

KB4-CON

Get in Position to Disposition

(what the heck is PhishER and how it works)

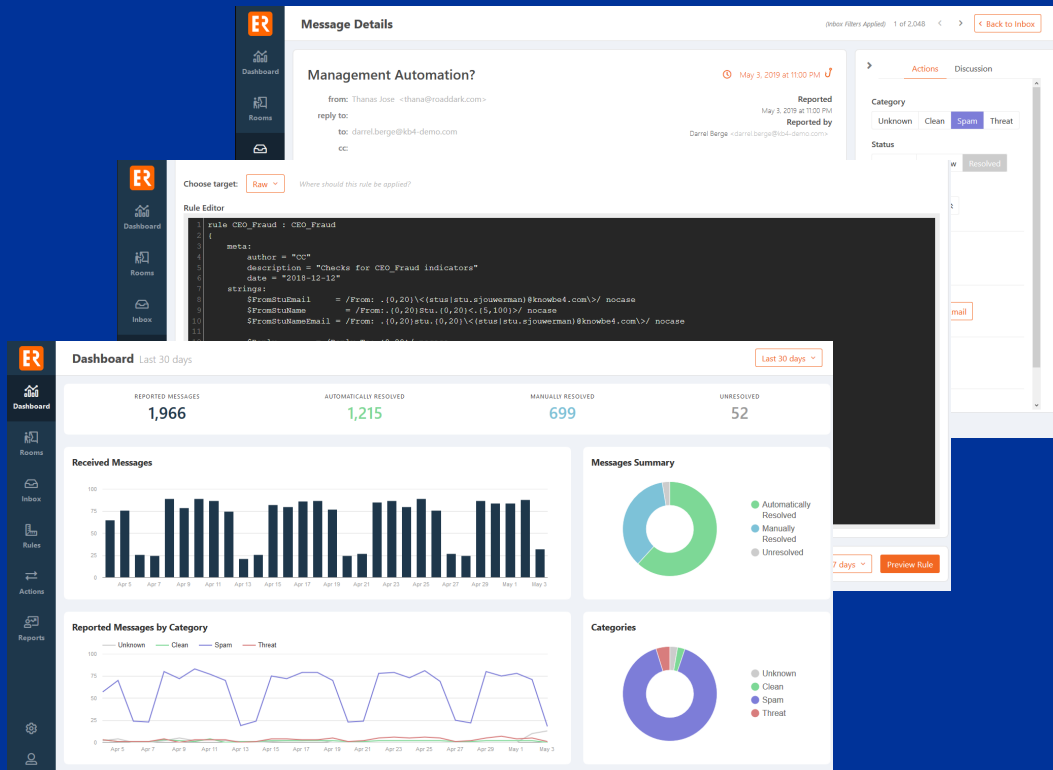
Greg Kras, Chief Product Officer

Chris Cline, Product Manager

KnowBe4

KnowBe4

PhishER



What is PhishER

- New product made available on Dec 17th 2018.
- A hosted platform which helps you identify and respond to user-reported messages.
- Helps you differentiate between the threats and the benign messages - quickly.
- Rules and Actions allow you to categorize messages and automate responses.
- Simply put, it saves time.

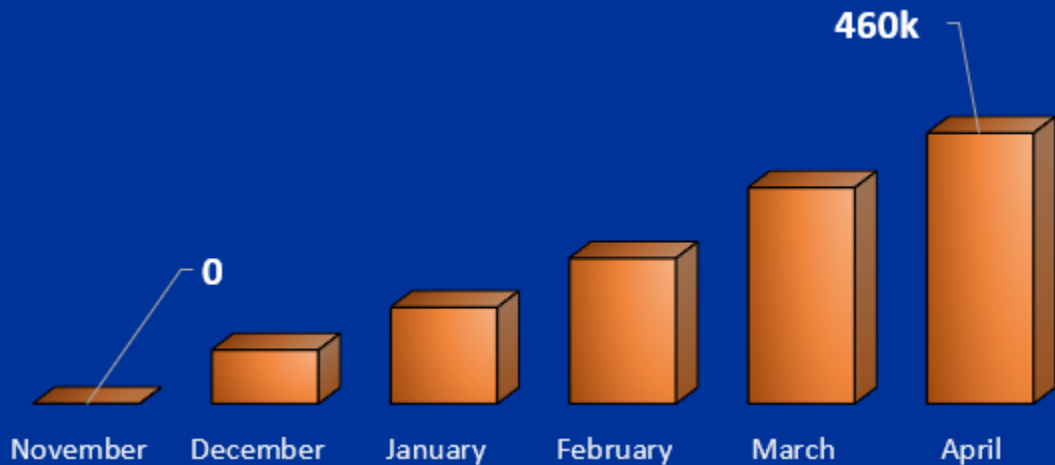
PhishER



How does PhishER work?

1. Users report an email via the Phish Alert Button (PAB) or forward an email to unique address.
2. PhishER receives the message and prepares it for processing and analysis.
3. Rules run over the messages and enrich the information about the messages in the form of tags.
4. Automated actions trigger based upon criteria such as tags.

PhishER



PhishER stats so far

- 460k PhishER reporters
- 500 PhishER accounts
- 1.5 million emails since launch
 - Tens of thousands every day, and growing quickly
- 1 million YARA rules matched
- .5 million actions run

PhisherER



(these are all the master updates since launch)

Improvements since launch

- ~1000 merges to master branch
- Constant enhancements (and fixes)
 - Data retention policies
 - Bulk tagging
 - Quick filtering
 - Quick actions
 - Message history
 - Email Templates
 - YARA rule preview
 - Dozens of minor enhancements

PhishER

Email Template Editor Delete Template

Name
Legit Email Response

Include Original Reporter
 Specify Recipients

From: no-reply@phisher.knowbe4.com From Name: KB4 InfoSec

Reply To: no-reply@phisher.knowbe4.c

Subject: Legit Email Alert {PhishER}

H1 H2 B I U G ” ☰ ☷ 🔗 📎 ✎ Insert placeholder ⌵

Hi [[reporter_name]],
The email you reported at [[reported_time]] from [[sender_email]] was found to be a legitimate email. You should act accordingly.

Email Subject: [[subject]]
Email Attachments: [[attachment_names]]

Include original email at the bottom of body

Better Responses

- Email Templates

As people began to use PhishER it became obvious that admins wanted to send a lot of emails from the platform.

- Placeholders

Email Template Editor allows you to insert placeholders to help personalize and legitimize emails sent from PhishER.

These emails are being used to acknowledge the users reporting messages, alter them to final disposition, and create escalation chains within organizations.

PhisherER

The screenshot displays the PhisherER interface. At the top, there's a 'Choose target:' dropdown set to 'Headers'. Below it is the 'Rule Editor' with a code editor containing the following YARA rule:

```
rule Spammers
{
  strings:
  $ = "tigerdirect320p.tigerdirect.com" nocase
  $ = "info@signpenguin.com" nocase
  $ = "messages-noreply@linkedin.com" nocase
  $ = "dell@campains.dell.com" nocase
  $ = "inbox-connect.com" nocase
  condition:
  any of them
}
```

Below the rule editor is a 'Matched Messages' section with a table of results:

Category	From	Subject	Reported At	Reported By	Reported By (Email)	Status	Tags	Priority	Matched
Spam	TigerDirectB2B	Huge Savings! Laptops Starting At \$179	Apr 5, 2019, 2:16 PM		christians@knowbe4.com	Resolved	SPAM	3	True
Spam	TigerDirectB2B	Jaw Dropping Deals Are A Click Away! Save Up To \$220 On SSD's	Apr 4, 2019, 2:15 PM		christians@knowbe4.com	Resolved	SPAM	3	True
Spam	TigerDirectB2B	Save The Most Important Files For Any-Size Business! SSD's Starting At \$19	Apr 3, 2019, 7:48 PM		christians@knowbe4.com	Resolved	SPAM	3	True

Better Workflows

- Rules Preview
- QuickActions
- Live Updates

YARA is powerful but can be complex. Rules Preview allows you to verify that the Rule you've spent time building actually matches the expected messages before releasing it to the wild.

Some organizations want fine controls and others employ rougher dispositioning. With QuickActions, you can fire the actions you need faster.

Live Updates are easy! Who wants to refresh?

Phisher

Select Retention Type

- Absolute** - Permanently delete all records of the message. This
- Timestamps and Dispositioning only** - Permanently delete
- Limited** - Ent

▼ **Marked as read** by User **Greg Kras** on **Apr 30, 2019 at 5:41 PM**

- Message was marked as read

▼ **Field changed** by Action **Ali Test 4/30/19** triggered by **Sandy Vandebult** on **Apr 30, 2019 at 2:53 PM**

- Category changed from Unknown to Clean
- Status changed from Received to Resolved
- Severity changed from Unknown to Low

▼ **Email sent** by Action **Ali Test 4/30/19** triggered by **Sandy Vandebult** on **Apr 30, 2019 at 2:53 PM**

- Email sent to alik@knowbe4.com

▼ **Rules pipeline completed** on **Apr 30, 2019 at 2:53 PM**

- Status changed from processing to processed

▼ **Rules pipeline completed, Tag changed** by Rule **random typing** on **Apr 30, 2019 at 2:54 PM**

- Status changed from processing to processed
- Tags added: RANDOM RULE 1

Better Auditing

- Data Retention

Sometimes it's more important NOT to have data. Depending on how sensitive your data is, you can select anything from a limited obfuscation up to permanent and complete deletion.

- Message History

Auditing is a big deal for most organizations.

Now everything that happens to a message is timestamped. You can see who did what when.

Phisher

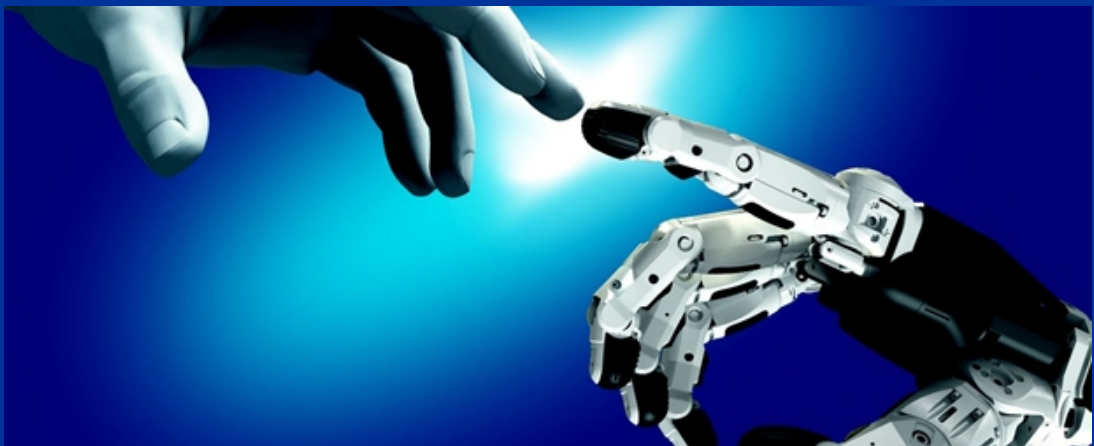
Let's do a demo

Launch it!

The screenshot displays the Phisher web interface. On the left is a dark sidebar with navigation icons for Dashboard, Rooms, Inbox, Rules, Actions, and Reports. The main content area is divided into several sections:

- Message Details:** Shows an email titled "Management Automation?" from "Thomas Jose" to "darrel.berge@kb4-demo.com". It includes a "Reported" status and a "Reported by" field.
- Rule Editor:** A "Choose target" dropdown is set to "Raw". Below it, a code editor shows a rule configuration for "CEO_Fraud" with a meta description and a complex #strings section for filtering.
- Dashboard (Last 30 days):** A summary card shows: 1,966 Reported Messages, 1,215 Automatically Resolved, 699 Manually Resolved, and 52 Unresolved. Below this are four charts:
 - Received Messages:** A bar chart showing daily message volume from April 5 to May 3.
 - Messages Summary:** A donut chart showing the distribution of message resolution status: Automatically Resolved (green), Manually Resolved (blue), and Unresolved (grey).
 - Reported Messages by Category:** A line chart showing the volume of messages categorized as Unknown, Clean, Spam, or Threat over time.
 - Categories:** A donut chart showing the overall distribution of message categories: Unknown, Clean, Spam, and Threat.

PhishER



Right Around the Corner

- VirusTotal hash scans automated
 - The PhishER pipeline is important to keep speedy. A slow pipeline means that potentially dangerous messages stay in your IR inbox longer.
 - Sending just the hash to VT will allow us to push this back to an automated task during the pipeline.
- Apply rules on existing messages
 - Sometimes it takes a few iterations to get your YARA *just right*. With the Rule Replay function you'll be able to keep your data clean for longer term reporting.

PhishER

Q&A

Closing / Q & A

Make sure you come to Lifting the Veil Tomorrow at 2:30-3:15p at SABAL

Visit us in the labs if you want to get into more detail

And with that, we'd like to open up the floor for Q&A

The image features a tropical-themed background with palm tree silhouettes. A solid blue horizontal bar spans the middle of the image, containing the text "Thank You!".

Thank You!

KnowBe4

KnowBe4