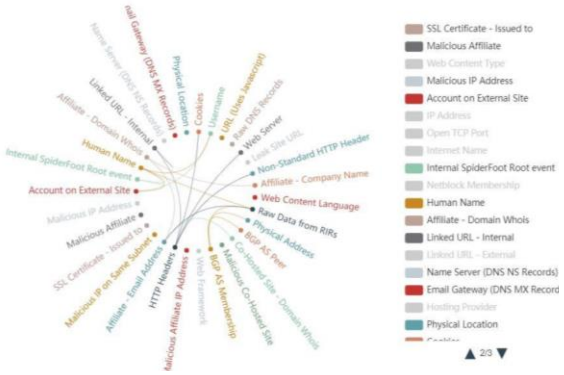
USING CYBER THREAT INTELLIGENCE IN INCIDENT RESPONSE

MINIMIZE LEGAL EXPOSURE FROM A DATA BREACH: A USE CASE SNAPSHOT

A Cyberattack is a terrifying experience for a business, especially for a small business. Reputational impacts, business interruption, and investigation and mitigation costs are among the initial concerns. The exposure to legal liability tops the list of worries when there's been a data breach. We assist clients with all these issues with our breach coaching experience and interdisciplinary team of incident response professionals. And our novel use of advanced cyber threat intelligence capabilities has uncovered hidden evidence for clients to form a legal defense, in the event of litigation or Payment Card Industry (PCI) fines.

THE CHALLENGE

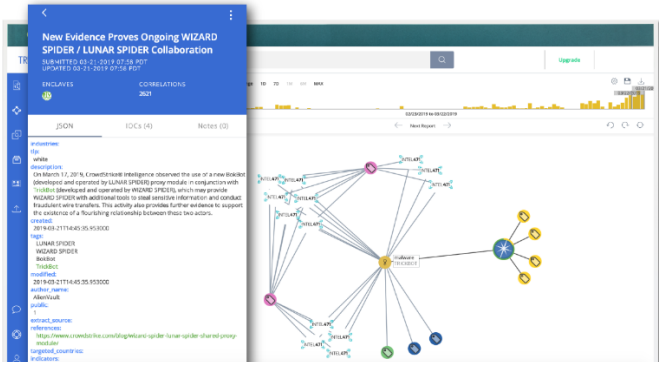
The law in every state now requires reporting of a data breach – notifications to the victims as well as, in many states, reporting to state officials. Industry sectors and European markets also require reporting, required under regulations like HIPAA, GDPR, and many more. For ecommerce vendors, the merchant agreement mandates reporting under the PCI Data Security Standard (PCI DSS). Couple the requirement to disclose details of the breach with the average length of time attackers remain burrowed inside to steal personal information (weeks to months by most reports), and the quantity of records lost can create a staggering cost component. **A multi-million-dollar legal exposure dilemma is both foreseeable and often quite common**!



Malicious leads categorized by type and revealed for inspection and analysis.

THE SOLUTION

This is where breach coaching with integrated cyber threat hunting comes in. **eos**edge Legal's Incident Response capability[1] recently designed and implemented



Link analysis of attack path data to correlate with historical attack profiles to find attack type matches.

cyber threat intelligence analysis to construct for clients a post-incident legal defense to defeat a plaintiff's claim that the online merchant was liable for credit card theft. Working collaboratively with eosCyber Alliance partners, the interdisciplinary team established a cause of compromise evidentiary portfolio that pointed to an online supply chain partner's liability rather than the online merchant. The impact of this research and evidence is that the client has evidence pointing to a third-party as causing the data breach rather than the client. This novel approach toward establishing defenses from liability is highly valuable to any data breach victim.

[1] ***eosedge Legal also offers prevention and retained cyberlaw counsel services.***

90 S. CASCADE AVE SUITE 1100 | COLORADO SPRINGS, CO 80903 | 719.357.8025 | WWW.EOSEDGELEGAL.COM