

DNS Records and Their History Matter: Beefing Up Your Cybersecurity Posture Using DNS Tools

Posted on January 20, 2020

The global cybersecurity landscape is becoming crowded both with threat actors and security solutions. When it comes to security threats specifically, attacks are becoming more and more sophisticated, and the amount of damage they cause is also increasing. In 2018, hackers stole almost [half a billion personal records](#).

These security breaches were accomplished by using different tactics such as phishing, denial-of-service (DoS), and ransomware attacks, to name a few. And the threat actors successfully carried out these attacks, not because victims don't use cybersecurity solutions, but because not all systems monitor every type of vulnerabilities — including the ones that have to do with DNS misconfigurations.

The key is for companies to decide which cybersecurity solutions best fit their business model strategically. For organizations that rely mainly on websites and email communications, including Domain Name System (DNS) record checks aided by a [DNS database](#) or [DNS lookup tool](#) may be their best bet.

How DNS Tools Can Strengthen a Company's Cybersecurity Posture

The Significance of DNS

DNS acts as a translator between human beings and computers. It converts what humans type into their web browsers into numerical strings called IP addresses, which are better understood by computers. So, when a user types in `whoisxmlapi.com`, for example, a DNS lookup takes place in a matter of milliseconds, where the system resolves the domain to the IP address, which is `206.225.82.106`.

DNS is akin to a global directory and has been an integral component of the Internet since the 1980s. Websites, emails, social media, and almost any service that uses the Internet rely on DNS to resolve IP addresses into hostnames every second of the day. Otherwise, these services stop working, gravely affecting business operations.

DNS as an Attack Vector

DNS is also, unfortunately, an effective attack vector. That is primarily because many organizations tend to overlook it when beefing up their cybersecurity infrastructure. But when bad actors find that a company's DNS server is unsecured and vulnerable, they can launch DNS-based attacks such as the following ones:

- **DoS attack:** Also called a "DNS flood attack," this is the most common type of DNS-based attack where a single IP address is sent multiple requests to cause your server, your server to overload, thus rendering it inaccessible.
- **Distributed DoS (DDoS) attack:** This is a type of DoS attack where thousands of requests coming from bots flood a target domain to overload your DNS server. As a result, your network goes offline.
- **DNS cache poisoning:** In this attack, a threat actor replaces an IP address in your DNS resolver's cache with a malicious one. The goal is to redirect traffic to a different website to

steal data or drop malware onto visitors' computers.

There are a lot more types of DNS-based attacks, but most of them are already variations of DoS attacks or DNS poisoning. Most of them have the same goal, which is to overload your server with multiple requests until it stops working or to redirect DNS requests to malicious sites.

Strengthen Cybersecurity with DNS History

For a long time, DNS worked as a real-time system where data related to queries and resolutions disappeared right after the event. There was no way to see which domains resolved to a particular IP address and all other DNS records in any zone. This feat, however, was addressed when Florian Weimer introduced the concept of [passive DNS](#) in 2005.

Passive DNS is a way for IT professionals and website administrators to get a glimpse of their **DNS history**. As such, it makes threat detection, response and investigation a lot easier.

What Analyzing DNS Records Can Tell You

Let's take a look at an example showing how DNS records can be a starting point for investigations and follow-up actions.

We ran [stk-frumonline\[.\]com](#), and [PhishTank](#) suspected this particular domain to be involved in phishing activities, on our [DNS Lookup API](#) and found two DNS records — an A record and a start of authority (SOA) record.



DNS record(s) found: 2



Report price: 1 credit

Type: 1

DNS type: A

Name: stk-frumonline.com.

TTL: 3599

R Rset Type: 1

Address: 164.132.51.185

Type: 6

DNS type: SOA

Name: stk-frumonline.com.

TTL: 21599

R Rset Type: 6

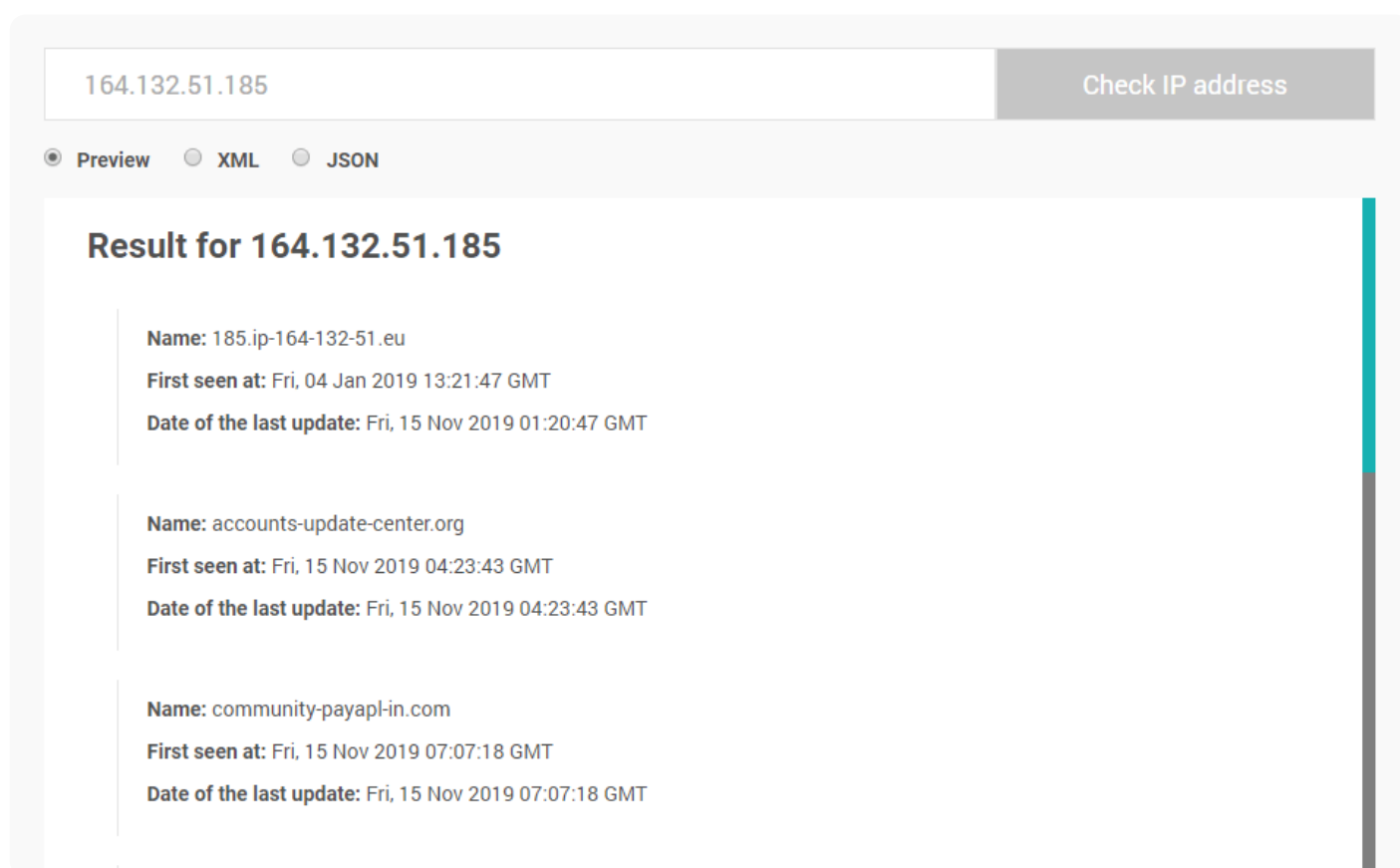
Admin: cloud-dns-hostmaster.google.com.

Host: ns-cloud-e1.googledomains.com.

Expire: 259200

Next, we used [Reverse IP/DNS Search](#) to see all of the domains that resolve to the same IP addresses, effectively detecting other potential phishing domains.

Stk-frumonline[.]com resolved to 164.132.51.185, and when we ran this IP address on Reverse IP Search, we found 13 associated domains.



The screenshot shows the WhoisXMLAPI Reverse IP Search interface. At the top, there is a search bar containing the IP address "164.132.51.185" and a button labeled "Check IP address". Below the search bar, there are three radio buttons for output format: "Preview" (selected), "XML", and "JSON". The main content area is titled "Result for 164.132.51.185" and displays three domains with their associated metadata:

Domain Name	First seen at	Date of the last update
185.ip-164-132-51.eu	Fri, 04 Jan 2019 13:21:47 GMT	Fri, 15 Nov 2019 01:20:47 GMT
accounts-update-center.org	Fri, 15 Nov 2019 04:23:43 GMT	Fri, 15 Nov 2019 04:23:43 GMT
community-payapl-in.com	Fri, 15 Nov 2019 07:07:18 GMT	Fri, 15 Nov 2019 07:07:18 GMT

If the domain is indeed involved in phishing activities, organizations would be better off blocking access to the other associated domains too.

Threat actors always look for weak points in an organization's overall IT ecosystem, and when they find a hole, they can infiltrate its network. That is why checking the overall health and integrity of your entire domain infrastructure is essential. Doing so can help you identify possible attack

vectors you'd otherwise miss.

Passive DNS-based tools give you a glimpse at your DNS configuration. You can integrate [DNS Lookup API](#) into your current security systems or download our [passive DNS database](#) to power up your threat intelligence.