CALIFORNIA RESILIENCY ALLIANCE

Informational Brief

Report ID #: 2017-0515-2230

Provide Feedback on this Report

Event: WannaCry Ransomware

Brief Date: Monday, May 15, 2017

Next Brief: none scheduled

Recipients: CRA members with interest in Cyber threats

Notice: The information in this brief is subject to change and the situation may have evolved since the sending of this brief.

Overview of WannaCry Ransomware

Type: Ransomware

Systems Affected: Microsoft Windows operating systems

Names: WannaCry, WCry, or Wanna Decryptor

Locations: as many as 74 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan

Number of Infections: tens of thousands

Discovered: The latest version of this ransomware variant was discovered the morning of May 12, 2017, by an independent security researcher.

(Source: US-CERT Alert (TA17-132A) - Indicators Associated With WannaCry Ransomware revision date 5/15/17 https://www.us-cert.gov/ncas/alerts/TA17-132A)

Alerts

US-CERT Alerts

Indicators Associated With WannaCry Ransomware Alert, revised May 15, 2017 (TA17-132A)
https://www.us-cert.gov/ncas/alerts/TA17-132A
This alert contains:

- Technical Details
- Initial Analysis
- Recommended Steps for Prevention
- Recommended Steps for Remediation

Alerts (continued)

US-CERT Alerts (continued)

Indicators Associated With WannaCry Ransomware Alert, May 15, 2017 (ICS-ALERT-17-135-01)
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01
This alert is a follow-up to US-CERT alert TA17-132A
This alert contains:

- List of ICS and medical device vendors have reported that they support products that use Microsoft Windows and have proactively issued customer notifications with recommendations for users

Microsoft Alerts

Microsoft Security Bulletin MS17-010 - Critical (May 14, 2017)
Security Update for Microsoft Windows SMB Server (4013389)
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

- Affected Software and Vulnerability Severity Ratings
- Vulnerability Information
- Mitigating Factors (none identified)
- Workarounds

Recommendations

See Alerts above for more technical recommendations.

US-CERT (United States Computer Emergency Readiness Team): In advice specific to the recent WannaCry ransomware threat, users should: (Source: https://www.us-cert.gov/security-publications/Ransomware 5/15/17)

- Be careful when clicking directly on links in emails, even if the sender appears to be known; attempt to verify web addresses independently (e.g., contact your organization's help desk or search the Internet for the main website of the organization or topic mentioned in the email).
- Exercise caution when opening email attachments. Be particularly wary of compressed or ZIP file attachments.
- Follow best practices for Server Message Block (SMB) and update to the latest version immediately. (See US-CERT's SMBv1 Current Activity for more information.)

Contact Information for Reporting

FBI Internet Crime Complaint Center
www.ic3.gov

FBI Cyber Division
Email: CyWatch@ic.fbi.gov
Phone: 855-292-3937

Contact Information for Reporting (continued)

FBI Cyber Task Forces
https://www.fbi.gov/contact-us/field-offices

Field Office	Address	Phone Numer
Los Angeles	11000 Wilshire Boulevard, Suite 1700	310-477-6565
Sacramento (Roseville)	2001 Freedom Way	916-746-7000
San Diego	10385 Vista Sorrento Parkway	858-320-1800
San Francisco	450 Golden Gate Avenue, 13th Floor	415-553-7400

United States Secret Service Electronic Crimes Task Force
www.secretservice.gov/investigation/#field

Field Office	Phone Numer
Los Angeles	213-533-4400
San Francisco	415-576-1210

United States Secret Service Local Field Offices
www.secretservice.gov/contact/

Field Office	Address	Phone Number
Camarillo	5051 Verdugo Way, #310	805-383-5745
Fresno	5200 North Palm Avenue, #207	559-487-5204
Los Angeles	725 South Figueroa Street, #1300	213-894-4830
Riverside	3801 University Avenue, #550	951-276-6781
Sacramento	501 I Street, #12100	916-325-5481
San Diego	550 West C Street, #660	619-557-5640
San Francisco	1700 Montgomery Street, #300	415-576-1210
San Jose	280 S First Street, #1111	408-535-5288
Santa Ana	200 W Santa Ana Blvd, #500	714-246-8257

DHS's National Cybersecurity and Communications Integration Center (NCCIC)
Email: NCCICCustomerService@hq.dhs.gov
Phone: 888-282-0870

Additional Resources

US-CERT How to Protect Your Network from Ransomware
US government interagency technical guidance document aimed to inform CIOs and CISOs at critical infrastructure entities.
https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

ICS-CERT Alerts
https://ics-cert.us-cert.gov/alerts

US-CERT Recommended Practices
https://ics-cert.us-cert.gov/Recommended-Practices

Additional Resources (continued)

DHS - Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies (Sept. 2016)
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

The following have additional FOUO documents available to members via their respective member portals:

- Infragard
- HSIN-CI

News Reports

WannaCry Attacks are Only the Beginning
CSO Online May 15, 2017
Thousands of organizations from around the world were caught off guard by the WannaCry ransomware attack launched Friday. As this rapidly spreading threat evolves, more cybercriminals are likely to attempt to profit from this and similar vulnerabilities. …
Article Links: http://www.csoonline.com/article/3196985/security/wannacry-attacks-are-only-the-beginning.html

Dealing with WannaCry on Monday morning, and the days ahead
CSO Online May 15, 2017
It's Monday. Across the globe organizations are likely having the same conversation: What happened? What is WannaCrypt (WannaCry)? Are we exposed? What can we do? If you're in the trenches, here's a brief outline that might help you manage some of the conversations you're going to have this week. …
Article Link: http://www.csoonline.com/article/3196784/security/dealing-with-wannacry-on-monday-morning-and-the-days-ahead.html

WannaCry...ransomware cyberattack as far as the eye can see
CSO Online May 15, 2017
WannaCry ransomware is yet another wake up call and not a sales opportunity. Let's dispel with the hyperbole and bull. Let's stop pointing fingers. Let's get down to the meat of the matter and have a good long look at what we have learned or at least should learn from the events of the weekend. …
Article Link: http://www.csoonline.com/article/3196302/security/wannacry-ransomware-cyberattack-as-far-as-the-eye-can-see.html

FS-ISAC Monitoring Ransomware Attack; No Financial Sector Impacts Yet Reported
ABA Banking Journal May 15, 2017
A massive ransomware cyber attack spread around the world on Friday, affecting more than 230,000 computers in about 150 countries, according to news reports over the weekend. Users of infected computers received a message that their files had been encrypted and that they should pay a ransom in bitcoin in order to decrypt their files….
Article Link: http://bankingjournal.aba.com/2017/05/fs-isac-monitoring-ransomware-attack-no-financial-sector-impacts-yet-reported/

News Reports (continued)

5 Emergency Mitigation Strategies to Combat WannaCry Outbreak
Bank Info Security May 14, 2017
Drop everything and patch all Windows devices against the SMB flaw. And above all, don't block the nonsense domain referenced by the WannaCry ransomware outbreak that began infecting tens of thousands of endpoints on May 12….
Article Link: http://www.bankinfosecurity.com/5-emergency-mitigation-strategies-combat-wannacry-outbreak-a-9914

WannaCry ransomware: Indian Banks Told to Update ATM software
FinExtra May 15, 2017
In the wake of the global WannaCry ransomware cyberattacks, the Reserve Bank of India has told the country's Windows XP-loving banks to run software updates, according to local press reports.
Article Link: https://www.finextra.com/newsarticle/30569/wannacry-ransomware-indian-banks-told-to-update-atm-software

WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerability
Security Intelligence May 14, 2017
On Friday, May 12, 2017, the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organizations in more than 100 countries within the span of 48 hours, the operators of malware known as WannaCry/WanaCrypt0r 2.0 are believed to have caused the biggest attack of its kind ever recorded. …
Article Link: https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

About the California Resiliency Alliance

The California Resiliency Alliance is a 501c3 non-profit empowering local and regional resiliency effort through cross-sector information sharing and partnerships.
Visit our website to learn more about our initiatives and becoming a member.