WHAT IS ATTACHMENT SANDBOXING AND WHY DO YOU NEED IT?

How often do you receive an email containing a file attached to it while working? It may be an Excel file (.XLS) of the latest analytics from your marketing department. It could be a Microsoft Word document (.DOC or .DOCX) containing a new proposal you and your team are working on. It even may be a PDF invoice from one of the many tools that your business utilizes. However, what many don't consider is how these attachments can be forged and weaponized to deliver malware to your organization.

With advances in email-based attacks it is imperative that IT admins, solution providers, and business leaders understand the need to protect their organization from not only malicious emails, but also the weaponized attachments that come with them.

What can one do to prevent malicious attachments from not only being opened on an endpoint, but from even reaching the hands of a message recipient? The answer to this problem is to use a high-quality attachment sandboxing solution.

WHAT IS ATTACHMENT SANDBOXING?

The problem with most email security solutions is that they block or approve attachments based on pre-defined configurations from the solution administrator. This could simply mean blocking a certain file type or certain naming conventions that are known to be malicious. Using this methodology of filtering leaves organizations completely exposed to zero-day threats and file names that can easily be faked.

Attachment sandboxing prevents the threat of these malicious attachments that could easily bypass simple email security methodologies. Attachment sandboxing takes each individual message with an attachment and examines the file by itself by extracting the attachment from the message. It will then place the attachment within a virtual protected environment or 'sandbox' and open it to catch any malicious activity or attempts to download additional components that could also perform nefarious activities.

WHY SHOULD I USE IT?

The growing complexity and sophistication of email-based threats coupled with the advent of automation, bots, and artificial intelligence has made it simpler for threat actors to act. This shortening of the attack lifecycle has allowed them to propagate spam attacks faster than ever before with lethal efficiency. This includes weaponized attachments that can be quickly spoofed, mimicked, and delivered.

While most IT admins will engage their end-users in regular, comprehensive cybersecurity training and employ email security solutions, it just isn't enough anymore to stop malicious attachments. No matter how much training you dole out, the best strategy is to ensure a malicious message won't even reach the hands of an end-user. Attachment protection is the only surefire way to protect an organization from malicious attachment-based threats.

Where can one find a powerful, efficient, and scalable attachment sandboxing solution? Look no further than **VIPRE Email Security – Attachment Sandboxing.**

VIPRE EMAIL SECURITY – ATTACHMENT SANDBOXING

Attachment Sandboxing allows businesses to communicate with confidence, ensuring that users are protected against the worst and most elusive threats while never interrupting normal business operations. Safeguard email attachments with an extremely powerful yet easy to use solution that provides the best in attachment protection against malicious and zero-hour threats.

VIPRE's Behavioral Determination Engine is an artificial intelligence engine that uses machine learning to evaluate unknown attachments for potentially malicious behavior, used for true zero-hour threats with no prior detection history.

ATTACHMENT SANDBOXING ALSO FEATURES:

- Machine learning models based on the behavior of millions of observed malware samples.

- Attachment sandboxing provides a protected environment to catch any malicious activity or attempts to download any additional components that also perform malicious activities.

- A dynamic, isolated cloud virtual machine environment that scales easily to handle the load from all clients.

- Detailed behavioral analysis outputs that explain exactly what the attachment tried to do upon execution.

- An early release option to enable users to release their own attachments, depending on the risk profile of the end-users and the organization.

With the advancement of malicious email attachments organizations can't rely on basic email security solutions for protection. They must use an attachment sandboxing solution coupled with advanced, cloud-based email security that also provides exceptional protection against malicious URLs and complex phishing attacks.

FOR MORE INFORMATION visit www.VIPRE.com
call +1-855-885-5566 or send email to sales@VIPRE.com.

VIPRE®