Barracuda Email Threat Scanner

https://campus.barracuda.com/doc/78807326/

Use the free Barracuda Email Threat Scanner to discover spear phishing and targeted attacks that reside in your Microsoft 365 account. The scanner uses Barracuda Networks' artificial intelligence engine to scan your Microsoft 365 accounts for various attacks that might be sitting in user mailboxes. The cloud-based scanner runs in the background and can find threats including spear phishing attacks, business email compromise, and account takeover attempts. When finished, the scan highlights:

- Threats found in your organization – by number
- Threats found in your organization – by type
- Which of your employees have the most threats
- The status of your domain's DMARC record

Barracuda Email Threat Scanner scans emails received in the last 12 months. It takes about two minutes to sign up for the scan. The scan duration depends on the size of your Microsoft 365 mailboxes and can take from 1 to 24 hours.

Notes

You must have Global Admin privileges in your Microsoft 365 account to set up the Barracuda Email Threat Scanner. If you are not an administrator, you can request a demo on the opening page of the scanner.

Barracuda values your privacy. To learn more about scan privacy and the Microsoft permissions required to run a scan, refer to Data Privacy for the Barracuda Email Threat Scanner.

Starting the Scan

If you have a Barracuda account:

1. Navigate to https://scan.barracudanetworks.com.
2. Enter your Barracuda account credentials and click **Sign In**.
3. Review the Barracuda Networks Privacy Policy. If you agree, select the checkbox.
4. Click **Scan Now**.

The Barracuda Email Threat Scanner immediately begins scanning your Microsoft 365 account for threats. While the scan is in progress, status messages at the top of the screen inform you of **Scan status**, time **Started**, **Time remaining**, **Emails scanned**, and number of **Threats detected** so far.

If you *do not* already have a Barracuda account:

1. Navigate to https://scan.barracudanetworks.com.
2. Click **Sign Up with Microsoft 365**.
3. Click the appropriate Microsoft 365 account.
4. If you are not already signed into your Microsoft 365 account, enter the corresponding password, and click **Sign In**. If you are already signed in, this step does not appear.
5. Review the permissions requested by Microsoft. If you accept, click **Accept**.
6. Create a Barracuda Networks account, including your email, a password, and phone number. Review the Barracuda Networks Privacy Policy. If you agree, select the checkbox.
7. Click **Scan Now**.

The Barracuda Email Threat Scanner immediately begins scanning your Microsoft 365 account for threats. While the scan is in progress, status messages at the top of the screen inform you of **Scan status**, time **Started**, **Time remaining**, **Emails scanned**, and number of **Threats detected** so far.

Scan Summary

Reviewing the Scan Summary

When the threat scan is complete, the header section displays a green bar and the **Scan Status** is **Scan completed**. The header also displays the time the scan was completed, the **Scan duration**, total number of **Emails scanned** in your Microsoft 365 account and, of those, the number of **Threats detected**.

The Scan Summary shows your results at a glance. Click **Details** in any section to see detailed information later in the report.

- **Threats Found** – Number of threat emails found in all of your employee inboxes for each of the past 12 months. The cumulative total of threats for the past 12 months displays above the graph. Hover over any point for the number of threats in that month.
- **Employees with Threats** – Total number of unique employees who received at least one threat email for each of the past 12 months. Cumulative total for the year displays above the graph. Hover over any point for the number of employees affected in that month.
- **Threat Types Found** – Total email threats received for the past 12 months, shown by category. Hover over each threat type to see the number of threats in that category during the last 12 months and also for more information about that threat type.
- **Domain DMARC Status** – Number of your organization's domains in each of the DMARC protection status categories.

Employees

The Employees section shows your employees and information about the attacks they received, if

any.

Risk Level – At the top of the Employees section, boxes show employees with mailboxes in your Microsoft 365 account. Each box displays the total number of employees and the number of employees in the High, Medium, and Low-Risk categories. Click a box to see employees in that group displayed in the sortable Employees table. By default, the table is sorted by Risk-Level.

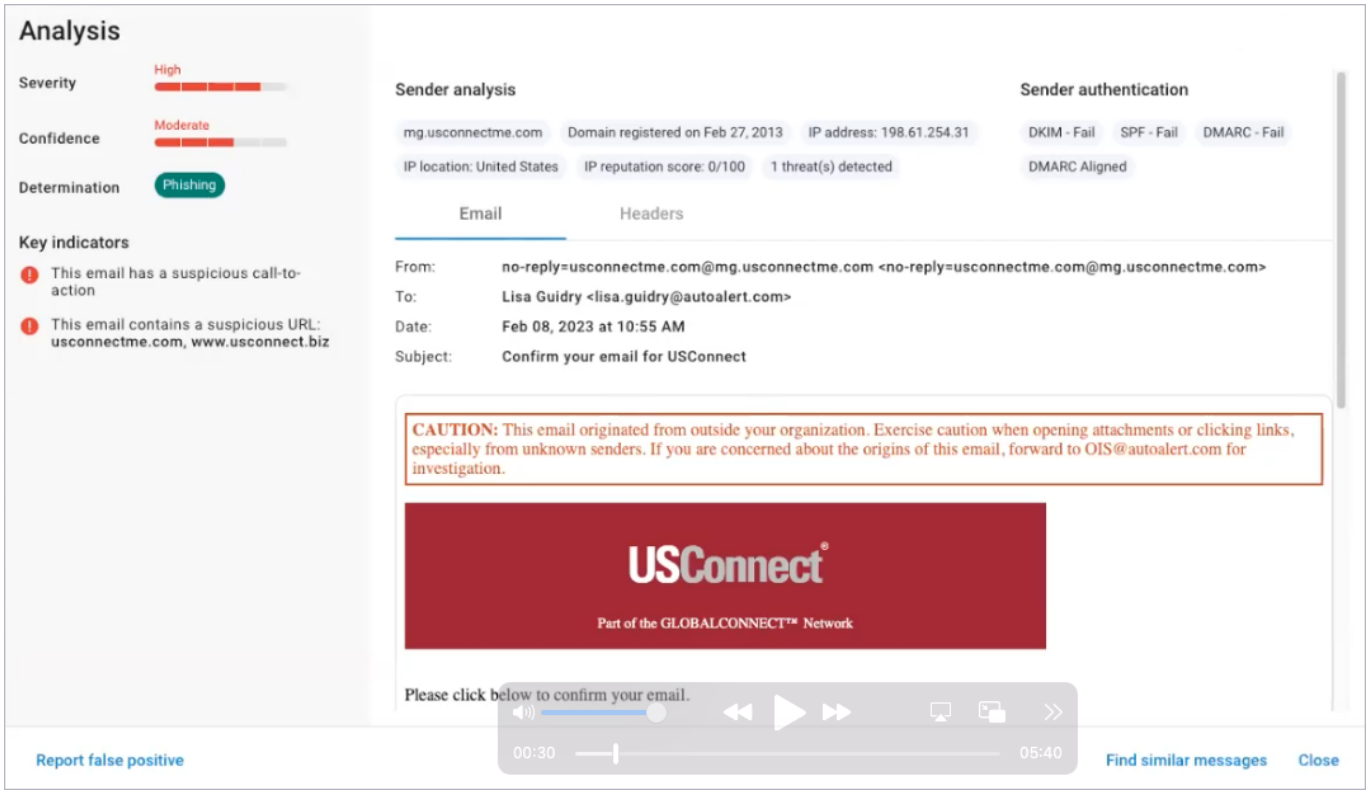
Risk level is affected by factors including whether the employee has access to financial files or is an executive in your organization; the number and type of factors for an individual determines their risk level. High-risk factors for each individual, if they exist, are displayed in the table.

Searching – To narrow the list of employees displayed, use the Search employees box. You might use search terms including full or partial name, email, or title.

Viewing Emails – If an employee has received one or more threats, click **View Details** to see more information. Locate the email threat you want to examine, then click **View Email**.

The attack information page includes:

- Date and time the email was received in your system
- Analysis of the email, describing why it is a threat.
- Recipient, Sender, Date, and Subject information.
- Email tab – displays the text of the email and any attachments.
- Header tab – displays the header information for this email.



Search for Similar Messages opens Barracuda Forensics & Incident Response, a separate Barracuda Networks product, if your organization has it enabled. Barracuda Forensics & Incident Response can locate and take action on messages received by your organization that are identical to or similar to this threat that you already received. Learn more about Barracuda Forensics & Incident Response in Barracuda Campus and on its product page on the Barracuda website.

Click **Back** to return to the list of threats found. Click **Close** to return to the scan report.

Threats

The Threats section shows details about the threats detected in your organization's mailboxes.

The Threats table displays the following information:

- **Received** – The most recent (or first) date that someone in your organization received this email.
- **Recipients** – The number of recipients in your organization who received this email threat.
- **Sample Recipient** – Information for one of the recipients in your organization who received the email threat. This recipient is chosen at random.
- **Email** – The subject line and sender information for this email threat. See also **Action** below.
- **Attack Type** – The category of attack that describes this email threat. Hover over the attack type to learn more about it.
- **Action** – Click **View Email** to see details about the email threat. See **Viewing the Email**

below.

To locate a specific threat or threat category:

- **Searching** – Enter one or more search terms in the **Search threats** box.
- **Filtering** – Click the **Filter** field to select a specific attack type. By default, the filter displays **All Attack Types** and all emails with all attack types are displayed in the table.

Viewing an Email

Click **View Email** to see more information about the email threat. Click **Dismiss** to return to the scan report.

Refer to Viewing an Email in the **Employees** section above for details.

DMARC Protection Status of Your Domains

This section shows the domains in your system and their DMARC protection status. The total number of your domains is shown at the top of the Domains section.

The DMARC protection status is shown for each domain.

Click **View Details** to see more information for each domain. If one or more of your domains is Not Configured, the scan strongly recommends obtaining Barracuda Networks' Domain Fraud Protection to set up DMARC

To narrow the list of domains displayed, use the **Search domains** box. You might use search terms including full or partial domain name or status.

For additional information on DMARC, refer to Domain Fraud Protection Background and Configuring Domain Fraud Protection with Barracuda.

Barracuda Domain Fraud Protection is available in the Barracuda Email Protection Premium and Email Protection Premium Plus plans.

Sharing the Scan Report

You can choose share the scan report with others, either by downloading a PDF or by sharing a private link.

Creating a PDF

1. In the upper right corner of the scan results, click **Share**.
2. Select **Export as PDF**.
   The PDF downloads automatically to your usual download location.

The file name of the PDF includes the date you exported your scan results.

Creating Shared Link

1. In the upper right corner of the scan results, click **Share**.
2. Verify that the slider is in the green **Enabled** position. (See **Disabling Sharing** below.)
3. Click **Copy** to copy the private, unique link to your clipboard.
4. Paste the link into an trusted message to your recipients.
   Recipients click the link and view your scan report.

Link Expiration

The shareable link expires 7 days after you create the scan. The expiration date displays below the share link. After this date, your recipients will no longer be able to view your scan report.

If needed, repeat the steps above to obtain a new link to the same report.

Disabling Sharing

If you decide that you no longer want to share the report with others, you can disable their access to your report.

To disable sharing the scan report:

1. In the upper right corner of the scan results, click **Share**.
2. Move the slider to the **Disabled** position.

The link is automatically disabled and recipients can no longer access your scan report.

Next Steps

Obtaining Impersonation Protection

The Barracuda Email Threat Scanner shows the various threats that have been able to get through to your employees' mailboxes. Try Impersonation Protection for free for 14 days to see how it can continue to detect these threats.

To request a free 14-day trial, click **Start a Free Trial**, located in the upper and lower right corners of your completed scan report.

Removing Attacks Found During the Scan

If the scan found attacks, obtain Impersonation Protection and continue with Removing Attacks Found during a Barracuda Email Threat Scan.

Figures