



Detecting and preventing domain name abuse in .eu

Lieven Desmet, KU Leuven – Marc Van Wesemael, EURid

Registration of DNs with fraudulent/criminal intentions

- Types of abuse
 - >> To attract traffic to websites (use of reputation of somebody else)
 - >> To distribute malware
 - >> To send SPAM
 - To sell illegal products (drugs, counterfeited goods, fake medication, etc.)
 - To sell products and not deliver
 - Often (very) short term use (hours or days)

Key issue: fake identity of the registrant

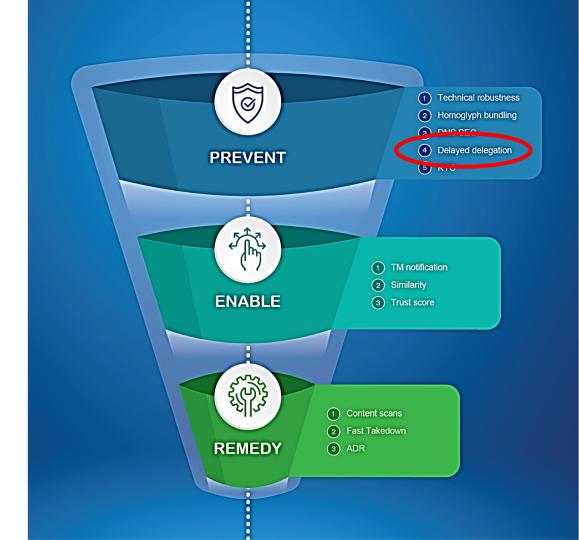




The .eu trust strategy

- Delayed delegation
 - Predict at time of registration whether a domain namewill be used abusively





https://link.eurid.eu/prediction1

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

> Thomas Vissen⁴, Jun Spoonen⁵, Pieter Agten⁵, Dick Jump sen⁵, Marc Van Wissensof⁵, Head Pleusen⁵, Wieter Joon Domast⁶
>
> ⁵ inco-DictriSer, EU Leaves, Brighten (Electrises-Listenso@Ge, Koberwa Jo.

Abstrace. This endy crossolody surethinks 1 is south as fugiented data to blood his passive intellection engaging powers in the CPL. We explore the countries of the control of the countries and endough expended delaborate or between the countries and endough expended delaborate or between the countries and the countries of the

1 Introdu

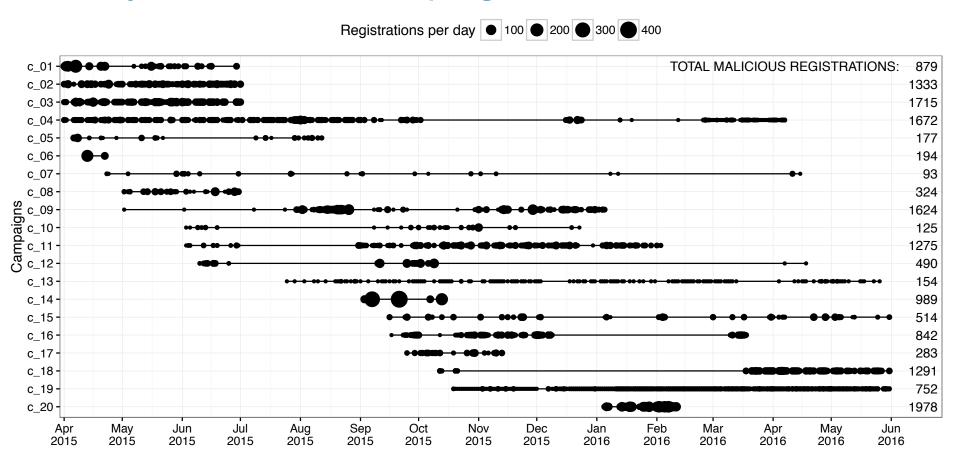
The Lemma Same (Section 1995) is some of the top relambings in that has also been performed in the size of the siz

The first publication is available at Elevinger via High Polycology 13, 1007/879 0-219-00022-4-21

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



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%)

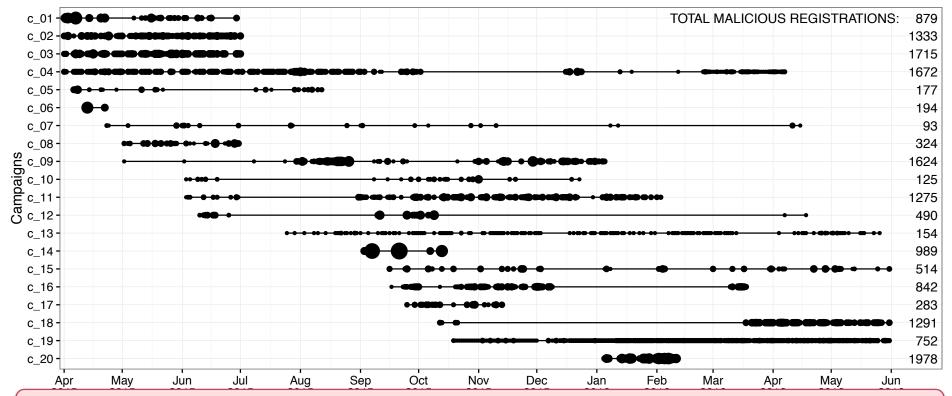




Insight 2: Small set of malicious actors







At most 20 actors represent 80% of malicious registrations

Insight 3: Top facilitators for malicious registrations



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





Insight 3: Top facilitators for malicious registrations



	Nb of	Contribution		
	malicious	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%





Quick overview of other insights



- Majority of blacklisted domains is spam-based
- Blacklisting happens shortly after registration
- Malicious actors exhibit "human behavior"
 - » Some work 9-to-5, take holidays, …
 - ›› They sometimes make typos
 - >> They vary over time





https://link.eurid.eu/prediction4

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

...

The Described Nature Mean Conference on controlled to the Conference of the Conferen

1 Introduction

Domain menus namain a major facilitato of cyboratiscis. Mi ficious actore confinencialy object domains in their cyboraries had oppostine, such as quasa, pleiding, malatone distribution and boster Claff. Due to this crucial rule is a syboratismia and boster Claff. Due to this crucial rule is a syboratismia operations. Augment matter in the control hapithy important recently objective. The most well-flower construents are malacious de mains in a Societius. So-called "hopetation providers" court fast of domain some that are successful with histories does that of domain some that are successful with histories does

Se Ecosystem insights: Malicious online activities de typis not occur in an isolated or dispensed inshire [6, 113], he contemporalist involves anticles, bother related absolves or

Registration-time prediction of malicious intent

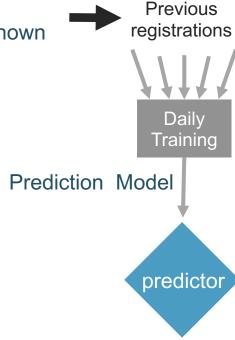
J. Spooren et al., PREMADOMA: An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations, Annual Computer Security Applications Conference (ACSAC 2019), December 2019.

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





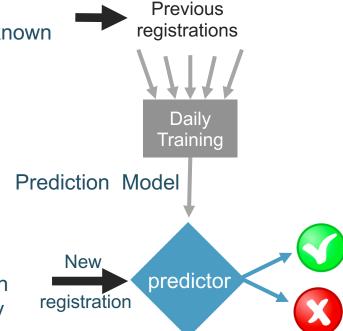
Previous registrations for which the results (abuse/no abuse) is known







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



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





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



Daily Training 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







Underlying assumptions/rationales for our predictors

- Similarity-based agglomerative clustering
 - » Domains belonging to the same campaign have very similar registration details





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





Evaluation on historical data

Ground truth-based evaluation

» Recall: 66.23%

>> Precision: 84.57

» False positive rate: 0.30%

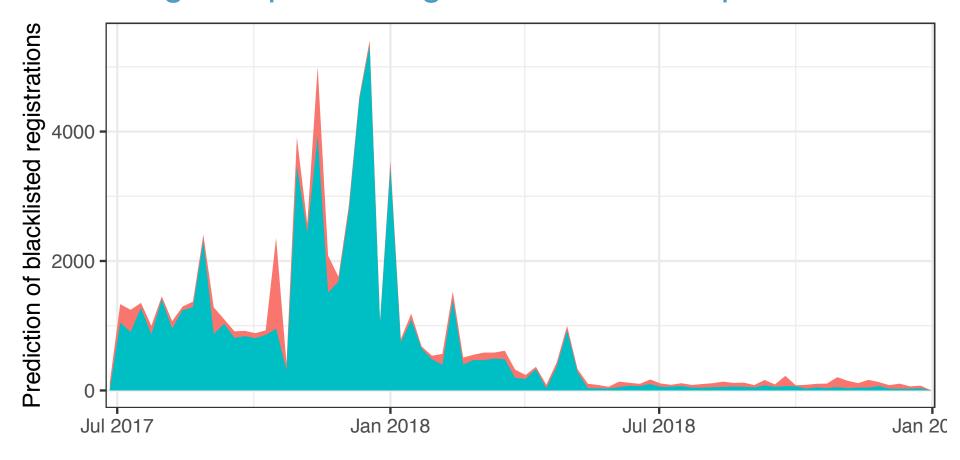
Campaign-based evaluation

>> 17 out of the 20 campaigns are well predicted





Detecting and preventing abuse in .eu: "1 picture ..."



Home News Register a domain name My .eu Become a registrar WHOIS About us Contact Us

Over 25 000 domain names suspended with ties to identity fraud

▼ Tweet« Back to the news page

On 29 January 2018, EURid susp

With actions as such, our focus in enforcement, both on a national towards building the most trust illegal activity online. "With our than man for potential abuse, leading EURid Legal Manager."

In 2017, we suspended 20 126 c

.eu

Home

Register a domain name

My .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.

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

I, as well as with our registrar channel, we

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

I, as well as with our registrar channel, we in name space, taking a stand against

nonitor our domain names for potential pared to 2017, where we suspended 20 126

abusive domain names, were up to 35 336 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 .eю 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





https://link.eurid.eu/prediction3

Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations

Thomas Vissen*, Peter Janssen*, Wanter Joosen*, Lieven Deux *Inoc-Distrible, KU Leaven

we distribute or relative such inventor remarks (IIII.

10 this legal in seen that or six was four form in a finite real in the relative six was four real in and how offsiche flow you. It ship coper, we see that the relative six was found in the relative six was found in the relative six was disting the distribute or relative to an improved was distributed or relative to an improved was distributed at least to relative dismits some used to relative the relative six was seen to be in relative to the relative six was to be in the relative six which is the relative six was to be in the relative six was to be in the relative six when it is also the data of the relative six when is belief in the data or compare of these manifectors denote, we see that when in belief in the data or compare of easily.

L DITECTORION

L DITE

growthen their strate, The second of thesis is seen for the property of the property of the property of the Second property of the second property of the prop

heir ground

III. DeFAIRT AND CANDRASS MEDITIFICATION
on mathers
In this section, we first describe the data used in
page. Next, we establish the starting point of our watime mate by identifying the five most active campaigns present in
a

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.

Incompleteness of the blacklists

- Failed to detect?
- Never active/malicious?

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





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 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%





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%





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









Detecting and preventing domain name abuse in .eu

Lieven Desmet, KU Leuven – Marc Van Wesemael, EURid