Singletree Engineering

CISA Tabletop Exercise Package – Ransomware

February 3, 2023

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Table of Contents

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:WHITE information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.

Handling Instructions

TLP: WHITE

The title of this document is Singletree Bitcoin Ransomware Situation Manual. This document is unclassified and designated as “*Traffic Light Protocol (TLP):WHITE*”: Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:WHITE and Singletree sponsor guidelines.

For questions about this event or recommendations for improvement contact: John Kuk, doctoral student at George Washington University, john.kuk@gwu.edu of Singletree.

Exercise Overview

<table>
<tr><th>Exercise Name</th><th colspan="2">Singletree Bitcoin Ransomware</th></tr>
<tr><td>Exercise Date, Time, and Location</td><td colspan="2">February 3, 2023
Time (9:00 a.m. – 12:00 p.m.)
Singletree HQ</td></tr>
<tr><td rowspan="10">Exercise Schedule</td><td>Time</td><td>Activity</td></tr>
<tr><td>9:00 a.m.</td><td>Cyber Threat Briefing</td></tr>
<tr><td>9:30 a.m.</td><td>Exercise Module 1</td></tr>
<tr><td>10:30 a.m.</td><td>Break</td></tr>
<tr><td>10:45 a.m.</td><td>Continue Module 1</td></tr>
<tr><td>11:30 a.m.</td><td>Hotwash</td></tr>
<tr><td>12:00 p.m.</td><td>Lunch</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>Scope</td><td colspan="2">3 hour facilitated, discussion-based Tabletop Exercise</td></tr>
<tr><td>Purpose</td><td colspan="2">To examine the coordination, collaboration, information sharing, and response capabilities of Singletree in reaction to a significant cyber incident.</td></tr>
<tr><td>Objectives</td><td colspan="2">1. Examine the ability for Singletree to respond to a significant cyber incident.
2. Evaluate the ability for Singletree to coordinate information sharing during a significant cyber incident.
3. Inform development/update of Singletree cyber incident response plans.
4. Explore processes for requesting additional incident response resources once Singletree resources are exhausted.
5. Explore Singletree processes for addressing public affairs.</td></tr>
<tr><td>Threat or Hazard</td><td colspan="2">Cyber</td></tr>
<tr><td>Scenario</td><td colspan="2">A threat actor targets a system administrator through a phishing email as an entry point into <Organization> networks/systems. Attackers compromise Personally</td></tr>
</table>

Exercise Name	Singletree Bitcoin Ransomware
	Identifiable Information (PII), deface public facing websites and install ransomware on Singletree computers.
Sponsor	Singletree
Participating Organizations	Singletree Engineering
Points of Contact	**Insert Organization POC(s)** **Singletree Engineering** security@singletree.com

General Information

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

Players will participate in the following:

- Cyber threat briefing
- Scenario modules:
    - **Module 1:** This module introduces a scenario where Singletree Engineering has become the victim of a sophisticated cybersecurity attack involving ransomeware. An employee accidentally opens an email infecting not only their laptop but the whole company. Everytime the ransomware infected another machine on the network it would require 5 bitcoins to release each machine amassing to 375 bitcoins or an estimated 7 million USD.
- Hotwash

Exercise Guidelines

- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions and/or suggested actions to resolve or mitigate a problem.

- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations to negatively impact your participation in the exercise.

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

Module 1:

Day 1: 16:01 UTC

It seems the ransomware attack involved an employee "John" who accidentally opened an email communication notifying them that their employment has ended, and HR needs them to visit a site to process the termination. For fear of losing his job, John hastily opened the email and followed a link which began downloading an application which quickly locked the laptop he was working on. A message appeared indicating that the machine was locked and that to release the lock it would require 5 bitcoins to release. The 5 increased to 10, 15, 20, and quickly started to increase to 375 bitcoins which is an estimated 7 million USD. What John didn't know was that there was a virus attached to the ransomware and that every increase of 5 led to another company machine being infected and locked.

Day 1: 16:17 UTC

The employee reports to his manager that his work laptop compromised with Ransomware.

Day 1: 17:01 UTC

CSIRT on-call alerted about ransomware.

Day 1: 18:00 UTC

CSIRT performed analysis and with the information constructed a list of machines to isolate.

Discussion Questions

1. How would these incidents be assessed within your organization? Do you have defined cybersecurity incident severity levels and/or escalation criteria?
2. What actions would be taken at this point? By whom?
3. What notifications would be made? Consider internal (e.g., to leadership) and external (e.g., to law enforcement, government partners, etc.) notifications.
4. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
5. Do you pay the ransom?
    a. Who decides?
    b. What is the process?
    c. What are the advantages/disadvantages to paying?
    d. What are the potential political ramifications?
    e. What outside partners/entities do you need to contact?
6. What capabilities and resources are required for responding to this series of incidents?
    a. What internal resources do you depend on?
    b. Are your current resources sufficient?
    c. Do you have personnel tasked with incident response or a designated cyber incident response team within your organization?
        i. If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?

        ii. Who is responsible for activating the cyber incident response personnel and under what circumstances?
        iii. What are the cyber incident response team/personnel's roles and responsibilities?
    d. Who do you contact if you need additional third-party assistance?

7. What are your public affairs concerns?
    a. Who is responsible for coordinating the public message? Is this process a part of any established plan?
    b. How would your department respond to the media reports?
    c. What information are you sharing with the public? Employees?
    d. Are public information personnel trained to manage messaging related to cyber incidents?
    e. Does your department have pre-drafted statements in place to respond to media outlets?
    f. Does your department have staff trained to manage your social media presence?
8. What impact will the sale of sensitive or Personally Identifiable Information (PII) have on your response and recovery activities?
    a. Have your public relations priorities changed?
    b. Will it trigger any additional legal and/or regulatory notifications?
9. What sources of cybersecurity threat intelligence does your organization receive? For example, information from CISA, Federal Bureau of Investigation (FBI), open source reporting, security service providers, or others?
    a. What cyber threat information is most useful?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across your organization?
2. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
    a. How often is training provided?
    b. Does the training cover:
        i. Review of organizational acceptable use and IT policies,
        ii. Awareness of prominent cyber threats,
        iii. Password procedures, and
        iv. Whom to contact and how to report suspicious activities?
    c. Is training required to obtain network access?
    d. What security-related training does your organization provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems?
    e. How often do they receive the training?
3. How do employees report suspected phishing attempts?
    a. What actions does your department take when suspicious emails are reported?

   b. Are there formal policies or plans that would be followed?
   c. Does your organization conduct phishing self-assessments?
4. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
   a. What are your most significant threats and vulnerabilities?
   b. What are your highest cyber security risks?
5. Does your IT department have a patch management plan in place? If so,
   a. Are risk assessments performed on all servers on the network?
   b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
   c. Does this plan include a risk management strategy that addresses the following considerations?
      i. The risks of not patching reported vulnerabilities,
      ii. Extended downtime,
      iii. Impaired functionality, and
      iv. The loss of data?
6. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?
   a. How would your department respond to the local media reports?
   b. What information are you sharing with citizens? Employees?
   c. Are public information personnel trained to manage messaging related to cyber incidents?
   d. Does your department have pre-drafted statements in place to respond to media outlets?
   e. Are they trained to manage your social media presence?
   f. Are all personnel trained to report any contact with the media to appropriate public information personnel?
7. What information would your organization communicate to the public?
8. Who is responsible for public information related to the incident? What training or preparation have they received?
9. What are the legal issues you must address?
10. What policies should your organization have? Does it exercise these policies? If so, how often?
11. What legal documents should your organization have in place (for example with third-party vendors)?
12. What is the role of the legal department in this scenario?
13. Does your state have security breach notification laws? If so, what do they include?

Appendix A: Attacks and Facts

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of computers making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the "master" because it controls any subsequent computers that become infected. The other infected computers carry out the actual attack and are known as "daemons." The attack begins when the master computer sends a command to the daemons, which includes the address of the target. Large numbers of data packets are sent to this address, where extremely high volumes (floods) of data slow down web server performance and prevent acceptance of legitimate network traffic. The cost of a DDoS attack can pose sever loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the OSI Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- Understanding Denial-of-Service Attacks (https://www.us-cert.gov/ncas/tips/ST04-015)
- DDoS Quick Guide (https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)
- Guide to DDoS Attacks (https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf)

Social Engineering

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e. email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely operating system platform dependent. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, know where to forward them and keeping software and systems up-to-date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.us-cert.gov/ncas/tips/ST04-014)
- The Most Common Social Engineering Attacks (https://resources.infosecinstitute.com/common-social-engineering-attacks/)

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Ransomware (https://www.us-cert.gov/Ransomware)
- Protecting Against Ransomware (https://www.us-cert.gov/ncas/tips/ST19-001)
- Indicators Associated With WannaCry Ransomware (https://www.us-cert.gov/ncas/alerts/TA17-132A)
- Incident trends report (Ransomware) (https://www.ncsc.gov.uk/report/incident-trends-report#ransomware)

Appendix B: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf
- Federal Information Security Modernization Act of 2014 (Dec 2014) https://www.dhs.gov/fisma
- OMB Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

Presidential Directives

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
- Presidential Policy Directive-41: United States Cyber Incident Coordination (Jul 2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex to Presidential Policy Directive-41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) https://www.hsdl.org/?view&did=797545
- Presidential Policy Directive-8: National Preparedness (Mar 2011), (Updated Sep 2015) https://www.dhs.gov/presidential-policy-directive-8-national-preparedness
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) https://www.hsdl.org/?view&did=731040

Strategies and Frameworks

- National Cyber Incident Response Plan (Dec 2016) https://www.us-cert.gov/ncirp
- National Cyber Strategy of the United States of America (Sep 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- U.S Department of Homeland Security Cybersecurity Strategy (May 2018) https://www.hsdl.org/?view&did=810462
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Protection Framework, Second Edition (Jun 2016) https://www.fema.gov/media-library-data/1466017309052-85051ed62fe595d4ad026edf4d85541e/National_Protection_Framework2nd.pdf

- Office of Management and Budget (OMB) Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015) http://www.thecre.com/forum4/wp-content/uploads/2015/11/OMB-Cybersecurity-Implementation-Plan.pdf

Key Points of Contact

- Department of Homeland Security/Cybersecurity and Infrastructure Security Agency (CISA) (contact: central@cisa.dhs.gov)
- Federal Bureau of Investigation (FBI)
  - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
  - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
- National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/)

Other Available Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (http://www.nascio.org/Advocacy/Cybersecurity)
- National Governors Association (NGA) (https://www.nga.org/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (http://www.isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
- International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
- National Council of ISACs (https://www.nationalisacs.org/)

References Cited

"*Wannacry Two Years Later: How Did We Get The Data?”*. (2019, Nay 27). Retrieved August 22, 2019, from Armis IOT Security: ttps://go.armis.com/hubfs/Armis-WannaCry-How-Did-We-Get-The-Data-WP.pdf

CISA. (2018, July). *Alert (TA18-201A) - Emotet Malware*. Retrieved from us-cert.gov.

Davis, J. (2018, 31 July). *1.4 million patient records breached in UnityPoint Health phishing attack*. Retrieved July 2019, from HealthCare IT News:

ttps://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack

Davis, J. (2019, April 11). *Minnesota DHS Reports Health Data Breach from 2018 Email Hack*. Retrieved 2019, from Health IT Security: https://healthitsecurity.com/news/minnesota-dhs-reports-health-data-breach-from-2018-email-hack

Kottler, S. (2018, March 1). *February 28th DDoS Incident Report*. Retrieved 2019, from The GitHub Blog: https://github.blog/2018-03-01-ddos-incident-report/

Palo Alto Networks. (2019, February 2). *PAN-OS 8.0: PAN-OS Phishing Attack Prevention*. Retrieved July 2019, from Palo Alto Networks Knowledge Base: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRpCAK

Seri, B. (n.d.). *"Two Years In and WannaCry is Still Unmanageable"*. Retrieved August 22, 2019, from Armis IOT Security Blog: https://www.armis.com/resources/iot-security-blog/wannacry/

Sullivan, P. (2018, July 31). *Mat-Su Declares Disaster for Cyber Attack*. Retrieved July 2019, from Matanuska-Susitna Borough: https://www.matsugov.us/news/mat-su-declares-disaster-from-cyber-attack

Symantec Threat Intelligence. (2017, October 23). *What you need to know about the WannaCry Ransomware*. Retrieved 2019, from Symantec Threat Intelligence Blog: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack