Ransomware Zugzwang

June 9, 2023

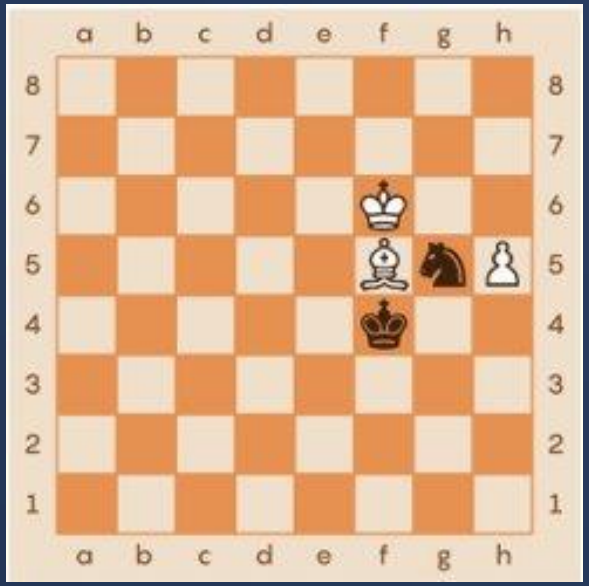
Scott Small
Director of Threat Intelligence
Tidal Cyber

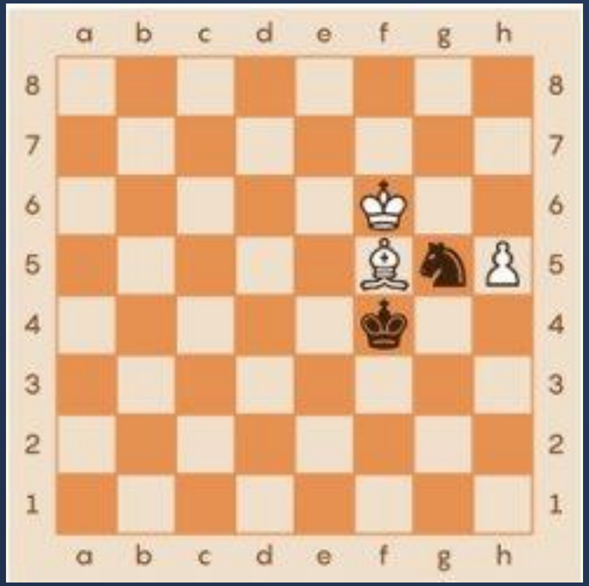
Éireann Leverett
Principal Risk Scientist
Tidal Cyber

TIDAL
THREAT-INFORMED DEFENSE

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

TIDAL

THREAT-INFORMED DEFENSE

2023 Ransomware Landscape

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%)

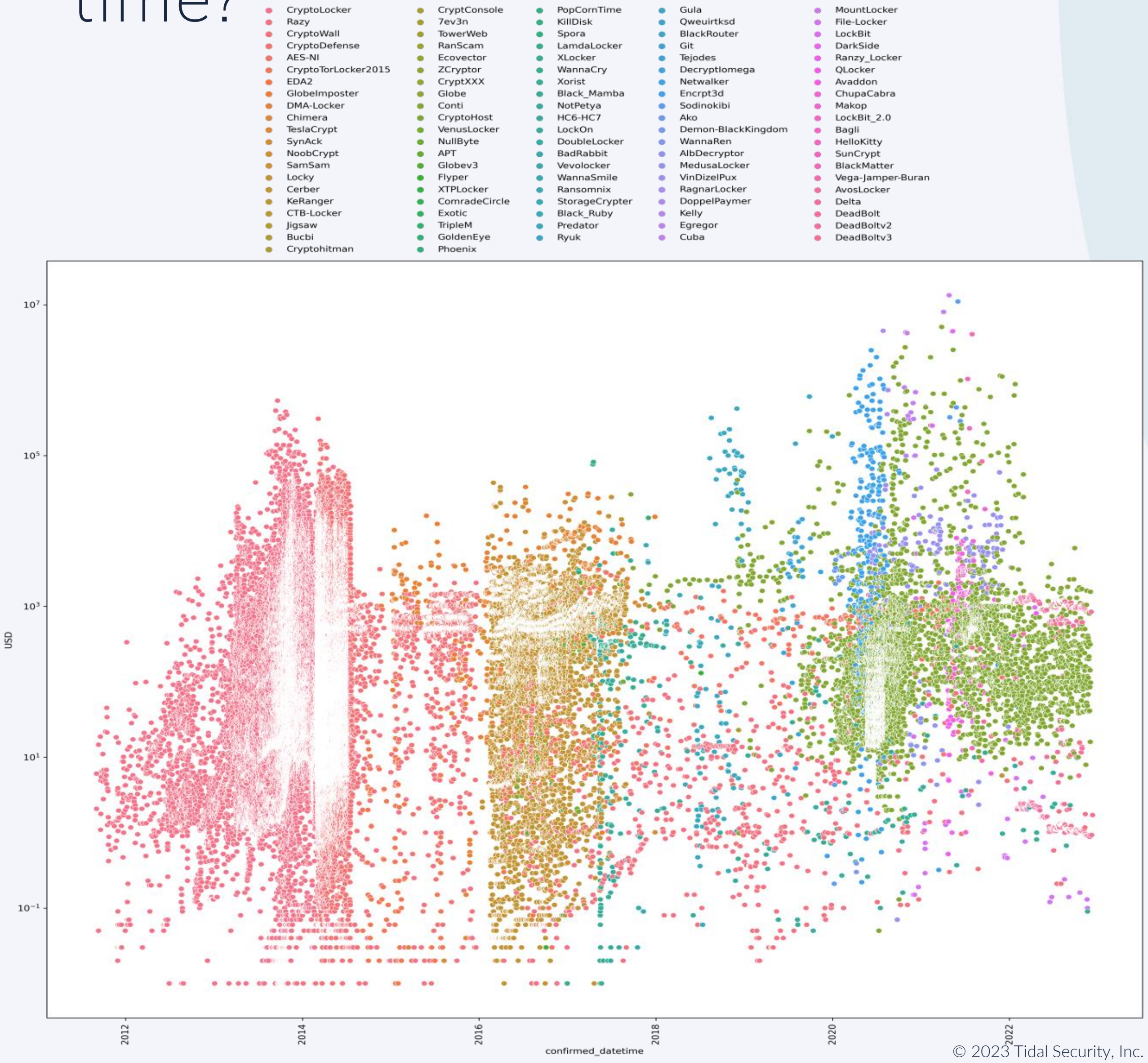
↓ Total ransom payments (40.3%)

↓ 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?



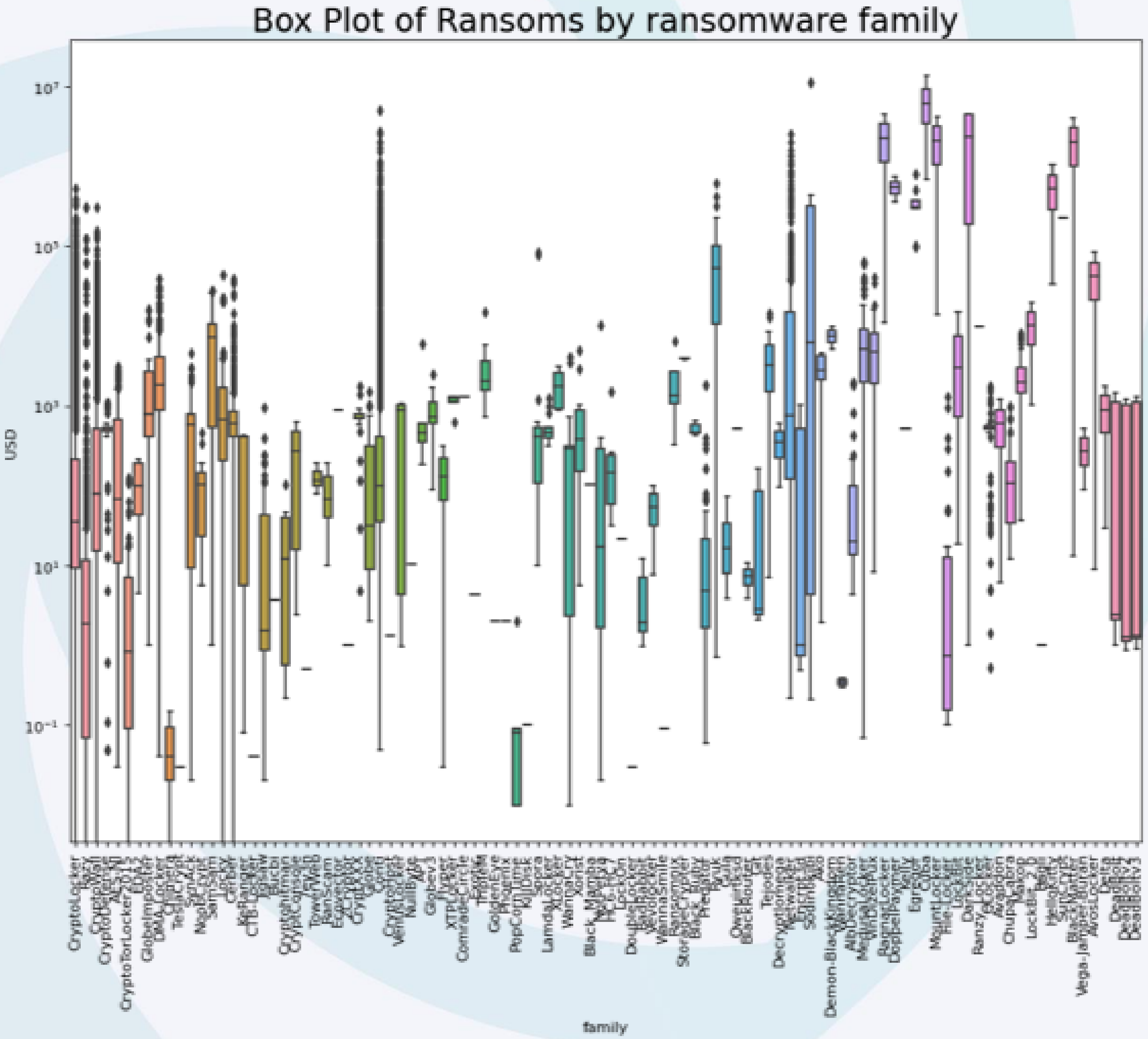
Spearmans Correlation Coefficient	1.00
P-Value	0.000

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!



Spearmans Correlation Coefficient	0.952
P-Value	0.000

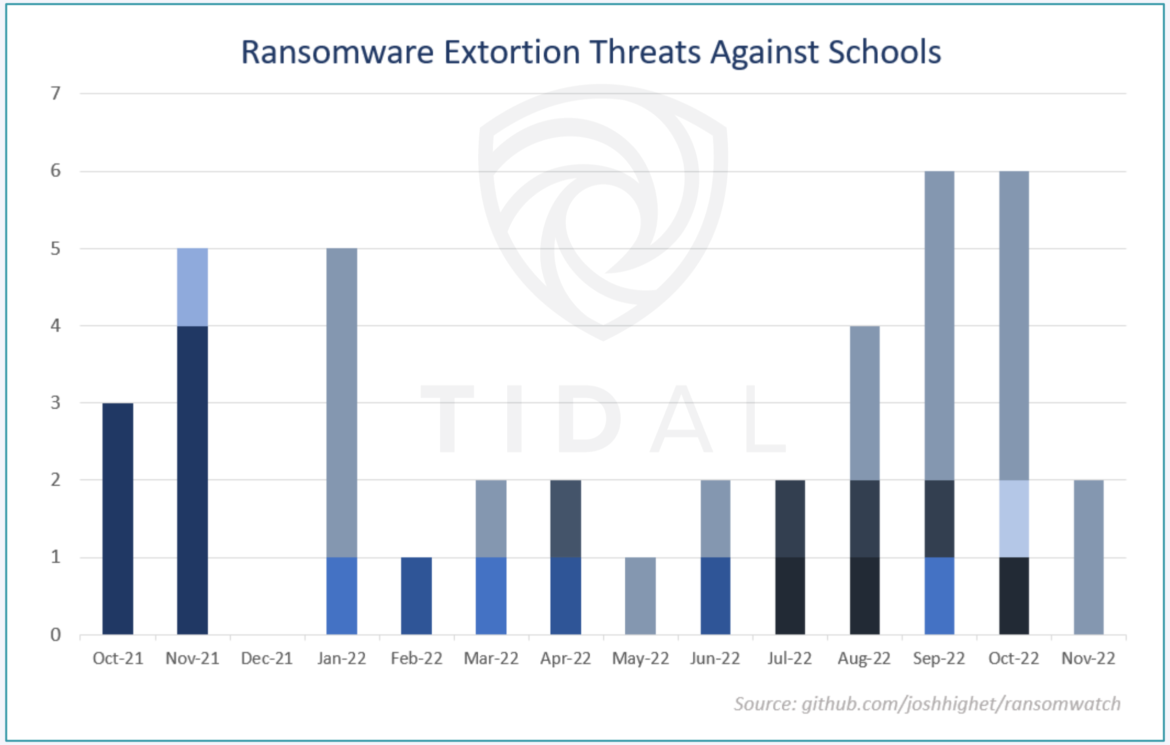
Sector Analysis

Threats to Public Services

Ransomware trends against vulnerable sectors:

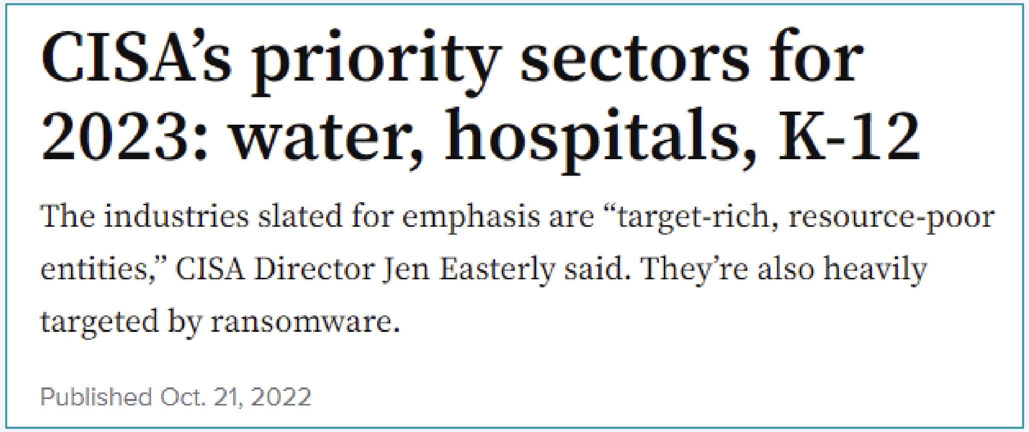
- Utilities
- Education
- Healthcare

“Critical infrastructure” covers a lot these days



Ransomware Extortion Threats Against Schools

Source: github.com/joshhighet/ransomwatch



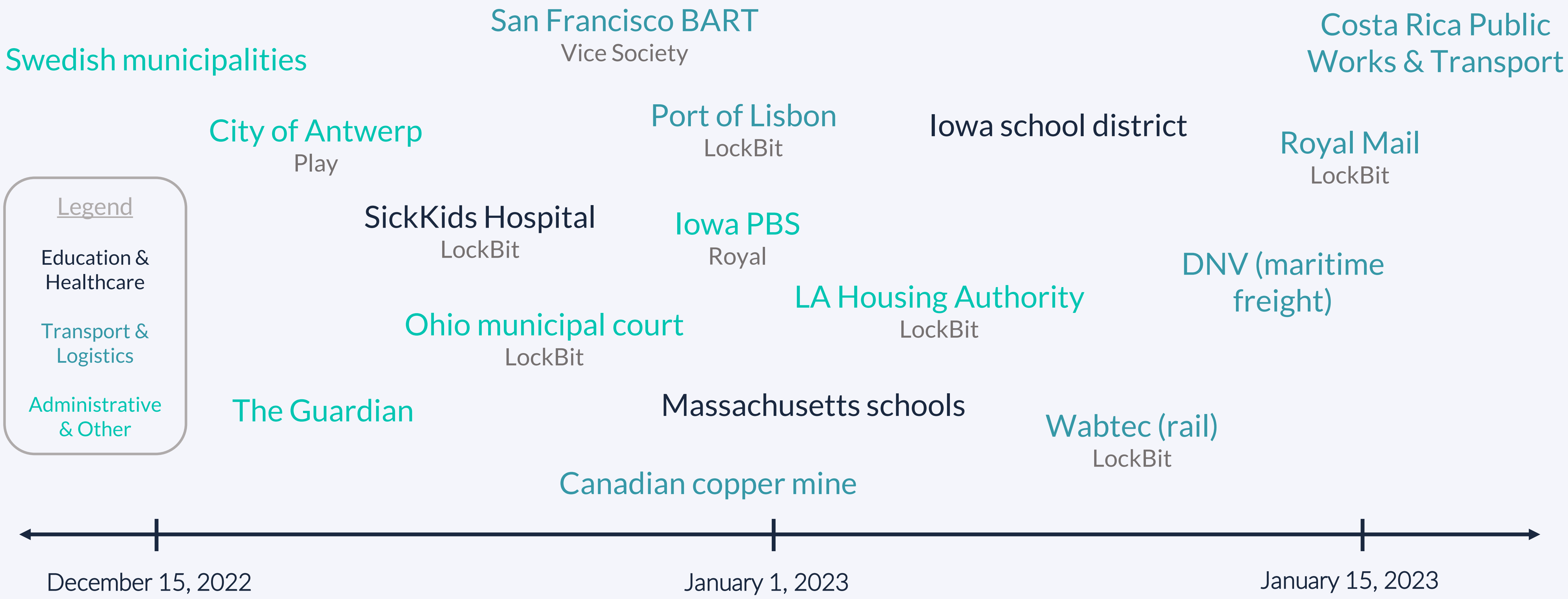
CISA’s priority sectors for 2023: water, hospitals, K-12

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



Legend

Education & Healthcare

Transport & Logistics

Administrative & Other

Swedish municipalities

City of Antwerp
Play

The Guardian

SickKids Hospital
LockBit

San Francisco BART
Vice Society

Ohio municipal court
LockBit

Canadian copper mine

Port of Lisbon
LockBit

Iowa PBS
Royal

Massachusetts schools

LA Housing Authority
LockBit

Iowa school district

Wabtec (rail)
LockBit

DNV (maritime freight)

Royal Mail
LockBit

Costa Rica Public Works & Transport

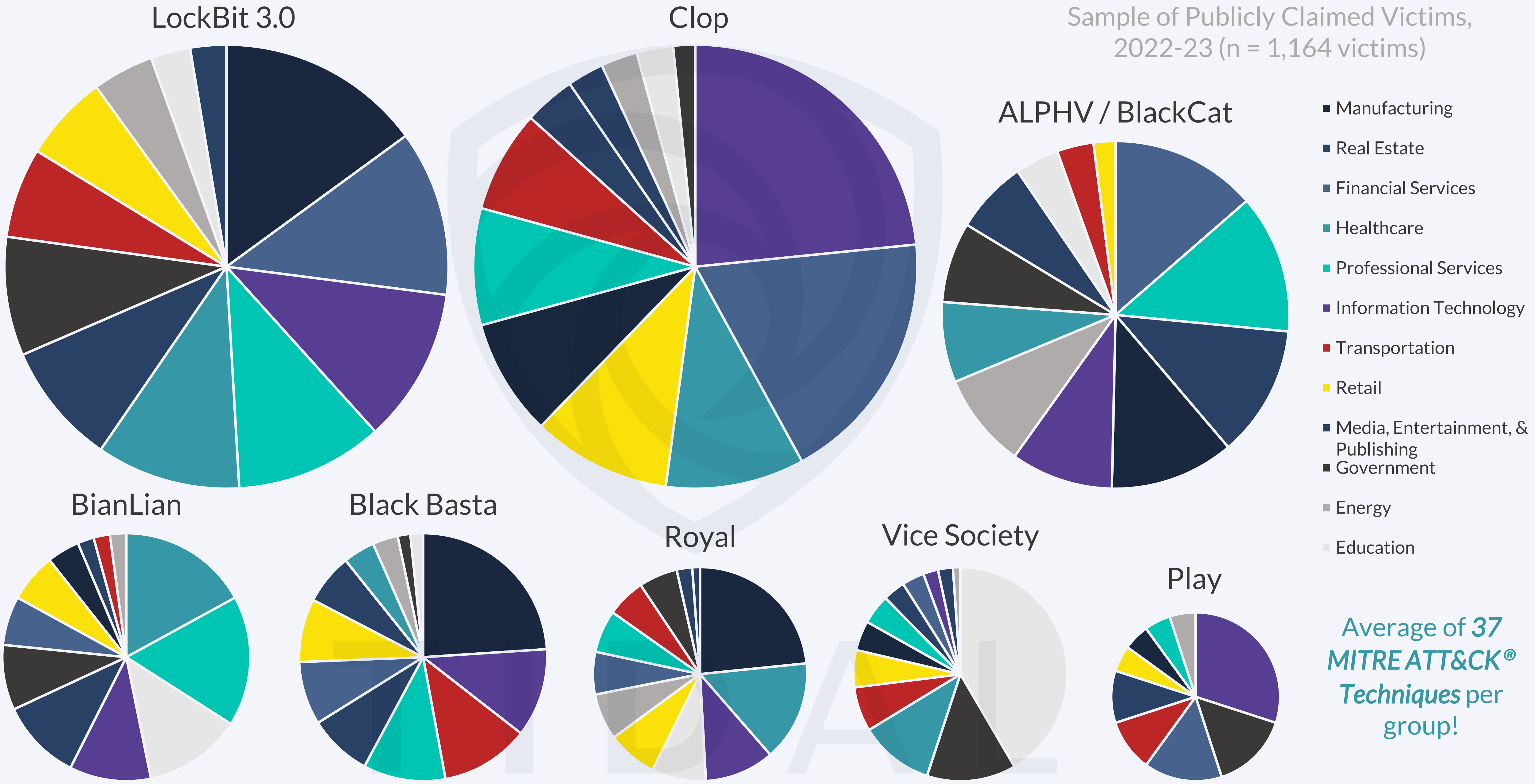
December 15, 2022

January 1, 2023

January 15, 2023

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)

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

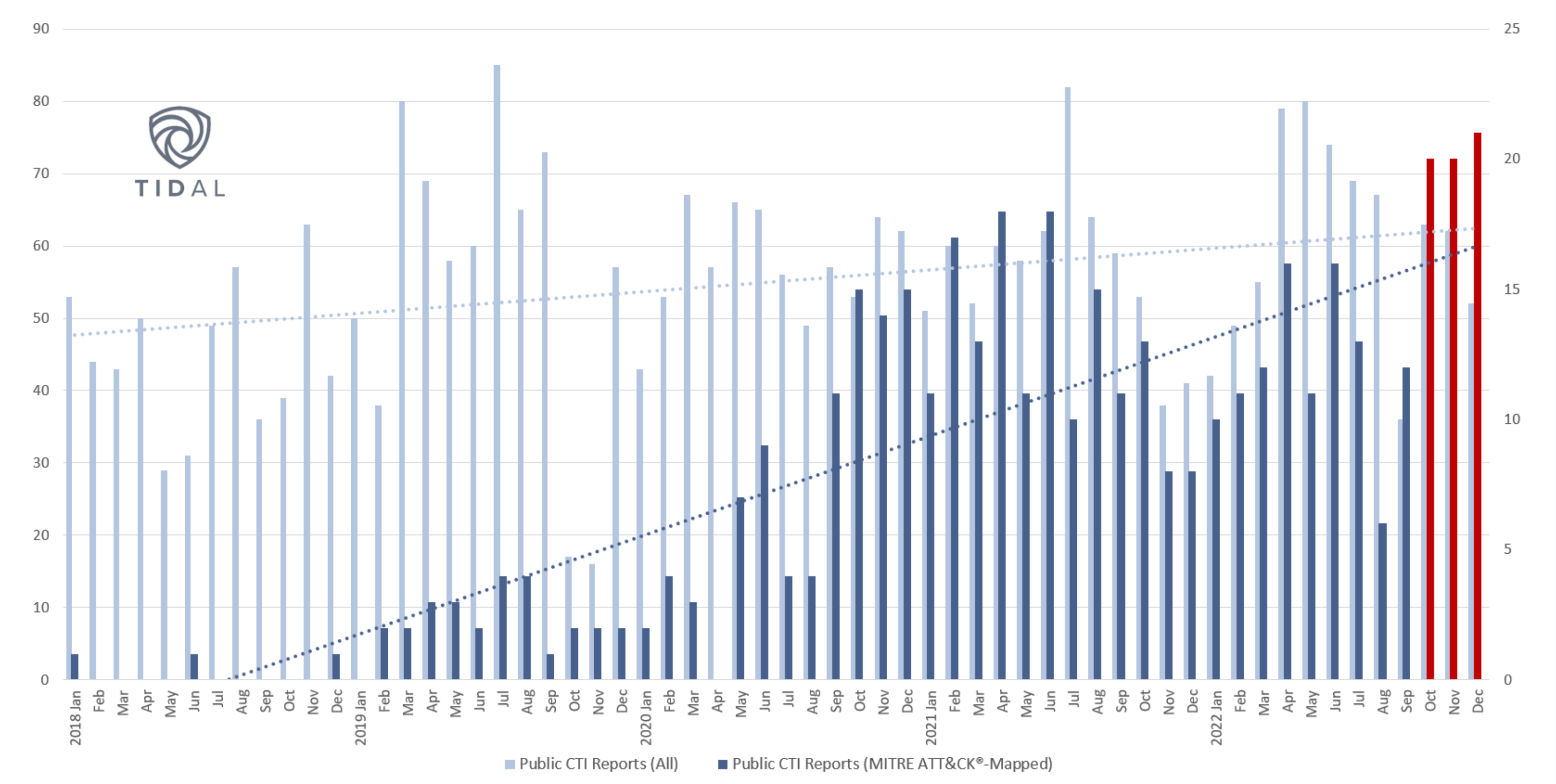
Ransomware TTPs

Optimizing Defensive ROI

TIDAL

THREAT-INFORMED DEFENSE

Setting the Stage: TTP Intelligence Trends

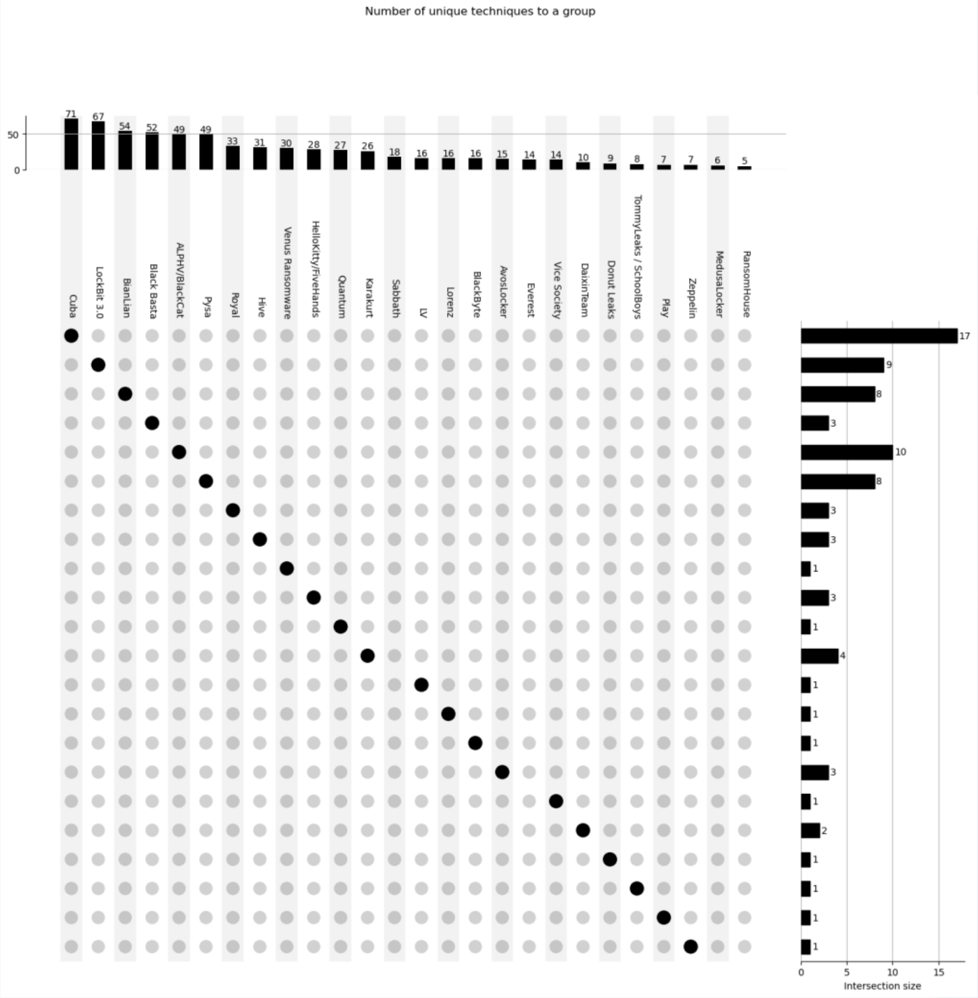


Increased awareness & adoption of a **threat-informed** mindset → growing public, ATT&CK mapped CTI reporting

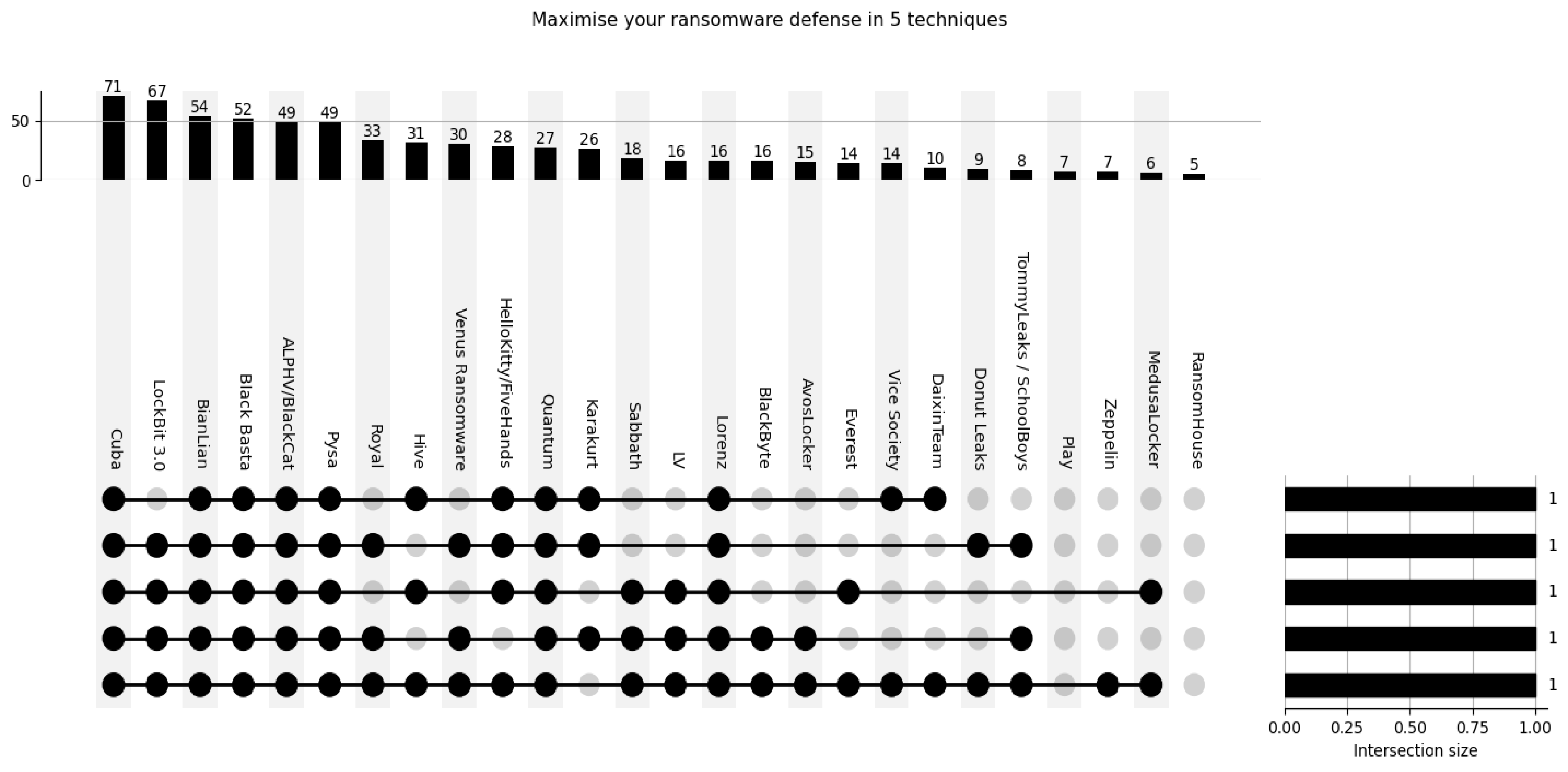
Faster pivoting & translation into defensive capabilities

TTP Evolution

Some techniques are only used by one group.

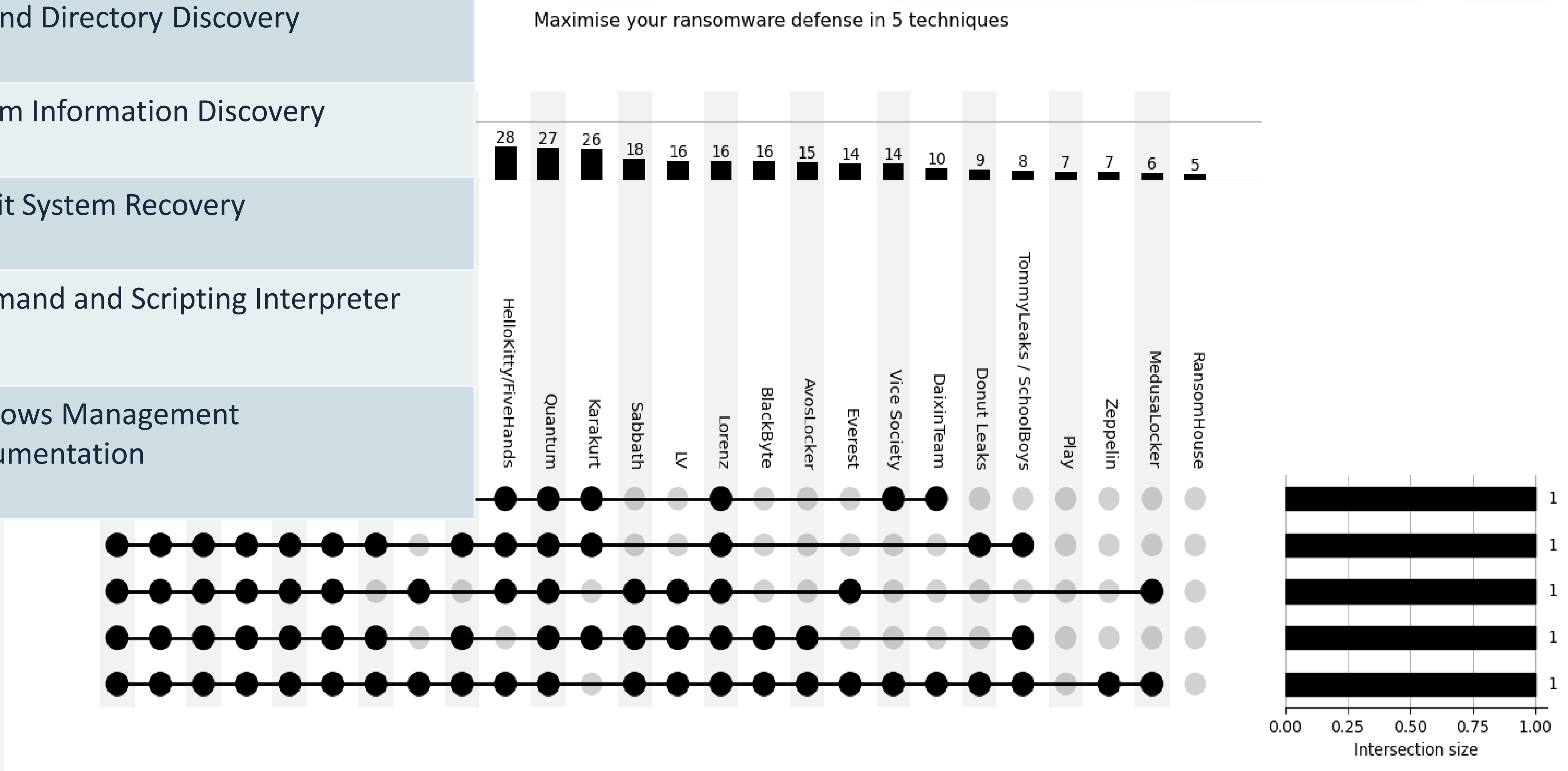


Maximise your defensive advantage


Maximise your ransomware defense in 5 techniques

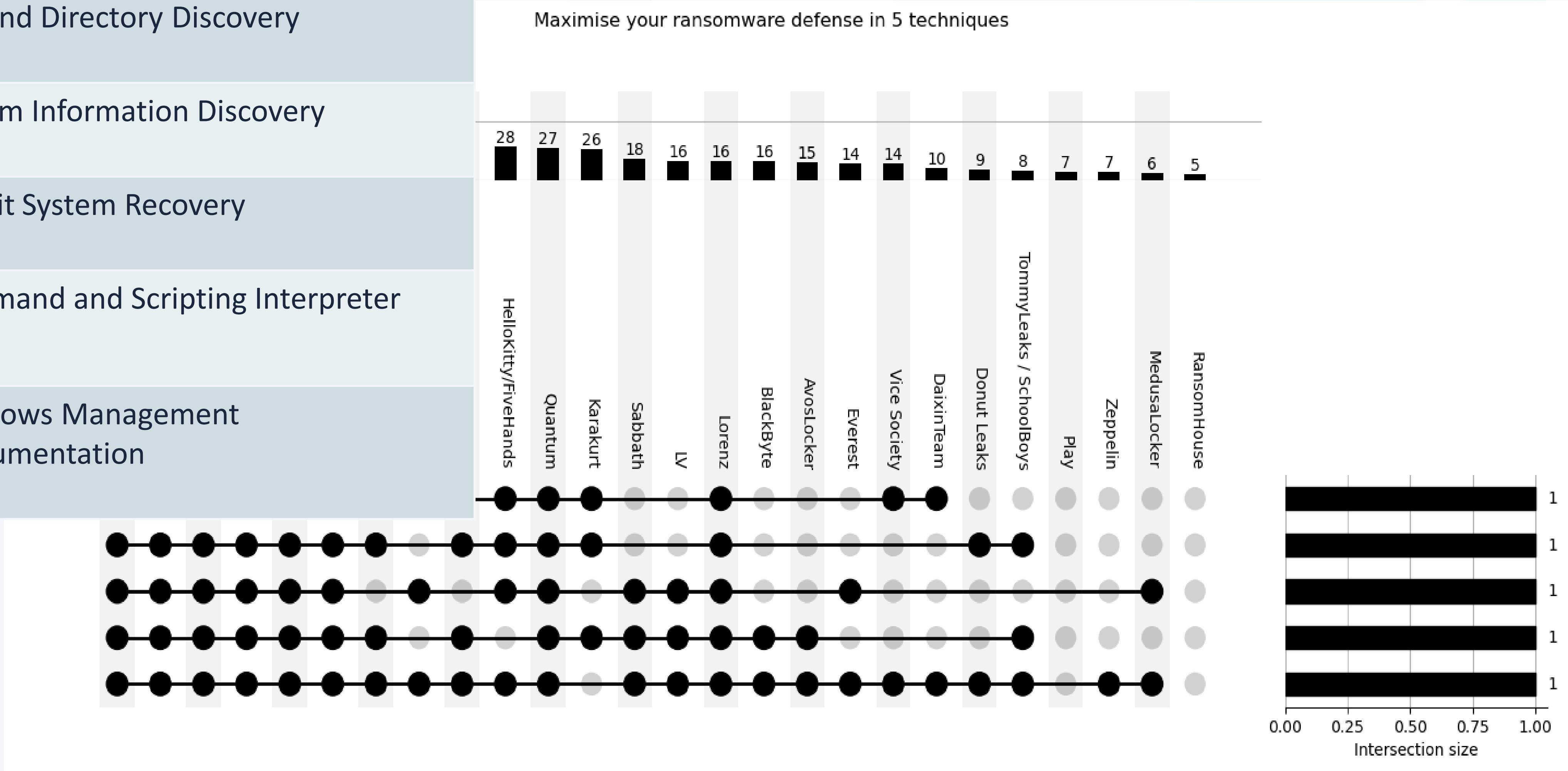
Maximise your defensive advantage

T1486	Data Encrypted for Impact
T1083	File and Directory Discovery
T1082	System Information Discovery
T1490	Inhibit System Recovery
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation



Maximise your defensive advantage

~~T1486~~	~~Data Encrypted for Impact~~
T1083	File and Directory Discovery
T1082	System Information Discovery
T1490	Inhibit System Recovery
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation



Top Observed Ransomware Techniques

Tidal Study of Public CTI Reporting on Most-Active 2022-23 Extortion Groups

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1486	**Data Encrypted for Impact**	Impact	50	6	10	5
T1082	**System Information Discovery**	Discovery	30	4	14	24
T1083	**File and Directory Discovery**	Discovery	29	3	17	6
T1490	**Inhibit System Recovery**	Impact	23	5	18	9
T1059.001	**PowerShell**	Execution	20	5	183	22
T1047	**Windows Management Instrumentation**	Execution	19	3	40	10
T1489	**Service Stop**	Impact	17	7	9	3
T1112	**Modify Registry**	Defense Evasion	16	6	65	44
T1562.001	**Disable or Modify Tools**	Defense Evasion	16	6	77	38
T1059.003	**Windows Command Shell**	Execution	14	2	21	5
T1190	**Exploit Public-Facing Application**	Initial Access	14	2	80	0
T1133	**External Remote Services**	Persistence, Initial Access	13	3	7	1
T1021.001	**Remote Desktop Protocol**	Lateral Movement	13	4	14	3
T1018	**Remote System Discovery**	Discovery	13	4	15	20

Defending Against Top Observed Ransomware Techniques

Some Thoughts

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

Top Common TTPs

Ransomware & Data Extortion Landscape

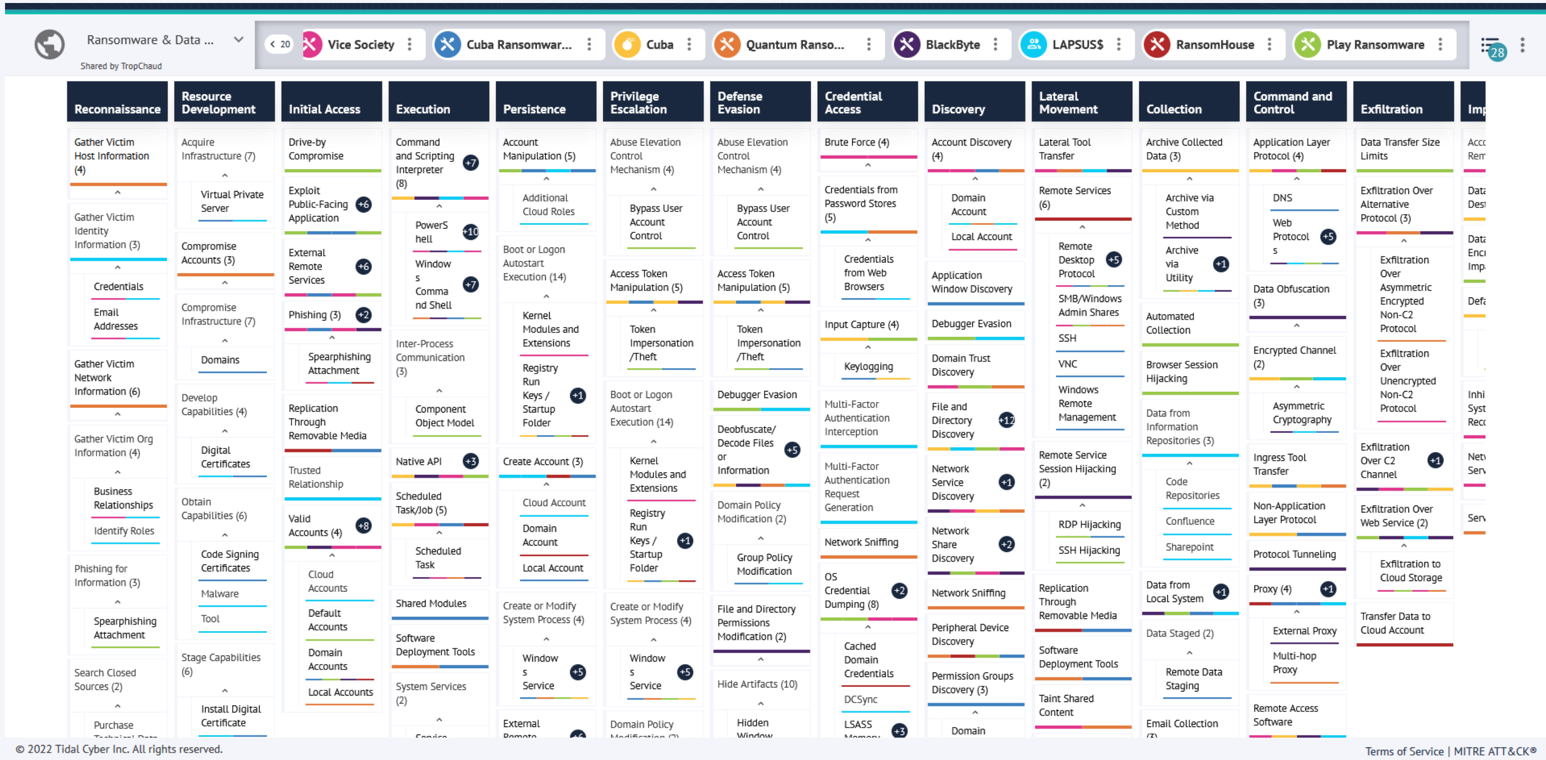
29 groups & families (& counting)

- 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?



Ransomware & Data ...

Shared by TropChaud

< 20 · Vice Society · Cuba Ransomwar... · Cuba · Quantum Ranso... · BlackByte · LAPSUS$ · RansomHouse · Play Ransomware · 28

Reconnaissance
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
  - Credentials
  - Email Addresses
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
  - Business Relationships
  - Identify Roles
- Phishing for Information (3)
  - Spearphishing Attachment
- Search Closed Sources (2)
  - Purchase Technical Data

Resource Development
- Acquire Infrastructure (7)
  - Virtual Private Server
- Compromise Accounts (3)
- Compromise Infrastructure (7)
  - Domains
- Develop Capabilities (4)
  - Digital Certificates
- Obtain Capabilities (6)
  - Code Signing Certificates
  - Malware
  - Tool
- Stage Capabilities (6)
  - Install Digital Certificate

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application +6
- External Remote Services +6
- Phishing (3) +2
  - Spearphishing Attachment
- Replication Through Removable Media
- Trusted Relationship
- Valid Accounts (4) +8
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution
- Command and Scripting Interpreter (8) +7
  - PowerShell +10
  - Windows Command Shell +7
- Inter-Process Communication (3)
  - Component Object Model
- Native API +3
- Scheduled Task/Job (5)
  - Scheduled Task
- Shared Modules
- Software Deployment Tools
- System Services (2)
  - Service

Persistence
- Account Manipulation (5)
  - Additional Cloud Roles
- Boot or Logon Autostart Execution (14)
  - Kernel Modules and Extensions
  - Registry Run Keys / Startup Folder +1
- Create Account (3)
  - Cloud Account
  - Domain Account
  - Local Account
- Create or Modify System Process (4)
  - Windows Service +5
- External Remote +6

Privilege Escalation
- Abuse Elevation Control Mechanism (4)
  - Bypass User Account Control
- Access Token Manipulation (5)
  - Token Impersonation /Theft
- Boot or Logon Autostart Execution (14)
  - Kernel Modules and Extensions
  - Registry Run Keys / Startup Folder +1
- Create or Modify System Process (4)
  - Windows Service +5
- Domain Policy Modification (2)

Defense Evasion
- Abuse Elevation Control Mechanism (4)
  - Bypass User Account Control
- Access Token Manipulation (5)
  - Token Impersonation /Theft
- Debugger Evasion
- Deobfuscate/ Decode Files or Information +5
- Domain Policy Modification (2)
  - Group Policy Modification
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
  - Hidden Window

Credential Access
- Brute Force (4)
- Credentials from Password Stores (5)
  - Credentials from Web Browsers
- Input Capture (4)
  - Keylogging
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8) +2
  - Cached Domain Credentials
  - DCSync
  - LSASS Memory +3

Discovery
- Account Discovery (4)
  - Domain Account
  - Local Account
- Application Window Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery +12
- Network Service Discovery +1
- Network Share Discovery +2
- Network Sniffing
- Peripheral Device Discovery
- Permission Groups Discovery (3)
  - Domain

Lateral Movement
- Lateral Tool Transfer
- Remote Services (6)
  - Remote Desktop Protocol +5
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
- Remote Service Session Hijacking (2)
  - RDP Hijacking
  - SSH Hijacking
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Collection
- Archive Collected Data (3)
  - Archive via Custom Method
  - Archive via Utility +1
- Automated Collection
- Browser Session Hijacking
- Data from Information Repositories (3)
  - Code Repositories
  - Confluence
  - Sharepoint
- Data from Local System +1
- Data Staged (2)
  - Remote Data Staging
- Email Collection (3)

Command and Control
- Application Layer Protocol (4)
  - DNS
  - Web Protocols +5
- Data Obfuscation (3)
- Encrypted Channel (2)
  - Asymmetric Cryptography
- Ingress Tool Transfer
- Non-Application Layer Protocol
- Protocol Tunneling
- Proxy (4) +1
  - External Proxy
  - Multi-hop Proxy
- Remote Access Software

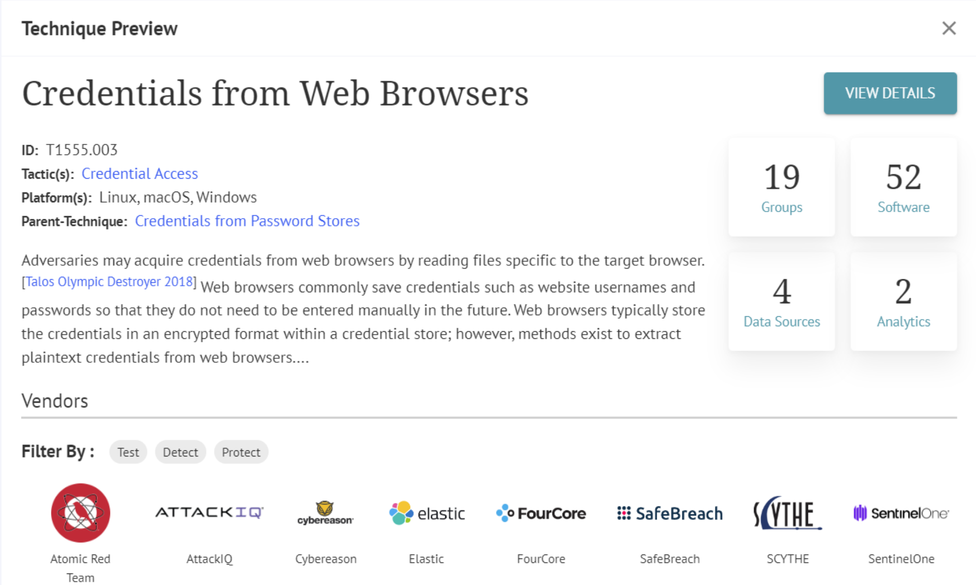
Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- Exfiltration Over C2 Channel +1
- Exfiltration Over Web Service (2)
  - Exfiltration to Cloud Storage
- Transfer Data to Cloud Account

Imp
- Acc Rem
- Data Dest
- Data Encr Imp
- Defa
- Inhi Syst Reco
- Netw Serv
- Serv

Terms of Service | MITRE ATT&CK®

app.tidalcyber.com > Community Spotlight > Ransomware & Data Extortion Landscape Matrix

Intelligence-Informed Detection Engineering



Technique Preview

Credentials from Web Browsers

VIEW DETAILS

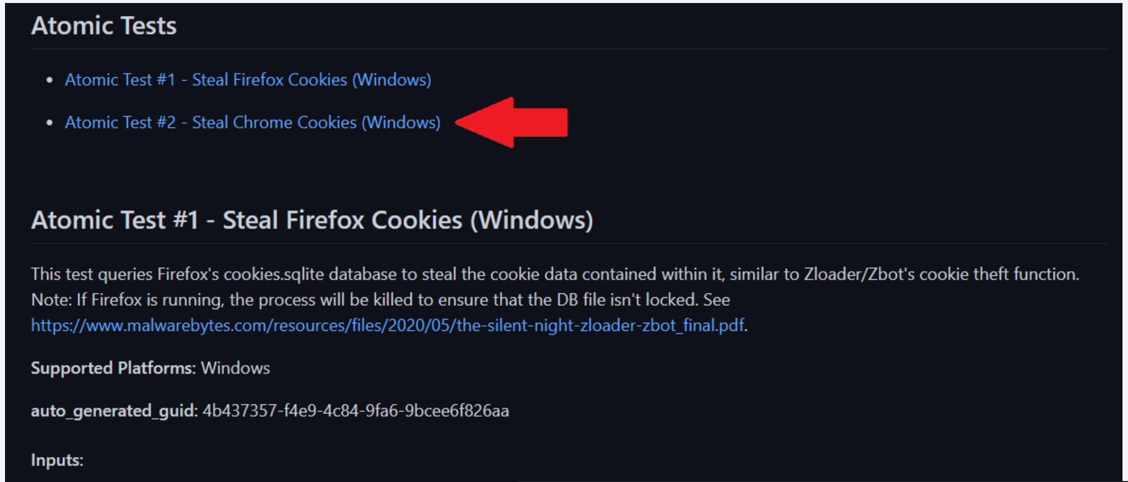
ID: T1555.003
Tactic(s): Credential Access
Platform(s): Linux, macOS, Windows
Parent-Technique: Credentials from Password Stores

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. [Talos Olympic Destroyer 2018] Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers....

19 Groups	52 Software
4 Data Sources	2 Analytics

Vendors

Filter By : Test Detect Protect



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 Zloader/Zbot'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/files/2020/05/the-silent-night-zloader-zbot_final.pdf.

Supported Platforms: Windows

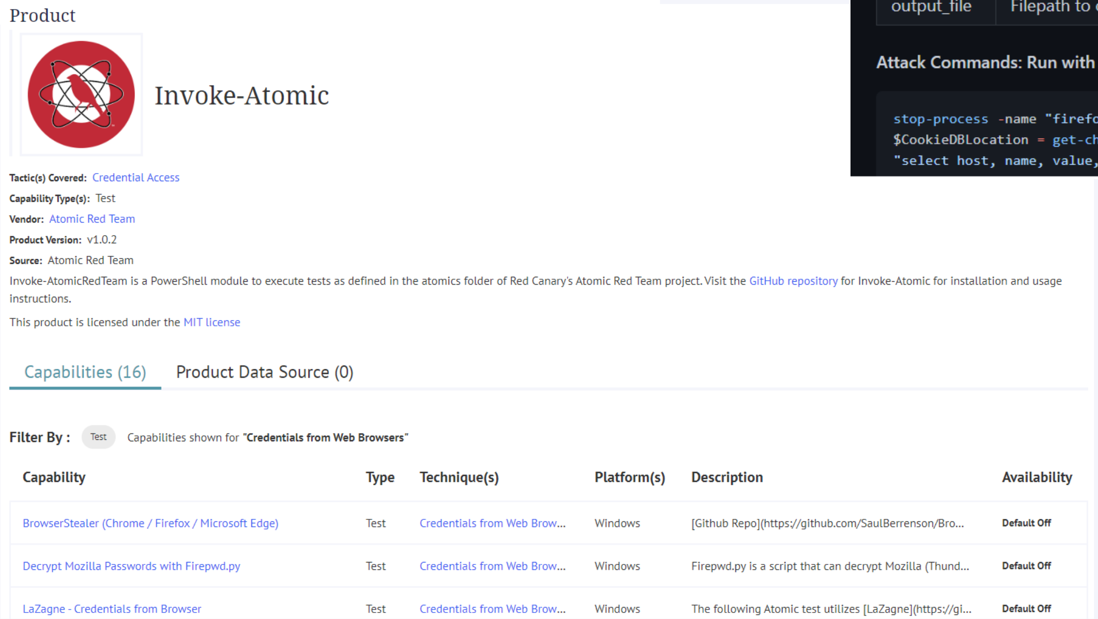
auto_generated_guid: 4b437357-f4e9-4c84-9fa6-9bcee6f826aa

Inputs:

Name	Description	Type	
sqlite3_path	Path to sqlite3	Path	$env:ten
output_file	Filepath to output cookies	Path	$env:ten

Attack Commands: Run with `powershell`!

```
stop-process -name "firefox" -force -erroraction silentlyco
$CookieDBLocation = get-childitem -path "$env:appdata\Mozil
"select host, name, value, path, expiry, isSecure, isHttpOn
```



Product

Invoke-Atomic

Tactic(s) Covered: Credential Access
Capability Type(s): Test
Vendor: Atomic Red Team
Product Version: v1.0.2
Source: Atomic Red Team

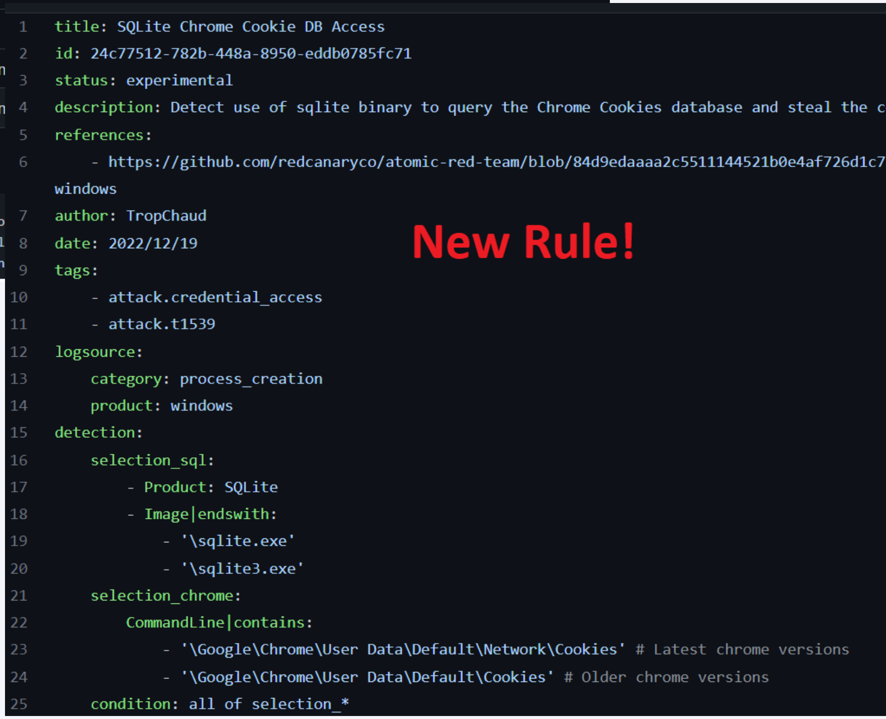
Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the atomics folder of Red Canary's Atomic Red Team project. Visit the GitHub repository for Invoke-Atomic for installation and usage instructions.

This product is licensed under the MIT license

Capabilities (16) Product Data Source (0)

Filter By : Test Capabilities shown for **"Credentials from Web Browsers"**

Capability	Type	Technique(s)	Platform(s)	Description	Availability
BrowserStealer (Chrome / Firefox / Microsoft Edge)	Test	Credentials from Web Brow...	Windows	[Github Repo](https://github.com/SaulBerrenson/Bro...	Default Off
Decrypt Mozilla Passwords with Firepwd.py	Test	Credentials from Web Brow...	Windows	Firepwd.py is a script that can decrypt Mozilla (Thund...	Default Off
LaZagne - Credentials from Browser	Test	Credentials from Web Brow...	Windows	The following Atomic test utilizes [LaZagne](https://gi...	Default Off



```
title: SQLite Chrome Cookie DB Access
id: 24c77512-782b-448a-8950-eddb0785fc71
status: experimental
description: Detect use of sqlite binary to query the Chrome Cookies database and steal the c
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7
windows
author: TropChaud
date: 2022/12/19
tags:
    - attack.credential_access
    - attack.t1539
logsource:
    category: process_creation
    product: windows
detection:
    selection_sql:
        - Product: SQLite
        - Image|endswith:
            - '\sqlite.exe'
            - '\sqlite3.exe'
    selection_chrome:
        CommandLine|contains:
            - '\Google\Chrome\User Data\Default\Network\Cookies' # Latest chrome versions
            - '\Google\Chrome\User Data\Default\Cookies' # Older chrome versions
    condition: all of selection_*
```

New Rule!

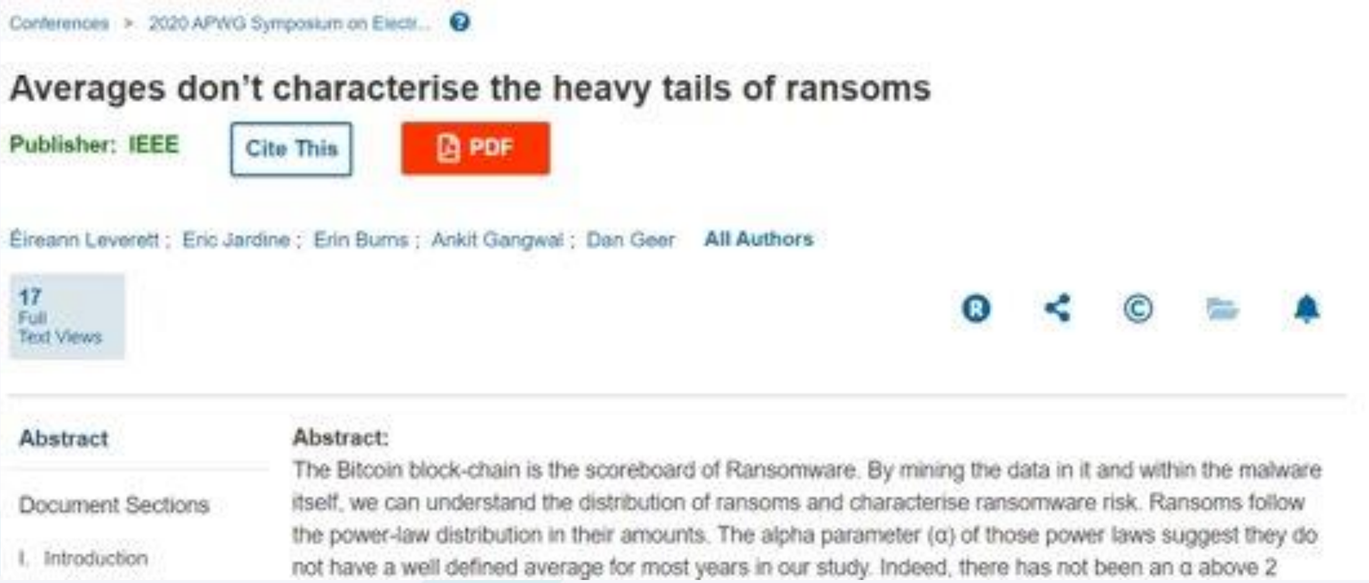
Ransomware Payment Intelligence

Ransomware "Market" Overview

TIDAL

THREAT-INFORMED DEFENSE

Stop using averages to describe your ransom data set.



Averages don’t characterise the heavy tails of ransoms

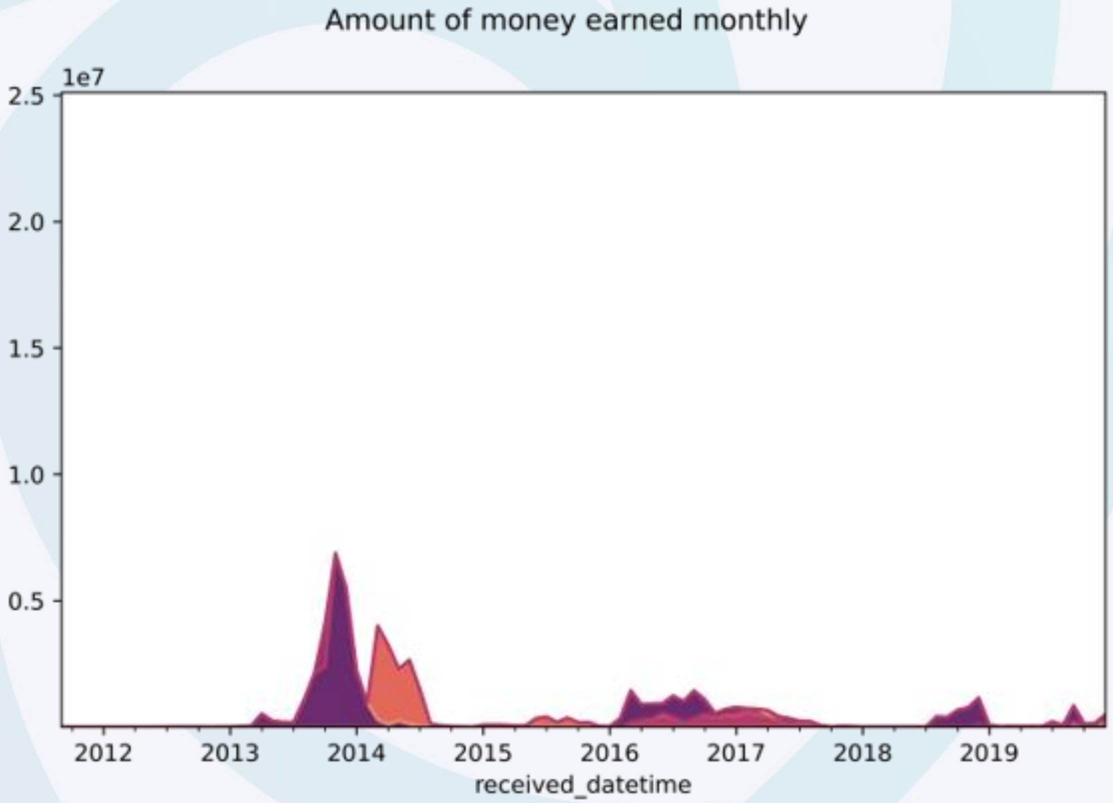
Publisher: IEEE

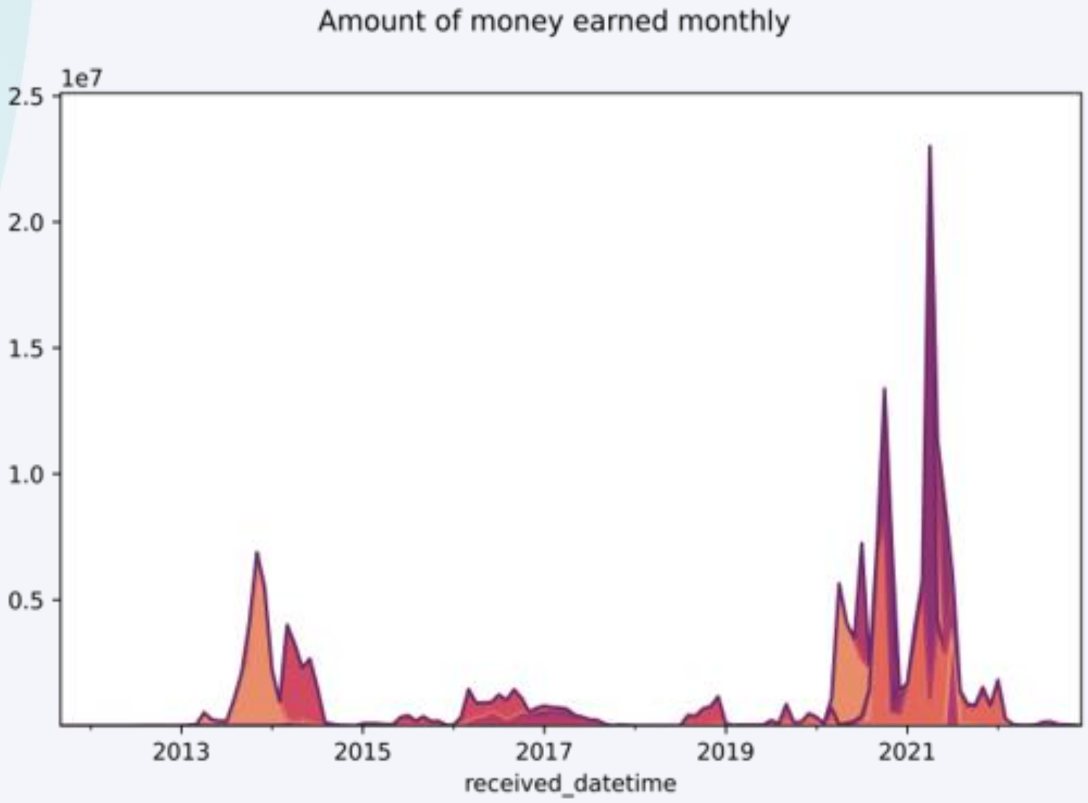
Éireann Leverett ; Eric Jardine ; Erin Burns ; Ankit Gangwal ; Dan Geer

Abstract:

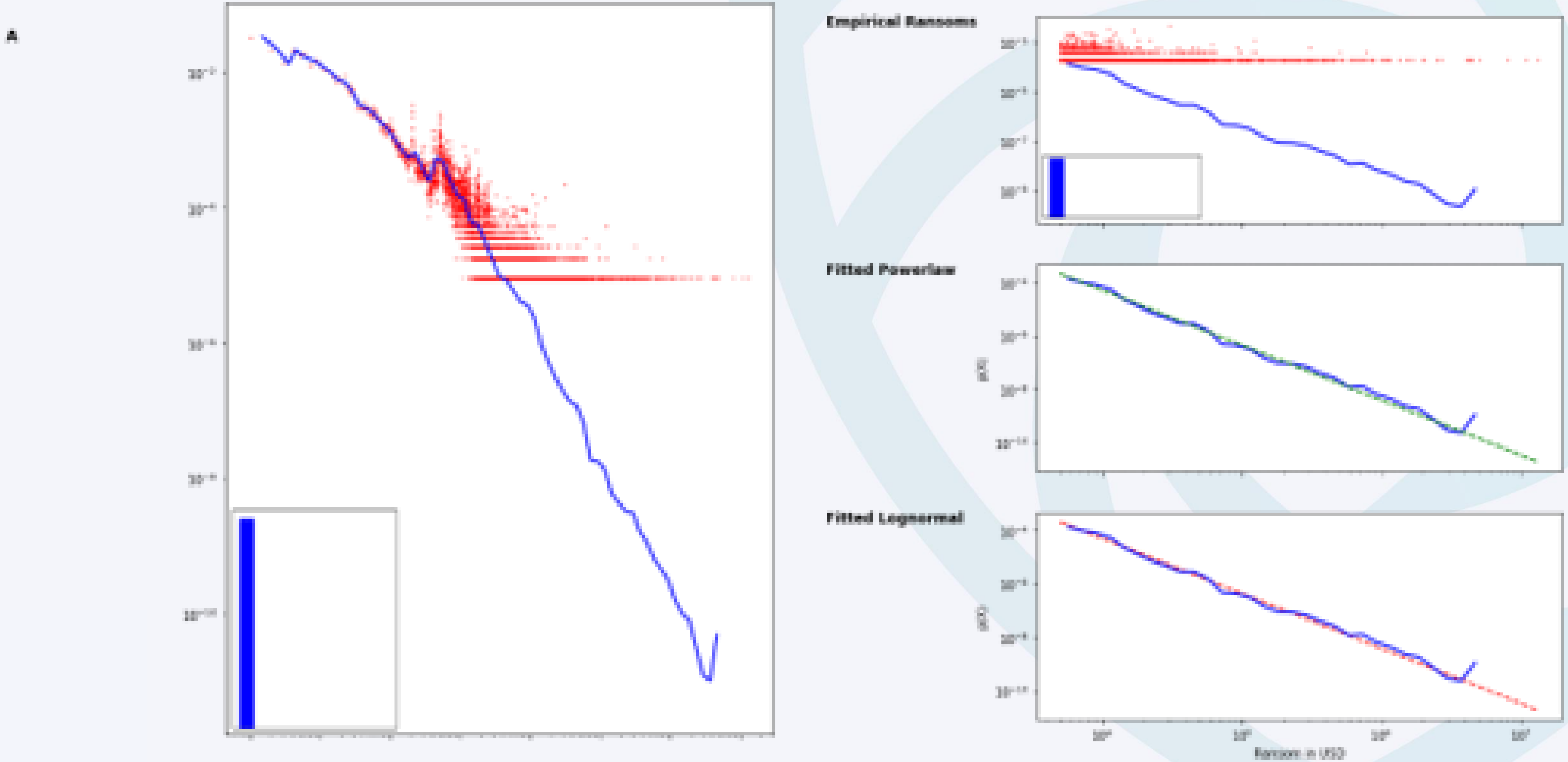
The Bitcoin block-chain is the scoreboard of Ransomware. By mining the data in it and within the malware itself, we can understand the distribution of ransoms and characterise ransomware risk. Ransoms follow the power-law distribution in their amounts. The alpha parameter (α) of those power laws suggest they do not have a well defined average for most years in our study. Indeed, there has not been an α above 2

Before and After our warning

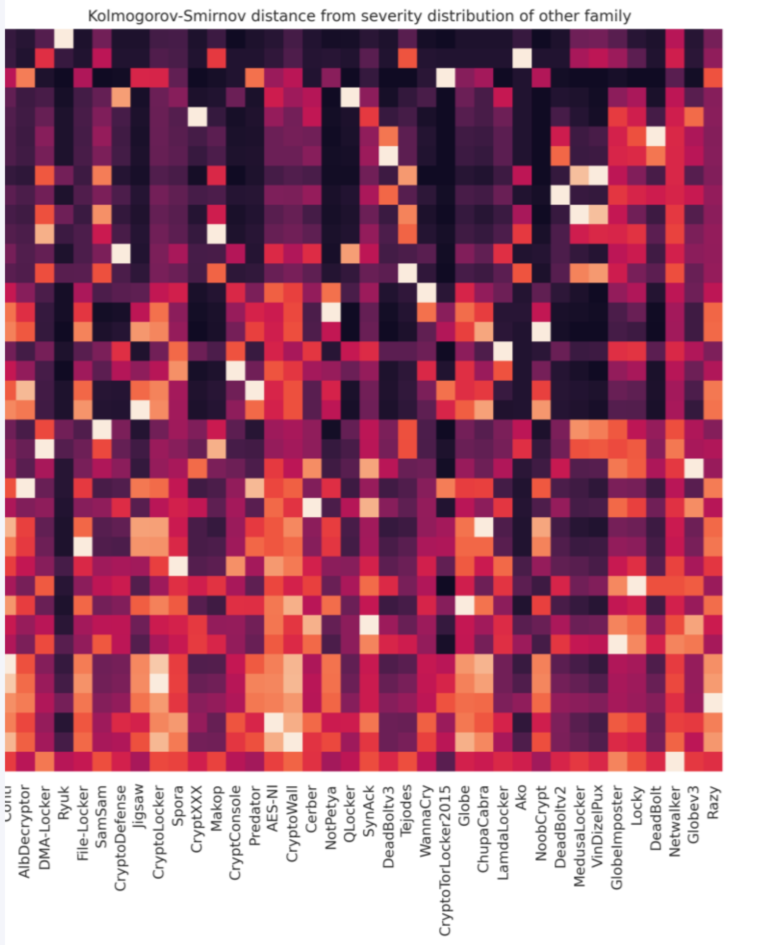




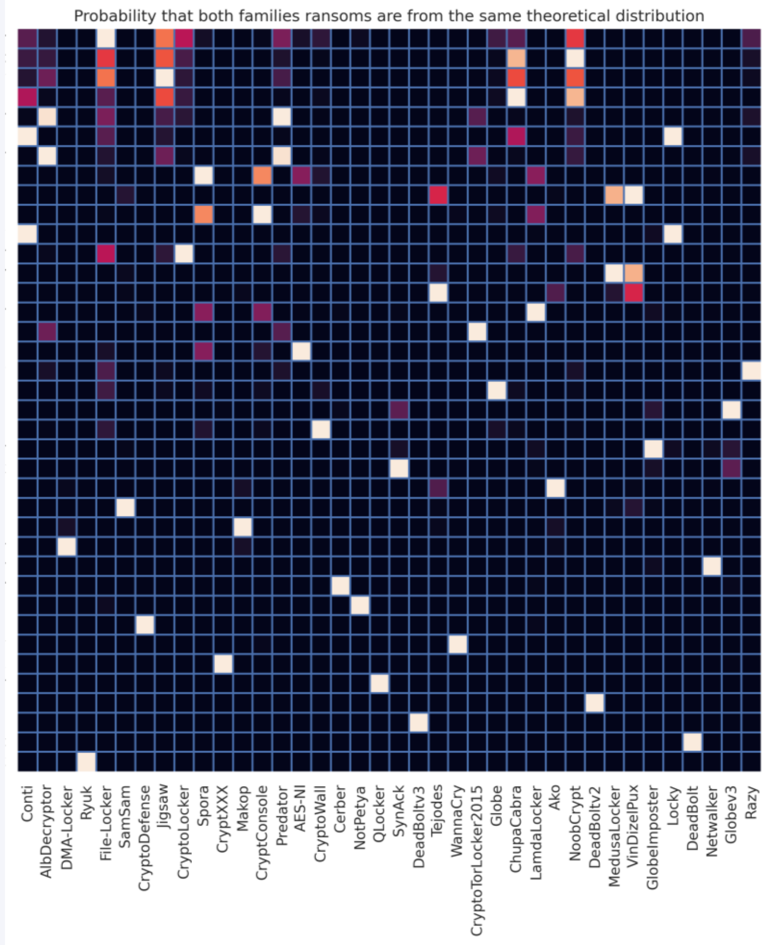
You can fit powerlaws or lognormals to ransom data.



But you shouldn't!



Kolmogorov-Smirnov distance from severity distribution of other family

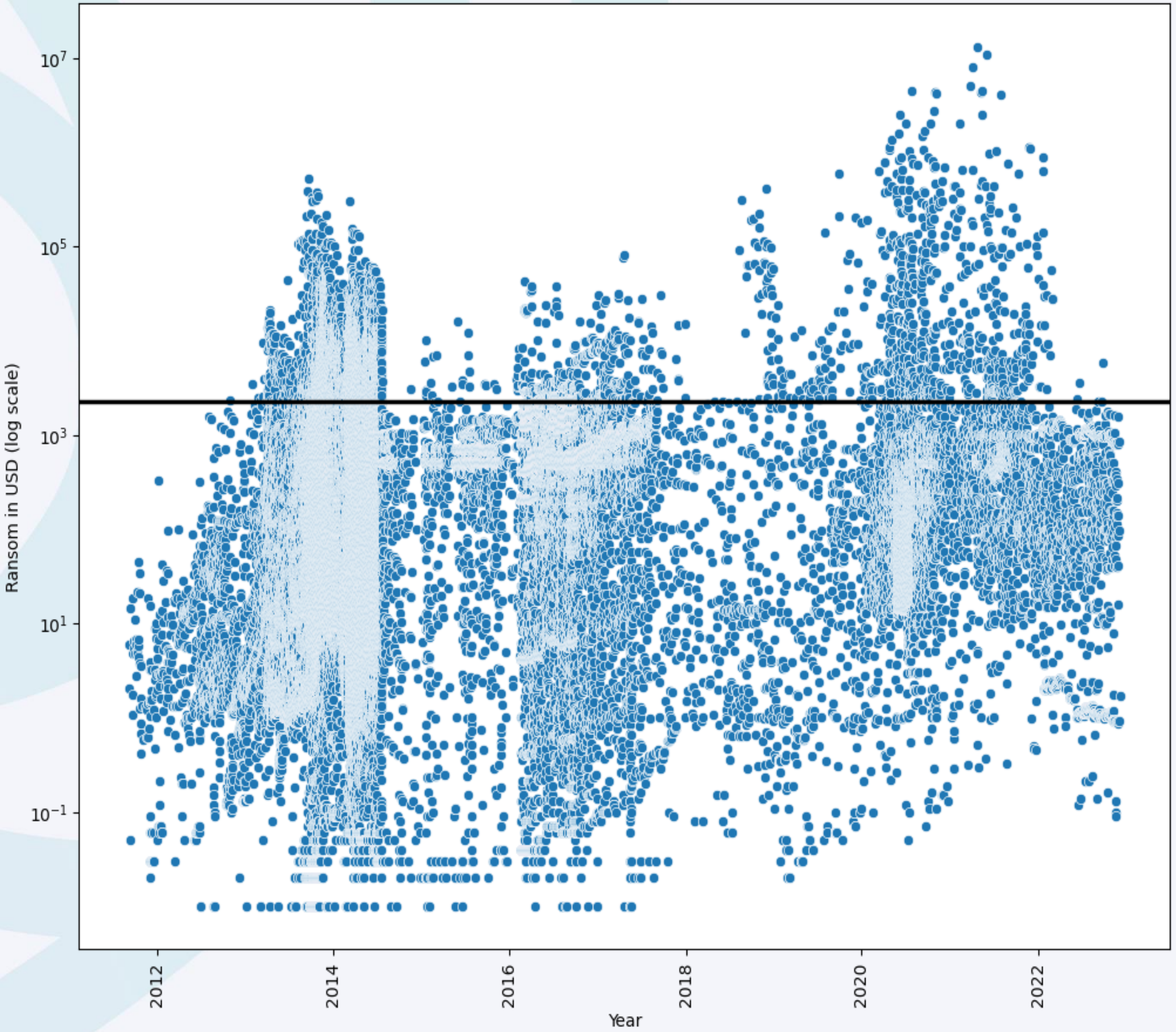


Probability that both families ransoms are from the same theoretical distribution

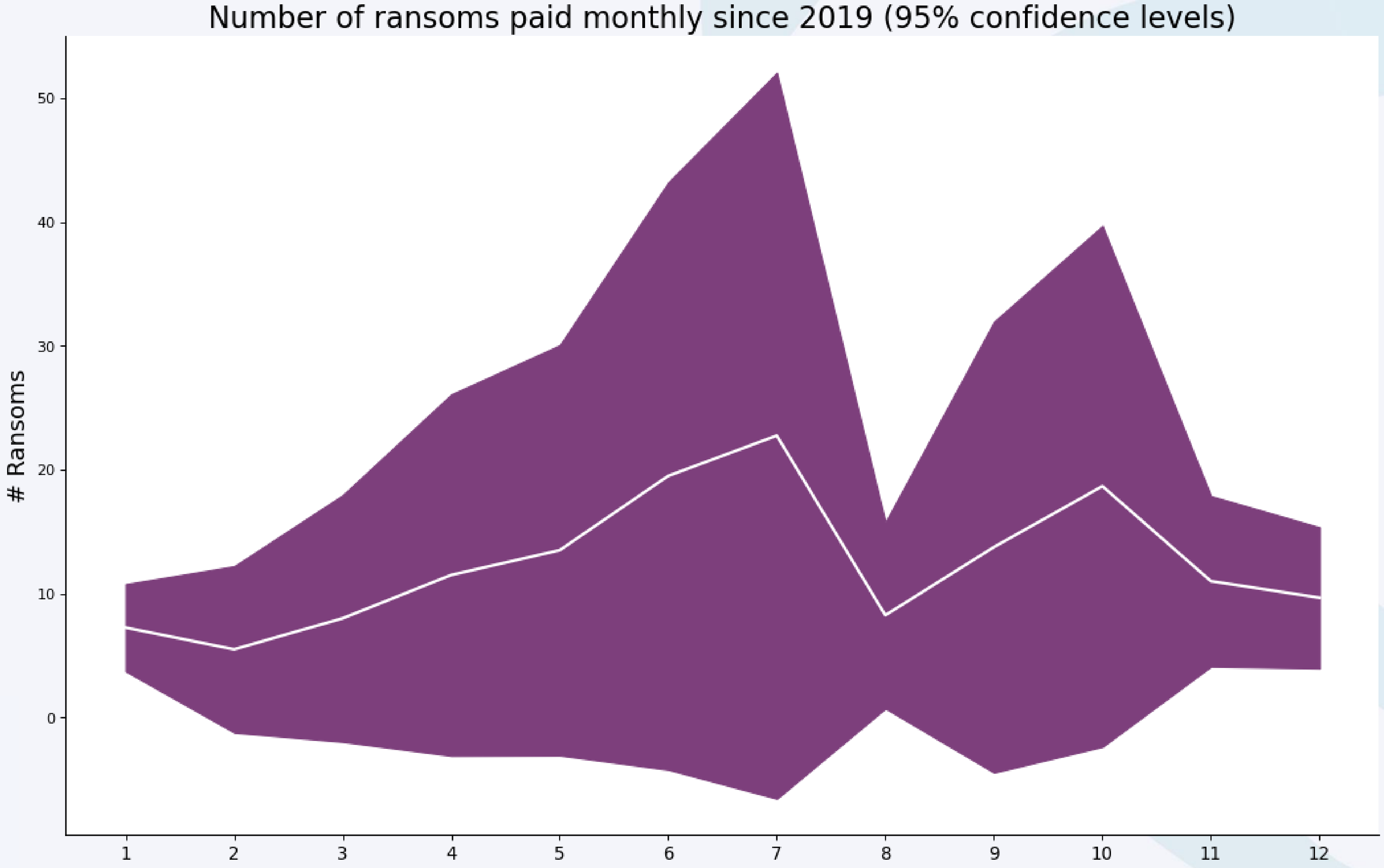
- Left is the KS distance
- Right is the probability (P-Value) that both severities are from the same distribution.
  - White is highly likely to be the same
  - Black is highly unlikely to be the same
- You can also do this for frequency and get similar results.

92% of ransoms are below average

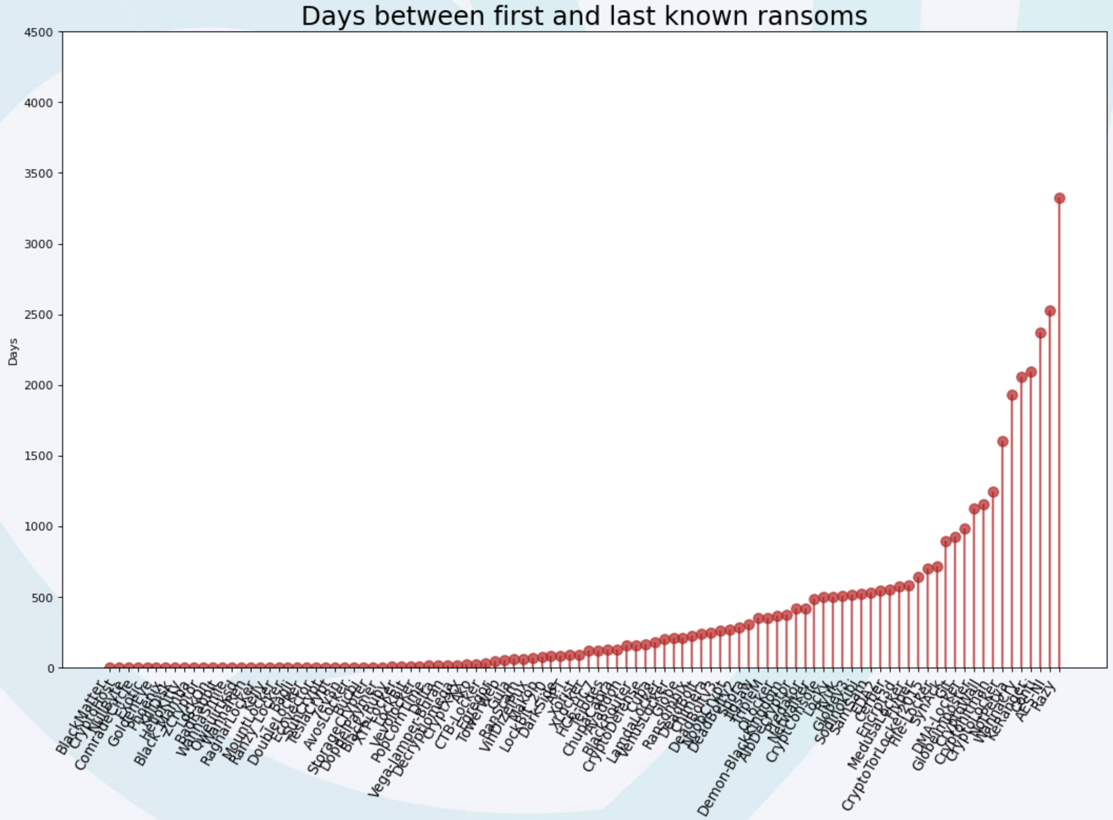
A decade of ransoms.

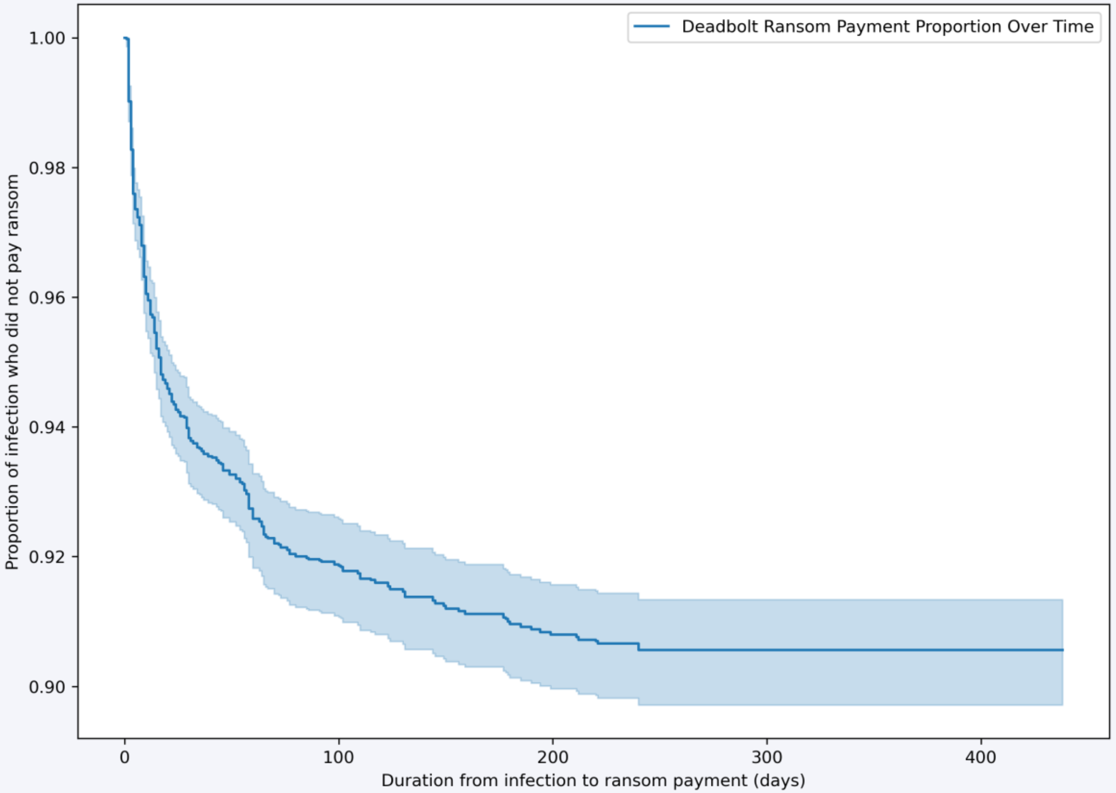


July is peak ransom paying season



On time and financial surveillance

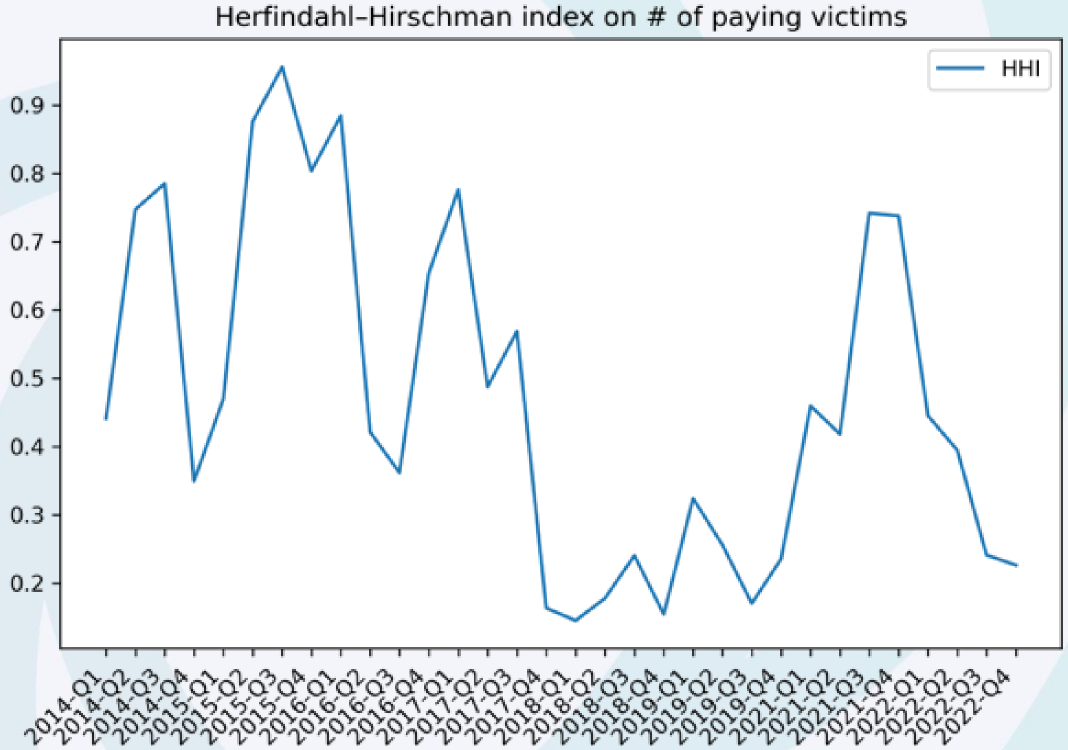


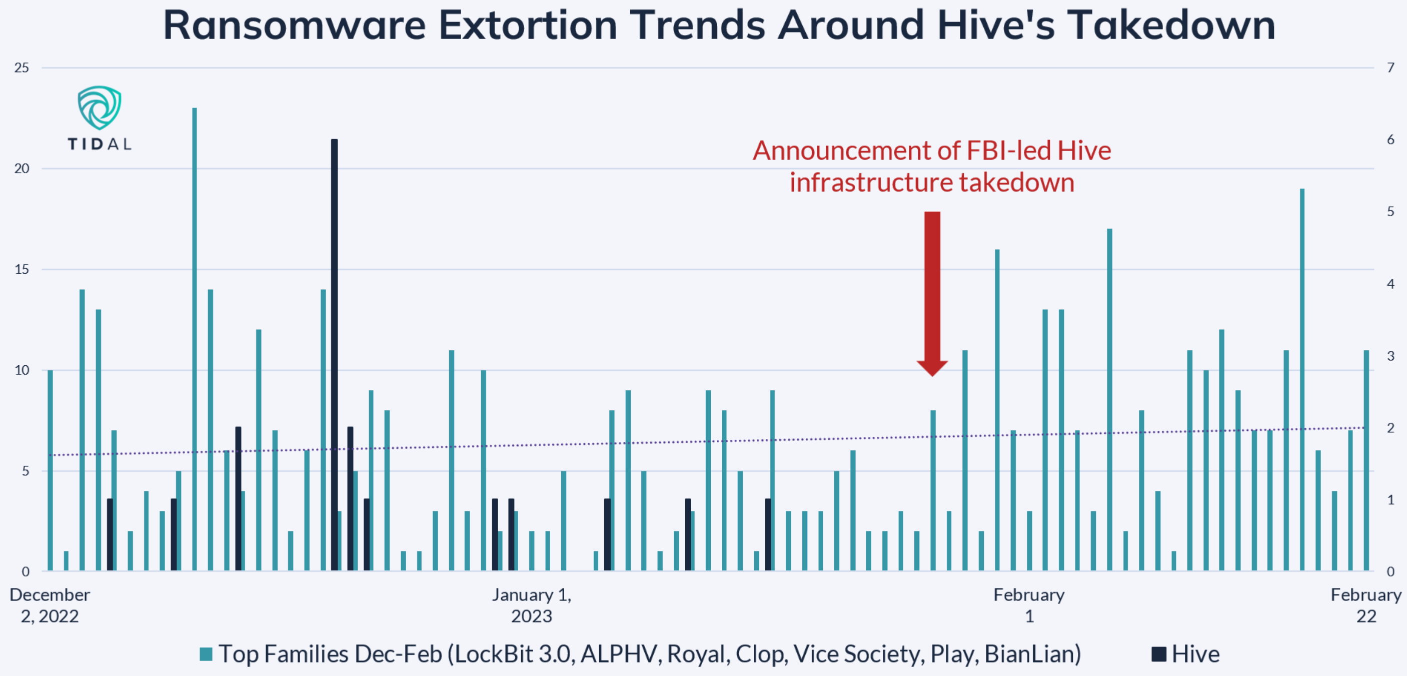


Market Concentration and Ransomware

High Y-axis = "monopoly"

Low Y-axis = "free market"





Announcement of FBI-led Hive infrastructure takedown

Thank you!

TIDAL