Cofense Intelligence™

VON MENSCHEN GEPRÜFTE, PHISHING-SPEZIFISCHE INFORMATIONEN ÜBER BEDROHUNGEN

Die Forschungsabteilung von Cofense hat ermittelt, dass 2016 97% aller Phishing-E-Mails 2016 Ransomware enthielten. Diese Zahlen sind beunruhigend. Doch was können Sie tun um Ihr Unternehmen davor zu bewahren, selbst Opfer solcher E-Mails zu werden? Cofense Intelligence meldet gefährliche E-Mails zuverlässig und rechtzeitig, und stärkt so die Fähigkeit Ihres Unternehmens, akute Phishing-Angriffe schnell zu erkennen und darauf zu reagieren.

Unsere Sicherheitslösung

Cofense Intelligence ist der führende Cybersicherheitsservice, der Unternehmen dabei hilft, gefährliche Malware- und Phishing-Angriffe aufzuhalten. Wir benutzen firmeneigene Verfahren um die Hauptbedrohungen für Ihr Unternehmen automatisch zu identifizieren, und bieten Ihnen rechtzeitig wirksame Tools und Anleitungen um Angriffe zu finden, die sonst unbemerkt geblieben wären.

Die wichtigste Methode, um Malware in Unternehmen zu installieren, besteht aus mittelbaren oder unmittelbaren E-Mail-Attacken. Phishing E-Mails mit bösartigen Anhängen oder Links sind immer noch in der Lage, die Sicherheitsvorkehrungen der meisten Unternehmen zu umgehen und den E-mail-Benutzer zu erreichen.

Die meisten Sicherheitsanbieter warten mit der Analyse einer Bedrohung und der Bestätigung, dass es sich um eine bösartige Bedrohung handelt, bis diese bereits einen Fuß in der Tür hat. Normalerweise müssen dem Anbieter dazu erst mehrere Meldungen von Kunden über bösartige Dateien oder Endgeräte vorliegen. Folglich vergeht viel Zeit zwischen der Lancierung eines Angriffs und dem Zeitpunkt, an dem das Unternehmen über zuverlässige Informationen darüber verfügt. Da jede Bedrohung für sich genommen untersucht wird, werden sämtliche Bedrohungen als gleichwertig gemeldet, ohne Kontext zum Angriff oder Angriffen, mit denen sie zusammenhängen.

Infolge dieses Ansatzes verfügen Sicherheitsexperten nicht über die Bedrohungserkenntnisse, die zur Abwehr des Angriffs oder zur Priorisierung einer passenden Antwort erforderlich sind.

Cofense geht die Identifizierung von täglichen Bedrohungen völlig anders an – nämlich bevor sie Ihr Netzwerk infizieren.

Täglich erreichen uns über eine Millionen Nachrichten aus zahlreichen Quellen. Angriffe werden automatisch aufgegliedert um Zusammenhänge zwischen ihnen zu ermitteln. Unsere einzigartigen Clustering-Algorithmen sortieren bösartige E-Mails nach einer Reihe von Faktoren und halten Ausschau nach neuen Bedrohungen in Form von E-Mails mit gefährlichen Links und/oder Anhängen. Sobald ein neuer Cluster identifiziert wird, werden seine Merkmale in unserem Bedrohungsrepositorium dokumentiert und aktualisiert.

Wichtigste Vorteile

- ✓ Zeitnahe, präzise und umsetzbare Phishing-Bedrohungserkenntnisse
- ✓ Nutzbare Phishing-Bedrohungserkenntnisse
- ✓ Spezialisierte Bedrohungsanalytiker helfen bei der Umsetzung von Bedrohungserkenntnissen und liefern entsprechende Anleitungen
- ✓ Angriffsanalysen und -kontexte helfen dabei, schnell fundierte Entscheidungen zu treffen

Mithilfe von firmeneigenen Methoden werden die gefährlichen Inhalte von jeder bestätigten Phishing-Kampagne ermittelt, um die Art der Bedrohung festzustellen. Diese Informationen werden dann in unserer Datensammlungen aktualisiert, um weitere kampagnen- und zeitrahmenübergreifende Analysen durchführen zu können. Bedrohungserkenntnisse, die anhand von diesen Analysen gewonnen werden, werden Ihren Sicherheitsteams und Ihrer Sicherheitsinfrastruktur in verschiedenen Nutzungsformaten zur Verfügung gestellt, sodass entsprechende Maßnahmen ergriffen werden können.

Dank diesem proaktiven Ansatz in Bezug auf Bedrohungsanalysen können Sie Ihre bestehende Sicherheitsinfrastruktur so vorbereiten, dass möglicherweise bösartige Angriffe unterbrochen werden. Angriffstaktiken, die auf einen Einbruch in Ihr Netzwerk abzielen, werden ebenso aufgedeckt wie die Zusammenhänge zwischen Phishing-Kampagnen und Kompromittierungsindikatoren (Indicators of Compromise, IOCs). Die Kombination aus wirksamen Bedrohungsdaten und Einblick in die Zusammenhänge zwischen Phishing-Angriffen und ihren Triebfedern hilft Ihrem Team bei der Begegnung, Erforschung und Priorisierung.

Die einzigartigen Sicherheitserkenntnisse von Cofense verschaffen Ihnen die Werkzeuge, die Sie zur Identifizierung, Blockierung und Erforschung von täglichen Sicherheitsbedrohungen, mit denen Ihr Unternehmen konfrontiert wird, benötigen. Diese exakten Informationen stehen Ihren Teams in verschiedenen Formaten zur Verfügung und ermöglichen eine gezielte Vorbereitung und Abwehr von Angriffen auf Ihr Netzwerk.

- Menschenlesbare Berichte über Bedrohungserkenntnisse liefern eingehende Trendanalysen der wichtigsten Bedrohungen. Diese Berichte umfassen auch eine Expertenanalyse der Angriffsmethodologie.
- Maschinenlesbare Bedrohungserkenntnisse (MRTI), die direkt in Sicherheitsanlagen und Bedrohungsrepositorien einfließen. Firewalls, IDS/IPS, SIEM können neuartige Bedrohungen jetzt im frühesten Angriffsstadium erkennen und abwehren.
- SaaS-Erforschungsanwendungen, um Phishing- und Malware-Angriffe zu untersuchen. Diese Abruftools liefern die aktuellsten Erkenntnisse über Angriffe und die Art und Weise, in der sie ausgeführt werden.
- Sachkundige Anleitungen vom erstklassigen Sicherheitsteam von Cofense, um Sie bei der Umsetzung der besten Verfahren zur Reduzierung von Netzwerkbedrohungen zu unterstützen.

> Wir verarbeiten Cofense-Berichte immer zuerst, da wir diese Meldungen sehr ernst nehmen. Cofense Intelligence liefert uns die besten, brauchbarsten Phishing-Bedrohungserkenntnisse.
>
> **Bedrohungsanalytiker eines großen Finanzdienstleisters**

Der Intelligence-Service von Cofense funktioniert, da er Folgendes bietet:

Brauchbarkeit	Cofense Intelligence bietet Bedrohungserkenntnisse in verschiedenen Formen an. Die maschinenlesbaren Bedrohungserkenntnisse (MRTI) entsprechen industriellen Normen zur schnellen Eingliederung in bestehende Sicherheitsanlagen. Analyseberichte im PDF- und HTML-Format werden für Bedrohungsanalytiker und Computer-Notfallteams optimiert.
Zuverlässigkeit	Cofense Intelligence benachrichtigt Kunden nur über bestätigte Bedrohungen, die durch unsere geschulten Analytiker überprüft worden sind, und stellt damit eine hohe Signalwirkung sicher.
Pünktlichkeit	MRTI werden an dem Tag veröffentlicht, an dem neue Angriffe bestätigt werden. Strategische Analyseberichte werden wöchentlich veröffentlicht. Die Untersuchungsanwendung ist tagtäglich rund um die Uhr verfügbar.
Ein frischer Blick	Der Cofense Intelligence-Service gewinnt Bedrohungserkenntnisse aus zahlreichen bösartigen E-Mail- und Spam-Quellen, die benutzt werden um tagtäglich gefährliche Inhalte bei Ihren Mitarbeitern abzuliefern.
Kontextbezogenheit	Cofense Intelligence veröffentlicht Bedrohungserkenntnisse, die darlegen, wie die einzelnen Elemente eines Angriffs sich ineinander fügen und Zusammenhänge zwischen augenscheinlich unterschiedlichen Angriffen aufdecken.
Anwenderfreundlichkeit	Wir helfen Ihnen bei der Umsetzung des Service und bieten langfristige Unterstützung, um sicherzustellen, dass Sie den Service optimal nutzen können.

Cofense™, ehemals PhishMe®, ist der weltweit führende Anbieter von Anti-Phishing-Lösungen. Wir bieten einen auf Zusammenarbeit basierenden Cybersicherheitsansatz, mit dem wir es ermöglichen, unternehmensweit gegen aktive E-Mail Bedrohungen vorzugehen. Unsere Verteidigungslösungen kombinieren marktführende Technologien und aktuelle Angriffsintelligenz von Mitarbeitern um laufende Angriffe schneller zu stoppen und weitere Sicherheitsverstöße früh zu erkennen.
Von der Sensibilisierung der Mitarbeiter bis zur Sicherheitsautomatisierung und Integration sind unsere Lösungen darauf ausgelegt, die Angriffskette zu unterbrechen um die Auswirkungen von Spear Phishing, Ransomware, Malware und Business Email Compromise E-Mails schnell einzudämmen.
Tausende globale Unternehmen im Bereich Verteidigung, Energie, Finanzen, Gesundheitswesen und Fertigung profitieren bereits durch angepasstes Mitarbeiterverhalten von der Möglichkeit, schneller auf Vorfälle reagieren zu können und das Risiko von Sicherheitsverstössen zu vermindern.

COFENSE

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

Weitere Informationen finden Sie unter **www.cofense.com.**