Incident Response back in the days... true story
Joey Perry, CISM, CDPSE
IT Operations Manager
jperry@jaxenergy.com
The good guys are way behind and the gap is exponentially growing
What does a cyber incident look like?
What does a cyber incident look like?
Why is it so hard?

- Unknown area, fear of the unknown
- Intimidating figures
- Loss of control
- Multiple stakeholders
- Real management pressure
- Public interest
- No planning at all
Consequences

- Mistakes
- Disorder & chaos
- Acceleration & amplification of the situation losses
So where do we start?
“Know your enemy and know yourself and you can fight a hundred battles without disaster”

(Sun Tzu)

- Who are your threat actors
- What are they after
- Your capabilities
- Your environment
- Your tools
- Who should be part of an IR process
Ransomware as a Service
Ransomware as a Service

Translation guidelines

1. All fields must be filled.
2. Anything between "" should be only copied and not translated.
3. The field "English" should be filled with the name of the language you're translating to (e.g. Deutsch, Español).
4. The characters used must be UTF-8 supported.
5. Only one translation is allowed per day.

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:
- English
- Português
- العربية
- Deutsch
- Italiano
- Español
- Русский
- Latvieski

Your personal files have been encrypted. In order to decrypt them you'll have to pay %RANSOM% BTC

If the payment is not made until %LIMIT%, the cost for the private key will increase to %RANSOM_MULTIPLIED% BTC.
Ransomware as a Service

Plastic • One Month C&C Subscription
- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.01306361 BTC

Bronze • Three Month C&C Subscription
- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.03265903 BTC

Silver • Six Month C&C Subscription
- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.05443172 BTC

Gold • One Year C&C Subscription
- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.08709076 BTC

Platinum • Three Year C&C Subscription
- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.14152248 BTC

Features
- Packages are compiled with your Bitcoin and Email addresses so you are paid directly by your victim
  - Each package also supports Testnet mode, so you can test the ransomware in a virtual machine before distribution
  - Packages utilize advanced polymorphic techniques to avoid over 90% of popular antivirus products
Create the plan
# Table of Contents

I. Purpose

II. Definitions

III. Roles & Responsibilities

IV. Stakeholders

V. Incident Assessment

VI. Impact Criteria

VII. Scope Criteria

VIII. Threat Escalation Protocol

IX. Process Workflow

X. Response Procedures

XI. Appendix
Practice makes perfect

- Who should practice?
- How to practice?
Continuously improve

• Validate the plan
• Re-assess based on strategic industry incidents
• Re-assess based on the changing threat landscape
• Re-assess based on organizational changes
• Re-assess based on changing capabilities/tooling
• Test, test, test
Remote working changes processes
Normal Wiring Process

1. Login
2. Credential to the Financial Sys.
3. Generate a new Wire
4. Manager’s approval (SoD)
5. Wire request sent
W. Wire transfer
Covid-19 changes

- Offices closed
- VPN access introduced new risks
- Users utilized emails for core processes
- Bank’s employees working remote and ease their wire approval processes
1. OWA
2. Wire request though email
3. Internal approvals through emails
4. Wire request sent
W. Wire transfer
Credential Theft

1. Fraudulent Wire request though email, with fake approval processes text in the email body

2. Wire request email sent

2. Wire transfer
Preparations!

• Appropriate tools

• Excellent IR team

• Supporting processes & procedures.
Sometimes it’s just not enough
IR plan cannot be an isolated effort

• All security initiatives must work together to facilitate cyber resilience
Thank you
# Roles & Responsibilities

<table>
<thead>
<tr>
<th>Detection &amp; Analysis</th>
<th>End Users</th>
<th>Help Desk</th>
<th>MSSP/Strategic Vendors</th>
<th>Cybersecurity</th>
<th>IT Operations</th>
<th>CISO</th>
<th>Legal</th>
<th>Human Resources</th>
<th>Public Relations</th>
<th>Management</th>
<th>Senior Enforcement</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report a suspected incident, such as a service disruption, a suspicious email, or an unusual endpoint behavior.</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Open a help desk ticket</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td>-</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gather answers to incident-related questions</td>
<td>C</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Perform indicator of compromise (IoC) search (firewall, IDP, email gateway, SEM, logs, etc.)</td>
<td>-</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Determine what, if any, systems or devices were compromised (e.g. end-user devices, servers, applications)</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Assess the impact to servers, applications, storage, or other systems</td>
<td>-</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Determine the scope/breadth of the incident</td>
<td>-</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
### Table 3. Threat Escalation Protocol

<table>
<thead>
<tr>
<th>Threat Escalation Protocol (TEP)</th>
<th>Criteria</th>
<th>Stakeholders</th>
</tr>
</thead>
</table>
| **TEP Tier 1**                  | • High impact, high scope  
                                    • High impact, medium scope  
                                    • Medium impact, high scope | • End User  
                                    • Help Desk  
                                    • Cybersecurity*  
                                    • IT Operations  
                                    • CISO  
                                    • Legal, HR, Customer Service  
                                    • Senior Management  
                                    • External Third Parties |
| **TEP Tier 2**                  | • High impact, low scope  
                                    • Medium impact, medium scope  
                                    • Medium impact, low scope  
                                    • Low impact, high scope  
                                    • Low impact, medium scope | • End User  
                                    • Help Desk  
                                    • Cybersecurity*  
                                    • IT Operations  
                                    • CISO |
| **TEP Tier 3**                  | • Low impact, medium scope  
                                    • Low impact, low scope | • End User  
                                    • Help Desk  
                                    • Cybersecurity* |