

Detecting and preventing DNS abuse in .eu

Lieven Desmet, KU Leuven – lieven.desmet@cs.kuleuven.be

Malicious use of domain names

- › Domain names are often abused by cyber criminals
 - › Spam, botnet C&C infrastructure, phishing, malware, ...
- › To avoid blacklisting, malicious actors often deploy a hit-and-run strategy
 - › 60% are only active for 1 day after registration [Hao et al]

[Hao et al] "Understanding the Domain Registration Behavior of Spammers" IMC 2013

Research hypothesis:

“Malicious actors register domains in bulk, and do so for longer periods of time.”

The .eu trust strategy

› Delayed delegation

- ›› Predict at time of registration whether a domain name will be used abusively





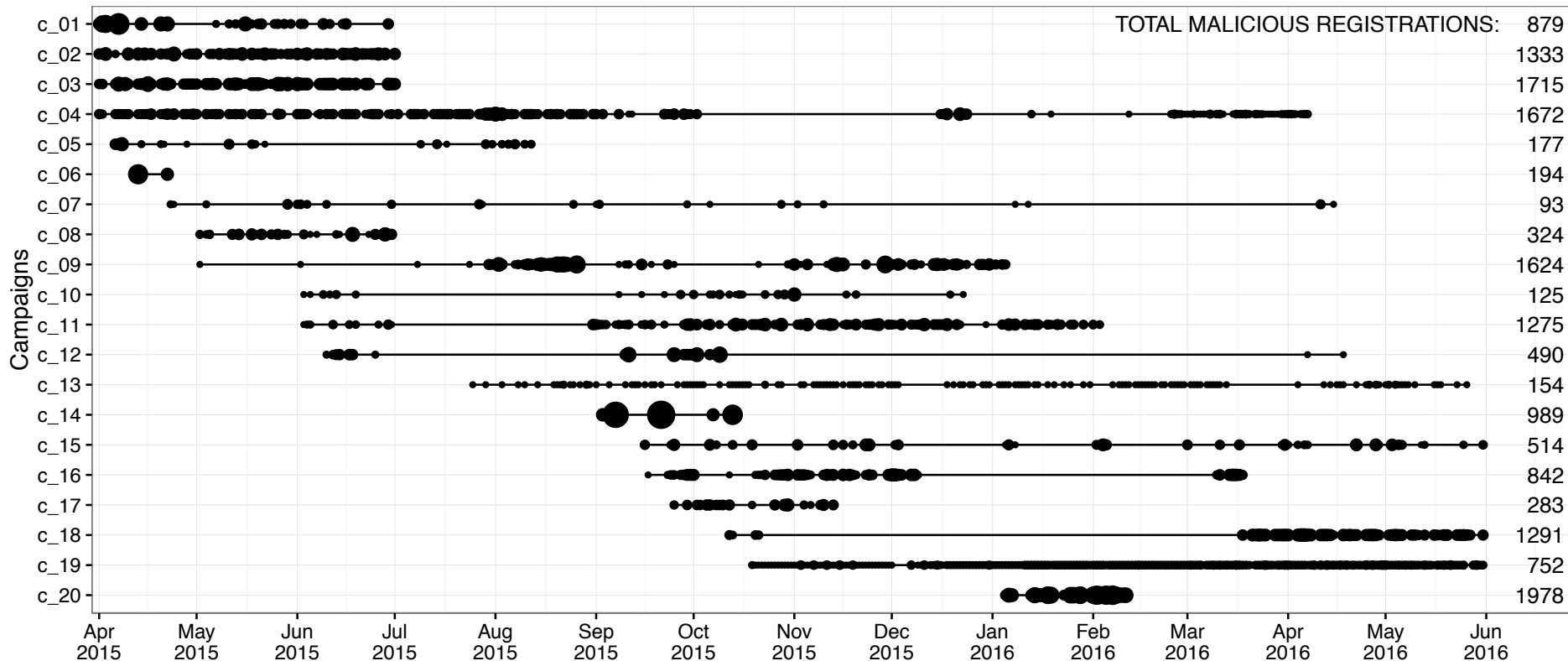
Insights in malicious domain registrations

*T. Vissers et al., **Exploring the ecosystem of malicious domain registrations in the .eu TLD**, Research in Attacks, Intrusions, and Defenses (RAID 2017), September 2017.*



Activity of identified campaigns

Registrations per day ● 100 ● 200 ● 300 ● 400



Insight 1: Varying campaign characteristics



- › Simple campaign (c_14)
- › Single (fake) registrant used throughout the campaign

- **41 days active**
- **989 blacklisted registrations**
(= 95.37%)

Example campaign (c_11)

› Multiple fake registrant details

›› Combinations of

- 2 email accounts,
- 3 phone numbers,
- 4 street addresses

- **8 months active**
- **1,275 blacklisted registrations**
(= 53.96%)

Example of an advanced campaign (c_15)

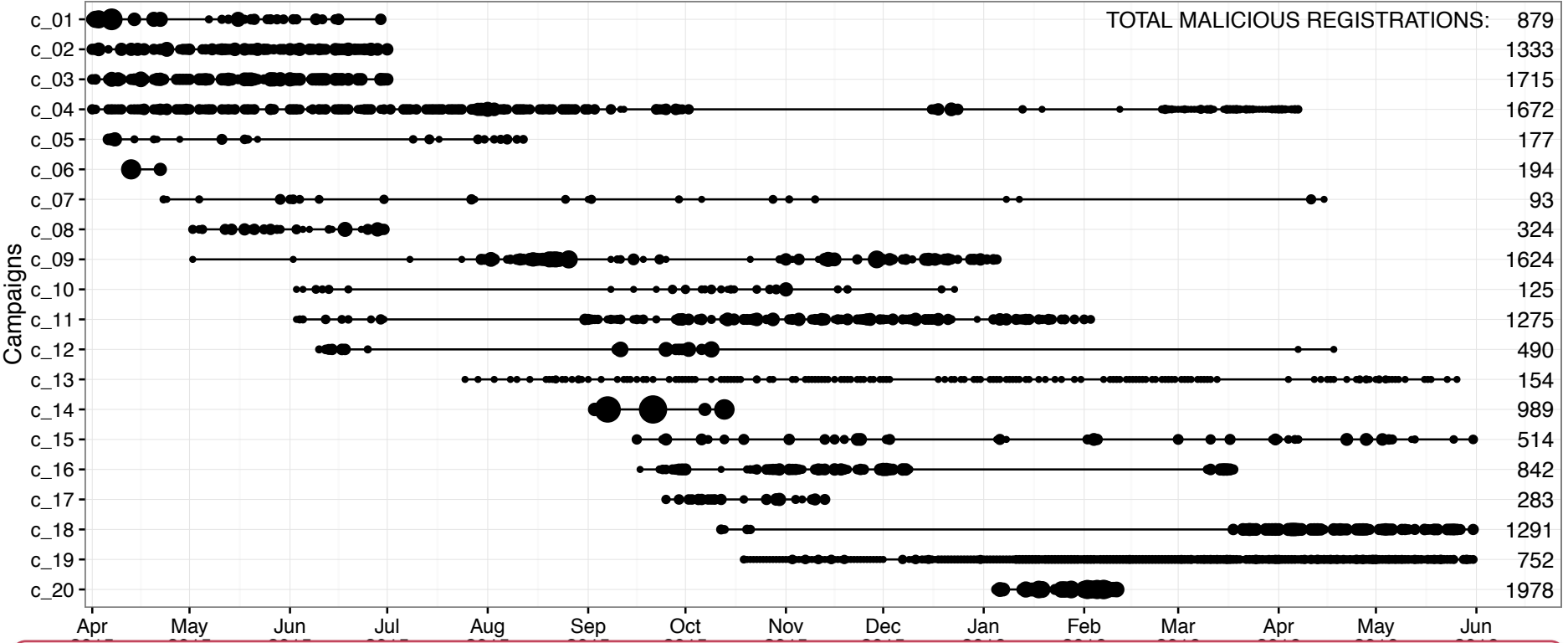
- › Registrant details:
 - › 98 fake registrants
 - › Generated by Laravel Faker tool
- › Domain names:
 - › Consist out of 2-3 Dutch words
 - › Dutch words are reused across registrants
- › Batches of 8, 16, 24 or 32 registrations

- **8+ months active**
- **514 blacklisted registrations**
(= 26.95%)

Insight 2: Small set of malicious actors



Registrations per day ● 100 ● 200 ● 300 ● 400



At most 20 actors represent 80% of malicious registrations

Insight 3: Top facilitators for malicious registrations

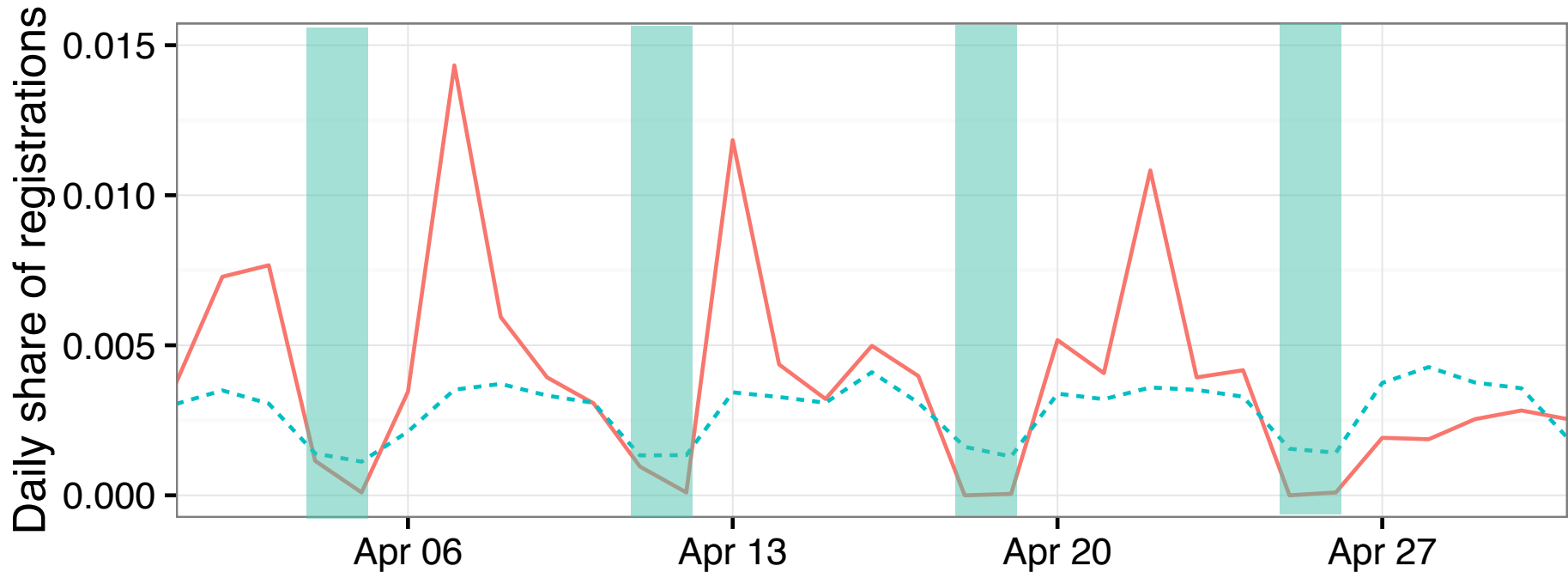


	Nb of malicious	Contribution Malicious	Benign	Toxicity
1. registrar_5	10,353	49.61%	2.27%	36.25%
2. registrar_3	3,004	14.39%	2.64%	12.41%
3. registrar_7	2,327	11.15%	0.46%	38.67%
1. gmail.com	4,221	20.23%	24.79%	2.08%
2. yahoo.com	3,348	16.04%	1.49%	21.85%
3. aol.com	2,134	10.23%	0.31%	46.28%

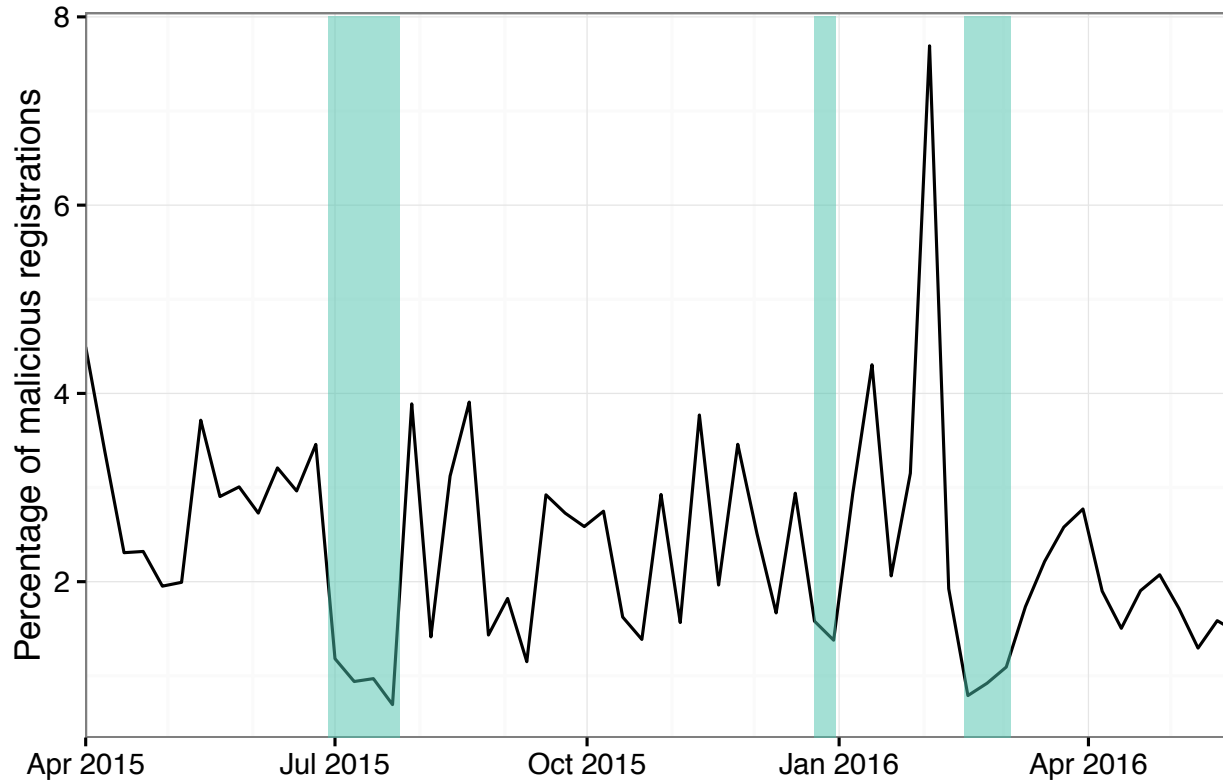
Insight 4: Some campaigns align with regular business activity patterns (1)



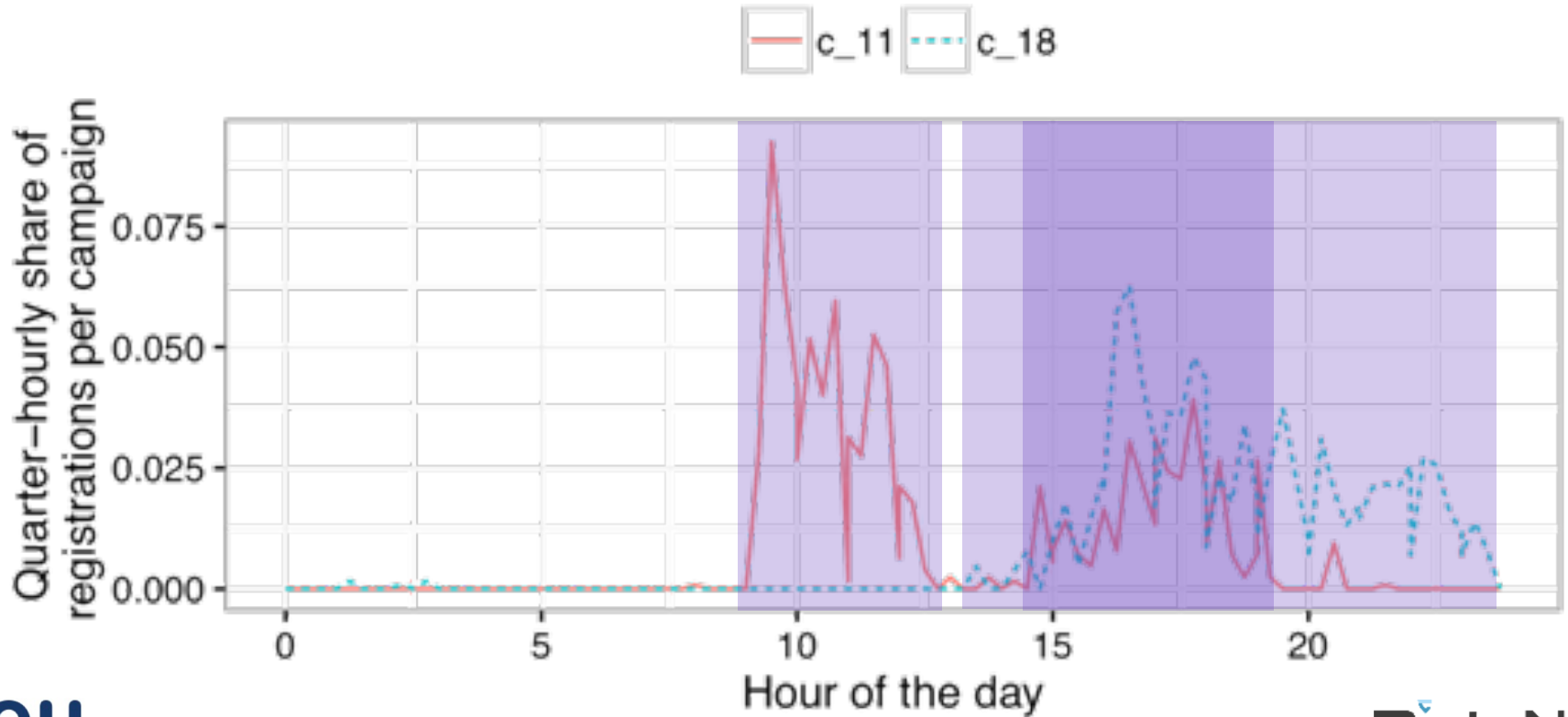
Malicious registrations All registrations



Insight 4: Some campaigns align with regular business activity patterns (2)



Insight 4: Some campaigns align with regular business activity patterns (3)





Registration-time prediction of malicious intent

J. Spooren et al., PREMADOMA: An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations, Annual Computer Security Applications Conference (ACSAC 2019), December 2019.



Pro-active detection and prevention

Previous registrations for which the results (abuse/no abuse) is known

Previous registrations

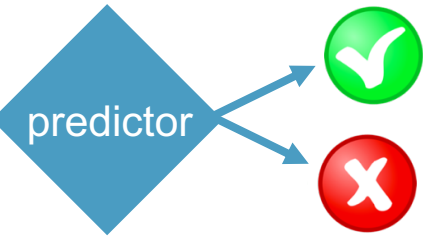


Prediction Model

- Domains with malicious intent can be
- Detected early
 - Delayed
 - Prevented from being registered

For each new registration, the system predicts if the domain will be used for malicious activity

New registration



Underlying assumptions/rationales for our predictors

- › Similarity-based agglomerative clustering
 - ›› Domains belonging to the same campaign have very similar registration details
- › Reputation-based classification
 - ›› Domains using registration facilitators with a bad reputation (e.g. email providers or registrars), are likely to be malicious as well

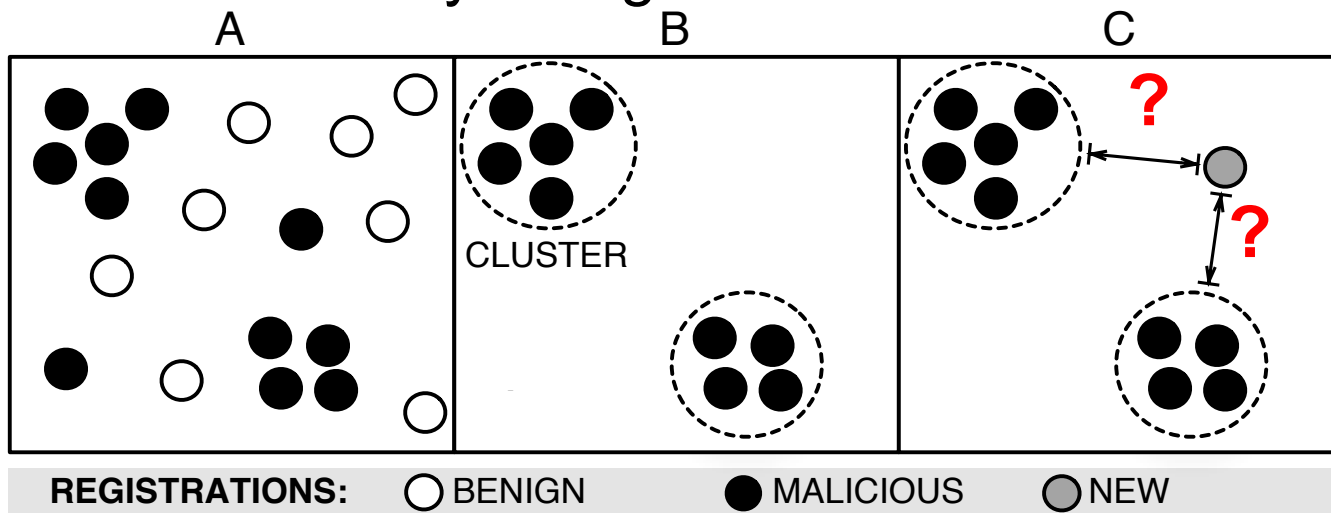
Predictor 1:

Reputation-based classification

- › Reputation features of “facilitators”
- › Facilitators:
 - ›› Technical facilitators: registrar, name servers
 - ›› Communication means: email provider and phone number
- › Reputation score:
 - ›› Represent contribution and toxicity of facilitator to malicious registrations

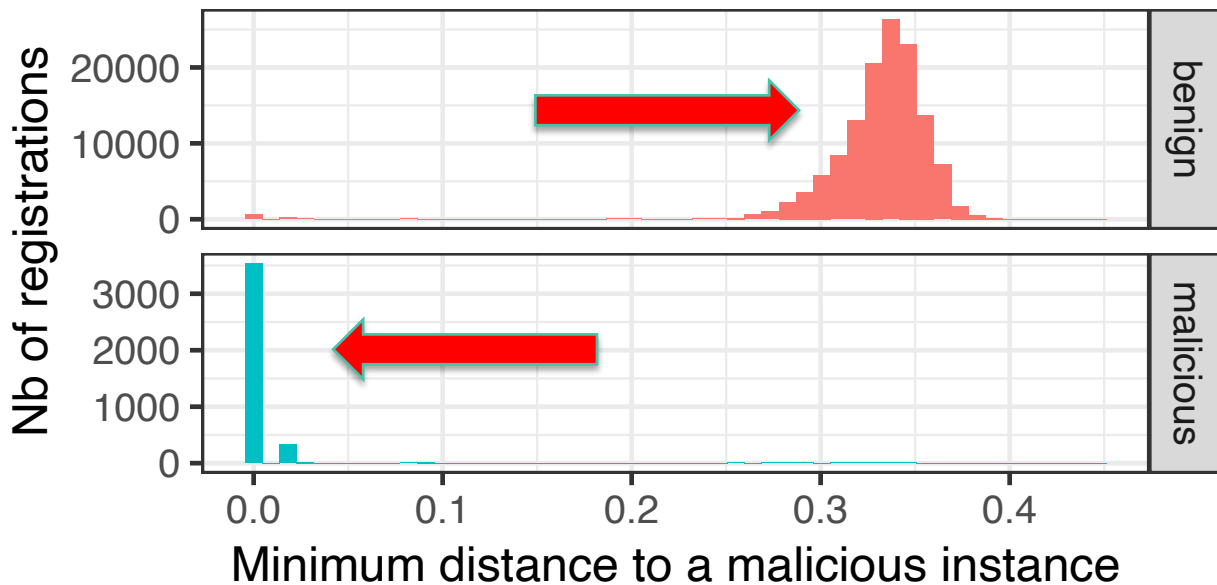
Predictor 2: Similarity-based clustering

- › Agglomerative clustering of malicious samples
- › Based on the similarity of registration data



Can we differentiate between benign and malicious samples?

- › Closest distance of a registration to malicious domain

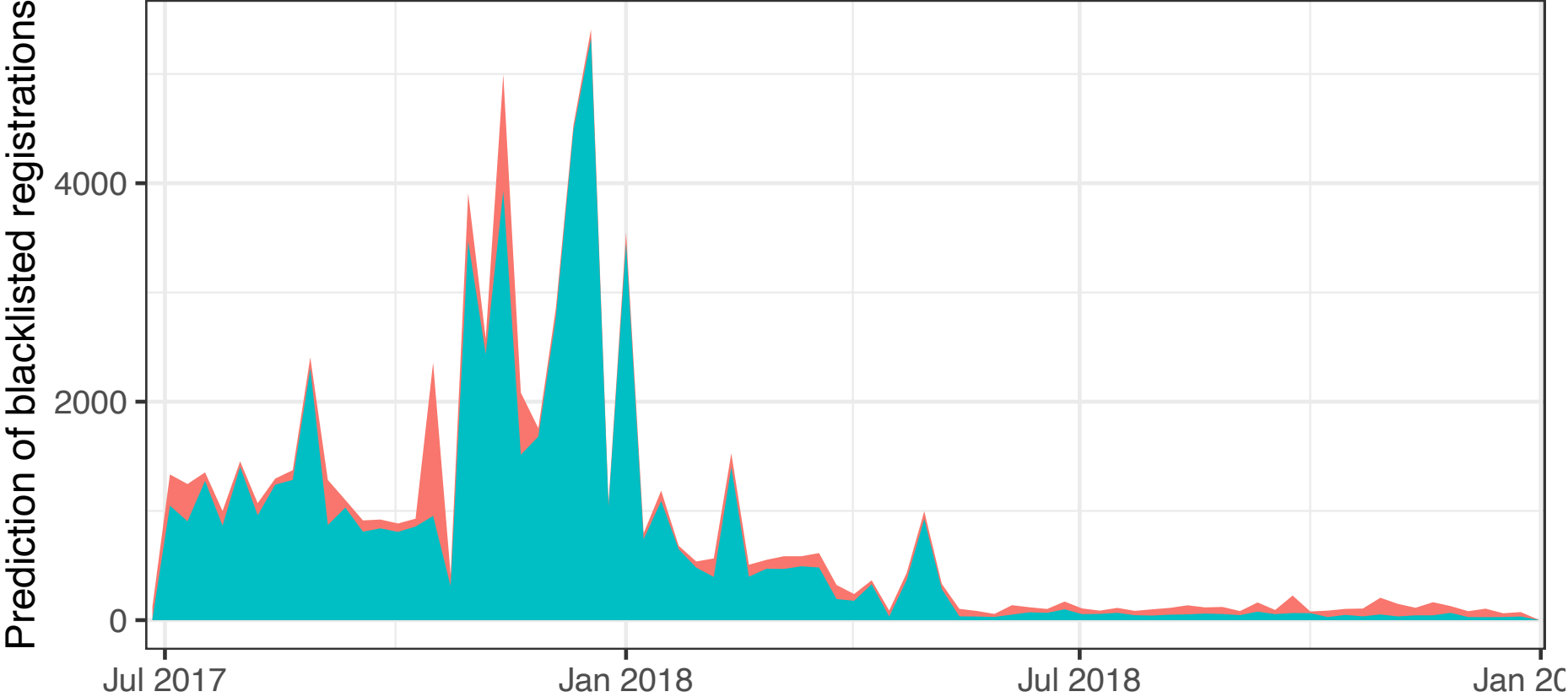


Evaluation on historical data

- › Ground truth-based evaluation
 - › Recall: 66.23%
 - › Precision: 84.57
 - › False positive rate: 0.30%

- › Campaign-based evaluation
 - › 17 out of the 20 campaigns are well predicted

Detecting and preventing abuse in .eu: “1 picture ...”



Over 25 000 domain names suspended with ties to identity fraud

[Tweet](#)[← Back to the news page](#)

On 29 January 2018, EURid suspended 25 000 domain names with ties to identity fraud.

With actions as such, our focus is on the safety of online consumers. Via close collaborative efforts with law enforcement, both on a national and international level, as well as with our registrar channel, we are working to predict at the time of registration whether or not a domain name might be used in an abusive way in an effort to prevent such malicious domain names from becoming active in the first place. "With our trust & security program, we are monitoring our domain names for potential abuse, leading to 25 000 domain name suspensions thus far in 2018," said Geo Van Langenhove, EURid Legal Manager.

In 2017, we suspended 20 126 abusive domain names, compared to 20 126 abusive domain names suspended in 2017.

Over 11 000 abusive domain names suspended

[Tweet](#)[← Back to the news page](#)

On 21 June 2018, EURid suspended 11 760 domain names that were registered with non-eligible registration data, of which some have been reported for abuse.

With actions as such, our focus is on the safety of online consumers. Via close collaborative efforts with law enforcement, both on a national and international level, as well as with our registrar channel, we are working to predict at the time of registration whether or not a domain name might be used in an abusive way in an effort to prevent such malicious domain names from becoming active in the first place. "With our trust & security program, we are monitoring our domain names for potential abuse, leading to 11 760 domain name suspensions thus far in 2018," said Geo Van Langenhove, EURid Legal Manager.

In 2017, we suspended 20 126 abusive domain names, compared to 20 126 abusive domain names suspended in 2017.

Learn more about the ways we're building a trustworthy .eu and .euo domain name space at trust.eurid.eu.

Learn more about the ways we're building a trustworthy .eu and .euo domain name space at trust.eurid.eu.



Predictive Algorithms

Through the use of historical data and self-learning algorithms, we are working to predict at the time of registration whether or not a domain name might be used in an abusive way in an effort to prevent such malicious domain names from becoming active in the first place.

As part of the EURid's Trust & Security program, 58,966 domains were suspended in 2018.

Operational results

- › Period: July 2017 – December 2018 (18 months)
 - › Recall: 85.51%
 - › Precision: 72.04%
 - › False positive rate: 2.86%
- › Very big campaigns (October 2017 - March 2018)
- › Incomplete ground truth

Abstract—This paper analyzes the effectiveness of domain blacklisting against malicious DNS registrations. We evaluate the impact of domain blacklisting on the registration of malicious domains and the impact of domain blacklisting on the registration of malicious domains. We evaluate the impact of domain blacklisting on the registration of malicious domains and the impact of domain blacklisting on the registration of malicious domains. We evaluate the impact of domain blacklisting on the registration of malicious domains and the impact of domain blacklisting on the registration of malicious domains.

The main findings of this paper are: 1) The effectiveness of domain blacklisting is highly dependent on the type of malicious domain. 2) The effectiveness of domain blacklisting is highly dependent on the type of malicious domain. 3) The effectiveness of domain blacklisting is highly dependent on the type of malicious domain.

Ground truth analysis

T. Vissers et al., Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations, IEEE Workshop on Traffic Measurements for Cybersecurity (WTMC 2019), May 2019.



Sources of ground truth



Google Safe Browsing



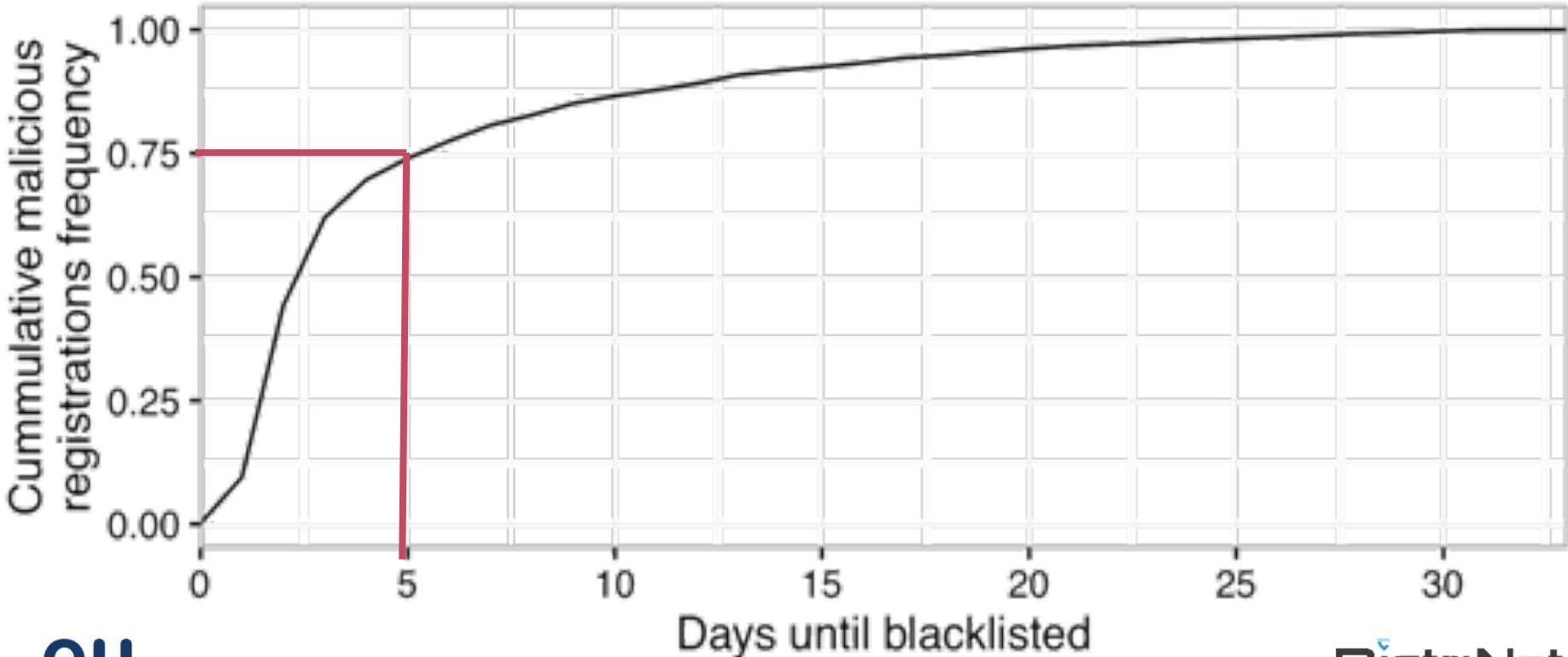
- › Around 60K domains to check per day
- › Simplified view: once on a abuse list, always considered malicious

Types of abuse recorded

- › Majority of abuses are related to spam (93.68%)
- › Different coverage statistics per abuse list for .eu:
 - › Spamhaus DBL: 81.07%
 - › SURBL multi list: 50.04%
 - › Google Safe Browsing: 1.81%


Registration period: Apr 2015 – May 2016

Delay of the ground truth



Incompleteness of the blacklists

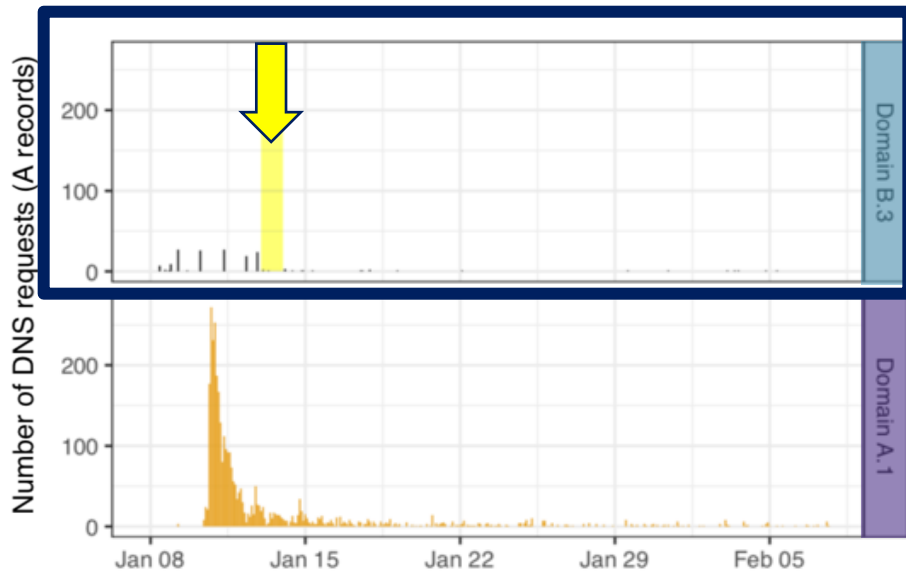
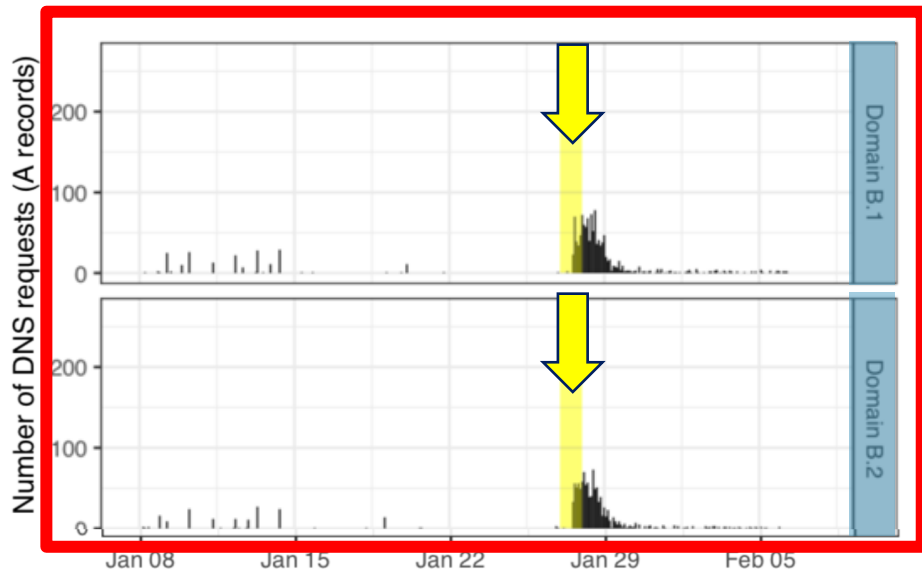
- › Failed to detect?
- › Never active/malicious?



	Active	Dormant
Blacklisted	Blocked	Pro-actively blocked
Non-blacklisted	Missed	Unused

Campaign related activity

- › E.g. spam triggers multiple DNS requests:
 - ›› SPF, DMARC, DKIM, MX, A

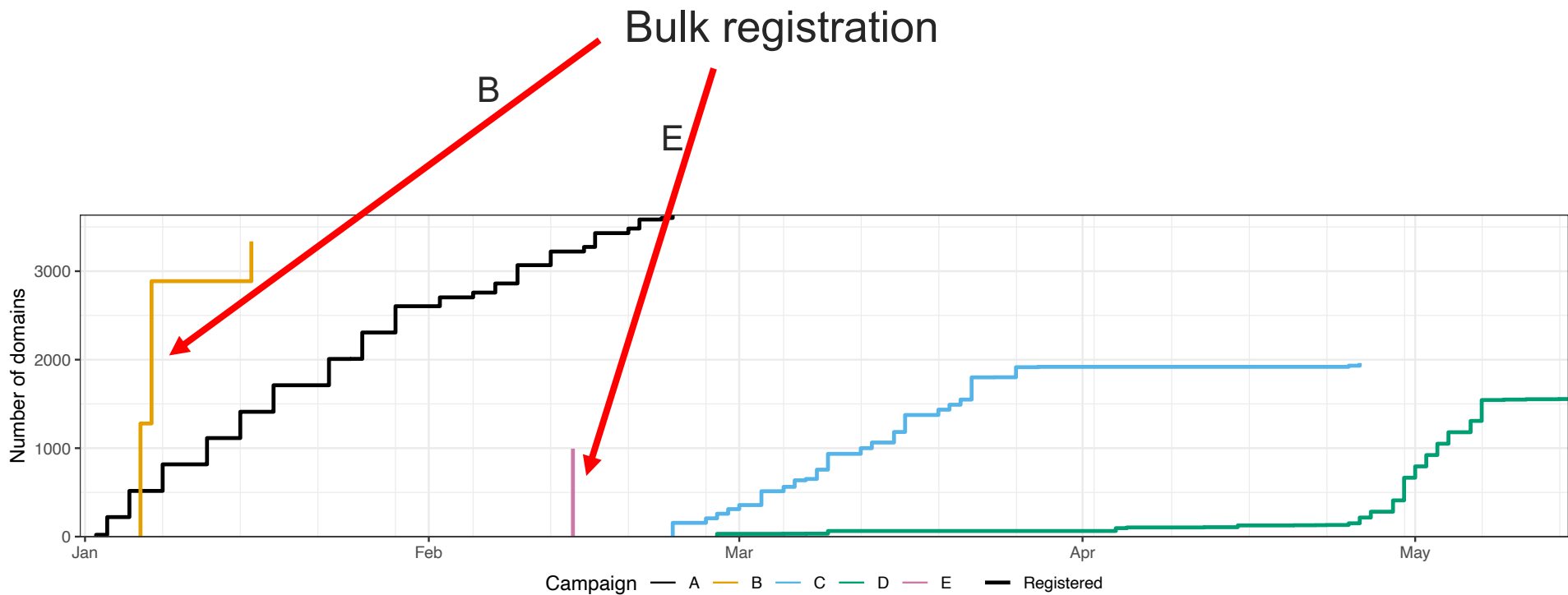


Active vs Dormant – Blacklisted vs Non-blacklisted

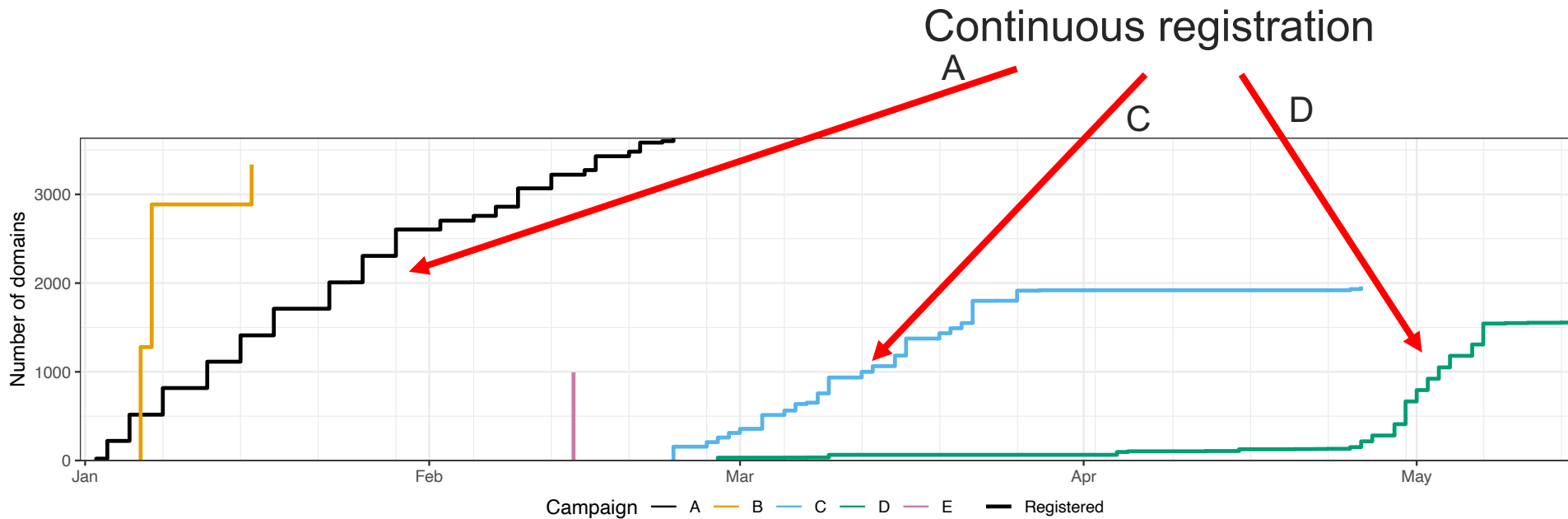
- › 5 largest campaigns in .eu (Q1-Q2 2018)
- › Based on passively-logged DNS requests (.eu TLD server)

	Active	Dormant
Blacklisted	Blocked 54.8%	Proactive 2.9%
Non-blacklisted	Missed 14.1%	Unused 14.0%

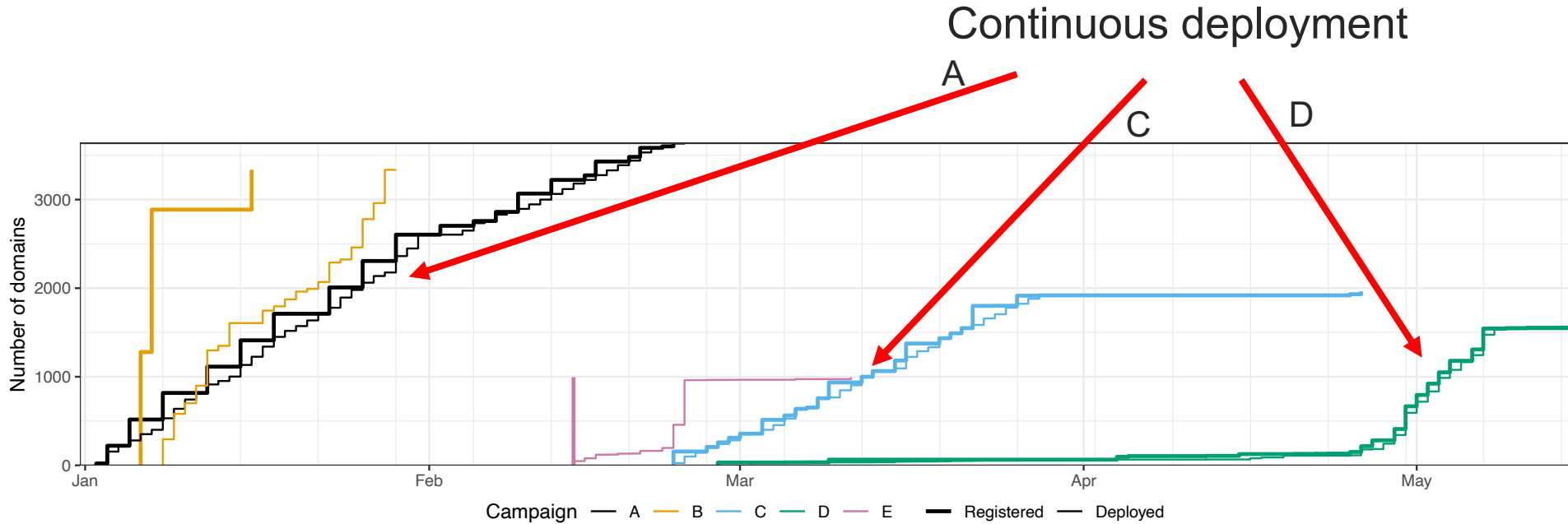
1. Registration strategy



1. Registration strategy

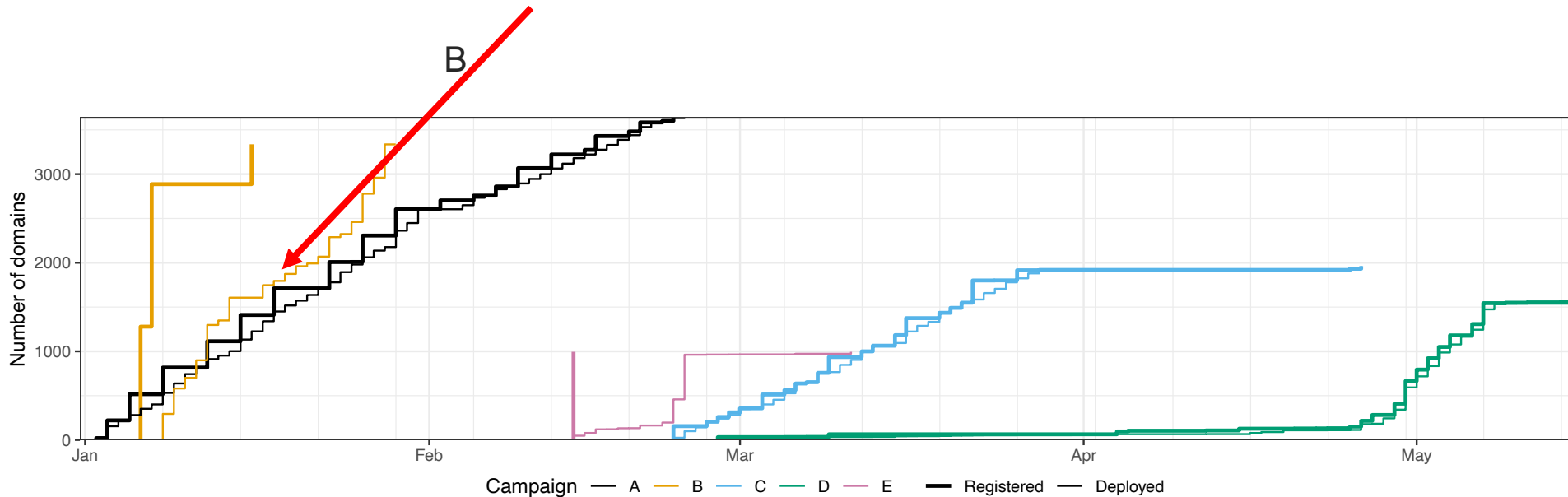


2. Deployment strategy (thin line)



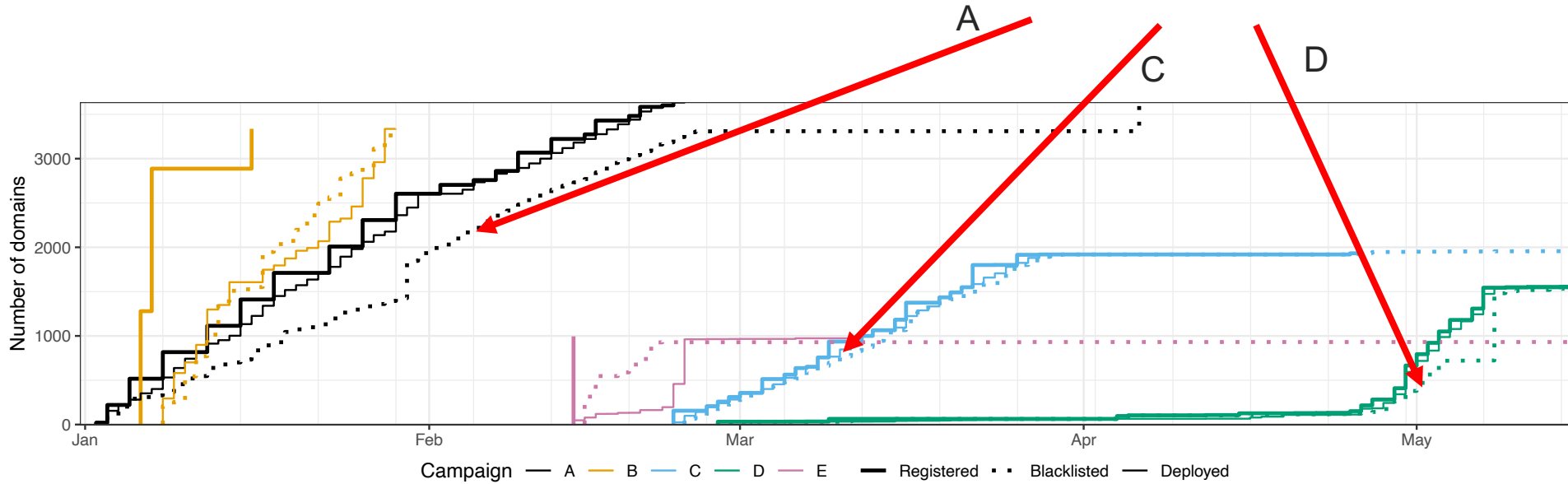
2. Deployment strategy (thin line)

Gradual deployment,
although registered in bulk

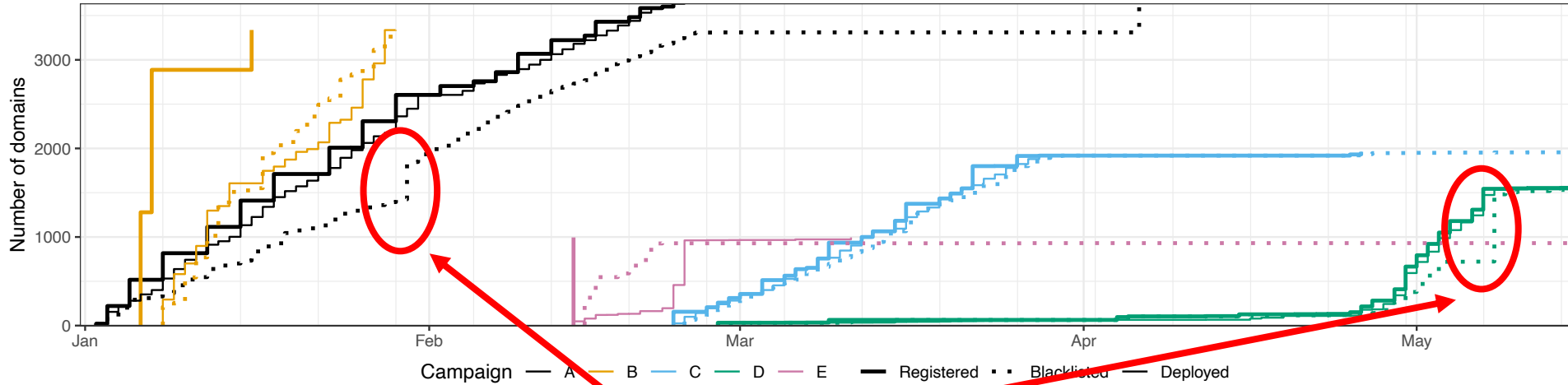


3. Domain blacklisting (dotted line)

Reactive blacklisting



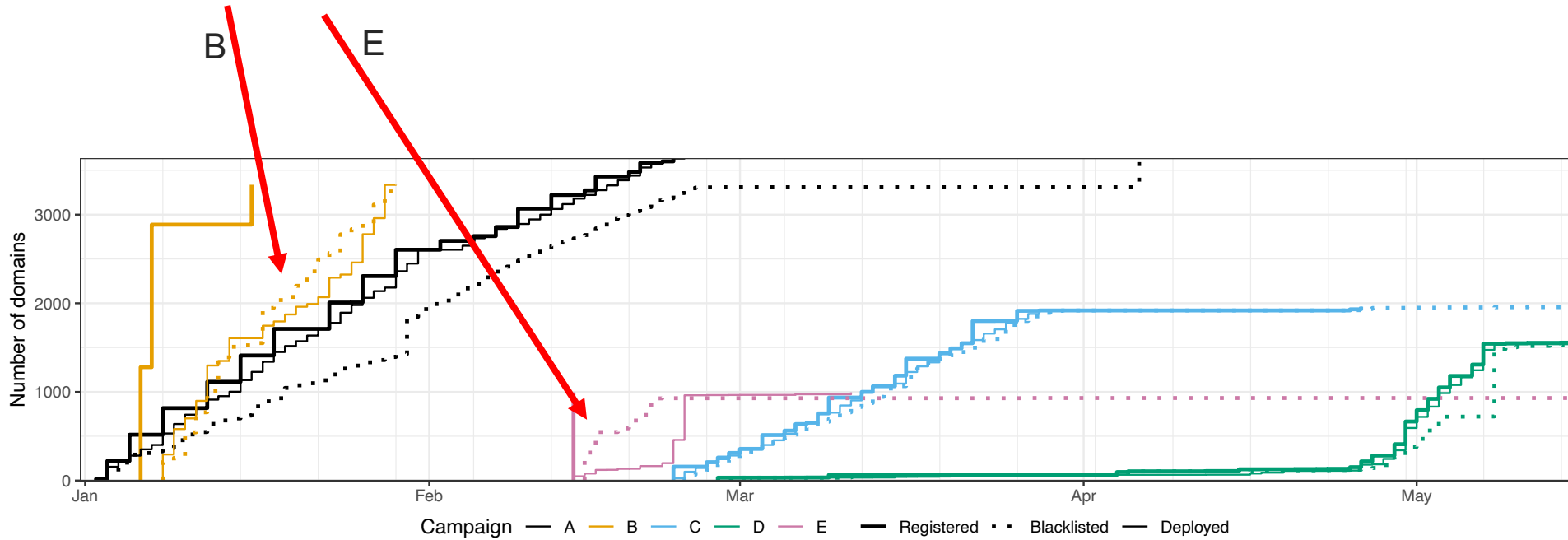
3. Domain blacklisting (dotted line)



Blacklisting in batch

3. Domain blacklisting (dotted line)

Pro-active blacklisting



Key takeaways

Rather small set of bad actors

- › Up to 20 campaigns are responsible for 80% of malicious registrations

- › Top facilitators:
 - ›› About half of the malicious registrations via 1 registrar
 - ›› 1 public email provider are malicious with a high toxicity

Registration-time detection and prevention

- › Two prediction models predict at registration-time the malicious intent
- › Captures the majority of malicious domain registrations
- › Incompleteness of ground truth makes analysis hard
- › Interesting to see how this will further impact the security landscape

Attackers vs Defenders

- › Ground truth is (somewhat) tricky
 - ›› Bias towards spam
 - ›› Delay in labeling
 - ›› “Incompleteness”
- › 2 different ecosystems:
 - ›› abusive registration
 - ›› abusive activity
- › Interesting to see how it will further impact the abuse landscape

Interested in more? Some reading material...

Exploring the ecosystem of malicious domain registrations in the .eu TLD

Thomas Vissers*, Jan Spooens*, Peter Agius*, Dirk Janssens*, Peter Janssens*, Marc Van Winsume*, Frank Peeters*, Wouter Joosen*, and Liesem Dierckx*

* KU Leuven, Belgium
† Ghent University, Belgium
‡ Ghent University, Belgium

Abstract. This study extensively examines 11 months of registration data that identify large-scale malicious campaign presence in the .eu TLD. We explore the ecosystem and machine-generated domain creation patterns that increasingly require large amounts of domains for cyber-attacks, malware use. Although these malicious domains are short-lived, they are not necessarily registered and monitored, we establish that at least 80% of the domains can be traced back to operational agencies, law enforcement, and security. We further report on insights in the operational agencies that increase and observe, amongst other findings, that these provisions can only partially attenuate the harm. We apply a granular domain categorization to validate the campaign identification patterns and to estimate the acceptance and analysis of malicious registrations in a TLD zone.

Keywords: malicious domain names, campaigns, DNS records

1 Introduction

The Domain Name System (DNS) is one of the key technologies that has allowed the web to expand to its current dimensions. Virtually all communications on the web require the resolution of domain names to IP addresses. Malicious actors use misconfigurations, and also increasingly deploy spams, phishing, domain names to execute their abusive operations. For instance, phishing attacks, the resulting spam results, bot networks and controlled (C&C) connections and malware distribution. These activities usually require domain names to operate.

Widespread domain blacklisting are required and used to stop malicious domain names directly after abusive activities have been observed and reported. As a consequence, attackers changed to a list-and-run strategy, in which malicious domain names are registered and used for a short period of time. This domain names

registration is just for a single day in 95% of the cases [1]. These domain names

are used to register malicious domain names whenever we refer to a domain name that is registered for less than 24 hours.

* This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

† This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

‡ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

The final publication is available at Springer via <https://doi.org/10.1007/978-3-03-023222-1>

Detection of Algorithmically Generated Domain Names used by Botnets: A Dual Arms Race.

Jan Spooens
Dierckx KU Leuven
Herlev, Belgium
jan.spooens@kuleuven.be

Davy Prevensier
Herlev, Belgium
davy.prevensier@kuleuven.be

Liesem Dierckx
Herlev, Belgium
liesem.dierckx@kuleuven.be

Peter Janssens
Herlev, Belgium
Peter.janssens@kuleuven.be

Wouter Joosen
Herlev, Belgium
wouter.joosen@kuleuven.be

ABSTRACT

Malware typically uses Domain Generation Algorithms (DGAs) as a technique to contact their Command and Control servers. In recent years, different approaches to automatically detect generated domain names have been proposed, based on machine learning. The first problem in this address is to identify and automatically compare these DGA detection algorithms due to the lack of a standard benchmark. The second problem then investigates the difficulty for an adversary to circumvent these classifiers when the machine learning based using these DGA datasets are known. In this paper we compare two different approaches on the state-of-the-art DGA detection machine learning using manually generated botnets and a long running, automatic botnet network. We show that the deep learning approach performs consistently better on all of the benchmark datasets, with an average classification accuracy of 98.7% versus 93.8% for the manually generated botnets. We also show that one of the dangers of manual feature engineering is that DGAs can adapt their strategy based on knowledge of the botnets used to detect them. To demonstrate this, we use the knowledge of the used botnets set to design a new DGA which makes the random forest classifier previous tests a classification accuracy of 95.9%.

The deep learning classifier is also (almost) less affected, reducing its accuracy to 94.7%.

Keywords: botnets, domain generation algorithms, machine learning

CCS CONCEPTS

Security and privacy → Malware and its mitigation; Computing applications → Network and network classification and organization

KEYWORDS

Malware Detection, Domain Generation Algorithms, Machine Learning

1 Introduction

The Domain Name System (DNS) is one of the key technologies that has allowed the web to expand to its current dimensions. Virtually all communications on the web require the resolution of domain names to IP addresses. Malicious actors use misconfigurations, and also increasingly deploy spams, phishing, domain names to execute their abusive operations. For instance, phishing attacks, the resulting spam results, bot networks and controlled (C&C) connections and malware distribution. These activities usually require domain names to operate.

Widespread domain blacklisting are required and used to stop malicious domain names directly after abusive activities have been observed and reported. As a consequence, attackers changed to a list-and-run strategy, in which malicious domain names are registered and used for a short period of time. This domain names registration is just for a single day in 95% of the cases [1]. These domain names

are used to register malicious domain names whenever we refer to a domain name that is registered for less than 24 hours.

* This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

† This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

‡ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

§ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

¶ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

|| This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊞ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊠ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊡ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊣ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊥ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊦ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊧ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊨ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊩ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊪ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊫ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊬ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊭ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊮ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊯ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊰ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊱ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊲ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

⊳ This work is partially supported by the Ghent University research project 'The Role of the Internet in the Security of the European Union'.

Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations

Thomas Vissers*, Peter Janssens*, Wouter Joosen*, Liesem Dierckx*

* KU Leuven, Belgium
† Ghent University, Belgium

Abstract. Blacklists are widely used in security research. However, there is little insight into how they operate, what their main focus is, and how effective they are. In this paper, we combine DNS traffic measurements with domain registration and blacklisting data. We aim to assess and report to what extent researchers can extrapolate on existing blacklisting studies. We focus on large-scale malware campaigns that register thousands of domain names used in cyber-attacks to evaluate the situation. We show that blacklisting operates on both reactive, and to a lesser extent, proactive detection methods. Furthermore, by examining behavioral aspects of these malware domains, we can pinpoint when blacklisting fails to counter domain campaigns.

INTRODUCTION

The Internet consists billions of devices, ranging from servers and personal computers to tablets, mobile phones, broadcasted applications, and many more. Malicious actors can compromise the behavior of vulnerable devices which could be compromised, or even tricking users into unknowingly installing malware on their devices. One such malware is present on a machine, it can be used to attack other machines, used as a launching point for a denial of service, or communications, and e-mail addresses, except the contents of the malware originating from the same is essential for the ability to decrypt and many more malicious activities. Large pools [1] of infected machines, called botnets [2] exist, which are controlled from Command and Control (C&C) servers (as depicted in Figure 1).

In our previous study, we extensively analyzed the occurrence of malware registrations within [3]. We found that the vast majority of blacklisted registrations could be attributed to a small set of cybercriminal networks. We found that these cybercriminals consistently set up large-scale campaigns, probing thousands of domain names used in cyber attacks. An important finding of this study is that a substantial amount of campaign registrations were never actively used to attack. Alternatively, blacklisting might simply fail to detect some malware behavior. At this time, there is no clear understanding of this discrepancy, in part because blacklisting methods are somewhat opaque, as they typically combine multiple tactics to achieve detection. However, the security community broadly agrees that blacklisting and other threats are not enough. For example, many detection and prevention systems are ineffective against threats that prevent traffic for maliciousness (e.g., [4], [5], [6]). Furthermore, the understanding of cybercriminal ecosystems relies on malware usage blacklists as a main indicator of malice (e.g., [7], [8]).

The goal of this paper is to assess the effectiveness of domain blacklisting as a main indicator of malice (e.g., [7], [8]).

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

By identifying the first used active campaigns present in our dataset.

PREMADDA: An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations

Thomas Vissers*, Peter Janssens*, Wouter Joosen*, Liesem Dierckx*

* KU Leuven, Belgium
† Ghent University, Belgium

‡ Ghent University, Belgium

§ Ghent University, Belgium

|| Ghent University, Belgium

⊞ Ghent University, Belgium

⊠ Ghent University, Belgium

⊡ Ghent University, Belgium

⊣ Ghent University, Belgium

⊥ Ghent University, Belgium

⊦ Ghent University, Belgium

⊧ Ghent University, Belgium

⊨ Ghent University, Belgium

⊩ Ghent University, Belgium

⊪ Ghent University, Belgium

⊫ Ghent University, Belgium

⊬ Ghent University, Belgium

⊭ Ghent University, Belgium

⊮ Ghent University, Belgium

⊯ Ghent University, Belgium

⊰ Ghent University, Belgium

⊱ Ghent University, Belgium

⊲ Ghent University, Belgium

⊳ Ghent University, Belgium

⊴ Ghent University, Belgium

⊵ Ghent University, Belgium

⊶ Ghent University, Belgium

⊷ Ghent University, Belgium

⊸ Ghent University, Belgium

⊹ Ghent University, Belgium

⊺ Ghent University, Belgium

⊻ Ghent University, Belgium

⊼ Ghent University, Belgium

⊽ Ghent University, Belgium

⊾ Ghent University, Belgium

⊿ Ghent University, Belgium

⊠ Ghent University, Belgium

⊡ Ghent University, Belgium

⊣ Ghent University, Belgium

⊥ Ghent University, Belgium

⊦ Ghent University, Belgium

⊧ Ghent University, Belgium

⊨ Ghent University, Belgium

⊩ Ghent University, Belgium

⊪ Ghent University, Belgium

⊫ Ghent University, Belgium

⊬ Ghent University, Belgium

⊭ Ghent University, Belgium

⊮ Ghent University, Belgium

⊯ Ghent University, Belgium

⊰ Ghent University, Belgium

⊱ Ghent University, Belgium

⊲ Ghent University, Belgium

⊳ Ghent University, Belgium

⊴ Ghent University, Belgium

⊵ Ghent University, Belgium

⊶ Ghent University, Belgium

⊷ Ghent University, Belgium

⊸ Ghent University, Belgium

⊹ Ghent University, Belgium

⊺ Ghent University, Belgium

⊻ Ghent University, Belgium

⊼ Ghent University, Belgium

⊽ Ghent University, Belgium

⊾ Ghent University, Belgium

⊿ Ghent University, Belgium

⊠ Ghent University, Belgium

⊡ Ghent University, Belgium

⊣ Ghent University, Belgium

⊥ Ghent University, Belgium

⊦ Ghent University, Belgium

⊧ Ghent University, Belgium

⊨ Ghent University, Belgium

⊩ Ghent University, Belgium

⊪ Ghent University, Belgium

⊫ Ghent University, Belgium

⊬ Ghent University, Belgium

⊭ Ghent University, Belgium

⊮ Ghent University, Belgium

⊯ Ghent University, Belgium

⊰ Ghent University, Belgium

⊱ Ghent University, Belgium

⊲ Ghent University, Belgium

⊳ Ghent University, Belgium

⊴ Ghent University, Belgium

⊵ Ghent University, Belgium

⊶ Ghent University, Belgium

⊷ Ghent University, Belgium

⊸ Ghent University, Belgium

⊹ Ghent University, Belgium

⊺ Ghent University, Belgium

⊻ Ghent University, Belgium

⊼ Ghent University, Belgium

⊽ Ghent University, Belgium

⊾ Ghent University, Belgium

⊿ Ghent University, Belgium

⊠ Ghent University, Belgium

⊡ Ghent University, Belgium

⊣ Ghent University, Belgium

⊥ Ghent University, Belgium

⊦ Ghent University, Belgium

⊧ Ghent University, Belgium

⊨ Ghent University, Belgium

⊩ Ghent University, Belgium

⊪ Ghent University, Belgium

⊫ Ghent University, Belgium

⊬ Ghent University, Belgium

⊭ Ghent University, Belgium

⊮ Ghent University, Belgium

⊯ Ghent University, Belgium

⊰ Ghent University, Belgium

⊱ Ghent University, Belgium

⊲ Ghent University, Belgium

⊳ Ghent University, Belgium

⊴ Ghent University, Belgium

⊵ Ghent University, Belgium

⊶ Ghent University, Belgium

⊷ Ghent University, Belgium

⊸ Ghent University, Belgium

⊹ Ghent University, Belgium

⊺ Ghent University, Belgium

⊻ Ghent University, Belgium

⊼ Ghent University, Belgium

⊽ Ghent University, Belgium

⊾ Ghent University, Belgium

⊿ Ghent University, Belgium

⊠ Ghent University, Belgium

⊡ Ghent University, Belgium

⊣ Ghent University, Belgium

⊥ Ghent University, Belgium

⊦ Ghent University, Belgium

⊧ Ghent University, Belgium

⊨ Ghent University, Belgium

⊩ Ghent University, Belgium

⊪ Ghent University, Belgium

⊫ Ghent University, Belgium

⊬ Ghent University, Belgium

⊭ Ghent University, Belgium

⊮ Ghent University, Belgium

⊯ Ghent University, Belgium

⊰ Ghent University, Belgium

⊱ Ghent University, Belgium

⊲ Ghent University, Belgium

Detecting and preventing DNS abuse in .eu

Lieven Desmet, KU Leuven – lieven.desmet@cs.kuleuven.be