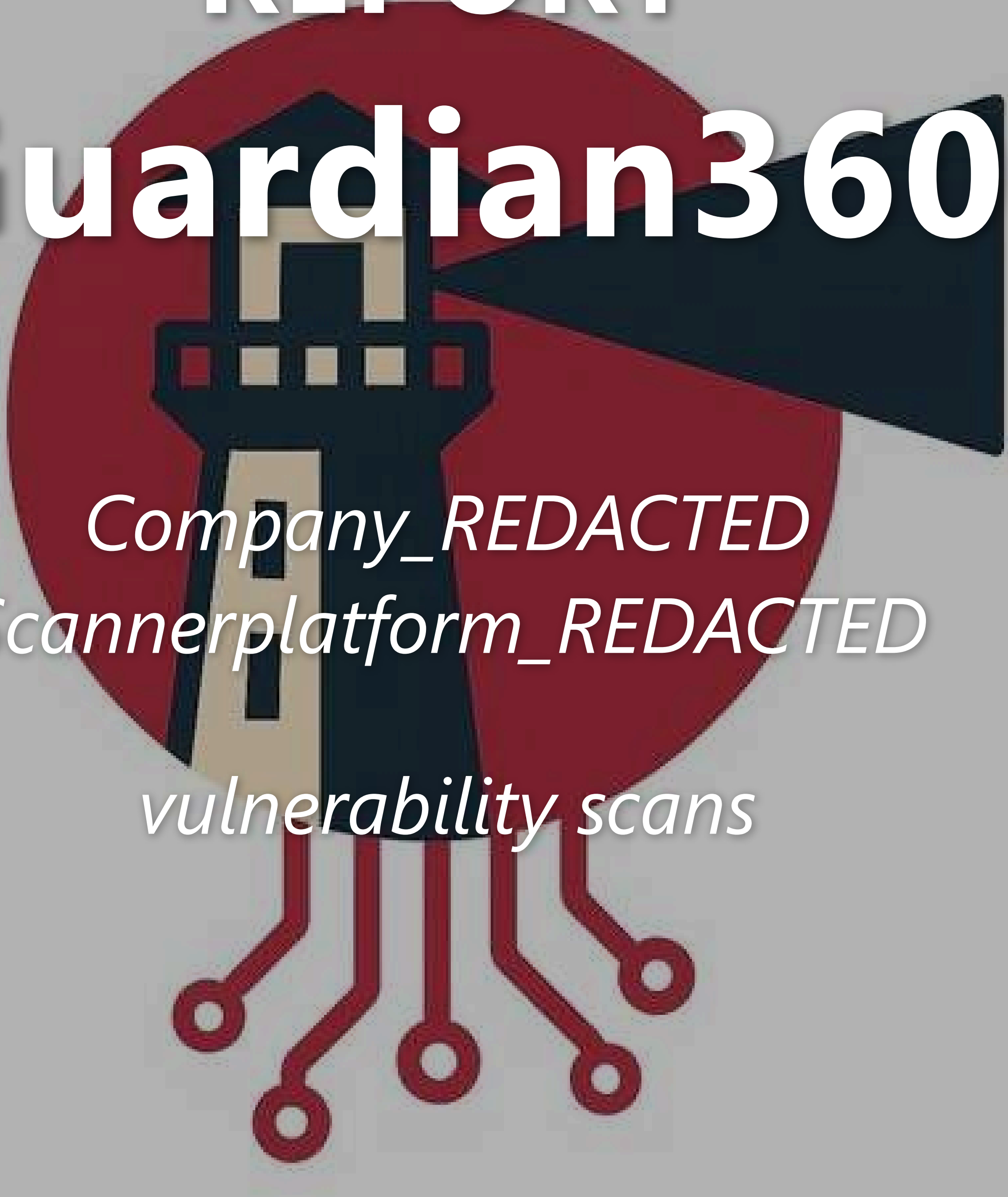
netcure

REPORT

Guardian360



Company_REDACTED
Scannerplatform_REDACTED

vulnerability scans

May 2025

Redacted
Redacted
Redacted
Redacted
Redacted

Table of contents

Introduction

This report presents the results of the recently conducted vulnerability scan at, a crucial component of our ongoing efforts to safeguard your digital environment. The purpose of this report is to identify and address potential vulnerabilities within your network infrastructure, ultimately aiming to protect your organization against cyber threats. Our dedicated team of security experts has carried out a thorough investigation and performed a detailed analysis of your systems, applications, and network configurations. This assessment included the identification of known vulnerabilities, configuration errors, and potential risks that could compromise the integrity and confidentiality of your data. This report not only provides an overview of the identified vulnerabilities but also includes recommendations and strategies to strengthen your security posture. It is intended as a practical tool to inform you of potential risks, enabling you to take proactive measures to protect your organization. We believe in transparency and collaboration. Therefore, we invite you to review these findings carefully and reach out to us for further discussion or clarification. Your involvement in enhancing your security infrastructure is essential, and we are ready to support you in implementing effective security measures.

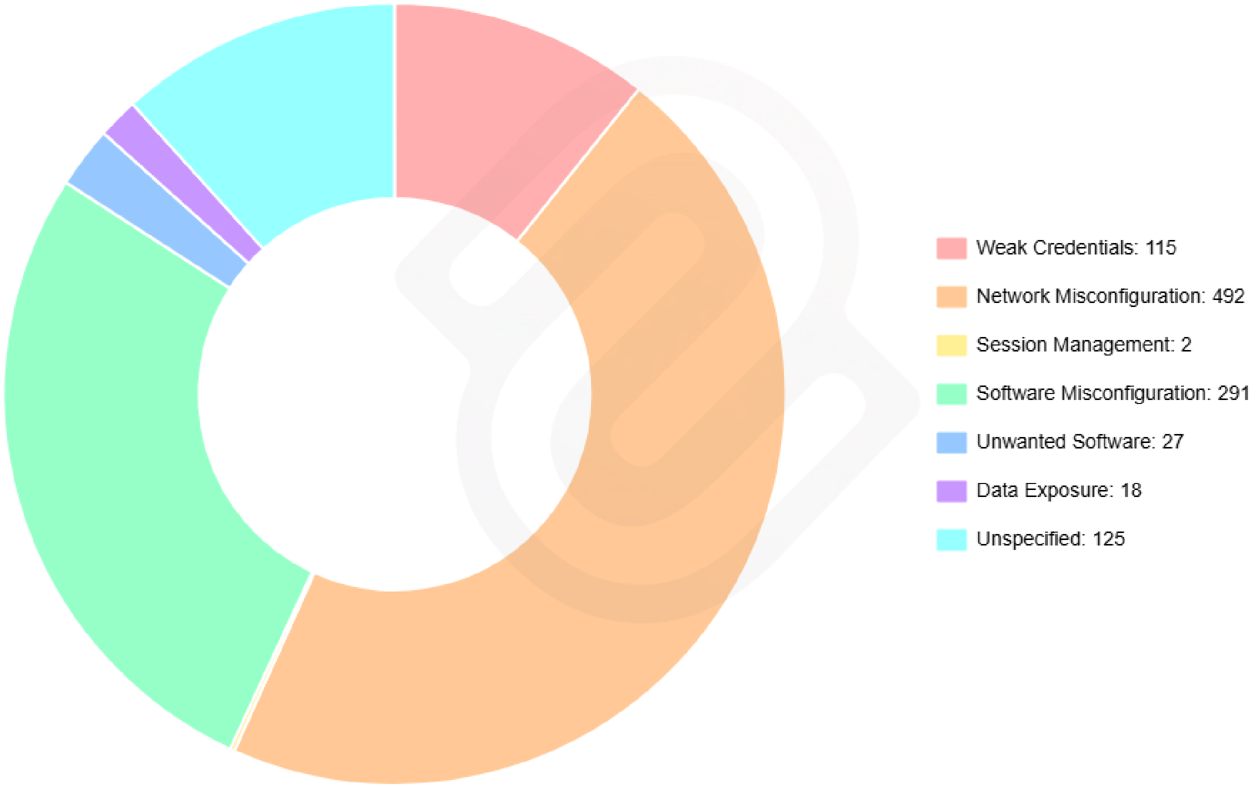
If you have any questions about this report, you can always contact us at soc@netcure.be

Vulnerabilities by Risk Level

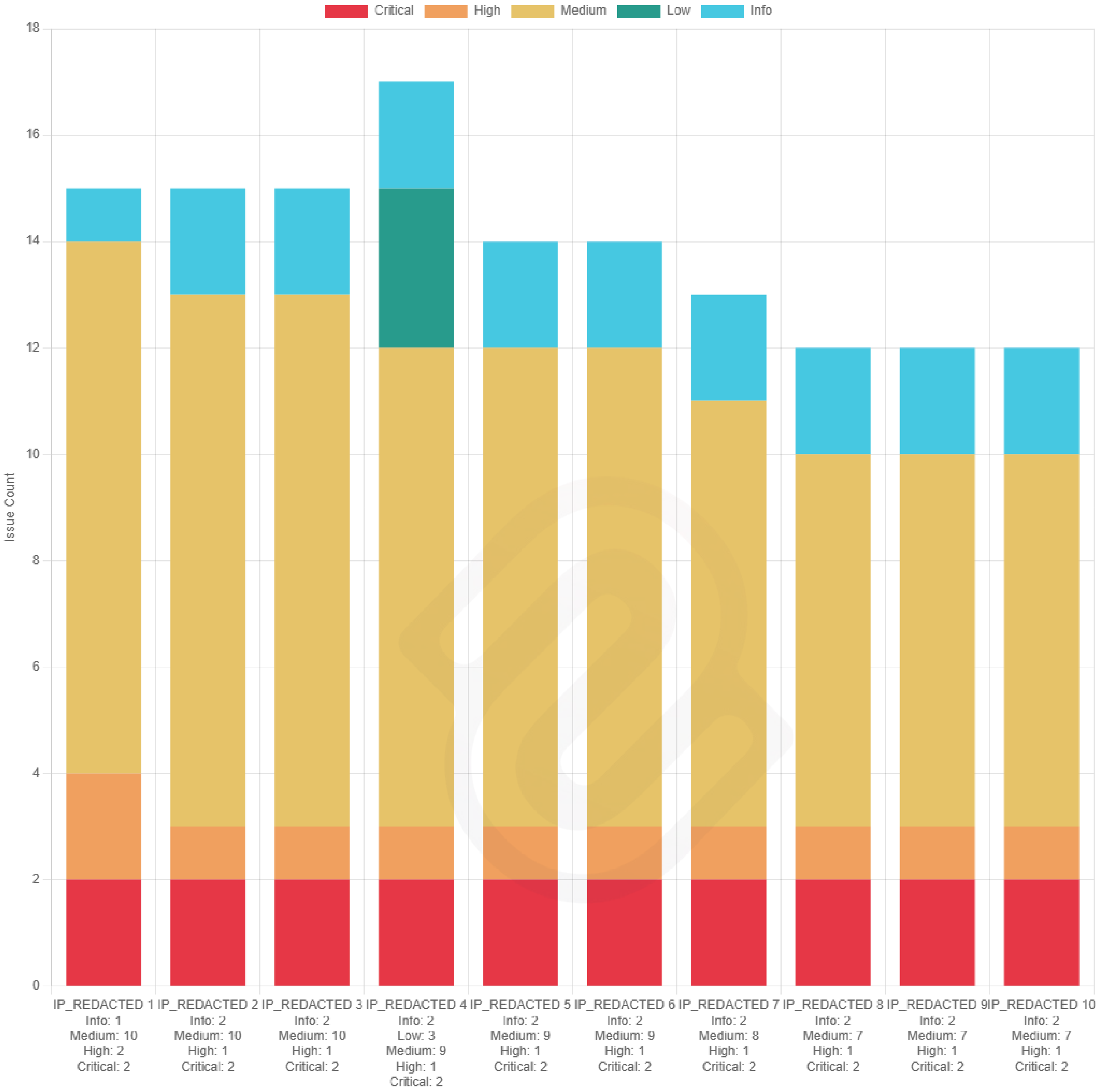
In Guardian360, risk levels are determined based on the type of vulnerability or nonconformity identified and the context in which it appears. A single finding can be associated with multiple risk indicators depending on the systems affected and the severity of the issue. Below is a summary table of the risk levels detected during the most recent scans:

critical	high	medium	low	info
115 *(Weak Credentials: 115)*	64 *(Network Misconfiguration: 62)* *(Session Management: 2)*	601 *(Network Misconfiguration: 333)* *(Software Misconfiguration: 241)* *(Unwanted Software: 27)*	165 *(Network Misconfiguration: 97)* *(Software Misconfiguration: 50)* *(Data Exposure: 18)*	125 *(Unspecified: 125)*

Amount of issues per nonconformity



Top IPs by Risk Severity (Stacked by Risk Level)



Vulnerability Descriptions

In the section below, you will find detailed descriptions of all identified vulnerabilities and security findings that were discovered during the assessment. For each finding, we have included recommended mitigation and prevention measures. **Please note that this overview is limited to findings classified as critical**. These are the most severe risks, with the highest potential to negatively impact your systems, data, or operations. It is essential to address these issues promptly in order to reduce your exposure to cyber threats and improve the resilience of your digital environment.

3.1 Issue: HTTP default or weak credentials found

Nonconformity

Weak Credentials

Description

Valid (default/weak) login credentials were found. This might provide an attacker full access to the application or service and potentially provides access to the underlying operating system.

Technical Details

- **port:** 80

Solution

Please change default credentials by setting a strong password and integrate this step in your deployment procedures.\nWe recommend setting passwords longer than 15 characters preferably in the style of four words like: stopped computer Verb bezig@\nThese are much harder to crack by brute force attacks and hash crackers.

IP Addresses

IP	Detected at	FQDN	Scannerobject
IP_REDACTED	2025-01-09 12:20:27	FQDN_Redacted	Scannerobject_Redacted

3.2 Issue: SMB default or weak credentials found

Nonconformity

Weak Credentials

Description

Valid (default/weak) login credentials were found. This might provide an attacker full access to the application or service and potentially provides access to the underlying operating system. To verify SMB access with valid credentials use the following steps on a Linux environment like Debian or Ubuntu. Install the Impacket library to perform SMB connections: $ apt-get update $ apt-get-y install git python3-setuptools $ git clone https://github.com/SecureAuthCorp/impacket.git $ cd impacket/ $ python3 setup.py install To test a valid username/password credential perform the following command: $ smbclient.py :@ To test anonymous access perform the following the command: $ smbclient.py-no-pass If an error is returned this will mean authentication was unsuccessful. Otherwise authentication was successful and a user session can be attempted with the 'login' command. NOTE: this does not always allow for any other SMB commands to be executed. However an authenticated session could be sufficient in certain circumstances. For example in the scenario where a vulnerability is exploited on authenticated sessions.

Technical Details

- **port:** 445

Solution

Please change default credentials by setting a strong password and integrate this step in your deployment procedures. We recommend setting passwords longer than 15 characters preferably in the style of four words like: stopped computer Verb bezig@ These are much harder to crack by brute force attacks and hash crackers. If anonymous access was possible please consider hardening your Windows system by setting the following group policies in Computer Configuration => Windows Settings => Security Settings => Local Policies => Security Options: * Network access: Allow anonymous SID/Name translation (disable) * Network access: Do not allow anonymous enumeration of SAM accounts (enable) * Network access: Do not allow anonymous enumeration of SAM accounts and shares (enable) * Network access: Let Everyone permissions apply to anonymous users (disable) * Network access: Named Pipes that can be accessed anonymously (none) * Network access: Shares that can be accessed anonymously (none) For more information regarding these steps see the following links: * https://jbcomp.com/disable-smb-null-windows-2012/ * https://www.blumira.com/integration/how-to-disable-null-session-in-windows/ In situations where the system is not running Windows please refer to the system's manual or contact the specific vendor on how to mitigate this issue. If no mitigation is possible on the system itself consider filtering access based on source IP addresses.

IP Addresses

IP	Detected at	FQDN	Scannerobject
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:35:25	FQDN_Redacted	Scannerobject_Redacted

3.3 Issue: FTP default or weak credentials found

Nonconformity

Weak Credentials

Description

Valid (default/weak) login credentials were found. This might provide an attacker full access to the application or service and potentially provides access to the underlying operating system.

Technical Details

- **port:** 21

Solution

Please change default credentials by setting a strong password and integrate this step in your deployment procedures.\nWe recommend setting passwords longer than 15 characters preferably in the style of four words like: stopped computer Verb bezig@\nThese are much harder to crack by brute force attacks and hash crackers.

IP Addresses

IP	Detected at	FQDN	Scannerobject
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:36:03	FQDN_Redacted	Scannerobject_Redacted

3.4 Issue: SNMP default or weak credentials found

Nonconformity

Weak Credentials

Description

Valid (default/weak) login credentials were found. This might provide an attacker full access to the application or service and potentially provides access to the underlying operating system.

Technical Details

- **port:** 161

Solution

Please change default credentials by setting a strong password and integrate this step in your deployment procedures.\nWe recommend setting passwords longer than 15 characters preferably in the style of four words like: stopped computer Verb bezig@\nThese are much harder to crack by brute force attacks and hash crackers.

IP Addresses

IP	Detected at	FQDN	Scannerobject
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted

Rows continuing on next page...

IP	Detected at	FQDN	Scanner_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted

Rows continuing on next page...

IP	Detected at	FQDN	Scanner_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted

Rows continuing on next page...

IP	Detected at	FQDN	Scanner_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-01-09 12:43:23	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-02-20 13:21:53	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-02-20 13:21:53	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-02-20 13:21:53	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-03-08 13:29:36	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-03-08 13:29:36	FQDN_Redacted	Scannerobject_Redacted
IP_REDACTED	2025-03-21 13:13:00	FQDN_Redacted	Scannerobject_Redacted