Cofense Integration Brief

COFENSE INTELLIGENCE™ RSA® NETWITNESS SUITE

Operationalize Phishing Intelligence for Threat Defense & Response

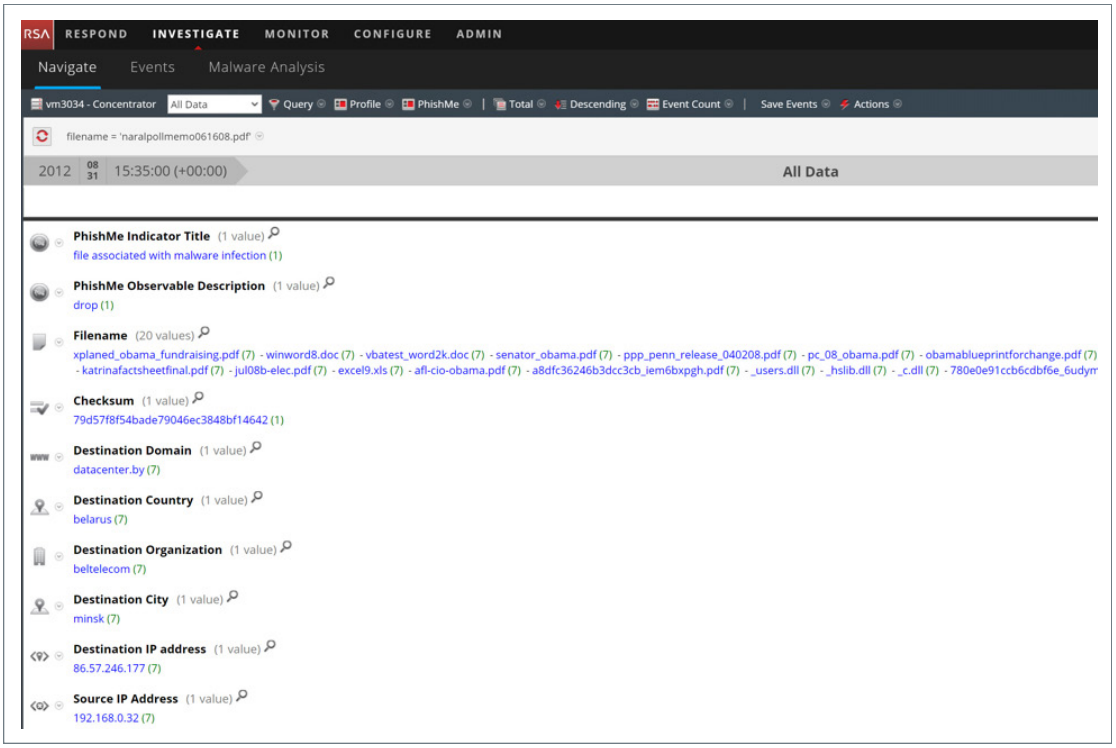
Cofense® and RSA® NetWitness® Suite interoperate for visibility into one of the biggest cybersecurity risks — phishing. With many of today's data breaches attributed to phishing, security teams require insight into adversary criminal infrastructure that can be operationalized to alert and respond to phishing threats.

Cofense Intelligence™ is 100% human-verified phishing-specific threat intelligence delivered as machine-readable threat intelligence (MRTI). Customers receive a fully-vetted source of phishing intelligence verified by Cofense researchers. Cofense provides security teams with context around the criminal infrastructure to extend beyond a list of Indicators of Compromise (IOCs), and enable teams to see their adversary's full operation as opposed to one-offs that change rapidly. By leveraging the STIX standard, Cofense Threat Intelligence data can be imported into RSA NetWitness Suite to diagnose infected corporate systems, and proactively detect or defend against attacks before they happen.

Phishing Intelligence

- ✓ Cofense Intelligence via STIX XML format connects and structures phishing indicators for consumption by RSA NetWitness Suite
- ✓ Relevant and contextual MRTI with no false positives
- ✓ High fidelity intelligence about hpishing, malware, and botnet infrastructure
- ✓ Human-readable reports to understand attacker TTPs

The RSA NetWitness Evolved SIEM is designed to bring together log, network and endpoint data with business insights and threat intelligence into one, non-siloed analytics engine to find attacks that could otherwise go undetected. The Suite also features User Interfaces (UI) built to help analysts respond to attacks that have the greatest potential to do the most harm to an organization. The end-to-end visibility and use of data in one SIEM to detect and respond separates RSA NetWitness Suite from other solutions in the market.



filename = 'naralpollmemo061608.pdf'

2012 08 31 15:35:00 (+00:00) All Data

PhishMe Indicator Title (1 value)
file associated with malware infection (1)

PhishMe Observable Description (1 value)
drop (1)

Filename (20 values)
xplaned_obama_fundraising.pdf (7) - winword8.doc (7) - vbatest_word2k.doc (7) - senator_obama.pdf (7) - ppp_penn_release_040208.pdf (7) - pc_08_obama.pdf (7) - obamablueprintforchange.pdf (7) - katrinafactsheetfinal.pdf (7) - jul08b-elec.pdf (7) - excel9.xls (7) - afl-cio-obama.pdf (7) - a8dfc36246b3dcc3cb_iem6bxpgh.pdf (7) - _users.dll (7) - _hslib.dll (7) - _c.dll (7) - 780e0e91ccb6cdbf6e_6udym

Checksum (1 value)
79d57f8f54bade79046ec3848bf14642 (1)

Destination Domain (1 value)
datacenter.by (7)

Destination Country (1 value)
belarus (7)

Destination Organization (1 value)
beltelecom (7)

Destination City (1 value)
minsk (7)

Destination IP address (1 value)
86.57.246.177 (7)

Source IP Address (1 value)
192.168.0.32 (7)

IR Team Challenges

Attackers Evading Technical Controls

As technology evolves to defend against threats, the attackers' creativity enables them to find ways into the employees' inbox hoping they will open the attachment or click the link. Employees conditioned to recognize and report suspicious email contribute valuable human intelligence that may otherwise go unnoticed for an extended period of time.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Correlation and prioritization of security events and the confidence to deny the communication is absolutely critical when seconds matter in blocking the threat.

Alert Fatigue

Too many threat intelligence feeds are full of false positives that distract security analysts. Excessive alerts only exasperate overwhelmed analysts with a finite amount of time.

The Solution

Cofense Intelligence indicators provide security teams with visibility into phishing criminal infrastructure. Analysts operationalize their response workflow against phishing URLs, IPs, domains, files, command and control (C2), payload, and exfiltration sites, when they configure NetWitness to alert on activity matching the indicators.Additionally, human-readable contextual executive and technical reports that illustrate the phishing infrastructure produced by Intelligence are available. Security teams are much more confident in the action they take based on thorough indicator report analysis when NetWitness correlates activity across their configuration rules. Cofense Intelligence reports not only identify the security risk, butexplicitly state why indicators are malicious so that analysts don't have to do additional research. Armed with human-verified phishing intelligence indicators and verbose reports that can be associated with events captured by NetWitness.

How It Works

Cofense Intelligence ingested into RSA NetWitness software connect and optimize the workflow. The phishing indicators in machine-readable threat intelligence (MRTI) correspond to risk-based threat ratings enabling security teams to quickly identify the latest phishing attacks bypassing their perimeter.

The human-verified intelligence from Cofense Intelligence affords analysts opportunity to prioritize and decisively respond to events with high fidelity data. Analysts can then navigate to Cofense's portal with access to human-readable Active Threat Reports with detailed insight into the attacker TTPs. These reports start with an executive overview and then describe the attack vector used to gain access to your employee's computer. The Cofense Intelligence service includes enriched IOC event data such as:

- **URLs**
- **Domains**
- **IPs**
- **Infrastructure Type: C2, Payload, Exfiltration**
- **Filenames and hashes**

With the powerful combination of internally-generated attack intelligence, 100% human-verified threat intelligence, and incident response event data made visible and actionable in NetWitness, security teams can respond quickly and with confidence to mitigate identified threats.

About RSA

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users worldwide and works with more than 90 percent of the Fortune 500.

TECHNOLOGY
RSA READY
PARTNER

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.

COFENSE

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