - Firefox - Vulnerable Versions before version 38.0
    - Allow denial of service
    - Possibly executing arbitrary code
    - May allow attacker to obtain sensitive information from memory
  - Internet Explorer - Vulnerable Versions 6-11
    - Multiple vulnerabilities allow arbitrary code or cause denial of service via crafted website
  - Mitigation: Update/Patch

A web browser, or simply “browser,” is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

KEY POINTS
- Multiple versions allow remote attackers to bypass protection and write to file system
  - Vulnerable versions
    - Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux,
    - Adobe AIR before 17.0.0.172,
    - Adobe AIR SDK before 17.0.0.172
    - Adobe AIR SDK & Compiler before 17.0.0.172
  - Mitigation
    - Update/patch

Adobe Flash Player (labeled Shockwave Flash in Internet Explorer and Firefox) is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio. Flash Player can run from a web browser as a browser plug-in or on supported mobile devices.

KEY POINTS
- Allow denial of service (infinite loop and CPU consumption) via crafted packet
  - Vulnerable versions
    - Versions between 1.12.x and 1.12.5, 1.10.x and 1.10.14, 1.10.x-1.10.14 and 1.12.x to 1.12.5
  - Mitigation
    - Update/patch

Wireshark® is a network protocol analyzer that you can use to capture and interactively browse the traffic running on a computer network. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. It is freely available as open-source, and is released under the GNU General Public License version 2.

Resources
https://www.us-cert.gov/ncas/bulletins/SB15-152
**Linux Kernel**

The Linux kernel is a Unix-like computer operating system kernel, in computing, the kernel is a computer program that manages I/O (input/output) requests from software and translates them into data processing instructions for the central processing unit and other electronic components of a computer and it is a fundamental part of a modern computer's operating system.

**Vulnerable versions**
- Kernel versions before 4.0

**Mitigation**
- Update/patch

**Resources**
- [https://www.us-cert.gov/ncas/bulletins/SB15-152](https://www.us-cert.gov/ncas/bulletins/SB15-152)

**Cisco Unified MeetingPlace**

Cisco Unified MeetingPlace is a web-based conference software that integrates audio, video, and web conferencing capabilities.

**Vulnerable versions**
- Versions 8.6(1.2) and 8.6(1.9)

**Mitigation**
- Update/patch

**Resources**
- [https://www.us-cert.gov/ncas/bulletins/SB15-159](https://www.us-cert.gov/ncas/bulletins/SB15-159)
HUMAN

Cyber Awareness Update: Law Enforcement, Military, and Government Employees

KEY POINTS

- Hacktivism: Often-subversive use of computers and computer networks to promote a political agenda.

- FBI warns of activity against government personnel:
  - Doxing
  - Swatting
  - Cyber attacks

- Mitigation:
  - Privacy settings/OPSEC on Social Networking Sites
  - Security on home computers/wireless
  - Phishing awareness
  - Social engineering awareness
  - Monitor web and credit reports
  - Two-factor authentication on email

FBI Warns that Law Enforcement and Public Officials Are at Increasing Risk of Social Engineering and Hacking Attacks

HUMAN

Hacktivist Targeting Law Enforcement, Military, and Government Employees

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

11

JUNE 2015

http://www.ic3.gov/media/2015/150421.aspx

KEY POINTS

- Multiple vulnerabilities in multiple products:
  - Access server, web security system, wireless systems, etc.
  - Allows remote attacks, session hijacks, file uploads, script injection, denial of service, and other attacks.

- Vulnerable versions:
  - Cisco Unified Communications Manager 10.0
  - Cisco Wireless LAN Controller (WLC) devices before 7.0.241, 7.1.x through 7.4.x before 7.4.122, and 7.5.x and 7.6.x before 7.6.120
  - Cisco Secure Access Control Server Solution Engine (ACSE) 5.5(0.1)
  - Cisco IOS 15.3S
  - Cisco Unified Intelligence Center 10.6(1)
  - Cisco FireSIGHT System Software 5.3.0
  - Multiple others

- Do you know hardware configuration? Does it impact you?

- Mitigation: Update

A network is information systems implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, controllers, key distribution centers and the like or control devices.

https://www.us-cert.gov/ncas/bulletins/SB15-145

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

12

JUNE 2015

https://www.us-cert.gov/ncas/bulletins/SB15-145

Resources
**NETWORK**

Bluecoat web appliance

**KEY POINTS**
- May allow attackers to hijack web sessions and administrator authentications
- Vulnerable versions: Versions 3.6.x and 3.8.x before 3.8.4
- Mitigation: Update/patch

**Resources**
- [https://www.us-cert.gov/ncas/bulletins/SB15-159](https://www.us-cert.gov/ncas/bulletins/SB15-159)

---

**NETWORK**

Aruba Networks ClearPass Policy Manager

**KEY POINTS**
- May allow attackers to hijack web sessions and administrator authentications
- Vulnerable versions: Before 6.5.0
- Mitigation: Update/patch

**Resources**
- [https://www.us-cert.gov/ncas/bulletins/SB15-152](https://www.us-cert.gov/ncas/bulletins/SB15-152)

---

**“WHAT DO I NEED TO DO?”**

**Recommendations**
- Form a relationship/partnership with your IT and cybersecurity departments
- Review/sign up for alerts through US CERT
- Use CDSE resources, such as webinars, free eLearning courses, and more

**WHAT IS MY ROLE IN THIS?**

- If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.

**Resources**
- CDSE: [http://www.cdse.edu](http://www.cdse.edu)
- US CERT: [https://www.us-cert.gov/ncas](https://www.us-cert.gov/ncas)
• Privileged User webinar: July 9, 2015
• RMF Steps 1-6 Courses: July 2015
• Update to CDSE Virtual Environments
  o Current VE is being broken out into three unique environments for ease of use
  o Updated student workbooks
  o Upgraded Red Hat Enterprise Linux® environment

THANKS FOR JOINING US!
CHECK OUT OUR UPCOMING WEBINARS:

QUESTIONS?