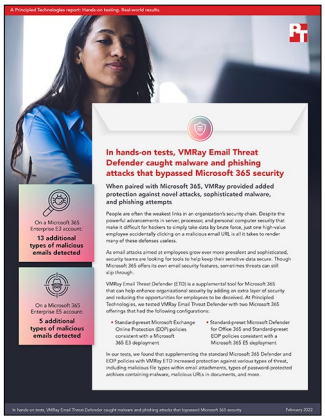

The science behind the report:

In hands-on tests, VMRay Email Threat Defender caught malware and phishing attacks that bypassed Microsoft 365 security

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report In hands-on tests, VMRay Email Threat Defender caught malware and phishing attacks that bypassed Microsoft 365 security.

We concluded our hands-on testing on November 18, 2021. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on September 15, 2021 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Types of attack that VMRay Email Threat Defender identified for the E3 account that Microsoft Exchange Online Protection (EOP) alone did not.

Enhanced protection for E3 Standard EOP policies	
Quantity	Type of attack
4	Malicious files in attachments
2	Password-protected archive attachments containing malware
2	Hidden, malicious macros within files
1	Malicious URL within a document
4	Obscured or shortened URLs within the email body

Table 2: Types of attack that VMRay Email Threat Defender identified for the E5 account that Microsoft EOP and Defender for Office 365 alone did not.

Enhanced protection for E5 Standard EOP and Standard Defender policies	
Quantity	Type of attack
3	Malicious files in attachments
1	Password-protected archive attachments containing malware
1	Hidden, malicious macros within files

A note on our test methodology

Typically, our reports include a detailed testing methodology and hardware/software disclosure that specifies exactly how we tested and which tools we used so that anyone can repeat our tests. In this report, we are intentionally not including all of the information necessary for the reader to reproduce our testing because doing so would instruct the reader on how to bypass standard preset Microsoft 365 security policies and deliver malicious e-mails to inboxes.

Specifically, we are omitting the following information:

- Where we obtained malware samples and the specific malware we sent
- Where we obtained links to the latest phishing sites and which phishing links we sent
- The content of emails and/or attachments we sent
- Alterations we made to attacks or additional steps we took to make them less likely to be detected by Microsoft security measures, such as:
  - Software or commands we used to make alterations to malware samples
  - Techniques we used to obscure phishing URLs
  - Theories on why a specific type of attack worked or failed

In addition, some of our tests used malicious email samples that VMRay obtained from customers. VMRay scrubbed these emails of all identifying customer information before we used them for testing. We do not have any identifying information from these customers, and we do not know where, specifically, these attacks originated. Even so, we are choosing not to disclose the information we do have about these emails, just in case it may unintentionally expose VMRay client information. Specifically, we are omitting the following:

- Email contents
- File attachment types
- File contents

How we tested

To protect our production infrastructure from any accidentally detonated malware, we manipulated and sent malware for the majority of our testing from the following cloud VM:

Table 3: Cloud VM configuration information.

Microsoft Azure B2s VM	
Operating system	Windows 10
Number of vCPUs	2
Memory	4 GiB
Temp storage	8 GiB
HDD Managed Disk	32 Gib

We logged into the Microsoft Administrator Portal and VMRay Email Threat Defender (ETD) Management from our typical work laptops, as there was no risk of accidental malware detonation for that activity.

To test VMRay ETD, we created a trial account for Microsoft 365 with E5 and VMRay ETD. We created the following target email accounts on the E5 domain with VMRay ETD:

- No protection policies (default E3 presets) with VMRay ETD*
- Standard EOP protection policies (Standard E3 presets) with VMRay ETD*
- Standard EOP protection policies and Standard Microsoft Defender protection policies (Standard E5 presets) with VMRay ETD

Note that because we configured VMRay ETD to scan emails only after Microsoft allows them to arrive at the inbox, this setup enabled us to test three types of Microsoft protection with and without VMRay ETD. (If Microsoft protection quarantined the emails, they would never reach the inbox and therefore never reach VMRay ETD in the first place. If VMRay ETD quarantined an email, that meant the email made it past the Microsoft protection associated with that account.)

Additionally, we chose not to use Strict EOP and Strict Defender protection policies, as the Strict settings can lead to many false positives. We believe that Strict EOP and Strict Defender for E5 is not a common configuration for most accounts that malicious actors would target.

After setting up these email accounts, we created a separate account from which to send malicious emails. For each attack, we sent a separate email to each of the three target accounts, performing modifications as necessary to avoid any attachments having the same hash as previously sent emails.

**Though we did not use a true E3 deployment, we tested this account with Microsoft Defender policies disabled, thus enabling us to test policies consistent with both E3 and E5 deployments from a single domain.*

Read the report at https://facts.pt/IEPmtN3 ▶

This project was commissioned by VMRay.

Principled Technologies®

Facts matter.®