Ransomware as a Science

Bakuei Matsukawa (Trend Micro, Researcher), Erin Burns (Concinnity Risks, UK)
Vladimir Kropotov (Trend Micro, Researcher), Éireann Leverett (Concinnity Risks, UK)
Fyodor Yarochkin (Trend Micro, Researcher),
Robert McArdle (Trend Micro, Director FTR),
Shingo Matsugaya (Trend Micro, Researcher)

TLP: Amber
Agenda

Introduction
Sourcing the data
Understanding the data
Data fusion (playing with the data)
Conclusions and QA
Introduction

• We have data, lots of data of different types
• We try to view ransomware holistically, all groups, all types of victims
  • All ransomware actors (profiteers/state actors/noobs)
  • All victims (paying/not paying/blocked by endpoint)
  • Interdisciplinary (Binaries/Networks/Financials/Risk)
• We have some novel techniques for tracking threat actors
• We have some evidence for policy makers to consider
  • We are aiming for a theory of change beyond “make backups”
Data sources and knowledge domains

Detection Telemetry
Network Infrastructure

Underground forums
Various data leaks

Blockchain and Financial Transactions
Monetization strategies and Business processes

Time Series analysis
Statistical Methods
(DataSci/AI/ML/Quantum/ZeroTrust/Buzzword Bingo/ J/K)
How do we bridge all these?

- Financial Transactions
- Monetisation strategies
- Business processes
- Strategic
- Operational
- Technical
- Tactical
- Various data leaks
- Underground forums
- Detection Telemetry
- Network Infrastructure
- Binaries
How do we **bridge** all these?

Time Series Analysis!
Sourcing the data
## Detections: ransomware over time by geolocation

<table>
<thead>
<tr>
<th></th>
<th>Jul-21</th>
<th>Aug-21</th>
<th>Sep-21</th>
<th>Oct-21</th>
<th>Nov-21</th>
<th>Dec-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>26.5%</td>
<td>United States</td>
<td>20.2%</td>
<td>United States</td>
<td>19.5%</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>10.7%</td>
<td>France</td>
<td>7.2%</td>
<td>Hong Kong</td>
<td>9.9%</td>
</tr>
<tr>
<td>3</td>
<td>India</td>
<td>6.1%</td>
<td>India</td>
<td>6.5%</td>
<td>Germany</td>
<td>7.9%</td>
</tr>
<tr>
<td>4</td>
<td>Germany</td>
<td>4.8%</td>
<td>Hong Kong</td>
<td>5.8%</td>
<td>France</td>
<td>4.6%</td>
</tr>
<tr>
<td>5</td>
<td>Brazil</td>
<td>4.8%</td>
<td>Germany</td>
<td>4.6%</td>
<td>Turkey</td>
<td>4.2%</td>
</tr>
</tbody>
</table>
## Detection by business size

<table>
<thead>
<tr>
<th>Dec-21</th>
<th>Top 1 - United States</th>
<th>Top 2 - France</th>
<th>Top 3 - Hong Kong</th>
<th>Top 4 - Italy</th>
<th>Top 5 - India</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAZE</td>
<td>WCRY</td>
<td>WCRY</td>
<td>WCRY</td>
<td>WCRY</td>
</tr>
<tr>
<td></td>
<td>220</td>
<td>168</td>
<td>41</td>
<td>20</td>
<td>1,274</td>
</tr>
<tr>
<td></td>
<td>LOCKY</td>
<td>LOCKBIT</td>
<td>LOCKY</td>
<td>GANDCRAB</td>
<td>GANDCRAB</td>
</tr>
<tr>
<td></td>
<td>145</td>
<td>30</td>
<td>2</td>
<td>15</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>3 CRYPTOR</td>
<td>HIDDENETEAR</td>
<td>RYUK</td>
<td>MOUNTLOCKER</td>
<td>MOUNTLOCKER</td>
</tr>
<tr>
<td></td>
<td>125</td>
<td>15</td>
<td>1</td>
<td>12</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>MOUNTLOCKER</td>
<td>Gorf</td>
<td>CRYPTOMODADV</td>
<td>SODINOKIBI</td>
<td>EGREGOR</td>
</tr>
<tr>
<td></td>
<td>106</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>MORRISCRIPT</td>
<td>THANOS</td>
<td>Cryptomod</td>
<td>EGREGOR</td>
<td>SODINOKIBI</td>
</tr>
<tr>
<td></td>
<td>71</td>
<td>7</td>
<td>1</td>
<td>7</td>
<td>33</td>
</tr>
</tbody>
</table>

### Enterprise

|        | MAZE                  | WCRY           | WCRY              | WCRY         | WCRY         |
|        | 176                   | 168            | 41                | 19           | 1,131        |
|        | LOCKY                 | LOCKBIT        | LOCKY             | HIVE         | GANDCRAB     |
|        | 63                    | 7              | 2                 | 2            | 94           |
|        | 3 GANDCRAB            | HIDDENETEAR    | CRYPTOMODADV      | LOCKY        | MOUNTLOCKER  |
|        | 61                    | 4              | 1                 | 2            | 66           |
|        | WCRI                  | WANA           | ERIS              | CRYPTCTB     | EGREGOR      |
|        | 46                    | 3              | 1                 | 2            | 42           |
|        | Filecoder             | Gorf           | WANA              | CONTI        | SODINOKIBI   |
|        | 43                    | 3              | 1                 | 1            | 33           |

### SMB

|        | CRYPTOR              | LOCKBIT        | Genasom           | GANDCRAB     | WCRY         |
|        | 125                   | 21             | 1                 | 15           | 120          |
|        | MORRISCRIPT           | Gorf           | MOUNTLOCKER       | SODINOKIBI   | StopCrypt    |
|        | 71                    | 6              | 1                 | 8            | 3            |
|        | MOUNTLOCKER           | CRYPTESLA      | SODINOKIBI        | EGREGOR      | PolyRansom   |
|        | 70                    | 1              | 1                 | 7            | 2            |
|        | LOCKY                 | CRYPTOX        | CONTI             | LOCKBIT      |              |
|        | 55                    | 1              | 5                 |              | 2            |

### Consumers

|        | CERBER                | THANOS         | RYUK              | CERBER       | WCRY         |
|        | 32                    | 6              | 1                 | 6            | 23           |
|        | LOCKY                 | HIDDENETEAR    | CRYPTOMODADV      | StopCrypt    | StopCrypt    |
|        | 27                    | 5              | 3                 | 4            | 12           |
|        | CRYPTOMODADV          | Gorf           | COBRA             | Gorf         | VIRLOCK      |
|        | 5                     | 3              | 1                 | 2            | 6            |
|        | GANDCRAB              | StopCrypt      | Shade             | CERBER       |                |
|        | 5                     | 3              | 1                 | 2            | 5            |
|        | WCRI                  | CERBER         | Shade             | PETYA        |              |
|        | 4                     | 2              | 1                 | 4            |              |
Frequency versus severity?

Number of Ransoms Paid monthly

Amount of money earned monthly

received_datetime

received_datetime

Number of Ransoms Paid monthly

Amount of money earned monthly

received_datetime

received_datetime
#Leaks sites

## Top 10 Ransom & Extortion Groups

<table>
<thead>
<tr>
<th>Ransom</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conti</td>
<td>805</td>
</tr>
<tr>
<td>LockBit</td>
<td>666</td>
</tr>
<tr>
<td>MAZE</td>
<td>330</td>
</tr>
<tr>
<td>Sodinokibi</td>
<td>309</td>
</tr>
<tr>
<td>Pysa</td>
<td>307</td>
</tr>
<tr>
<td>DoppelPaymer</td>
<td>206</td>
</tr>
<tr>
<td>Egregor</td>
<td>197</td>
</tr>
<tr>
<td>Avaddon</td>
<td>184</td>
</tr>
<tr>
<td>NetWalker</td>
<td>178</td>
</tr>
<tr>
<td>CLOP</td>
<td>119</td>
</tr>
</tbody>
</table>

## Top 10 Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>2477</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>263</td>
</tr>
<tr>
<td>France</td>
<td>251</td>
</tr>
<tr>
<td>Canada</td>
<td>234</td>
</tr>
<tr>
<td>Germany</td>
<td>201</td>
</tr>
<tr>
<td>Italy</td>
<td>189</td>
</tr>
<tr>
<td>Australia</td>
<td>96</td>
</tr>
<tr>
<td>Spain</td>
<td>93</td>
</tr>
<tr>
<td>India</td>
<td>88</td>
</tr>
<tr>
<td>Brazil</td>
<td>86</td>
</tr>
</tbody>
</table>
Leaks: Targeted sector

- IT, 9.6%
- Financial, 7.6%
- Construction, 6.9%
- Professional Services, 6.6%
- Health Care, 6.5%
- Materials, 6.2%
- Manufacturing, 5.8%
- Transportation, 5.2%
- Legal, 4.7%
- Retail, 4.2%
- Foods & Staples, 4.3%
- Academic, 3.5%
- Automobiles, 3.7%
- Energy & Utilities, 3.2%
- Apparel & Fashion, 3.1%
- Media & Entertainment, 3.0%
- Government, 2.9%
Leaks: Targeted region over time
Leaks: Groups activity over time
Number of leaks over time Conti

Time (monthly since August 2020 till April 2022) Paid/Not Paid
Where paid?

United Kingdom:
- Paid: 3 (5.4%)
- Not Paid: 53 (94.6%)

France:
- Paid: 3 (8.6%)
- Not Paid: 32 (91.4%)

Canada:
- Paid: 6 (11.5%)
- Not Paid: 46 (88.5%)

Italy:
- Paid: 2 (7.1%)
- Not Paid: 26 (92.9%)

Germany:
- Paid: 5 (10.2%)
- Not Paid: 44 (89.8%)

United States:
- Paid: 53 (11.5%)
- Not Paid: 408 (88.5%)
A decade of ransoms isn’t an emergency. This is a long game now, and we need better strategy.
Ransoms summed by time of day in UTC

Ransom sums hourly from named families with Error Bands (95% confidence)
Ransom frequency by month
Most people pay very quickly

Delaying payment might be a good nudge towards not paying.

As you can see here, 50% of those who pay do so in about a week.
Understanding the data
What are the risks to the RAAS users?

Access to the “victim” infrastructure
Risks of “victims” not paying the ransom
Ransomware infrastructure
Ransomware group: services and people
Cost of Access 40k, lower bound of ransom >40K
2 weeks later attempt to extort for 500k (upper bound)
Data Fusion
Threat Actor Metrics

Persistence of attack attempts (single, low hanging fruits, advanced)
Dependence Ransom on the victim size, revenue, industry
Does Ransom is negotiable?
Targeted/opportunistic
Victim selection criteria (geo region, company scale, industries, geo/industry exclusion list i.e. not target medical and education
Operational cadence (frequency of access) -victims per week/size?
Method of initial access
33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB in one wallet. On May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB was transferred to address XXXXXXXXXXXXXX950klpjcauwuy4uj39ym43hs6cfssegq (the “Subject Address”), and it has not moved since.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.
People...
Ransoms correlate strongly to malware family

Spearmans correlation coefficient for family:

0.951

Samples are correlated (reject null hypothesis if $p < 0.05$):

$p = 0.000$

$N = 116761$
Severity characterizations

- Cerber Ransoms Value Over Time
- DMA-Locker Ransoms Value Over Time
- DeadBolt Ransoms Value Over Time
We can measure that statistical distance using the Cramer von Mises metric. Red shows they are similar and black shows they are very different. A better way to view that though is with the associated p-value of the distance metric.
Black here means we are almost certain the ransoms are drawn from different distributions, and white means it is highly likely they are drawn from the same distribution.

This could be a predator effect, or it could be a prey effect. In other words, because the victims are all similar (all use a certain technology or are a similar size), or it could be because the gangs negotiation tactics are similar.
Frequency Characterizations

Cerber Ransom Occurrences Per Week

Egregor Ransom Occurrences Per Week

DeadBolt Ransom Occurrences Per Week
Rapid cost estimation:

The impact of an event will typically cost between 10-50% of the Annual Returning Revenue of the company involved. Assuming no network segregation, no endpoint protection, and lateral movement on behalf of the attacker.
A theory of change beyond “make backups”

Most people aren’t paying. Given we know this, should we optimise DFIR for those who DON’T?

How do we increase the friction of people to pay?

- Sanctions
- KYC/AML
- Delays (less likely to pay as time goes on)?

How do we reduce the losses of those who choose not to pay?

Transition from “backup” to RESTORATION
A theory of change beyond “make backups” II

Traceability of transactions
Infrastructure policing
Micro-perimeterization
Business process policy
Negotiation onion denylisting
When you pay, you’re paying to victimise 10-20 others
Turn the tide:
  Calling out that most people are not paying regularly and with evidence
How much does this cost society?

- Estimated cost to society: $1,062,322,217.08
- Estimate fast where you are
- Prediction of risks and evolution of the threat landscape
Conclusion and Q&A

Scope of ransomware impacts
Broad overview of operating patterns of gangs
Time series analysis for DFIR
Evidence based policy recommendations

Join the MSR-SIG Data WG
Research team