Thinking Beyond Ransomware

John C. Checco
Resident CISO, Financial Services
The Ransomware Frenzy
The Ransomware Frenzy
The Ransomware Frenzy
The Ransomware Frenzy
The Ransomware Frenzy

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted].
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
Ransomware 101

- Colonial Pipeline ($4.4M)
- JBS Foods ($11M)
- Kia Motors ($20M)
- Acer & Quanta ($50M)
- Brenntag Chemical ($7.5M)
- Axa Insurance (undisclosed)
- NBA (undisclosed)

proofpoint.
<table>
<thead>
<tr>
<th>Ransomware Varieties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locker Ransomware</strong></td>
</tr>
<tr>
<td>Requires End User</td>
</tr>
<tr>
<td>Social Engineering</td>
</tr>
<tr>
<td>Locks System</td>
</tr>
<tr>
<td>Bitcoin Payment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Crypto Ransomware</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires End User</td>
</tr>
<tr>
<td>Favors TOR</td>
</tr>
<tr>
<td>Encrypts Files</td>
</tr>
<tr>
<td>Bitcoin Payment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SamSam Ransomware</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Execution</td>
</tr>
<tr>
<td>Vulnerable Servers</td>
</tr>
<tr>
<td>Encrypts Files</td>
</tr>
<tr>
<td>Bitcoin Payment</td>
</tr>
</tbody>
</table>
Ransomware Attack Chains

INITIAL ACCESS
- RDP brute force
- Vulnerable internet-facing system
- Weak application settings

CREDENTIAL THEFT
- Mimikatz
- LSA secrets
- Credential vault
- Credentials in plaintext
- Abuse of service accounts

LATERAL MOVEMENT
- Cobalt Strike
- WMI
- Abuse of management tools
- PsExec

PERSISTENCE
- New accounts
- GPO changes
- Shadow IT tools
- Scheduled task
- Service registration

PAYLOAD
- RobbinHood
- Maze
- PonyFinal
- Vatet loader
- REvil
- NetWalker

Source: https://www.microsoft.com/security/blog/2020/04/28/
Threading the Needle – **Vehicles versus Payloads**

- **Social Engineering**
- **Watering Hole**
- **Account Compromise**
- **Technical Vulnerability**

- **Ransomware**
- **Trojans**
- **RATs**
Threading the Needle – Vehicles versus Payloads
Where Security Programs EXCEL

- Security Education
- Perimeter Protection
- Malware Detection
- Reducing Attack Surface
Breaking the Ransomware Attack Chain

1. **Reconnaissance**
   - It starts with a phishing email

2. **Weaponization**
   - Then a user clicks on a malicious link

3. **Delivery**
   - If a connection is made, malicious website launches exploits

4. **Exploitation**
   - Connection is confirmed, and malicious site starts to send malware

5. **Command and Control**
   - Hacker attempts to take control of systems

6. **Exfiltration**
   - If the attack is successful, systems are breached and data is stolen

---

1st Line of Defense
- Spam filter

2nd Line of Defense
- Web filter

3rd Line of Defense
- Intrusion detection

4th Line of Defense
- Virus detection

5th Line of Defense
- App control and IP reputation

6th Line of Defense
- Sandboxing

Source: IDC Health Insights
**Increased Barrier to Entry → More Complex Attacks**

**Desired Malware Delivery Path**
- Broad Delivery
- Minimal Steps
- Total Automation

**Adjusted Malware Delivery Path**
- Targeted Delivery
- Multiple Indirect Steps
- Threat Actor (Human) Interaction

- Phishing Email → Microsoft Word Attachment → Intermediary Powershell Script → Emotet → Bazaloader → Trickbot → Ryuk

- email with number for call center → call center directs victim to website → victim downloads spreadsheet → enable macros → Campo Loader DLL dropped & run from Public folder

- web traffic to retrieve EXE → Bazarloader EXE → Bazarloader C2 traffic → data exfiltration, reconnaissance, network exploitation, follow-up malware
Where Security Programs OVERTHINK

- Allowing Business to Manage by Exception
- Performance Metrics vs Operational Risks
- Over-Reliance on Trending Analytics
- Over-Reliance or Misuse of Frameworks
- Comingling Attack Delivery with Payloads
- Tunnel Vision on Attribution & Threat Actors
Email contains malicious attachment
Email contains malicious URL
Email Route Verification

Minimize Information Loss
Prevent Data Leakage
Defend Email from Threats

Email Protection
URL Defense

Risk Tolerance
Policies
Controls

Use Cases

Frameworks
CMMC C2M2
NIST CSF ISO-27001
ISO-27002 NIST SP800-53 SCF / UCF
ATT&CK / D3FEND VERIS STIX / TAXII

Metrics vs Risks

Minimize Information Loss
Prevent Data Leakage
Defend Email from Threats

Email Protection
URL Defense
Volatility of TTPs
Mapping Activity to MITRE ATT&CK TTPs

- T1027 - Compressed Executable
- T1027 - Password Protected
- T1047 - WMI
- T1053 - Task Scheduler
- T1059 - HTA
- T1059 - JavaScript
- T1059 - LCG Kit
- T1059 - Office VBA Macro
- T1059 - PowerShell
- T1059 - VBS
- T1059 - XL4 macros
- T1566 - CAPTCHA
- T1566 - Cookie Reloaded
- T1566 - Personalized Logo
- T1566 - Social Engineering
### Applying the NIST Cyber Security Framework (CSF)

<table>
<thead>
<tr>
<th></th>
<th>Attack Chain (Delivery)</th>
<th>Ransomware (Impact)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Users</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protect</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Attack Chain (Delivery):**
- **Identify**
  - Devices
  - Applications
  - Networks
  - Data
  - Users

**Ransomware (Impact):**
- **Respond**
- **Recover**

**Attack Chain (Delivery) Key:**
- ✓ indicates a stage of the attack chain is considered.

**Ransomware (Impact) Key:**
- ✓ indicates a stage of the impact is considered.

---

**Ransomware (Impact):**
- **Respond**
- **Recover**
Key Takeaways

- Employ Data Lifecycle Management
- Effectively Manage Delivery vs Payloads
- Better Diagnostics: Reduce Noise Signals
- Appropriate Level of Response to Risk
- Top-Down Security Assessment
- Determine What Can / Can’t Be Controlled
- Make RPO & RTO Great Again

proofpoint.