Powering Asset Discovery with Domain and Subdomain Intelligence Sources

Posted on September 21, 2020

Everyone leaves digital footprints behind while using Internet-based technologies. Besides, in the process of improving digital services, acquiring new companies, and doing business in general, organizations inadvertently create digital trails. When threat actors pick up the scent, the result could be devastating and costly.

Asset discovery can help organizations keep track of their technological assets, so they can apply the necessary protection and keep their overall infrastructure safe from malicious actors. How so? Let's take a closer look.

What Is Asset Discovery?

Asset discovery is a cybersecurity process that enables organizations to map out and possibly reduce their attack surface. It involves conducting a detailed inventory and monitoring the status of all systems connected to a given network. Hence, it is an absolutely crucial business practice, and among the questions it addresses are:

- What services are running within your infrastructure?
- What do these services do?
- Are there any third-party scripts running on these pages?
- Are there forgotten pages from phased-out services?

Organizations get a clearer understanding of their infrastructure by answering these questions. In the process, they can also determine how wide their attack surface is – since each asset left unguarded or not documented can serve as an entry point for attacks.

The Importance of Asset Discovery

Consider the British Airways data breach that occurred in 2018 and during which the culprits stole personally identifiable information (PII), including the credit card numbers and corresponding three-

digit CVV codes of about 500,000 customers. The data breach caused the airlines to incur a £183-million penalty.

While even the best of us could fall victim to cybercrime, the resulting financial and reputational damage of a data breach may be preventable when all digital assets are accounted for and regularly monitored.

In the example cited above, the threat actors modified a problematic third-party script that was n on the airline's baggage information page. The modification caused sensitive information typed by customers to be transmitted to baways[.]com, a lookalike domain controlled by the perpetrators.

Asset Discovery: What It Involves

With more organizations dividing their technology between on-premises and the cloud, asset discovery has become more extensive. Apart from performing an inventory of the company's hardware and software, organizations can make asset discovery more accurate and inclusive by obtaining information from domain and IP intelligence sources.

Subdomains

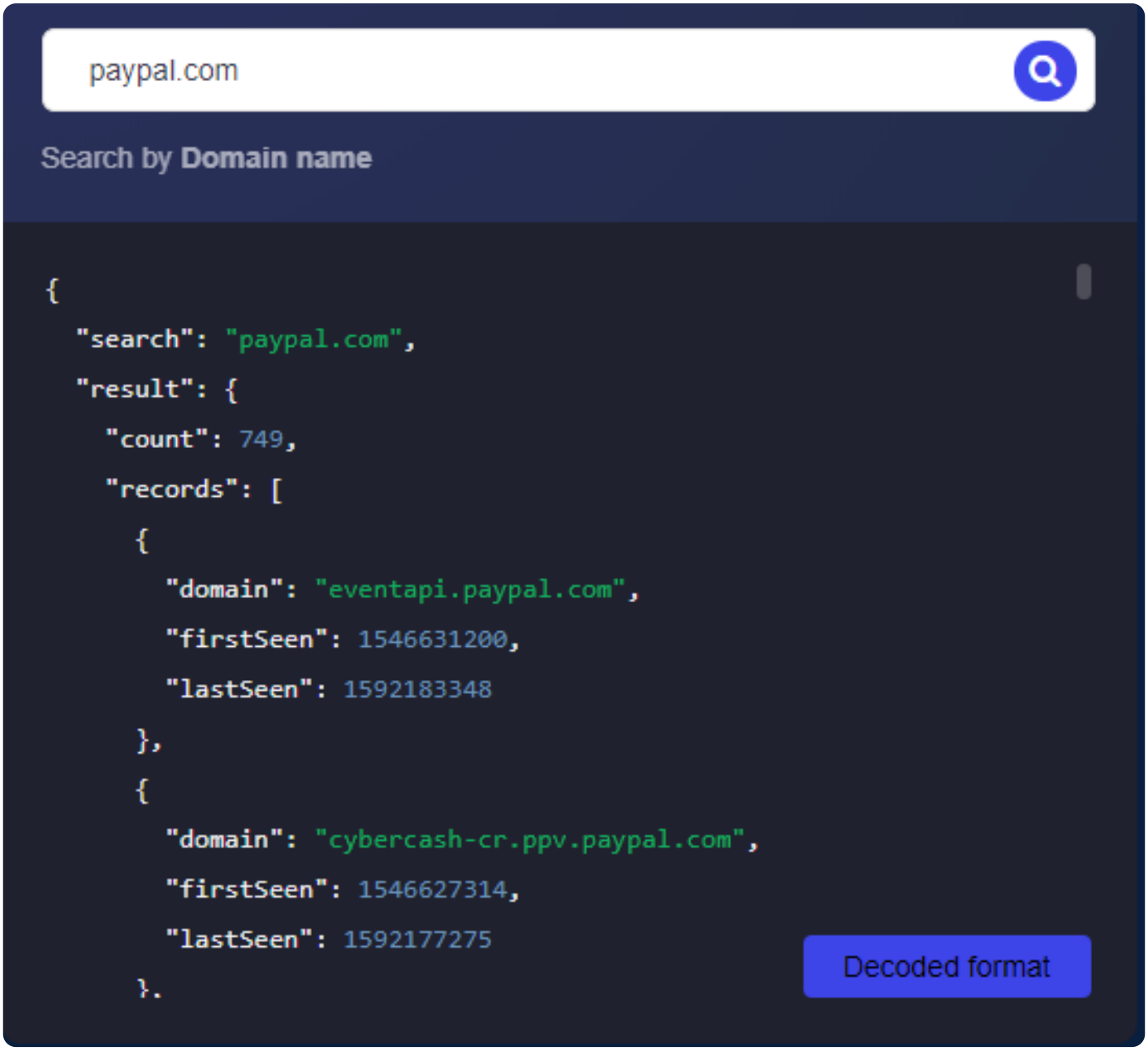
You can start by getting a list of all your subdomains as there may be forgotten pages. We ran britishairways[.]com on Subdomain Lookup API and obtained 14 subdomains. They are listed below, along with the dates when they were last updated:

- wap[.]britishairways[.]com 15 June 2020
- ns2[.]britishairways[.]com 15 June 2020
- avios[.]britishairways[.]com 14 June 2020
- travelnews[.]britishairways[.]com 15 June 2020

- onbusiness[.]britishairways[.]com 8 June 2020
- baggageclaim[.]britishairways[.]com 27 January 2020
- events[.]britishairways[.]com 15 June 2020
- toflytoserve[.]britishairways[.]com 15 June 2020
- press[.]britishairways[.]com 15 June 2020
- origin-www[.]britishairways[.]com 15 June 2020
- baads[.]britishairways[.]com 14 June 2020
- www[.]britishairways[.]com 13 July 2020
- ns1[.]britishairways[.]com 15 June 2020
- www-cloud[.]britishairways[.]com 13 June 2020

Most of the subdomains have only been updated recently, except for baggageclaim[.]britishairways[.]com, which was last updated more than six months ago—and so may require special attention.

Monitoring and protecting subdomains should be relatively easy for those that only have a few subdomains. But imagine technology companies that have dozens or even hundreds of subdomains such as paypal[.]com. Subdomains Lookup API returned a total of 749 subdomains, and if not tested and managed correctly, this also translates to possible attack vectors.


paypal.com
Search by Domain name
{
"search": "paypal.com",
"result": {
"count": 749,
"records": [
{
"domain": "eventapi.paypal.com",
"firstSeen": 1546631200,
"lastSeen": 1592183348
},
{
"domain": "cybercash-cr.ppv.paypal.com",
"firstSeen": 1546627314,
"lastSeen": 1592177275
},
Decoded format

DNS Records

Another critical detail to continually monitor is your domains' Domain Name System (DNS)records. Doing so would help security teams reduce the risk of DNS hijacking and support earlydetection.

DNS hijacking enables threat actors to change the IP address that a domain or subdomain resolves to. Such hijacking has happened multiple times, most notably in attacks against banks where clients are redirected to a website that looks exactly like their official login pages. Clients would key in their usernames and passwords unknowingly, giving the data to threat actors.

In the case of British Airways, the hackers were able to steal sensitive client information because they redirected traffic to a different domain.

The DNS lookup result for the subdomain baggageclaim[.]britishairways[.]com, for instance, reveals that it resolved to three different A records (IP addresses). Reverse IP Lookup shows that baggageclaim-prd-1972598507[.]eu-west-1[.]elb[.]amazonaws[.]com shares each IP address with one other domain. We listed the IP addresses below, along with the other domains that share them.

- 54[.]72[.]87[.]20 ec2-54-72-87-20[.]eu-west-1[.]compute[.]amazonaws[.]com
- 52[.]212[.]32[.]213 ec2-52-212-32-213[.]eu-west-1[.]compute[.]amazonaws[.]com
- 34[.]247[.]31[.]118 ec2-34-247-31-118[.]eu-west-1[.]compute[.]amazonaws[.]com

It's important to regularly check domain associations as sharing an IP address with a malicious domain could affect your network. Aside from the A record, it's crucial to monitor other DNS records, including mail server and nameserver records. Threat actors have successfully modified mail server details in the past as part of their schemes.

IP Netblocks

To make sure that the IP addresses your subdomains resolve to are the correct ones, you can also check their IP Netblocks details. For the IP addresses associated with baggageclaim[.]britishairways[.]com, IP Netblocks API reveals that all of them are enterprise connections of Amazon[.]com. With the consideration that British Airways uses Amazon Web Services (AWS) for its web hosting needs, then this is probably normal. Nevertheless, constant

monitoring of DNS records is a good way to secure your network.

Let's say, for example, that one of your subdomains suddenly resolves to the IP address 189[.]42[.]210[.]84. A reverse IP lookup would tell you that the IP address is associated with only one domain—mxd[.]ceb[.]com[.]br. Threat intelligence platforms and other security systems would flag this IP address since it has been reported 542 times on AbuseIPDB for various reasons, including Secure Shell (SSH) brute-force attacks and failed login attempts.

IP Netblocks API, on the other hand, further revealed that the IP address belongs to the IP range 189[.]42[.]210[.]80–189[.]42[.]210[.]95, which is owned by Claro S.A., a telecommunications company based in Brazil. The details on record also include abuse and administrative contacts.

Therefore, IP Netblocks can help verify the network and ownership information of an IP address that a domain or subdomain resolves to. Aside from that, it provides additional data points for investigation if an unknown IP address is observed.

Digital assets such as subdomains and DNS records can serve as attack vectors. Leaving them

unaccounted for and unprotected increases an organization's attack surface. And when threat actors get hold of these assets, they could stay undetected for a while. British Airways' 2018 data breach is an example of this. The attackers have been redirecting client information to their own network for about two weeks before the attack was detected.

Asset discovery could take time, yet it's a process that should be non-negotiable for organizations, big or small. After all, threat actors don't distinguish between small and large companies. As long as they see an entry point, they would come barging in and data might get compromised.