OpSec

Secure · Enhance · Protect

DATASHEET

Early Warning System

Daily intelligence reporting of confusingly similar domain registrations, SSL certificate creations on hostnames, and more, related to your brands.

Updated: July 22 2020

The OpSec Online AntiFraud Services provides preventative intelligence, detection, and mitigation of fraudulent phishing attacks targeting specific brands. Phishing sites using SSL certificates have increased to over half of all detections.

Early Warning System

OpSec Online's Early Warning System (EWS) is a daily intelligence report providing new domain registrations plus associated DNS records, dropped domain registrations, and SSL certificate creations associated with identified brand keywords. This powerful tool delivers actionable intelligence brand owners can use to protect their organization from targeted phishing, spearphishing, and business email compromise (BEC) type of attacks that commonly target corporate employees. Further, monitoring for SSL certificate creations provides insights on both domain names and hostnames that may be used for phishing scams or some other nefarious, false brand association scheme.

How it works

New Domain Registrations

New domains are registered and dropped every day using confusingly similar brand names:

Brand domain name misappropriation is typically due to:

- Malicious, fraudulent intent,
- Traffic diversion purposes, or
- Benign, non-threatening motives.

Common brand misuse typosquats: **Paypa1.org**, **G00gle.biz**, **rnicros0ft.com**.

OpSec Online harvests registrations daily from legacy and new gTLD registries.

.com	.biz	.org	.work
.club	.xyz	.net	.info

Some registries allow for harvesting real-time registrations.

SSL Certificates

A SSL certificate on a website can provide a false sense of security if the SSL certificate is created by a threat actor.

Certain Certificate Authorities offer 90-day Domain Validation certificates at no charge. Threat actors have been taking advantage of this promotion to trick victims into believing their websites are valid.

In reality, Domain Validation SSL certificates only encrypts data submitted to the site directly to the domain owner.

SSL certificates are created through organizations called Certificate Authorities (CA).

Variations can include hostnames with multiple subdomains, legacy and new gTLDs, and ccTLDs, plus both old and new domain registrations.

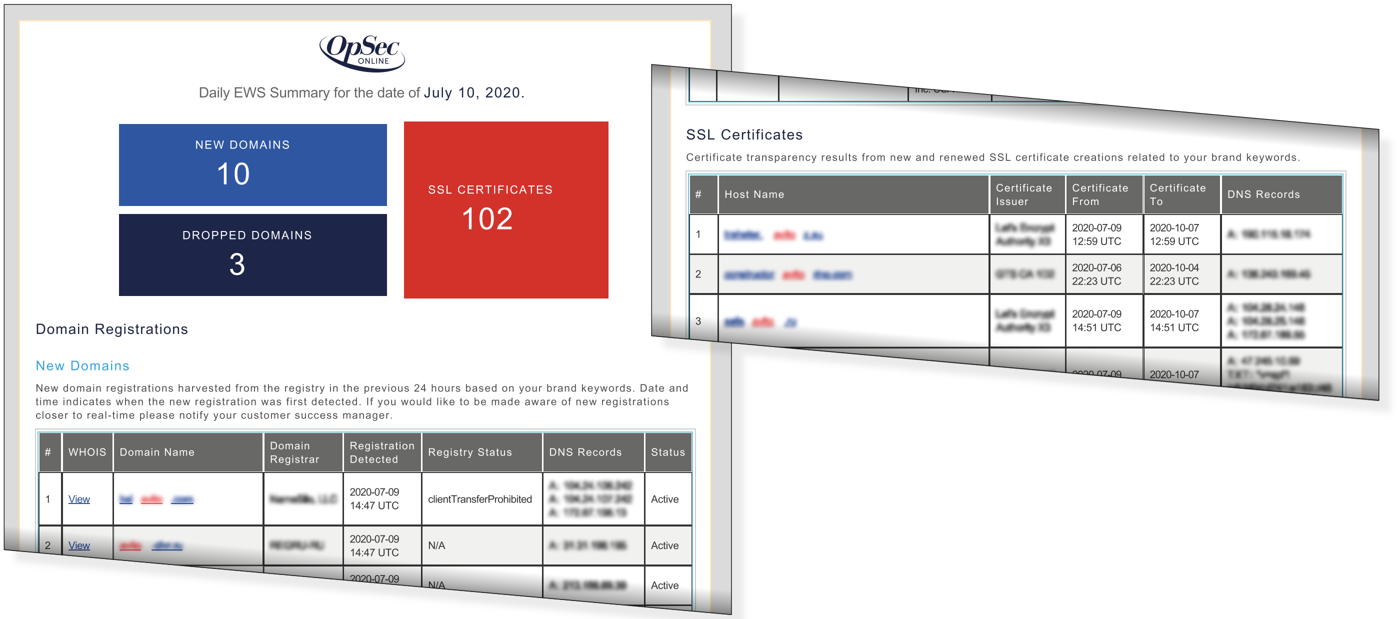
OpSec Online harvests the hostnames where new SSL certificates have been created.

13:27
https://domain.cctld
https://host.name.gtld
https://www.domain.tld
OpSec
Secure · Enhance · Protect

The AntiFraud Security Operations Center (SOC) reviews the results for phishy content.

A summary email is sent to designated contacts every day with the newest results. More frequent alerts are also available.

EWS results are also pushed to the customer online portal.



Daily EWS Summary for the date of July 10, 2020.

NEW DOMAINS
10

DROPPED DOMAINS
3

SSL CERTIFICATES
102

Domain Registrations

New Domains

New domain registrations harvested from the registry in the previous 24 hours based on your brand keywords. Date and time indicates when the new registration was first detected. If you would like to be made aware of new registrations closer to real-time please notify your customer success manager.

#	WHOIS	Domain Name	Domain Registrar	Registration Detected	Registry Status	DNS Records	Status
1	View	[redacted]	[redacted]	2020-07-09 14:47 UTC	clientTransferProhibited	[redacted]	Active
2	View	[redacted]	[redacted]	2020-07-09 14:47 UTC	N/A	[redacted]	Active
				2020-07-09	N/A	[redacted]	Active

SSL Certificates

Certificate transparency results from new and renewed SSL certificate creations related to your brand keywords.

#	Host Name	Certificate Issuer	Certificate From	Certificate To	DNS Records
1	[redacted]	[redacted]	2020-07-09 12:59 UTC	2020-10-07 12:59 UTC	[redacted]
2	[redacted]	[redacted]	2020-07-06 22:23 UTC	2020-10-04 22:23 UTC	[redacted]
3	[redacted]	[redacted]	2020-07-09 14:51 UTC	2020-10-07 14:51 UTC	[redacted]
			2020-07-09	2020-10-07	[redacted]

Key Features

- Daily summary of new and dropped gTLD domain registrations, registrar, registry status, and DNS records (if available)
- SSL certificate reporting includes new creations, date created and expiration date, the certificate issuer and associated DNS records
- SSL certificate results include hostnames, including subdomains and domains, and ccTLDs
- Alerts available as often as every 2 hours when there is new data to report, and in real-time when using the OpSec Online API for results

Recommended Best Practices

- Divert incoming emails from lookalike domains directly to the organization's IT Security team for review
- Monitor suspicious results for future fraudulent activity
- Share intelligence with trusted partners to ensure they are following best practices in validating invoicing or changes in payment procedures

Threat Intelligence Improves Protection

The OpSec Online Early Warning System is a powerful layer of intelligence that is essential to any corporate anti-phishing and brand protection strategy. In monitoring brand domain misuse and new brand-associated SSL certificates, an organization has the ammunition to more comprehensively shield their employees, customers, and partners from fraudulent phishing attacks.

About OpSec

For nearly forty years, brands, institutions, and governments around the world have relied on OpSec to ensure the integrity of goods and documents. In a world of rising fraud and black-market alternatives, we are the layer of truth that powers revenue-generating relationships. This is only possible through a unique combination of proven security experience, deep industry expertise, the market's broadest range of solutions, and a commitment to digital and physical integration leadership. For brands that depend on sustained relationships with customers, OpSec secures integrity, enhances loyalty, and protects revenue. For more information please visit **www.opsecsecurity.com.**

OPSEC WORLDWIDE OFFICES

The Americas
Boston, MA, USA
Lancaster, PA, USA
San Francisco, CA, USA
Meridian, ID, USA
Santo Domingo, DOM

Europe
London, GBR
Leicester, GBR
Washington, GBR
Munich, DEU
Santa Venera, MLT
Vilnius, LTU

Asia
Kowloon, HKG
Shanghai, CHN
Beijing, CHN
Tokyo, JPN

OpSec
Secure · Enhance · Protect

www.opsecsecurity.com