Table of Contents

1. Top 10 MOST COSTLY Ransomware infections from 2019
2. Ransomware Technical Analysis
3. Defensive Framework
4. Summary
5. Conversation/Discussion
10. Albany, N.Y.

Recovery And Mitigation Costs: $300,000

Strain? Undisclosed
How? Undisclosed
Damage? Minimal – No massive outage
Story? Albany had backups!

Recovery And Mitigation Costs: $400,000

Strain? Ryuk

How? Undisclosed

Damage? Law enforcement down (no 911)

Story? County paid $400,000 ransom and received key.

2 week outage
8. Lake City, Fla.

**Recovery And Mitigation Costs:** $500,000

Strain? Ryuk
How? Undisclosed
Damage? Everything but police and fire depts.
Story? Initial ransom was $700K, negotiated to $460K. Estimated that recovery would have been 3X more costly

Recovery And Mitigation Costs: Less than $1 mil

Strain? Ryuk
How? Undisclosed
Damage? Only 158 of 3,500 desktops
Story?

1. Demanded $5.3 million in bitcoin
2. City countered with $400,000
3. Attacker rejected counteroffer
4. City went about restoring from backups
6. Riviera Beach, Fla.

Recovery And Mitigation Costs: $1.5 million

Strain? Undisclosed
How? Email Attachment
Damage? All online systems, email, phones & water pump stations.
Story? After 3 weeks, city council agreed to paid $592K.
5. New Orleans

Recovery And Mitigation Costs: At Least $3 million

Strain? Ryuk

How? Email Phishing Link – entered creds

Damage? 450 servers, 3,500 laptops. No city data lost.
4. 22 Texas Towns

Recovery And Mitigation Costs: At least $12 million

Strain? Sodinokibi (so-dee'-no-kee-bee)

How? 3\textsuperscript{rd}-party provider infected

Damage? Most IT systems.

Story? After 3 weeks

- $3.25 incurred by county governments
- $2.34 million incurred by cities and towns
- $1.8 million incurred by educational institutions
- $5 million miscellaneous in nature.
3. Baltimore

Recovery And Mitigation Costs: $18.2 million

Strain? RobbinHood
How? Undisclosed
Damage? Online payments, email down
Story? Demand for roughly $76,000 in exchange for a decryption key – city refused.

- $8.2 in lost revenue
- $10 mil in recovery
- $2.8 in forensics and detection
- $5 mil for new systems
2. Norsk Hydro

Recovery And Mitigation Costs: $71 mil

Strain? LockerGoga

How? Undisclosed but used PsExec to spread.

Damage? Production down

Story? Norsk Hydro being forced to switch off production lines and resort to manual operations for reporting, billing and invoicing.
1. Demant

Recovery And Mitigation Costs: $95 mil

Strain? Undisclosed
How? Undisclosed
Damage? All IT system down for 7+ weeks.
Threats Haven’t Changed… nor has the way we protect and defend them.

- **Commodity Malware**
- **Insiders**
- **Hacktivists**
- **Terrorists**
- **Organized Crime**
- **State Sponsored**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Gain</td>
<td>Scareware, Spam/Phishing, Ransomware</td>
</tr>
<tr>
<td>Revenge</td>
<td>Edward Snowden, Chelsea (Bradley) Manning</td>
</tr>
<tr>
<td>Financial Gain</td>
<td>Ohio Company</td>
</tr>
<tr>
<td>Notoriety</td>
<td>Anonymous, WikiLeaks</td>
</tr>
<tr>
<td>Fundraising</td>
<td>ISIS, Antifa Cyber Army</td>
</tr>
<tr>
<td>Communications</td>
<td>Credit, Debit Card, ACH, PHI, PCI Theft</td>
</tr>
<tr>
<td>Propaganda</td>
<td>N. Korea, Russia, Iran, USA?</td>
</tr>
</tbody>
</table>

- **Financial Gain**
- **Revenge**
- **Financial Gain**
- **Defamation**
- **Notoriety**
- **Fundraising**
- **Communications**
- **Propaganda**

...nor has the way we protect and defend them.
Attackers are methodical and often predictable

Anatomy of an Attack: Threat Kill Chain

- **Reconnaissance & Planning**
  - Spearphishing

- **Initial Compromise**
  - Malware

- **Command & Control**
  - Brute force and unauthorized account access

- **Lateral Movement**
  - VPN

- **Target Attainment**
  - Financial transfer

- **Exfiltration Corruption Disruption**

---

**Exfiltration**
**Corruption**
**Disruption**
Ransomware Infection Timeline

- T-00:00: Exploitation and Infection
- T-00:05: Delivery and Execution
- T-00:10: Backup Spoliation
- T-02:00: File Encryption
- ~T-15:00: User Notification and Cleanup
Initial Exploit and Infection

Unusual Activity Detected
We detected something unusual about a recent activity to your Microsoft e-mail account. To help keep you safe, we required an extra security challenge. You will need to verify your Microsoft e-mail account below to confirm that the recent activity was yours and to regain access and enjoy our unlimited service. Failure to verify will lead to permanent suspension of your account.

Verify Now

What happened?

- Using a shared computer to access your account.
- Logging in your Microsoft account from blacklisted IP.
- Not logging off your account after usage.

Thanks for using your Microsoft account to bring the people we can change your connection settings anytime and find more at https://profile.live.com/services.

Unusual Activity Detected

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information: www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

The Microsoft team
Initial Exploit and Infection

- Phishing
  - Links
  - Attachments

- Exploit kits
  - Favor Adobe Flash and IE vulnerabilities
Connection to a C&C Server
Ransomware Delivery and Execution (1 of 2)

- Delivered via SSL
  - Difficult to recover executable from wire
- Executable files in %APPDATA% and %TEMP%
- Auto-execution on restart
Ransomware Delivery and Execution (2 of 2)

- Registry keys for the persistence are added in various places, i.e:
  - HKEY_USERS -> [current user’s SID]:
    - “Software\Microsoft\Windows\CurrentVersion\Run”
    - “Software\Microsoft\Windows\CurrentVersion\RunOnce”
    - “Software\Microsoft\Windows\CurrentVersion\Policies\Explorer” -> “Run”
    - “Software\Microsoft\Command Processor” -> “AutoRun”
• **Ryuk** will spread through the network using PsExec or Group Policy trying to infect as many endpoints and servers as possible.

• Unpatched systems via RDP (especially public facing)

• SMB – Server Message Block v1 & v2. Used for Network Shares.
Suspicious Process Activity

- **Remove** Windows volume *shadow copies*
  - vssadmin.exe delete shadows /all /quiet
  - WMIC.exe "shadowcopy delete"
- **Boot Config Modification - BCDEdit.exe**
  - C:\Windows\System32\bcdedit.exe" /set {current} safeboot network
  - Bcdedit.exe "/set {default} recoveryenabled no"
New Process: Excessive File Access

- New Process: Usually a never seen before
- Excessive File Access

```
<table>
<thead>
<tr>
<th>Log Date</th>
<th>11/12/2016 8:01:00.008 am</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Log Date</td>
<td>11/12/2016 8:01:00.008 am</td>
</tr>
<tr>
<td>Last Log Date</td>
<td>11/12/2016 8:01:00.008 am</td>
</tr>
<tr>
<td>Object</td>
<td>C:\Users\Charles.Lindbergh\AppData\Roaming\</td>
</tr>
<tr>
<td>Object Name</td>
<td>Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td>
</tr>
<tr>
<td>Priority</td>
<td>47</td>
</tr>
<tr>
<td>Process Name</td>
<td>7zbcda.exe</td>
</tr>
<tr>
<td>Process ID</td>
<td>33632</td>
</tr>
<tr>
<td>Session</td>
<td>SHA1=F44AC74B7AD88D1A09D182635DA27FCB3D90B9EF</td>
</tr>
</tbody>
</table>
```

Top Common Event

- Object Accessed 2.626k

```
<table>
<thead>
<tr>
<th>Type Here</th>
<th>Type Here</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Blanks)</td>
<td>(NonBlanks)</td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\AppData\Roaming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\AppData\Roaming\7z.dll</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\Documents\File1025.txt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\Documents\File1024.txt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\Documents\File1023.txt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Users\Charles.Lindbergh\Documents\File1022.txt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
User Notification

• Extortion demand and instructions for payment and decryption stored to hard drive
• Often saved to same folder as encrypted files
• Variants often distinguishable by how instructions are presented
  
  • CryptoWall v3 example: HELP_DECRYPT.(txt/png/html/url)
  • CryptoWall v4 example: HELP_YOUR_FILES.(txt/png)
  • Locky: changes desktop wallpaper to instructions
Most variants remove themselves after encryption has completed

```plaintext
====[Actions]===
"C:\WINDOWS\system32\cmd.exe" /c DEL C:\Users\ \Desktop\59DDDE~1.EXE
C:\Users\ \AppData\Roaming\nhkcxha.exe
bcdedit.exe /set {current} advancedoptions off
bcdedit.exe /set {current} optionsedit off
bcdedit.exe /set {current} bootstatuspolicy IgnoreAllFailures
bcdedit.exe /set {current} bootems off
bcdedit.exe /set {current} recoveryenabled off
"C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet
"C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet
"C:\WINDOWS\system32\cmd.exe" /c DEL C:\Users\ \AppData\Roaming\nhkcxha.exe
"C:\WINDOWS\system32\NOTEPAD.EXE" C:\Users\ \Desktop\help_recover_instructions.TXT
```
You are Infected - What can you do?

1. Pay Ransom and HOPE you get the decryption key!
2. Wipe System & Restore from backup
Ransomware

Defensive Best-Practices
Defend Against Ransomware (1 of 2)

• Maintain BACKUPS
• Educate yourselves and your users
  • Don’t open dubious attachments
  • Don’t click on dubious links
• Develop run books
  • Ransomware incident response & disaster recovery plans
• PATCH, PATCH, PATCH!
  • 75% of breaches are because of NO PATCHING.
• Disable macros
• Be cautious of small zipped files (.zip .rar .gz .7z)
Defend Against Ransomware (2 of 2)

- Invest in Security - Products and Personnel
  - NG Firewalls, IDS/IPS, email filter, AV, SIEM & UEBA
  - Pay the 🍀️ for Security Analysts
- LEAST PRIVILEGE – users have more rights than they need
- Correlate against Threat Lists
- Endpoint tools (EDR – Endpoint, Detection & Response)
  - Updated Anti-Virus signatures; App Whitelisting
  - Monitor for Ransomware behaviors
- Password complexity enforcement
- Insurance Policy
Ransomware

Defensive Framework
Connection to a C&C Server

- Connect to a Command And Control (C2) node
Detecting Ransomware: Suspicious Executables

- Ransomware delivery and execution
  - Network traffic rules
  - File execution from %APPDATA% and %TEMP%
Detecting Ransomware: Autorun Registry Keys

- Monitor Registry Run Keys

### Registry Integrity Monitor Policy Manager
- **Launch Policy Item Manager**

<table>
<thead>
<tr>
<th>Action</th>
<th>Policy Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MS SQL Server Registry</td>
<td>Monitor registry changes involving MS SQL Server</td>
</tr>
<tr>
<td></td>
<td>RBP Dono Runtino</td>
<td>Monitor registry changes involving RBP Dono Runtino</td>
</tr>
<tr>
<td></td>
<td>AutoRun Keys</td>
<td>Monitor registry changes involving AutoRun Keys</td>
</tr>
</tbody>
</table>

**AutoRun Keys Policy Properties**
- **Name**: AutoRun Keys
- **Description**: This policy monitors the standard L4 AutoRun keys on all major versions of Windows

<table>
<thead>
<tr>
<th>Monitored Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Containment

- Kill processes
  - Endpoint protection system
- Remove host’s network connectivity
  - Switch port, WI-FI block
  - Disable host NICs
- Forcefully and quickly shut down host

```powershell
#LocalHost
if($LocalHost -like $ImpactedHost)
{
    Get-WmiObject -Class Win32_NetworkAdapter -ComputerName $ImpactedHost -Filter 'NetConnectionStatus = 2' | %{ $_.disable() }
}
```

```powershell
#LocalHost
if($LocalHost -like $ImpactedHost -OR $LocalIP)
{
    Stop-Computer -Force -ComputerName $ImpactedHost
}
```

#RemoteHost