roksit

Use Case

DEFEND FROM FIRSTLY SEEN DOMAINS

‘Zero-Day Attack’ is a term used to describe the threat of an unknown security vulnerability in computer software or application.

Since the vulnerability is not known in advance, the exploits often occur without the users’ knowledge.

Usually, a patch is required to resolve the issue, and it can only be released after the application developers are made aware of it, which is most of the time, they do not have enough time to address the issue.

%67

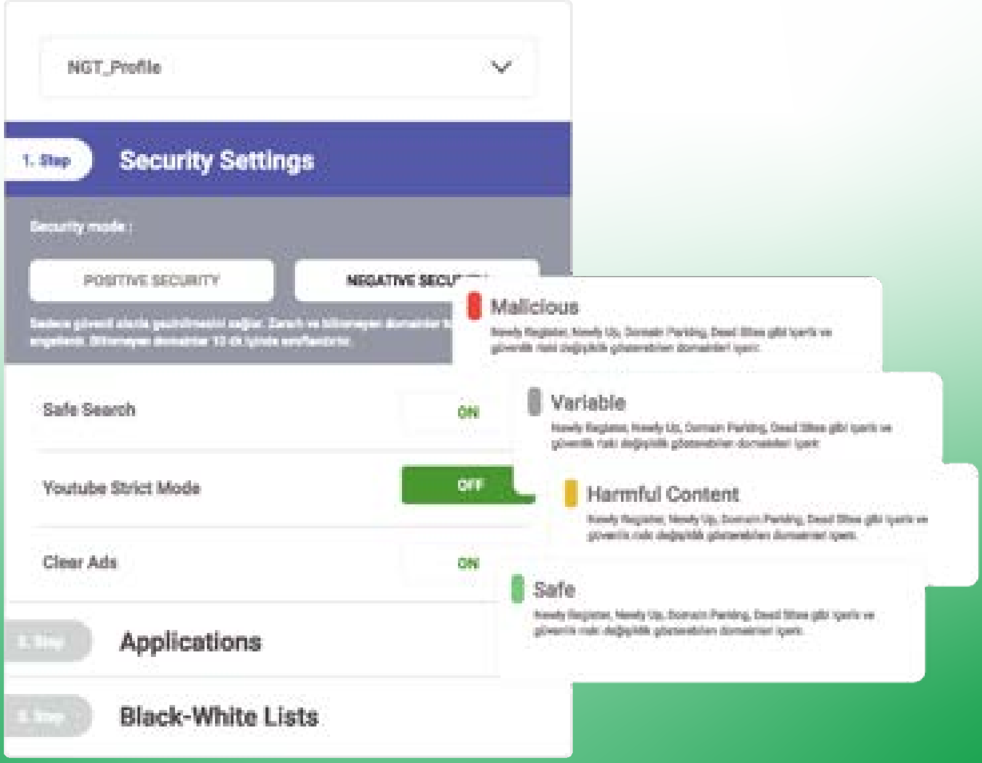
67% of cyber-attacks, including phishing and ransomware, are accomplished in less than two hours.

Most security products fail to detect these attacks within the first two hours when they are the most dangerous. Organisations are vulnerable to zero-day attacks since the average detection time is about 12 hours.

Roksit ‘s Solution

Today, Roksit Dynamic Threat Database Cyber X-Ray contains approximately 500 milliondomains that are being classified continuously. Domains requested for the frst time, which are not in the Cyber X-Ray database, are marked as First-seen domains by the artificial intelligence and are being classified immediately.

Roksit Positive Security Model allows any network connection attempt to a ‘First-seen’ domain to be temporarily blocked for a maximum of 10 minutes until it is classified as ‘Allowed’ according to network security policies.



NGT_Profile

1. Step Security Settings

Security mode :

POSITIVE SECURITY NEGATIVE SECU

Sadece güvenli alanlara gezinilmesini sağlar. Zararlı ve bilinmeyen domainler b engellenir. Bilinmeyen domainler 10 dk içinde sınıflandırılır.

Safe Search ON

Youtube Strict Mode OFF

Clear Ads ON

2. Step Applications

3. Step Black-White Lists

Malicious

Newly Register, Newly Up, Domain Parking, Dead Sites gibi içerik ve güvenlik riski değişiklik gösterebilen domainleri içerir.

Variable

Newly Register, Newly Up, Domain Parking, Dead Sites gibi içerik ve güvenlik riski değişiklik gösterebilen domainleri içerir.

Harmful Content

Newly Register, Newly Up, Domain Parking, Dead Sites gibi içerik ve güvenlik riski değişiklik gösterebilen domainleri içerir.

Safe

Newly Register, Newly Up, Domain Parking, Dead Sites gibi içerik ve güvenlik riski değişiklik gösterebilen domainleri içerir.

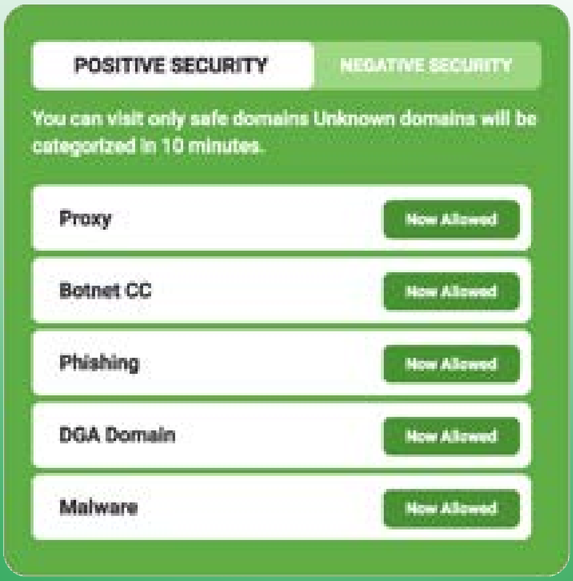
Positive Security Model

Cyber X-Ray scores 'First-seen' domains in a maximum of 10 minutes by checking more than 450 features (such as MX Record, TTL, domain age, CTI, Crawler, HTTPS, SSL, and so on) and categorising them with its artificial intelligence and deep learning algorithms.

To avoid false positives, malicious domain data is also gathered from nearly 400 CyberIntelligence Centres, including the USOM, which strengthens the scoring process but does not affect the category per se.

The connection will not be allowed if the relevant domain falls into the 'Block' category according to network security policies. Users will only be able to access it after it has been labelled 'Allowed' or 'Whitelisted' by the affected network security policy.

As a result, the network is protected from Zero-Day attacks with Roksit's 'Positive Security Model'.



You can visit only safe domains Unknown domains will be categorized in 10 minutes.

Proxy	Now Allowed
Botnet CC	Now Allowed
Phishing	Now Allowed
DGA Domain	Now Allowed
Malware	Now Allowed

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