Draft Computer Security Incident Response Plan

Ransomware Threat Playbook

Last Edit Date: November 2016

Page 1 of this document contains the emergency first steps
Emergency First Steps

- **End-User: Do not turn off your computer**
  - Malware can be designed to cause even further harm when a computer is turned off then back on.

- **Call 5KTechnical Services (469) 656-3159 X 201** and open a priority 1 ticket – write down the ticket ID number.
  - The affected machine and person that initiated the call needs to be fully available.

- **Follow the instructions received**
  - You will probably be instructed to disconnect your computer from the network by removing the network cable from your computer.

- **Notify the Executive Director or the Computer Security Incident Response Team (CSIRT) Leader**

*Instructions Continue on Page XX*
Table of Contents

Will update this last

- Emergency First Steps
- CSIRT Members Required
- Ransomware Playbook Objective
- Ransomware Overview
- Ransomware Implications - To Pay or Not to Pay
- Ransomware Threat Response Communications Plan
- End-User Instructions for a Ransomware Attack
- Critical To Successful Ransomware Incident Response
- Ransomware Cyber-kill Chain
- Disrupting the Ransomware Chain of Events
- Ransomware Response Scenario
- Event Reported by End-User
- Alert Raised by Monitoring System
- Identifying Other Infected Devices
- Generating IoCs from URLs and Hashes
- Deploying the IoCs
- Identifying the Source of the Ransomware Infection
- Investigate Whether the Victim’s PC was Infected by an Exploit Kit/Drive-by Download
- Generating IoCs from Phishing Emails
- Restoration Options
- Post-incident Analysis and Forensics
- Ransomware Article
- Resources
CSIRT Team Members Required

- Executive Director
- Elder Board Member
- IT Advisory Team Member
- CSIRT Manager
- 5K Technical Services – Lead Engineer
- Consultant
- Insurance Broker
- Cyber Attorney (Broker will call Baker Hostetler)
- Law Enforcement
- Victim(s) - personal computer owner
- Depending on severity
  - Communications
  - Human Resources
  - Congregation services
Overview of Ransomware

• Ransomware is malware that covertly installs on a computer, without the knowledge of users, and encrypts files so users can access their information

• It is installed in one of two ways
  • The result of a successful phishing attack
  • A result of a victim browsing a website that has the malware awaiting (a drive-by)

• It stays asleep or spreads without victim’s interaction until it receives a command from the hacker to encrypt files or completely lock the computer

• When the attack commences
  • Victim gets a message that their computer or files have been encrypted
  • The message will also instruct the victim that a fee (ransom) can be paid to decrypt the computer or files
Critical to Successful Ransomware Incident Response

- **Current Ransomware Technical Knowledge**
- **Backups**
  - Backup all critical information from servers and end-user devices
  - Backups stored offline
  - Backup restores recently tested
- **Ransomware Incident Response Plan**
  - Documented plan in place
  - Plan recently exercised and lessons learned incorporated
- **Business Continuity Plan**
  - What is the ability to sustain business operations without access to certain systems?
    - For how long?
    - Recently tested?
Ransomware Implications
To Pay or Not to Pay

- A victim of a ransomware attack is placed in the role of hostage, especially if there is no or poor preparedness.
- Substantive preparation minimizes the impact both physically and psychologically.
- Without preparation, employee training, adequate backup, a good business continuity plan, a victim may be in a position of having to pay.
- Law authorities recommend not paying. It rewards the offender and doesn’t guarantee that the offender will hold up their end of the deal.
- How will the agreement to pay impact the organization’s reputation?
- What is the recommendation of NDCBF’s cyber law representative?
Ransomware Response Scenario

- The initiation of the Ransomware response playbook is reactive
  - We react to the main execution trigger which usually is an employee(s) reporting their files have been encrypted
  - The goal is to quickly identify, contain, eradicate and recover from the infection(s) in a controlled and comprehensive manner, as soon as possible

- Create Indicators of Compromise (IoCs) to Automate:
  - Identification of existing ransomware infections
  - Block future ransomware infections

- Attempt to determine how victim’s device was infected
  - Use this information to block the threat on the proxies and SMTP gateways.
    - For the latter, link the instructions with the Phishing playbook
Ransomware Threat Response Communications Plan

• **Initial Notifications**
  - NDCBF IT Coordinator
  - 5K Technical Services
  - NDCBF Computer Security Incident Response Team Executive and Team (CSIRT) Leader

• **CSIRT Notifications**
  - **Cyber Insurance – BCS Insurance Company**
    - Jennifer Lang Kelley
    - Hotchkiss Insurance Agency, LLC
    - 972.512.7793 /jlangkelley@hiallc.com
    - Notice of Claim, see Policy RPS-P-0139172 page 3 of 37
    - Joan Dambrosio – (415) 365-9820
    - RPS Cyber 24/7 Breach Response Counsel Hotline (855) 217-5204

• **NDCBF Cyber Law Attorney**

• **Law Enforcement**

• **Other internal and external notifications to be defined by the CSIRT**
Initiation – Indicator of Compromise

- An NDCBF Staff or Lay-Staff has encountered a Ransomware message on an NDCBF owned computer.

Example of a Ransomware Attack Initiation
Procedures: When a Ransomware Attack is Noticed

• End-User: Do not turn off your computer
  • Malware can be designed to cause even further harm when a computer is turned off then back on

• Call to 5KTechnical Services (469) 656-3159 X 201 and open a priority 1 ticket – write down the ticket ID number
  • The affected machine and person that initiated the call needs to be fully available

• Follow the instructions received
  • You will probably be instructed to disconnect your computer from the network by removing the network cable from your computer

• Notify the Executive Director or the Computer Security Incident Response Team (CSIRT) Leader
Suspected Ransomware Attack is Reported

• The Executive Director and/or the CSRIT Leader initiates a conference
  • Dial into conference bridge (Get number from Chip)
  • Designate recorder to document the bridge discussion
  • Record the conference bridge call

• During the Bridge Discussion, Event Categorized
  • False Positive
    • Instructions
  • Event but not an incident
    • Instructions
  • Ransomware Incident
Goal: Triage the incident and take the computer offline as soon as possible

- User reports an incident over the phone or in an email
- Open a ticket with 5K Technical Services
- If the incident was reported through an email, open the company address book and call the user back
- Validate with the user whether it is a genuine ransomware case
  - Did a window pop up with demanding a ransom?
  - Has a text file with the instructions been placed on the Desktop?
  - Have the file extensions been changed to .abc, .xxx or similar?
  - Are the files unavailable?

- **Ask the user to disconnect the device from the network. If the user connects to the network with a wireless card, he/she must turn the wireless card off.**
Event Reported by End-User (page 2 of 2)

- Take the following details from the end-user and register them into the ticket:
  - Name of employee
  - Contact details
  - Computer name
  - IP address
  - What happened? How the problem was identified and when?
  - Is the user aware he/she clicked on a suspicious link or attachment lately?
- Let the user know the 5K Technical Services ticket number
- Assure the user that someone from 5K Technical Services will come soon to replace the device
- Go to the Identifying Other Infected Devices to identify other affected devices on our infrastructure
- In parallel, go to Identify the Source of the Infection section to prevent further infections
Goal: Validate alert, identify offending device, take it off the network to prevent encryption of mapped network drives

- Validate the incident:
  - If the alert is based on an IoC, which has been manually added, go to...
  - If a URL was flagged from the proxy logs, check why:
    - Go to https://otx.alienvault.com and search for the hostname
    - Check reputation with any of the tools on https://zeltser.com/lookup-malicious-websites/
  - If the URL was flagged from the IDS logs, verify why the file hash was flagged
    - Go to https://www.virustotal.com and search for the file hash
    - Go to https://otx.alienvault.com and search for the file hash
If the alert is genuine, open a ticket in with 5K Technical Services. Otherwise acknowledge the alert in the Monitoring System and flag it as false positive.

Identify the affected endpoint:
- Get the source IP address from the alert, add the IP to the 5K support ticket
- Search in the DHCP logs to identify the computer leasing this IP address
- Once you have the computer name, write an email to it@royalacacia.com and ask IT which user owns the computer in question

Open the company address book and call the user on the phone

Inform the user what happened to his/her PC

Ask the user to disconnect the device from the network
Alert Raised by Monitoring System (page 3 of 3)

– Take the following details from the end-user and append them to the ticket:
  – Is the user aware he/she clicked on a suspicious link or attachment lately?
  – Let the user know the ticket number from JIRA
  – Tell the user that someone will come soon to replace the device
  – Proceed to Incident Resolution
Escalation Decision??

- Executive Director and/or the Computer Security Incident Response Team (CSIRT) Leader review ticket with 5K Technical Services
  - This would be step 2.1.3
- If Time Permits, CSIRT Conference
- Event Categorized (2.1.5)
  - False Positive
    - Instructions
  - Event but not an incident
    - Instructions
  - Event escalated to a Ransomware Incident
    - Go to 2.2
2.2.1 Assign Ransomware Incident Response Lead

- **Questions**
  - This is an NDCBF internal staff responsibility
  - Who will this be (see CSIRT)?
- **5K Technical Services will be closely involved**
- **Incident Response Lead**
  - Technical
  - Managerial
    - Ensuring proper procedures, documentation,
  - Communications
    - Leadership and staff
    - Possibly external like law enforcement
- **Need to have a leadership discussion and decisions**
- **2.2.4 should also be discussed during this leadership planning meeting**
2.2 Ransomware Analysis
Administrative Tracking

- Henry needs to develop this more
- Need to incorporate asset and document tracking
  - Assets will be transferred to 5K Technical Services for remediation
  - Documents may be transferred to law authorities for criminal investigations
- Need to add asset transfer procedures and documents to processes
2.2 Ransomware Analysis
Ransomware Cyber-Kill Chain

- The ransomware executable is delivered via:
  - Attachments or web links in phishing emails
  - Malvertising on innocuous web pages
  - Drive-by downloads (e.g. fake antivirus)

- The payload is executed on the end user’s device
- The ransomware installs itself on the victim’s computer
- The ransomware generates a unique encryption/decryption key pair
- The ransomware contacts a command and control (C2) server on the Internet to deposit the decryption key
- The malware starts encrypting the files on the hard disk, mapped network drives and USB devices with the encryption key
- Once the process finishes, the files become inaccessible. The malware places a text file on the desktop and/or a splash screen pops-up with the instructions to pay and restore the original files.
Disrupting the Ransomware Chain of Events (page 1 of 2)

◆ The ransomware executable is delivered via:
  - Attachments or web links in phishing emails
    - Block incoming emails on the SMTP server, removing emails from user inboxes, warn users to not click on certain links and attachments
  - Malvertising on innocuous web pages
    - Block malicious URLs on the web proxy, identify computers that visited malicious websites on certain URLs using the proxy logs
  - Drive-by downloads (e.g. fake antivirus)
    - Block malicious URLs on the web proxy, identify computers that visited malicious websites using the proxy logs, deploy custom AV signatures to block certain files to be downloaded, identify PCs with ETDR that downloaded files with certain IoCs

◆ The payload is executed on the end user’s device and the ransomware installs itself
  - Application whitelisting, identify PCs using the HIDS logs that executed certain files
Disrupting the Ransomware Chain of Events (page 2 of 2)

• The ransomware generates a unique encryption/decryption key pair

• The ransomware contacts a C2 server on the Internet to deposit the decryption key
  – Identify and/or block traffic on NIDS and the proxy

• The malware starts encrypting the files on the hard disk, mapped network drives and USB devices with the encryption key
  – Monitor end-user devices and shared folders for certain file extensions, such as .abc, .xxx, .yyy, .zzz

• Once the process finishes, the files become inaccessible. The malware places a text file on the desktop and/or a splash screen pops-up with the instructions to pay and restore the original files.
  – Monitor endpoints for ransomware related text or HTML files in the desktop folder
3.1 Containment & Eradication
Identifying Other Infected Devices (page 1 of 3)

- If one network device is infected, assume other network devices could also be infected.
- This objective is to generate IoCs to find the same pattern across the infrastructure:
  - Go to the Monitoring Tool and log into device.
  - Filter on the detailed proxy logs.
  - Filter on the username of the affected user (all users should be authenticated to the proxy).
  - Filter out URLs that has been categorized, you should only have uncategorized URLs on the list.
  - Export your list to a CSV file.
  - Sort the list by URLs, remove duplicates.
Identifying Other Infected Devices (page 2 of 3)

- Try to find URLs with 2-3 of the following properties
  - Weird URLs:
    - IP address in the URL
    - Random characters in the hostname of the URL (e.g. http://fbdfsufsuehrtgkf.com)
    - URL contains lots of random letters and/or numbers (e.g.http://ezglobalmarketing.com/wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E804FD704B43166264942AB4248A83B5E7984901B8CB83E4B038)
  - Careful ** Requests to Tor2Web (e.g. https://3fdzgtam4qk625n6.fi/) **
    - VirusTotal.com list this site as possibly malicious – Need validation
  - POST requests
  - Weird User-Agent strings, such as:
    - IE6 (e.g. Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1))
    - Programmatic libraries (e.g. python-requests/1.2.0)
    - dJava (e.g. Java/1.6.0_13)
  - Missing User-Agent
If you find suspicious C2 server URLs, try to validate them on http://otx.alienvault.com

Compile a final list of suspicious URLs

Upload the list to the 5K Technical Services ticket

Continue with the Generating IoCs from URLs and Hashes section
Generating IoCs from URLs and Hashes (page 1 of 2)

- Generating IoCs from flagged URLs
- Patterns used to block the URLs on the proxy and identify other infected machines
  - Get the list of flagged URLs/hashes from the 5K Technical Services ticket
  - Subscribe to Threat Intelligence (TI) feed:
    - Go to http://otx.alienvault.com and search for URL
    - Click on Subscribe in order to subscribe to the feed. This will install the relevant IoCs from OTX into our Monitoring system automatically.
  - If none of the IoCs are on the TI feed, you need to generate IoCs manually:
    - Go to the proxy logs again
    - Find 2-3 properties associated with the flagged URL, such as:
      - The request is POST
      - The User-Agent field is dodgy (Java, Python, IE6 etc.)
      - URL contains more than 128 random characters
      - URL contains .php
      - URL contains lots of slashes (/)
      - URL contains WordPress related things (wp-content)
      - URL contains dodgy TLDs (for instance .tk, .ru)
Test your assumption on the proxy logs in the server. Use your pattern and check how many false positives and true positives it produces.

If the pattern is good enough, append your results to the 5K Technical Services ticket.

Continue with the Deploying the IoCs section.
Deploying the IoCs

- Deploy a new rule to the Server to provide alerts for new future infection attempts
- Search for the pattern in the proxy logs in order to identify other computers already affected. If you identify other affected PCs
  - Open a new 5K Technical Services ticket
  - Execute the steps in the *If the alert is raised by the Monitoring section*
- Send the patterns to *it@royalacacia.com* and ask IT to block these URLs on the proxy (talk with Corey)
- Resolve the incident
Purpose is to assess how the end-user device got infected

To be used to block malicious emails or URLs as necessary.

Investigate whether the malware has been delivered by email to the victim:

- Go to the Monitoring System and log into Server
- Filter on the email logs associated with the user from the last 3 days
- Filter again on emails where the recipient was the victim
- Remove email logs where the sender was from the company (*@royalacacia.com)
- Export the list of emails into a CSV file. It should only contain emails sent to the victim from the Internet within the last 3 days.
- Send the CSV file to it@royalacacia.com and ask them to retrieve the full emails from the user’s inbox. Upload the CSV to the ticket, too.
Identifying the Source of the Ransomware Infection (page 2 of 3)

− Once you get the emails in a zip file, go through them to identify suspicious links or attachments.
  − Look for links that does not point to the same URL displayed on the screen (e.g. `<a href="http://malware.com">http://www.bbc.co.uk</a>`)
  − Check the domain in the ‘From:’ field correspond to the topic of the email (e.g. package delivery notification emails from UPS will not come from john@mypersonalblog.com)
  − Scan suspicious URLs as necessary on:
    − [http://www.virustotal.com](http://www.virustotal.com)
    − [http://www.phishtank.com](http://www.phishtank.com)
    − or any other tool from [https://zeltser.com/lookup-malicious-websites/](https://zeltser.com/lookup-malicious-websites/)
If you identify a suspicious URL
   - Download the malicious file with ‘curl’
   - Upload the file to http://www.virustotal.com and/or to the sandbox on http://malwr.com
   - If you suspect the file is malicious (e.g. it was flagged by VirusTotal or opens a lot of network connections), generate an SHA256 hash
   - Checking the email attachments>
   - Upload the file to the following services. Be careful, do not upload files if they might contain sensitive data!
     - http://www.virustotal.com
     - http://malwr.com
   - If you suspect the file is malicious (e.g. it was flagged by VirusTotal or opens a lot of network connections)
     - Rename the file as: virus_<filename>_<extension>_invalid
     - Generate SHA256 hash
     - Attach the file and hash to JIRA

Go to the Generating IoCs from Phishing Emails Otherwise continue to check on the proxy logs.
Investigate Whether the Victim’s PC was Infected by an Exploit Kit/Drive-by Download (page 1 of 2)

- Go to the Monitoring System and log into Server
- Filter on the proxy logs from the last 3 days
- Filter on the username of the affected user (all users should be authenticated to the proxy)
- Filter out URLs that has been categorized, you should only have uncategorized URLs on your list.
- Export list to CSV
- Sort the list by URLs, remove duplicates
- Search for suspicious URLs, such as:
  - IP address in the URL
  - Random characters in the hostname of the URL (e.g. http://asdhgugadaasd.com)
  - URL contains lots of random letters and/or numbers
  - WordPress sites are involved (wp-content ...)
- Get the hash from the log if a file download was involved
If you found some suspicious URLs/_hashes, and try to validate them on:

- [http://otx.alienvault.com](http://otx.alienvault.com)
- [http://www.virustotal.com](http://www.virustotal.com)
- Visit the suspected URL in the sandbox on [http://anubis.iseclab.org](http://anubis.iseclab.org)

In case you have high confidence in some of the URLs, compile a list and upload it to the 5K Technical Services Ticket.

Go to the Generating IoCs from URLs and Hashes for blocking them.
Generating IoCs from Phishing Emails (page 1 of 2)

- Process for generating IoCs from identified phishing emails to block further emails
- If the URL in the email was malicious
- In case a single URL was flagged as suspicious
  - Generate IoC from the host part of the URL (http://malware.com/index.php?key=3werw234234fsdfsdfècom)
  - 5K Technology Services block what@ndcbf.org to block the host part of the URL on the proxy - Corey
  - Search for the host part in the proxy logs to retrospectively identify other PCs visiting the malicious URL
  - If other PCs are affected, open a new 5K Technical Services ticket and apply the If the alert is raised by the Monitoring System process
  - Add a new rule to the Monitoring System and Server in order to monitor the proxy logs for new visitors
Generate IoCs from Phishing Emails (page 2 of 2)

- Process for generating IoCs from identified phishing emails to block further emails
- If the attachment in the email was malicious
- In case a file hash was flagged as suspicious
  - Get the SHA256 hash uploaded earlier from 5K Technical Services Ticket
  - Go to the Monitoring System and log into server
  - Search in the proxy logs to check if any of the file downloads has involved the same file with the SHA256 hash
  - If other computers are identified that downloaded the same file, follow the If the alert is raised by the Monitoring System process
3.1 Recovery – Restoration Options (page 1 of 2)

- **Restore from a recent backup**
  - Determine state of backups
  - On a separate computer, initiate backup restore
  - Verify files restored

- **Decrypt your files using a 3rd party decryptor (this is a very slim chance)**
  - Determine the strain
  - If possible, locate the appropriate decryptor/unlocker

- **Do nothing - lose the encrypted data**
  - May be appropriate option:
    - If the impact of losing the files are minimal
    - Decryption doesn’t work
    - Where paying the ransom is not available
  - Rid the computer(s) of all ransomware – may require rebuilding the infected computer(s)
  - Back up encrypted files
    - Computer experts may uncover a decryption method at some later date
Restoration Options (page 2 of 2)

- Do nothing - lose the encrypted data (continued)
  - Prevent future attacks
    - Install and maintain high-quality antivirus software
    - Configure high-grade backup/restore system
    - Test the backup/restore system regularly
    - Implement security awareness training combined with simulated phishing attacks

- Negotiate and /or Pay the Ransom
  - Least recommended
    - No guarantee of decryption once ransom paid
    - Rewards the attacker
  - Locate payment method instructions
  - Obtain Bitcoin account
  - Install a TOR browser
  - Pay the ransom
  - Hopefully receive key to decrypt files
    - Ensure all components that were connected to system at the time of infection are connected during decryption
4.0 Post-Incident Analysis and Forensics

- Lessons Learned
- Recurrence Prevention
- Forensics and Legal Issues

---

- Open a new ticket
- Add the IoCs to the new ticket
- Link the old ticket together with the new ticket
- Resolve the 5K Technical Services ticket
- Open the Mitigation of Phishing Campaigns (10001-INV-USER-SOCIAL) playbook from the playbook repository
- Block emails part of the phishing campaign by following the instructions in the other playbook
Ransomware Article Are you prepared to respond to ransomware the right way?

Rob Gresham explains the evolution of ransomware and shares insights into smarter ways to prepare and respond

CSO | Feb 23, 2016 3:31 PM PT

http://www.csoonline.com/article/3037018/leadership-management/are-you-prepared-to-respond-to-ransomware-the-right-way.html
Resources

**Content Sources:**

- **Demisto**

- **KnowBe4**

- **SANS Institute**
Contact:
Henry Draughon
Process Delivery Systems
(972) 980-9041
hdraughon@processdeliverysystems.com
www.processdeliverysystems.com