Cofense Vision™

QUARANTINE PHISHING ATTACKS IN PROGRESS

Cofense Vision™ enables your SOC team to understand the totality of a phishing attack. Working with Cofense Triage™, our platform reveals "who else" received phishing emails reported by employees. It finds and quarantines ALL emails in an active phishing campaign, including unreported emails, so you can block the threat faster.

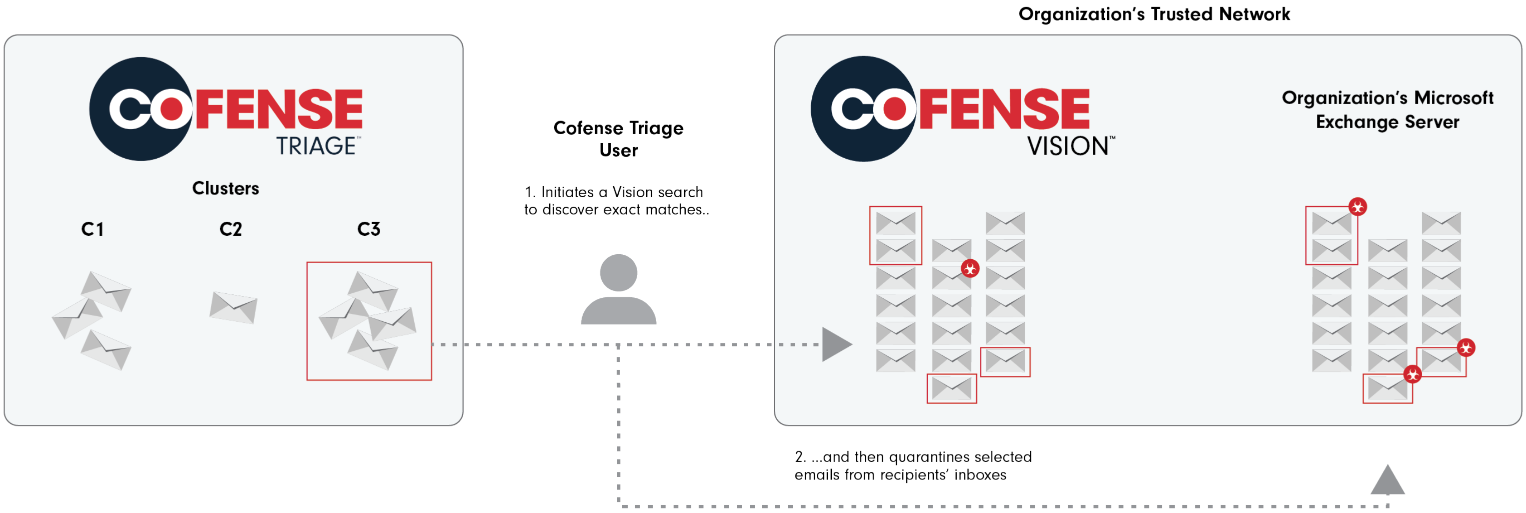
Cofense Triage organizes phishing emails into clusters, by malicious criteria. Cofense Vision precisely identifies all emails in a cluster, across your organization, giving you the full picture of an attack faster. It searches well beyond Sender, Subject, and Date, checking every mailbox to find all recipients. It's the smarter way see and stop the whole phishing attack.

- Quickly identify all recipients of complex phishing attacks
- Single-click quarantine to remove threat from all mailboxes
- Proactively hunt for unreported threats
- Transparent audit and governance of mitigation actions

With Cofense Vision now integrated with Cofense Triage 2.1, operators can quickly find unreported emails that match reported clusters—and mitigate the risk by quarantining them directly from within Cofense Triage. Stop unfolding attacks quickly and seamlessly.

Key Benefits

- ✓ Cofense Vision with Cofense Triage precisely determines all the messages in the campaign across your ENTIRE organization
- ✓ Fast detection of threats
- ✓ One-click quarantine of malicious messages
- ✓ Faster incident response and mitigation
- ✓ Ability to automate remediation tasks and quickly respond to threats


Organization's Trusted Network
COFENSE TRIAGE™
Clusters
C1
C2
C3
Cofense Triage User
1. Initiates a Vision search to discover exact matches..
COFENSE VISION™
Organization's Microsoft Exchange Server
2. ...and then quarantines selected emails from recipients' inboxes

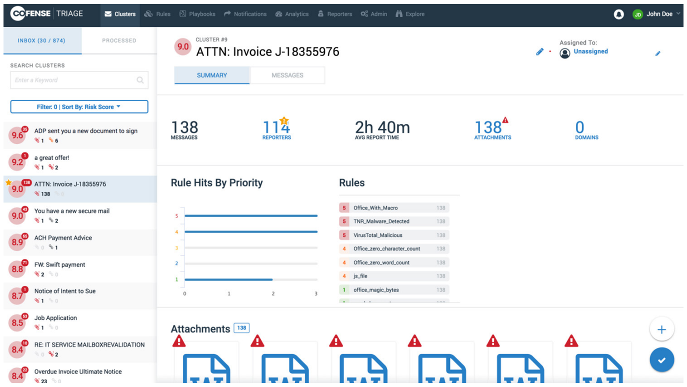
Find the Entire Campaign and Dig Deeper with Cofense Vision

LEARN MORE AT COFENSE.COM/VISION

Find the Entire Phishing Campaign One Cluster at a Time

Cofense Vision stores, indexes, and enriches a moving window of emails in a client environment. Using the Cofense Vision Discover feature, security operations teams are able to find the full breadth of an attack, quickly and efficiently.

Cofense Vision Discover can precisely determine all of the messages that are part of a phishing campaign across your ENTIRE organization. It searches all of the messages that meet a set of criteria, so operators can quickly find the emails, quarantine, and mitigate the threat.



Score		Cluster		
9.6	35	ADP sent you a new document to sign	1	6
9.2	1	a great offer!	1	2
9.0	138	ATTN: Invoice J-18355976	138	0
9.0	43	You have a new secure mail	1	2
8.9	65	ACH Payment Advice	0	1
8.8	71	FW: Swift payment	2	0
8.7	1	Notice of Intent to Sue	1	0
8.5	53	Job Application	1	0
8.4	10	RE: IT SERVICE MAILBOXREVALIDATION	0	2
8.4	22	Overdue Invoice Ultimate Notice	23	0

CLUSTER #9
9.0 ATTN: Invoice J-18355976

138 MESSAGES
114 REPORTERS
2h 40m AVG REPORT TIME
138 ATTACHMENTS
0 DOMAINS

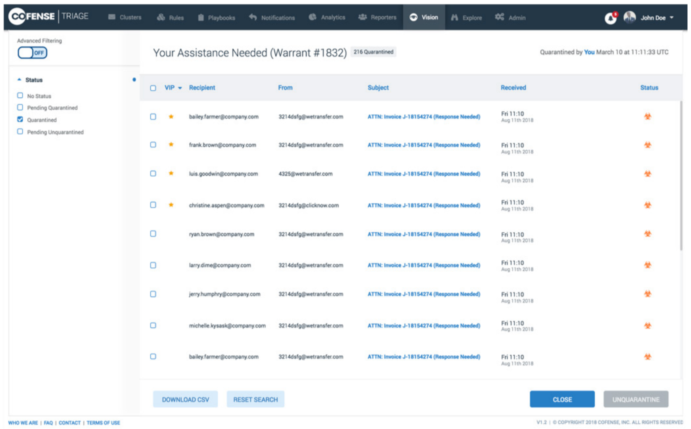
Rules

Priority	Rule	Hits
5	Office_With_Macro	138
5	TNR_Malware_Detected	138
5	VirusTotal_Malicious	138
4	Office_zero_character_count	138
4	Office_zero_word_count	138
4	js_file	138
1	office_magic_bytes	138

Attachments 138

Search Against a Broader List of Criteria

Messages stored in Cofense Vision can be queried based upon Sender, Subject and Date, which Microsoft offers today, but they can be further queried with criteria beyond what is available via Microsoft's API. As threat actors alter their techniques, operators can start hunting for similar items, and quickly find and mitigate attacks with similar patterns. The key to managing a phishing threat is being able to determine where that email is lurking in your email environment.



Status
□ No Status
□ Pending Quarantined
☑ Quarantined
□ Pending Unquarantined

Your Assistance Needed (Warrant #1832) 216 Quarantined

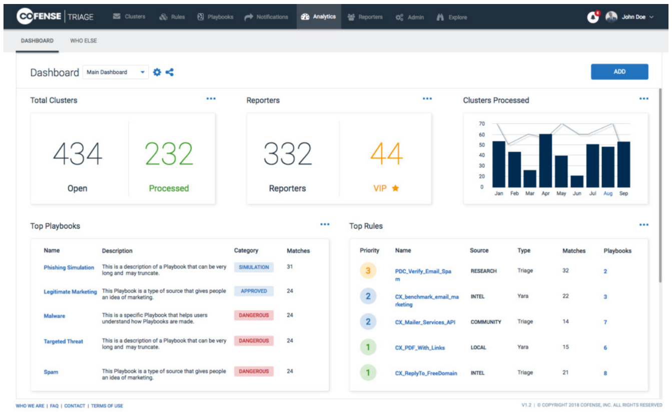
Quarantined by You March 10 at 11:11:33 UTC

□	VIP	Recipient	From	Subject	Received	Status
□	★	bailey.farmer@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□	★	frank.brown@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□	★	luis.goodwin@company.com	4325@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□	★	christine.aspen@company.com	3214dsfg@clicknow.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□		ryan.brown@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□		larry.dime@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□		jerry.humphry@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□		michelle.kysask@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣
□		bailey.farmer@company.com	3214dsfg@wetransfer.com	ATTN: Invoice J-18154274 (Response Needed)	Fri 11:10 Aug 11th 2018	☣

V1.2 | © COPYRIGHT 2018 COFENSE, INC. ALL RIGHTS RESERVED

Quarantine the Threat to Ensure It Doesn't Spread

Once the threat is detected, Cofense Vision Quarantine can rapidly isolate the messages in the Microsoft Exchange® or Office 365® mailboxes. A simple click will quarantine the bad from all user inboxes, without disrupting your organization's day-to-day activities.



Total Clusters
434 Open
232 Processed

Reporters
332 Reporters
44 VIP ★

Top Playbooks

Name	Description	Category	Matches
Phishing Simulation	This is a description of a Playbook that can be very long and may truncate.	SIMULATION	31
Legitimate Marketing	This Playbook is a type of source that gives people an idea of marketing.	APPROVED	24
Malware	This is a specific Playbook that helps users understand how Playbooks are made.	DANGEROUS	24
Targeted Threat	This is a description of a Playbook that can be very long and may truncate.	DANGEROUS	24
Spam	This Playbook is a type of source that gives people an idea of marketing.	DANGEROUS	24

Top Rules

Priority	Name	Source	Type	Matches	Playbooks
3	PDC_Verify_Email_Spam	RESEARCH	Triage	32	2
2	CX_benchmark_email_marketing	INTEL	Yara	22	3
2	CX_Mailer_Services_API	COMMUNITY	Triage	14	7
1	CX_PDF_With_Links	LOCAL	Yara	15	6
1	CX_ReplyTo_FreeDomain	INTEL	Triage	21	8

V1.2 | © COPYRIGHT 2018 COFENSE, INC. ALL RIGHTS RESERVED

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175