

DETECT INVISIBLE MALICIOUS TRAFFIC

There are 79 million malware domains in the Cyber X-Ray database. Approximately 85% of these domains do not have an IP address.

Below is an example of a malicious traffic report found in a passive state. Since domains do not have IP addresses, it is recorded as 0.0.0.0 That is why you cannot see infected machines constantly trying to connect botnet ccs in other security devices that work in Layer 7 (Application Layer) such as firewalls, proxy devices, IPS etc...

		Source				Destination		Decision	
#	Time	Src Ip	Host Name	User	Subdomain	Dest. Ip	Category		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	google.com	0.0.0.0	Search Engines		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	facebook.com	0.0.0.0	Social Networks		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	shopify.com	0.0.0.0	Business Services		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	slack.com	0.0.0.0	Technology and Computer		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	bestingcorona.com	0.0.0.0	Malware/Virus		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	facebook.com	0.0.0.0	Social Networks		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	facebook.com	0.0.0.0	Technology and Computer		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	shopify.com	0.0.0.0	Business Services		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	google.com	0.0.0.0	Search Engines		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	facebook.com	0.0.0.0	Social Networks		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	google.com	0.0.0.0	Search Engines		
38	2022-02-12 12:07:18	10.0.0.27	oracle-db	Admin	bestingcorona.com	0.0.0.0	Technology and Computer		

Figure 1: Same Malicious Traffic Report

Domains without an IP Address

Malicious Domains

Some malicious domains prefer to be active only until they command the zombie army and when they do not have an IP address at other times, resulting in them being undetected in protocols other than DNS. These malicious traffics are "command center connection requests" generated by infected zombie devices. The fact that the domain does not have an IP address causes no event about malicious traffic on devices such as IPS, URL Filter.

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 the 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.





Some malicious activities described above can only be seen as a result of DNS Log analysis because infected clients are trying to connect to domains that do not have IP addresses. Roksit DNS Visibility product shows infected devices constantly trying to connect to the commandcenter. These are suspicious activities that need to be analysed by SOC teams carefully.

<div>DomainComputerUserSrc IpDomain IpUTM/NGFW</div>						
Domain	Category	User	UTM HTTP Request	Proxy HTTP Request	DNS Request	Attack Result
qjcycc.com	DGA Domain	CEO	Passed	Passed	Passed	Attack Successful
Faccebook.com	Phishing	Darek Baker	Passed	Blocked	Passed	Attack Blocked By Proxy
zzgg123.com	Malware/Virus	Daniel	Passed	Passed	Passed	Attack Successful
51news.xyz	Pornography	Natalie Burkard	Passed	Passed	Passed	Attack Successful



roksit.com

About Roksit

Roksit started out as a domain classification project. After developing a dynamic domain classification infrastructure, in 2016 it went on to provide cloud-based secure DNS service for enterprise-level customers. Soon after, it has focused on DNS analysis and Advanced DNS Visibility products for the needs of enterprise networks. Today, with three integrated products, it enables institutions to connect to the internet securely, while providing all DNS analysis data that SOC teams need.

Roksit's name and its logo are trademarks of Roksit Software R&D Inc, in the all countries. The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on Roksit's current product plans and strategy, which are subject to change by Roksit without notice. Roksit shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or similar materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from Roksit or its channel partners or licensors, or altering the terms and conditions of the applicable agreement governing access to the Roksit or related products and services. 15December2022-Version:001