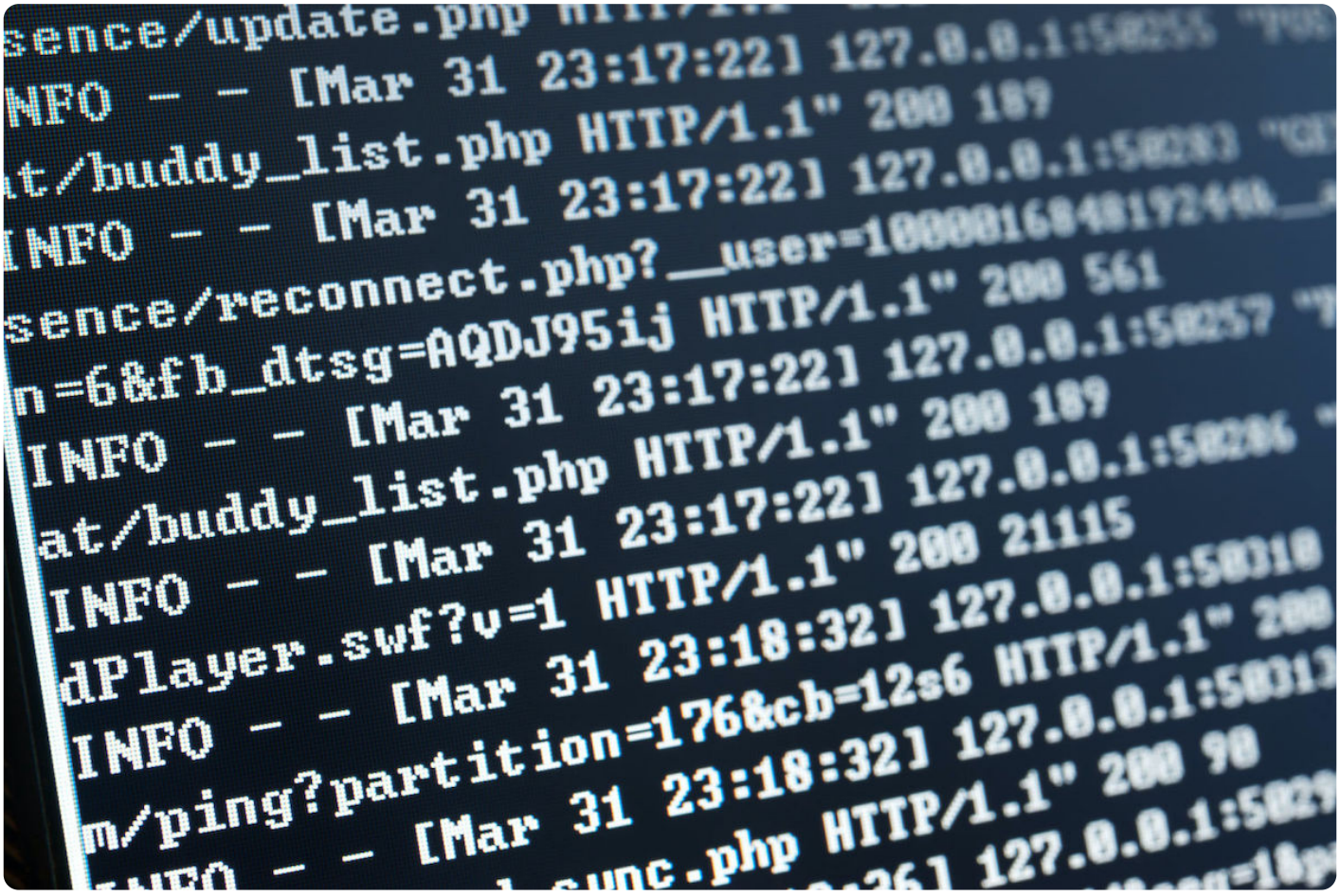
Improving Managed Security Service Provision with a GeoIP Database

Posted on April 22, 2020



A data breach can have a lasting impact on an affected organization, with consequences ranging from reputation damage to loss of customer trust and staggering legal fines that result from lawsuits and settlement fees. Recent studies estimate the cost of a data breach caused by malicious attacks at $4.45 million. More than 70% of U.S. users also said that they'd avoid a company that does not sufficiently secure its data.

When it comes to securing your crown jewels and customer data, safeguarding all possible attack entry points should be a top priority. Organizations today must employ proactive and multilayered approaches to security that cover all their bases—endpoints, network, and data storage (whether in-house or cloud-based).

One way of ensuring sufficient protection is through a managed security service provider (MSSP) that uses a GeoIP database such as IP Geolocation Data Feed. This post offers some specific recommendations.

How MSSPs Can Harness the Power of IP Geolocation Data Feed

A GeoIP database pertains to a comprehensive source of relevant and accurate IP geolocation information. With it, organizations can block email addresses, owners, and domains connected to all known malicious IP addresses from accessing any of their Internet-facing network components. It also helps them cross-check if a site visitor is indeed who he/she claims to be or is from. This verification capability is especially useful for organizations that allow financial transactions on their portals (e.g., banks, online shops, etc.).

More specifically, a GeoIP database enables security professionals to screen traffic in real time to make sure that bad traffic (with known or unknown ties to malicious activities and actors) will not be able to breach their defenses. The tool is particularly useful for the following applications:

Protection from Phishing and Its Various Forms

The majority of email attacks succeed because of the effective social engineering ploys that allow

cybercriminals to trick users into following malicious links, downloading malware disguised as harmless attachments, or divulging personally identifiable information (PII). In business email compromise (BEC) attacks, cybercriminals succeed because they were able to make victims believe they were from the same office.

IP Geolocation Data Feed can thwart a threat like BEC, allowing cybersecurity personnel to quickly check if an email sender's address indeed corresponds to a senior executive's known IP address. If they don't match, further communication with the email address in question can be immediately stopped, thus nipping a likely BEC attack in the bud.

Fraud Prevention

Any site that processes financial transactions is at risk of becoming a fraud target. If cybercriminals brute-force their way into user accounts, they would probably get away with siphoning off funds if the organization doesn't employ sufficient security measures.

In such a case, a GeoIP database can be integrated into financial forms to verify if the current visitor's IP address matches the one on the account holder's records. Although it is possible for account owners to have several IP addresses (depending on how they access the network or what devices they use), this additional check would clue site administrators in on potential fraudulent transactions. The visitor can be asked further proof of identification before proceeding with the transaction. This process reduces the chances that unauthorized users are granted access to customers' accounts.

Defense Against Unknown Threats

The amount of new malware created every day continues to rise. Threats have also evolved to become stealthier, thus, better at evading detection. One way of protecting against unknown threats is by looking at their indicators of compromise (IoCs). These usually come in the form of email addresses, the owner's name and organization, and domains.

By identifying all IP addresses connected to these IoCs using IP Geolocation Data Feed, organizations can pinpoint currently unknown potential threat sources. They can then include all

the IP addresses and other relevant information as an added layer of security defense.

Limiting Access to Protected Media

Recent stats show that Internet users access piracy websites around 300 billion times a year. This practice is expected to cost the TV and film industry alone an amount of $52 billion by 2022. That amount can cause a small production outfit to go out of business. It is also the reason for the rise in the use of digital rights management (DRM).

But did you know that DRM can be further enhanced by the integration of IP Geolocation Data Feed? As an additional verification layer, a streamer's IP address can be validated using the tool to make sure he/she is an actual paying subscriber and not just a freeloader.

By 2021, organizations are predicted to lose as much as $6 trillion to cybercrime. That said, they need all the protection they can get. Large enterprises with their own security teams may be sufficiently protected, but what about smaller companies? Small and medium-sized businesses (SMBs) can seek the aid of MSSPs to take care of their digital assets and customer data. A service provider that uses all potential threat intelligence sources, including IP Geolocation Data Feed, would be a good bet to make.