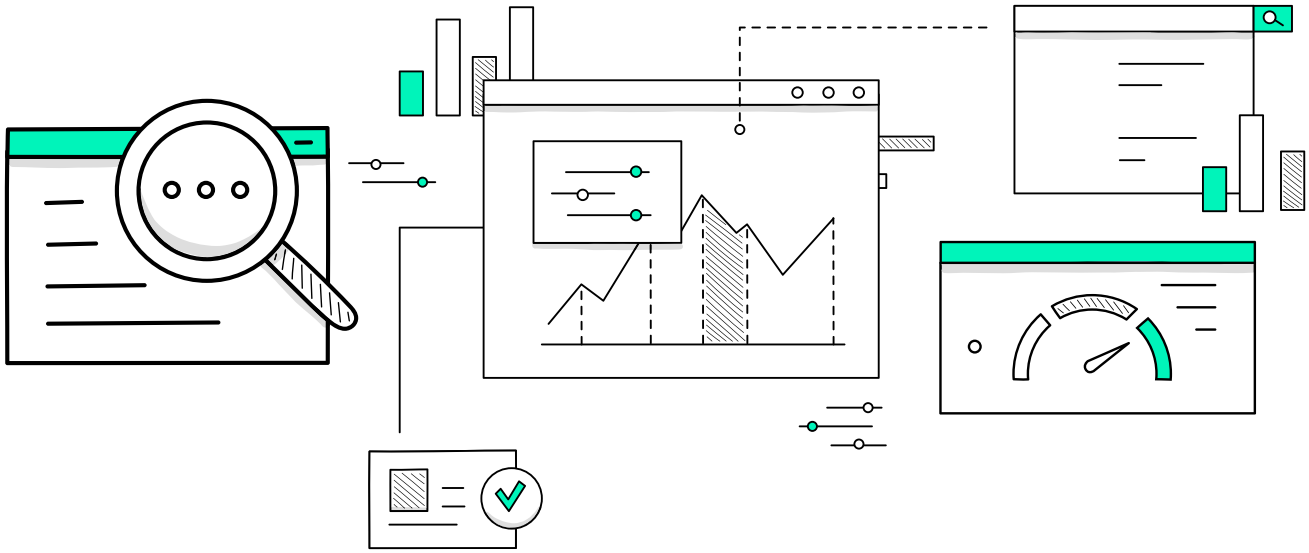
DNSSense



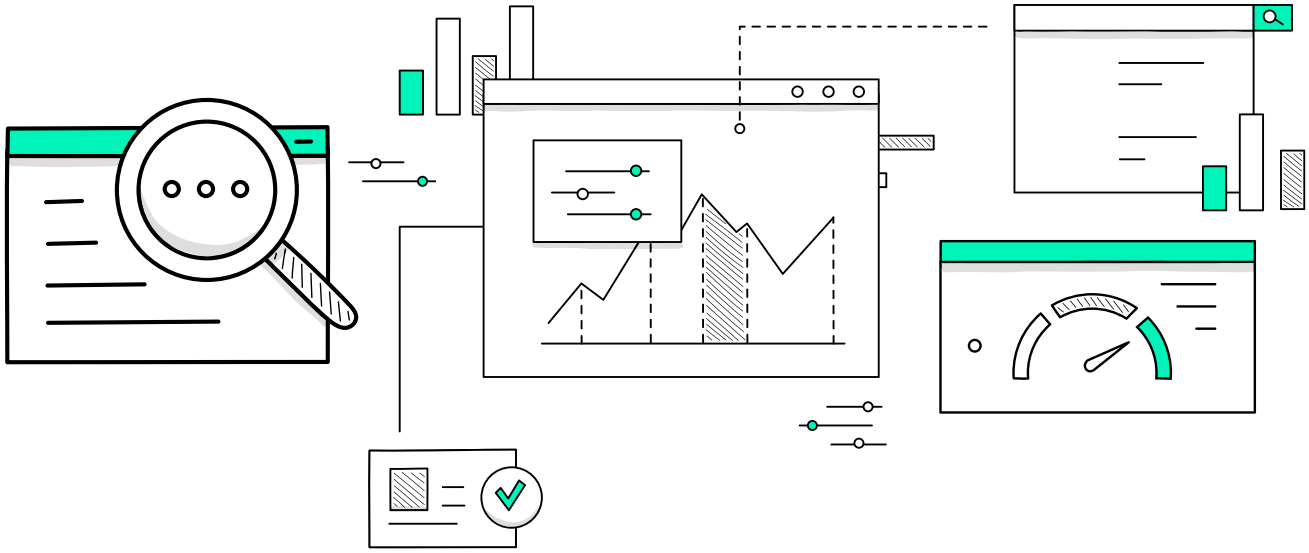
REPORTS and ANALYZES PROVIDED by DNS & SECURITY GAP VISIBILITY

REPORT

Table Of Contents

Introduction

DNS & Security Gap visibility is a virtual appliance server running in-house. It produces advanced DNS visibility and security
analysis reports by reading the existing internal DNS logs of the institution. Reports and analyzes can be reported from the
web-based interface of the product, as well as the data that needs to be examined are instantly transmitted to the SIEM product. It
saves a minimum of 1000 times the amount of EPS by transmitting only the logs containing security risks to the SIEM product.
A single DNS visibility appliance can analyze more than one hundred DNS server logs of different brands and models.
Supported DNS server brands
Windows DNS Server, Infoblox, F5, Citrix, Bind
In this document, the reports and analyzes provided by the DNS & Security Gap visibility product will be explained.



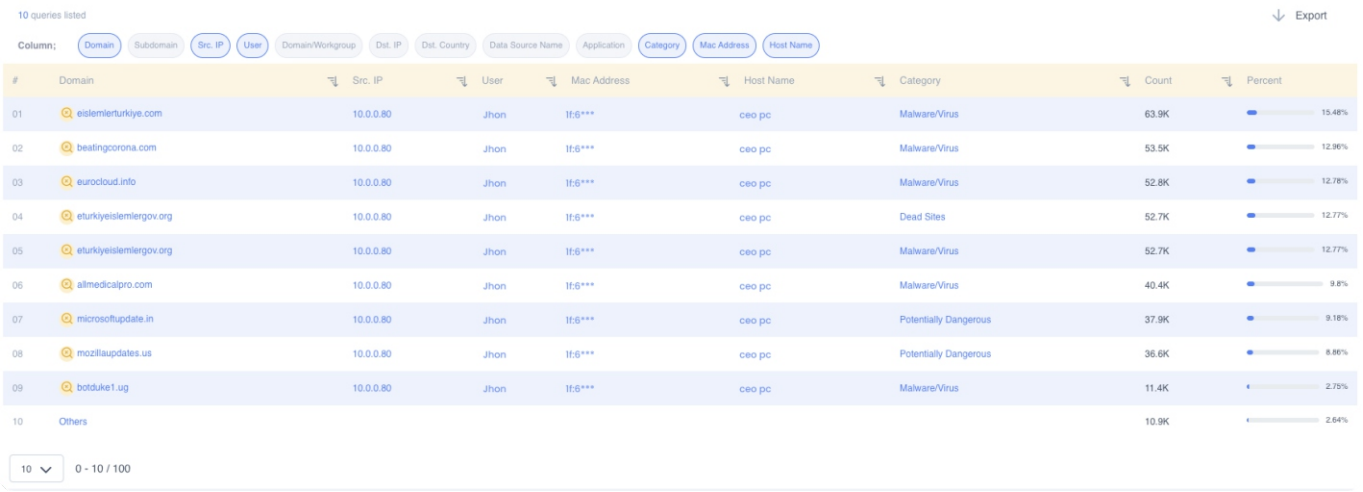
Malicious Traffic Detection

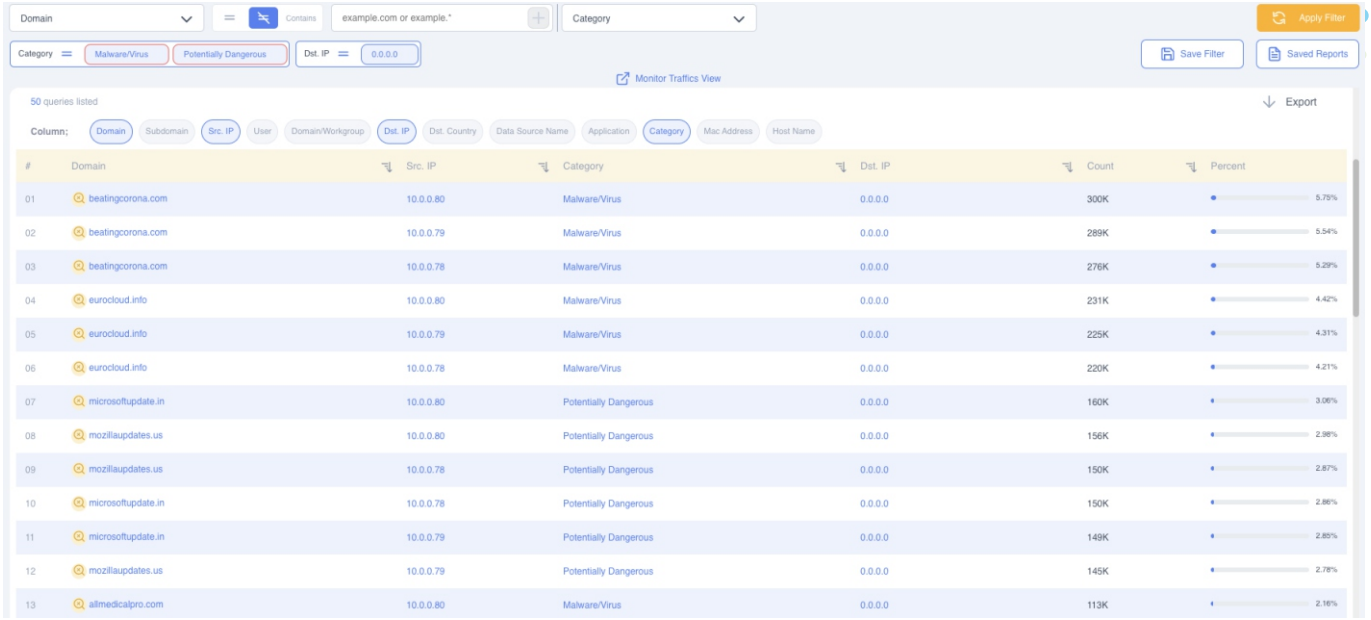
DNSSense detects malicious domains and devices querying these domains from DNS logs. In addition to DNS logs, Active Directory
Security log, DNS query user, DHCP log, Mac address and hostname records are enriched.
DNSSense classifies domains into 72 categories based on content and security level. Unclassified domains are logged as Firstly
Seen. Classification is guaranteed within 10 minutes without any intervention.

Invisible Malicious Traffic Detection
(Only with DNS Visibility)

Domains without an IP address

DNSSense detects malicious domains and devices querying these domains from DNS logs. In addition to DNS logs, Active Directory
Security log, DNS query user, DHCP log, Mac address and hostname records are enriched.
DNSSense classifies domains into 72 categories based on content and security level. Unclassified domains are logged as Firstly
Seen. Classification is guaranteed within 10 minutes without any intervention.





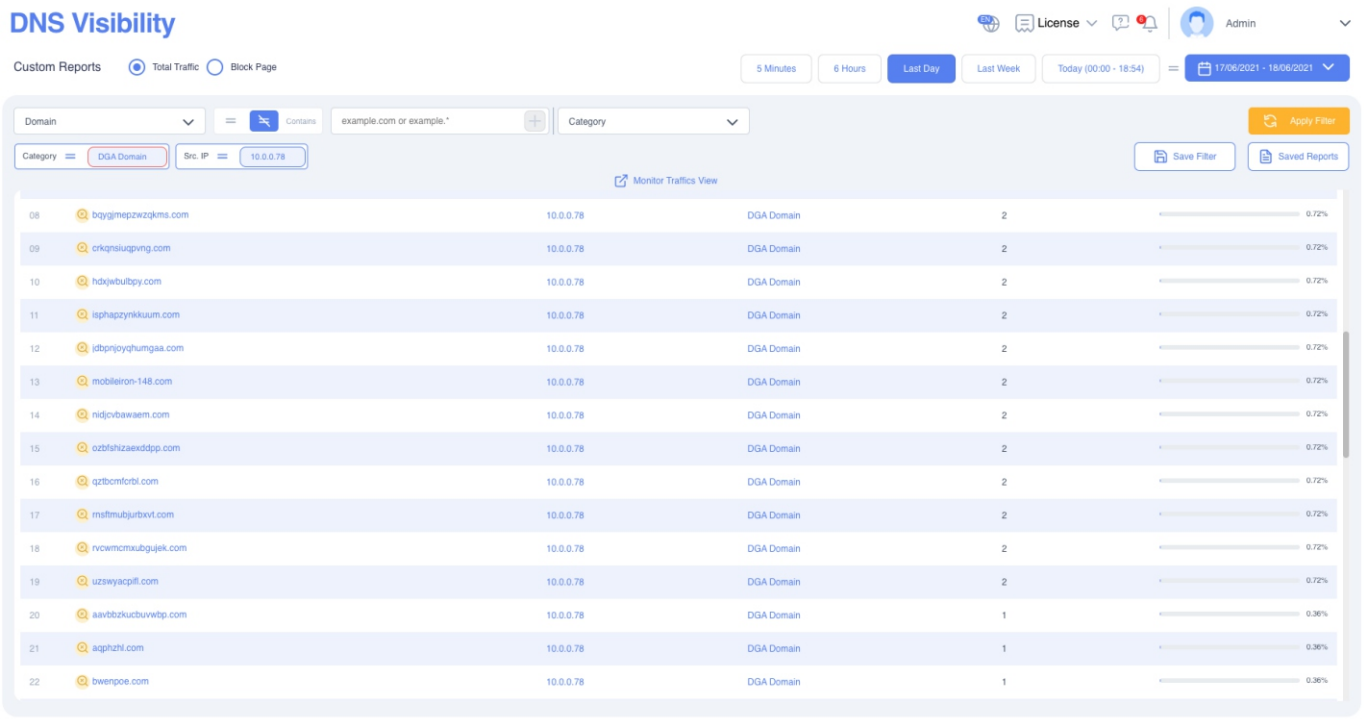
DGA *(Domain Generation Algorithm)* Domains

Another malicious activity that can only be viewed with DNS Log analysis is DGA (Domain Generation Algorithm) Domain queries. DGA domains are domains generated instantly by the machine according to the system clock. Domains are registered only when command is given and the Botnet CC ip address is entered. With the OTP logic used in Two-factor authentication (2FA), domains are queried only a few times.

In this way, the owner of the zombie army aims at two things;

- To prevent the command center connection domains from being detected by security researchers
- Unlocking the zombie army with a timer

Example report of a zombie device trying to connect to Botnet CC



Infected Device Detection

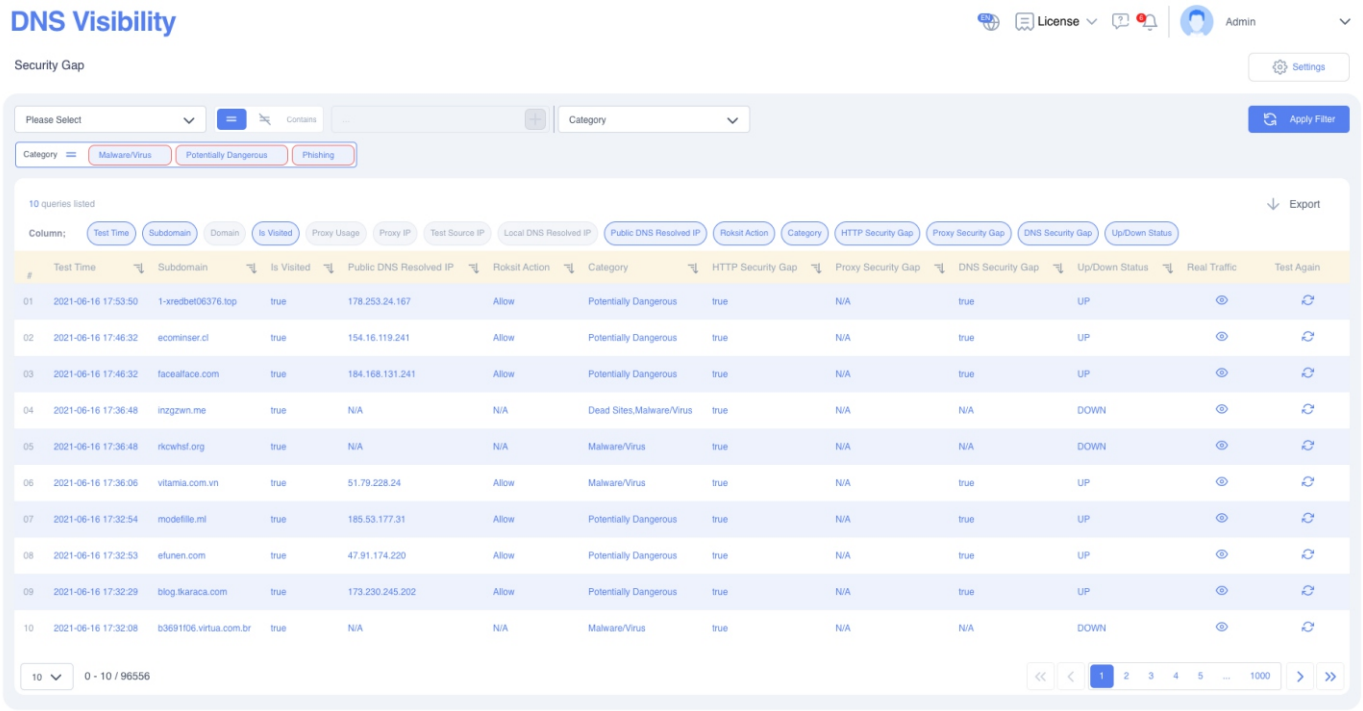
When DNSSense analyzes the DNS logs, it adds the permanent Active Directory User Name, Hostname and mac address to the report instead of the variable IP addresses. Thus, users and devices that constantly generate malicious traffic can be retrospectively examined and infected devices can be detected. As with the malicious traffic reports, examples of which are seen above, infected devices that are constantly trying to connect to the command center can be reported on the net. In addition, DNS Firewall, "Threat Hunter" modules of DNSSense make VMI connection to devices that make malicious DNS query, and processes, dlls and files that make malicious DNS query on the device can be detected.

Security Gap

The Security Gap feature is used to separate the records that the SoC team should prioritize while investigating the detected malicious traffic. Security Gap reports malicious traffic that cannot be detected by the Organization's existing security devices. Thus, it is ensured that successful attacks are given priority. For example, in a detected phishing attack, users who make the connection to the malicious link as a result of the failure of the existing security devices to be detected, are aimed to be determined instantly and to take quick action.

Security Gap simulates connecting to malicious domain in 3 different ways,

- Test with DNS query from existing DNS server
- Test with Http/Https request via proxy server
- Tests to reach malicious domain with direct connection http/https through Gateway.
  Security Gap = False if malicious traffic is blocked, Security Gap = True if not blocked.



Contextual Domain Info Enrichment (CDIE)

Previous reports included reports and findings if malicious traffic had been detected by DNSSense. However, in highly professionally designed attacks such as Solarwinds Sunburst, carefully selected domains could not be detected by any security vendor in the 9-months period between March 2020 and December 2020.

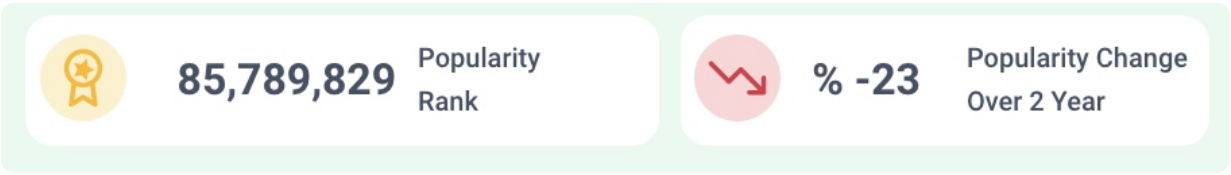
For the detection of such sophisticated attacks, DNSSense detects the anomaly of the corporate traffic regardless of the security level of the domain. It enriches detected anomalous traffic by leveraging Cyber-Xray infrastructure and enables the SoC team to detect sophisticated attacks. DNS Visibility anomaly detection system can give a warning when an abnormal situation occurs by learning the traffic of the institution. DNS Visibility has several anomaly detection rules. One of these rules is triggered when the domain is requested from the corporate network for the first time in the last 1 year. Thus, even if the domain entered for the first time is classified as safe, it will be examined. Relational data obtained from Cyber-Xray is reported in DNS Visibility, as well as all data is sent to the SIEM product.

Let's examine the issue through the scenario where Microsoft servers are connected to the domains microsofttoolkit.top and "microsoft365.today" for the first time. An alarm is generated on DNS Visibility immediately after a DNS query is made. Relational data to these domains are queried from Cyber-Xray and sent to the SIEM product. The submitted data are summarized under 8 headings. More detailed historical data can be viewed from the product web interface. The SoC team can perform the relationship of the domain with Microsoft and the evaluation of the alarm with this data.

1st domain to review is “mikrosofttoolkit.top”
For more detailed information review from the Cyber-Xray web interface:
https://www.Cyber-xray.com/#/anonymous-admin/dashboard/microsofttoolkit.top

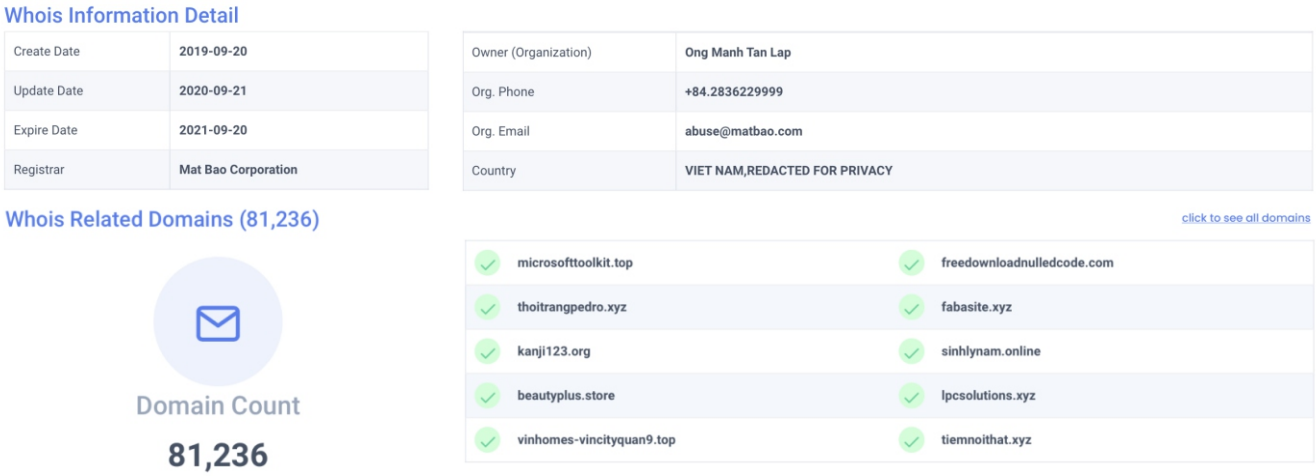
Popularity Score,

Calculated according to the inlinks and outlinks given to the domain from other internet domains. The more a domain receives links from many different domains, the more its popularity score increases. The popularity is calculated on the Cyber-Xray platform at 3-month intervals. The change in popularity in the last 2 years is also seen.



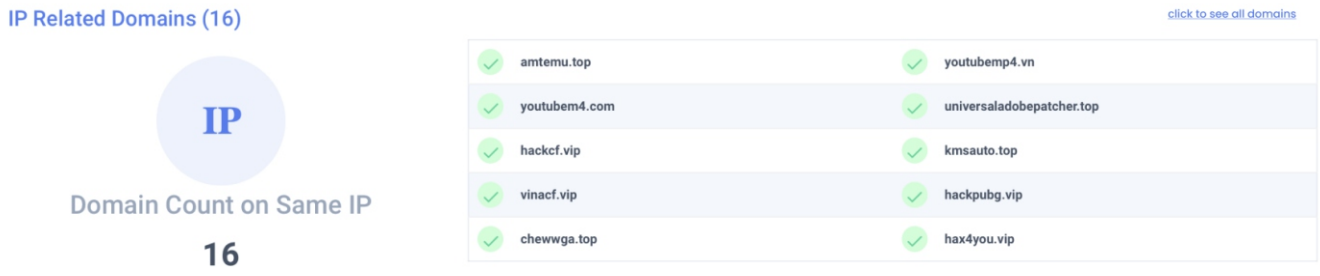
Whois and Whois releted other domain,

In the Whois records, there is no Microsoft domain in the list of other domains purchased by the owner of the domain.



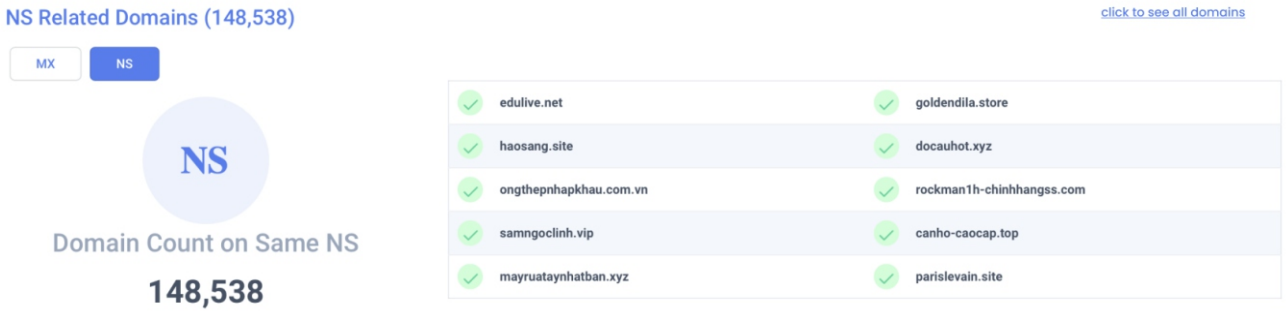
IP usage history and ip relation with other domain,

It is seen that it does not use the same ip address as any microsoft domain.



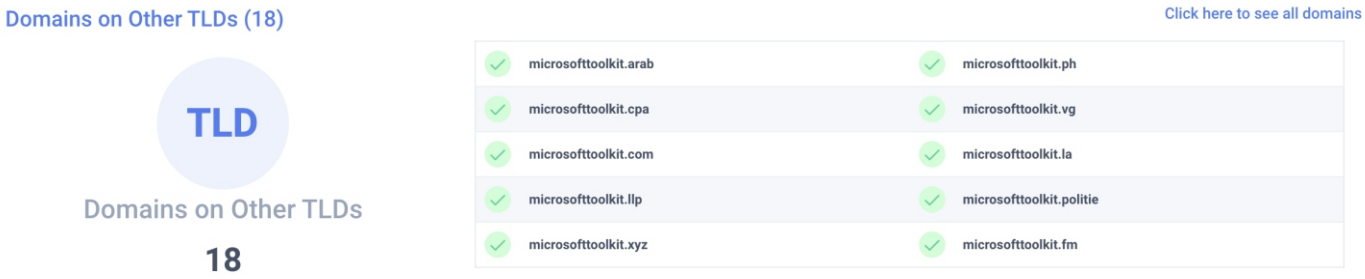
Name Server and Mail Server history, Domains using the same NS and MX server

We see that it does not show any similarity with the DNS server and mail server used by Microsoft domains



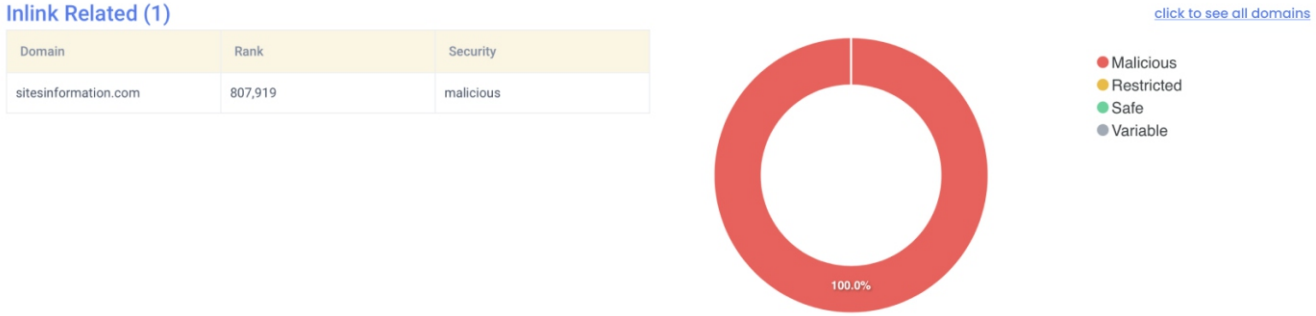
Other TLDs with the same name

We see that it does not show any similarity with the DNS server and mail server used by Microsoft domains



Inlink,

All domains that link to **microsofttoolkit.top** can be seen in the Inlink report. If there is no domain trusted by Microsoft, it can be expected to link from Microsoft domains. But only one malicious domain **microsofttoolkit.top** is linked.



Outlink,

When the “ ” domain was crawled, no link to any external domain was found. Although this data is not as much as inlink, it can be useful in terms of domain security scoring.

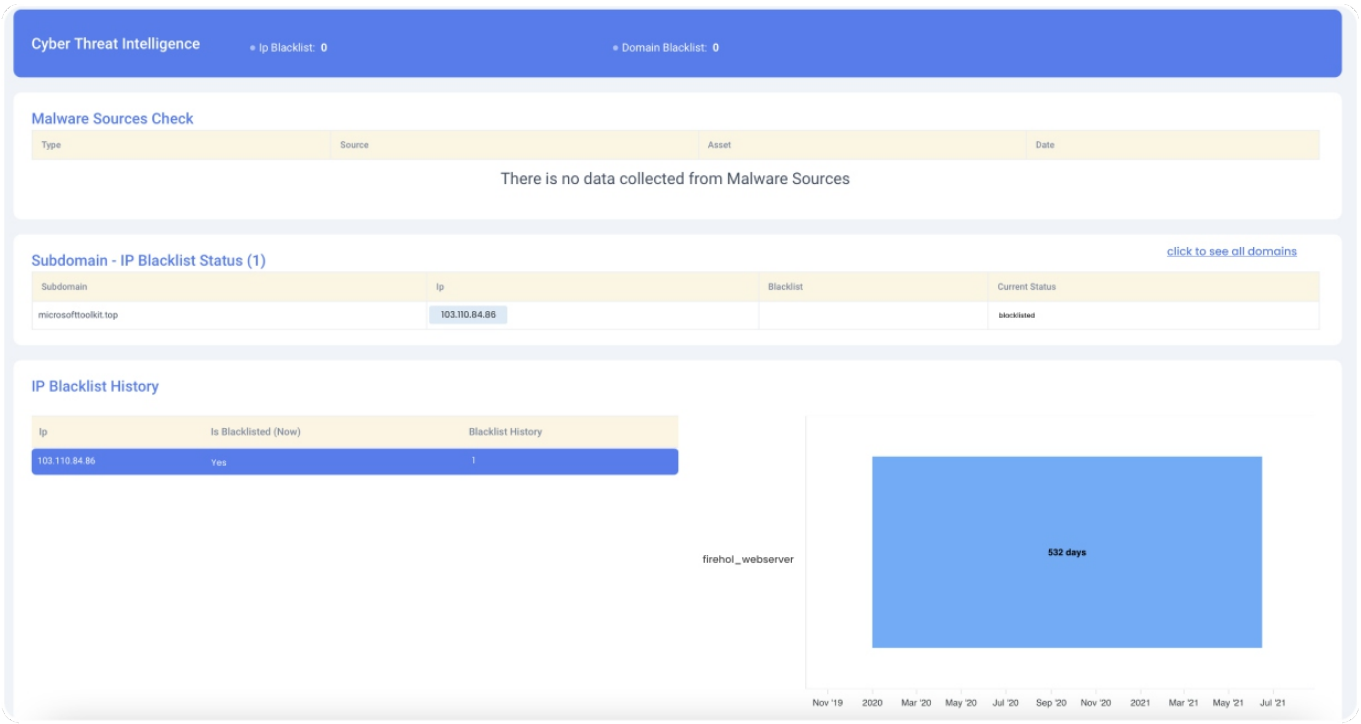
Outlink Related

No Data!

IP and domain OSINT Records,

The entry and exit dates of the subdomains of the domain or the IP addresses it uses are reported to any OSINT list in the world.

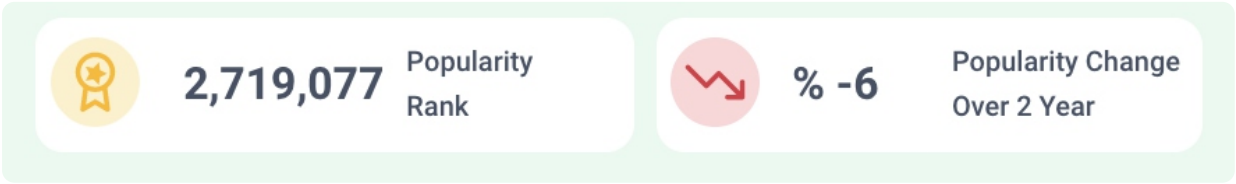
microsofttoolkit.top has no subdomains. The ip address it used has been in the same blacklist for 532 days.



2nd domain to review is “mikrosoft365.today”
For more detailed information review from the Cyber-Xray web interface:
https://www.Cyber-xray.com/#/anonymous-admin/dashboard/microsoft365.today

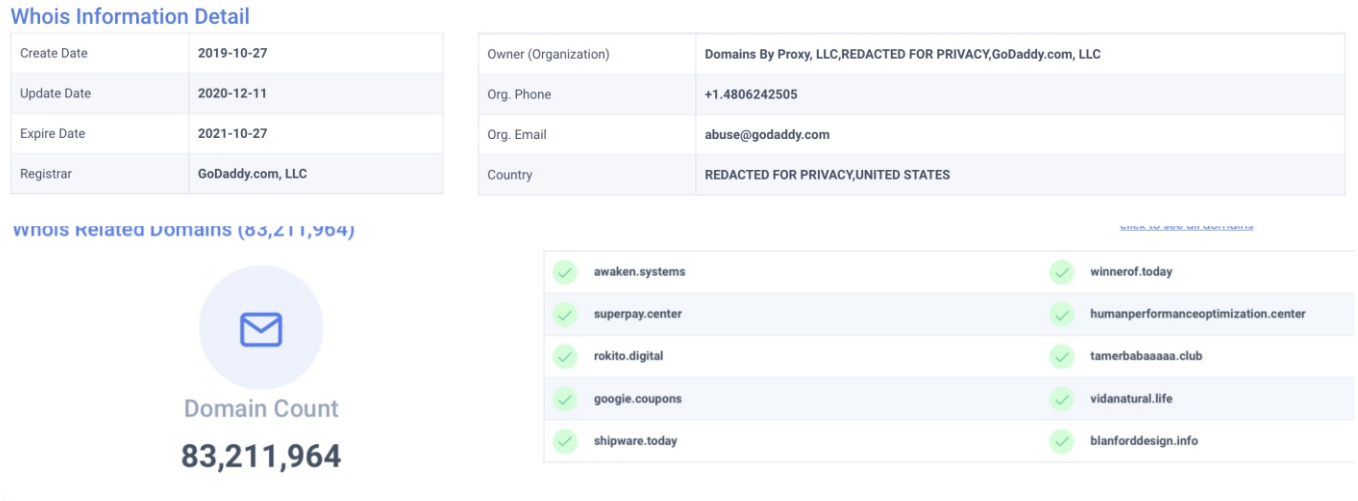
Popularity Score,

Calculated according to the inlinks and outlinks given to the domain from other internet domains. The more a domain receives links from many different domains, the more its popularity score increases. The popularity is calculated on the Cyber-Xray platform at 3-month intervals. The change in popularity in the last 2 years is also seen.



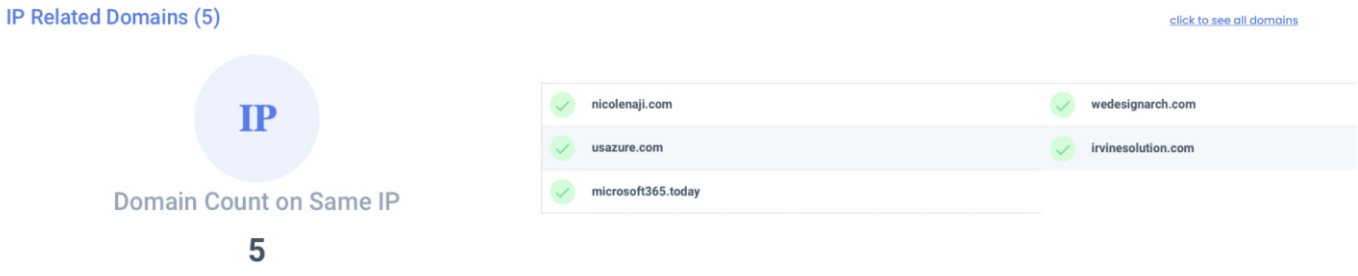
Whois and Whois releted other domain,

In the Whois records, there is no Microsoft domain in the list of other domains purchased by the owner of the domain.



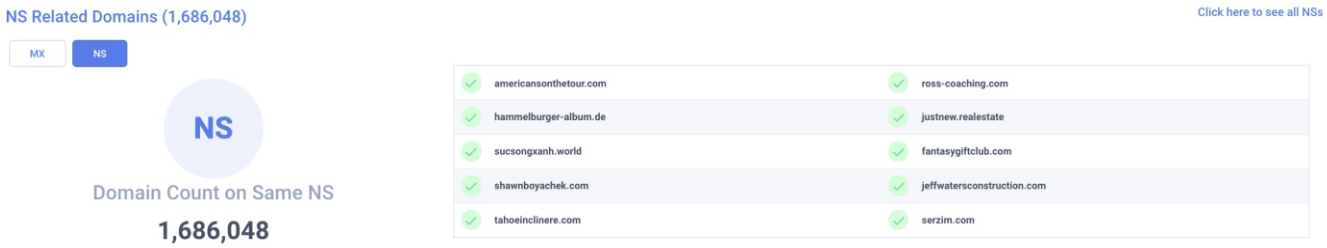
IP usage history and ip relation with other domain,

It is seen that it use the same 5 ip addresses.

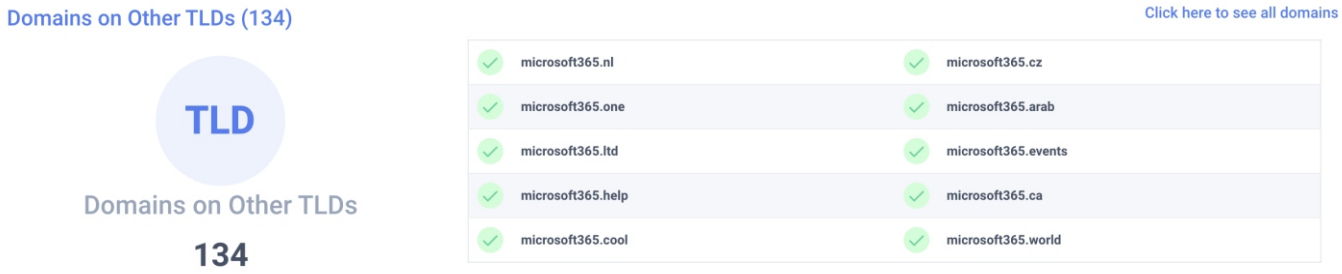


Name Server and Mail Server history, Domains using the same NS and MX server

We see that it does not show any similarity with the DNS server and mail server used by Microsoft domains

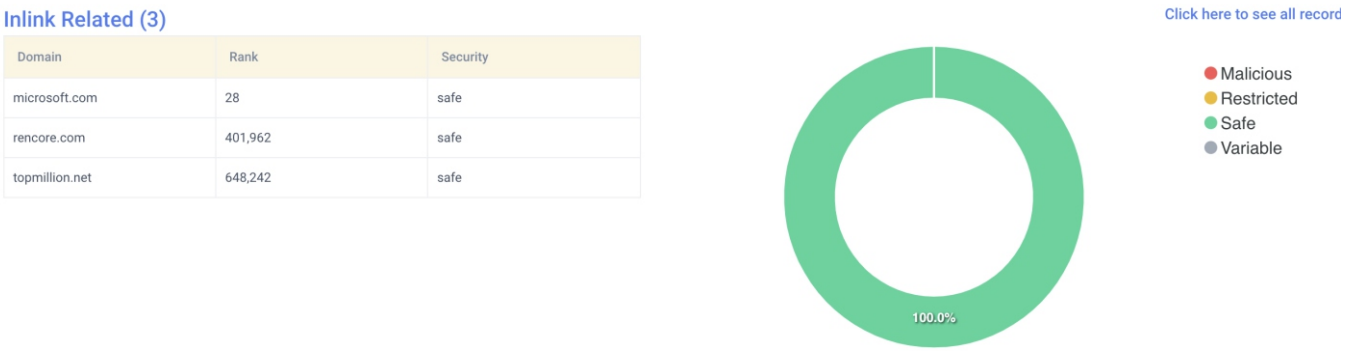


Other TLDs with the same name



Inlink,

The above information seems that the domain does not belong to microsoft, but it is seen that there is a link to the **"microsoft365.today"** domain from “microsoft.com”.
In addition, having popular and reliable domains in other linking domains increases the reliability of **"microsoft365.today"**.



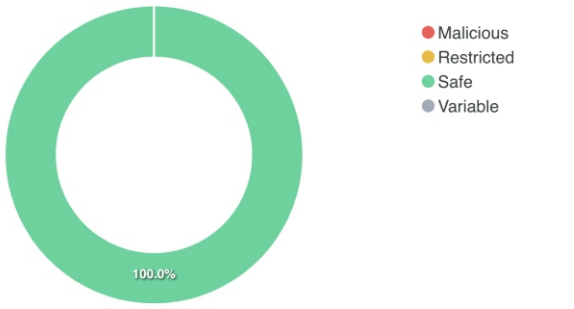
Outlink,

When the **“microsoft365.today”** domain is crawled, it is seen that it contains links to 22 all trusted domains.

Outlink Related (28)

Click here to see all records

Domain	Rank	Security
windows.net	332	safe
google.com	2	safe
github.com	17	safe
pinterest.com	22	safe
live.com	304	safe
microsoft.com	28	safe
michev.info	1,428,213	safe
pcmag.com	890	safe
sitemaps.org	187	safe
live.com	304	safe



IP and domain OSINT Records,

The entry and exit dates of the subdomains of the domain or the IP addresses it uses are reported to any OSINT list in the world.

Malware Sources Check

Type	Source	Asset	Date

There is no data collected from Malware Sources

Subdomain - IP Blacklist Status (2)

Click here to see all domains

Subdomain	Ip	Blacklist	Current Status
www.microsoft365.today	62.151.181.155	firehol_webserver pushing	blacklisted
microsoft365.today	62.151.181.155	firehol_webserver pushing	blacklisted

IP Blacklist History

Ip	Is Blacklisted (Now)	Blacklist History
62.151.181.155	Yes	3