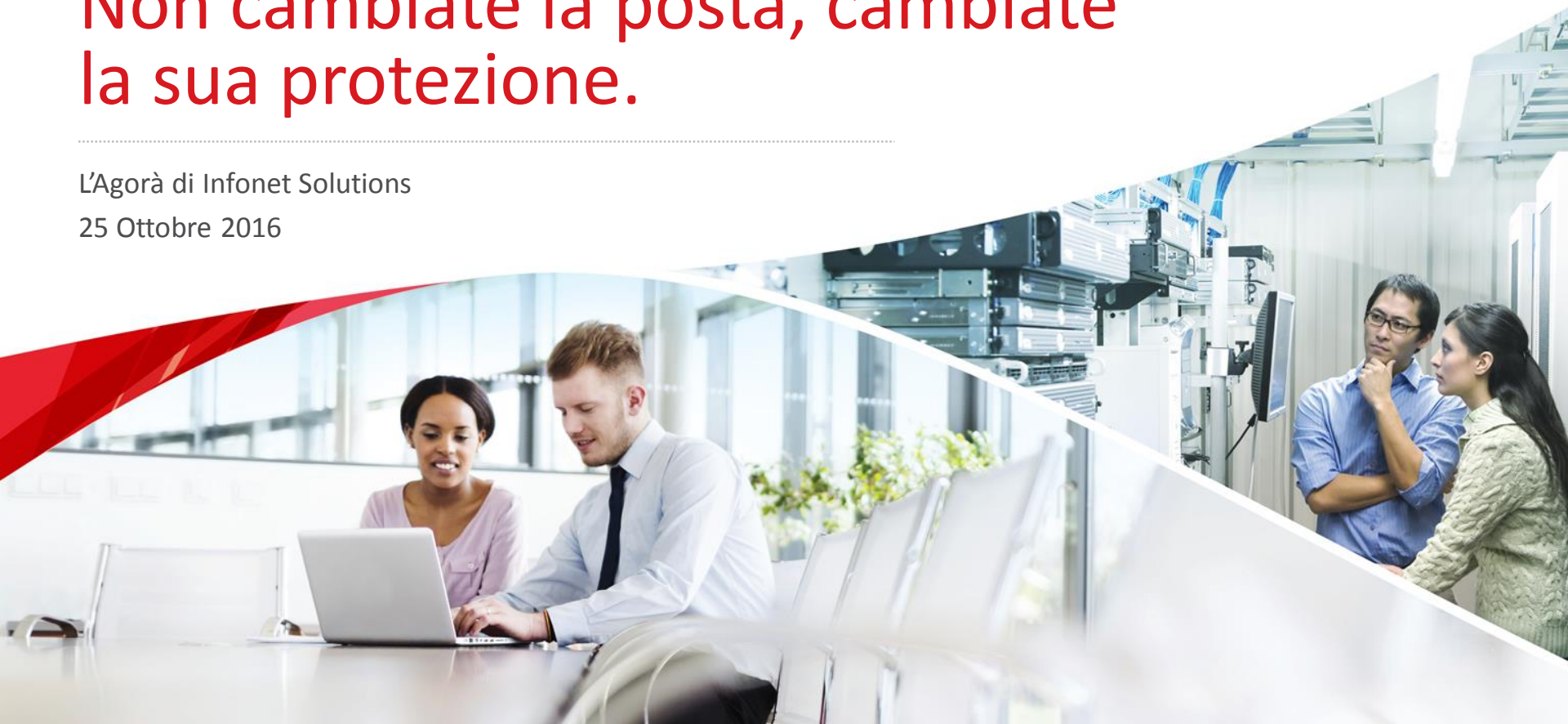
C’è un ransomware per te? Non cambiate la posta, cambiate la sua protezione.

L’Agorà di Infonet Solutions

25 Ottobre 2016



Willie Sutton

"That's Where the Money is..."

— Willie Sutton

Email: il principale vettore d'infezione

- Il 91% degli attacchi mirati inizia con una mail di "spear phishing"
- Il tempo medio impiegato ad aprire una mail "spear phishing" dal primo impiegato che la riceve è 1 minuto e 40 secondi. *Source*

- Un ransomware impiega meno di un minuto a criptare i dati su un PC *Source*

Perchè gli attacchi via email sono diffusi?

- Gli impiegati di un'organizzazione sono obiettivi facili
- La posta è il percorso più agevole per entrare in una organizzazione
- I costi associati a ransomware, minacce note e sconosciute sono tangibili & quantificabili

Tre punti importanti

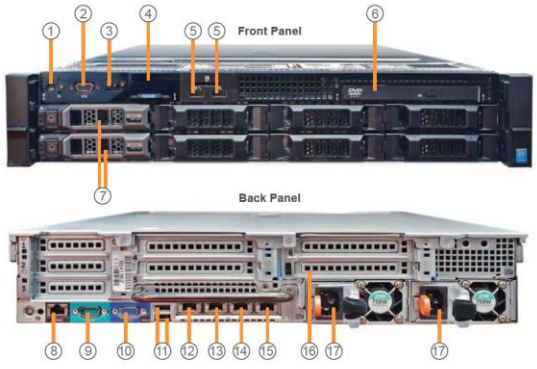
Rilevamento: identificare e blocca le email di spear-phishing che sono spesso parte della fase iniziale di una campagna di attacco o ransomware mirato

Interoperabilità: lavorare senza problemi con soluzioni anti-spam o di mail gateway già esistenti per rilevare attacchi di spear-phishing che potrebbero contenere malware avanzato o ransomware

ROI: investimento limitato con benefici tangibili per evitare i costi ed i rischi conseguenti a attacchi mirati e ransomware.

Deep Discovery Email Inspector

Protezione da attacchi via mail



(1) Power-on indicator/button
(2) Front video connector
(3) LCD menu buttons
(4) LCD panel
(5) USB 2.0 connectors
(6) Optical drive
(7) Hard drives
(8) iDRAC port
(9) Serial connector
(10) Back video connector
(11) USB 3.0 connectors
(12) Management port eth0
(13) Data port eth1
(14) Data port eth2
(15) Data port eth3
(16) Fiber NIC slot
(17) Power supply connectors

Note: Your device comes with the Copper Ethernet NIC. If your purchase includes the optional Fiber Ethernet NIC, plug it to the appliance through the Fiber NIC slot.

Tecnologie raffinate per identificare e bloccare mail di spear-phishing

- Il motore di sandboxing personalizzato analizza e-mail inclusi gli allegati e URL.
- Lavora in modo trasparente con i gateway di posta elettronica esistenti
- Può essere installato in linea (MTA), solo monitoraggio (BCC o SPAN / TAP)
- Fornisce password per i file protetti

➢ ***Elabora fino a 800.000 mail al giorno***

Tecnologia sofisticata migliora la rilevazione

Sandbox personalizzata

Risk level:
Notable Characteristics
Anti-security, self-preservation
Autostart or other system reconfiguration
Deception, social engineering
File drop, download, sharing, or replication
Hijack, redirection, or data theft
Malformed, defective, or with known malware traits
Process, service, or memory object change
Rootkit, cloaking
Suspicious network or messaging activity
Other threat characteristics

Sandboxes to Match Your Environment

- System configurations, drivers, installed applications and language settings so sandbox cannot be evaded: better detection without evasion
- Safe external access through *live mode* to detect and analyze multi-stage downloads, URLs, C&C and more.
- Part of integrated appliance or scalable standalone capability

Attachment Analysis

- Attachments are unpacked, decompressed, and unlocked.
- Detection engines identify advanced malware, document exploits and ransomware
- Wide range of file types supported: Windows executables, Microsoft Office, PDF, Zip, Java

URL Analysis

- Reputation-checked via Smart Protection Network
- Page content is scanned and sandboxed to discover redirects, advanced malware, and exploits used in drive-by downloads

Tecnologia sofisticata migliora la rilevazione

Allegati protetti da password?

Esame dei contenuti, euristica, lista di password definita dal cliente per facilitare l'analisi dei file compressi protetti

Gestione delle policy

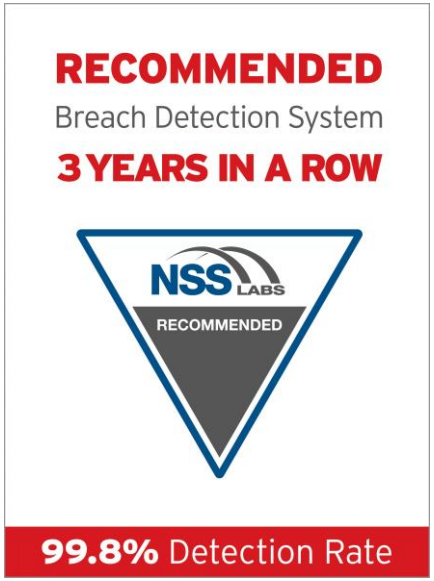
Quarantena o tag sono configurabili in base alla gravità di rilevamento. Scelta manuale/automatica del tipo di allegato da analizzare in sandbox.

Correlated Threat Intelligence

Un portale integrato correla minacce individuate a livello locale con intelligence globale che fornisce caratteristiche del malware, le origini, le varianti, relative C & C, IP, profilo attaccante, e indica come bonificare.

Tecnologia sofisticata approvata

- Motori e tecnologia basati sul pluripremiato Deep Discovery Inspector
- Il test BDS di NSS Labs ha evidenziato che Trend Micro rileva il 100% delle minacce e-mail
- Certificazione ICSA per il rilevamento delle minacce avanzata



Trend Micro: Connected Threat Defense

Abilita risposta rapida, attraverso la distribuzione di firme e aggiornamenti di sicurezza in tempo reale

Valuta potenziali vulnerabilità e protegge proattivamente PC, server e gateway

Analizza il rischio e la natura di attacco e attaccante, e valuta l'impatto delle minacce retrospettivamente

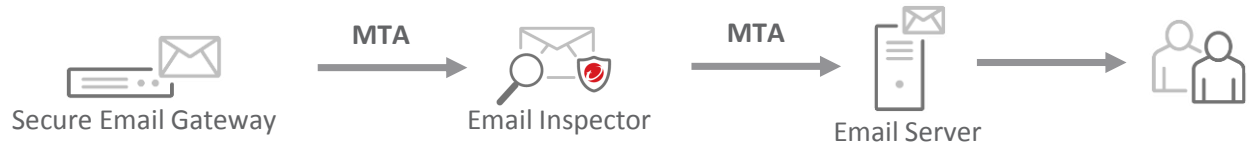
Rileva il malware avanzato, il comportamento e le comunicazioni invisibili alle difese normali

Rapido investimento in sicurezza

Opzioni di installazione

MTA Mode

- Blocca le mail maligne
- Fornisce analisi delle minacce e notifiche
- Possibili più DDEI in cascata con bypass se non disponibili



BCC Mode

- Analisi passiva delle mail
- Fornisce analisi delle minacce e notifiche
- Monitor in differita

SPAN/TAP Mode

- Ascolta il traffico
- Fornisce analisi delle minacce e notifiche
- Monitor in differita

Rapido investimento in sicurezza

Soluzione a basso costo

- Informazioni sulle minacce è integrato e a costo zero ... senza canone di abbonamento aggiuntivo richiesto.
- Un solo appliance fa tutto ... non più caselle di e-mail e web
- Non ci sono costi d’integrazione o di sviluppo personalizzati per l'analisi sandbox personalizzato
- Nessun costo per investimenti persi, eliminati e sostituiti
- Funziona con Exchange, Notes o qualsiasi server di posta SMTP

Provare Deep Discovery Email Inspector

- POC con supporto Trend Micro

- 60 gg di test con risultati immediati

- Possibilità di convertire il POC in acquisto

Grazie

tiberio_molino@trendmicro.it