Trend Micro™

DEEP DISCOVERY™ EMAIL INSPECTOR

Stoppen Sie gezielte E-Mail-Angriffe, die Sie mit Ransomware infizieren oder zu Datenverlust führen können

Komplexe, zielgerichtete Angriffe haben schon oft unter Beweis gestellt, dass sie herkömmliche Sicherheitsmaßnahmen einfach umgehen und vertrauliche Daten entwenden oder wichtige Daten verschlüsseln können, bis Lösegeldforderungen erfüllt werden. Trend Micro Forschungen haben ergeben, dass über 90 % dieser Angriffe mit einer Spear-Phishing-E-Mail beginnen, die einen bösartigen Dateianhang oder eine URL enthält, die von herkömmlichen E-Mail- oder Endpunktsicherheitslösungen nicht erkannt werden.

Deep Discovery Email Inspector nutzt innovative Techniken zur Erkennung und Abwehr von Spear-Phishing-E-Mails, über die ahnungslosen Mitarbeitern komplexe Malware und Ransomware zugestellt wird. Der Email Inspector wird hinter ihr bestehendes E-Mail-Gateway integriert. Die Lösung erkennt und sperrt speziell entwickeltete Spear-Phishing-E-Mails, die zielgerichtete Angriffe über bösartige Anhänge und URLs durchführen, sowie andere komplexe Bedrohungen und Ransomware.

WESENTLICHE FUNKTIONEN

Transparenz
Arbeitet reibungslos mit einem bestehenden Spam-Filter oder einem sicheren E-Mail-Gateway zusammen, um Spear-Phishing-E-Mail-Angriffe zu erkennen, die in Anhängen und URLs komplexe Malware (einschließlich Ransomware) enthalten.

Umfassende Erkennungstechniken
Erkennt Zero-Day-Exploits, komplexe Bedrohungen, Ransomware und Angreifer-verhalten. Dabei werden Techniken wie Datei-, IP- und Web-Reputation, statische Analysen, heuristische Analysen, Algorithmen und benutzerdefinierte Sandbox-Analysen eingesetzt, um bekannte und unbekannte Bedrohungen zu erkennen. Lokale Bedrohungsdaten werden mit Bedrohungserkenntnissen von Trend Micro korreliert.

Flexibilität
Sie haben die Wahl zwischen den folgenden Installationsoptionen: Inline-Sperrung/ Quarantäne, Protokollieren oder Entfernen einer erkannten Bedrohung aus einer E-Mail und Benachrichtigung des Benutzers.

Benutzerdefinierte Sandbox-Analysen
Nutzt virtuelle Images, die genau Ihren Systemkonfigurationen, Treibern, installierten Anwendungen und Sprachversionen entsprechen. Dieser Ansatz verbessert die Erkennungsrate komplexer Bedrohungen, die darauf abzielen, standardmäßige virtuelle Images zu umgehen. Die benutzerdefinierte Sandbox-Umgebung umfasst den sicheren externen *Live-Modus-Zugriff*, der mehrstufige Downloads, URLs, Command-and-Control (C&C) und mehr erkennt und analysiert. Sandboxing-Funktionen werden als Teil einer integrierten Appliance oder als skalierbare eigenständige Funktion angeboten.

Schutz vor Ransomware-Angriffen
Wenn ein Spear-Phishing-Angriff gestartet wird, dauert es durchschnittlich nur eine Minute und 40 Sekunden, bis der erste Benutzer die bösartige E-Mail öffnet.[1] Da E-Mails der bevorzugte Übertragungsweg für Ransomware sind, bedeutet dies eine Gefährdung aller Benutzer in Ihrem Unternehmen. Durch ein Blockieren von schadhaften Inhalten einer Datei werden bösartige E-Mails bereits am Gateway abgefangen und kommen nicht ins Unternehmensnetzwerk hinein.

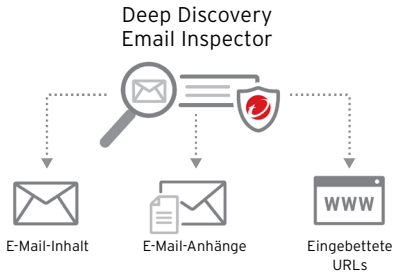
Entscheidende Vorteile

Besserer Schutz

- Stoppt Spear-Phishing-E-Mails, mit denen die meisten zielgerichteten Angriffe gestartet werden
- Blockiert Ransomware, bevor Schaden entsteht
- Findet mithilfe von benutzerdefiniertem Sandboxing Bedrohungen, die für Standard-E-Mail-Sicherheitslösungen nicht erkennbar sind

Sichtbare Rendite

- Stoppt zielgerichtete Spear-Phishing- und Ransomware-Angriffe, wodurch die kostenintensive Behebung von durch Viren verursachten Problemen vermieden wird
- Arbeitet reibungslos mit bestehenden E-Mail-Sicherheitslösungen zusammen
- Tauscht IOCs mit Netzwerk- und Endpunktsicherheitsschichten aus



NSS LABS RECOMMENDED
Trend Micro™ Deep Discovery
100%
Data Breach Rate
- 2017 -
EMPFOHLEN seit 4 Jahren in Folge

ICSA labs CERTIFIED

Email Inspector kann jeden Versuch, Ransomware über ahnungslose Mitarbeiter einzuschleusen, durch Identifikation folgender Angriffsmuster erkennen und abwehren:

- Bekannte Ransomware: Pattern- und Reputation-basierte Analyse
- Unbekannte Ransomware: Kommunikationsmerkmale, Skript-Emulation, Zero-Day-Exploits, zielgerichtete und kennwortgeschützte Malware
- Änderungen an großen Mengen von Dateien, Verschlüsselungsverhalten und Änderungen an wiederhergestellten Backup-Dateien durch benutzerdefiniertes Sandboxing

Wenn Ransomware entdeckt wurde, kann verhindert werden, dass sie einem Empfänger zugestellt wird und Daten verschlüsselt. IOCs können zur Abwehr nachfolgender Angriffe mit anderen Netzwerk- und Endpunktkontrollen ausgetauscht werden.

Deep Discovery Email Inspector ist eine Komponente von Trend Micro Network Defense – unterstützt durch XGen™ Security.

DIE DEEP DISCOVERY EMAIL INSPECTOR APPLIANCE – HARDWARESPEZIFIKATIONEN

Hardwarespezifikationen	Modell 7100	Modell 9100
Installationsoptionen	Modus MTA, BCC oder SPAN/TAP	Modus MTA, BCC oder SPAN/TAP
Kapazität	Bis zu 400.000 E-Mails pro Tag	Bis zu 800.000 E-Mails pro Tag
Formfaktor	1U Rack montierbar, 48,26 cm	2U Rack montierbar, 48,26 cm
Abmessungen	43,4 cm x 64,2 cm x 4,28 cm	43,4 cm x 75,58 cm x 8,73 cm
Gewicht	19,9 kg	31,5 kg
Verwaltungsports	10/100/1000 BASE-T RJ45 Port x 1 iDRAC Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 Port x 1 iDRAC Enterprise RD45 x 1
Datenports	10/100/1000 BASE-T RJ45 x 3	10/100/1000 BASE-T RJ45 x 3
Wechselstromversorgung	100 bis 240 VAC	100 bis 240 VAC
AC-Eingangsstrom	7,4 A bis 3,7 A	10 A bis 5 A
Festplatten	2 x 600 GB 2,5 Zoll SAS	2 x 4 TB 3,5 Zoll SATA
Unterstützung von Internetprotokollen	IPv4/IPv6	IPv4/IPv6
RAID-Konfiguration	RAID 1	RAID 1
Stromversorgung	550 W (redundant)	750 W (redundant)
Stromverbrauch (max.)	604 W	847 W
Wärmeabgabe	2133 BTU/h (max.)	2891 BTU/h (max.)
Betriebstemperatur	10 bis 35 °C	10 bis 35 °C
Hardwaregarantie	3 Jahre	3 Jahre
Optionale Glasfaser-Netzwerkkarte	Dual Port Fiber Gigabit (SX/LX)	Dual Port Fiber Gigabit (SX/LX)

ERKENNUNG UND ABWEHR VON

- Gezielten Angriffen und komplexen Bedrohungen
- Phishing, Spear-Phishing und anderen E-Mail-Bedrohungen
- Zero-Day-Malware und Exploits in Dokumenten
- Ransomware-Angriffen

KOMPONENTEN DER DEEP DISCOVERY PLATTFORM

Deep Discovery Email Inspector ist Teil der Deep Discovery Plattform. Er bietet Schutz vor komplexen Bedrohungen für den E-Mail-Verkehr, also dort, wo es für Ihr Unternehmen besonders darauf ankommt – und ergänzt vorhandene Sicherheitslösungen.

Deep Discovery Inspector ist eine sofort einsetzbare Netzwerk-Appliance, die alle Ports und über 107 Protokolle auf zielgerichtete Angriffe überwacht. Umfassende Erkennungstechniken, einschließlich Onboard-Sandboxing, sorgen dafür, dass zielgerichtete Angriffe schnell erkannt werden.

Deep Discovery Analyzer bietet erweiterte Sandbox-Analysen, mit denen der Wert von Sicherheitsprodukten wie Endpunktschutz, Web- und E-Mail-Gateways, Netzwerksicherheit und anderen Deep Discovery Produkten gesteigert wird. Verdächtige Objekte oder URLs können automatisch oder manuell zur Analyse an Deep Discovery Analyzer gesendet werden. Mithilfe umfassender Erkennungs- und Umgehungsschutztechniken kann Deep Discovery Analyzer Ransomware, komplexe Malware, Zero-Day-Exploits, C&C-Kommunikation sowie mehrstufige Downloads erkennen, die von bösartigen Nutzlasten oder URLs auf Windows, Mac und Android Betriebssystemen stammen.

1 2016 Verizon Data Breach Investigations Report

TREND MICRO™

Securing Your Journey to the Cloud