Defensive Measures

Adversary Actions in the face of adversity

johnhering
@johnhering

Follow

cybersecurity is one of the few domains where the edge of human performance meets the edge of human performance.

11:03 PM - 29 Mar 2016

Cause / Effect - What is working?

Investigated

- ***Blocking IoCs (IPs / Domains), Releases***
- ***Signatures***
- ***Vulnerabilities***
- **Patching**
- **Takedowns**
- ~~***Incident Response / Evictions***~~
- ***Civil Cases – limited data***
- **Indictments & Arrests**

IoC Releases

IoC Releases for CyberCrime

Significant Lack of Data (sample set of 2!)

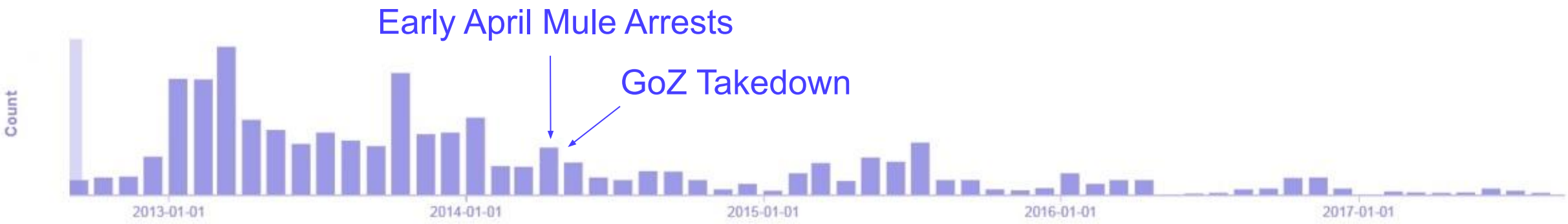
- **Network IOCs**
  - Cyber Crime – Short Lived
  - In Data Set avg. delta :
    - ~140 days since last seen
    - ~200 days since first appearance
  - Signatures work better
- **Malware (hashes)**
  - CyberCrime – Known Malware
  - APT – *New Malware*!

GOLD EVERGREEN

Roughly – The Business Club

ZeuS -> ZeuS as a Service (GoZ)

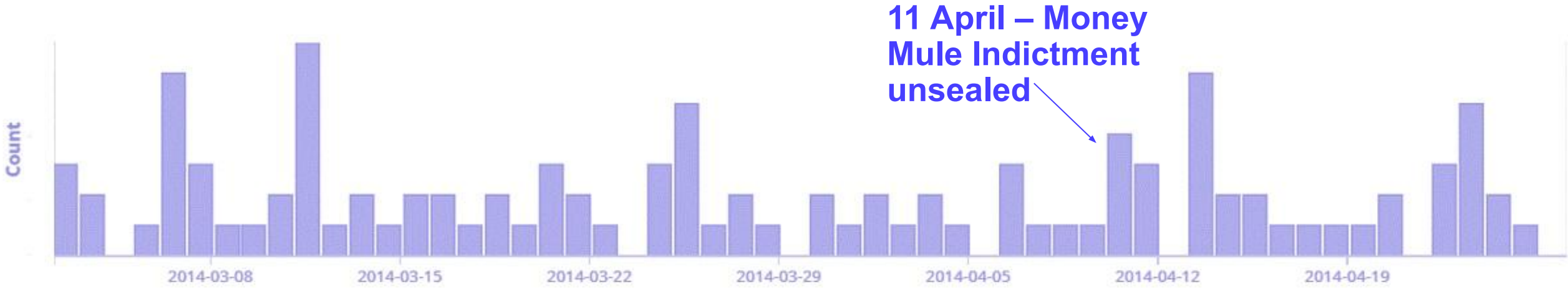
GOLD EVERGREEN



- **Just Cryptolocker and Game Over Zeus**

GOLD EVERGREEN

April 2014 Mule Arrests



- **Rise in GameOver Zeus detections after mule arrests**

GOLD DRAKE

Dridex, Locky, Emotet

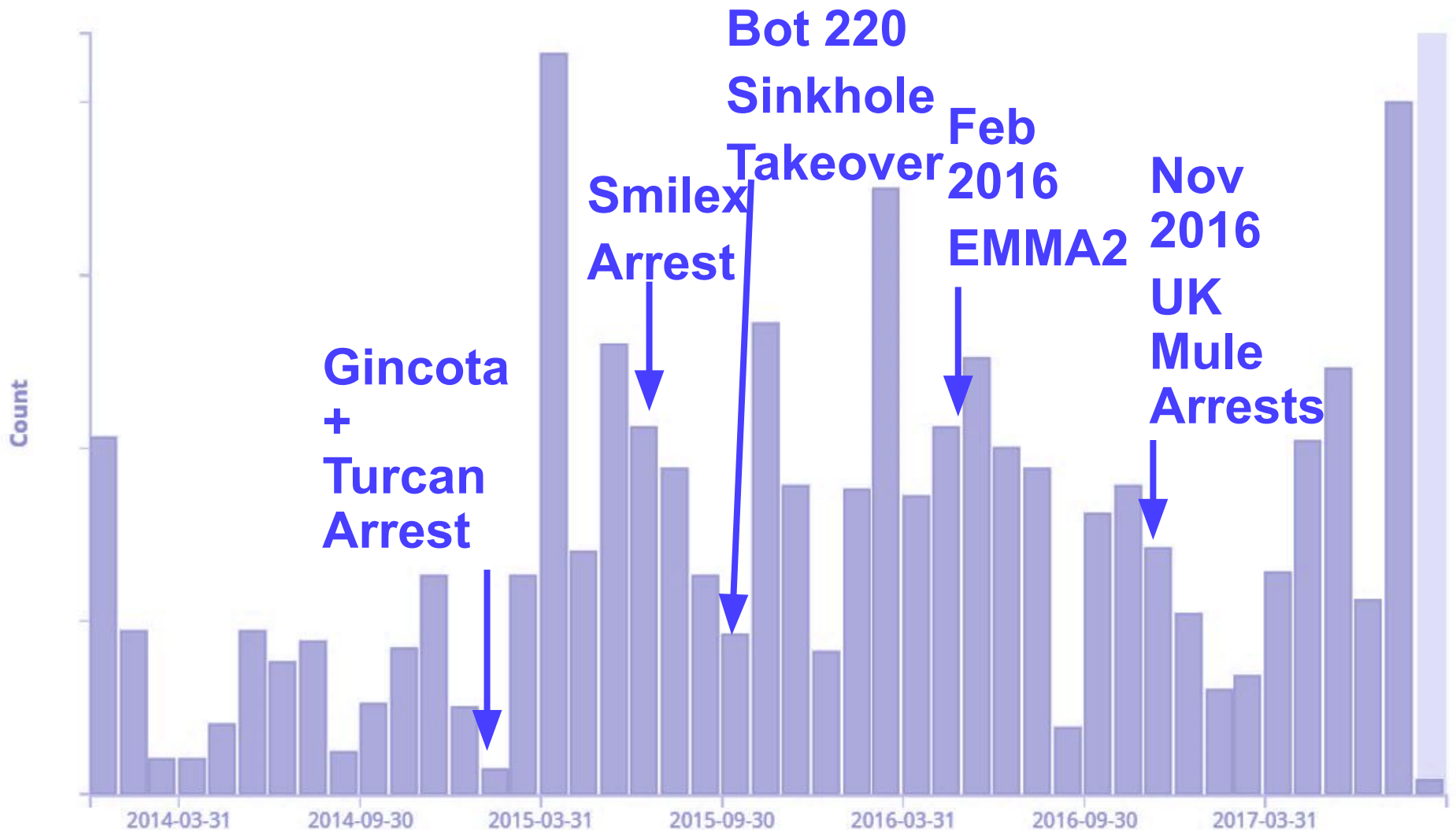
Dridex vis a vis Chrome

Reaction to Web Inject Patches

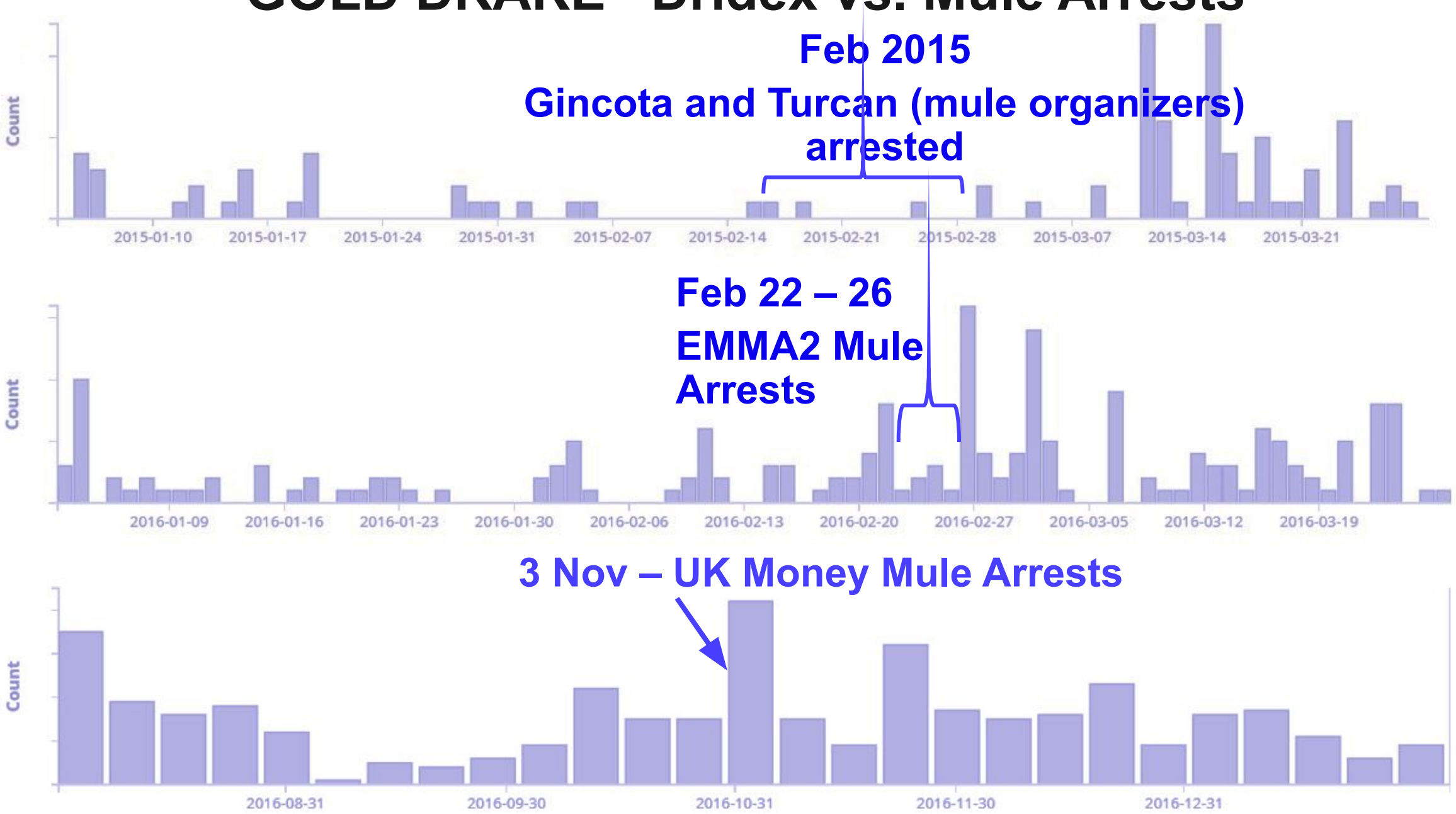
Chrome Version	Chrome Release Date	Dridex Version	Dridex Timestamp	Time Delta
40.0.2214.115	19.2.2015	2.093	11.3.2015	20 days
42.0.2311.90	14.4.2015	2.108	17.4.2015	3 days
43.0.2357.65	19.5.2015	3.011	26.5.2015	7 days
44.0.2403.89	21.7.2015	3.073	6.8.2015	16 days
45.0.2454.85	1.9.2015	3.102	25.9.2015	24 days
47.0.2526.73	1.12.2015	3.154	7.12.2015	6 days
48.0.2564.97	27.1.2016	3.167	29.1.2016	2 days
49.0.2623.87	8.3.2016	3.188	10.3.2016	2 days
51.0.2704.106	23.6.2016	3.225	24.6.2016	1 day
53.0.2785.116	14.9.2016	3.258	26.9.2016	12 days
54.0.2840.71	20.10.2016	3.269	17.11.2016	3 days
58.0.3029.81	19.4.2017	4.048	16.5.2017	27 days

Source: VB2017, ESET

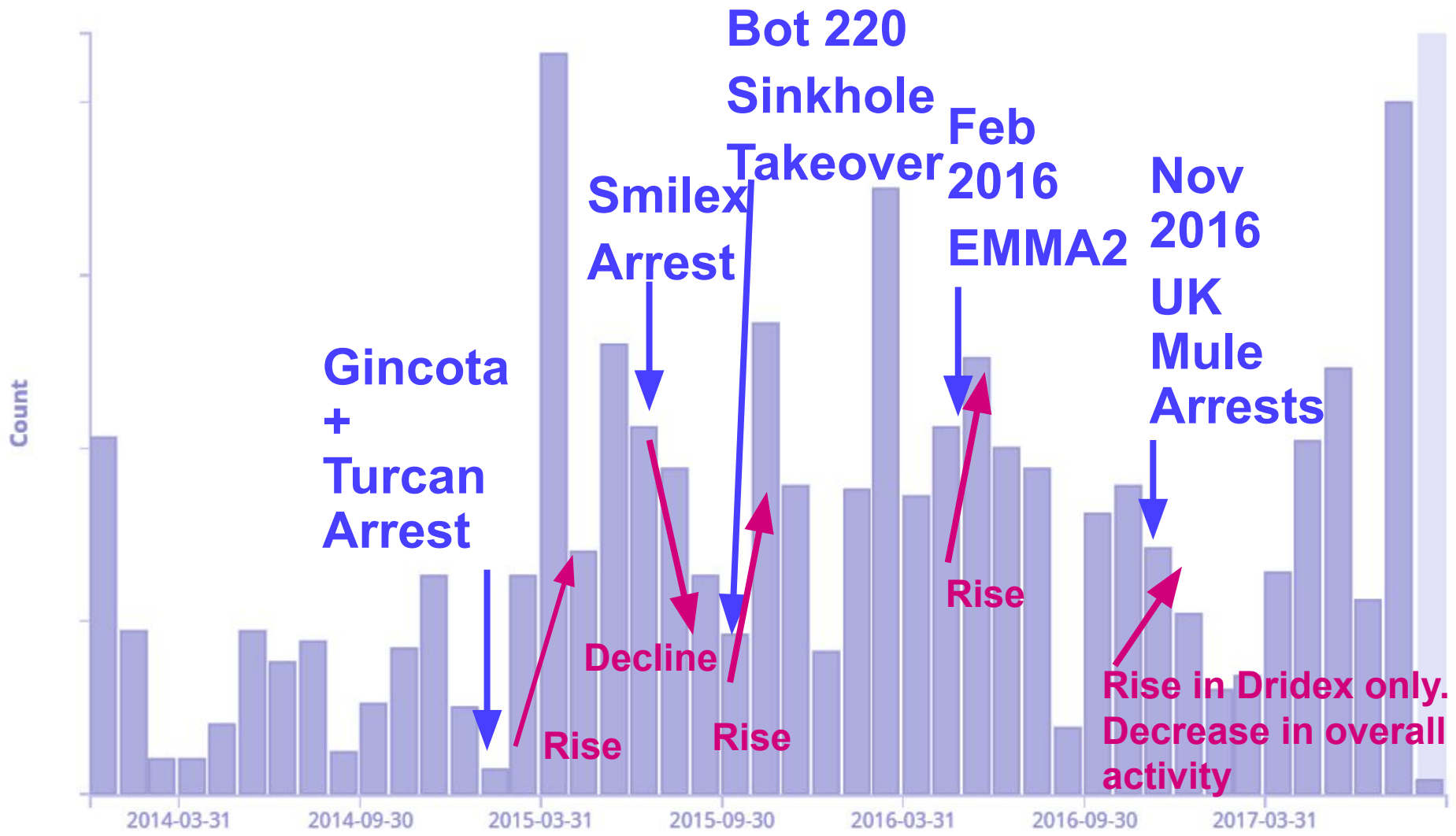
GOLD DRAKE – DRIDEX + LOCKY + EMOTET



GOLD DRAKE– Dridex vs. Mule Arrests



GOLD DRAKE – DRIDEX + LOCKY + EMOTET



GOLD DRAKE

Counterpoints / Takeaways

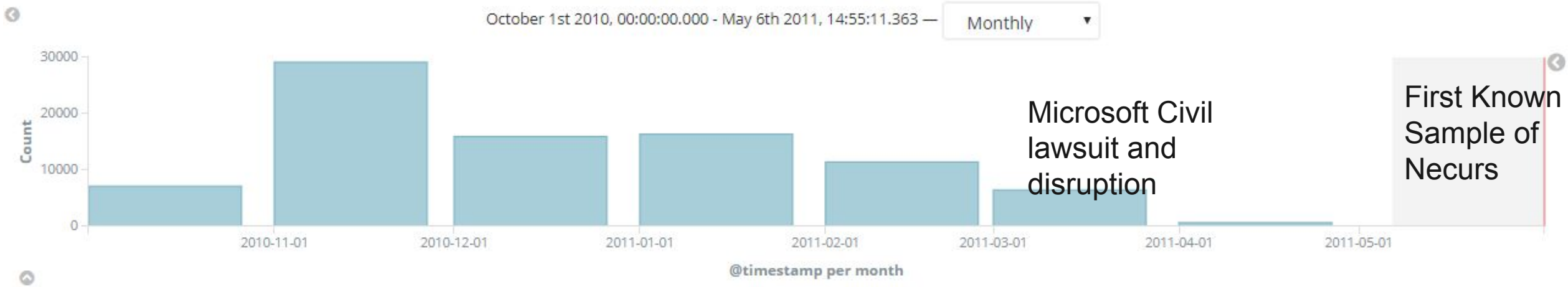
- **Strong Technical Skill**
  - **Quickly overcome technical countermeasures**
- **Mule Arrests Correspond with**
  - Short term Rise in Activity
  - Long term **Decrease** in Activity
- **Maybe the mule arrests are working…**
  - **Group seems to be trying different revenue models…**
- **Continuous Innovation and Modifications**

Are we creating “Superbugs”

Do Takedowns result in new stronger, botnets

Secureworks®

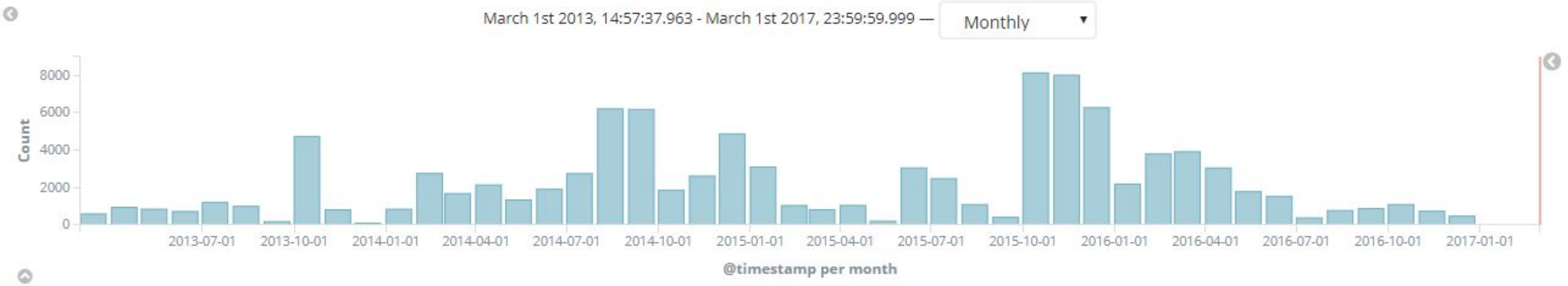
RUStock



Microsoft Civil lawsuit and disruption

First Known Sample of Necurs

Necurs



Unclear…

Attempts to measure…

- Takedowns vs. New Features
- Takedowns vs. New Infrastructure Schemes
- Takedowns vs. New Malware Families
  - Maybe slight correlation…
    - *After a takedown a new bot will be introduced … sometime in the future*

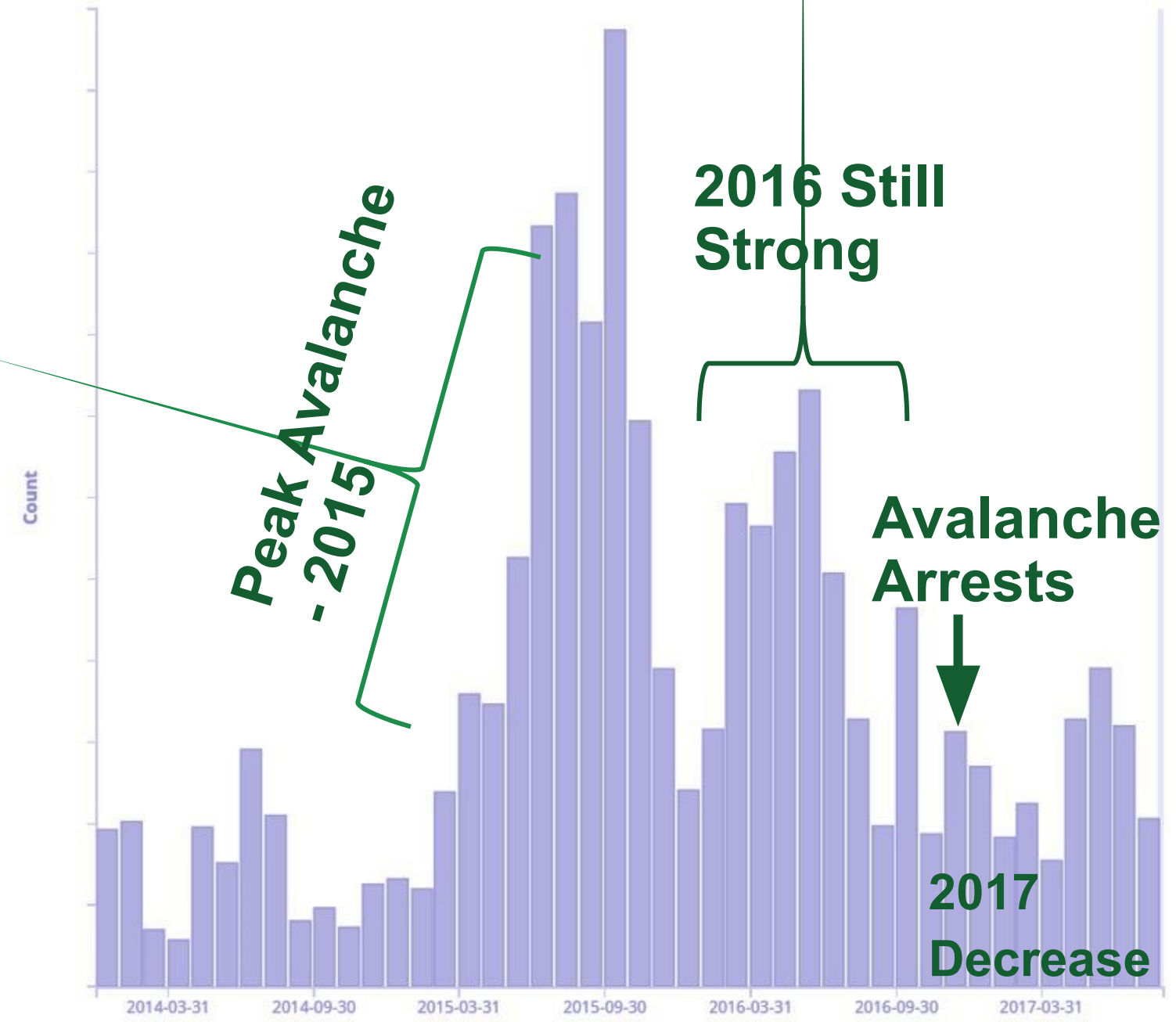
Avalanche

Bulletproof hosting
supporting multiple actors

Avalanche

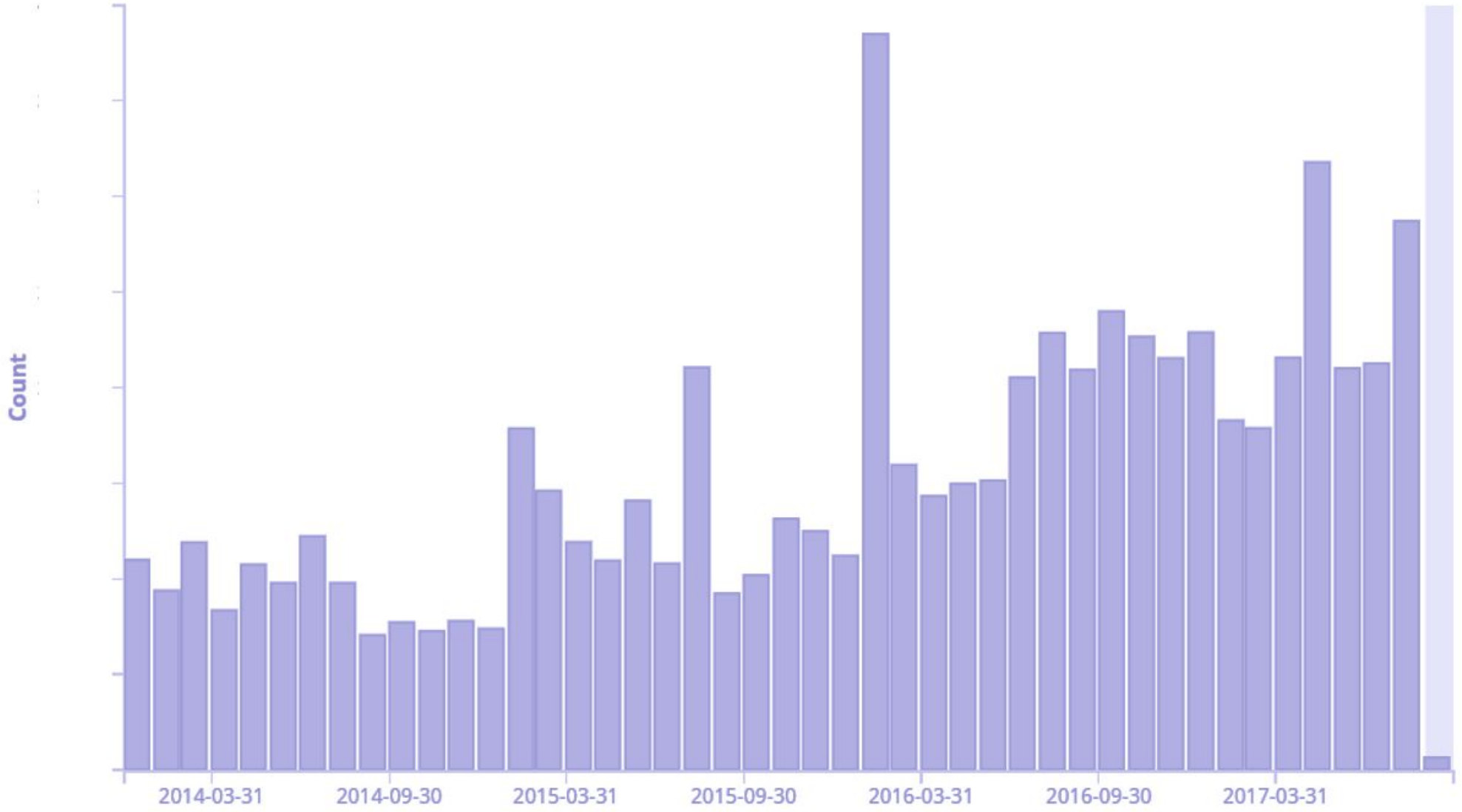
Activity 2014 - 2017

- Bulletproof hosting used by multiple actors, typically eastern European
- Avalanche arrests (most admins) Dec 2017



Cybercrime in general

“Organized” CyberCrime in General



Main Takeaways

What Doesn't Work

- Indictments w/o Arrest
- Takedowns w/o Arrest
- Wipe and Reimage

Inconclusive

- Patches
  - Not everyone applies on day 1
  - delivered via phish, then EK
- Civil Cases
  - Too little data
- Indicator releases
  - Too little data
  - Stale IoCs
- Super Bugs?
  - seem to innovate consistently

What works

- Technical Operator Arrests
- Takedowns accompanied by Arrests

Secureworks®