

CASE STUDY

When a Registrar Tackles DNS Abuse Head-On

Realtime Register takes the lead in developing threat intelligence-driven monitoring and mitigation of domain abuse

Growing Demand to Address DNS Abuse

DNS abuse is pervasive, happening on many technical levels and causing negative impacts beyond any specific sector, company, community, or user. While registrars *could* use a nuclear option to take a domain name fully offline, this option is often too blunt.

Increasing Prevalence

18M+ daily COVID-19 related malware & phishing emails

April 2020, Google



48K+ cases of typosquatting

March-June 2020, The World Intellectual Property Organization



Advancing DNS Abuse Policy & Research

As a member of the ICANN community, Realtime Register proactively engages in security and regulatory discussions, contributing to important initiatives targeting online abuse. In 2019, the team committed to dedicating resources and setting priorities to better investigate the technical levels underlying DNS abuse and guide policy to combat it.

One resulting project was the development of faster, on-demand monitoring and intelligence sharing within Realtime Register's ecosystem of partners and registrars.






KEY INFORMATION



Realtime Register is the leading independent wholesale registrar domain-management-as-a-service company.

Based in the Netherlands and with 15+ years in business, Realtime Register offers a platform enabling uniform, on-demand registrations of domain names. The company supports over 1,000 active resellers in 100+ countries, managing millions of domains at any given time.

Pulsedive features used:

-  Ingest **Heavy Duty Feed** with all risk levels, active and retired domains and URLs
-  **Submit** new IOCs for enrichment and evaluation
-  Ad-hoc **scanning** via API
-  **Pivoting** to research risky IOCs
-  Assess various intelligence sources for **fidelity and relevance** to DNS abuse

“ Ingesting Reputation Blocklists (RBLs) is easy. Making this data **visible** and **meaningful** to our customers is a very different story.”

- Theo Geurts, Privacy & GRC Officer, Realtime Register

CASE STUDY

When a Registrar Tackles DNS Abuse Head-On

Seeking: Meaningful Data for an Intuitive Platform

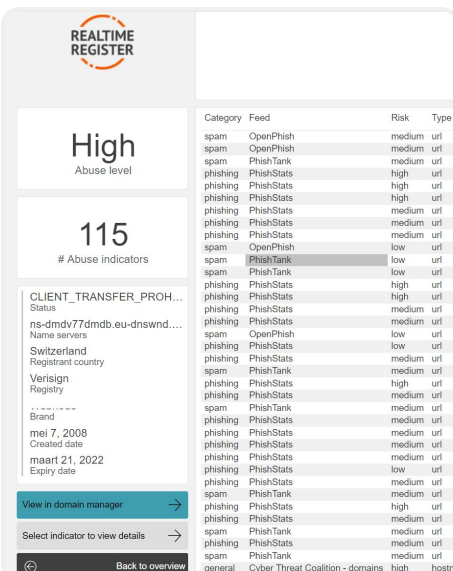
Led by CTO Wiebren Braakman, the Realtime Register team defined key requirements for various external vendors: collecting and processing data sources, performing on-demand enrichment, and supporting an easy-to-use platform accessible to all of Realtime Register’s customers.

For the intelligence component, third party providers would help distribute timely, detailed, and reliable information to help take precise actions on DNS Abuse incidents. Considerations included:

- ▶ **Quality intelligence** and contextual data related to domain abuse
- ▶ **Enrichment** of new domains and URLs discovered through internal research
- ▶ **Easy, custom integrations** with unique in-house tools
- ▶ **Multiple trusted intelligence sources** with visibility into source context
- ▶ **Partnership alignment**, without legal or licensing issues for data use within the platform
- ▶ **Additional investigation pathways** for customers, typically hosting companies or ICANN registrars, after discovering DNS Abuse in the Realtime Register Abuse Insight Platform

Building Intelligence Flows In and Out

Moving forward with Pulsedive, Realtime Register maximized value by implementing Pulsedive’s functions bidirectionally - sending new data in while also extracting enriched intelligence out.



Automating Heavy Duty Feed. Realtime Register parses and extracts the most relevant domain name and URL information via a scheduled daily ingestion of Pulsedive’s Heavy Duty Feed.

On-Demand API Enrichment. When the team discovers potentially malicious domain names, Realtime Register conducts ad-hoc enrichment through the Pulsedive API to pull back more comprehensive contextual data for additional research.

Allowing Users to Dive Deeper. Domains and URLs in the Realtime Register dashboard are linked directly to Pulsedive’s community platform, so customers can rescan indicators on demand through Pulsedive’s free interface. Users can also explore and pivot further using additional context not typically available on RBLs.

“ Realtime Register is now differentiated as an ICANN registrar with our **detailed abuse statistics** for domain names under management. This allows us to zero in on large incidents, effectively **taking action together with our customers.**”

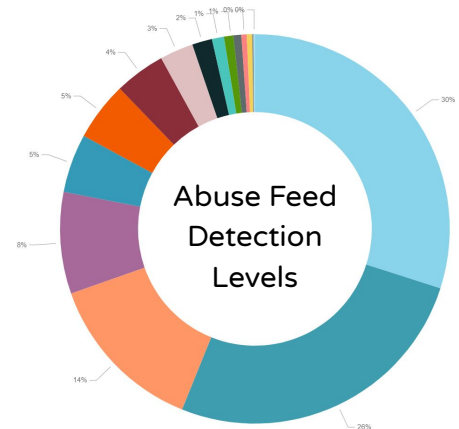
- Berend van Dalzen, CEO, Realtime Register

CASE STUDY

When a Registrar Tackles DNS Abuse Head-On

Zeroing in on Insights

Until Realtime Register began using Pulsedive, the team was not fully aware of how cybercrime operations would leverage their customers’ technical infrastructure. Enrichment of freshly submitted domains and URLs into Pulsedive, and then ingesting Feeds in the Realtime Register Abuse Insight Platform provided new layers of timely insight. With these findings, customers could focus on security hardening efforts within their own platforms.



Key Results

Timely, Quality Intelligence - in Bulk

When combating malware, accuracy and speed are of the essence.

Pulsedive helps Realtime Register pinpoint which RBL feeds are most useful on a daily basis. This allows Realtime Register to expand on custom functionality and notifications within the Realtime Register system for highly relevant feeds, such as *Abuse.ch*.

Informed Mitigation

Using this iterative model supports Realtime Register’s strategy for what to do next.

Realtime Register is now differentiated as an ICANN registrar with their level of detailed abuse statistics for domain names under management. The team can now zero in on incidents, acting on and mitigating the situation together with their customers.

Continuous Monitoring

Realtime Register was able to identify that DNS Abuse in their ecosystem was low - finding average abuse levels at 0.04%.

With ongoing daily monitoring, it is beneficial to benchmark measurements, continuously review abuse levels over time, and research further by categorizing abuse types, sources, and other key characteristics.

Understanding the Next Step

One major surprise was that 98% of all abuse is not actionable as a registrar, given the many technical layers involved.

As the nuclear option is often too blunt to address the multi-faceted issues that play out on a hosting/content level, revealing the prevalence of abuse clarified the need for additional mitigation measures.

CASE STUDY

When a Registrar Tackles DNS Abuse Head-On

Success by Collaboration: Shared Intel In, Improved Intel Out

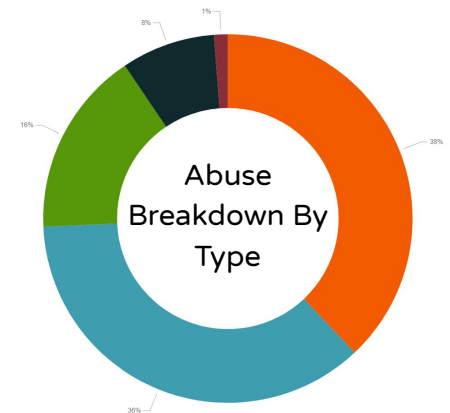
The Pulsedive and Realtime Register relationship extends beyond conventional threat intelligence platform use and feed ingestion. Realtime Register, with its unique access to domain registration monitoring and activity, provides Pulsedive with large sets of timely, unique data not otherwise found in the open source threat intelligence landscape.

In turn, the Realtime Register team benefits from instant, on-demand contextualization and risk assessment, as well as the implementation of new, high-fidelity sources without a need to maintain or update integrations by their in-house team.

What's Next: Scaling the Platform

Realtime Register is in the process of educating and onboarding all customers to the free Realtime Register Abuse Insight Platform.

Since kicking off the project, the team has introduced three new projects to enhance detection of domain name abuse, slated to launch in the coming year. A step ahead of new ICANN initiatives, laws, and regulations, the platform will grow in usage and maturity as the industry response to DNS Abuse continues to develop.



“With the new domain abuse detection projects we’re working on, I am looking forward to submitting our results to the Pulsedive Platform and Feed, so everyone in the community can benefit from shared intelligence.”

Theo Geurts, Privacy & GRC Officer, Realtime Register

Feed

[Learn More](#)

[Upgrade](#)

A configurable CSV of vetted threat intelligence.

High-fidelity, timely threat intelligence is critical to reducing false positives and prioritizing alerts effectively. The Pulsedive Feed streamlines cyber threat intelligence ingestion by replacing 30+ feed parsers and configurations with just one. Every domain, IP, and URL is enriched with real-time scanning, adding valuable context for further investigation.

Pulsedive Feed is trivial to configure and solution agnostic, making it easy to take advantage of.