The Power of the Collective

COFENSE™ AT-A-GLANCE

What do you get when you combine best-in-class incident-response technologies with employee-sourced attack intelligence? Complete, collaborative and collective defense against email-based cyberattacks. Cofense's solutions anticipate and disrupt the attack kill chain at delivery, triggering enterprise-wide security automation, orchestration and response. Now you can disrupt attacks in progress to stay ahead of breaches. Quickly mitigate threats such as spear phishing, ransomware, malware and business email compromise.

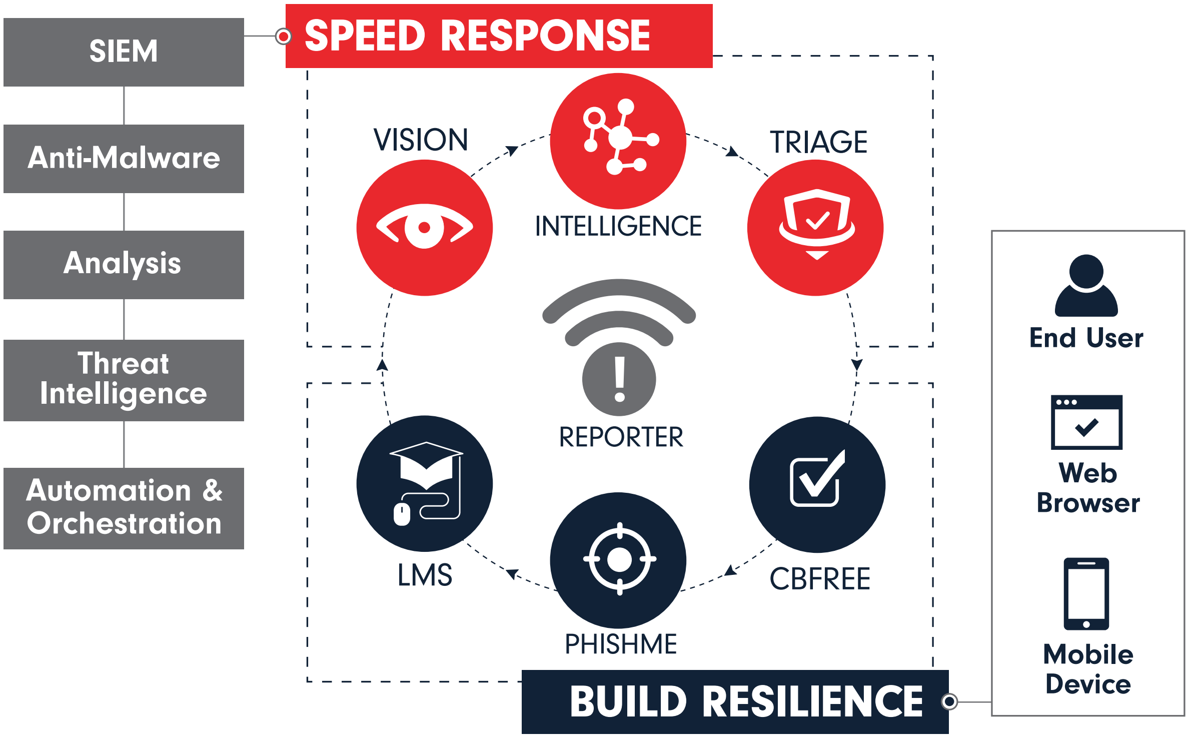
Phishing is the #1 Attack Method

Phishing is the primary method of entry in cyber-attacks world-wide and many high profile breaches emanate from a single, successful phish. Since it typically takes more than 101 days to detect a breach, global organizations need to focus their efforts on prevention and response to neutralize these highly successful attack methods.

Human-Driven Phishing Solutions

Even with record investments, the number of breaches attributed to phishing attacks, continues to grow. It's obvious that "next-gen" technology alone can't solve the problem. That's why Cofense solutions focus on engaging the human–your last line of defense after a phish bypasses other technology–for better prevention and response. Cofense delivers a comprehensive human phishing defense platform. It fortifies employees and enables incident response teams to quickly analyze and respond to targeted phishing attacks.

OUR SOLUTIONS FOR YOUR ORGANIZATION



Turn Employees into Informants

The powerful combination of Cofense PhishMe™ and Cofense Reporter™ conditions employees to resist phishing attempts and empowers them to become part of the defense by reporting potentially malicious phishing attacks in real time.

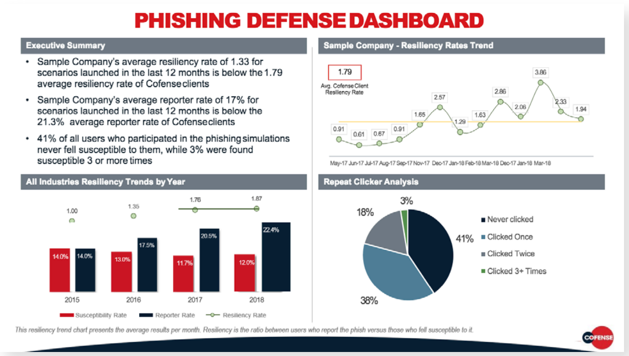
Cofense PhishMe™ - Reducing Employee Susceptibility to Phishing

Cofense PhishMe uses industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts– transforming your biggest liability into your strongest defense.

Provided as a SaaS-based conditioning platform, Cofense PhishMe generates customized phishing attack scenarios recreating a variety of such real-world attack techniques as:

- **Spear phishing attacks**
- **Social engineering attacks**
- **Malware and malicious attachments**
- **Drive-by attacks**
- **Advanced conversational phishing attacks**

Cofense PhishMe™ is easy to administer and provides deep metrics, benchmarking, and reporting options, including custom Board Reports. Users can get up and running quickly and automate their phishing programs by leveraging built-in playbooks - a series of prepared scenarios, landing pages, attachments, and educational pages distributed to run over the course of a year – easing the administration of your phishing program. Cofense PhishMe is the only solution able to track Microsoft Office® attachments - the number one phishing attack type. The solution also provides pre-built and customizable phishing scenarios in an ever-expanding library of content in multiple languages, featuring HTML 5 templates, videos, and gaming modules.



PHISHING DEFENSE DASHBOARD

Executive Summary

- Sample Company's average resiliency rate of 1.33 for scenarios launched in the last 12 months is below the 1.79 average resiliency rate of Cofense clients
- Sample Company's average reporter rate of 17% for scenarios launched in the last 12 months is below the 21.3% average reporter rate of Cofense clients
- 41% of all users who participated in the phishing simulations never fell susceptible to them, while 3% were found susceptible 3 or more times

Sample Company - Resiliency Rates Trend

All Industries Resiliency Trends by Year

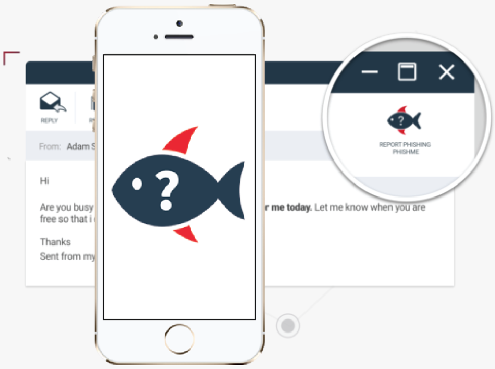
Repeat Clicker Analysis

This resiliency trend chart presents the average results per month. Resiliency is the ratio between users who report the phish versus those who fell susceptible to it.

Cofense PhishMe is easy to administer and provides deep metrics, benchmarking and custom Board Reports.

Cofense Reporter™ - Simple Reporting for all Employees

Cofense Reporter™ is an easy-to-use add-in that enables users to report suspicious emails with a simple click from their email client. Cofense Reporter can be deployed on desktop mail clients and on mail clients on Apple and Android mobile devices. The user-generated reports are then forwarded to your security teams, containing the full header and attachments of reported emails for further security analysis and incident response. Cofense Reporter is included as part of any standard Cofense PhishMe license to help customers gather internal attack intelligence. It works with most popular email solutions including Outlook, Office 365, Gmail, and IBM Notes.



Cofense Mobile Reporter is the only solution removing that attack blind spot.

Cofense CBFree™ - CBTs for FREE

Cofense recognizes security awareness Computer Based Training (CBT) helps check-a-box to satisfy compliance needs. That's why we developed a set of SCORM-compliant materials free for any organization that needs it. Our library of security awareness CBTs includes multiple awareness, compliance, and game modules that have been developed using the latest eLearning techniques and trends that promote substantial engagement by the pupil. Each module takes about 5 minutes to complete and comes with an optional 5 minutes of interactive Q&A. CBFree works with or without an LMS so is easily added into any online learning program.

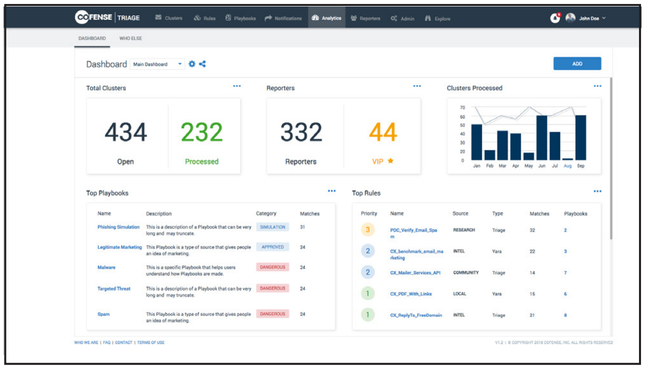
Speed Incident Response

Cofense VisionTM and Cofense IntelligenceTM strengthen your organization's ability to quickly identify and respond to phishing attacks in progress. With the entire employee-base now reporting malicious emails, the SOC and IR teams must collect, prioritize, analyze and respond efficiently to keep up with the volume of reported threats.

Cofense Triage™ and Cofense Vision™ - Phishing Security Orchestration, Automation and Response Platform

Cofense Triage is the first phishing-specific incident response platform that stops attacks in progress. Cofense Triage operationalizes the collection and prioritization of employee-reported threats whether from other sources or directly from Cofense Reporter. It drives faster, more effective phishing analysis and mitigation - automating front-line analysis and orchestrating response across your security teams.

Cofense Vision stores, indexes, and enriches a moving window of email messages in a client environment, enabling security teams to take action against unreported malicious emails. Using Cofense Vision Discover, security operations teams are able to extend Cofense clustering logic to find the full breadth of an attack, quickly and efficiently. Once discovered, Cofense Vision Quarantine allows operators to rapidly remove threats from users' mailboxes.



Total Clusters

434 Open | 232 Processed

Reporters

332 Reporters | 44 VIP ★

Clusters Processed

Top Playbooks

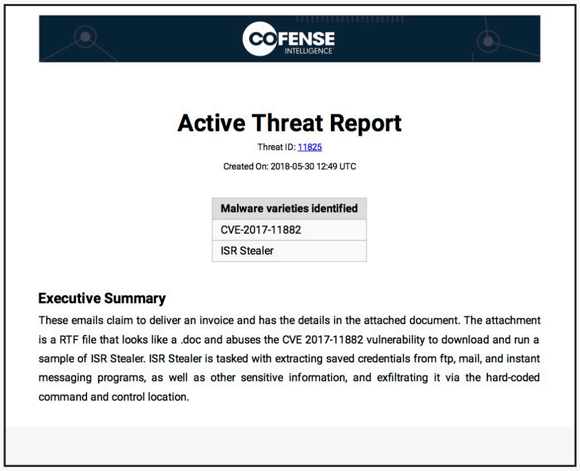
Name	Description	Category	Matches
Phishing Simulation	This is a description of a Playbook that can be very long and may truncate.	SIMULATION	31
Legitimate Marketing	This Playbook is a type of source that gives people an idea of marketing.	APPROVED	24
Malware	This is a specific Playbook that helps users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

Cofense Triage provides real-time visibility and fast verification of attacks in progress.

Together, Cofense Triage and Cofense Vision delivers a Phishing Security Orchestration, Automation and Response (SOAR) platform that powers faster, more efficient phishing mitigation. Cofense Triage lets incident responders find "bad" faster, while Cofense Vision finds malicious emails across the organization and stops them before they become a threat.



Active Threat Report

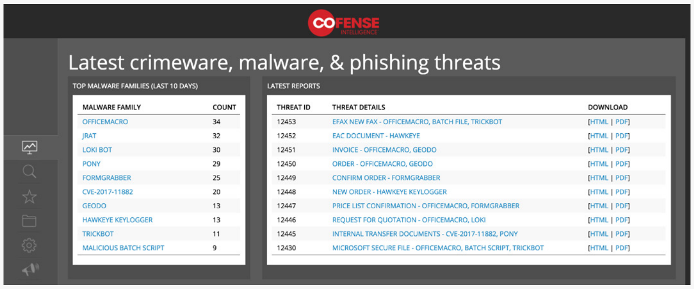
Threat ID: 11825

Created On: 2018-05-30 12:49 UTC

Malware varieties identified
CVE-2017-11882
ISR Stealer

Executive Summary

These emails claim to deliver an invoice and has the details in the attached document. The attachment is a RTF file that looks like a .doc and abuses the CVE 2017-11882 vulnerability to download and run a sample of ISR Stealer. ISR Stealer is tasked with extracting saved credentials from ftp, mail, and instant messaging programs, as well as other sensitive information, and exfiltrating it via the hard-coded command and control location.



Latest crimeware, malware, & phishing threats

TOP MALWARE FAMILIES (LAST 10 DAYS)

MALWARE FAMILY	COUNT
OFFICEMACRO	34
JRAT	32
LOKI BOT	30
PONY	29
FORMGRABBER	25
CVE-2017-11882	20
GEODO	13
HAWKEYE KEYLOGGER	13
TRICKBOT	11
MALICIOUS BATCH SCRIPT	9

LATEST REPORTS

THREAT ID	THREAT DETAILS	DOWNLOAD
12453	EFAX NEW FAX - OFFICEMACRO, BATCH FILE, TRICKBOT	[HTML | PDF]
12452	EAC DOCUMENT - HAWKEYE	[HTML | PDF]
12451	INVOICE - OFFICEMACRO, GEODO	[HTML | PDF]
12450	ORDER - OFFICEMACRO, GEODO	[HTML | PDF]
12449	CONFIRM ORDER - FORMGRABBER	[HTML | PDF]
12448	NEW ORDER - HAWKEYE KEYLOGGER	[HTML | PDF]
12447	PRICE LIST CONFIRMATION - OFFICEMACRO, FORMGRABBER	[HTML | PDF]
12446	REQUEST FOR QUOTATION - OFFICEMACRO, LOKI	[HTML | PDF]
12445	INTERNAL TRANSFER DOCUMENTS - CVE-2017-11882, PONY	[HTML | PDF]
12430	MICROSOFT SECURE FILE - OFFICEMACRO, BATCH SCRIPT, TRICKBOT	[HTML | PDF]

Cofense Intelligence is available via a restful API to access machine -readable threat intelligence (MRTI) in STIX, JSON, and CEF formats.

Cofense Intelligence™ - Phishing Threat Intelligence

Cofense Intelligence is a phishing-specific threat intelligence solution that delivers the right information at the right time to help defend your network. Cofense Intelligence uses proprietary techniques to analyze millions of messages daily from a wide variety of sources. It automatically dissect messages to identify new and emerging phishing and malware threats. A team of analysts dive into these messages to eliminate false positives while delivering the right intelligence when it is needed. Cofense Intelligence is distributed in multiple formats including Machine-Readable Threat Intelligence (MRTI) for quick and easy integration into other security solutions.

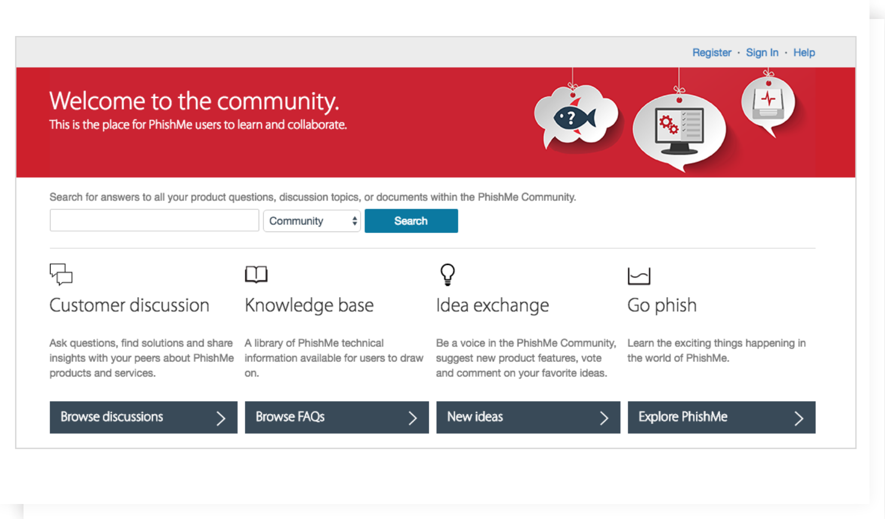
- **TIMELY:** Real-time analysis, Real-time publishing. New reports are published as they are confirmed throughout the day.
- **ACCURATE:** Our analysts provide context by connecting the indicators to malware families. We tell you that something is bad how bad, why it is bad and which malware is involved.
- **RELEVANT:** Our analysts dissect malware and determine which indicators are important to help determine if malware is running inside your perimeter and preemptively block it.
- **CONSUMABLE:** Delivered in the format you need. Intelligence Feed Formats include: Machine-Readable Threat Intelligence - STIX, JSON, CEF; Human-Readable Threat Intelligence - PDF, HTML; SaaS Investigation platform - Web, API.

Ensuring Success with Cofense Professional Services

If resources are limited, dedicated professional services are available for partially or fully-managed deployments of Cofense solutions, including a dedicated Cofense security expert assigned exclusively to each account to assist in the creation, execution and analysis of your phishing defense programs. Programs are customized for an organization's requirements and diverse cultural environments.

Cofense Support and Community

Each Cofense license includes access to our world-class customer support and customer community platform.



Welcome to the community.

This is the place for PhishMe users to learn and collaborate.

Search for answers to all your product questions, discussion topics, or documents within the PhishMe Community.

Customer discussion

Ask questions, find solutions and share insights with your peers about PhishMe products and services.

Knowledge base

A library of PhishMe technical information available for users to draw on.

Idea exchange

Be a voice in the PhishMe Community, suggest new product features, vote and comment on your favorite ideas.

Go phish

Learn the exciting things happening in the world of PhishMe.

Cofense Support

Our support provides expert advice for implementing Cofense's solutions, including:

- Reviewing scenarios against industry best practices
- Effectively leveraging Cofense solutions
- Providing assistance for new features and scenarios
- Tailoring comprehensive phishing defense programs for each organization

Cofense Community

The Cofense Community provides an easily accessible online knowledge-base where users can share and can come together to discover, develop and connect to expert resources and peer advisors to improve and grow their Cofense programs. The Cofense Community is a place for users of Cofense solutions and products to access all the information and tools needed to improve and expand their anti-phishing programs.

CofenseTM, 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