Third-Party Risk Assessment: How Domain Intelligence Can Fill in Visibility Gaps

Posted on December 10, 2019

To maintain an uninterrupted flow of their operations, organizations depend on a vast array of information systems (ISs) provided by third parties. By enlisting the help of vendors, partners, and suppliers, businesses can boost their revenue due to increased productivity and significant cost reduction.

This interdependency between entities in a diverse ecosystem has brought along a host of challenges as well. Systemic cyber risks, in particular, have become a vital issue for stakeholders in regulated industries. Examples include:

- **The "Zombie Zero" attack:** The Zombie Zero malware came pre-installed in China-made barcode scanners used by shipping and logistics centers. It targets corporate networks to steal information about shipments, including sender and receiver details and package values.
- **The SWIFT-related heist of 2015-2016:** Cybercriminals exploited a vulnerability in the Society for Worldwide Interbank Telecommunication (SWIFT) networks of banks in Nepal, Bangladesh, Vietnam, and Ecuador with malware. They were able to steal operator credentials to manipulate the affected systems and delete transaction records. The total amount stolen reached an estimated US $90 million.
- **The Wannacry ransomware outbreak of 2017:** The ransomware crippled around 200,000 computers running outdated Microsoft Windows OSs. Files on affected systems were rendered inaccessible unless payments in the form of bitcoin were made.

A Ponemon Institute study revealed that 59% of companies succumb to vendor-caused data breaches. A lack of visibility due to inadequate data was cited as a top contributing factor to most of these.

Where Risk Assessments Go Wrong

Managing third-party relationships through consistent risk evaluations is critical to catch vulnerabilities and unknown threats residing in complex infrastructures. Also known as "third-party governance," this involves performing due diligence on all connected third-parties and their

activities and evaluating mitigation plans for enhancement.

While cybersecurity among organizations has generally improved, one problem that companies and cyber-risk assessors continually face is data quality. In the financial sector, for instance, concerns about the "accuracy and actionability of risk assessment data" was identified by a joint BitSight and Center for Financial Professionals survey.

Security professionals often report the following issues concerning inaccurate data:

Unprocessed Data

Zone files and other threat intelligence come from various sources with their own formats. From registrars to Internet service providers (ISPs), multiple parties collect registrant information inconsistently. This practice renders data incomplete, redundant, or prone to error. It also complicates data aggregation and analysis for security assessors.

Inaccurate Data Sets

Some cyber intelligence providers and other third-party vendors and suppliers don't have the time or resources to audit their data. Others don't even have access to viable data, as they don't have the proper agreements with domain registrars in place. As such, security assessors sometimes have to work with WHOIS records that either do not contain any or have invalid data.

Incomplete Subdomain Information

Having access to subdomain information allows threat assessors to discover incorrect host configurations, malicious IP addresses and ranges, and network vulnerabilities. Risk assessors need to have access to updated subdomain data to precisely determine risk scores for all clients

and stakeholders.

How Domain Intelligence Can Help

Reliable domain intelligence platforms provide security vendors and analysts with well-parsed and well-structured data that result in fewer false positives and that can be integrated into existing systems.

To address the challenges mentioned in the previous section, organizations can make use of our tools to enhance their risk assessment programs:

IP Netblocks API

Security software-as-a-service (SaaS) providers can begin assessments by evaluating the quality of the client's network traffic. They collect IP addresses from logs to identify each organization's IP range, the users within its network, and its website visitors. From there, they can dig deeper into connected IP addresses to ban entire netblocks should these prove malicious.

IP Netblocks API delivers well-parsed, well-structured, and up-to-date information on IP ranges. The information it provides includes a given IP address's subnetwork name, organization name, ownership information, and country code, among others. These capabilities address pain points #1 (unprocessed data) and #2 (inaccurate data sets) above.

WHOIS API

Understanding a client's or a vendor's domain infrastructure helps cybersecurity researchers to investigate attacks, mitigate intrusions, and reveal gaps. WHOIS API indexes more than 6.7 billion

domain records – and counting – to provide users with complete information on each active domain. Users can easily integrate it into their threat detection and response systems. It also provides data down to the subdomain level that addresses pain point #3 (incomplete subdomain information) above.

DNS Database Download

Looking into passive Domain Name System (DNS) replication data is a non-intrusive method to conduct reconnaissance on external parties. Historic DNS databases provide threat hunters with critical points on how domains have changes hands in the past and whether such changes point to involvement in malicious activities. DNS Database Download provides all information on any active domain obtainable via registries, publicly available sources, ISPs, and other possible sources. It addresses all three pain points cited above.

Seasoned infosec professionals know all too well that vendor security doesn't stop at endpoint protection. Real and adequate threat protection also requires third-party risk assessments. Reliable, up-to-date, and accurate domain intelligence allows organizations to monitor their overall cyber-risk posture.