Cofense Integration Brief

COFENSE AND SPLUNK ENTERPRISE SECURITY

Operationalize Phishing Intelligence for Threat Defense & Response

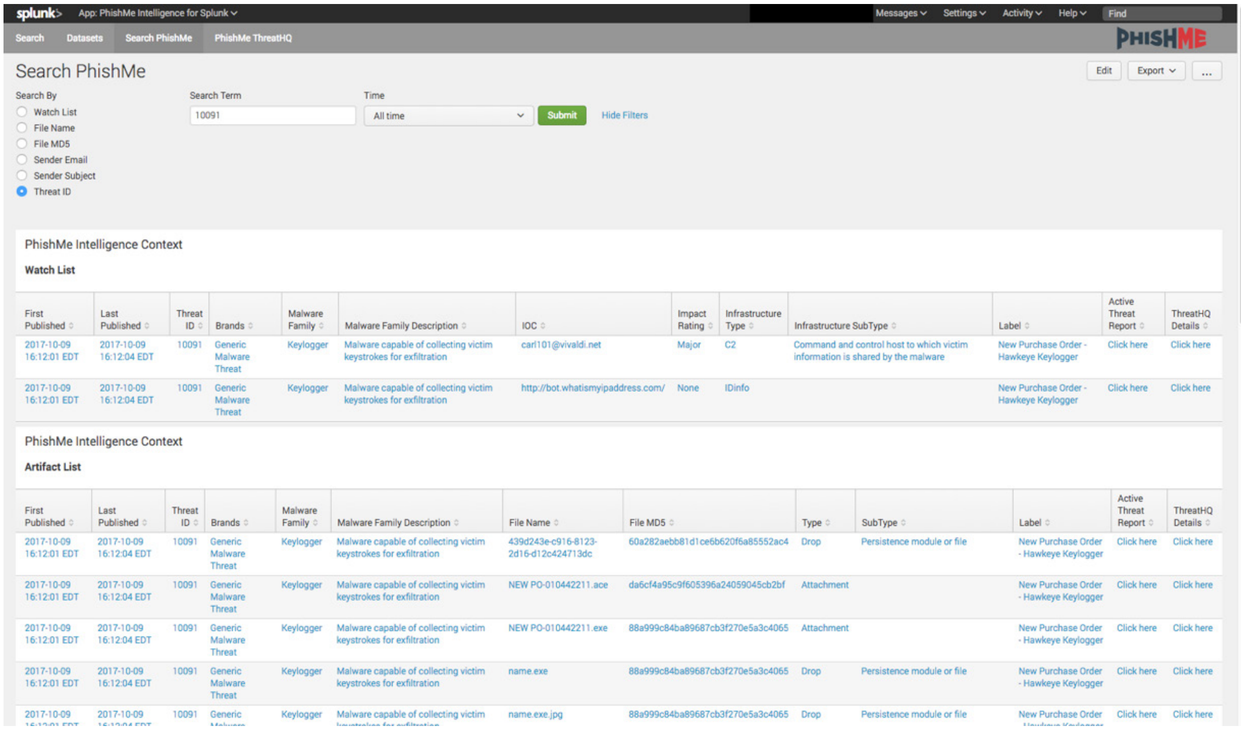
Cofense® and Splunk® integrate for visibility into one of the biggest cyber security risks — phishing. With many of today's data breaches attributed to phishing, security teams require insight into adversary criminal infrastructure that can be operationalized to alert and respond to phishing threats.

Cofense Intelligence™ is 100% human-verified machine-readable threat intelligence (MRTI). Customers receive a fully-vetted source of intelligence verified by Cofense researchers. Cofense also 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. A Splunk Add-On leverages Cofense-provided RESTful APIs to ingest sources of phishing intelligence into the platform and analysts can then operationalize their workflow based on phishing indicators and their impact.

Phishing Intelligence

- ✓ Cofense Intelligence Add-on automatically connects and structures Cofense Intelligence for consumption by Splunk users
- ✓ Relevant and contextual MRTI with no false positives
- ✓ High fidelity intelligence about phishing, malware, and botnet infrastructure
- ✓ Human-readable reports to understand attacker TTPs

Splunk Enterprise Security (ES) is a premium security solution that enables security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguarding business. ES enables security teams to use all data to gain organization-wide visibility and security intelligence. Regardless of deployment model, ES can be used for continuous monitoring, incident response, running a security operations center or for providing executives a window into business risk.



Search PhishMe

Search By
○ Watch List
○ File Name
○ File MD5
○ Sender Email
○ Sender Subject
● Threat ID

Search Term: 10091

Time: All time

PhishMe Intelligence Context

Watch List

First Published	Last Published	Threat ID	Brands	Malware Family	Malware Family Description	IOC	Impact Rating	Infrastructure Type	Infrastructure SubType	Label	Active Threat Report	ThreatHQ Details
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	carl101@vivaldi.net	Major	C2	Command and control host to which victim information is shared by the malware	New Purchase Order - Hawkeye Keylogger	Click here	Click here
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	http://bot.whatismyipaddress.com/	None	IDinfo		New Purchase Order - Hawkeye Keylogger	Click here	Click here

PhishMe Intelligence Context

Artifact List

First Published	Last Published	Threat ID	Brands	Malware Family	Malware Family Description	File Name	File MD5	Type	SubType	Label	Active Threat Report	ThreatHQ Details
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	439d243e-c916-8123-2d16-d12c424713dc	60a282aebb81d1ce6b620f6a85552ac4	Drop	Persistence module or file	New Purchase Order - Hawkeye Keylogger	Click here	Click here
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	NEW PO-010442211.ace	da6cf4a95c9f605396a24059045cb2bf	Attachment		New Purchase Order - Hawkeye Keylogger	Click here	Click here
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	NEW PO-010442211.exe	88a999c84ba89687cb3f270e5a3c4065	Attachment		New Purchase Order - Hawkeye Keylogger	Click here	Click here
2017-10-09 16:12:01 EDT	2017-10-09 16:12:04 EDT	10091	Generic Malware Threat	Keylogger	Malware capable of collecting victim keystrokes for exfiltration	name.exe	88a999c84ba89687cb3f270e5a3c4065	Drop	Persistence module or file	New Purchase Order - Hawkeye Keylogger	Click here	Click here
2017-10-09	2017-10-09	10091	Generic	Keylogger	Malware capable of collecting victim	name.exe.jpg	88a999c84ba89687cb3f270e5a3c4065	Drop	Persistence module or file	New Purchase Order	Click here	Click here

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 IOCs provide security teams with visibility into phishing criminal infrastructure. Splunkers gain insight into phishing URLs, IPs, domains, files, command and control (C2), payload, and exfiltration sites. Additionally, human-readable contextual executive and technical reports are available from the Add-On that illustrate the phishing infrastructure produced by Cofense. Security teams are much more confident in the action they take based on thorough indicator report analysis. Cofense Intelligence reports not only identify what is a security risk, but explicitly state why indicators are malicious so that analysts don't have to do additional research. Armed with human-verified intelligence indicators and verbose reports, security teams can defend the enterprise against the number one threat vector facing companies today – phishing.

How it Works

Cofense Intelligence Add-Ons for Splunk software connect and optimize the workflow. The Cofense Intelligence Add-on automatically converts Cofense machine-readable threat intelligence (MRTI) into risk-based threat lists enabling security teams to quickly identify the latest phishing attacks bypassing their perimeter.

The Splunk Add-On enables analysts to prioritize and decisively respond to high fidelity events. Using the Add-Ons, incident responders can see the context of every alert and access human-readable Active Threat Reports when detailed insight into the attacker TTPs are required. 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 Add-On for Splunk includes enriched IOC event data such as:

- **IOC Type: URL, File Hash, IP Address, Domain**
- **Published Date**
- **Malware Description**
- **Threat ID**
- **Infrastructure Type: C2, Payload, Exfiltration**
- **Malware Family**
- **Impact Rating**
- **Link to Active Threat Report**

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

About Splunk

Splunk Inc. provides the leading platform for Operational Intelligence. Splunk® software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. More than 12,000 organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs.

splunk>

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