Wiz Threat Intelligence

Wiz Threat Intelligence (Wiz TI) gathers information from the cloud threat landscape to keep you informed about the latest threats to your environment. Wiz TI identifies Indicators of Compromise (IoCs), explores the Tactics, Techniques, and Procedures (TTPs) utilized by threat actors, and discerns threat behaviors. It enables organizations to mitigate risks and improves their ability to detect and respond to actual threats.

Wiz TI uses both in-house and external threat intelligence sources to detect and address security risks and threats in your environment. The Wiz Threat Research team conducts extensive cloud-focused threat intelligence research, enhancing the product with valuable insights about various risks and threats.

Wiz TI includes:

- The Threat Center
- In-depth investigation of new cloud threats
- Public cloud threat intelligence
- Various capabilities

Threat Center

The Threat Center is an in-product board where the Wiz Threat Research team shares emerging threats and insights along with valuable information about how your environment may be impacted. It contains both internal threat advisories and public ones. Learn more about the Threat Center.

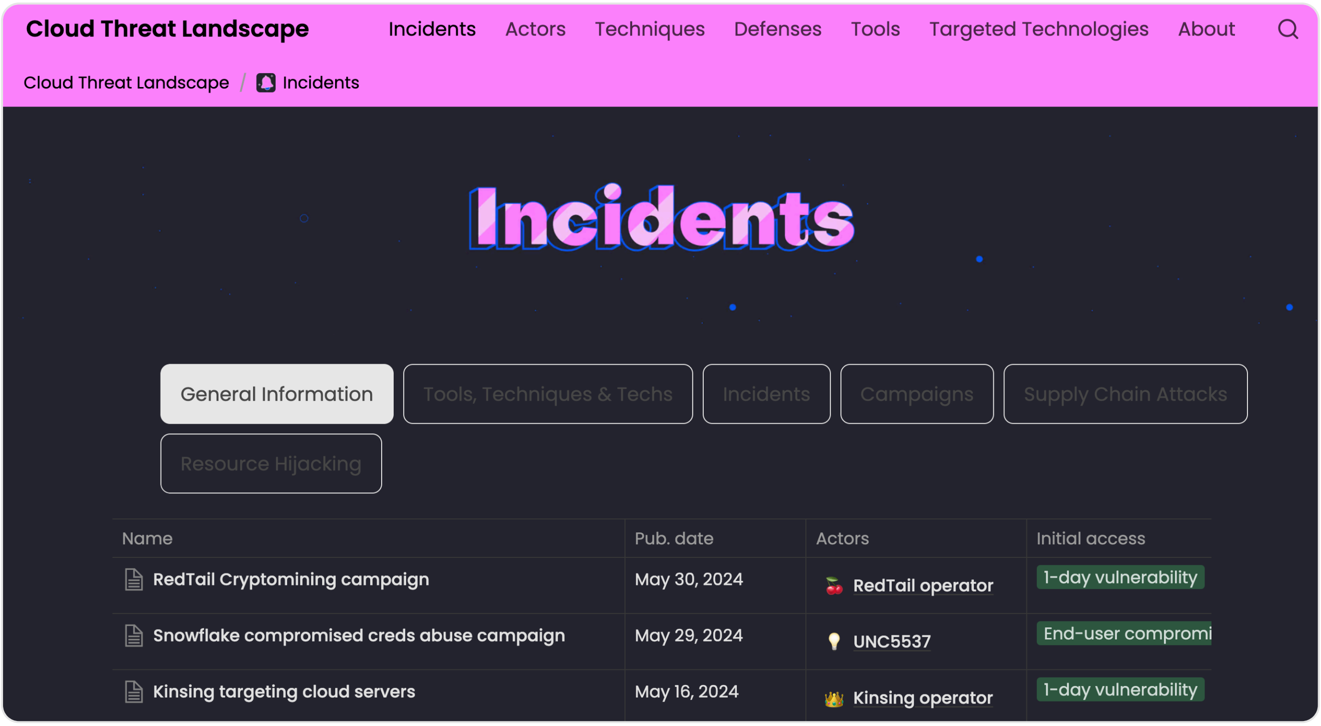
In-depth investigation of new cloud threats

The Wiz research team leverages its threat-hunting capabilities to uncover and investigate new threat actors and incidents in the cloud. The Threat Research team uses various tools and methods, including Wiz's threat detection tools such as the Wiz Runtime Sensor to uncover new threats in the cloud.

The team also regularly publishes insights on new cloud threats, for example PyLoose and Redirection Roulette.

Public cloud threat intelligence

Wiz maintains the Cloud Threat Landscape, a comprehensive threat intelligence database of cloud security incidents, actors, tools, and techniques investigated by the Threat Research team. The Cloud Threat Landscape is available publicly for the benefit of the cloud security community to use.



Name	Pub. date	Actors	Initial access
RedTail Cryptomining campaign	May 30, 2024	🍒 RedTail operator	1-day vulnerability
Snowflake compromised creds abuse campaign	May 29, 2024	💡 UNC5537	End-user compromi
Kinsing targeting cloud servers	May 16, 2024	👑 Kinsing operator	1-day vulnerability

Wiz is also a sponsor, maintainer, and contributor to the CloudVulnDB project, thereby facilitating the creation of a centralized cloud vulnerability database. This is by cataloging CSPs' security mistakes and listing the steps CSPs' customers can take to detect or prevent these in their environments.

Capabilities

Wiz TI utilizes advanced processes and research tools to add and improve built-in Policies to accommodate new and emerging cloud threats:

Tactics, Techniques, and Procedures (TTPs)

The Wiz research team investigates various TTPs that are used by threat actors in the cloud based on ongoing threat intelligence research, threat hunting, and in response to high-profile incidents such as LAPSUS$.

By being well-acquainted with potentially malicious behaviors, the team crafts a vast set of built-in Threat Detection Rules to identify these behaviors in your environment based on data from cloud events and the Runtime Sensor. Learn about cloud events & detection and Threat Detection Rules.

IP address and domain reputation

Wiz leverages Recorded Future and internally-developed tools to identify mal addresses and domains associated with cyber attacks, data breaches, or othe

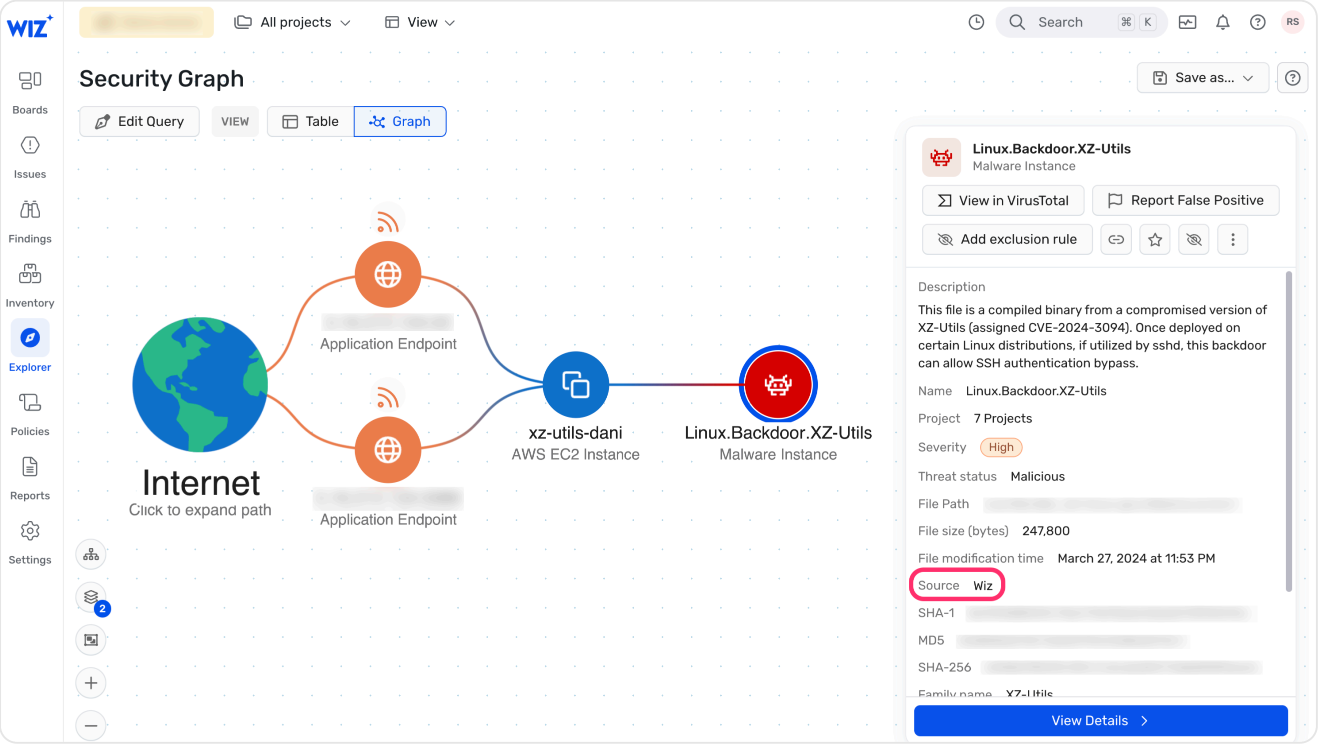
English ▲

malicious activities. Learn about malicious IP and domain detection. Wiz's built-in Threat Detection Rules incorporate this data to help identify malicious activity and improve detection accuracy and severity. Learn more about Threat Detection Rules.

Malware detections

Wiz partners with the market leader ReversingLabs to identify malicious file hashes. The Wiz Research Team also constantly investigates emerging threats and maintains hash detections and a proprietary collection of pattern-detection YARA Rules that have been manually examined by them and confirmed to be malware.

Based on these file hashes, Wiz identifies malware while agentlessly scanning snapshots and detects real-time execution of malware on workloads covered by the Runtime Sensor. Learn about malware detection.



Linux.Backdoor.XZ-Utils
Malware Instance

Description
This file is a compiled binary from a compromised version of XZ-Utils (assigned CVE-2024-3094). Once deployed on certain Linux distributions, if utilized by sshd, this backdoor can allow SSH authentication bypass.

Name Linux.Backdoor.XZ-Utils
Project 7 Projects
Severity High
Threat status Malicious
File Path [redacted]
File size (bytes) 247,800
File modification time March 27, 2024 at 11:53 PM
Source Wiz
SHA-1 [redacted]
MD5 [redacted]
SHA-256 [redacted]
Family name XZ-Utils

Vulnerabilities

Wiz leverages multiple updated vulnerability databases to keep pace with the ever-changing world of vulnerability assessment. The Wiz Vulnerability Catalog is automatically updated daily from many different open-source and commercial feeds.

These vulnerabilities can then be detected in your code and cloud resources during workload scanning and code scanning. Learn more about vulnerability detection.

Software misconfigurations

The Wiz Threat Research team uses open-source Nuclei templates to craft Host Configuration Rules. By leveraging threat intel research and threat hunting, they craft only the most relevant rules to detect potentially exploitable misconfiguratio about the Dynamic Scanner matcher for Host Configuration Rules.

English ▲

Updated 10 days ago

← Threat Advisories Overview

July 2024 →

Did this page help you? Yes No

English