Ransomware…NOT Coming to a City Near You

Marc Bleicher
CTO, Surefire Cyber
Agenda

- Ransomware Scare-tistics
  - By the numbers FBI ransomware statistics
  - Where is ransomware impacting cities
  - Trends of ransomware over the last 3 years
- Part 1—In a Ransomware Situation
  - Ransomware lifecycle
  - The parts of the attack you don’t see
  - Why are municipalities a target
- Part 2—What You Can Do
  - Recommendations
  - Things to Consider
  - Steps to become resilient
  - Resources and where to get help
Ransomware FBI Statistics (~Last 3 Years)

# of Ransomware Complaints received by the FBI Internet cybercrime center (IC3)

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>3,729</td>
</tr>
<tr>
<td>2020</td>
<td>2,047</td>
</tr>
<tr>
<td>2021</td>
<td>2,474</td>
</tr>
</tbody>
</table>

Adjusted Losses

- **$49.2 M+**: 2019
- **$29.1 M+**: 2020
- **$8.9 M+**: 2021

*Adjusted Loss does not include estimates of:
- Lost business
- Time/Wages
- Data/Files
- Systems/Equipment
- 3rd party services

*Note: The adjusted loss figures do not include estimates for 3rd party services.*
Ransomware Municipality Impact

City and Municipality Areas Targeted

- Cities/Townships: 28%
- County: 25%
- Library: 16%
- Law Enforcement: 14%
- Education: 13%
- Other: 4%

$665,000 to $40.53M

Breach costs

53.2%

Attacks targeted towards cities & local schools

10

# of days in downtime

Surefire Cyber Inc. Confidential and Proprietary
Ransomware Attacks 2013-Present
Ransomware & Extortion Trends

**Supply Chain Attacks**

- SolarWinds
- Kaseya
- Colonial Pipeline
- JBS SA

**Double Extortion**

Monetize the victims' weak spots

- Encrypt data (1)
- Exfiltrate data (2)
- Multiple-ways to profit from the same victim

**RaaS**

Ransomware as a Service (Raas)

- SaaS model for ransomware
- Like a franchise or subscription for cyber criminals

**Access Brokers**

Step 1 in ransomware attacks

- Cybercriminals who specialize in breaching companies
- Selling the access to ransomware groups

**DDoS**

Denial of Service

- Adds another level of extortion to the attack
- Increases pressure on the victim to pay

Hit one target that provides collateral impact across many
A Glimpse into Ransomware

What you see and What you don’t see
Ransomware Lifecycle

The Attack

Discovery
1-3 Days

1 - 3 Days

Due Diligence/OFAC

Negotiations

2 days to a week+

Going on in parallel
- Forensic Investigation
- Network and Endpoint Monitoring

Restoration & Recovery

Weeks to Months

Ransom Settlement

3-12 hours

Surefire Cyber Inc. Confidential and Proprietary
Reconnaissance for Ransomware

1. Identify a vulnerable target(s)
2. Determine profitability of a successful attack
3. Determine how to exploit the vulnerability
Initial Access Brokers

What’s for Sale?
• Administrator Credentials
• Web Shell Access
• Remote Desktop Access
• VPN Access
• Remote Management Tool Access
• Admin Panel Access
• By Request on-demand access

Initial Access Brokers (IABs) specialize in breaching organizations then selling access to ransomware threat actors.
**Negotiations & Recovery Strategy**

- Determine if you have backups
- Test and Validate backups are viable
- Assess overall damage & level of effort to restore basic operations
- Threat actor communications to stall or gain additional information
- Obtain as much proof-of-life to determine & validate value of data
- Who else is exposed and at risk with staying down or having data leaked?
- What’s the impact if your data gets leaked
- What are there regulatory and compliance impacts?
- Are there other means to recover the data. Think outside the box...(email attachments)
- Who is paying, how much, who is responsible for what?
- How long would you be able to continue as BAU without paying?
- What are the consequences of an extended outage?
Restoration and Recovery

- Business Interruption
- Notification Requirements
- Forensic Investigation
- Expertise/Consultants
- Legal Fees
- Lost Revenue

Baltimore

- Original Ransom Demand: $76,000
- Total Cost to Recover: $18 Million

Atlanta

- Original Ransom Demand: $51,000
- Total Cost to Recover: $17 Million

Surefire Cyber Inc. Confidential and Proprietary
How is ransomware run like a business?

- Ransomware-as-a-Service
- Internal policies and Hierarchies
- HR and Recruitment
- Ecosystem of with funding and full-service vendors
  - Providers
  - Product Creators
  - Financiers
- Re-investment to scale the business
- Innovation is rewarded
What Makes You a Target?

- Attacks at certain times of the year on critical services and systems increase pressure
- Increase in attacks starting in late summer. Before and over the holiday season
- Type and volume of data
  - Gateway to critical infrastructure
  - Access to public records also gives access to cyber criminals to exploit
  - Contractual, billing, and financial information for the municipality and citizens
- Lack of funding
  - Cybersecurity staff
  - Limited ability to acquire and implement technology, policies and training
- Municipalities are ideal targets because of the essential services provided to citizens
  - For profit businesses can go under, but governments cannot
- Smart cities expand the attack surface
  - More connected devices means more opportunity for attack
  - Internet of Things (IoT) used across different city services
  - Web of linked systems with that are connected through a variety of platforms
What You Can Do Now

Don’t Become a Victim
Top 5 Tech Recommendations

1. **Backups**
   - Offsite/Offline or Off network backups
   - If feasible consider leverage cloud capabilities
   - Ability to restore your critical data is the most significant factor in determining whether to pay a ransom or not

2. **Multi-factor Authentication**
   - Require MFA for as many services as possible prioritizing mail, remote access and accounts with access to critical data
   - Prioritize MFA for remote employees and users who have elevated privileges based on their role

3. **Endpoint Security**
   - Anti-virus software won’t cut it anymore
   - Advanced endpoint detection and response software should be installed on as many critical systems as standard practice
   - Ideally every device should have advanced endpoint security

4. **Patching & Updates**
   - Timely patching is one of the most efficient and cost-effective steps your organization can take
   - A lot of organizations outsource this responsibility

5. **Insurance & Planning**
   - Verify you have cyber insurance and what it includes
   - Create an Incident Response plan with communication protocols and a list of key stakeholders to call in when there is an incident
   - Test your IR Plan at least twice a year
Do’s and Do Nots of Ransomware

**Do**

• Take Systems off the network
• Preserve all data and systems
• Engage cyber insurance and legal counsel
• Engage with an external response firm
• Exercise your BCP and IR Plan

**Do Not**

• Power systems off
• Wipe/re-build data and systems
• Attempt anything without legal advice from counsel & carrier
• Attempt to communicate with the threat actor
• Discuss anything outside the communication protocols
5 Things to consider Now

1. What does your insurance policy cover in terms of BI, EO, etc. and does it have extortion and ransomware clauses?
2. Does your municipality have a practical and easy to follow IR Plan with response & communication protocols?
3. Who else is at risk if we get attacked? (citizens, services, partners, etc.)
4. Who makes the decision on whether to negotiate with the criminals and approve a ransom?
5. What is the absolute worst-case scenario we could be in?
State & Federal Resources

CISA
Resources for State, Local, Tribal, and Territorial (SLTT) Governments
- https://www.cisa.gov/uscert/resources/sltt
- https://www.cisa.gov/uscert/search?g=state%20resources

NGA (National Governors Association)
- https://www.nga.org/center/publications/cyber-liability-insurance-for-states/

Multi-State Information Sharing and Analysis (MS-ISAC)
- https://www.cisecurity.org/ms-isac
- https://learn.cisecurity.org/ms-isac-registration
- https://learn.cisecurity.org/ei-isac-registration (Election Information Sharing & Analysis)
Private Sector Resources

• **NetDiligence**
  - Breach Plan Connect (Build a practical and custom Incident Response Plan)
  - eRisk Hub a go-to resource for all things relevant to insurance, cybersecurity, and planning
    • [https://eriskhub.com/](https://eriskhub.com/)

• **Information Sharing and Analysis (ISAO)**
  - List of all 50 states Cyber Information Sharing Groups
    • [https://www.isao.org/information-sharing-groups/](https://www.isao.org/information-sharing-groups/)

• **Security Vendors & Cyber Insurance Resources Programs**
  - No shameless plugs please reach out to marc@surefirecyber.com for a full list and recommendations
Q&A