Domain Histories Reveal Bad Actors

Posted on August 15, 2018

The European Union's General Data Protection Regulation (GDPR) places the responsibility for data privacy on organizations and their Boards of Directors. In the event of a data breach, GDPR may fine organizations up to $24 million or 4 percent of its global revenues in the previous year. It's important to note, however, that GDPR doesn't only affect Europe-based companies.

GDPR's Global Reach

The long arm of the regulation authorities reaches across the globe to companies that maintain the private information of the European Union (EU) citizens. So, if a company based in the United States exposes private details of the EU citizens, then the EU will levy penalties on the US company. For instance, if the Equifax data breach had occurred a year later than it did (in September 2018 instead of September 2017), the EU could have sued the company for global annual revenues, not only for the breach, and also for the lapse in the time it took for the company to come clean about the penetration (40 days).

The stakes have never been higher for companies and the cybersecurity professionals devoted to protecting their employers and clients from such breaches. Instead of considering GDPR a threat to companies, however, infosec specialists can see the regulation as a spur to proactively defending companies against cyber attacks.

Learn from History

Companies can begin fortifying their defenses right away by examining the origins of websites that have already posed threats to their companies. Cyber threat specialists can start their research in two areas: phishbait that hackers have sent to the company staff and websites with domain names similar to target companies.

Phishing involves hackers emailing information they deem relevant to the users' work or even diversions. For instance, many defense contractors have been caught out by clicking on links to fake professional conferences related to the industry interests. Instead, the website they accessed downloaded malware onto their computers. The malware could then track and capture the user's

activity and vital credentials to sensitive information.

Infosec professionals can investigate the histories of malicious websites to determine their origins. Changes in the registrar's name, the last date of update, the WHOIS server and modifications to other identifying data can provide leads on the authors of the malware and other websites they may have infected. Once investigators have thoroughly looked into the root of infected websites, they can update their firewalls so as to block any malevolent IP addresses. Security staff can also update malware lists that identify websites with criminal histories.

Professionals can also use a historical forensics approach to investigating the origins of websites that seek to deceive users into believing they are authorized company sites. Fake sites trick users with small, sometimes hidden spellings in domain names that casual computer users do not observe. The fake websites may also be sources of malware or themselves serve as traps for user credentials to vital data and accounts.

Research into the history of changes of these fake websites can disclose who has maintained the websites over time. Investigation may also reveal who may be supporting a collection of fraudulent websites. Infosec staff can block fake websites at the network firewall layer. They can also notify the company's management of the misdirection. The organization's leadership may choose to deliver the authors of fake website(s) a desist order or they may notify law enforcement authorities if the fraudulent IP address poses a clear and present danger to customers and the public at large.

Tools at Our Disposal

WHOIS tools like Whois History API aid security analysts, security researchers, security architects, malware analysts, and threat investigators reveal the origins of suspicious websites. The API will enables infosec professionals to view relevant historical WHOIS records to find out how a domain's ownership has been evolving. The evidence sheds light on the origin of bad actors and their online channels of ill-intent.