Barracuda®

Email Threat Scan Remediation Checklist

Ransomware, CEO spoofing, and other advanced persistent threats are so well designed that legacy security systems don't stand a chance at fighting them off. As companies head to the cloud and take advantage of business productivity suites like Office 365, additional layers of security are a must. Whether you know it or not, there's a good chance that latent cyber threats already exist within your production email environment just waiting to wreak havoc. The Barracuda Email Threat Scanner scans Office 365 mailboxes to identify sophisticated threats in your email environment, and provides immediate remediation guidance and strategies on how to prevent future risks.

This preparation checklist includes some of the key areas to consider after you've run your ETS scan:

☑ Run Barracuda Email Threat Scanner against all Office 365 mailboxes.

Your initial scan will find all known threats that were possibly missed. The scan will identify which mailboxes contain risks, who the mailbox belongs to, the sender of the risk, and details about the risk including what the risk is targeting.

□ My scan identified risks within user mailboxes.

□ Delete the email and attachment from the inbox as soon as possible.
□ Provide the employee with specific instructions on how to safely remove risky email.
□ Investigate whether the threat had been opened.

□ My scan identified threats that were sent internally (from one employee to another).

□ Investigate whether the sender's email account has been compromised.
□ Investigate whether the sender's endpoints have been compromised.
□ Change sender's passwords.

□ Some employees are receiving more threats than others.

□ Check whether employees have public credentials (indexed by search engines).
□ Remove employee name/information from public website.
□ Investigate if employees are visiting suspicious websites.

□ Threats are coming in from external vendors or colleagues.

□ Alert affected employees, and notify vendors and colleagues who are sending threats.
□ Monitor for additional threats from those sources.
□ Blacklist spammer's email address and IP.

□ Executives are being targeted by spear phishers.

□ Remove threat from inbox as soon as possible.
□ Change name on public website to throw off CEO/Executive spoofers.
□ Educate internal folks of correct name, spelling, title, etc. in order to better identify threats.

Once the threats are neutralized, Barracuda advises customers to begin using Advanced Threat Detection to prevent these new threats from entering the system. While Barracuda Essentials for Office 365 provides multi-layered security and advanced threat protection moving forward, it's advised that you work to identify and eliminate latent threats that exist within your production email.