

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]

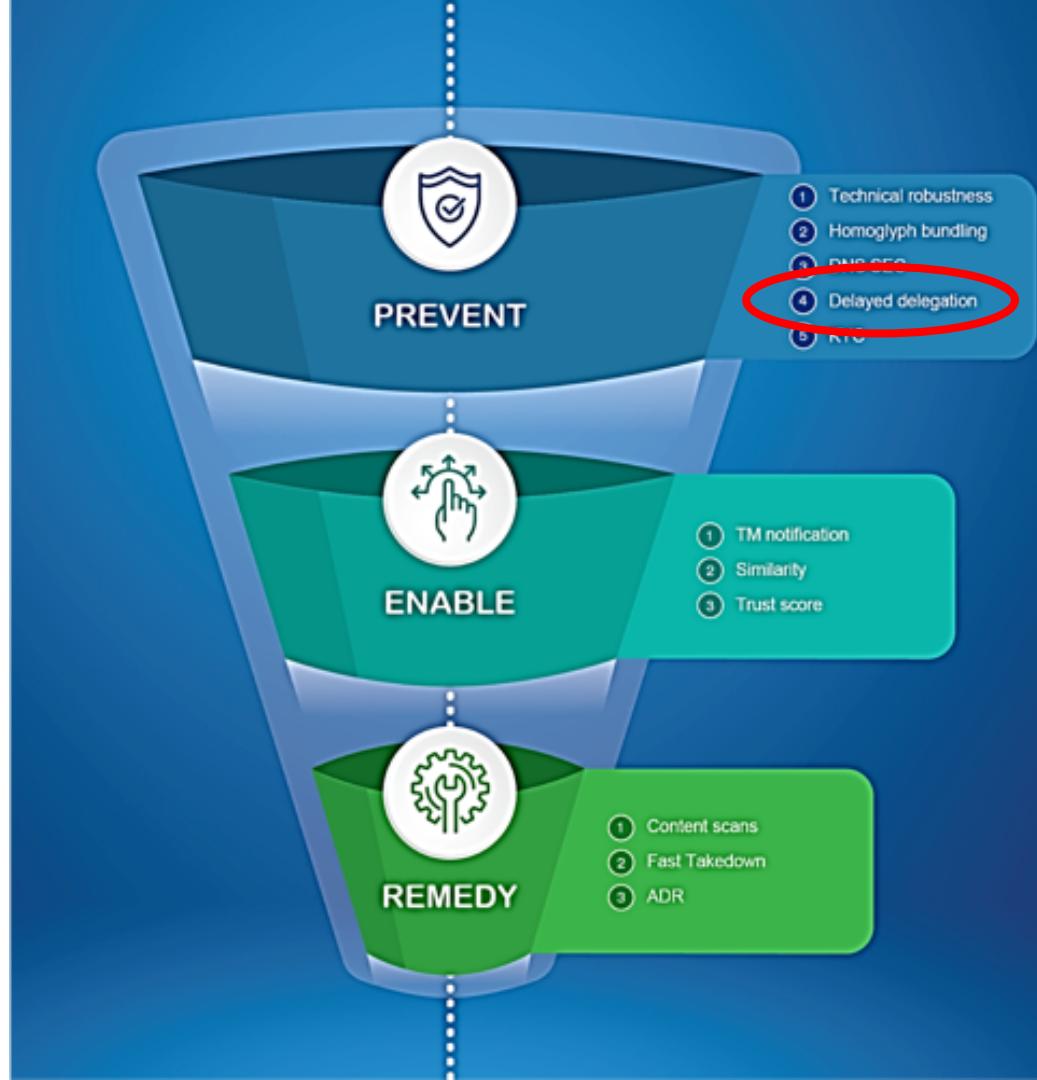
[Hao et al] "Understanding the Domain Registration Behavior of Spammers" IMC 2013

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



<https://link.eurid.eu/prediction1>

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

Thijs Vissers^a, Jan Spreijer^a, Peter Apelt^b, Dick Jagerman^c, Peter Joosen^d, Marc Van Wouwe^e, Frank Pieters^f, Werner Joosen^g, and Lieve Joosen^h

^a iMinds-Distech, Maastricht, Belgium
^b University of Twente, Enschede, The Netherlands
^c University of Twente, Enschede, The Netherlands
^d University of Twente, Enschede, The Netherlands
^e KPN, The Hague, The Netherlands
^f University of Twente, Enschede, The Netherlands
^g University of Twente, Enschede, The Netherlands
^h University of Twente, Enschede, The Netherlands

Abstract. The .eu zone currently contains 14 million of registered domains due to its highly dynamic ecosystem. In this paper we analyze the ecosystem of malicious domain registrations in the .eu TLD. We first identify the most active registrars and abuse contacts. We then analyze the top 1000 malicious domain names and their abuse contacts. Finally, we analyze the top 1000 malicious domain names and their abuse contacts. We find that the most active registrars are located in the United States and the most active abuse contacts are located in the United Kingdom. We also find that the most active registrars are located in the United States and the most active abuse contacts are located in the United Kingdom. We further report on insights in the operational aspects of the malicious domain ecosystem. We find that the most active registrars are located in the United States and the most active abuse contacts are located in the United Kingdom. We further report on insights in the operational aspects of the malicious domain ecosystem. We find that the most active registrars are located in the United States and the most active abuse contacts are located in the United Kingdom.

Keywords: malicious domain names, campaigns, DNSSEC security

1 Introduction

The Domain Name System (DNS) is one of the key technologies that has allowed the Internet to grow into the global communication network it is today. The DNS system requires the resolution of domain names to IP addresses. Malicious actors can use the DNS system to spread malware or to perform other types of attacks. One way to prevent such attacks is to use DNSSEC to provide secure domain name resolution to protect their website operations. For instance, phising attacks, the distribution of malware, and denial-of-service attacks can all be prevented by using DNSSEC.

Malicious domain blacklists are created to help to detect malicious domain names. These blacklists are used by various services to detect malicious domain names. A compromised attacker changes to a different one or creates a new one. A new domain name is then added to the malicious domain blacklist. This process repeats until the attacker is detected.

^a No one for many malicious domain names, whenever we like to do some more that is required to be found in a malicious service or activity.

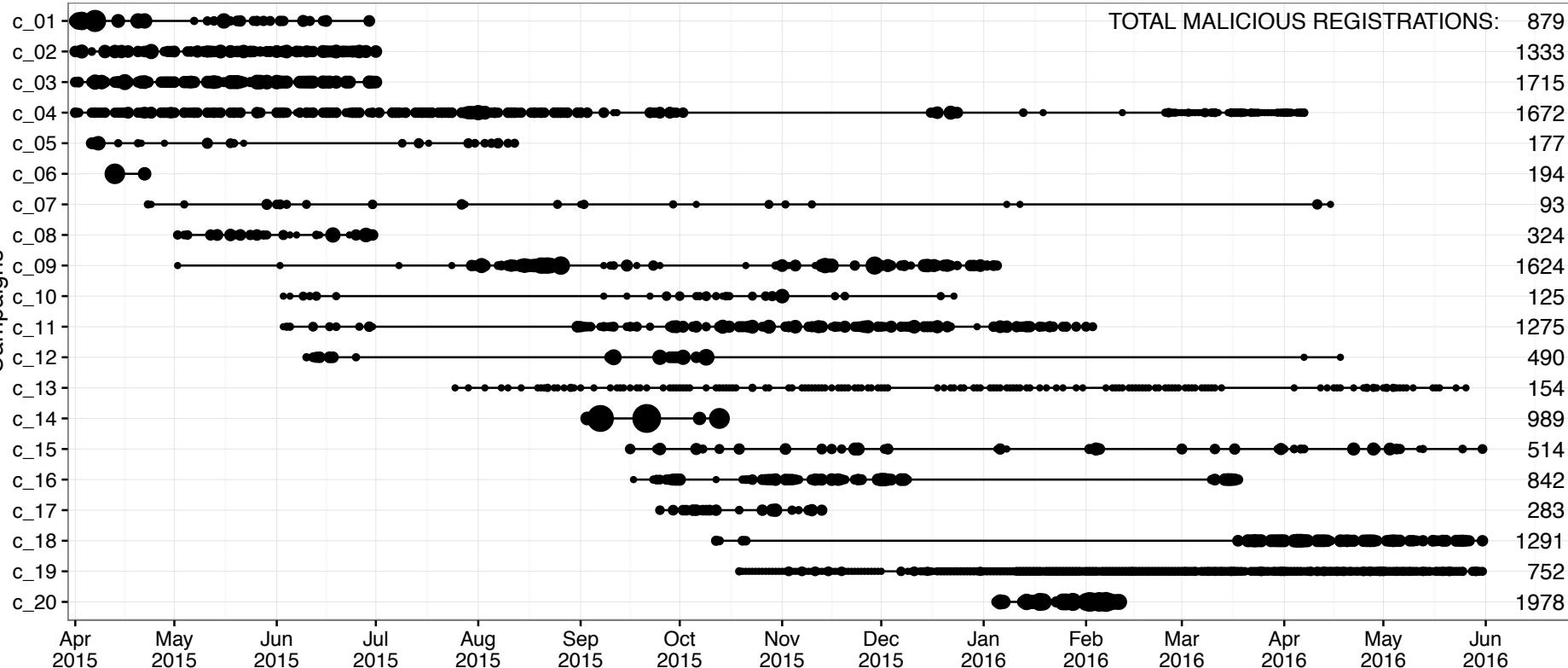
The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-319-60250-4_21

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



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)

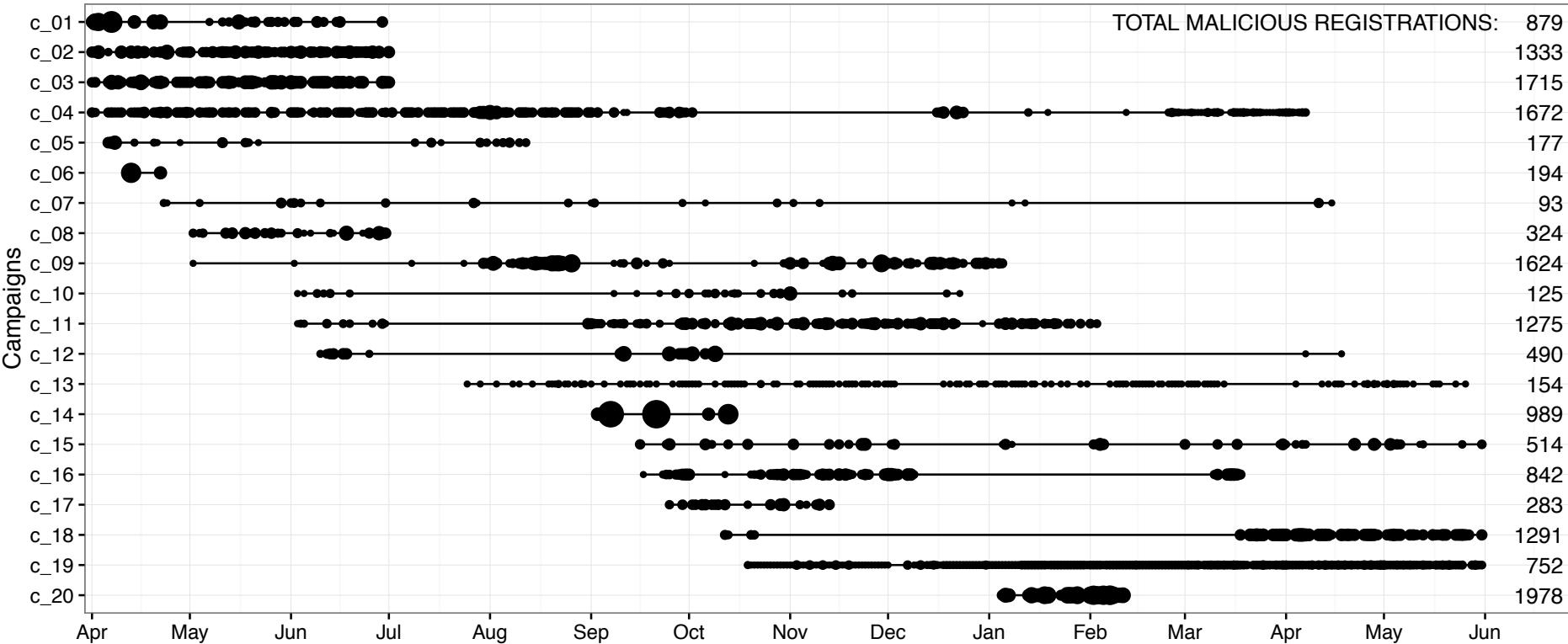
- › Registrant details:
 - » 98 fake registrants
 - » Generated by Laravel Faker tool
- › Domain names:
 - » Consist out of 2-3 Dutch words
 - » Dutch words are reused across registrants
- › Batches of 8, 16, 24 or 32 registrations

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

Insight 2: Small set of malicious actors



Registrations per day



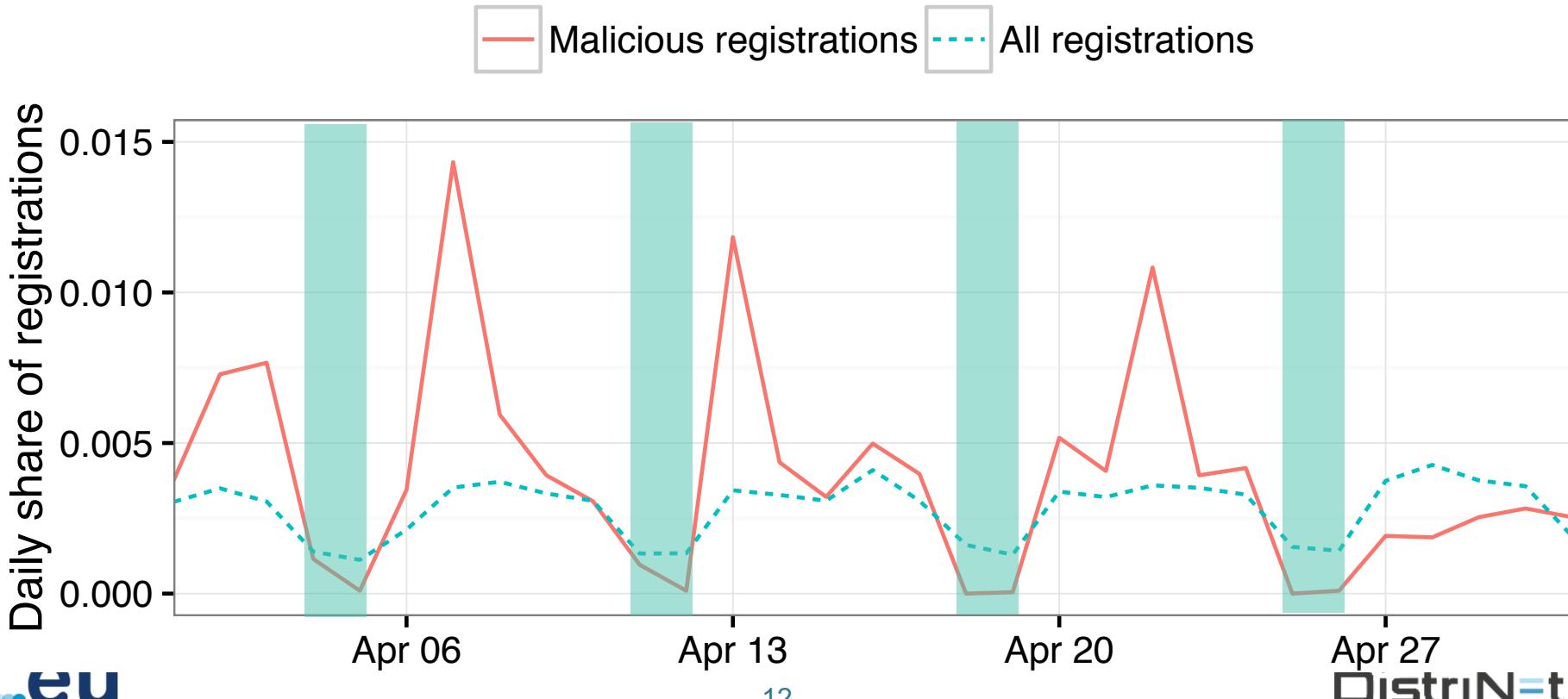
At most 20 actors represent 80% of malicious registrations

Insight 3: Top facilitators for malicious registrations

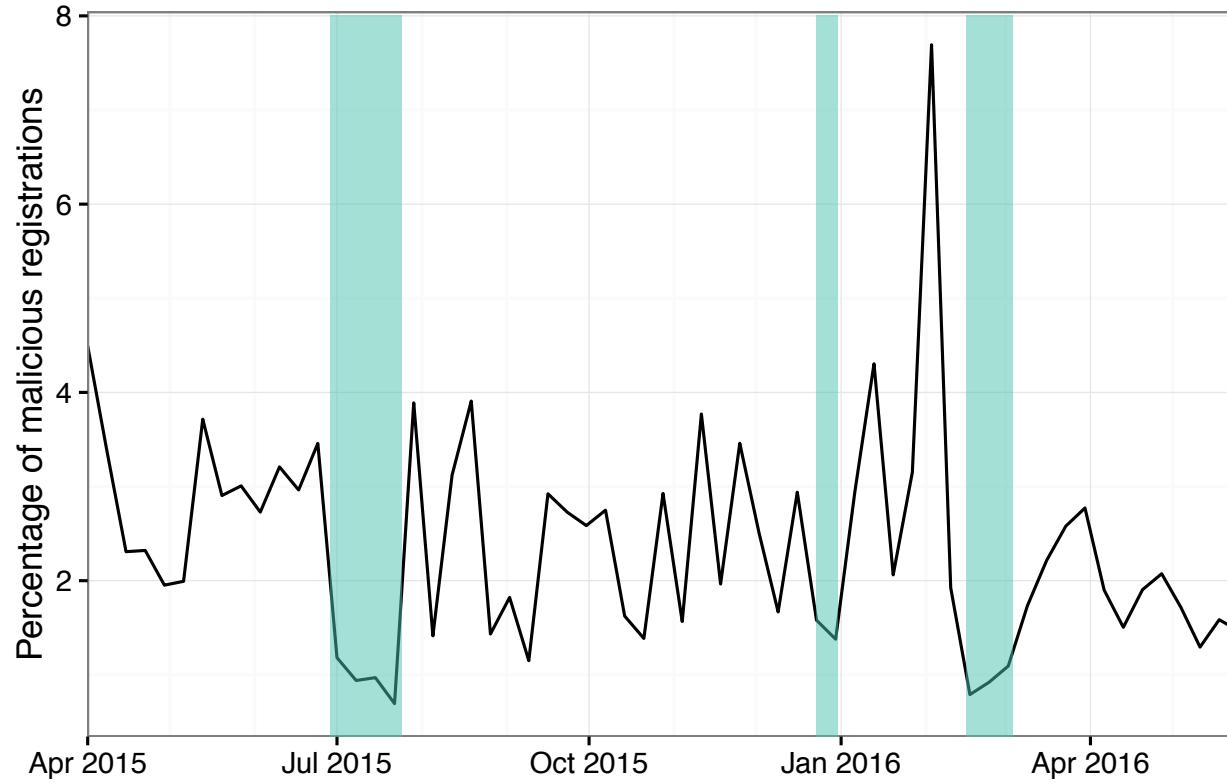


	Nb of malicious	Contribution Malicious	Benign	Toxicity
1. registrar_5	10,353	49.61%	2.27%	36.25%
2. registrar_3	3,004	14.39%	2.64%	12.41%
3. registrar_7	2,327	11.15%	0.46%	38.67%
1. gmail.com	4,221	20.23%	24.79%	2.08%
2. yahoo.com	3,348	16.04%	1.49%	21.85%
3. aol.com	2,134	10.23%	0.31%	46.28%

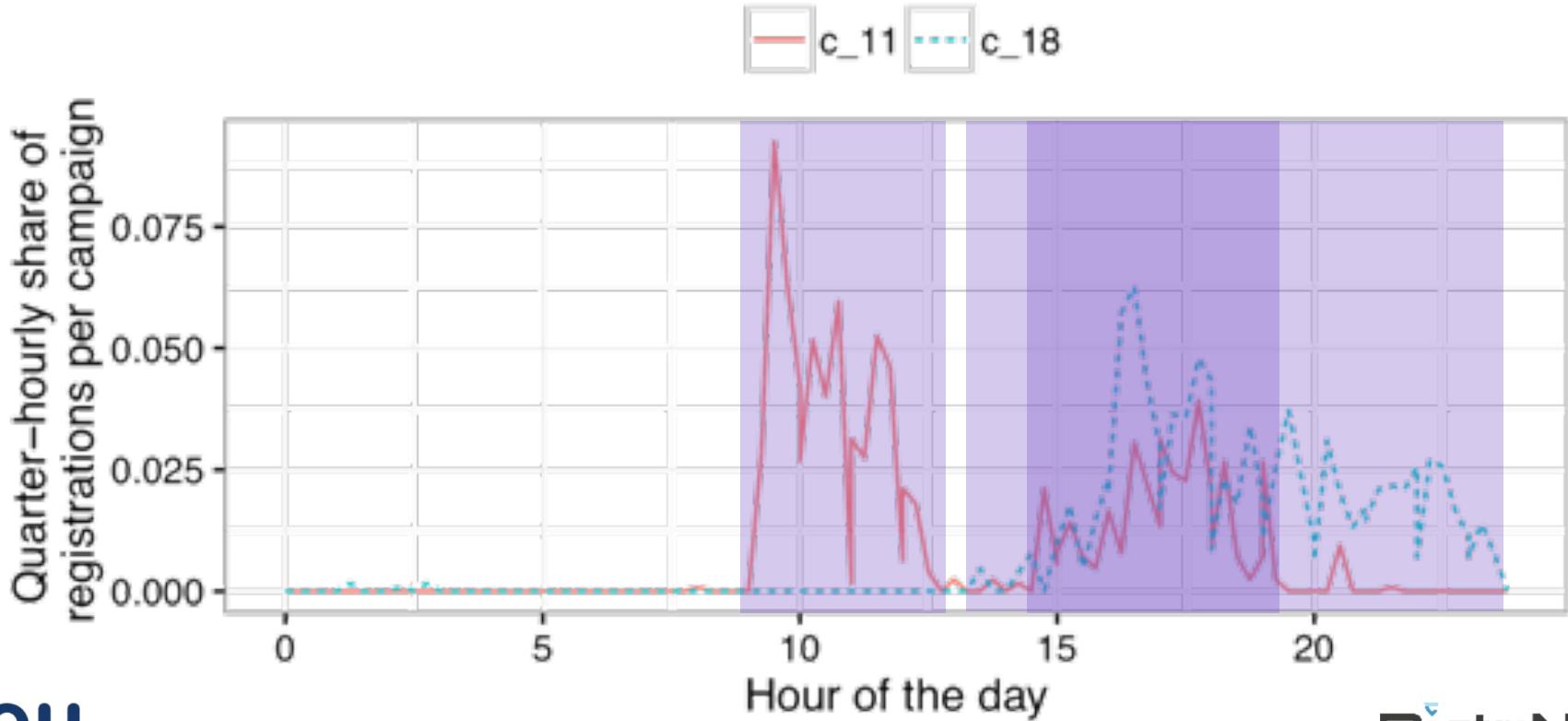
Insight 4: Some campaigns align with regular business activity patterns (1)



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

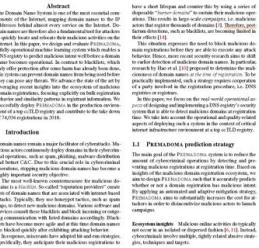


Insight 4: Some campaigns align with regular business activity patterns (3)



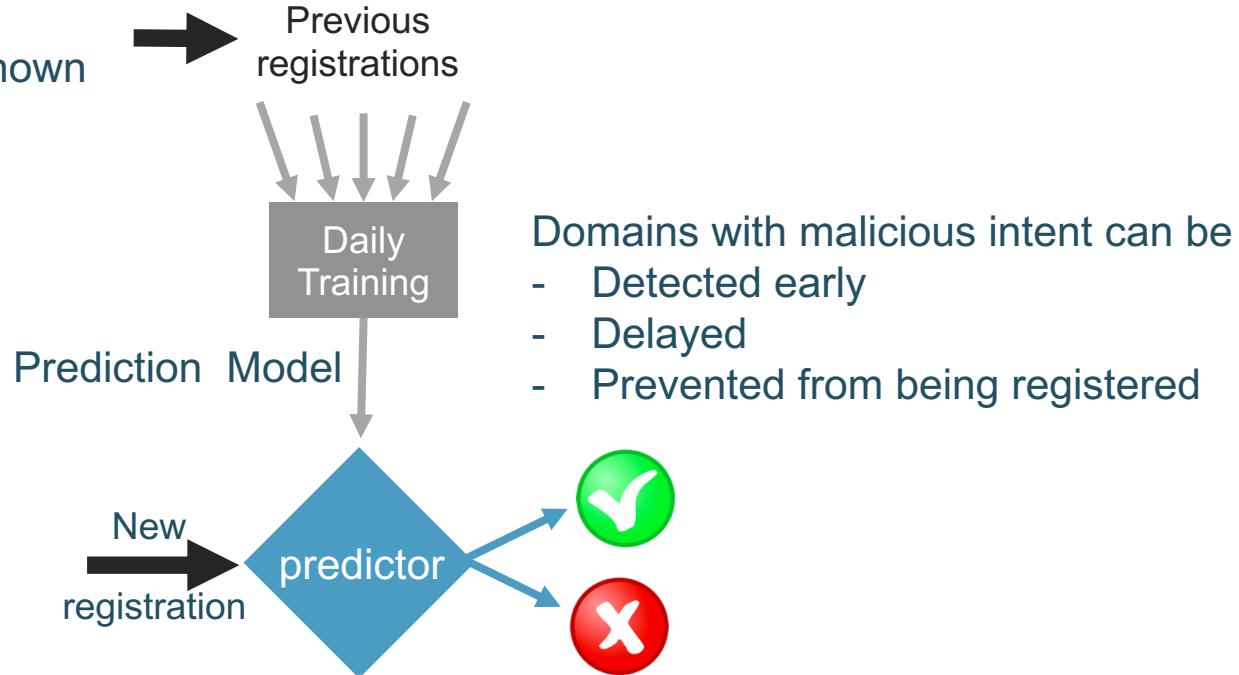
Registration-time prediction of malicious intent

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



Underlying assumptions/rationales for our predictors

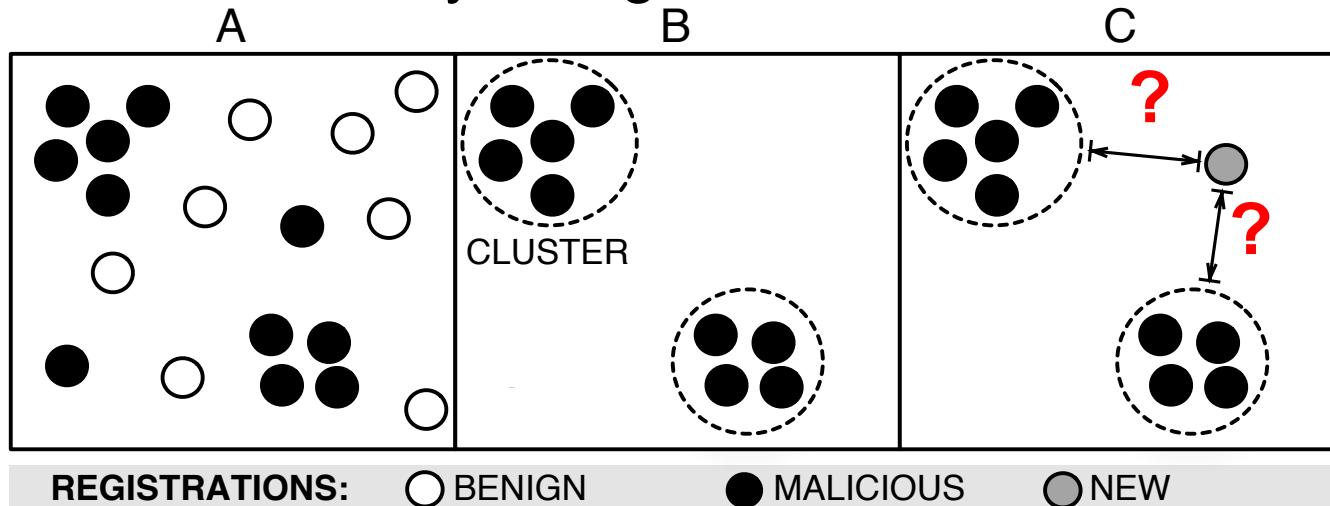
- › Similarity-based agglomerative clustering
 - » Domains belonging to the same campaign have very similar registration details
- › Reputation-based classification
 - » Domains using registration facilitators with a bad reputation (e.g. email providers or registrars), are likely to be malicious as well

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

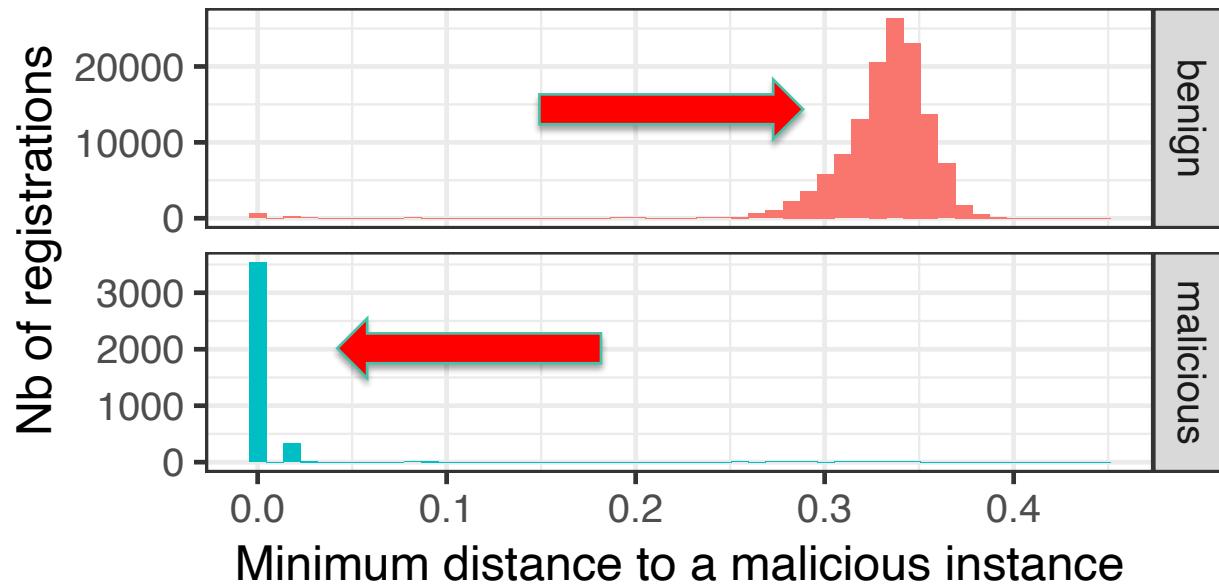
Predictor 2: Similarity-based clustering

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



Can we differentiate between benign and malicious samples?

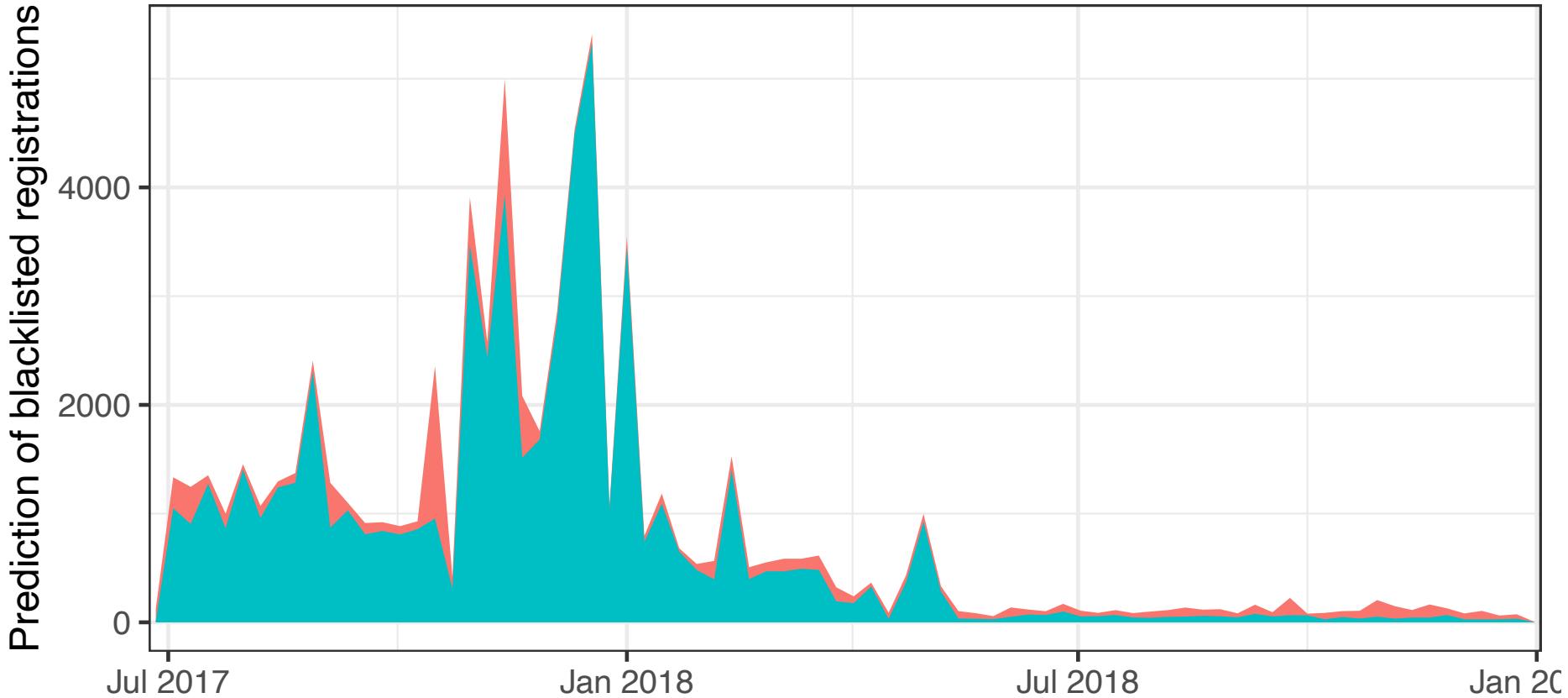
- › Closest distance of a registration to malicious domain



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

[« Back to the news page](#)

On 29 January 2018, EURid susp

With actions as such, our focus is enforcement, both on a national towards building the most trusty illegal activity online. "With our th names for potential abuse, leadi EURid Legal Manager.

In 2017, we suspended 20 126 t enforcement.



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.

Over 11 000 abusive domain names suspended

[« 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, as well as with our registrar channel, we are in name space, taking a stand against

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

"We're up to 36 336 abusive domain name suspensions thus far in 2018," said Geo Van Langenhove, EURid Legal Manager.

Learn more about the ways we're building a trustworthy .eu and .eio domain name space at [trust.eurid.eu](#).

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—Domain blacklisting is widely used to quickly resolve user queries to malicious domains. In this paper, we set out to further understand how such can be done effectively. We first introduce a dataset of over 100,000 domain names that contain DNS records associated with domain registrars and their corresponding IP addresses. This dataset is used to evaluate the effectiveness of domain blacklisting against malicious domains. We focus on large-scale experiments to evaluate the effectiveness of domain blacklisting against malicious domains. We show that blacklisted operators are both more effective and faster than other operators. More specifically, by looking at forming DNS requests from different sources, we find that the effectiveness of domain blacklisting is highly dependent on the source of the request. This makes it difficult to draw conclusions about the effectiveness of domain blacklisting.

DNS continues to serve as a major facilitator of internet-based crime. From phishing and spam to botnet command and control, DNS is often the primary communication channel for malicious actors. As a result, many registrars now offer services to help combat malicious domain names. One such service is domain registration for malicious purposes as described in [1].

In our previous study, we concentrated on the security of domain blacklisting. We found that the vast majority of the blacklisted registrations could be attributed to a small number of registrars. This led us to conclude that the problem lies with the way in which registrars provide the filtering of domain names used in these attacks.

In this paper, we take a closer look at the effectiveness of domain blacklisting, while closely adhering to the methodology of our previous study. The main conclusion is that some campaign registrations are very actively used to conduct malicious behavior. At this time, there is no way to identify these specific registrations. Therefore, we combine multiple tactics to achieve detection. However, the success of these tactics is heavily dependent on the source that transmits them as requests. For example, many detections and preventions are successful when the requests are transmitted via email for most registrars (e.g. [3] [4] [5]). Furthermore, the success of domain blacklisting is heavily dependent on the way in which blacklisting is a main indicator of malice (e.g. [7] [9]).

This work was funded by the Flemish Government.

The authors thank the anonymous reviewers for their valuable feedback.

We also thank the domain registrars that participated in our experiments.

We hope the use of creative and practical blacklisting techniques will lead to a better understanding of how campaigns operate.

Finally, we would like to stress that improved detection is relative to active and dormant registrations.

• We hope the use of creative and practical blacklisting techniques will lead to a better understanding of how campaigns operate.

• We hope the use of large-scale registration and deployment of domain blacklisting will lead to a better understanding of how campaigns operate.

• We hope the remainder of the paper is received as follows:

– Part I: The remainder of the paper is received as follows:

– Part II: The remainder of the paper is received as follows:

– Part III: The remainder of the paper is received as follows:

– Part IV: The remainder of the paper is received as follows:

– Part V: The remainder of the paper is received as follows:

– Part VI: The remainder of the paper is received as follows:

– Part VII: The remainder of the paper is received as follows:

– Part VIII: The remainder of the paper is received as follows:

– Part IX: The remainder of the paper is received as follows:

– Part X: The remainder of the paper is received as follows:

– Part XI: The remainder of the paper is received as follows:

– Part XII: The remainder of the paper is received as follows:

– Part XIII: The remainder of the paper is received as follows:

– Part XIV: The remainder of the paper is received as follows:

– Part XV: The remainder of the paper is received as follows:

– Part XVI: The remainder of the paper is received as follows:

– Part XVII: The remainder of the paper is received as follows:

– Part XVIII: The remainder of the paper is received as follows:

– Part XVIX: The remainder of the paper is received as follows:

– Part XX: The remainder of the paper is received as follows:

– Part XXI: The remainder of the paper is received as follows:

– Part XXII: The remainder of the paper is received as follows:

– Part XXIII: The remainder of the paper is received as follows:

– Part XXIV: The remainder of the paper is received as follows:

– Part XXV: The remainder of the paper is received as follows:

– Part XXVI: The remainder of the paper is received as follows:

– Part XXVII: The remainder of the paper is received as follows:

– Part XXVIII: The remainder of the paper is received as follows:

– Part XXIX: The remainder of the paper is received as follows:

– Part XXX: The remainder of the paper is received as follows:

– Part XXXI: The remainder of the paper is received as follows:

– Part XXXII: The remainder of the paper is received as follows:

– Part XXXIII: The remainder of the paper is received as follows:

– Part XXXIV: The remainder of the paper is received as follows:

– Part XXXV: The remainder of the paper is received as follows:

– Part XXXVI: The remainder of the paper is received as follows:

– Part XXXVII: The remainder of the paper is received as follows:

– Part XXXVIII: The remainder of the paper is received as follows:

– Part XXXIX: The remainder of the paper is received as follows:

– Part XXXX: The remainder of the paper is received as follows:

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



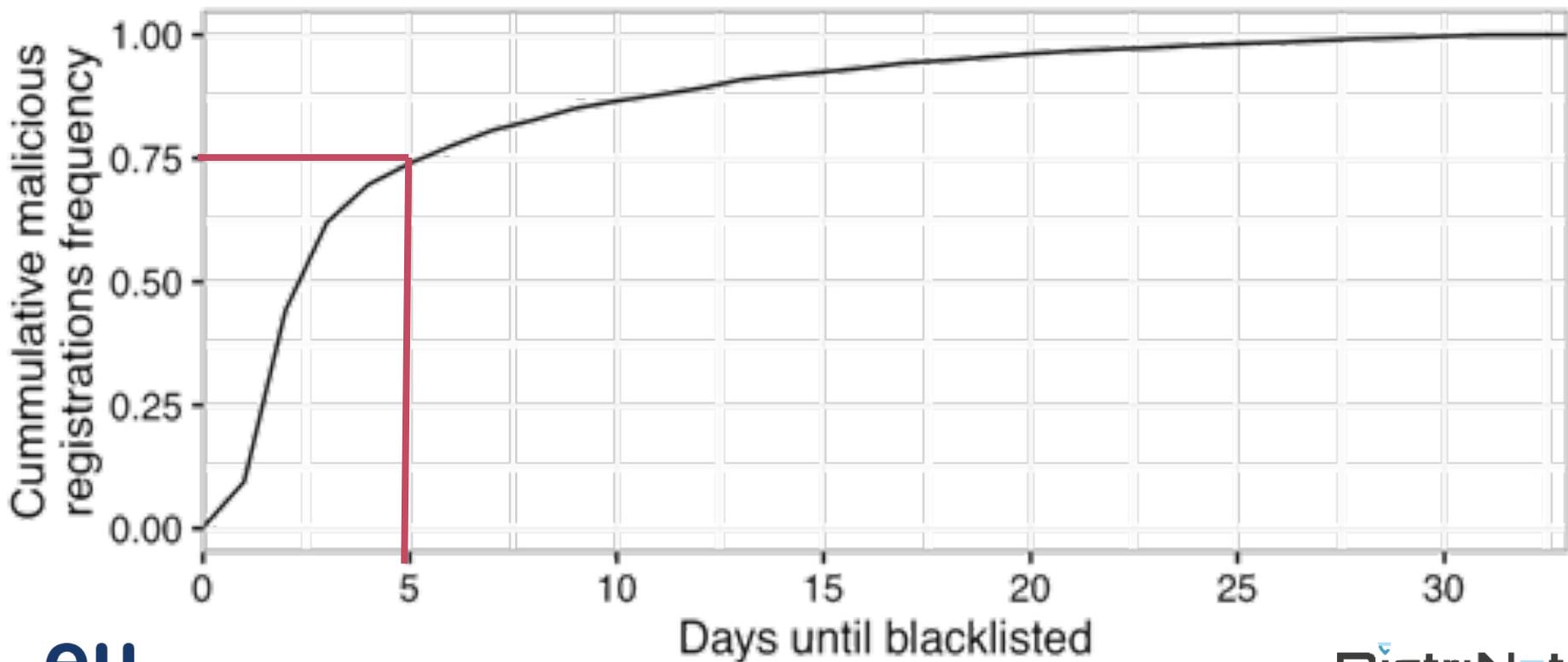
Google Safe Browsing

- › 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%

Delay of the ground truth



Incompleteness of the blacklists

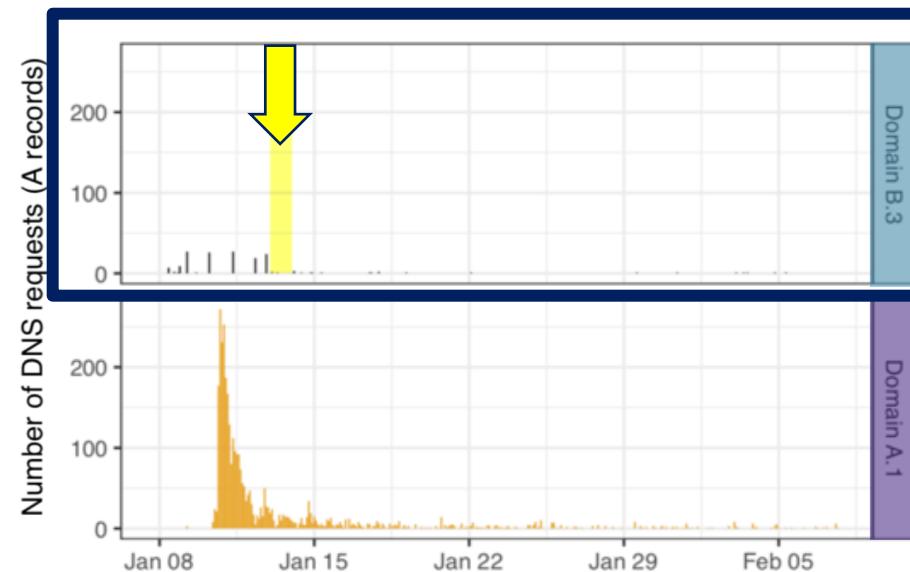
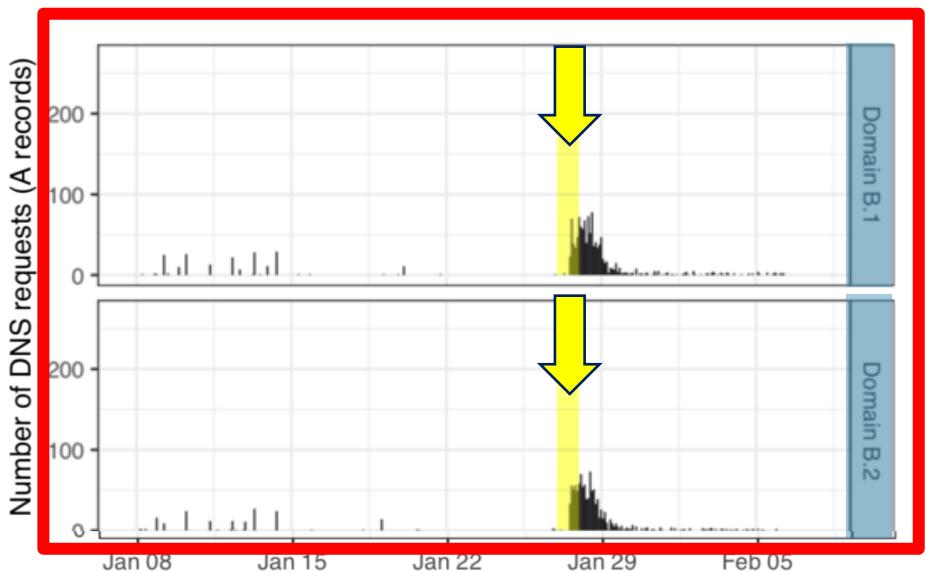
- › Failed to detect?
- › Never active/malicious?



	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

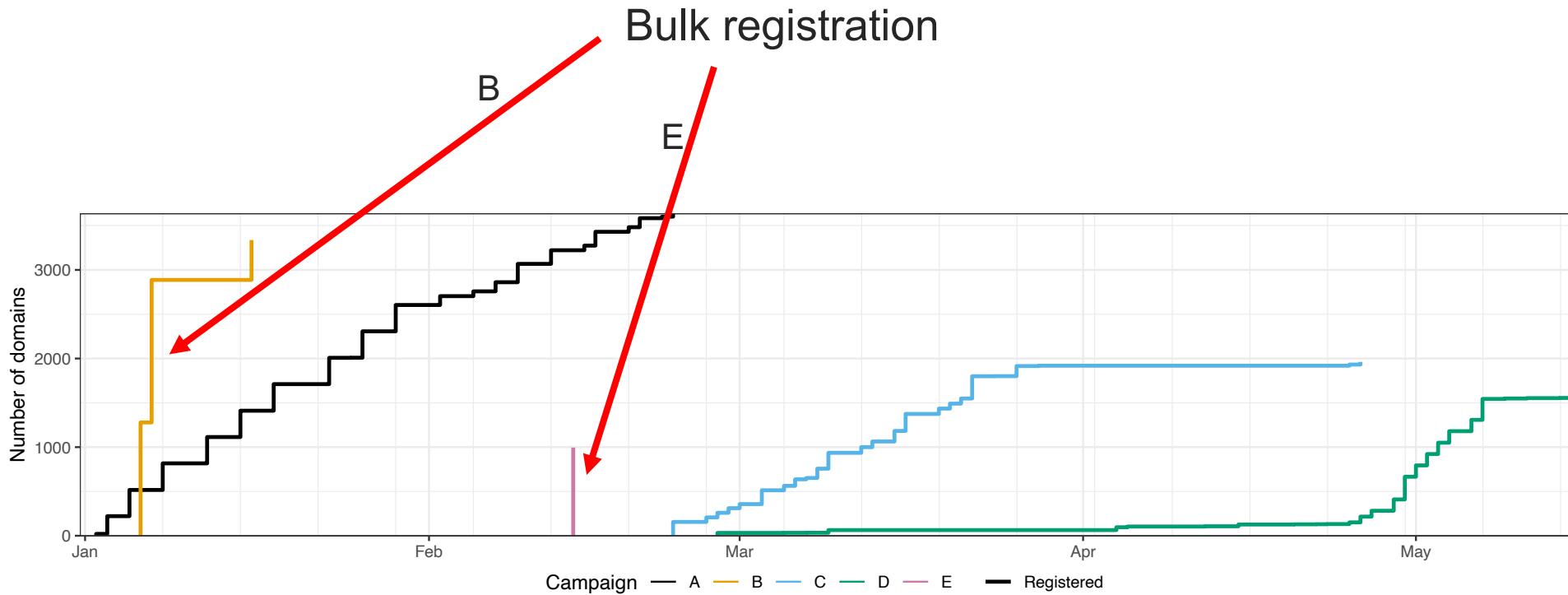


Active vs Dormant – Blacklisted vs Non-blacklisted

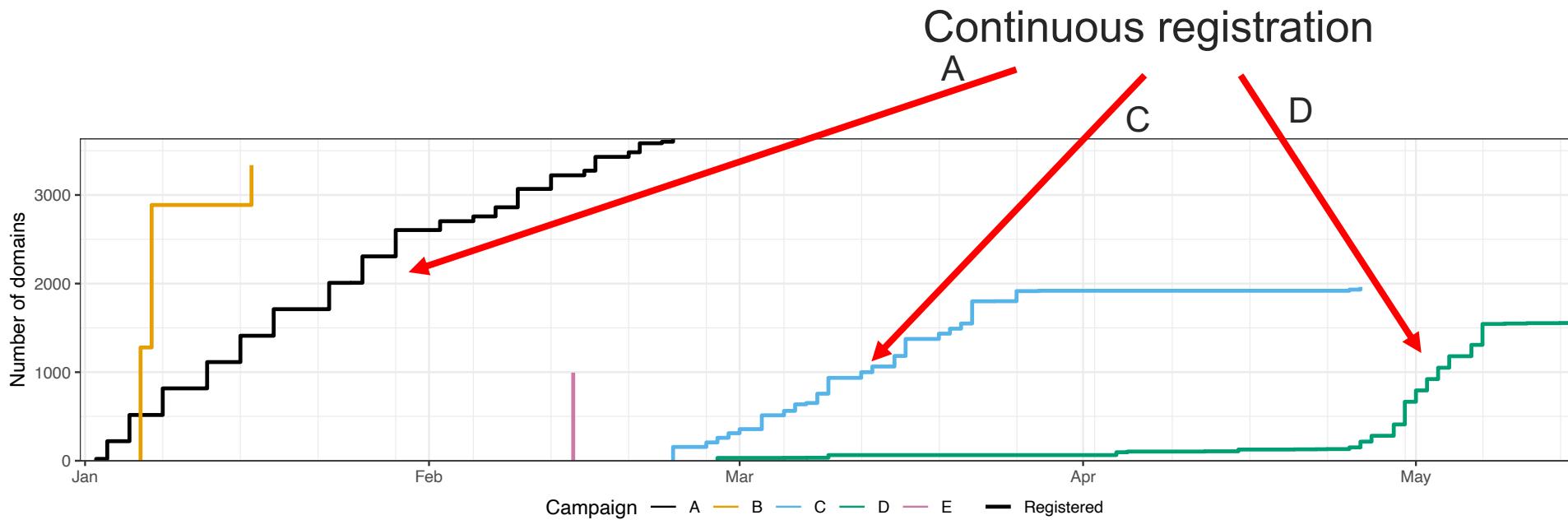
- › 5 largest campaigns in .eu (Q1-Q2 2018)
- › Based on passively-logged DNS requests (.eu TLD server)

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

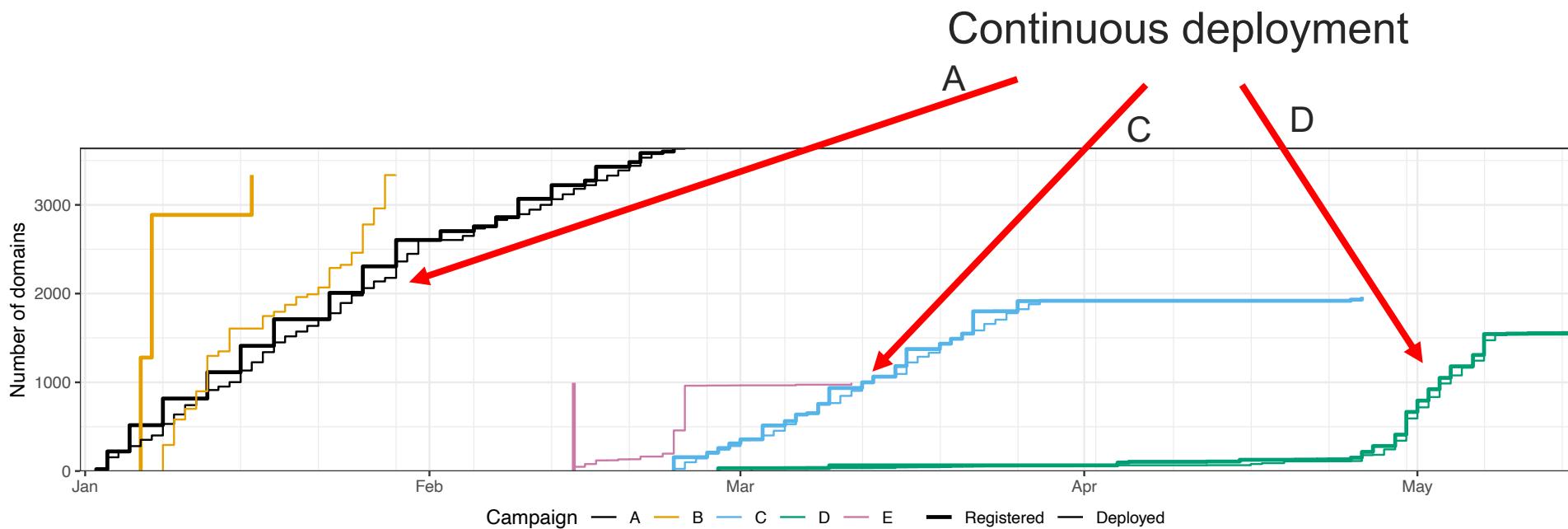
1. Registration strategy



1. Registration strategy

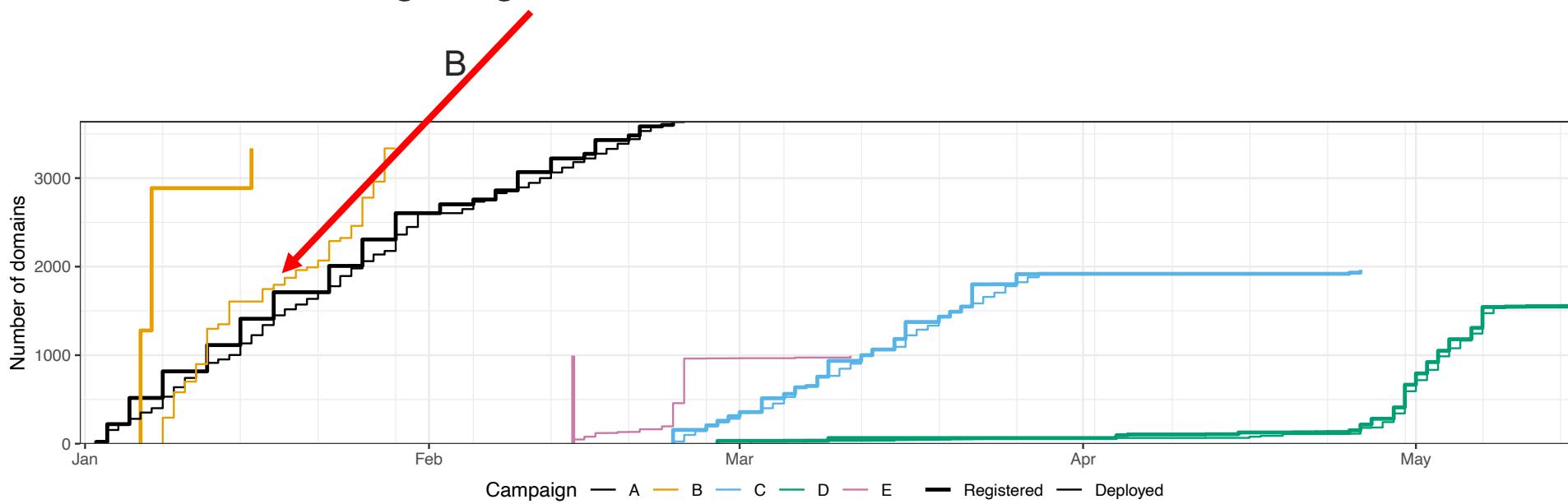


2. Deployment strategy (thin line)

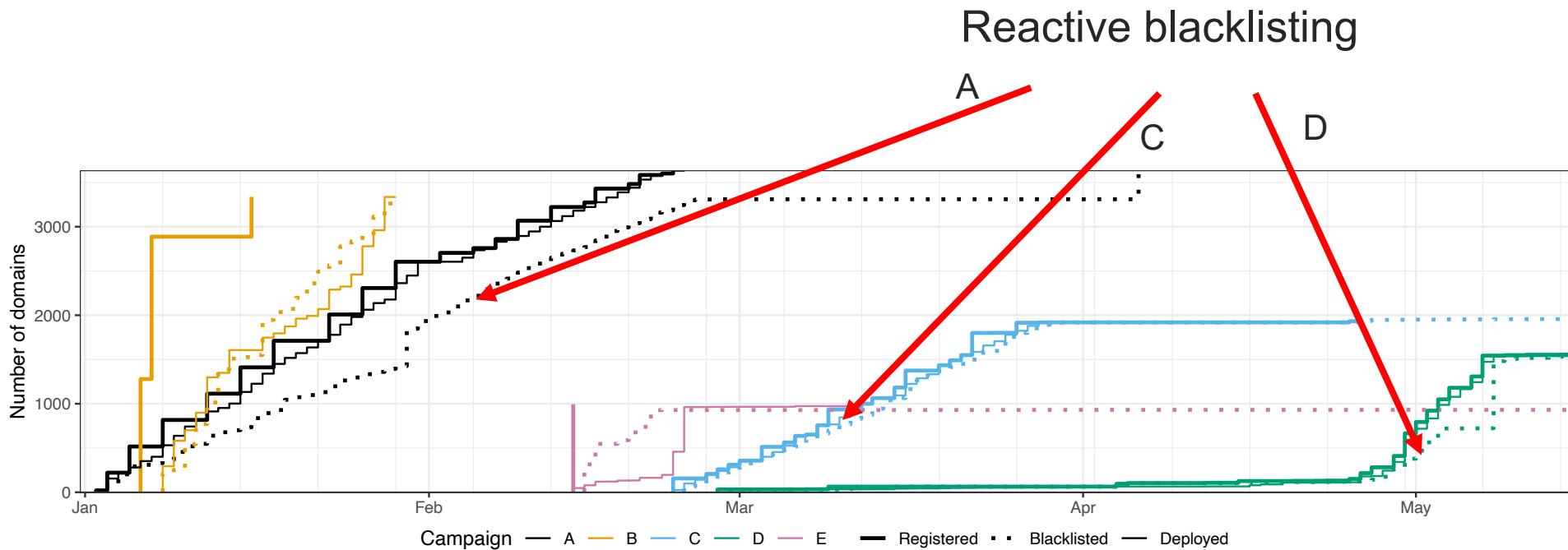


2. Deployment strategy (thin line)

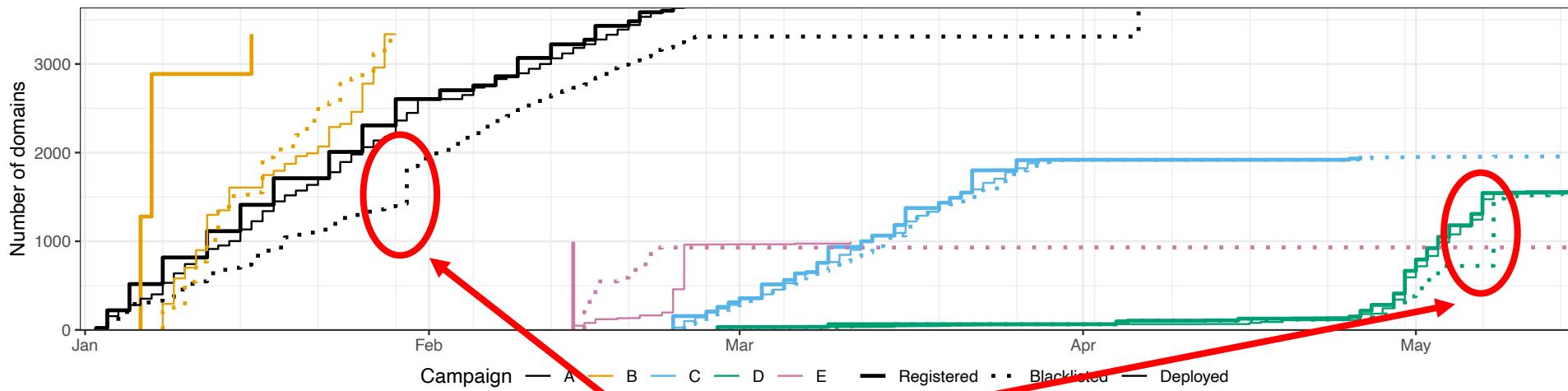
Gradual deployment,
although registered in bulk



3. Domain blacklisting (dotted line)

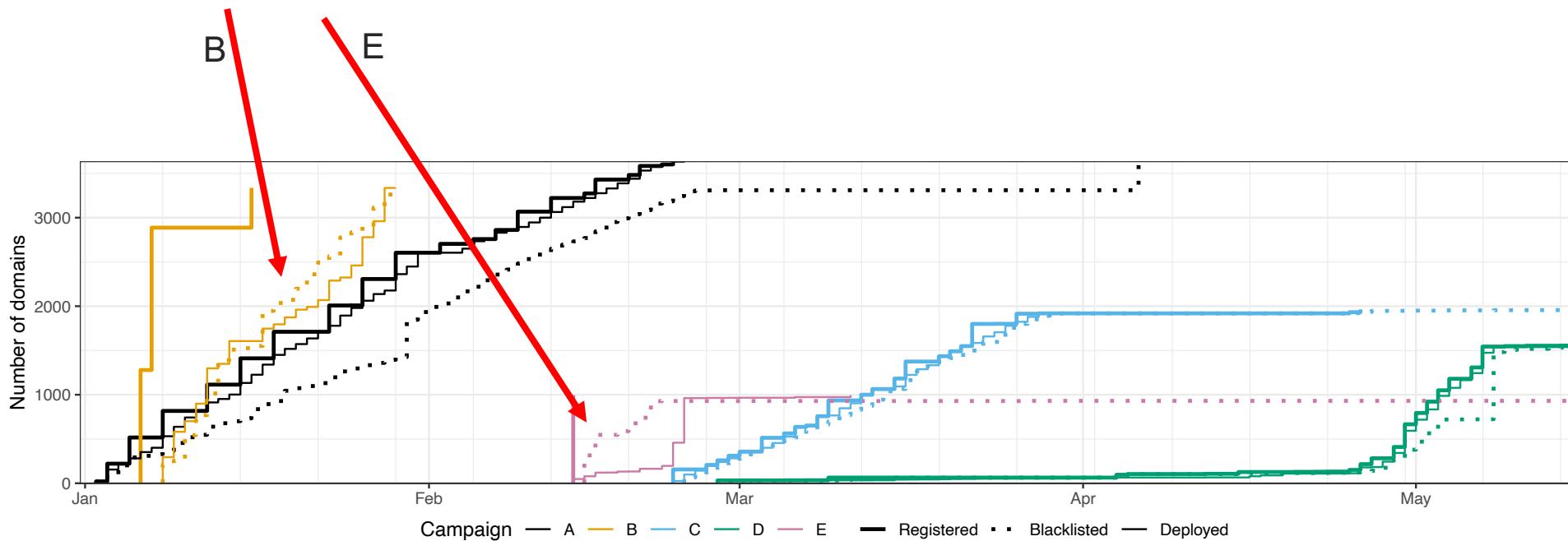


3. Domain blacklisting (dotted line)



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 Vervaeke¹, Peter Agiotis², Frédéric Janssens², Peter Janssens², Marc Van Wouwe³, Frank Piessens², Wouter Joosen², and Lieven Decraene²

¹ Antwerp University, Antwerp, Belgium
(tvervaeke.lieven@ua.ac.be)
² Eindhoven University of Technology, Eindhoven, The Netherlands
(wouter.joosen@tue.nl)

Abstract. This study empirically scrutinizes 11 months of registration data to identify large-scale malicious campaigns present in the .eu TLD. We find that the .eu TLD is heavily used by malicious actors who register services that maliciously register large amounts of domains for one-shot, malicious use. Although these malicious domains are short lived, by collecting and analyzing the IP addresses associated with these domains, it can be found in 20 to 25 campaigns with varying duration times. These campaigns are highly geographically dispersed, spread over all business and observe, amongst other findings, that their processes are highly automated. We also propose a methodology for applying a process to validate the campaign identification process and to estimate the ecosystem analysis of malicious registrations in a TLD space.

Keywords: malicious domain names, campaigns, DNS security

1 Introduction

The Domain Name System (DNS) is one of the most critical infrastructures 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 activities have been observed to abuse the DNS system to perform various types of domain names to execute their abusive operations. For instance, phishing attacks, distributing spam emails, botnet command and control (C2C) connections and malware distribution are some of the most common examples.

Wide-spread domain names are curated and used to spoof malicious domain names. In the early days of the Internet, when the number of domain names was low, as a consequence, attackers changed to a hit-and-run strategy, in which multiple domain names are operational for only a very small time window after the initial registration [1]. This strategy is still in use at the moment [2]. Once domain names

¹ We use the term malicious domain to indicate whether or not a domain name that is registered to be malicious or a malicious service or activity.

The final publication is available at Springer via <http://dx.doi.org/10.1007/s11393-010-0211>

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

Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations

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

Abstract

The Domain Name System is one of the most essential components of the Internet, mapping domain names to the IP addresses of the servers that host them. As such, domain names are therefore also a fundamental tool for attackers to quickly locate and educate their malicious activities on the Internet. In this paper, we introduce PREDAMOIA, a fully operational machine learning system which monitors a DNS registry to predict malicious intent well before a domain name is registered. Unlike other systems that can only offer protection after some harm has already been done, this system can prevent domain names from being used before they are even registered. We evaluate PREDAMOIA by leveraging recent insights into the ecosystem of malicious domain registrations, focusing explicitly on bulk registration behavior. Our results show that PREDAMOIA can successfully deploy PREDAMOIA in the production environment of a top-level registry and contribute to the take down of 74,000 registrations in 2018.

1 Introduction

Domain names remain a major facilitator of cyberattacks. Malicious actors continuously deploy domains in their cybercriminal operations, such as spam, phishing, malware distribution and botnet command-and-control. To prevent these operations, stopping malicious domain names has become a highly important security objective.

The most common mechanism for malicious domains is a blacklisting. Such so-called "repotation providers" curate lists of domain names that are associated with specific bad actors. These lists are often updated in real time, using various traps, to detect new malicious domains. Various software and services consult blacklists and block incoming or outgoing connections to these domains. While blacklists have become more agile and as a result domain names are blocked quickly after detecting an active behavior.

Attackers, however, have adapted to this kind of mitigation. Specifically, they anticipate their malicious registrations to how a short lifespan and counter this by using a series of disposable "burner domains" to sustain their malicious operations. This results in large-scale campaigns, i.e., malicious domain registrations, that are hard to detect using traditional feature detections, such as blacklists, and become limited in their effects [14].

This motivates the need to block malicious domain registrations before they are able to execute any attack behavior. Hence, more recent research efforts aim to detect malicious domain names at the earliest possible time. For example, Hu et al. [10] propose to determine the maliciousness of domain names at the time of registration. To achieve this, they propose a proxy involved in the registration process, i.e., DNS registrars or registrants.

In this paper, we focus on the real-world operational aspects of designing and implementing a DNS registry's security system that is able to detect malicious domain registration attempts. We propose PREDAMOIA, a machine learning system that is able to detect malicious domain registrations in real time. PREDAMOIA is specifically designed to be the one fit for tasks in order to distinguish malicious attacks to launch campaigns.

Ecosystem insights

Cybercriminal activities do typically not occur in an isolated or dispersed fashion [6, 11]. Instead, cybercriminals utilize multiple, tightly related attack stages, techniques and targets.

<https://link.eurid.eu/prediction1>

<https://link.eurid.eu/prediction2>

<https://link.eurid.eu/prediction3>

<https://link.eurid.eu/prediction4>

[https://link.eurid.eu/prediction\[1-4\]](https://link.eurid.eu/prediction[1-4])

Detecting and preventing DNS abuse in .eu

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