groupsense

DATASHEET

DOMAIN ABUSE DETECTION & ALERTING

Protect your organization's brand from being compromised.

Domain fraud is a growing threat.

Fraud linked to domain names are an increasingly common threat to businesses. Domain abuse is when cybercriminals register domains for the intent of phishing, malware and/or botnets. Malicious domain registration is an easy and effective way for threat actors to steal credentials, divert website traffic and/or sell fraudulent products. Cybercriminals impersonate brands using spoofed domains which ultimately damages the brand's reputation for their own personal profit.

Domain abuse includes:

- Typosquatting
- Domain name registration under another Top-Level Domain (TLD)
- Replacing country code TLD's (ccTLD's)
- Using ccTLD's to replace .com or other general TLD's domains

Fraud linked to domain names is growing rapidly. According to a study undertaken by WIPO (World Intellectual Property Organization), the number of suits related to domain names increased by 12%*. Your organization's domain is an important digital asset and the business impact of it being misused or impersonated can be dangerous to your customers and reputation. Domain abuse can happen quickly and silently meaning early detection is the key to alleviate digital risk.

HOW IT WORKS

GroupSense logs new domain registrations every day across more than 1,000 generic and global Top-Level Domains ("gTLDs") and ccTLDs*, including.COM, .NET, .ORG and many more. Tens of thousands of new domains registered each day are then checked for similarities to legitimate Client domains, commonly known as "typosquatting," to identify lookalike domains of the type mostly used for phishing, social engineering and business email compromise (BEC) attacks. By request, GroupSense will contact the registrar and request the suspicious or malicious domains be taken down.

USE CASE

GroupSense detected a client-branded domain site that was actively harvesting customer data. At client's request, GroupSense successfully got the site taken down by the registrar.

BUSINESS IMPACT

- Revenue Loss
- Brand & Reputation Damage
- Operational/Business Disruption
- Increased Cyber Insurance Premiums
- PII Data Leaks
- Loss of Valuable Data
- Legal Consequences
- Customer/Employee Identity Theft
- Intellectual Property Loss

BENEFITS

- Save Time & Resources
- Reduce Risk & Stay Ahead of Emerging Threats
- Identify & Takedown Domain Attacks
- Detect Domain Impersonation
- Minimize Typosquatting
- Maintain the Reliability of Your Website

GROUPSENSE PROVIDES

- Assigned Threat Intelligence Analyst
- TraceLight™ Portal Access for Client Support
- Assigned Client Engagement Representative
- Custom Threat Actor Investigation & Reconnaissance
- Knowledge Base Articles & Reports for General Information

KNOWLEDGE IS POWER

When it comes to cybersecurity, knowledge is power and can make a difference in how you remediate the situation and what policies are impacted. GroupSense helps you prepare, and respond, instead of reacting to an attack.

THE GROUPSENSE DIFFERENCE

GroupSense blends technology with people to deliver better threat intelligence. With GroupSense, you gain seamless integration into both your security and business processes to give you the maximum flexibility in support of your threat program. GroupSense's Tracelight™ platform is a highly automated, cloud-based infrastructure that performs advanced, real-time data collection from the surface, deep and dark webs on behalf of clients. The platform provides GroupSense analysts a centralized threat profile creation function that is then utilized to passively collect and analyze data from millions of sources. With GroupSense, you combine powerful technology with human expertise.

ABOUT GROUPSENSE

GroupSense is a digital risk protection services company that delivers customer-specific intelligence that dramatically improves enterprise cybersecurity and fraud-management operations. Unlike generic cyber-intelligence vendors, GroupSense uses a combination of automated and human reconnaissance to create finished intelligence that maps to each customer's specific digital business footprint and risk profile. This enables customers to immediately use GroupSense's intelligence to reduce enterprise risk, without requiring any additional processing or management by overstretched security and fraud-prevention teams.

GroupSense is based in Arlington, Va., with a growing customer base that includes large enterprises, state and municipal governments, law enforcement agencies and more.

Find out how GroupSense can help your organization at www.groupsense.io