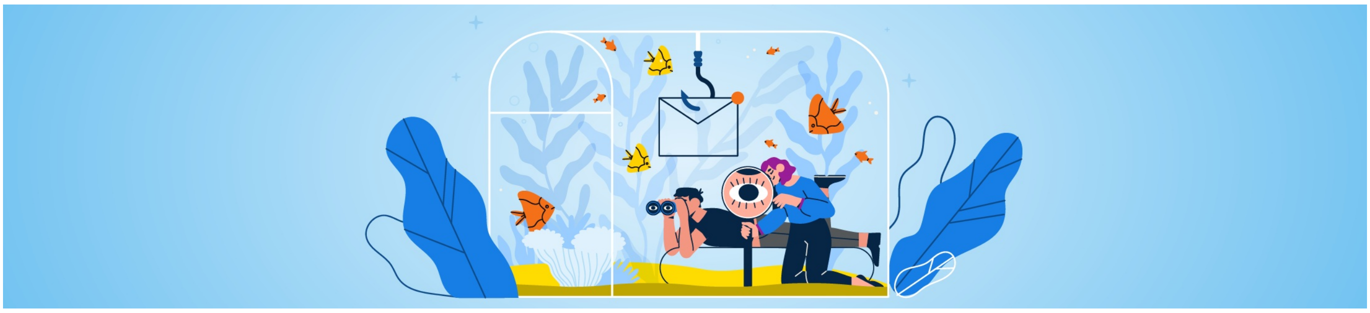

Security operations | 4 min read | Sep 21, 2021 | *by Ray Pugh and Hiranya Mir* | **Tags:** MDR, Tech tools

How we use VMRay to support Expel for Phishing

Tech helps us create space to focus on building human expertise. For example, tools like VMRay allow us to use a hands-on approach to phishing email triage here at Expel. Automated email solutions are an excellent supplement, but there's no replacement for human eyes on a suspicious sample that slips through the cracks.

TL;DR: We harness the human moment to identify the full scope of risk to our customer's environments.

As part of our phishing service, we use automation to triage phishing emails, and our analysts look at every email that our customers' users report. We also help our customers get the full picture of what's happening in their environment by integrating with their endpoint detection and response (EDR) tools.

How does it work?

First, a customer end-user hits the suspicious email reporting button, which generates an alert for analyst review in the Expel Workbench™. Enrichment and automation surface supplementary information in an easily digestible way. From there, we decide whether the email is benign or poses a threat to the customer environment.

When a threat is found, we quickly get to work answering two key questions:

1. Who else received this email?
2. Was anyone compromised?

To answer these questions, we use our integrations with the customer's existing security tech – whether it's email message trace logs stored in their SIEM, network traffic monitored through their firewall or endpoint signal through their EDR.

We use the indicators from a malicious email and the tech stack to determine whether compromises are present in the environment. If we spot a compromise, we notify our customer immediately so we can work in parallel to get the threat remediated.

In this post, we'll walk you through how we use VMRay for our Expel managed phishing service, and share our thoughts on how VMRay can help you protect your org's environment.

Tools we use to investigate potentially malicious emails

We use both internally built tools as well as enrichment pulled through third-party sources to perform analysis.

The most important capability in our investigative toolkit is VMRay.

Whether it's investigating a suspicious link that redirects to a credential harvester or a suspicious Microsoft Word document that may contain malicious macros – VMRay allows us to detonate these samples safely and generate a detailed report of resulting activity. Armed with this information, we provide detailed, thorough recommendations to our customers.

Why we chose VMRay

VMRay integrates well with our approach because, whether it's through manual input in the VMRay console or uploading content through the API, we're able to send numerous samples at one time for analysis simultaneously.

This tech gives our analysts the space to multitask and, as a result, ensure we provide timely results and responses to our customers. Considering we operate in an industry where minutes matter – this can make all the difference when it comes to stopping evil before bad things happen.

VMRay also makes it easy to interact with malicious content. It performs analysis automatically, and offers an interactive mode when needed. And, again, we love that it generates detailed analytical findings reports.

Investigating a phishing email using VMRay

We routinely use VMRay for two types of email threats: suspicious links within the body of an email and suspicious files included with an email as attachments.

For suspicious links, we submit the URL in question to VMRay for both static and dynamic analysis, defaulting to automated mode and including interactive mode in some circumstances.

This provides our analysts with the flexibility to simulate a normal user and extract all of the malicious indicators safely. The detailed report available immediately following analysis serves as the basis for scoping the customer's environment for signs of compromise.

Below is an example of what one of these reports look like.

VMRay web analysis report

VMray's web analysis report tells us that there's a redirect to another site which contains a logon page. This is a key indicator that we're dealing with a credential harvesting page.

Example VMRay visual cue

VMray generates screenshots after its analysis report to provide visual cues. In this case, we observe a suspicious URL enticing the user to interact with another link to access a fake proposal document.

Credential harvesting landing page

After the user interacts with the link they're redirected to a credential harvesting landing page

Fake sign-in page example

In the image above, you see that after several attempts the user is redirected to a Microsoft page which gives the illusion that it's legitimate.

Microsoft Defender for Endpoint

You'll see that we use Microsoft Defender for Endpoint to identify potential clickers by scoping for the malicious domains on the endpoint.

Microsoft Defender for Endpoint

Since we didn't generate any results scoping the malicious domain, we can confidently conclude that no one was compromised.

Some malware is configured to detect and evade sandboxes, so VMRay simulates a realistic user endpoint complete with files, user profiles, simulated cursor movement and other attributes to combat this attacker technique and fool the malware into executing.

If malicious, the file executes thinking it landed on an unsuspecting host and VMRay tracks all of its behavior. At the end, our analysts are able to review the results for key indicators which we can use to scope the customer's environment for signs of compromise.

VMRay dynamic analysis

Above is a screenshot of a VMray dynamic analysis report. What we're seeing indicates that the Excel file contains VBA macros which is a common way attackers embed malicious code. Another interesting observation is that upon execution it creates a process "curl" suggesting the file maybe trying download another payload.

How we use VMRay to further scope our customer's tech for signs of compromise

Analysts use the indicators from the VMRay analysis to scope the respective customer's environment for any signs of potential compromise. The Expel Workbench lets our analysts query automatically through the API, but analysts can also pivot directly into the console for further investigation when necessary.

If there aren't signs of compromise, which is often the case as we aim to stay ahead of the threat, we give our customers succinct recommendations to stop the threat in its tracks.

In cases where signs of active compromise are discovered, we engage the customer immediately for remediation and work collaboratively until the situation is fully resolved.

How you can use VMRay in your own environment

We've continually expanded our managed phishing service, which is why we've made an optimized integration with VMRay and its suite of capabilities a priority.

This helps us maintain efficiency and accuracy while minimizing risk for our analyst team. Analyzing numerous samples at the same time while gathering detailed data about each sample is truly a game changer, especially for a pervasive industry threat like phishing.

Lastly, the features and ease of use help analysts of all experience levels build their investigative muscles. Automating key pieces of the investigative process helps to speed up the already steep learning curve for newer team members.

Phishing attacks are on the rise – especially business email compromise (BEC). Want to find out how we protect our customers from BEC? Check out Expel for Email.

Get an Expel for Email free trial

Subscribe

Next Post ›   All Posts

The top keywords used in phishing email subject lines

Read More

12950 Worldgate Drive, Suite 200
Herndon, VA 20170
USA

Tel: 1-844-397-3524

What you can buy

Get in touch

Contac

Expel M

Ð
R
W
F
A
Q
b
R
e
p
b
f
t
V
A
W
S
e
r
a
b
i
h
g
Ð
y
C
o
r
e
e
r
s

AICPA SOC

ISO 27001 CERTIFIED BY schellman

B P W 2019