

Issued for Abuse

Measuring the Underground Trade in Code Signing Certificates

Kristián Kozák[◆], Bum Jun Kwon[★], Doowon Kim[★], Tudor Dumitraş[★]

MUNI

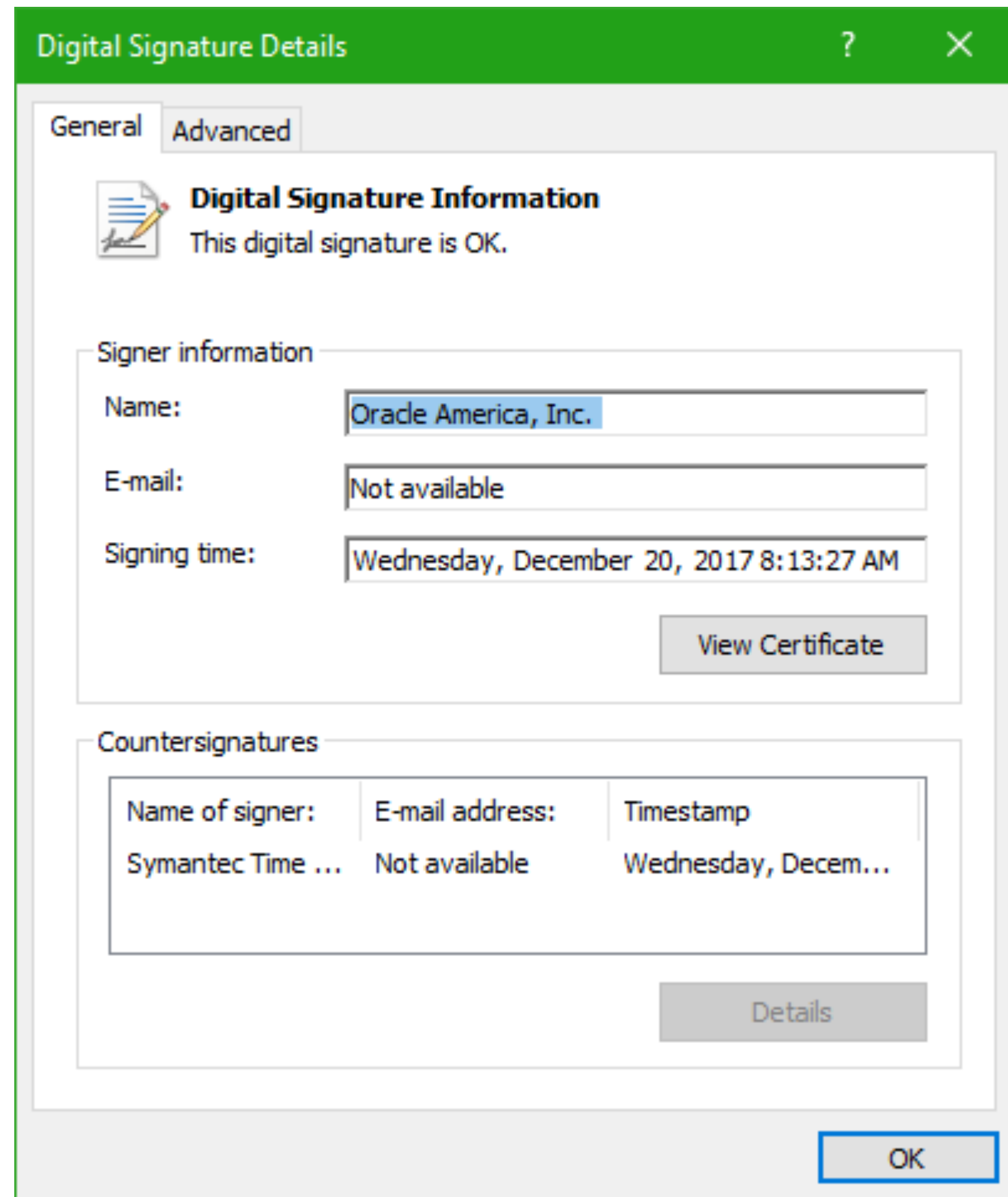
[◆] Masaryk University, Brno



[★] University of Maryland

Presented at
WEIS 2018

Code Signing: Overview



Code Signing Certificate:

Binding a signing key to a software publisher.

User Account Control



Do you want to allow this app from an unknown publisher to make changes to your device?

Microsoft Windows Setup

Publisher: Unknown

File origin: Hard drive on this computer

[Show more details](#)

Yes

No

Anonymous Certificates

Code signing designed to prevent anonymous publishers

PUP: Fine with code signing [Kotzias 2015]

Malware: Needs anonymous signatures [Kim 2017]

Where do the malware authors get the valid signatures?



What is their business model?

Research Methods & Goals

Black markets for code signing not studied systematically yet

Hard to formulate hypotheses a-priori

Inductive approach (hypotheses from data)

Gather evidence about the activity of underground vendors

Analyze usage of certificates in signed malware

Infer the role of the black market in the production of signed malware

Passive measurement

No influence over black market (exception: responsible disclosure)

Data Collection

Supply view

Observation of the black market

Manual analysis: August 2017

Automated collection of stock
information: Sep-Nov 2017

Demand view

Analysis of signed malware dataset

Collected: Apr-Aug 2017

Supply: Where is the black market?

Challenges

Past reports: E-shop already down

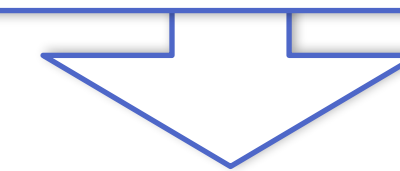
No goods at SilkRoad (data by [Christin 2013])

No goods among other general marketplaces

Data collection

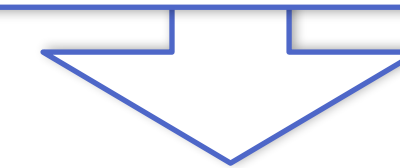
Start

Set of known sites



Expansion

Following links & handles



Saturation

No new sites anymore

Some remain inaccessible

Demand: Collection & Clustering

VirusTotal Hunting + Filtering

14,221 *correctly signed* malware samples

1,163 abusive certificates

Clustering of publisher identities

Ltd "Vet Fektor"

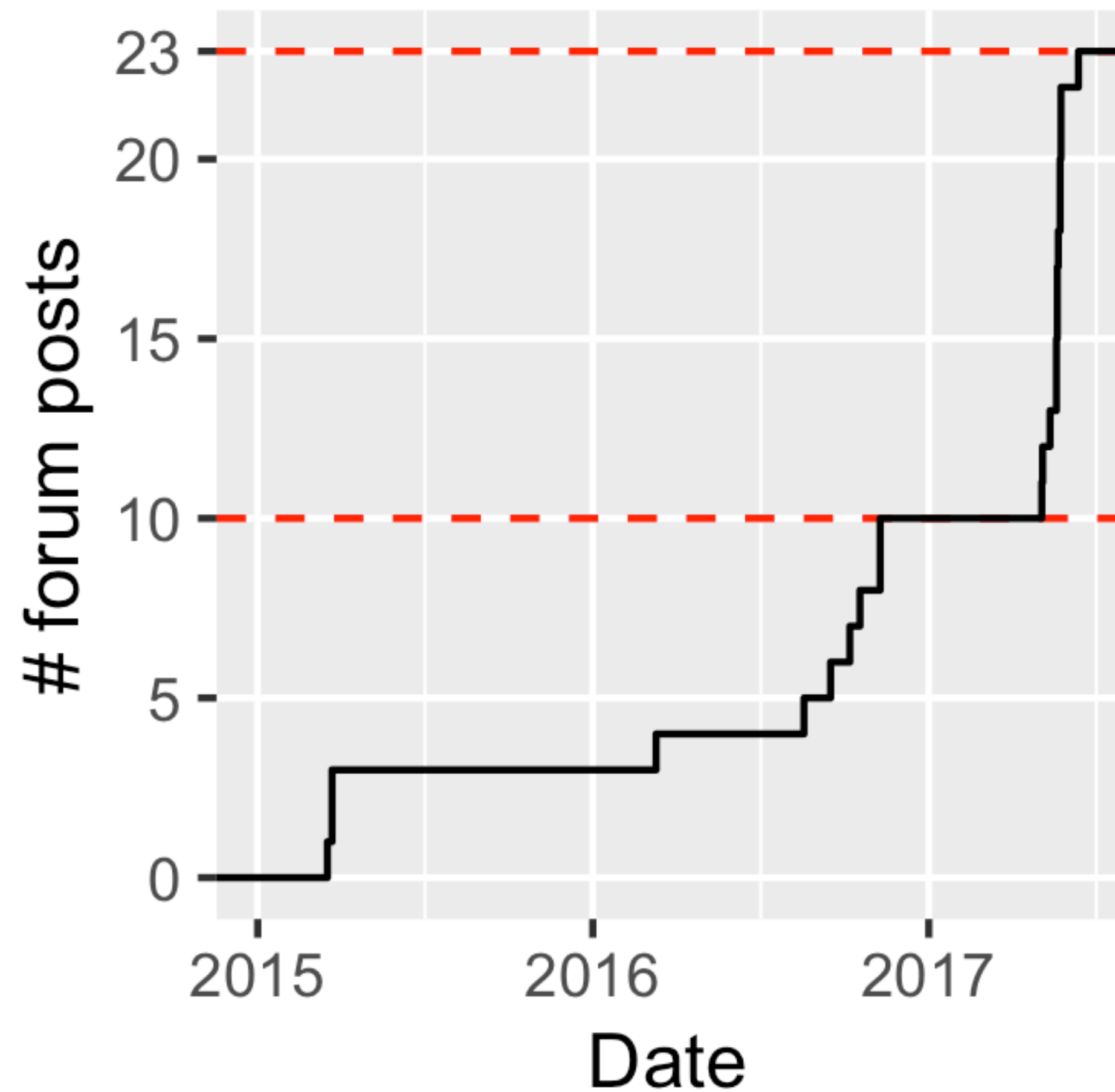
000, Vet – Fektor

LLC `VET FEKTOR`

AVClass: Malware family labeling

Graph analysis

Vendors and Activity



Business on forums + one new e-shop

4 vendors identified, each across multiple forums

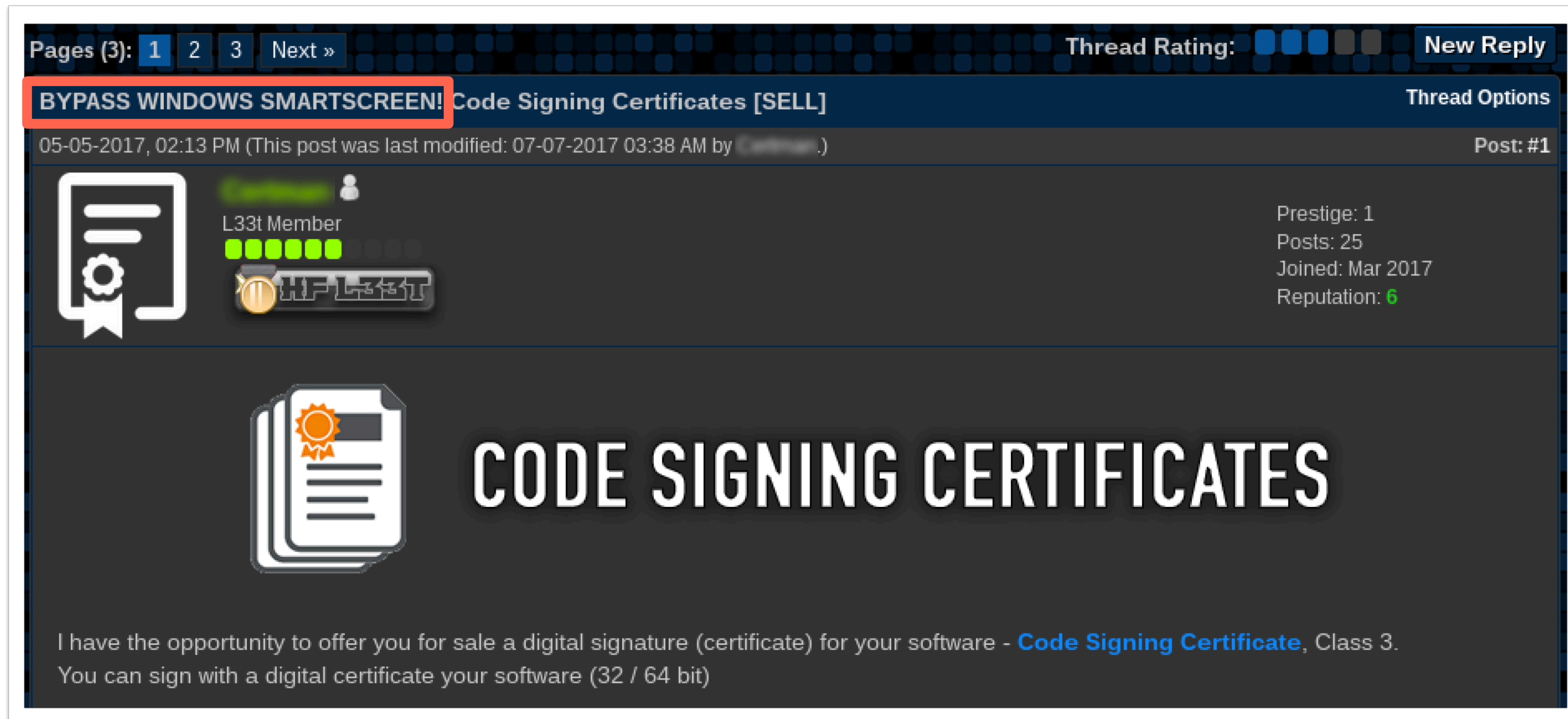
Post count increased more than 2-fold in early 2017

Mechanisms and Business Model


Selling anonymous code signing certificates

No evidence of other business models (signatures, PPI)

Each certificate is fresh, never used and sold only once



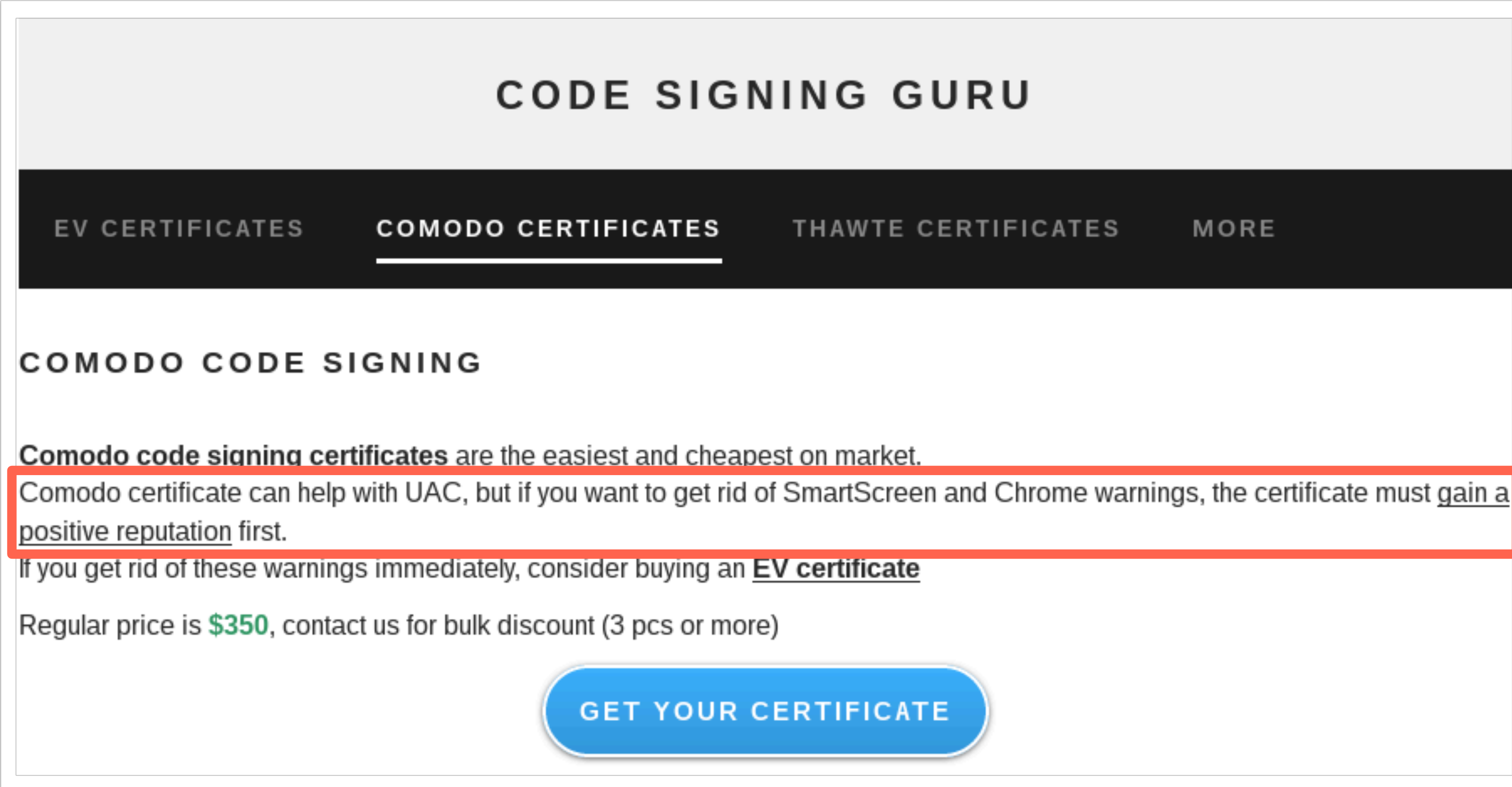
The screenshot shows a forum thread with the following details:

- Pages (3): 1 2 3 Next »
- Thread Rating: [Progress indicator]
- New Reply
- Thread Title: **BYPASS WINDOWS SMARTSCREEN! Code Signing Certificates [SELL]**
- Thread Options
- Post Date: 05-05-2017, 02:13 PM (This post was last modified: 07-07-2017 03:38 AM by [User])
- Post: #1
- User Profile: L33t Member (5 green stars, HP icon)
- User Stats: Prestige: 1, Posts: 25, Joined: Mar 2017, Reputation: 6
- Image:  **CODE SIGNING CERTIFICATES**
- Text: I have the opportunity to offer you for sale a digital signature (certificate) for your software - [Code Signing Certificate](#), Class 3. You can sign with a digital certificate your software (32 / 64 bit)

Driving the Demand

SmartScreen appears to drive the demand

Bypass SmartScreen = Build positive reputation



The screenshot shows a website for 'CODE SIGNING GURU'. The navigation bar includes 'EV CERTIFICATES', 'COMODO CERTIFICATES' (which is underlined), 'THAWTE CERTIFICATES', and 'MORE'. The main content area is titled 'COMODO CODE SIGNING'. A red box highlights the text: 'Comodo certificate can help with UAC, but if you want to get rid of SmartScreen and Chrome warnings, the certificate must gain a positive reputation first.' Below this, it says 'If you get rid of these warnings immediately, consider buying an EV certificate'. The regular price is listed as '\$350', with a note to contact for bulk discounts. A blue button at the bottom says 'GET YOUR CERTIFICATE'.

CODE SIGNING GURU

EV CERTIFICATES COMODO CERTIFICATES THAWTE CERTIFICATES MORE

COMODO CODE SIGNING

Comodo code signing certificates are the easiest and cheapest on market.

Comodo certificate can help with UAC, but if you want to get rid of SmartScreen and Chrome warnings, the certificate must gain a positive reputation first.

If you get rid of these warnings immediately, consider buying an EV certificate

Regular price is \$350, contact us for bulk discount (3 pcs or more)

GET YOUR CERTIFICATE

Origin of the Certificates

Supply side view

Vendors: Certificates are fresh + 1 year of validity

Lying \Rightarrow Loosing reputation \Rightarrow Sales more difficult

Demand side view

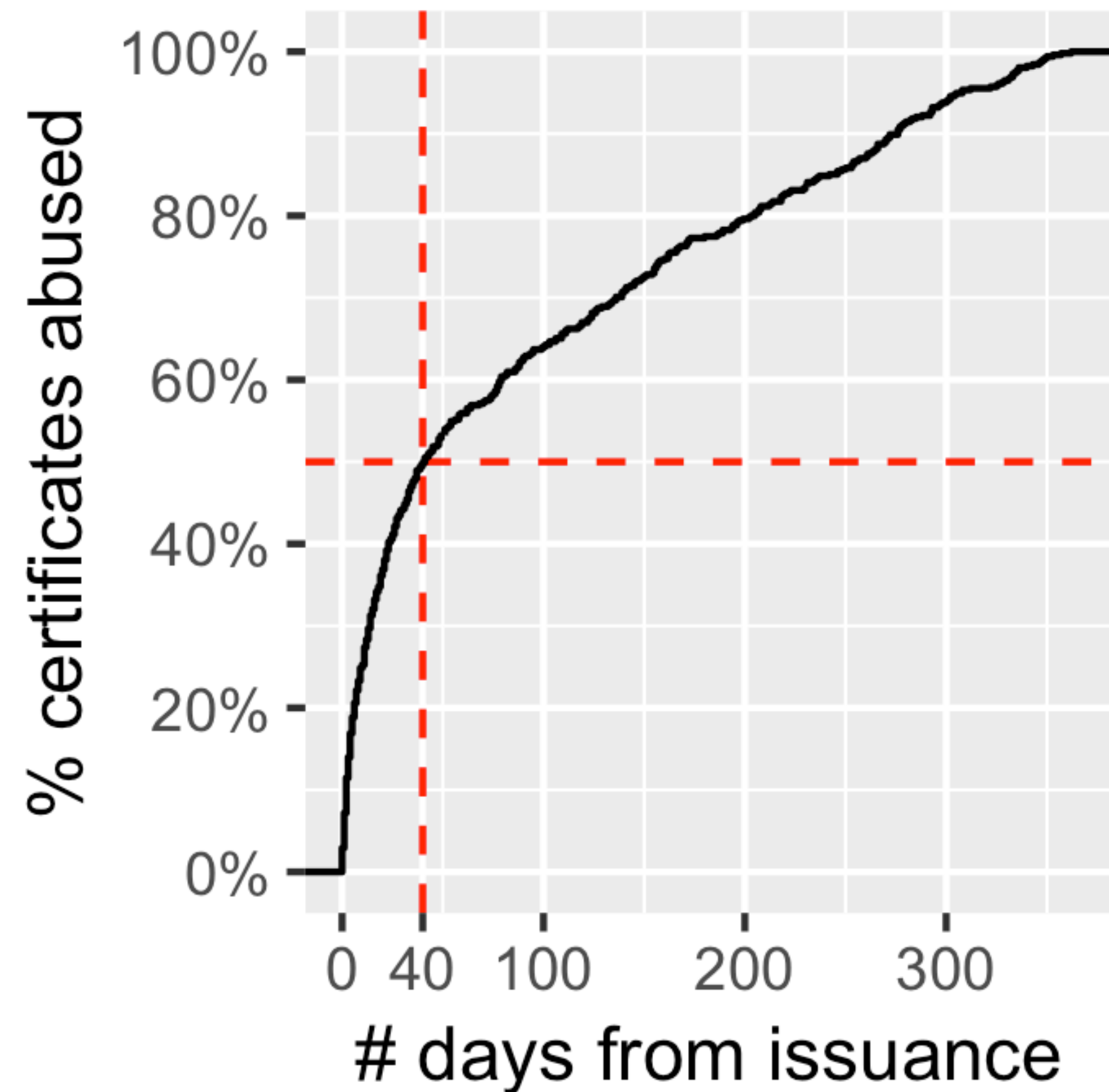
Are the certificates compromised or obtained from the CAs?

Prior methods [Kim et al., 2017] no longer usable

Idea: **Interval between issue date and abuse date**

- We compute an **upper bound**
- Assumption: Compromised certificates are uniformly likely to be stolen & abused during their lifetime

Certificate Origin: Issue to Abuse Interval



50% abused within the first 40 days

Certificates likely obtained from CAs directly

Not compromised from legitimate publishers

⇒ Contrary to previous reports

Sales Volumes: Evidence

Forums

Sales take place in private

Vouches & Stock updates provide limited insight

E-shop

3rd party payment component loaded on front-end

Providing the count of certificates on stock

Plus the date of stock updates, later used for linking the certificates

Sales Volumes: Estimate (E-shop)

Certificate	Regular (\$)	Black Market (\$)
Comodo	85	350
Thawte	300	600
EV (Comodo)	320	3,000

Duration	Revenue (\$)	Max. Profit (\$)
Month	4,600	2,850
Total	> 16.000	9,850

Observed sales

Sales of 41 non-EV certificates observed
EV certificates sold in private

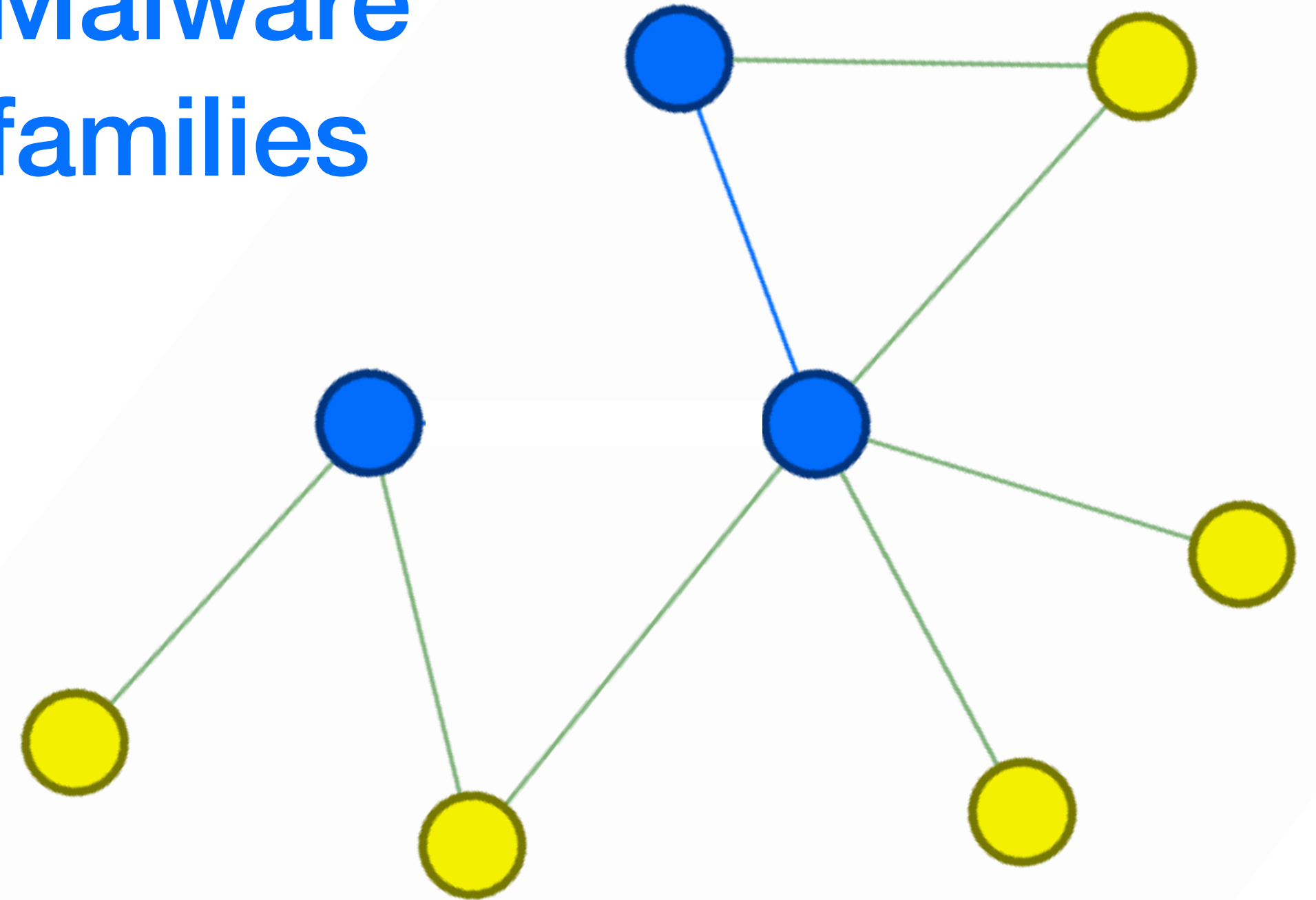
Vendors may incur additional costs for setting up fake identities etc.

Relationships

Certificate = a link

- between a publisher & a malware family
- between two malware families

Malware families



Publisher Identities

Major Component

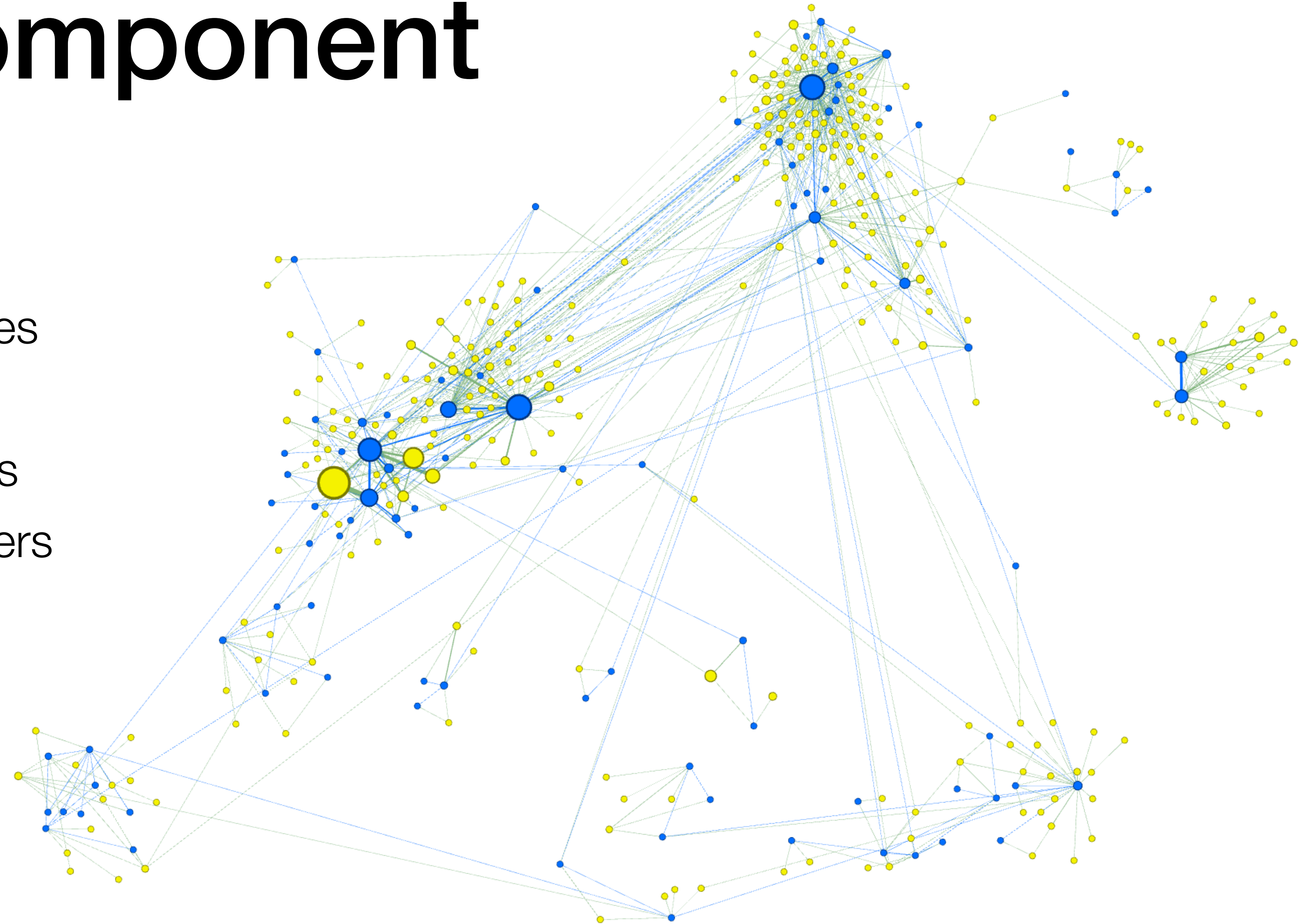
Contains

90% of malware samples

70% of certificates

50% of malware families

mostly Russian publishers



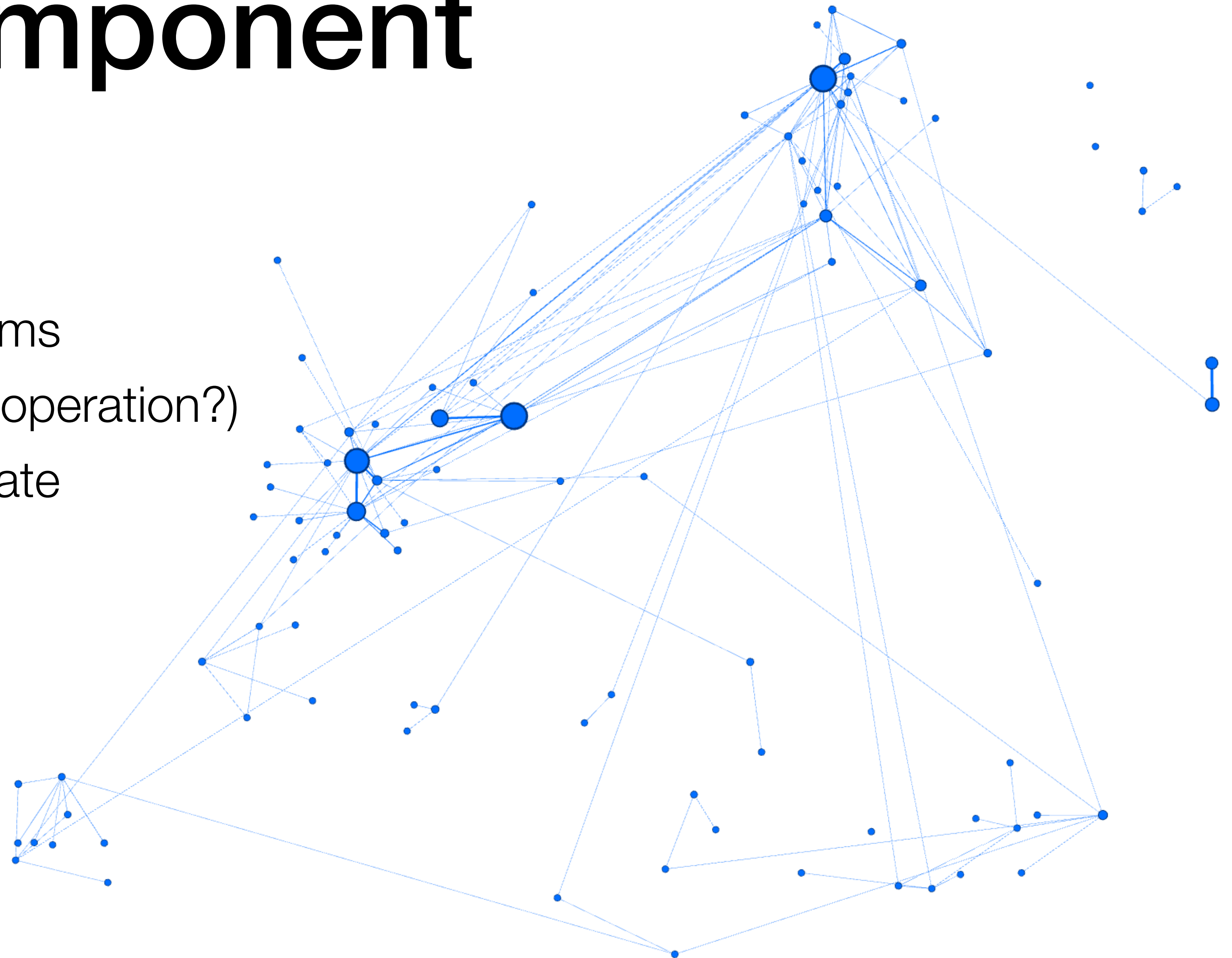
Major Component

Properties

Indicates smaller dev teams

Strong connectivity (= cooperation?)

Faster certificate abuse rate



Conclusions

Business model: Trading code signing certificates

Growing demand

Certificates appear to be obtained directly from CAs

Evidence consistent with a reliable supply of certificates

Market confidence, vendors able to respond to demand

Hypothesis: Use of shell or impersonated companies

Recommendation: Standardise the publisher name format

Data release: www.signedmalware.org

Publications

WEIS 2018

Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates

Kozák, K., Kwon, B. J., Kim, D., Dumitraş, T.

17th Annual Workshop on the Economics of Information Security (WEIS 2018)



The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI

Kim, D., Kwon, B. J., Kozák, K., Gates, Ch., Dumitraş, T.

27th USENIX Security Symposium (USENIX Security '18)

Thank you!

Kristián Kozák

kkozak@mail.muni.cz

signedmalware.org

Identifying Traded Certificates 1/2

Supply side: E-shop

Specified CA: **Thawte**

Claimed on a forum: **British publishers**

Observing stock: **Issue date**

Observed stock updates: occurred on **9 / 104** days

Assumptions

Vendor puts certificates in stock immediately

Vendor did not lie (about British publishers)

Identifying Traded Certificates 2/2

Matching criteria

Supply side: Thawte, British publisher, **9** potential issue dates

Demand side: Signed Malware Dataset

145 certificates issued during 104-day observation period

10 are by Thawte; 11 have a British publisher

5 are by Thawte & have a British publisher

All 5 match a potential issue date

Likelihood: If a cert is equally likely to be issued on any day ...

1 match by chance: $p = 9 / 104 = 8.7\%$

5 matches by chance: $p = (8.7\%)^5 = 0.0005\%$