Zugzwang

a situation in which the obligation to make a move in one's turn is a serious, often **decisive**, disadvantage.
Measuring the Ransomware Threat

Ransomware Landscape & Trends
The Big Picture

Several ransomware measures were "down" in 2022
• Payments (dramatically)
• Attacks (less so)
• Lifespan per family (good news?)

Possible drivers:
• Law enforcement arrests
• Russia-Ukraine conflict
• Ransom payment penalties (sanctions)

2022 Key Ransomware Metrics

Publicly claimed victims (10.4%)

Total ransom payments (40.3%)

Average ransomware lifespan (in days) (54.2%)

Source: “Ransomware revenue fell by $300 million in 2022 as more victims refuse to pay: report”, The Record from Recorded Future News

“Ransomware Revenue Down As More Victims Refuse to Pay”, Chainalysis
Are ransoms getting worse over time?

<table>
<thead>
<tr>
<th>Spearman's Correlation Coefficient</th>
<th>1.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Value</td>
<td>0.000</td>
</tr>
</tbody>
</table>
But only 16% are paying

- "In this research, the victims whose information was published on and later removed from the leak sites of Conti and LockBit (versions 2.0 and 3.0, respectively) are assumed to have paid the ransoms (henceforth to be referred to as paid cases), from which a rate of ransom payment is calculated. During the research period, 274 out of 1,716 victim profiles disappeared. This makes for a ransom payment rate of approximately 16% based on this data source, though it should be noted that this rate will vary for other ransomware families."

Source: What Decision Makers Need to Know About Ransomware Risk Trend Micro, Waratah Analytics
Correlation against gang is very high!

<table>
<thead>
<tr>
<th>Spearmans Correlation Coefficient</th>
<th>0.952</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Value</td>
<td>0.000</td>
</tr>
</tbody>
</table>
Threats to Public Services

Ransomware trends against vulnerable sectors:

• Utilities
• Education
• Healthcare

“Critical infrastructure” covers a lot these days

CISA's priority sectors for 2023: water, hospitals, K-12

The industries slated for emphasis are “target-rich, resource-poor entities,” CISA Director Jen Easterly said. They’re also heavily targeted by ransomware.

Published Oct. 21, 2022
Recent Ransom & Extortion Incidents
Key Threats Involving Public Services & Infrastructure

Ordered by date of disclosure/acknowledgement and attributed to suspected or alleged/claimed group (where known)
Ransomware’s Indiscriminate Attack Patterns

Sample of Publicly Claimed Victims, 2022-23 (n = 1,164 victims)

- LockBit 3.0
- Clop
- ALPHV / BlackCat
- BianLian
- Black Basta
- Royal
- Vice Society
- Play

Average of 37 MITRE ATT&CK® Techniques per group!
Ransomware TTPs

Optimizing Defensive ROI
Setting the Stage: TTP Intelligence Trends

Increased awareness & adoption of a threat-informed mindset → growing public, ATT&CK mapped CTI reporting

Faster pivoting & translation into defensive capabilities

TTP Evolution
Some techniques are only used by one group.
Maximise your defensive advantage

<table>
<thead>
<tr>
<th>T1486</th>
<th>Data Encrypted for Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1083</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>T1082</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>T1490</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td>T1059</td>
<td>Command and Scripting Interpreter</td>
</tr>
<tr>
<td>T1047</td>
<td>Windows Management Instrumentation</td>
</tr>
</tbody>
</table>

Maximise your ransomware defense in 5 techniques

© 2023 Tidal Security, Inc. All rights reserved.
## Maximise your defensive advantage

<table>
<thead>
<tr>
<th>T1486</th>
<th>Data Encrypted for Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1083</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>T1082</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>T1490</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td>T1059</td>
<td>Command and Scripting Interpreter</td>
</tr>
<tr>
<td>T1047</td>
<td>Windows Management Instrumentation</td>
</tr>
</tbody>
</table>

### Maximise your ransomware defense in 5 techniques

![Diagram showing ransomware defense techniques and intersection size](image-url)
<table>
<thead>
<tr>
<th>Technique ID</th>
<th>Technique Name</th>
<th>Tactic</th>
<th>Count from CTI</th>
<th>Mapped Data Components</th>
<th># Sigma Analytics</th>
<th># Atomic Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1486</td>
<td>Data Encrypted for Impact</td>
<td>Impact</td>
<td>50</td>
<td>6</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>T1082</td>
<td>System Information Discovery</td>
<td>Discovery</td>
<td>30</td>
<td>4</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td>T1083</td>
<td>File and Directory Discovery</td>
<td>Discovery</td>
<td>29</td>
<td>3</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>T1490</td>
<td>Inhibit System Recovery</td>
<td>Impact</td>
<td>23</td>
<td>5</td>
<td>18</td>
<td>9</td>
</tr>
<tr>
<td>T1059.001</td>
<td>PowerShell</td>
<td>Execution</td>
<td>20</td>
<td>5</td>
<td>183</td>
<td>22</td>
</tr>
<tr>
<td>T1047</td>
<td>Windows Management Instrumentation</td>
<td>Execution</td>
<td>19</td>
<td>3</td>
<td>40</td>
<td>10</td>
</tr>
<tr>
<td>T1489</td>
<td>Service Stop</td>
<td>Impact</td>
<td>17</td>
<td>7</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>T1112</td>
<td>Modify Registry</td>
<td>Defense Evasion</td>
<td>16</td>
<td>6</td>
<td>65</td>
<td>44</td>
</tr>
<tr>
<td>T1562.001</td>
<td>Disable or Modify Tools</td>
<td>Defense Evasion</td>
<td>16</td>
<td>6</td>
<td>77</td>
<td>38</td>
</tr>
<tr>
<td>T1059.003</td>
<td>Windows Command Shell</td>
<td>Execution</td>
<td>14</td>
<td>2</td>
<td>21</td>
<td>5</td>
</tr>
<tr>
<td>T1190</td>
<td>Exploit Public-Facing Application</td>
<td>Initial Access</td>
<td>14</td>
<td>2</td>
<td>80</td>
<td>0</td>
</tr>
<tr>
<td>T1133</td>
<td>External Remote Services</td>
<td>Persistence, Initial Access</td>
<td>13</td>
<td>3</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>T1021.001</td>
<td>Remote Desktop Protocol</td>
<td>Lateral Movement</td>
<td>13</td>
<td>4</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>T1018</td>
<td>Remote System Discovery</td>
<td>Discovery</td>
<td>13</td>
<td>4</td>
<td>15</td>
<td>20</td>
</tr>
</tbody>
</table>
### Defending Against Top Observed Ransomware Techniques

**Some Thoughts**

<table>
<thead>
<tr>
<th>Technique ID</th>
<th>Technique Name</th>
<th>Tactic</th>
<th>Count from CTI</th>
<th>Mapped Data Components</th>
<th># Sigma Analytics</th>
<th># Atomic Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1082</td>
<td>System Information Discovery</td>
<td>Discovery</td>
<td>30</td>
<td>4</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td>T1083</td>
<td>File and Directory Discovery</td>
<td>Discovery</td>
<td>29</td>
<td>3</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>T1059.001</td>
<td>PowerShell</td>
<td>Execution</td>
<td>20</td>
<td>5</td>
<td>183</td>
<td>22</td>
</tr>
<tr>
<td>T1047</td>
<td>Windows Management Instrumentation</td>
<td>Execution</td>
<td>19</td>
<td>3</td>
<td>40</td>
<td>10</td>
</tr>
<tr>
<td>T1112</td>
<td>Modify Registry</td>
<td>Defense Evasion</td>
<td>16</td>
<td>6</td>
<td>65</td>
<td>44</td>
</tr>
<tr>
<td>T1562.001</td>
<td>Disable or Modify Tools</td>
<td>Defense Evasion</td>
<td>16</td>
<td>6</td>
<td>77</td>
<td>38</td>
</tr>
<tr>
<td>T1133</td>
<td>External Remote Services</td>
<td>Persistence, Initial Access</td>
<td>13</td>
<td>3</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>T1021.001</td>
<td>Remote Desktop Protocol</td>
<td>Lateral Movement</td>
<td>13</td>
<td>4</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>T1018</td>
<td>Remote System Discovery</td>
<td>Discovery</td>
<td>13</td>
<td>4</td>
<td>15</td>
<td>20</td>
</tr>
</tbody>
</table>
Ransomware & Data Extortion Landscape

29 groups & families (& counting)

- Most-active threats, mainly based on leak site victim counts

704 technique references across 178 unique techniques & sub-techniques

A lot here! Prioritize (by what matters most to you)

- Industry threat analysis
- What can you detect now? What can’t you?
Intelligence-Informed Detection Engineering

Atomic Tests

- Atomic Test #1 - Steal Firefox Cookies (Windows)
- Atomic Test #2 - Steal Chrome Cookies (Windows)

Atomic Test #1 - Steal Firefox Cookies (Windows)

This test queries Firefox’s cookies.sqlite database to steal the cookie data contained within it, similar to zloody/Zoot’s cookie theft function. Note: If Firefox is running, the process will be killed to ensure that the DB file isn’t locked. See https://www.malwarebytes.com/resources/May-2020/The-silent-night-zookeeper-final.pdf.

Supported Platforms: Windows

auto_generated_guid: 4b437357-4ef4-d3d4-9af6-8c0c0e1826a

Product: Invoke-Atomic

Invoke-Atomic is a PowerShell module to execute tests as defined in the atomic list of Red Canary’s Atomic Red Team project. Visit the GitHub repository for Invoke-Atomic for installation and usage instructions.

Capabilities shown for “Credentials from Web Browsers”

- Browsers: Firefox / Chrome (Windows), Firefox / Microsoft Edge
- Disclosure Of Proxy Cookies with Pwning.py
-披露 Cookies of Web Browsers
- Cookies from Microsoft Edge
- Cookies from Browser
- Cookies from Web Browsers

Filter By:
- Capability
- Technique
- Type
- Platform
- Description
- Availability
Ransomware Payment Intelligence

Ransomware "Market" Overview
Stop using averages to describe your ransom data set.
Before and After our warning

Before our warning:

Amount of money earned monthly

After our warning:

Amount of money earned monthly

© 2023 Tidal Security, Inc. All rights reserved.
You can fit powerlaws or lognormals to ransom data.
But you shouldn't!

- Left is the KS distance
- Right is the probability (P-Value) that both severities are from the same distribution.
  - White is highly likely to be the same
  - Black is highly unlikely to be the same
- You can also do this for frequency and get similar results.
92% of ransoms are below average
July is peak ransom paying season

Number of ransoms paid monthly since 2019 (95% confidence levels)
On time and financial surveillance
Market Concentration and Ransomware

High Y-axis = "monopoly"
Low Y-axis = "free market"

Ransomware Extortion Trends Around Hive's Takedown

Announcement of FBI-led Hive infrastructure takedown
Thank you!