ONDOMAIN by RED SIFT

STOP PHISHING ATTACKS BY DISARMING LOOKALIKE DOMAINS ON DAY ZERO

For threat intelligence specialists who need to protect their domain perimeter, Red Sift offers OnDOMAIN, a cybersecurity solution that finds and uncovers impersonation domains in real-time.

Relentless attacks

20 seconds

A new phishing website is published and goes live every 20 seconds[1]

The dark side of security

82%

On average, 82% of phishing websites are encrypted by SSL[2]

Overwhelming volume

364.6M

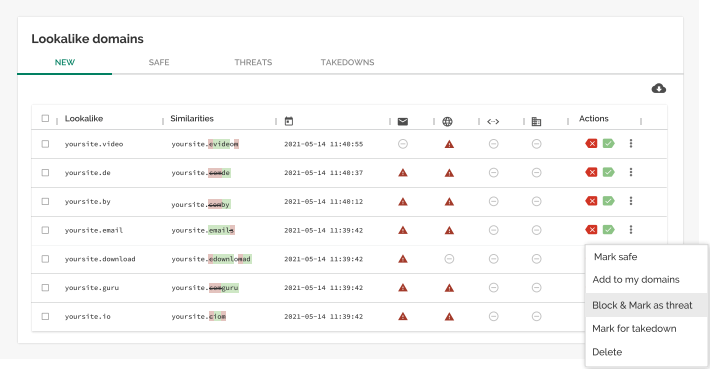
Q3 of 2021 closed with 364.6 million domain name registrations across all top-level domains[3]

OnDOMAIN enables Security personnel to quickly shut down phishing sites, discover and secure legitimate domains that have been forgotten about, and defend their brand against abuse and reputational damage.

Uncover

Unlike other domain monitoring products that only look at top-level domains (TLDs), OnDOMAIN monitors subdomains too. Any parked, forgotten, and impersonation domains are uncovered, and no stone is left unturned.

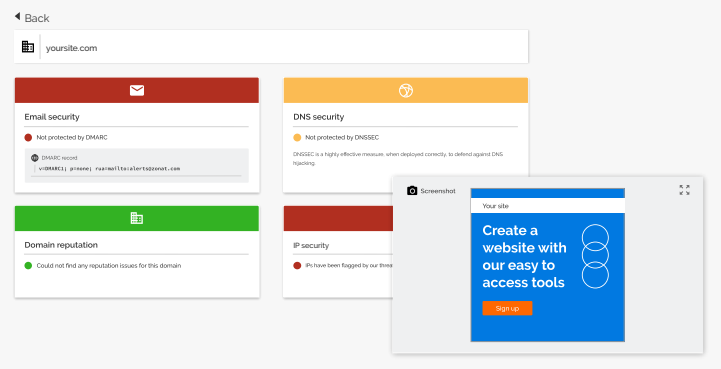
- **Domain discovery** We monitor 100-150 million domains and subdomains a day.
- ***SpatialMatch*** Checked against your assets using *SpatialMatch*, our innovative ensemble of GPT-3 with bigram-based multidimensional analysis instantly finds similarity in very large data sets.
- **Asset definition and scanning** Upload domain names and company logos to define your perimeter and visualize your brand estate.



Investigate

OnDOMAIN constantly absorbs and examines intelligence from a wide array of data sources to paint the full picture of a domain's health and validity. This includes rasterized web snapshots, certificate registration, DNS signals, live spam data, and web content with a history of changes available for analyst review.

- **Machine vision-based logo detection** Scans the web for both legitimate and illegitimate use of an organization's brand assets.
- **Domain screenshots** See screenshots of any impersonation domains in question.
- **WHOIS data** Monitor and log DNS changes, certificate validity, and other key domain parameters.



Ready to secure lookalike domain threats beyond your perimeter?

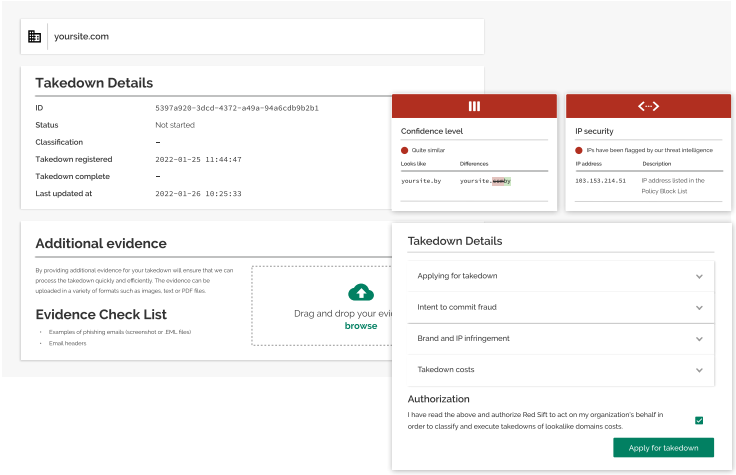
CONTACT US

RED SIFT

Takedown

Remove any doubt about attacks in their preparation phase using evidence gathered by OnDOMAIN in real-time. Sort threats by their imminence, save time with event-driven alerts, and issue one-click takedown notices once an impersonation domain has been identified.

- **Visibility into takedown status** Progress of the takedown can be easily monitored through a single pane of glass.
- **Speedy detection and takedown** OnDOMAIN's takedown service leverages existing relations with registrars and hosting providers to quickly effect domain takedown.



OnDOMAIN streamlines the SecOps triage process

Research shows that 61% of companies with IT departments say they would benefit from additional technology for managing alerts[4], such as automated SIEM alert triage with actionable insights. OnDOMAIN supports the capacity and information overload problem that exists for teams trying to stay on top of protecting their domain perimeter.

We solve this by giving users the context they need to take action and minimize time spent investigating suspicious activity. OnDOMAIN also integrates with your SIEM and SOAR in order to push relevant, actionable signals to SecOps teams for fast and efficient response.

Red Sift's interoperable cybersecurity platform

OnDOMAIN is the latest addition to the award-winning Red Sift cybersecurity suite. It integrates with OnINBOX for automated supply-chain analysis and OnDMARC for a detailed view of your existing domains. This means that data and processes can be shared across different branches of IT and Security departments, providing organizations with layered, enterprise-level threat protection.

Find out how you can combat domain impersonation and protect the threats beyond your perimeter.

CONTACT US

Crown Commercial Service Supplier

Member CyberExchange

Member of Microsoft Intelligent Security Association Microsoft

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

[1]*The SSL Store Blog 2020* [2]*APWG Trends Report Q2 2021* [3]*Verisign Domain Name Industry Brief Q3 2021* [4]*Sumo Logic 2020 State of SecOps and Automation Report*

RED SIFT

Red Sift enables security-first organizations to successfully communicate with and ensure the trust of their employees, vendors and customers. As the only integrated cloud email and brand protection platform, Red Sift automates BIMI and DMARC processes, makes it easy to identify and stop business email compromise, and secures domains from impersonation to prevent attacks.

Founded in 2015, Red Sift is a global organization with international offices in the UK, Spain, Australia, and North America. It boasts a client base of all sizes and across all industries, including Wise, Telefonica, Pipedrive, ITV, and top global law firms. Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at redsift.com.

redsift.com
contact@redsift.com
@redsift

v2.1 | Feb 22