
The value of (missing) security.

— Éireann Leverett —
@blackswanburst

Data > Dogma

Frequency

or

Severity

Q: Who gets hacked?

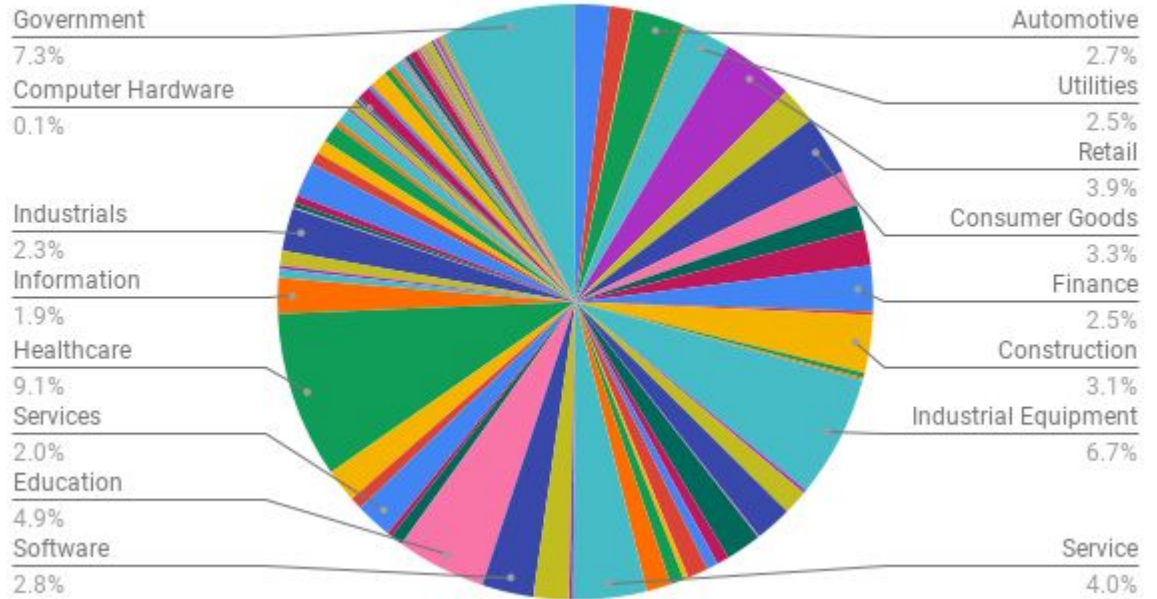


Everybody!

Image credit: an excellent twitter thread [1] on ransomware "targeting".

Hat-tip @uualen

Ransomware Attacks by Industry 2020 and 2021



Q: How do we know how much to spend?

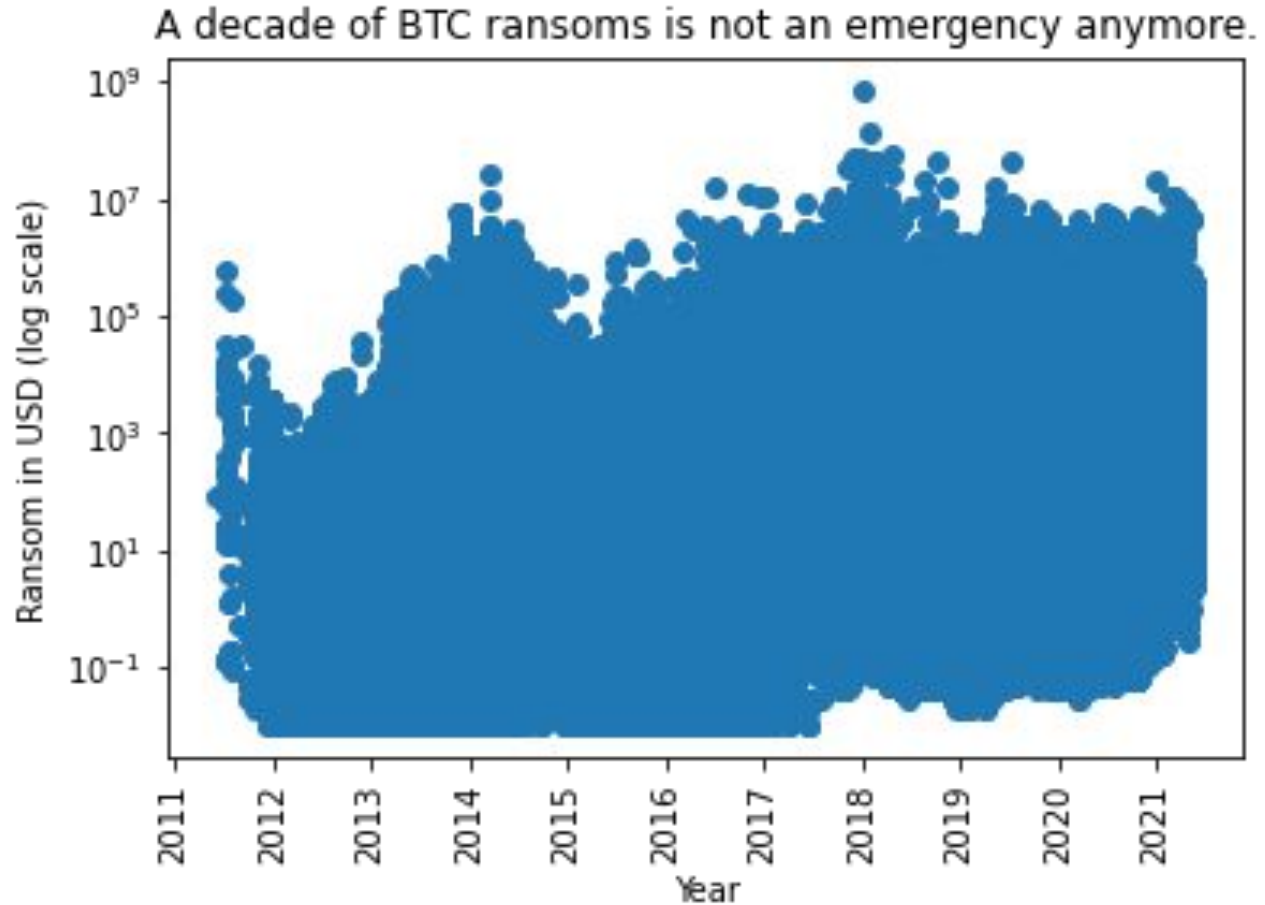


Initial access brokers are willing to spend up to 100k for access to 100 M dollar companies in the USA, averaging around 50k when doing so[1].

Ransom Sums by Family (USD)

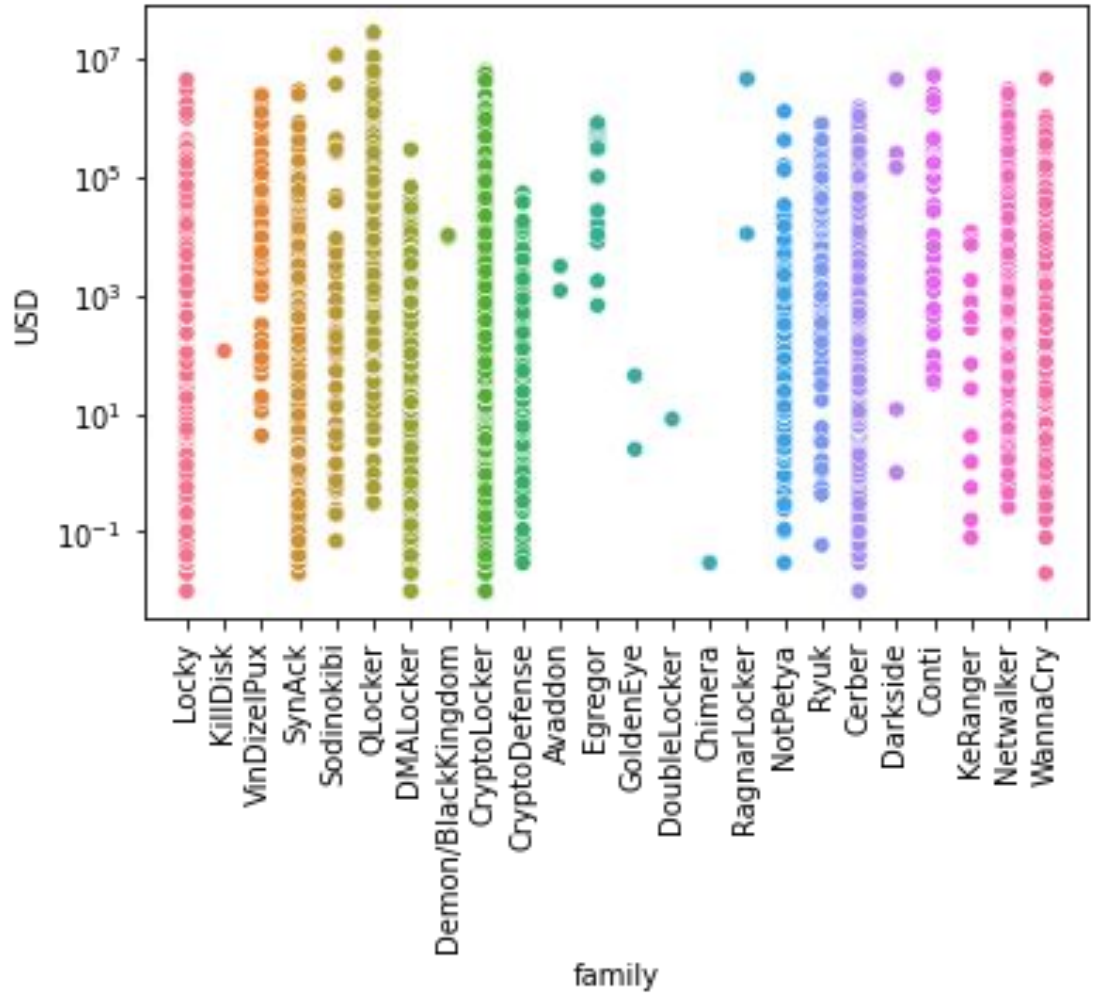


This is what ransomware looks like if you take the long and log view of a decade of activity.



So are some families more impactful than others? Are they capable of fetching bigger ransoms?

How do they determine their initial ransom price?



5% of ARR

General trend in negotiating[3]

10-40%

Of the ransomware insurance claim is the ransom.

10-50% of ARR

This is the cost of a catastrophe.

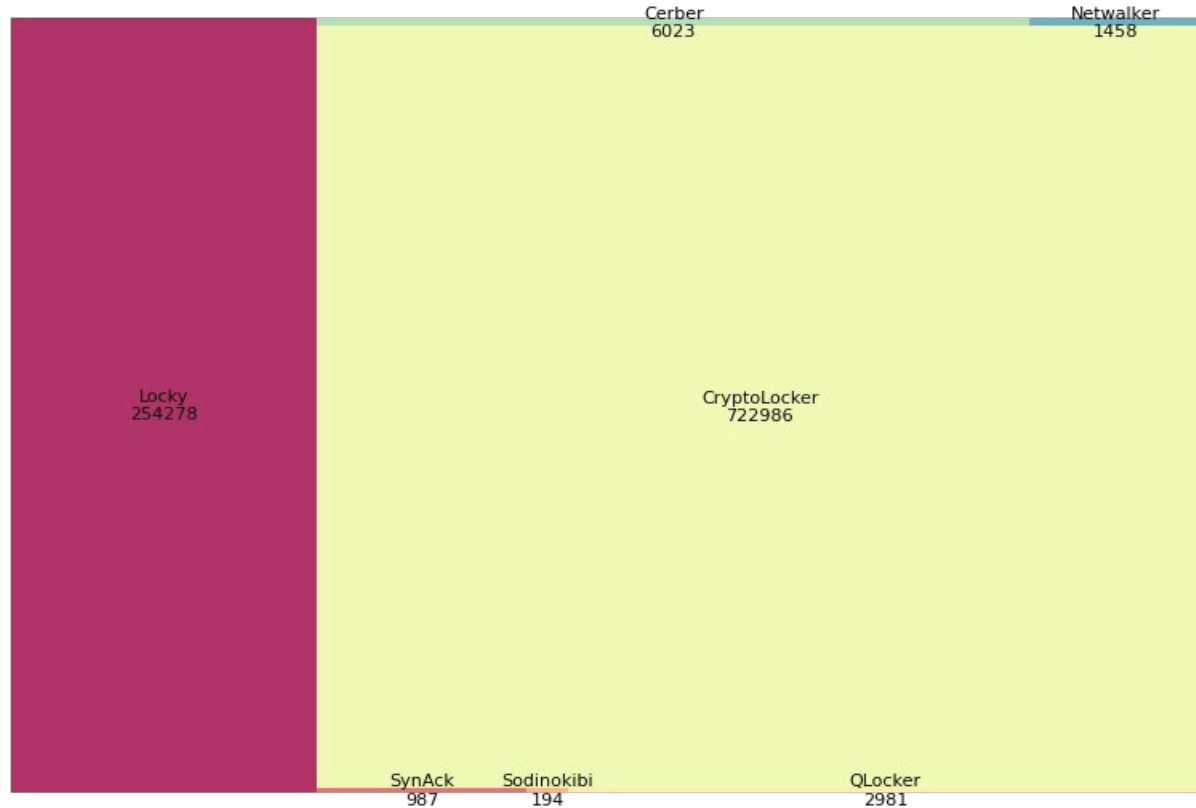
Q: How frequently are we hit?



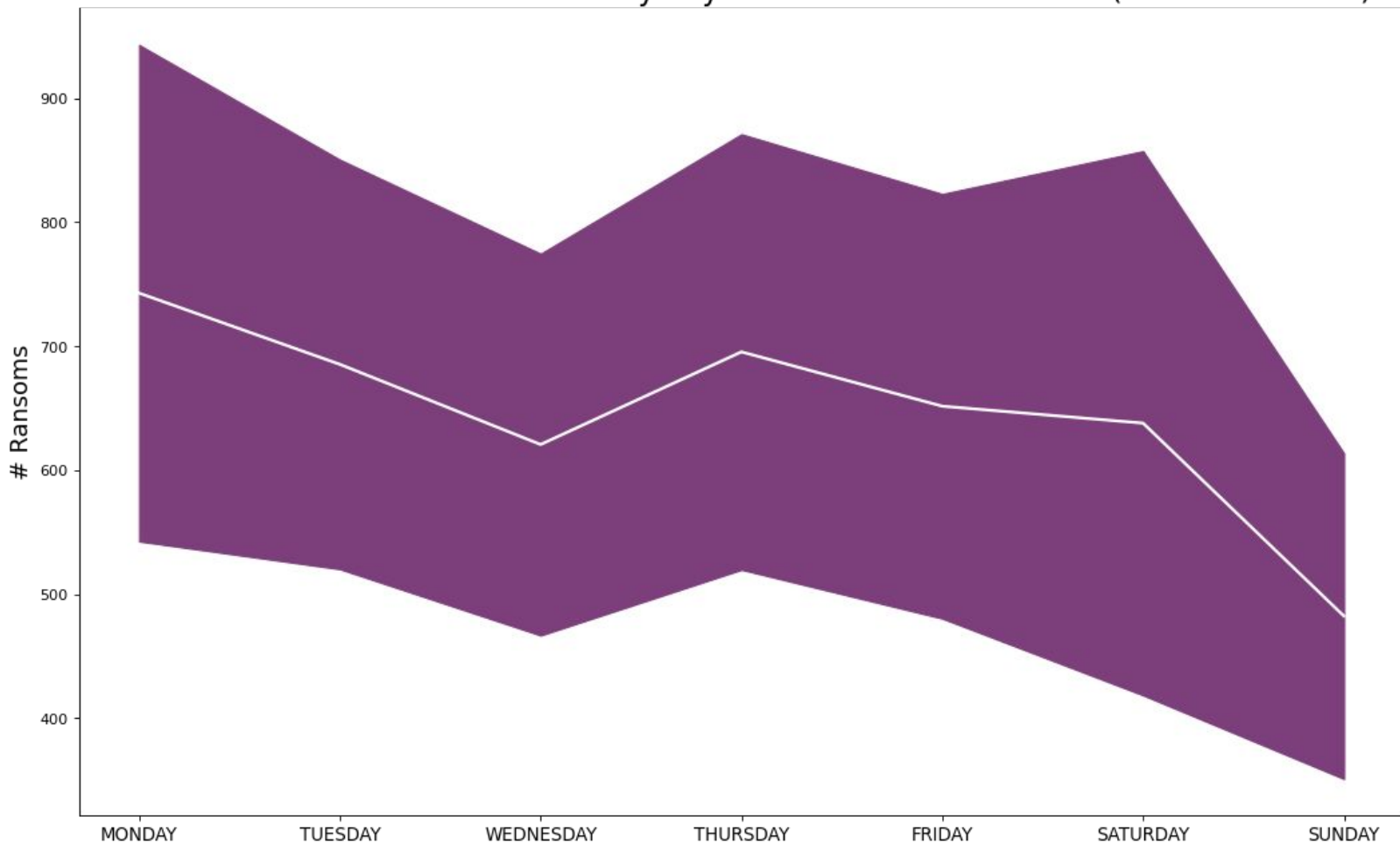
Perhaps you don't want to talk about old malware, because it doesn't help you sell new products.

However, I do...because it helps me estimate if we're getting better or worse.

Ransom Occurrences by Family



Ransom occurrences from all BTC by day of week with Error Bands (95% confidence)



2-3%

Of companies are hit annually[4]

1.5% of ARR

Is a good budget for ransomware prevention!

Q: How do we know if we are doing the right things?



Are you patching the right vulnerabilities?

**Only 4% of
vulnerabilities have
public exploits**

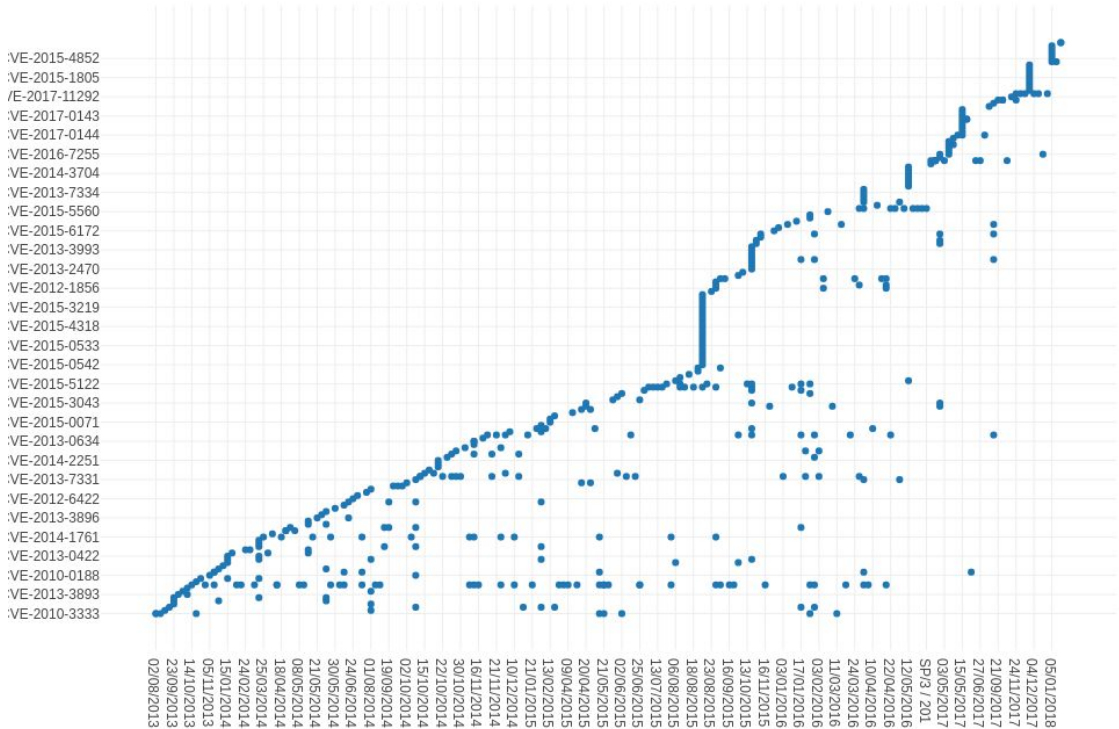
Householder, A.D., Chrabaszcz, J., Novelly, T., Warren, D. and Spring, J.M., 2020. Historical analysis of exploit availability timelines. In 13th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 20).

**Of those with public
exploits, 80% have
the exploit published
(23 days) before the
CVE**

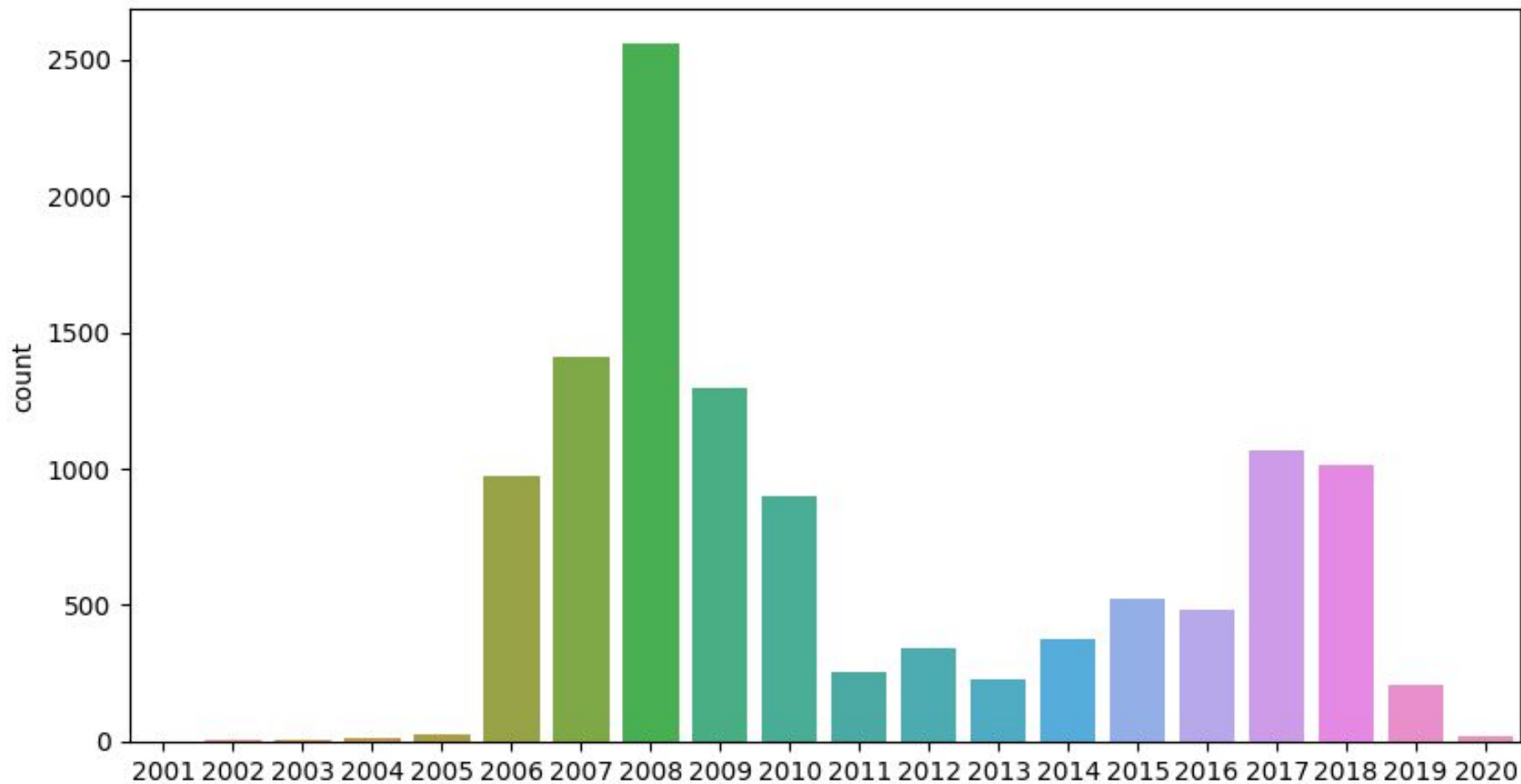
Chen 2020,
<https://unit42.paloaltonetworks.com/state-of-exploit-development/>

This graph is essentially what I learned as a penetration tester of industrial systems and critical infrastructure over the 4 years of my youth.

CVE Seen in Malicious Use Over Time



CVEs with exploits in ExploitDB according to MITRE
11696 total



Exploit Prediction Scoring System @ FIRST.org

Top rated CVEs from the last ninety days

We selected the 48 highest rated CVEs published in the last 90 days. They are shown here with the CVE and EPSS score.

CVE-2021-34473 87.6%	CVE-2021-29728 79.3%	CVE-2021-29702 48.6%	CVE-2021-21098 41.8%	CVE-2020-4935 37.6%	CVE-2021-28596 36.3%
CVE-2021-29703 82.7%	CVE-2021-29777 79.3%	CVE-2021-35464 43.6%	CVE-2021-20483 41.7%	CVE-2021-21101 36.3%	CVE-2021-28603 36.3%
CVE-2021-1675 79.9%	CVE-2021-34527 77.8%	CVE-2021-20430 43.2%	CVE-2021-20572 41.7%	CVE-2021-21102 36.3%	CVE-2021-28604 36.3%
CVE-2021-20560 79.3%	CVE-2021-36004 76.3%	CVE-2021-29766 43.2%	CVE-2021-20573 41.7%	CVE-2021-28586 36.3%	CVE-2021-28606 36.3%
CVE-2021-29736 79.3%	CVE-2021-20562 75.3%	CVE-2021-29767 43.2%	CVE-2020-4902 41.7%	CVE-2021-28589 36.3%	CVE-2021-28607 36.3%
CVE-2021-20579 79.3%	CVE-2021-29754 75.3%	CVE-2021-29784 43.2%	CVE-2021-34523 41.5%	CVE-2021-28590 36.3%	CVE-2021-28608 36.3%
CVE-2021-29722 79.3%	CVE-2021-36934 70.4%	CVE-2021-29951 41.9%	CVE-2021-29712 37.6%	CVE-2021-28591 36.3%	CVE-2021-28610 36.3%
CVE-2021-29723 79.3%	CVE-2021-29725 54.3%	CVE-2021-21090 41.8%	CVE-2020-4675 37.6%	CVE-2021-28592 36.3%	CVE-2021-28620 36.3%

Source: https://first.org/epss/data_stats, 2021-09-06

Q: How do we know how effective those treatments are?



Using counter factualls to understand impact

Wiley Online Library

Search



Login / Register

Risk Analysis
AN INTERNATIONAL JOURNAL
An Official Publication of the Society for Risk Analysis

Original Research Article | Open Access |

Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks

Edward J. Oughton , Daniel Ralph, Raghav Pant, Eireann Leverett, Jennifer Copic, Scott Thacker, Rabia Dada, Simon Ruffle, Michelle Tuveson, Jim W Hall,

First published: 27 February 2019 | <https://doi.org/10.1111/risa.13291> | Citations: 11



[Volume 39, Issue 9](#)
[Special Issue: Resilient Cyber-Physical-Social Systems](#)

September 2019
Pages 2012-2031



Figures



References



Related



Information

Recommended

Sometimes you have to invent the scale of the harm first.



Journal of Cyber Policy >

Volume 2, 2017 - Issue 2: The Internet of Things

Enter keywords, authors, DOI, ORCID e

Submit an article

Journal homepage

233

Views

4

CrossRef citations
to date

18

Altmetric

Original Articles


Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate

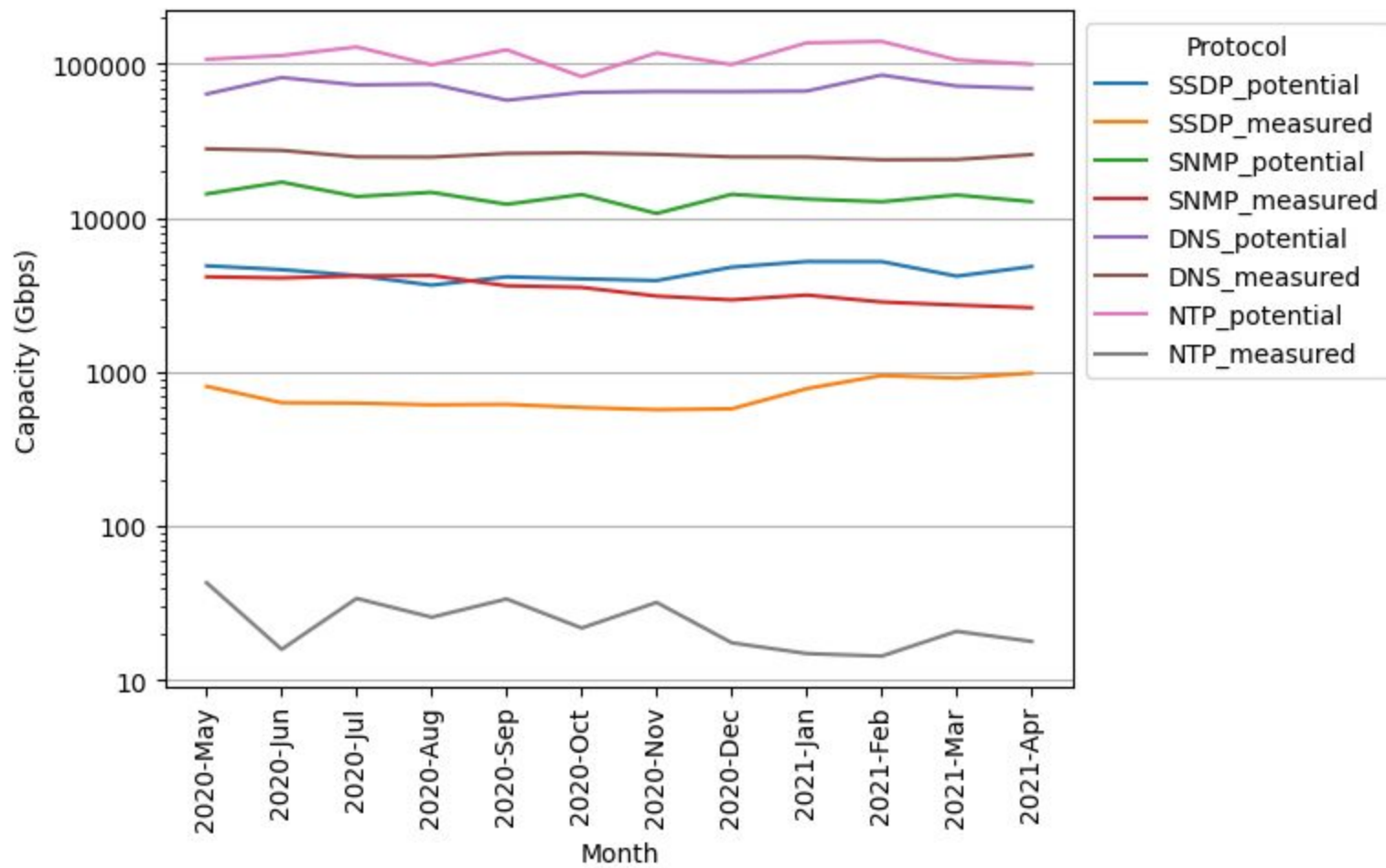
Eireann Leverett   & Aaron Kaplan

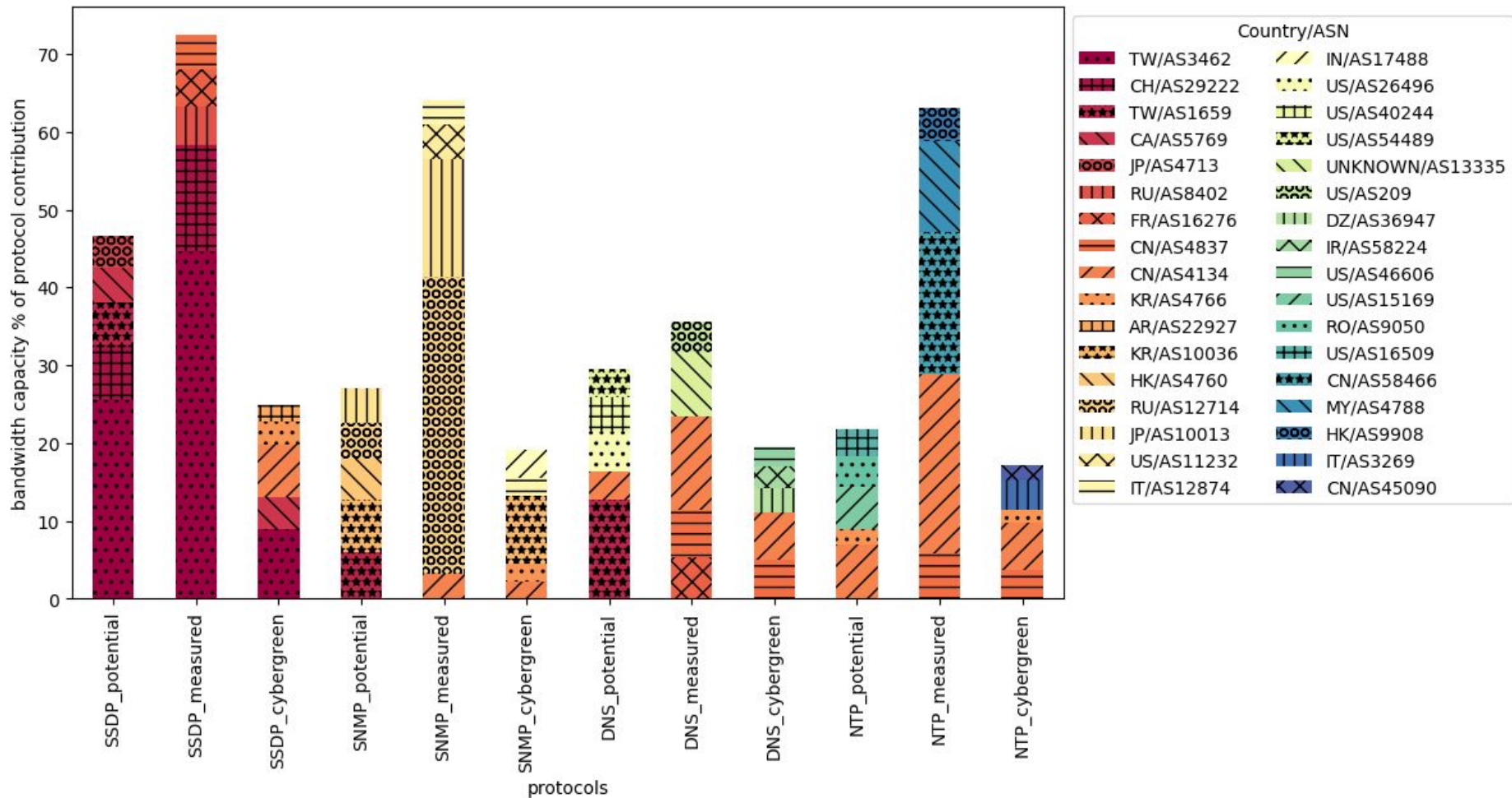
Pages 195-208 | Received 18 Apr 2017, Accepted 27 Jul 2017, Published online: 21 Aug 2017

Download citation

 <https://doi.org/10.1080/23738871.2017.1362020>

 Check for updates

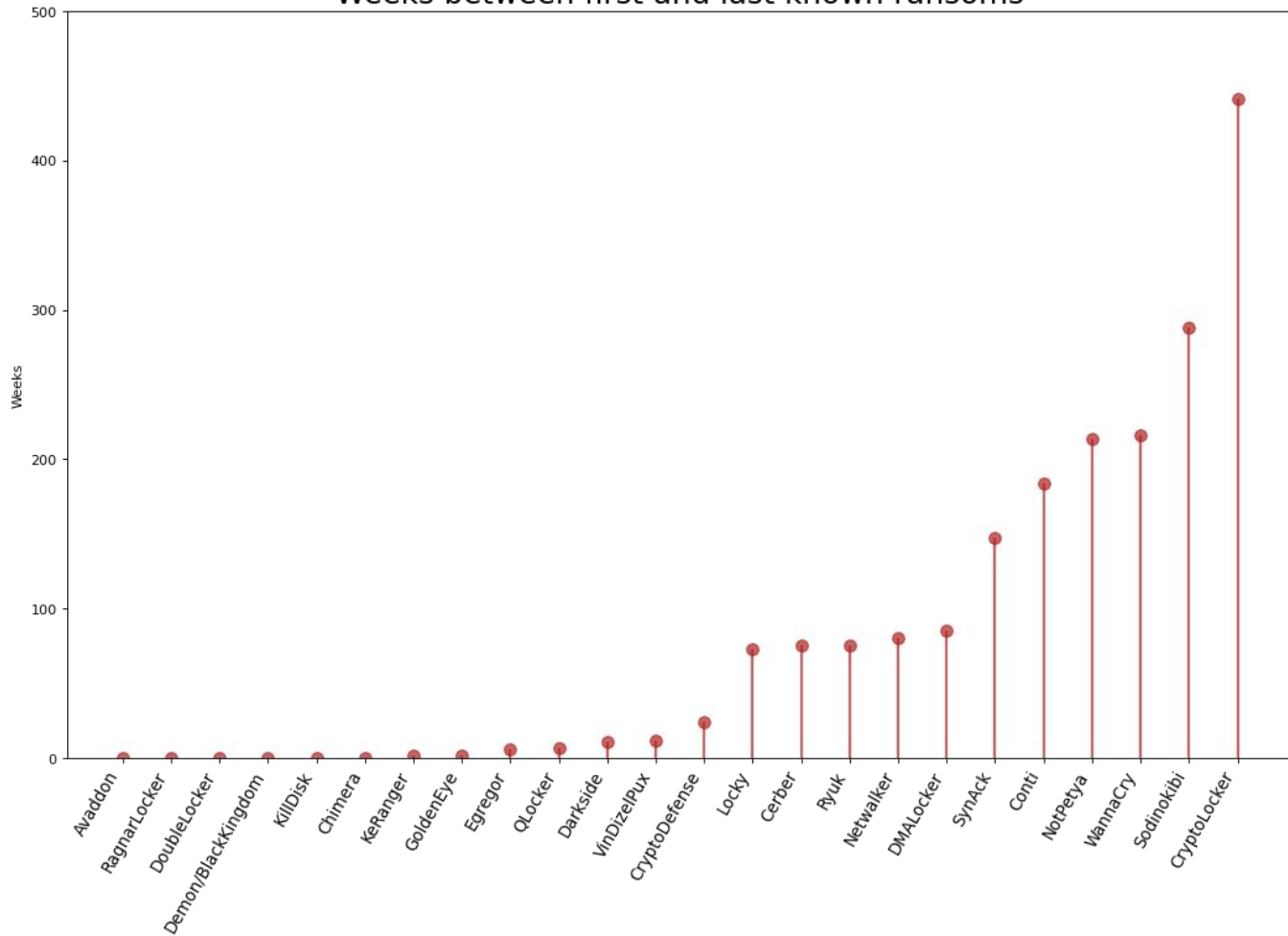




Q: A short crisis for you, business as usual for criminals?



Weeks between first and last known ransoms



Q: What if we could get ahead of the problems?



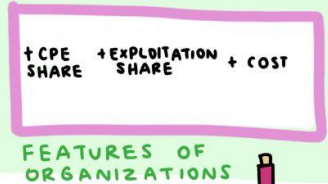
VULNCAST: WHY WAIT FOR ZERO DAYS?

MATILDA RHODE
EIREANN LEVERETT

4% OF VULNERABILITIES HAVE PUBLIC EXPLOITS
80% HAVE EXPLOITS PUBLISHED 23 DAYS BEFORE THE CVE

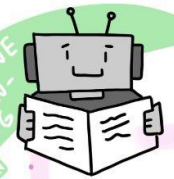


HARDER THE MORE SPECIFIC YOU GET...



UNDERSTAND THE RATE OF REPORTING

SEASONALITY? DE TREND? PLOT NOT RELEVANT
AUGMENTED DICKEY FULLER
CHECK AUTO CORRELATION ANALYSIS
FIND LIMITS
LOOK BACK
LOOK AHEAD



LITTLE'S LAW
 $QUEUE_SIZE = ARRIVAL_RATE * MEAN_SERVICE_TIME$

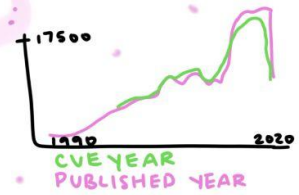
VILLAGE LOTTERY
 $YEARFRACTION * P * (MAXID + \frac{MAXID}{NUMOBS} - 1)$

SERIAL NUMBER PREDICTION



+ @NVD
+ @MITRE
+ PUBLICLY AVAILABLE DATA

QUEUE THEORY



SERIAL PREDICTION
EASIER TO PREDICT A YEAR IN ADVANCE

12 MONTHS
MEDIAN ERROR 5%
LOWER VARIANCE

PREDICTION FRAMEWORK
95% PREDICTION INTERVAL AS DISCRIMINATOR

CVSS OR VULNERABILITY TYPE

DEPEND ON PRODUCT & TYPE
SOME DO BETTER WIT JIT METHODS

SOME VULN TYPES
DATA IS DIRTY

VULNERABILITIES ARE FORESEEABLE
IMPROVE LOOKAHEAD?
WHAT ARE IMPLICATIONS?

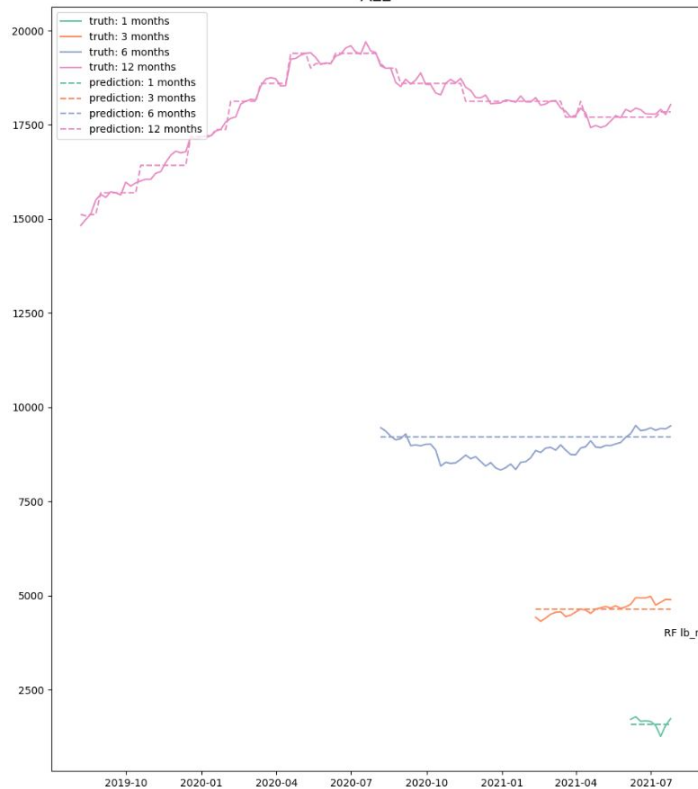
SHOULD VENDORS OR NVD PUBLISH THEIR OWN FORECASTS?



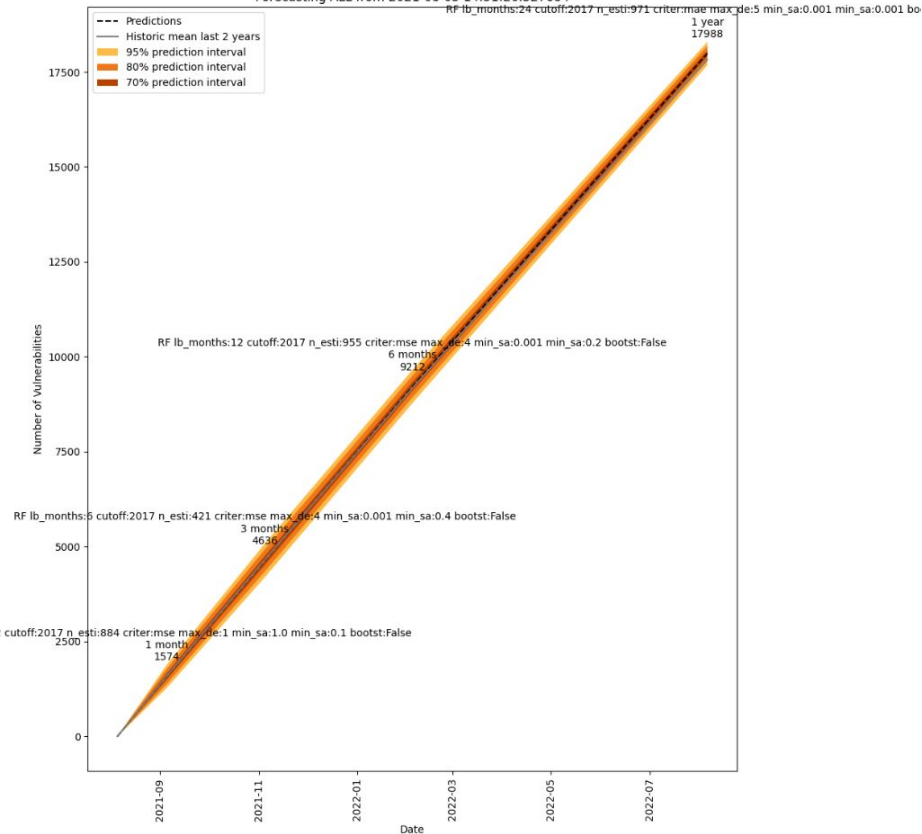
YOU CAN'T FORECAST EVERY PRODUCT

SPECIFIC PRODUCTS NOT AS PREDICTABLE

Historic predictions and future predictions
ALL



Forecasting ALL from 2021-08-05 14:51:26.327684



Q: If we did all that and there's residual risk, is this actually a public health problem?

Averages don't characterise the heavy tails of ransoms

1st Éireann Leverett

Founder of

Concinnity Risks

Cambridge, United Kingdom

eleverett[AT]concinnity-risks.com

2nd Eric Jardine

Assistant Professor

Department of Political Science, Virginia Tech

Blacksburg, United States

ejardine[AT]vt[DOT]edu

3rd Erin Burns

Founder of

Concinnity Risks

Cambridge, United Kingdom

eburns[AT]concinnity-risks.com

4th Ankit Gangwal

University of Padua, Italy

ankit.gangwal[AT]phd.unipd.it

5th Dan Geer

Senior Fellow In-Q-Tel

dan[AT]geer[DOT]org

So how big is the ransomware industry?



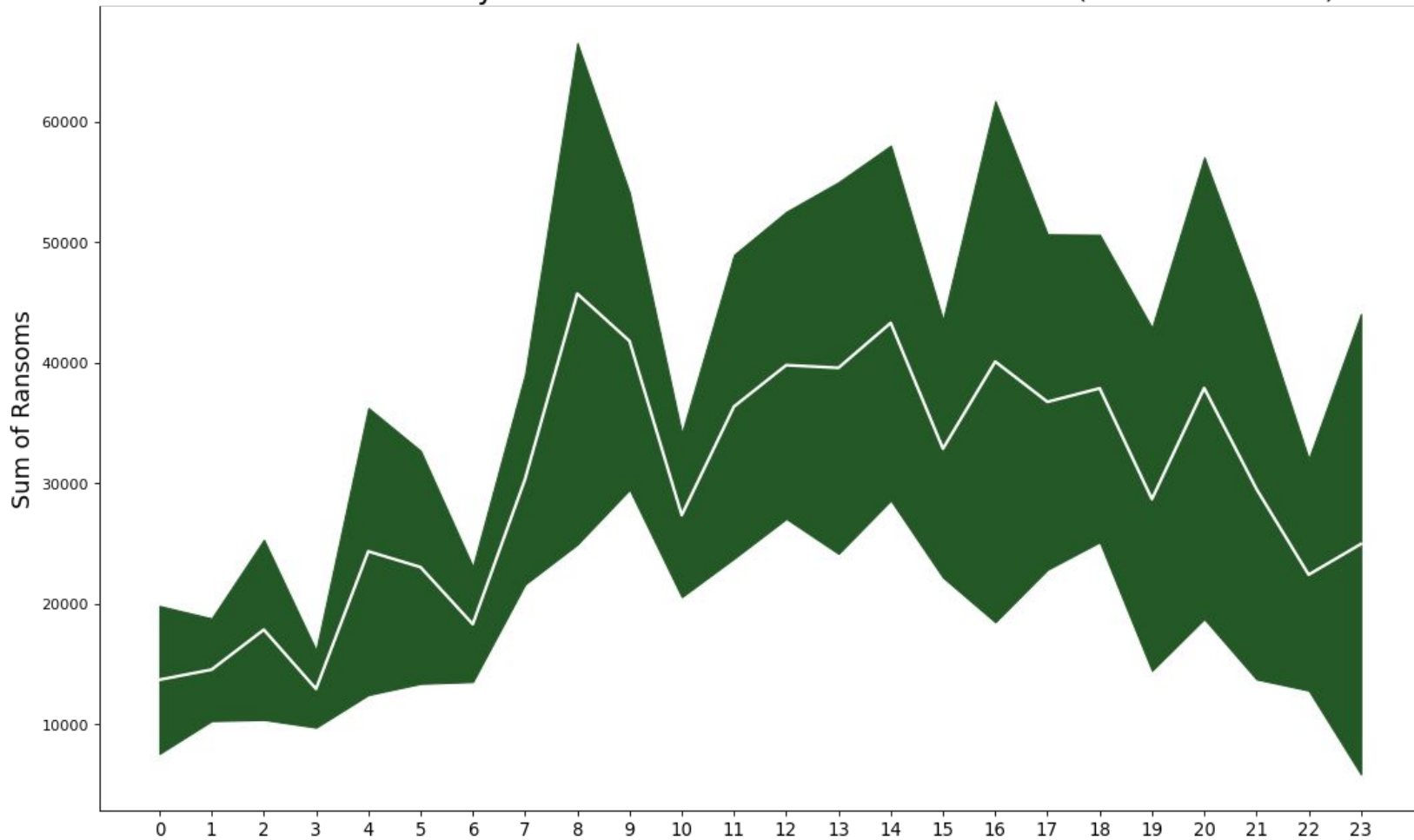
\$10,909,589,702

(if they cashed out daily at AVG price)

\$492,967,698,285

(if they cashed out daily at BTC ATH)

Ransom sums hourly from named families with Error Bands (95% confidence)



Thank you!

@blackswanburst



References and Footnotes

- [1] <https://mobile.twitter.com/uuallan/status/1400597409701548033>
- [2] <https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for>
- [3] <https://www.advintel.io/post/the-rise-demise-of-multi-million-ransomware-business-empire/>
- [4] <https://www.usenix.org/conference/soups2019/presentation/simoiu>