Barracuda
Your journey, secured.

STEP-BY-STEP GUIDE

Barracuda Email Threat Scanner for Office 365

PARTNER EDITION

Contents

Introduction

Overview

This guide contains the details on how to use Barracuda Email Threat Scanner (ETS) to demonstrate value, differentiate your services, and sell Barracuda email protection solutions for Microsoft Office 365.

What is Email Threat Scanner?

Barracuda Email Threat Scanner™

Email Threat Scanner is a free service that scans Office 365 environments to identify email attacks inside users' inboxes. Customers that run the scan can identify:

- Spear phishing
- Business email compromise
- Conversation hijacking
- Brand and domain impersonation
- Extortion
- Scamming
- URL phishing

Organizations that run a scan will be presented with a report that demonstrates:

- Email attacks inside users' inboxes
- Assessment of high-risk employees
- Domains at risk of spoofing and impersonation

The scan is quick to set up and works with any existing email security with no impact on email performance.

How to use Email Threat Scanner

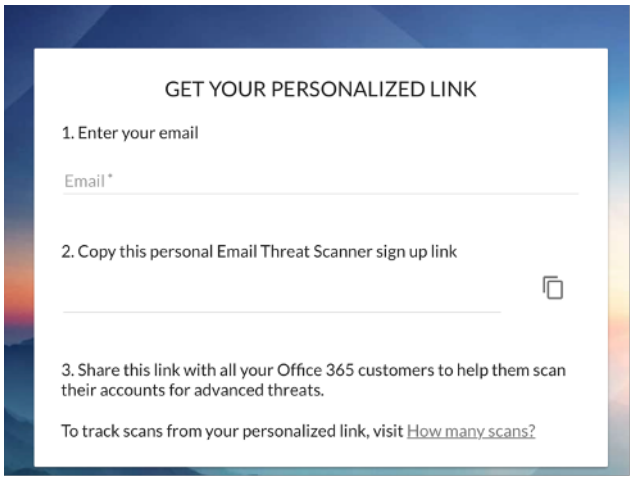
1. Create your personalized ETS link | **2. Position ETS to customers** | **3. Review ETS results with customers**

1. Create your personalized ETS link

Barracuda's partners can create a custom link for their customers' email threat scans. This allows for Barracuda to match customers back to partners and for partners to keep track of all the scans they initiate.

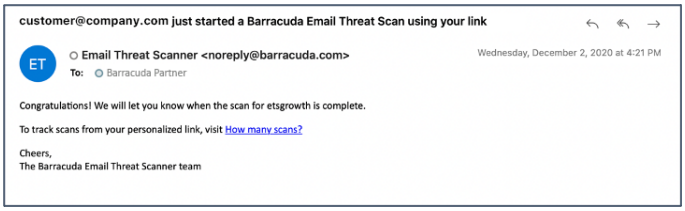
Step 1:

Partners can create their custom link here: https://scan.barracudanetworks.com/mylink



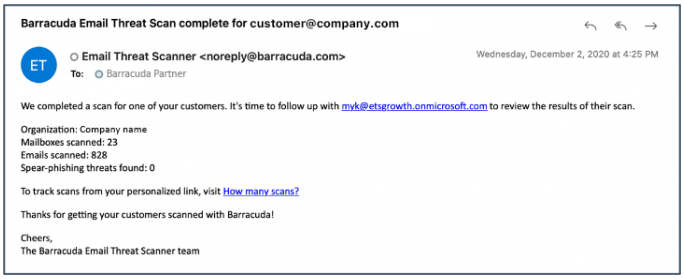
Step 2:

Partners will get an automated email notification when a customer initiates a scan.



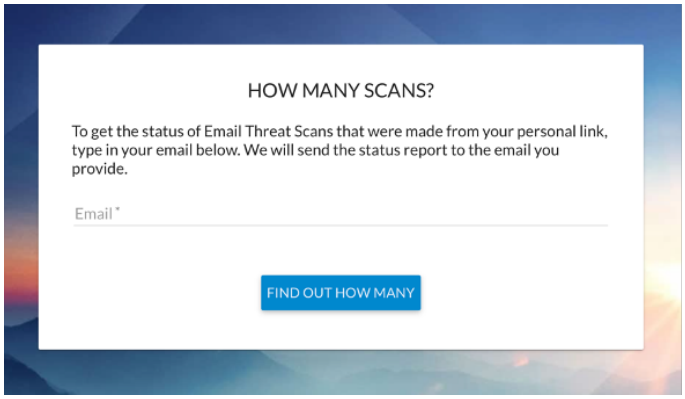
Step 3:

Partners will get an automated email notification when a customer scan is completed.



Step 4:

Partners can also review how many scans were made from their personal link:
https://scan.barracudanetworks.com/howmanyscans



2. Positioning ETS to customers

Who qualifies for Email Threat Scanner?

- All customers and prospects with Office 365
- All customers and prospects considering Barracuda email protection solutions
- Any customer with phishing or account takeover problems

Note: Customers will need to have an admin account for Office 365 to run the scan.

Key messages to customers

- Identify spear phishing and other social engineering attacks already inside your users' inboxes
- Assess and understand your email security vulnerabilities
- See why you need additional layers of defense and how Barracuda can help
- The scan works well with any existing email security with no impact on email performance

Email templates

OPTION 1

Subject: Do you think you are safe? Scan Office 365 for threats today

Did you know that 95% of organizations have Office 365 mailboxes that are harboring malicious emails? Many of these socially engineered attacks are able to slip through existing defenses, landing in users' inboxes and leaving your organization open to potential risk.

Because you're one of our loyal customers, I'd like to invite you to run a free scan offered by Barracuda that identifies spear phishing and other cyber fraud that may already exist in your Office 365 mailboxes.

Simply go to [ADD YOUR PERSONALIZED LINK HERE] to get started. It takes less than a minute to set up, there is no cost to you, and most importantly, there is no impact on your email performance.

Once your scan is complete, I'd like to do a personalized review of the results with you. When would be a good time to jump on a quick call so we can discuss your scan and next steps?

OPTION 2

Subject: Free security assessment for Office 365

Did you know that 95% of organizations have Office 365 mailboxes that are harboring malicious emails? Many of these threats slip through email gateways, and if left undetected, they can cause millions of dollars in losses.

We understand that it is critical for organizations to assess and understand their email security vulnerabilities. And it is important for us to ensure that you and your users are fully protected.

This is why we are offering a free security assessment of your Office 365 environment. Using artificial intelligence and API integration with Office 365, Barracuda Email Threat Scanner quickly finds email attacks currently sitting in your mailboxes.

Simply go to [ADD YOUR PERSONALIZED LINK HERE] to get started. It takes less than a minute to set up, with no impact on your email performance.

Once your scan is completed, we can review the results and discuss how to enhance your security posture with additional user awareness training and advanced threats detection tools.

For more information about the free Barracuda Email Threat Scanner, please don't hesitate to contact us.

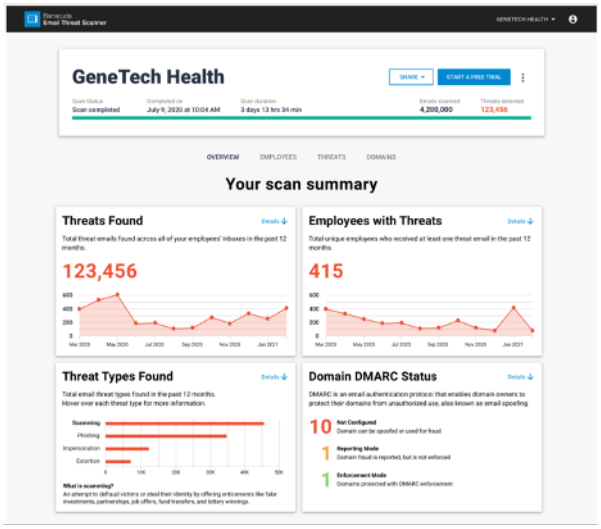
3. Review ETS results with customers

Set up time to review results before you meet the customer. Identify good examples of attacks that managed to get through.

ETS Dashboard

Partners that used a personalized link will receive an email notification when a scan is complete.

Set up time to review results with your customer.



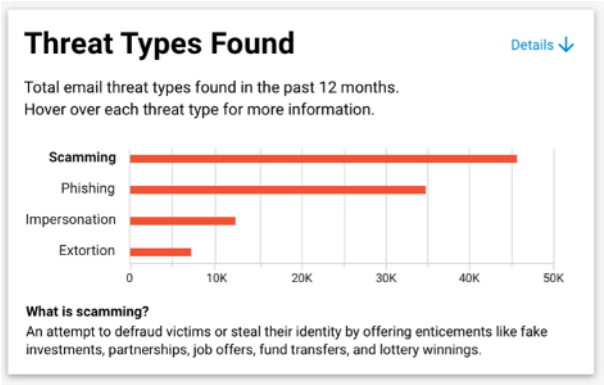
Threats over time

Show the total number of threats that have been missed by the customer's existing email security.

Threat types found

Explain that there are different types of threats targeting organizations today, and each organization is being targeted in a different way.

You can hover over each threat type for more information.

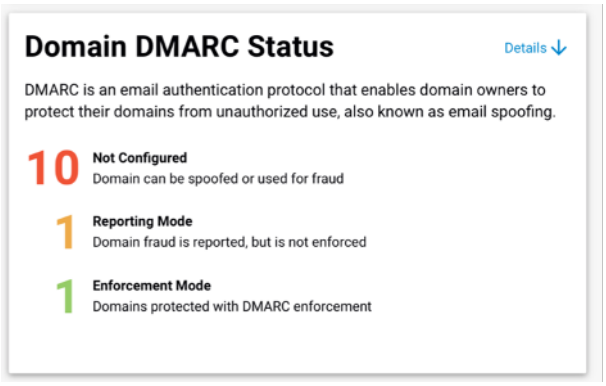


Domain fraud

DMARC enables domain owners to protect their domains from unauthorized use or domain spoofing.

ETS will list all email domains that currently don't have DMARC enforcement set up and are at risk for email domain spoofing.

Recommend your customer to adopt DMARC authentication.

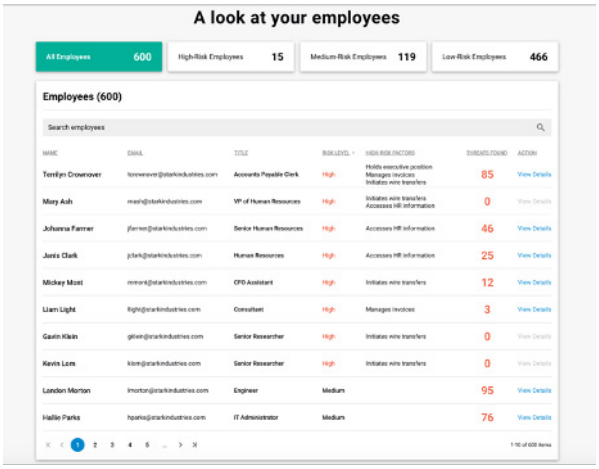


At-risk employees

Review high risk employees with your customer and discuss what they are currently doing to protect them.

What does the customer do to protect medium- or low-risk users? These individuals are often used as stepping stones to more high-value targets.

Click on ‘View details’ to review attacks received by an employee. Show examples where medium- and low-risk employees are being targeted.



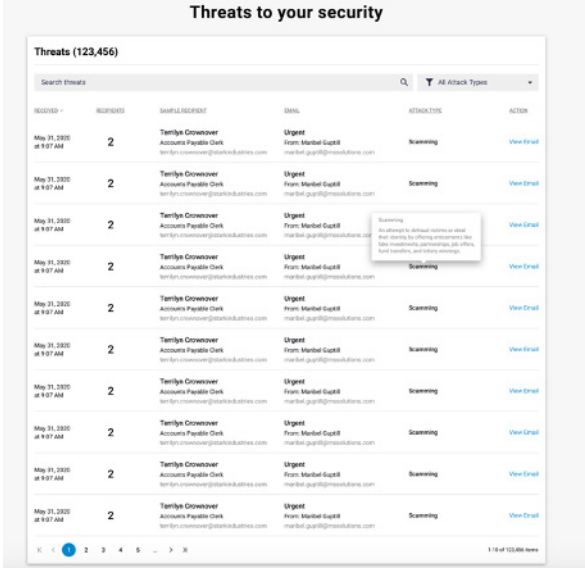
Threat insight

Review specific threats targeting your customer. Click on ‘View email’ to review the actual message that got through.

You can filter results by threat type. For example, select ‘Impersonation’ for targeted employee impersonations or BEC attacks.

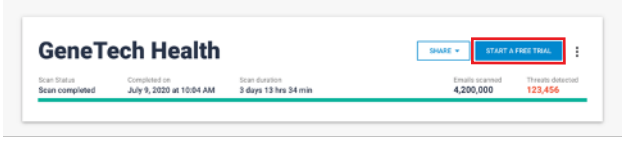
Filter on ‘phishing’ and look for examples of attacks that impersonate well-known brands such Microsoft, FedEx, etc.

Discuss why these types of threats get through, why email gateways are not always effective against these threats, and why Barracuda Sentinel is different.



Sentinel trial

Launch a Sentinel trial directly from the ETS dashboard to continue protecting your customer and their users.



Objection handling

Why are you asking for so many permissions?

Firstly, Barracuda does not get access to your login credentials. We use the standard OAuth protocol to authenticate with Office 365. This provides us with limited permissions to access email, and you can revoke these permissions at any time. ETS doesn't make any changes to your account without you explicitly doing it in the ETS UI. Operations that change Office 365 are clearly marked and require user confirmation.

We have a Data Privacy Solution Brief that covers this in greater detail.

Will running a scan have an effect on my Office 365 performance?

No, there is no impact on your email or Office 365 performance. ETS will run in the background, communicating directly with Office 365 using APIs.

Resources

Share with your customers

- VIDEO: ETS product video
- VIDEO: ETS permissions request explained
- SOLUTION BRIEF: ETS data privacy
- WEB: ETS landing page

Barracuda
Your journey, secured.