Interisle Report Identifies Inadequate Domain Security Practices as Root Causes of Security Incidents

HOPKINTON, MA, UNITED STATES, June 28, 2021 /EINPresswire.com/ -- Interisle Consulting Group today announced the publication of an industry report, Domain Security: A Critical Component of Enterprise Risk Management. The report describes the adverse and costly consequences when an organization becomes a victim of domain name hijackings or misuse. Interisle recommends that organizations need to include domain names in their enterprise risk management planning and execution.

Interisle's analysts describe incidents where major corporations, government agencies, financials, or crypto-currency exchanges fell victim to domain theft or “hijackings.” The research indicates that such hijacking incidents occur with disturbing frequency, even among the large enterprises or government services across the globe.

According to Dave Piscitello, Interisle partner and co-author, “Domain hijackings have ripple effects: not only is the victimized organization harmed but other or Internet users become victims of phishing, counterfeiting, or ransomware attacks, or fall prey to Business Email Compromise (BEC) attacks that use the hijacked domains for criminal purposes.”

Domain abuse is mentioned prominently in recent claim data reports from cyber insurance companies. Allianz reports that business disruption (a common consequence of domain hijacking) has become the most common cost driver behind claims. Coalition, Inc. reports that domain spoofing is a root cause of loss for funds transfer fraud incidents.

Surveys of the Forbes 2000 and the global financial industry reveal that domain security is undervalued and underutilized. Only 17 percent of the Forbes Global 2000 use Registry locks, the most effective means to prevent domain hijacking. A dismal 3 percent have deployed DNSSEC, an effective measure to prevent DNS cache poisoning, certain forms of phishing, or redirection attacks. Interisle conducted its own survey and found that domain security adoption among nearly 5000 FDIC-insured banks is worse than that reported for the Forbes Global 2000..

Domain security services may be unfamiliar to staff who are responsible for domain administration. Interisle’s study reveals that this appears likely among FDIC insured banks, many of whose domains are registered through domain registrars that only offer basic protection measures. To assist such staff, Interisle has prepared a Domain Security Evaluation that staff can

use to make informed decisions when choosing a registrar that can deploy secure, scalable, "enterprise-class" measures that they are needed to satisfy their organization's' risk tolerance.

Find Interisle's industry report at http://interisle.net/DomainSecurity2021.html
Comments can be submitted to criminaldomainabuse@interisle.net

David Piscitello
Interisle Consulting Group
criminaldomainabuse@interisle.net
