Cofense Integration Brief

COFENSE AND CARBON BLACK

Delivering Powerful Phishing Threat Defense & Response

Cofense delivers comprehensive human phishing defense solutions focused on fortifying employees – your last line of defense after a phishing attack evades your other technology. Cofense enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks. Armed with Cofense Intelligence™, organizations leverage 100% human-verified phishing threat intelligence capable of supporting endpoint security platforms.

Cb Response is purpose-built for enterprise SOC and incident response (IR) teams. Security IR and threat hunting teams leverage the speed, scalability, and historical data retention that Cb Response offers. Cb Response delivers continuous centralized recording for complete threat visibility across the enterprise. Additionally, Cb Response visually completes the attack kill chain to find the root cause and identify lateral movement to accelerate investigations.

Cb Response reduces time spent on IR through real-time response capabilities with complete remediation of compromised hosts. The forensic data obtained can then be used to mitigate the threat and protect against future attacks. When malicious content bypasses network defenses, Cb Response can actively hunt for the existence of hostile files on the endpoint in tandem with partner APIs such as Cofense Intelligence.

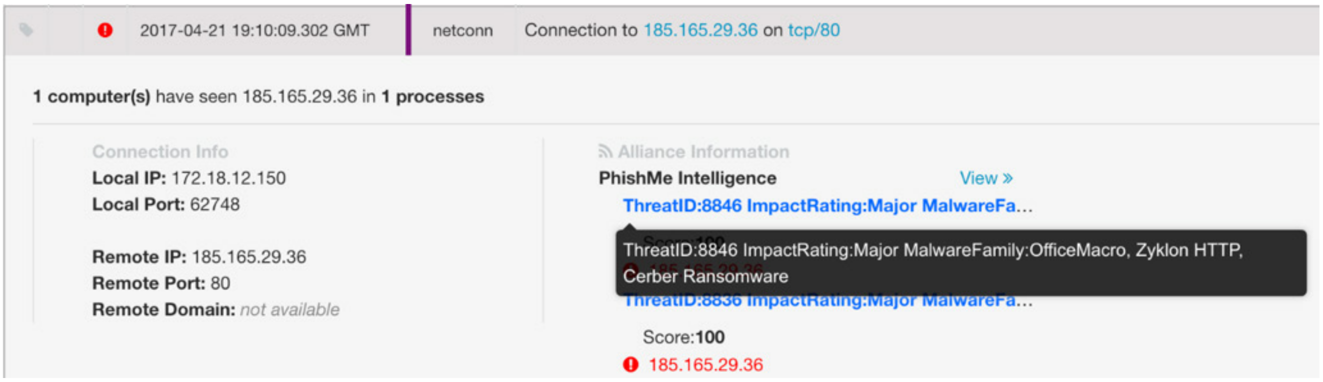
Phishing Intelligence

- ✓ Human-verified timely and contextual phishing (machine-readable threat intelligence) MRTI with no false positives
- ✓ High fidelity intelligence about phishing, malware, and botnet infrastructure
- ✓ Human-readable reports with context behind threat actor infrastructure to understand attacker tactics

Correlation and Actionable Decisions

- ✓ Real-time response and historical analysis driven from verified phishing threats with impact ratings for actionable decisions
- ✓ Network-based and file indicators used in phishing campaigns prioritized based on threat severity
- ✓ Watchlists and Investigations for complete visibility and continuous recording correlated to phishing threats
- ✓ Hunt phishing threats across endpoints efficiently without exhausting security team and endpoint resources

With Cofense Intelligence and Cb Response, security teams can detect and respond based on credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API that Cb Response polls for indicators and cross-correlates in the platform. The constant polling of credible human-verified phishing intelligence provides security teams with visibility into the latest global phishing threats. An endpoint communicating with network-based IOCs or hashes provided from Cofense Intelligence can quickly be protected or investigated based on predefined Cb Response configurations. Analysts have unobstructed views into credible phishing threats leading to higher confidence in the action taken based on the indicator results returned to the platform.



2017-04-21 19:10:09.302 GMT | netconn | Connection to 185.165.29.36 on tcp/80

1 computer(s) have seen 185.165.29.36 in **1 processes**

Connection Info

Local IP: 172.18.12.150
Local Port: 62748

Remote IP: 185.165.29.36
Remote Port: 80
Remote Domain: *not available*

Alliance Information

PhishMe Intelligence View »

ThreatID:8846 ImpactRating:Major MalwareFa...

ThreatID:8846 ImpactRating:Major MalwareFamily:OfficeMacro, Zyklon HTTP, Cerber Ransomware

ThreatID:8836 ImpactRating:Major MalwareFa...

Score:**100**

185.165.29.36

(Cofense Intelligence ransomware-based indicator detected communicating by Cb Response endpoint)

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. This can be thwarted through credible and trustworthy intelligence applied to network policies based on threat severity.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real-time 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.

How It Works

Cofense Intelligence and Cb Response provide analysts with the ability to investigate, validate, and remediate based on indicator impact ratings from phishing-specific machine-readable threat intelligence (MRTI). Using high fidelity phishing intelligence means that analysts can prioritize and decisively respond to alerts from intelligence consumed via Cofense's API. With Cb Response, security teams can operationalize Cofense Intelligence indicators through features such as:

- **Watchlists**
- **Investigations**
- **Triage Alerts**
- **Process Search**
- **Binary Search**
- **Banned Hashes**

Cofense Intelligence human-readable reports are linked from within Cb Response to provide analysts with IOC context. This context is the additional insight for security teams to understand the criminal infrastructure and support remediation decisions. Analysts and security leaders will have visibility into email message contents, malware artifacts with full threat detail, and executive summaries to easily understand the threat actor's operation and the risk to the business.

The combination of Cofense Intelligence and Cb Response provides clear insight for assertive action from the following types of indicators:

- **Payload URLs and Exfiltration Sites**
- **Command and Control Servers**
- **Malicious IP Addresses**
- **Compromised Domains**

Security teams can respond quickly and with confidence to mitigate identified threats. Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions that are detected and responded to across endpoints.

About Carbon Black

Carbon Black is the leading provider of next-generation endpoint security. With more than 9 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

Carbon Black.

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