3 Steps in Using Reverse IP/DNS Checks to Create an Attack Profile

Posted on May 22, 2020

Knowing the enemy, as they say, is winning half the battle. But in the world of cybersecurity, identifying the enemy can be very difficult sometimes. That said, creating an attack profile to know what type of enemy you could be up against is a good starting point. For all you know, a cyber attacker could be halfway around the world or right next door.

For that reason, organizations should enlist all possible resources to help them create an attack profile. Reverse IP/DNS API, which performs reverse IP/DNS checks, is one resource worth looking into. In a nutshell, the program allows cybersecurity experts to get a list of all domains that share the same IP address. As such, it could help unmask connections between indicators of compromise (IoCs), specifically, IP addresses and domain names.

Creating an Attack Profile Using Reverse IP/DNS Checks

Queries that go through Reverse IP/DNS API are run against one of the most extensive passive Domain Name System (DNS) databases in the market today. The database has more than 1.2 billion IPv4 records and over 1.4 billion domains and subdomains. These records are updated daily to ensure the relevance and accuracy of reverse IP/DNS query results.

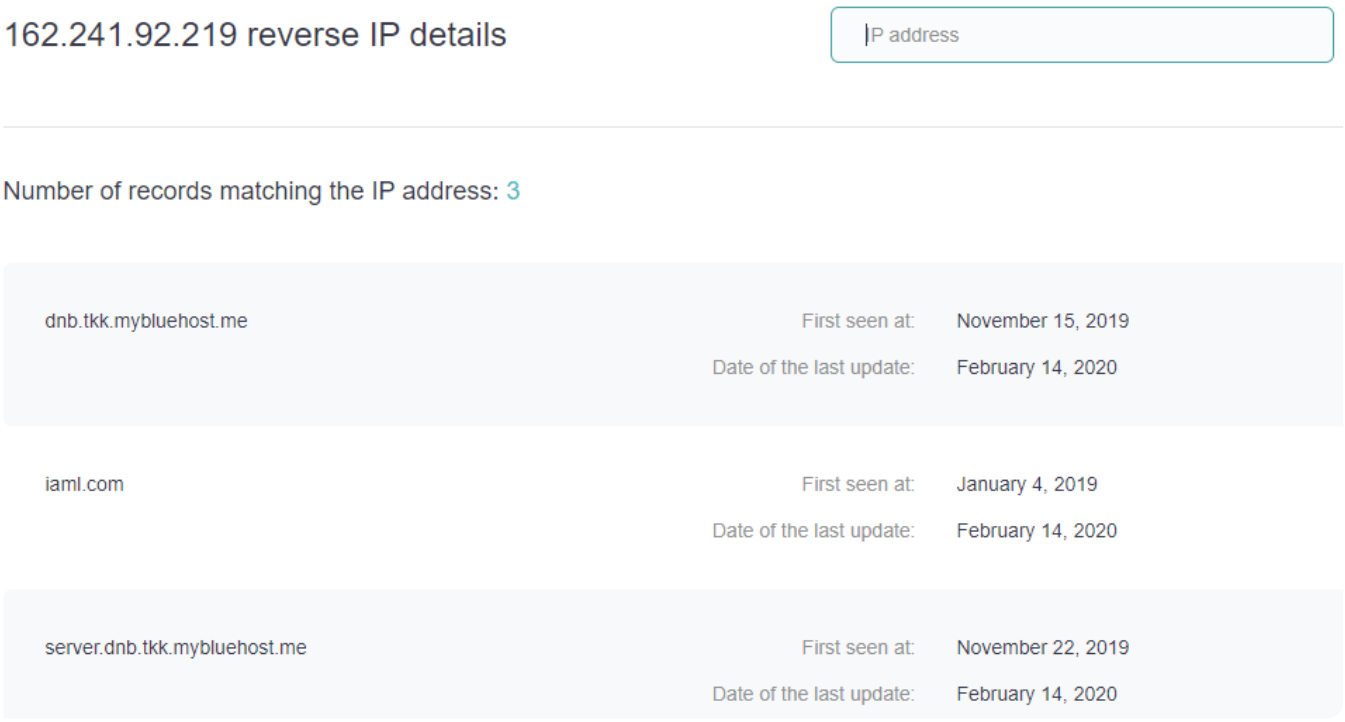
When used in conjunction with other security systems, Reverse IP/DNS API can reveal all domain names that resolve to the same IP address. In the following sections, we detailed how users can create an attack profile with the program's help.

1. Identify Domains That Resolve to the IP Address

An organization can identify a malicious IP address in various ways, such as through an alert from its threat intelligence platform (TIP) or by regularly checking cybersecurity news and IoC databases. As an example, we used 162[.]241[.]92[.]219, an IP address identified as an IoC in a targeted attack on financial service provider United Services Automobile Association (USAA). The particular attack uses Emotet to steal login credentials through a short message service (SMS) phishing or "smishing" campaign.

When we ran a reverse IP/DNS check on the IP address, the API returned three associated (sub-)domains:

- dnb[.]tkk[.]mybluehost[.]me
- iaml[.]com
- server[.]dnb[.]tkk[.]mybluehost[.]me



The output means that at one point, these domains resolved to the same malicious IP address associated with the smishing attack.

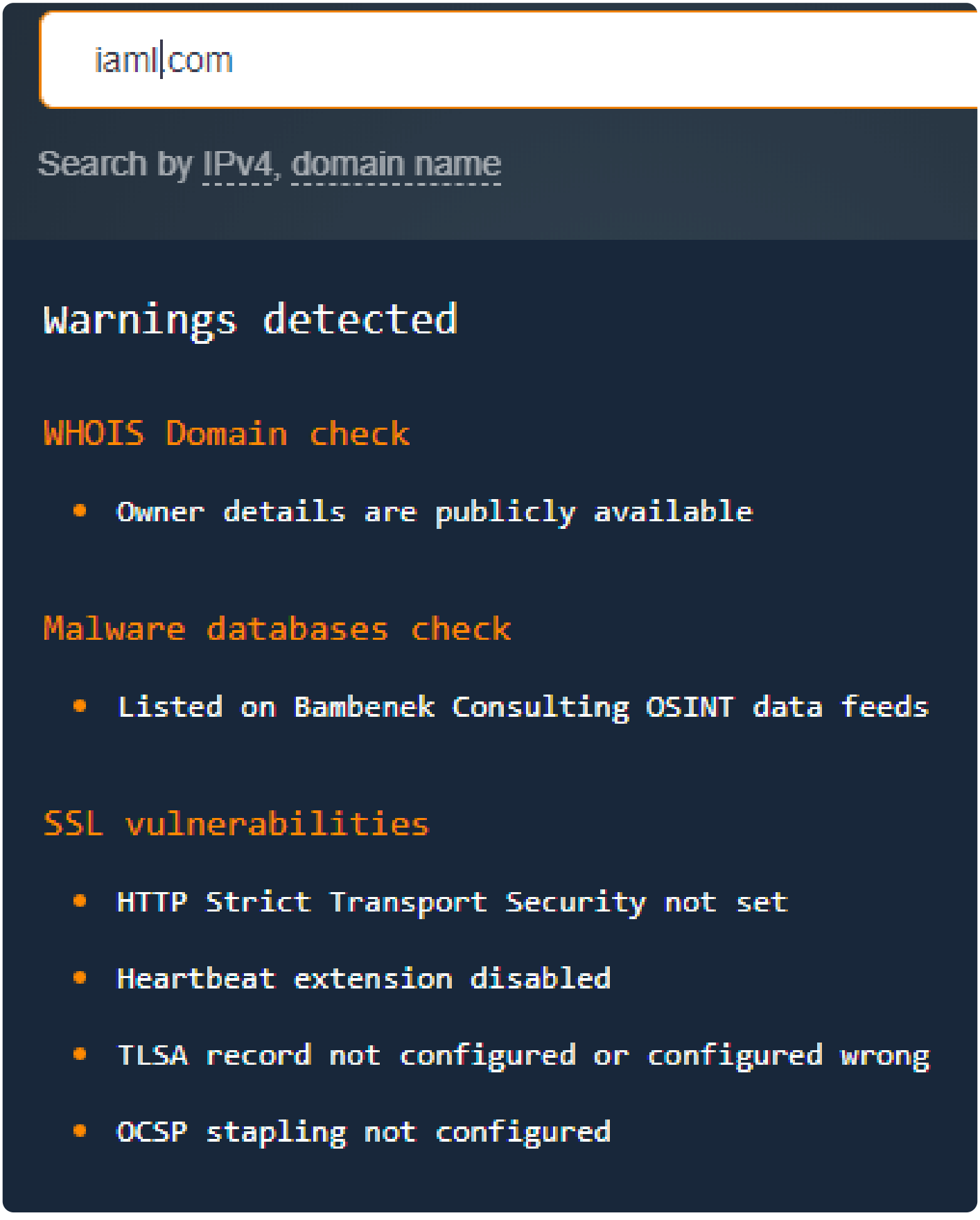
2. Check the Reputability of Connected Domains

IP address blacklisting may be considered too restrictive by organizations worried that they may

also be blocking prospective clients in the process. As such, the next step would be to confirm if the three domains are indeed malicious. How can this be done?

- **Malware databases:** Cybersecurity teams can check malware data feeds such as VirusTotal. Two of the domains, except dnb[.]tkk[.]mybluehost[.]me, in this case, were noticed communicating with malicious hosts. Iaml[.]com even downloaded a file from the said hosts. That could be how the smishing campaign perpetrators redirected victims to malware-infected sites.

- **Domain reputation checker:** Domain reputation checkers can also provide useful insights into suspicious domains. Domain Reputation API, for instance, detected that iaml[.]com is listed on the Bambenek Consulting Open-Source Intelligence (OSINT) data feeds.


iaml|com
Search by IPv4, domain name
Warnings detected
WHOIS Domain check
• Owner details are publicly available
Malware databases check
• Listed on Bambenek Consulting OSINT data feeds
SSL vulnerabilities
• HTTP Strict Transport Security not set
• Heartbeat extension disabled
• TLSA record not configured or configured wrong
• OCSP stapling not configured

While the other two domains passed the API's malware database check, they did have some Secure Sockets Layer (SSL) vulnerabilities.

- **Reverse IP/DNS record analysis:** Further analysis of Reverse IP/DNS API's results would also help in confirming suspicions. The program, for instance, first detected activity from the malicious IP address on February 11, 2020 — the attackers could have used it over the next days or even weeks.

According to the reverse IP/DNS check, all three domains were last updated (i.e., last associated with the IP address) three days later, on February 14, 2020. The fact that they were updated on the same day which coincides with the occurrence of the attack could be an indication of their connection to the same malicious activity.

3. Block the IP Address or Selected Domains Only

For the IoC we investigated, the second step proved that there was probably a need to block all domains returned by Reverse IP/DNS API due to vulnerabilities or their inclusion in blocklists. In this case, blocking at the IP address level would make sense and would be a lot more secure for the whole organization.

In some instances, however, the API might return some domains that seem innocent. Organizations can opt to have these domains closely monitored rather than blocked.

Understanding cyber attackers is not only crucial in incident response and cybercrime investigations, but also in mitigating cyber threats. When an organization succumbs to an attack, other companies shouldn't wait to gain the attacker's attention next. Instead, they should already start profiling attacks so they would know how to defend their infrastructure best.

Analysis and further investigation of the information gleaned from Reverse IP/DNS API can prove to be a critical element in creating an attack profile. Given an IP address, you can delve deeper into which domains could be involved with the malicious activities that the IP address is known for.