Typosquatting protection

Skurio analyst services

Identify threats to your brand with tailored threat analyst services

Typosquatting, also known as URL hijacking, uses a fake domain to make money or harm your business. The attacker registers a domain that closely resembles your website address. Then URL can then be used to host malicious content and / or send emails to targets. Depending on the objectives of the attackers, they may:

- Send phishing emails
- Produce a website mimicking the legitimate site to harvest personal details
- Distribute Malware
- Negatively impact the reputation of your business or an individual targeted within your business

Early warning and ongoing monitoring of typosquatted domains allows you to pre-empt potential attacks and establish counter measures to minimise or neutralise the threat.

Use Skurio Analyst services to provide typosquatting protection for your brand or VIPs.

Protect your brand or VIPs from impersonation or exploitation.

Key activities

Skurio Intelligence Analyst Services give you early warning and ongoing monitoring of typosquatted domains so you can pre-empt potential attacks and establish counter measures to minimise or neutralise the threat from typosquatting domains. Analyst activies provided with this service are described below. Chose form the standard or advanced service pack to meet your needs. All activities described in the standard pack are also included the advanced.

Standard

- Maintenance of brands or VIP list for on-going domain registration monitoring.
- Assessment of new domains to determine threat level and provide appropriate advice.
- Investigations and site takedowns can be requested at additional cost.

Advanced

- Additional processing activities including detailed threat investigations.
- Maintain a watchlist for daily check of the most high-risk domains.
- Maintain a watchlist for daily check of the most high-risk domains.
- Site takedown of malicious websites and/or content.

Deliverables

Standard

- Weekly report detailing newly registered domains with their corresponding risk score.
- Monthly summary report.

Advanced

- Daily notification of newly registered domains which indictate a potential threat (Mon-Fri)
- Investigation reports of suspicious domains including notification of status changes.

Engagement details

- Skurio will work with you to identify brand names / terms / or VIP names which require protection.
- Service costs will depend on the number of protected terms.
- Reporting information will be disseminated to the client via a secure client specific SharePoint site.

The Skurio Intelligence Analyst Team

- Our world-class team of intelligence analysts are truly experts in their field. They're the ideal team to supplement your internal staff whether providing scheduled services or incident response help when you need it most.
- Skurio analysts have backgrounds in service and government agency threat hunting as well as expertise in helping commercial and not-for-profit organisations with information security. You're in safe hands.

For more information or to request a demo:
Call +44 28 9082 6226 | sales@skurio.com | skurio.com