

# 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<sup>1</sup> The dark side of security

82%

On average, 82% of phishing websites are encrypted by SSL<sup>2</sup> Overwhelming volume

364.6M

Q3 of 2021 closed with 364.6 million domain name registrations across all top-level domains<sup>3</sup>

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.

#### Lookalike domains 6 Lookalike Similarities 1 yoursite.video yoursite.evideom 21-05-14 11:48:55 yoursite.de 2821-05-14 11:48:37 🛛 💌 yoursite.cemde . . voursite.bv 2821-05-14 11:48:12 . . 🛛 🖸 🔅 yoursite.email yoursite.emails 2821-05-14 11:39:42 . A 🛛 🖸 🔡 Mark safe \_\_\_\_\_yoursite.dow 2821-05-14 11:39:42 . yoursite.edownlowad Add to my domain yoursite.guru rsite.<mark>cem</mark>guru 2821-05-14 11:39:42 ▲ Block & Mark as threat 2821-05-14 11:39:42 yoursite.io ursite.<mark>cion</mark> Mark for takedown Delete

#### 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.

	⑦	
mail security	DNS security	
Not protected by DMARC	Not protected by DNSSEC	
DMARC record vubsult[] preset rearmailteralertstores.com	DNSSEC is a highly effective measure, when deployed co hijacking.	
<b>a</b>	Ser	Your site
iomain reputation	IP security	Create a website with
Could not find any reputation issues for this domain	IPs have been fagged by our threat	our easy to access tools

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.

D	5397a920-3dcd-4372-a49a-94a6cdb!	36261		<>
Status	Not started	Confi	dence level	IP security
Classification	-		e similar	Ps have been flagged by our threat intellig
lakedown registered	2022-01-25 11:44:47	Looks L		IP address Description
l'akedown complete	-	yours	te.by yoursite	183.153.214.51 P address listed in th
.ast updated at	2022-01-26 10:25:33			Policy Block List
		Та	kedown Details	
process the takedown quickly and ef	our takedown will ensure that we can ciently. The evidence can be		kedown Details	
ly providing additional evidence for rocess the takedown quickly and of plaaded in a variety of formats such	our takedown will ensure that we can clerith. The evidence can be as images, last or PDF files.	Drag and drop your evit		 
By providing additional evidence for	our Jakedown will ensure that we can an images, lead or POF Res. k List [] [] [] [] [] [] [] [] [] [] [] [] []	Drag and drop your evi browse	pplying for 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<sup>4</sup>, 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 supplychain 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













<sup>1</sup>The SSL Store Blog 2020

<sup>2</sup>APWG Trends Report Q2 2021

<sup>3</sup>Verisian Domain Name Industry Brief Q3 2021 <sup>4</sup>Sumo Loaic 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