REN-ISAC and FBI
2019 Threat Briefing

PERVASIVE THREATS IN CYBERSECURITY

Kristen Lane, FBI Cyber Division Intelligence Analyst
Kim Milford, REN-ISAC Executive Director
REN-ISAC: What We See
<table>
<thead>
<tr>
<th>INCIDENTS</th>
<th>Q3</th>
<th>Q2</th>
<th>Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Machines</td>
<td>9,829</td>
<td>15,318</td>
<td>12,332</td>
</tr>
<tr>
<td>Compromised Credential Notifications</td>
<td>5,709</td>
<td>3,119</td>
<td>2,204</td>
</tr>
<tr>
<td>Spam/Phish</td>
<td>252</td>
<td>275</td>
<td>48</td>
</tr>
<tr>
<td>Vulnerable Machines</td>
<td>168</td>
<td>7</td>
<td>25</td>
</tr>
<tr>
<td>Open Recursive DNS Resolvers</td>
<td>507</td>
<td>429</td>
<td>496</td>
</tr>
<tr>
<td>Open Mail Relays</td>
<td>13</td>
<td>21</td>
<td>15</td>
</tr>
<tr>
<td>Other</td>
<td>41</td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>16,519</strong></td>
<td><strong>19,181</strong></td>
<td><strong>15,141</strong></td>
</tr>
</tbody>
</table>
REN-ISAC CSIRT ACTIVITY, 2019

REN-ISAC CSIRT Incidents, Historical

- **2017**
  - Compromised Machines: 17,000
  - Compromised Credentials: 2,000
  - Spam/Phish: 1,000
  - Open Recursive DNS Resolvers: 1,000
  - Open Mail Relays: 1,000
  - Other: 1,000

- **2018**
  - Compromised Machines: 18,000
  - Compromised Credentials: 3,000
  - Spam/Phish: 2,000
  - Open Recursive DNS Resolvers: 2,000
  - Open Mail Relays: 2,000
  - Other: 2,000

- **2019**
  - Compromised Machines: 19,000
  - Compromised Credentials: 4,000
  - Spam/Phish: 3,000
  - Open Recursive DNS Resolvers: 3,000
  - Open Mail Relays: 3,000
  - Other: 3,000

#EDU19
COMPROMISED CREDENTIALS
Chegg Data Breach

- April: Breach
- Sept: Chegg notifies victims and regulatory authorities
- Oct: REN-ISAC received raw dump of credentials from an information sharing partner
  - 1500 emails sent to .edu domains with over 4,300,000 credentials
  - Feedback: significant re-use of credentials
Stolen Credentials

- Data exfiltration
- Phishing
- Privilege escalation
- Access to discounts and resources
- Underreported
  - If reported at all, generally a long delay
- Risk is uncertain, depends on circumstances
  - Requires analysis & resources
CYBERSECURITY EDUCATION
MULTI-FACTOR AUTHENTICATION
VULNERABILITIES AND EXPLOITS
REN-ISAC COMPROMISED MACHINES

Malware Exploit Incidents, 3Q 2019

Andromeda
Conficker
Nymaim
WannaCry
Ranybus
Tinba
Gozi
Mirai
Gamut
Matsnu
### COMPROMISED MACHINE INCIDENTS

#### Top 10 Exploits, 3Q 2019

<table>
<thead>
<tr>
<th>Exploit</th>
<th>Incidents Reported</th>
<th>Year Discovered</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andromeda</td>
<td>4787</td>
<td>2011</td>
<td>Botnet</td>
</tr>
<tr>
<td>Conficker</td>
<td>863</td>
<td>2008</td>
<td>Botnet</td>
</tr>
<tr>
<td>Nymaim</td>
<td>832</td>
<td>2013</td>
<td>Ransomware</td>
</tr>
<tr>
<td>WannaCry</td>
<td>402</td>
<td>2017</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Ranybus</td>
<td>385</td>
<td>2014</td>
<td>Spyware</td>
</tr>
<tr>
<td>Tinba</td>
<td>294</td>
<td>2012</td>
<td>Banking</td>
</tr>
<tr>
<td>Gozi</td>
<td>286</td>
<td>2013</td>
<td>Spyware</td>
</tr>
<tr>
<td>Mirai</td>
<td>248</td>
<td>2016</td>
<td>Botnet</td>
</tr>
<tr>
<td>Gamut</td>
<td>225</td>
<td>2013</td>
<td>Botnet</td>
</tr>
<tr>
<td>Matsnu</td>
<td>161</td>
<td>2014</td>
<td>Backdoor</td>
</tr>
</tbody>
</table>
RANSOMWARE
Ransomware

- Set ransomware strategy
- Evaluate current storage methods for scalability, security, manageability, and currency.
- Create backup strategy, consider 3-2-1
- Review RTO and RPO to ensure preparations in place to meet expectations
- Backup: On-site, cloud, hybrid, offline
OTHER NOTABLE TRENDS

- Cyberespionage
- ANU Breach Report
Session Evaluations

There are two ways to access the session and presenter evaluations:

1. In the online agenda, click on the “Evaluate Session” link.

2. From the mobile app, click on the session you want from the schedule > then scroll down or click on the associated resources > and the evaluation will pop up in the list.
References

• 2019 Verizon Data Breach Investigations Report
  • https://enterprise.verizon.com/resources/reports/dbir/

• FireEye Threat Report: APT40 Examining a China-Nexus Espionage Actor
  • https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

• Oct 2019 Chegg Data Breach

• Have I been pwned: https://haveibeenpwned.com/

Contact Information

FBI Incident Reporting: [https://www.ic3.gov/default.aspx](https://www.ic3.gov/default.aspx)
Kristen Lane: kmlane@fbi.gov

REN-ISAC Incident Reporting: soc@ren-isac.net
REN-ISAC General Inquiries: info@ren-isac.net
Kim Milford: kmilford@ren-isac.net

NOTE: This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution 4.0 International (CC BY 4.0), which grants usage to the general public, with appropriate credit to the author.