SKURIO ANALYST SUCCESS STORIES

DOMAIN MONITORING

Identifying malicious domains

SKURIO

Situation

Threat actors heavily exploit domain registrations to achieve a desired end goal. The end goal can include:
- Exploitation of a business name.
- Impersonation websites used for phishing and other malicious activity.
- A mail exchange to create phishing campaigns as a step to exploit a business.

Task

The Skurio Intelligence Analyst team were tasked with providing ongoing domain monitoring activities in order to identify malicious domains.

Action

The team created typosquatting alerts and reviewed results daily to identify domain registrations with similarities to the customer's brand. The analysts examined the content of domains to determine if there was any malicious intent. The team identified phishing websites, copyright infringements, trademark infringements and malicious mail servers.

Result

We now provide a weekly Intelligence Report to the customer detailing all the domains registered that are associated to their brand. Our report allowed the customer to conduct trend analysis to determine when they are more likely to be targeted. This has also allowed the customer to task our analyst team to conduct takedowns to mitigate the threat.