DarkDNS: Revisiting the Value of Rapid Zone Update

RAFFAELE SOMMESE, GAUTAM AKIWATE,
ANTONIA AFFINITO, MORITZ MULLER,
MATTIJS JONKER, KC CLAFFY

RIPE 89 - DNSWG – PRAGUE - 30/10/24

ICANN CZDS

- With the expansion of new generic TLDs (gTLDs), ICANN **mandated** zone files to be accessible through a simplified and centralized process: ICANN's **Centralized Zone Data Service**.
- Covers most of the gTLDs approved by ICANN!
- Facilitated a lot of research in DNS resilience, infrastructure and abuse.
- However,.....is one snapshot a day enough?!

ICANN CZDS

- With the expansion of new generic TLDs (gTLDs), ICANN **mandated** zone files to be accessible through a simplified and centralized process: ICANN's **Centralized Zone Data Service**.
- Covers most of the gTLDs approved by ICANN!
- Facilitated a lot of research in DNS resilience, infrastructure and abuse.
- However,.....**is one snapshot a day enough**?!

The problem of snapshots

Sunday, June 23, 2024, 6 PM

Monday, June 24, 2024, 6 PM

The problem of snapshots

Sunday, June 23, 2024, 8:54 PM

The need of more granular real-time data

Quickly detecting newly registered domains (i.e., for DNS Abuse detection)

DNS Hijacking detection

Live DNS infrastructural changes

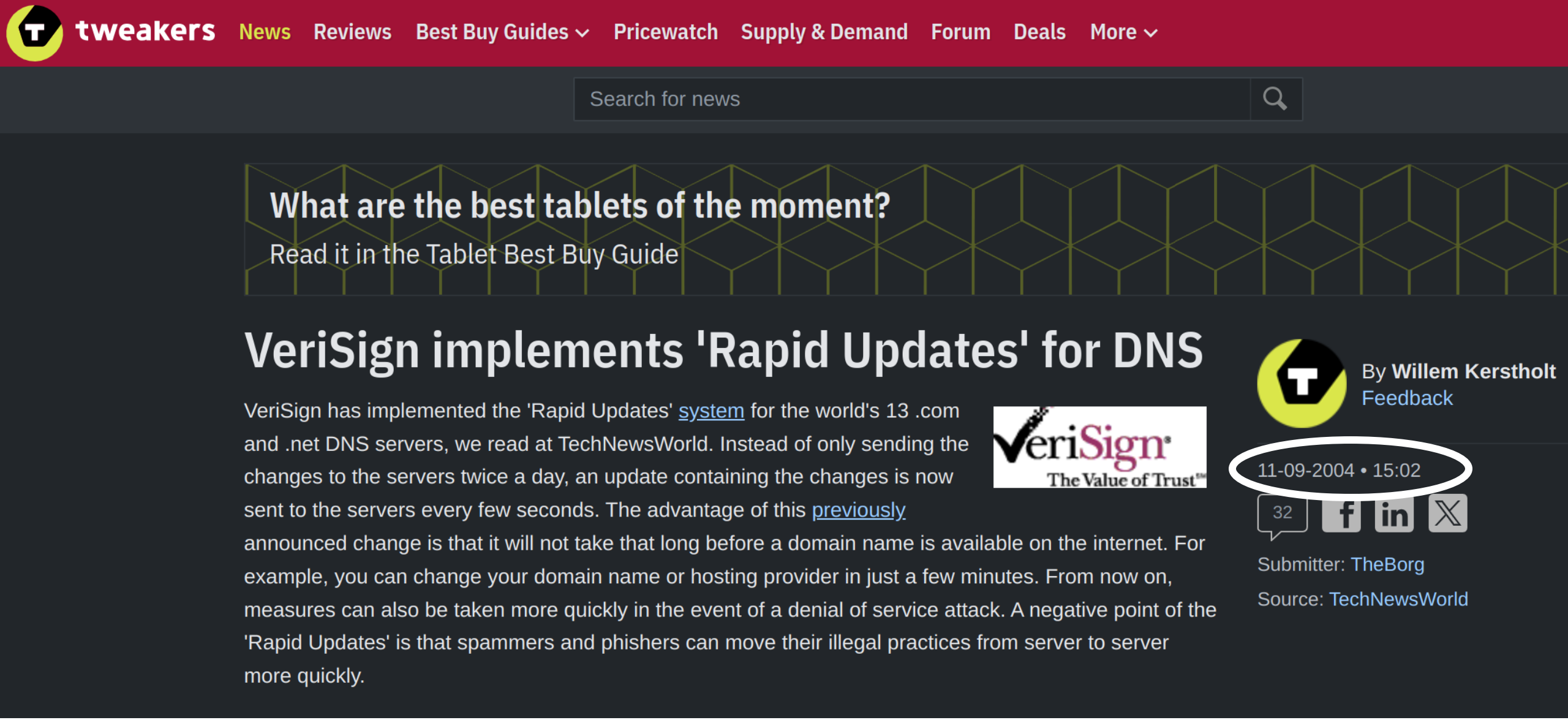
‘Short, Brutal Lives’: Life Expectancy for Malicious Domains

October 1, 2018 TH Author 0 Comments

Using a cooling-off period for domain names can help catch those registered by known bad actors.

Domain Name System (DNS) pioneer Paul Vixie for more than three years has been calling for a “cooling off” period for newly created Internet domain names as a way to deter cybercrime and other abuses. Domain names registered and spun up in less than a minute only encourage and breed malicious activity, he argues, and placing them in a holding pattern for a few minutes or hours can help vet them and catch any registered by known spammers and other bad actors.

Vixie — who is founder and CEO of threat intelligence firm Farsight Security — and his team have now taken an up-close look at the life cycle of new Internet domains, and their findings shine new light on the lifespan of malicious and suspicious domains. “Most of them die young, and most of them die after living short, brutal lives,” he says of newly created domains.



A blast from the past

10/28/2024

Alternatives?!

Passive DNS Data

- DomainTools Newly Observed Domain Names Feed (SIE NOD)

Limitations:

- Only "active queried" domains
- Commercial data source
- Limited availability

What else?

Alternatives?!

Passive DNS Data

- DomainTools Newly Observed Domain Names Feed (SIE NOD)

Limitations:

- Only "active queried" domains
- Commercial data source
- Limited availability

What else?

This Is a Local Domain: On Amassing Country-Code Top-Level Domains from Public Data

Authors: Raffaele Sommese,  Roland van Rijswijk-Deij, Mattijs Jonker | Authors Info & Claims

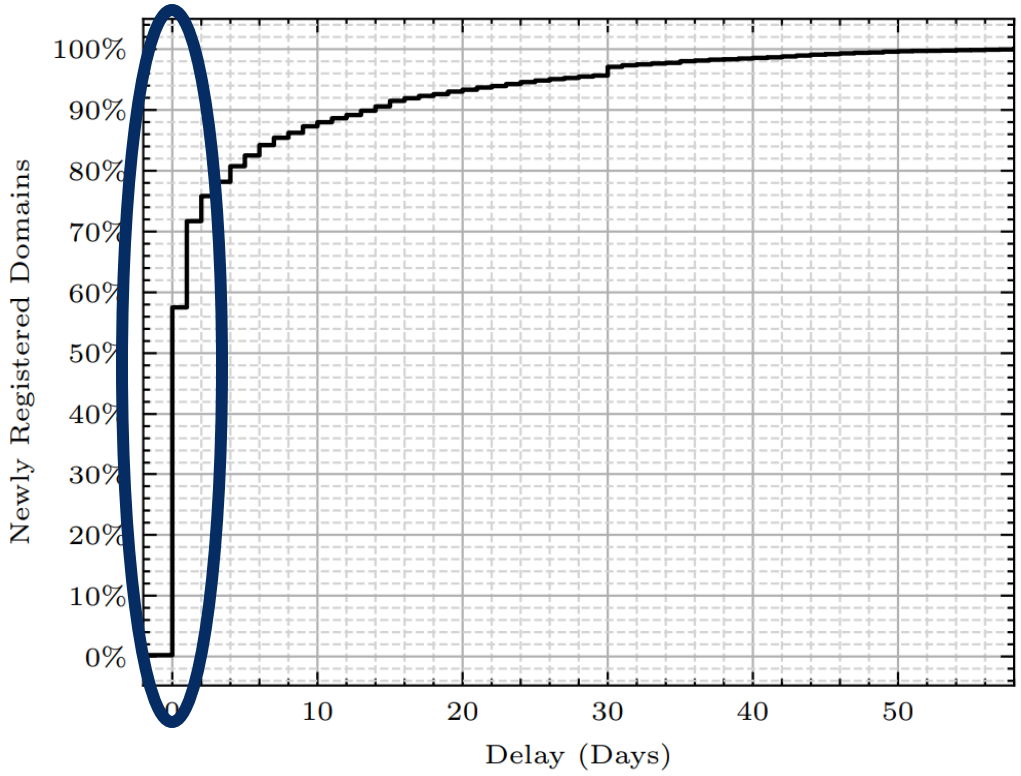
ACM SIGCOMM Computer Communication Review, Volume 54, Issue 2 • Pages 2 - 9 • https://doi.org/10.1145/3687234.3687236

We can learn ~half of second-level domains of a TLD from CT Logs!

This Is a Local Domain: On Amassing Country-Code Top-Level Domains from Public Data

Authors: Raffaele Sommese, Roland van Rijswijk-Deij, Mattijs Jonker | Authors Info & Claims

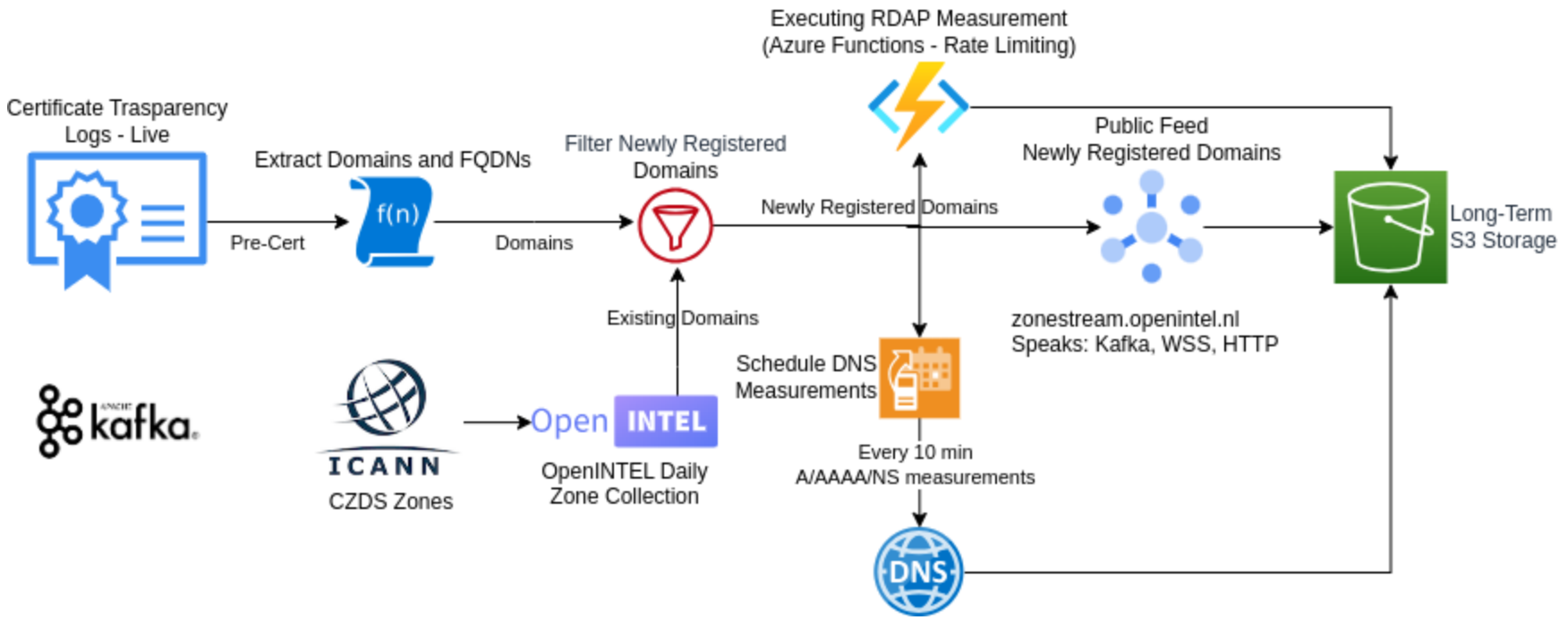
ACM SIGCOMM Computer Communication Review, Volume 54, Issue 2 • Pages 2 - 9 • https://doi.org/10.1145/3687234.3687236



Most of them in (**less than**) a day from registration!

Let's (quickly) discover: Newly Registered Domains

zonestream.openintel.nl



Newly registered domains

- We detected 42% of newly registered domains **before** they appeared in the CZDS snapshot.
- ~76K domains per day.
- Almost 1 domain per second.
- 1% of newly registered domains **never** appear in the next CZDS snapshot!

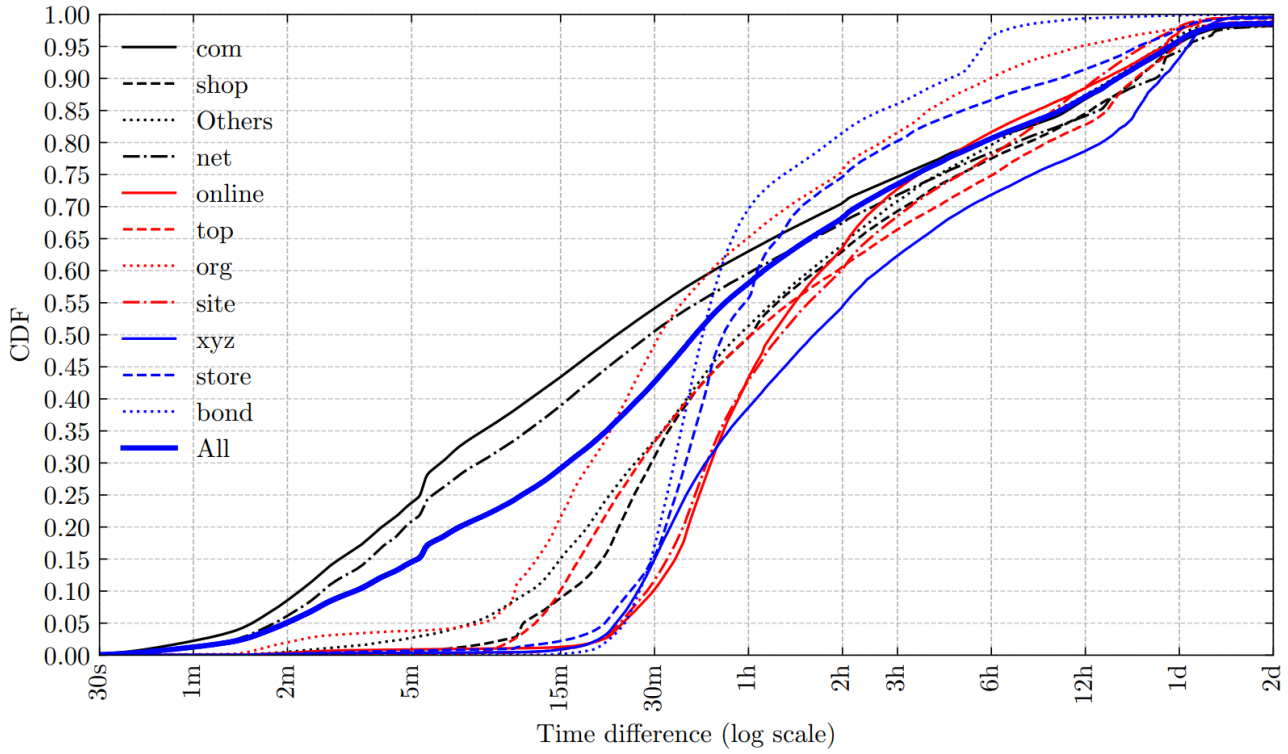
Newly registered domains

- We detected 42% of newly registered domains before they appeared in the CZDS snapshot.
- ~76K domains per day.
- Almost 1 domain per second.
- 1% of newly registered domains **never** appear in the next CZDS snapshot!

Quickly discovering

Compared to RDAP registration timestamp:

- 50% of newly registered domains detected **within 45 minutes** of their creation.
- ≈ 30% within 15 min.



In CT Logs, but never in CZDS

- Approximately 1% of the newly registered domains **never** appear in CZDS.
- Two main (possible) reasons:
  - Certificates issued for expired domains.
  - Domain lasting less than two zone snapshot interval -> **Transient domains**
- We used RDAP data to distinguish this two cases, finding **42K transient** domains over a 3-month period.
- **Invisible** so far to researchers!

In CT Logs, but never in CZDS

- Approximately 1% of the newly registered domains **never** appear in CZDS.
- Two main (possible) reasons:
  - Certificates issued for expired domains -> Let's not talk about this security nightmare
  - Domain lasting less than two zone snapshot interval -> **Transient domains**
- We used RDAP data to distinguish this two cases, finding **42K transient** domains over a 3-month period.
- **Invisible** so far to researchers!

In CT Logs, but never in CZDS

- Approximately 1% of the newly registered domains **never** appear in CZDS.
- Two main (possible) reasons:
  - Certificates issued for expired domains -> Let's not talk about this security nightmare
  - Domain lasting less than two zone snapshot interval -> Transient domains
- We used RDAP data to distinguish the two cases, finding **42K transient** domains over a 3-month period.
- **Invisible** so far to researchers!

Transient Domains

- Transient domains last at most 24 hours, half of them died within their **first 6 hours of life**.
- There are **few legitimate reasons** for this, most of these registrations are linked to malicious behavior as confirmed by prominent registrars.
- Reasons for early removal include **abuse**, account suspensions, or credit card fraud.
- **Blocklists** do not promptly or in some cases ever detect transient domains!
- And a missed opportunity for registries and registrars to share security warnings

Transient Domains

- Transient domains last at most 24 hours, half of them died within their **first 6 hours of life**.
- There are **few legitimate reasons** for this, most of these registrations are linked to malicious behavior as confirmed by prominent registrars.
- Reasons for early removal include **abuse**, account suspensions, or credit card fraud.
- **Blocklists** do not promptly or in some cases ever detect transient domains!
- And a missed opportunity for registries and registrars to share security warnings

Transient Domains

- Transient domains last at most 24 hours, half of them died within their **first 6 hours of life**.
- There are **few legitimate reasons** for this, most of these registrations are linked to malicious behavior as confirmed by prominent registrars.
- Reasons for early removal include **abuse**, account suspensions, or credit card fraud.
- **Blocklists** do not promptly or in some cases ever detect transient domains!
- And a missed opportunity for registries and registrars to share security warnings

Long-lived domains lookalike

- **Half** of these transient domains were using **Cloudflare** as DNS provider (i.e., for their authoritative nameservers) and ≈35% of them used Cloudflare as a CDN provider.
- Malicious actors are exploiting legitimate services for hosing content?!

Registrar	Domains	%
GoDaddy	8213	19.39%
Hostinger	6418	15.2%
NameCheap	4195	9.9%
Squarespace	2820	6.7%
Public Domain Registry	2625	6.2%
IONOS	2352	5.6%
Metaregistrar	1866	4.4%
NameSilo	1853	4.4%
Network Solutions, LLC	1670	3.9%
Tucows	1304	3.1%
Others	9042	21.3%
Total	42358	-

Table 3: Transient Domains Registrars Distribution.

What fraction of transient domains did we capture?

- We compared our transient domain feed with:
  - EPP transaction logs from .nl
    - Ground Truth, same idea of Rapid Zone Updates of .com, **non-public**
  - Newly Observed Domains from DomainTools
    - Passive DNS, **non-public**

Our detection vs EPP Ground Truth

- In 3 months, .nl registry observed 334 domains that were registered and deleted such that they were never captured in zone file snapshots.
- With our methodology, we found only 99 transient domains, or **29.6%** of the 334 .nl-identified transient domain names over a period of 3 months.
- Researchers and operators still have a huge blind spot regarding intra-day events.

Our detection vs EPP Ground Truth

- In 3 months, .nl registry observed 334 domains that were registered and deleted such that they were never captured in zone file snapshots.
- With our methodology, we found only 99 transient domains, or **29.6%** of the 334 .nl-identified transient domain names over a period of 3 months.
- Researchers and operators still have a huge blind spot regarding intra-day events.

Our detection vs DomainTools NOD

- DomainTools NOD feed detected in absolute numbers roughly 5% more domains than our methodology.
- However, the overlap between the two data sources was only ≈60%.
- ---> Each methodology provides additional, though incomplete, visibility into transient domains!

Our detection vs DomainTools NOD

- DomainTools NOD feed detected in absolute numbers roughly 5% more domains than our methodology.
- However, the overlap between the two data sources was only ≈60%.
- ---> Each methodology provides **additional**, though **incomplete**, visibility into transient domains!

Where next?

- The existence of transient domains is a measure of **success** in registrars detecting malicious domains in their early stages, before they can do damage.
- However, each registrar has to independently **relearn** the same signals as threat actors move across different registrars to evade detection.
- In the meantime, transient domains, in which malicious activity dominate, have been **invisible to researchers**.

Where next?

- The existence of transient domains is a measure of **success** in registrars detecting malicious domains in their early stages, before they can do damage.
- However, each registrar has to independently **relearn** the same signals as threat actors move across different registrars to evade detection.
- In the meantime, transient domains, in which malicious activity dominate, have been invisible to researchers.

Where next?

- The existence of transient domains is a measure of **success** in registrars detecting malicious domains in their early stages, before they can do damage.
- However, each registrar has to independently **relearn** the same signals as threat actors move across different registrars to evade detection.
- In the meantime, transient domains, in which malicious activity dominates, have been **invisible to researchers**.

A call to resurrect Rapid Zone Updates

- *"promote security and stability by providing a useful tool to online security companies, ISPs, search engines, financial services companies, and other stakeholders."* [RZU 2004]
- Due to the **ineffectiveness** of existing **uncoordinated** countermeasures, and the limited obligations of registrars to mitigate harm, we see a **need to expand transparency**.
- We can learn from history how to **mitigate the risk of abuse** of sharing data.
- CZDS represent a testament to the ability of managing this risks.

[RZU 2004] https://www.icann.org/en/system/files/files/memo-dns-update-service.pdf

A call to resurrect Rapid Zone Updates

- *"promote security and stability by providing a useful tool to online security companies, ISPs, search engines, financial services companies, and other stakeholders."* [RZU 2004]
- Due to the **ineffectiveness** of existing **uncoordinated** countermeasures, and the limited obligations of registrars to mitigate harm, we see a **need to expand transparency.**
- We can learn from history how to **mitigate the risk of abuse** of sharing data.
- CZDS represent a testament to the ability of managing this risks.

[RZU 2004] https://www.icann.org/en/system/files/files/memo-dns-update-service.pdf

A call to resurrect Rapid Zone Updates

- *"promote security and stability by providing a useful tool to online security companies, ISPs, search engines, financial services companies, and other stakeholders."* [RZU 2004]
- Due to the **ineffectiveness** of existing **uncoordinated** countermeasures, and the limited obligations of registrars to mitigate harm, we see a **need to expand transparency.**
- We can learn from history how to **mitigate the risk of abuse** of sharing data.
- The CZDS program represents a testament to the ability of managing this risk.

[RZU 2004] https://www.icann.org/en/system/files/files/memo-dns-update-service.pdf

SAC125: SSAC Report on Registrar Nameserver Management

The onus was placed on registrants to monitor….this approach has not proved practical….a growing understanding of the vulnerabilities….point toward a shift in the focus…..to a broader engagement involving registrars and registries, suggesting a **collaborative approach.**

5.2.4 Fine-grained visibility of changes to zone files.

- The DNS Transparency project – proposed many years ago but not yet deployed – would achieve the required level of transparency, allowing third parties to monitor changes to zones without inducing a vast number of active DNS queries on the Internet.

1. Internet Fire Brigade, Implement DNS Transparency v1.0 RFP. https://www.internetfire.org/projects/dns-transparency/rfps
2. For another example of DNS monitoring services, see DNS Check, Monitor DNS Records, https://www.dnscheck.co/monitor-dns-records

Help us to enable transparency

- How to navigate concerns of privacy and abuse?
  - System for Standardized Access/Disclosure (SSAD)
  - VIP Zones of trust?
- A call for action for **ccTLDs** to be an example of data sharing and collaborative effort in the fight for abuse!

DACS Design and Analysis of Communication Systems

Open INTEL

UNIVERSITY OF TWENTE.

Play with our data:

https://zonestream.openintel.nl

Full Paper

And reach us:

r.sommese@utwente.nl

kc@caida.org

RAFFAELE SOMMESE, GAUTAM AKIWATE,
ANTONIA AFFINITO, MORITZ MULLER,
MATTIJS JONKER, KC CLAFFY

caida

SIDN LABS

Stanford University