Conducting Passive Reconnaissance Using Website Contacts Database Intel and Search Results

Posted on January 12, 2020

Is your supplier or partner, or a new acquisition of yours a potential threat? If you're reading this, you're probably asking yourself the same thing.

Third-party vendor risks have become a pressing concern among businesses in the wake of recent supply chain attacks. Around 59% of organizations have encountered an attack that can be traced back to their suppliers. This number has probably increased as reports of new vendor-caused attacks make headlines every day.

Many organizations believe that vendor risk assessment should be a high priority as they engage with more service providers. Unfortunately, most do not have the resources to do so. Among those who do, only 36% believe that their third-party risk management programs work.

No Background Checks

The most significant finding from a Ponemon Institute survey was that 59% of users believe that their company leaders are willing to skip vendor assessment when rushing to close business deals. Users believe this creates more significant problems in the long run, no matter how robust their risk management programs are. Separate survey results echoed the same sentiment across different verticals.

Enter Passive Reconnaissance

Indeed, security breaches can be caused by top executives disregarding their existing protocols. The Marriott breach last year is a cautionary example of why an exhaustive risk evaluation of physical and digital assets should be performed before and after mergers.

The importance of vetting suppliers, vendors, and partners based on their security posture surely can't be emphasized enough. To avoid any ethical concerns and bureaucratic delays, security

analysts and cyber-risk assessors carry out passive reconnaissance by using a wealth of domain and threat intelligence sources.

Passive reconnaissance is an information gathering method wherein analysts examine public records and third parties' network and usage logs. The evidence gathered at this stage is then used to construct (or reconstruct) data breach scenarios. Passive reconnaissance can be done afterward, and digital forensics and incident response (DFIR) teams are mostly responsible for running it.

Passive reconnaissance is non-intrusive, as security professionals don't have to interact with a third party's network. It helps organizations maintain compliance since it doesn't circumvent or violate any privacy laws.

How to Do Passive Reconnaissance

There are a variety of ways for organizations to conduct passive reconnaissance. This article discusses a few methods.

Via a Website Contacts Database

There's so much information that cybersecurity researchers can retrieve from a single target domain or website. Analysts can map out a potential attacker's infrastructure or discover vulnerabilities with just a third party's domain information.

Website Contacts and Categorization Database can, for instance, be used to obtain critical data points on certain websites associated with the third party of interest and its affiliated networks. Information from such a database enables risk assessors to identify the owner of a website. Knowing that would allow users to dig deeper into the following:

- With Domain Reputation API, find out if any of a potential business partner's, supplier's, or company acquisition's digital assets are blacklisted

- With Threat Intelligence Platform, determine threat risks for a URL, such as its potential ties to malware

Via a Search Engine

Search engines can be used for passive reconnaissance in the same way any enthusiastic fan stalks his/her favorite celebrity. A simple Google search can quickly bring up a fair amount of information about a particular individual or company.

Here are the steps for pulling up the domain tree of a third-party website via Google.

- 1. Refresh your Google homepage to the "international" version. To do this, make sure that the URL appears as "https://google.com/ncr" before beginning your search. NCR stands for "no country redirect," which prevents Google from giving out location-biased results.

- 2. Type "site:websitename.com -site:www.websitename.com". Bear in mind that there should be a space between the first and second search phrase for this to work.

- 3. Hit the Enter key. You should see all the subdomains connected to your target domain.

Via a Browser Sniffer

User agents indicate what type of browser site visitors use, along with their language settings, request structures, installed plugins, and so forth. Analysts can examine this data via a browser or network sniffer to see if a particular site visitor is comes from an IP address assigned to a supplier or partner or not. Anomalous requests may look more differentiated and include specific files or file types, such as sensitive information like C-suites' email addresses, username and password combinations, and more. Browser sniffing, however, only works if users do not have extensions that prevent it.

Passive reconnaissance is an indispensable research tool for DFIR specialists, penetration testers, and similar staff to manage vendor risks. Search and browser data can serve as initial sources of data for extensive background checks that can then be correlated with more details from a **website contacts database** such as Website Contacts and Categorization Database.