RiskIQ External Threat Detection: Domain Threats

As brands increasingly transact business and engage with customers through their website, having an advanced domain infringement detection strategy is critical. Threat actors can register domains using trusted brand names to drive monetizable traffic to other sites, phish for sensitive data, distribute malware, sell counterfeit goods, and more.

RiskIQ Domain Threats detects the unauthorized use of brands within third-party registered domain names and continuously monitors their site content and behavior so organizations can prioritize infringements according to their brand impact and act quickly to protect itself and its customers.

RiskIQ's unique solution provides comprehensive detection of brand-related domains combined with the intelligent discovery of a brand's legitimate domain footprint to identify infringing domain names. Via our proprietary virtual-user technology, RiskIQ analyzes a brand's site content and behavior. Experiencing websites the same way that real users would ensures that we uncover malicious and fraudulent activities designed to elude detection by other detection methods.

Who Needs It?

Organizations like yours invest significant resources in designing, securing, and driving traffic to official websites to build and preserve customer loyalty and brand trust. However, these investments are undermined—and the security of the company and its customers threatened—when third parties register look-a-like domains containing the brand names, and variations and misspellings thereof, to divert users away from the legitimate site or sites.

Domain infringement targets a wide range of organizations with valuable data or strong public brand recognition, including:

- Financial institutions and payment providers
- Health insurance providers
- Internet and software companies
- Consumer brands
- Major media companies and news sources
- Government agencies
- E-commerce companies

Why Do They Need It?

Third-party actors may use infringing domains for relatively benign purposes, such as siphoning user traffic to a competitor, generating ad revenue on a parked page, or offering to sell the domain names to the organization for a profit. But infringing domains can also be used for more malicious purposes such as:

- Impersonating a brand to phish employees and customers for sensitive information or linking to phish pages using infringing domains
- Undermining marketing efforts by competing with authentic websites and confusing consumers
- Using a trusted brand name to lure users to malware infected sites
- Associating a brand with offensive or illegal content
- Violating domain name usage policies thus exposing the organization to increased risks or representing the brand in unauthorized manner

What Does RiskIQ Domain Threats Do, Exactly?

Comprehensive Domain Infringement and Threat Discovery

RiskIQ searches DNS zone files for exact matches to branded terms or close spelling variants within domain names not belonging to an organization. Our proprietary discovery technology automatically maps out an organization's websites and infrastructure and more accurately distinguishes legitimate sites from third-party registrations—even those falsely claiming brand association in their WhoIs data. The result is more accurate risk identification and fewer false positives for company-owned domains.

After identifying an infringing domain, RiskIQ's unique virtual user crawling infrastructure intelligently analyzes the website associated with it. The virtual users detect brand references, logos, and other site content, and experience any malicious redirect and other illicit behaviors from multiple geographic locations and browser types—just as a real human user would. This provides the additional context needed to determine how threat actors may be using each domain and the risk it poses to the associated organization. Unlike other domain infringement solutions, RiskIQ Domain Threats offers:

- Detect brand impersonation, traffic diversion, phishing, malware distribution, and other types of abuse occurring on infringing domains
- Continuously monitor evolving threats over time and create granular policy controls around site metadata, behavior, and page content to group and prioritize infringements
- Intelligently sort company-owned domains and legitimate web pages from infringement and fraud for more accurate recognition of threats

- Automatically contextualize threats with knowledge of related incidents to gain insight into how criminals are using an infringing domain and how to stop them

Contextualization of Domain Threats Across All Digital Channels

Effective security and fraud prevention strategies cannot treat domain infringement independently from other digital channels. Threat actors use the interconnectivity of today's digital world to increase their reach by using multiple channels to conduct their work. Cross-promoting their attack vectors across web, mobile, and social channels through links and redirects maximizes each attack's impact and can obfuscate the role of an infringing domain within a larger attack. Solutions looking at domain threats in isolation cannot contextualize the full extent of the threat.

As a leading provider of security services for phishing, malware, mobile application, digital ad-based, and social media threats, RiskIQ is uniquely positioned to provide security teams with an enhanced perspective to domain threats and unparalleled visibility into threats impacting a brand and its customers across all digital channels through a single pane of glass.

Remediation

RiskIQ enables customers to quickly respond to actionable alerts, contact appropriate parties to remove, locate, and take down any infringing domains, and minimize organizational and customer impact.

Continuous monitoring lets users know about successful threat remediation, and RiskIQ's post-resolution monitoring re-opens events and informs users of threats posing recurring risks to their organization.

Scales With Your Needs

As new gTLDs expand the size of the domain world, it becomes more and more difficult for organizations to maintain full visibility over their presence across the web and keep up with the malicious activities of hackers and cybercriminals seeking to exploit this complexity.

RiskIQ has developed an automated, highly scalable solution capable of continuously monitoring and analyzing domain infringement to identify and categorize risks in real-time. Only RiskIQ enables your brand to stay steps ahead of cybercriminals and discover threats from infringing domains before your customers do. Minimize and mitigate brand impact by empowering your organization to find, confirm, and take down domain infringements more quickly than before, without devoting resources to time-intensive manual domain monitoring.

What is the Workflow?

RiskIQ provides an easy-to-access online dashboard to investigate and respond to infringing domains. With full details in a quick snapshot, RiskIQ facilitates rapid incident review. For each incident or set of related incidents, a support analyst can take six actions:

1. Confirm and request enforcement
2. Dismiss as irrelevant
3. Mark for Review to determine appropriate response
4. Resolve and add to inventory of company-owned domains
5. Monitor as a potential future risk and alert on future changes and activities
6. Annotate: add notes, assign to a specified user to manage, email for follow-up or feedback, or tag with a set of custom labels for searching and reporting.

Reporting

RiskIQ provides an intuitive dashboard for monitoring and analyzing domain infringement events as well as enforcement efforts. You get:

- Executive summary reports and a snapshot of infringing domains that impact your organization worldwide
- Trends and benchmarks of domain protection improvements over time
- Custom reports and data drill-down with key metrics include:
  - Event generation time period
  - Current review status and status change history
  - Event uptime until resolution
  - Brands associated to events
  - Geographic distribution of events
  - Events by hosting organization

RISKIQ PROTECTS CORPORATE BRANDS AND THEIR CUSTOMERS ON THE INTERNET. The company combines a worldwide proxy network with synthetic clients that emulate real users to monitor, detect and take down malicious and copycat apps, drive by malware and malvertisements. RiskIQ is being used by leading financial institutions and brands in the US to protect their web assets, visitors, employees, and customers from security threats and fraud. To learn more about RiskIQ, visit www.riskiq.com.