

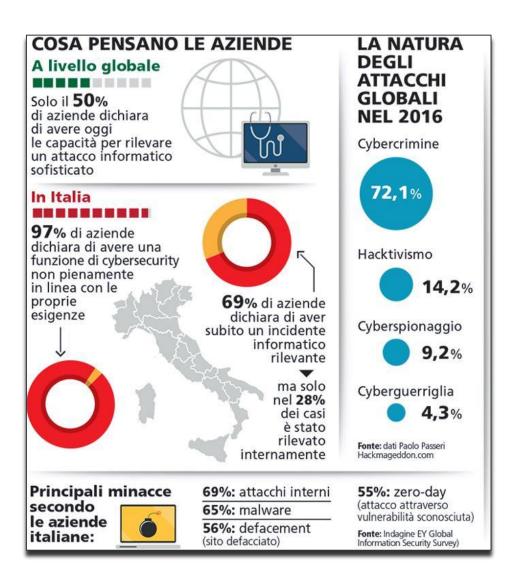
NUOVI SCENARI LAVORATIVI NUOVE MINACCE



NUOVI SCENARI LAVORATIVI



STATO DELL'ARTE: SECURITY IN ITALIA

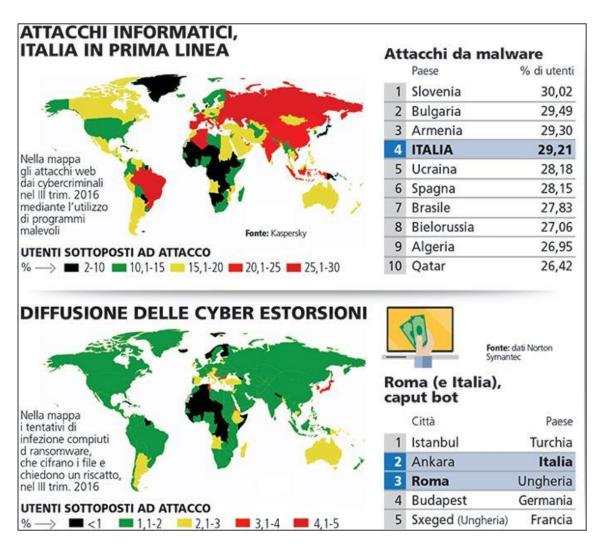


- Il 97% delle Aziende Italiane, contro il 50% di quelle globali, dichiara di non avere un Sistema di Sicurezza in grado di bloccare le minacce informatiche avanzate
- II 69% delle Aziende Italiane, dichiara di aver subito un attacco informatico rilevante

Fonte: La Stampa 2016



STATO DELL'ARTE: SECURITY IN ITALIA



 Italia e' al 4' posto nel mondo come attacchi Malware, 29% utenti internet sono stati colpiti nel 2016

 Roma e' la 3 citta' nel mondo colpita da cyber estorsioni (ramsomware ed affini)

Fonte: La Stampa 2016



"AntiVirus is Dead"

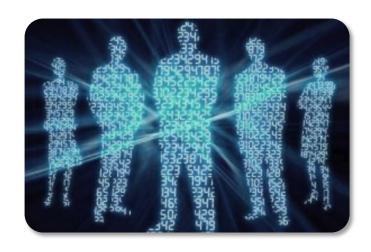
Brian Dye, Symantec's senior vice president information security (2014)



UNA NUOVA FRONTIERA DI ATTACCHI....

... LE MINACCE AVANZATE PERSISTENTI

Un' APT (Advanced Persistent Threat) è un nuovo tipo di minaccia intelligente, ad alto valore tecnologico, pensata per avere un ritorno economico prolungato nel tempo e pieno controllo di uno specifico target





Gli attributi che contraddistinguono una minaccia APT

- 1. Avanzata
- 2. Persistente
- 3. Targettizzata



MA IO SONO UN PESCE PICCOLO....



ERRATO!



MA VERAMENTE L'ANTIVIRUS E' MORTO ?

Esistono disponibili programmi che aggiungono ad un codice tutte le tecniche di evasione necessarie ad eludere un antivirus ed una sandbox standard creando delle vere ZERO DAY

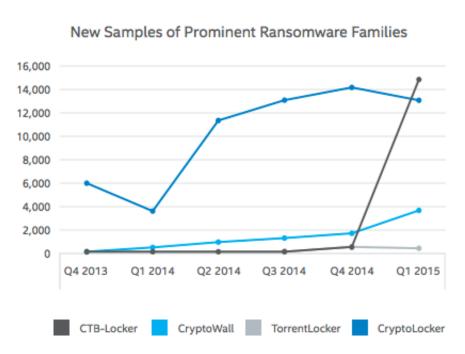


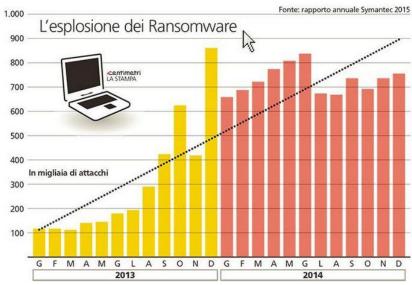




LA PROLIFERAZIONE DEL RANSOMWARE

Ransomware e' una forma di computer malware che blocca l'accesso al vostro computer o ai suoi file fino a quando non venga pagato un riscatto per riaverne l'accesso.







Source: McAfee 2015



10

La polizia dice: Pagate... O 2016 WatchGuard Technologies, Inc. All Rights Reserved

I PIU' DIFFUSI RANSOMWARE

Cryptolocker, CTB-Locker, CryptoWall, Tesla Script, CryptorBit, KeyHolder, Operation Global, TorrentLocker, CryptoDefense, ZeroLocker, Ransom32

Colpiscono utenti Windows, Mac, Linux...









Viene inettato il downloader nel PC attaccante tramite un drive by download (Quasi sempre una email di phising) oppure se gia' infetti e parte di una rete di BOT





Il downloader si attiva, contatta il server maligno C&C (Command e Control) in HTTP e scarica il vero e proprio malware *Trojan:Win32/Crilock.A.*

Il malware viene trasferito criptato con chiave 2048 bit quindi nessun antivirus perimetrale puo' analizzarlo se non lo conosce.

Semplice allora.... blocco i server pericolosi! Peccato che i server che contatta hanno un nome randomico sincronizzato con i server di destinazione (una sorta di autenticazione a due fattori)

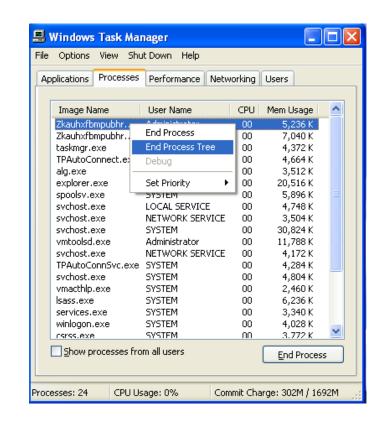
```
lea-
        eax, [ebp+SystemTime]
                         ; lpSystemTime
push
        eax
call
        ds:GetSystemTime
        [ebp+arq 0]
push
add
        esi, 3Ch
        edx, [ebp+SystemTime]
lea -
        ecx. esi
mov
        GenerateRandomDomainName
call.
```

xeogrhxquuubt.com; qaaepodedahnslq.org; wennvalsktiowt.ru



Il malware viene lanciato in background e cripta con chiave pubblica RSA-2048 bit i file dati del PC, dei dischi mappati e tutti i file raggiungibili tramite condivisioni di rete.

Il malware contiene tecniche di evasione che consentono di evitare di essere scoperti da antivirus locali





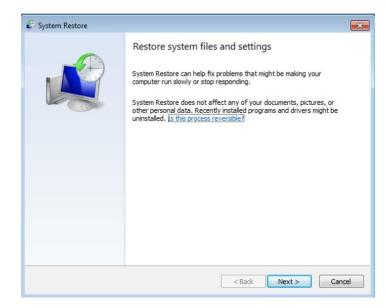
Se me ne accorgo in tempo.....

- Se il virus vi infetta, agisce molto velocemente, questione di minuti.
- Spegnete immediatamente il computer, anche brutalmente staccando la spina di alimentazione.
- Non riavviate il computer: ad ogni riavvio il virus continua a crittografare i vostri files, estendendo l'entità del danno.
- Rimuovete eventuali dispositivi USB connessi al sistema (pennette, hard disk, chiavette di firma digitale, ecc.).
- Se il computer è connesso in rete ad altri computer o server, staccate immediatamente il cavo di rete e spegnete tutti gli altri computer/server della rete.



Se me ne sono accorto in tempo.....

- Fate ripartire il computer in "Safe Mode with Networking"
- Accedere al profilo che è stato infettato.
 Avviare il browser Internet e scaricare un programma anti-spyware, lanciarlo e rimuovere Cryptolocker
- Recuperare una situazione predente del PC da un punto di ripristino passato, dalla linea di comando rstrui.exe e premere INVIO
- Dopo aver ripristinato il computer ad una data precedente, rilanciare il programma anti-spyware per eliminare eventuali residui del virus ransomware CryptoLocker





Se NON me ne accorgo in tempo.....

Comparira' una finesta dove vi informa della avvenuta criptazione dandovi 72 ore di tempo per pagare il riscatto o la chiave private verra' distrutta rendendo impossibile recuperare I file.

Il riscatto e' dell'ammontare di qualche centinaio di euro. Più si tarda nel pagamento, più il prezzo sale, fino a raggiungere anche venti volte la cifra iniziale.

Unica alternativa al pagamento.... recuperare i file da un backup





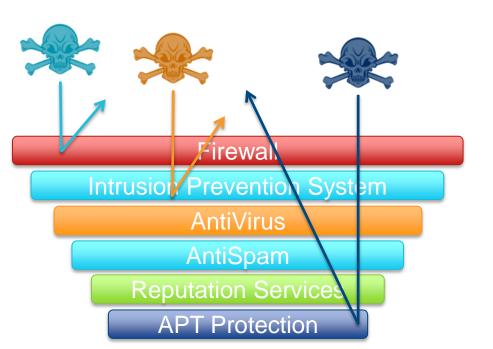




Minacce Avanzate: WATCHGUARD DEFENSE-IN-DEPTH

Advanced threats, per definizione utilizzano multipli vettori di attacco.

Non una sigola difesa vi proteggeranno completamente da un attacco APT ...





Piu' livelli di sicurezza avete, maggiore possibilita' avete di identificare e bloccare una advanced persistent threat.



LA SICUREZZA GLOBALE HA 4 COMPONENTI



Prevenzione

Previene che le minacce entrino nella rete.



Rilevazione

Rileva eventi pericolosi prima possano causare problemi.



Correlazione

Controlla le relazioni tra eventi di sicurezza per determinare il rischio



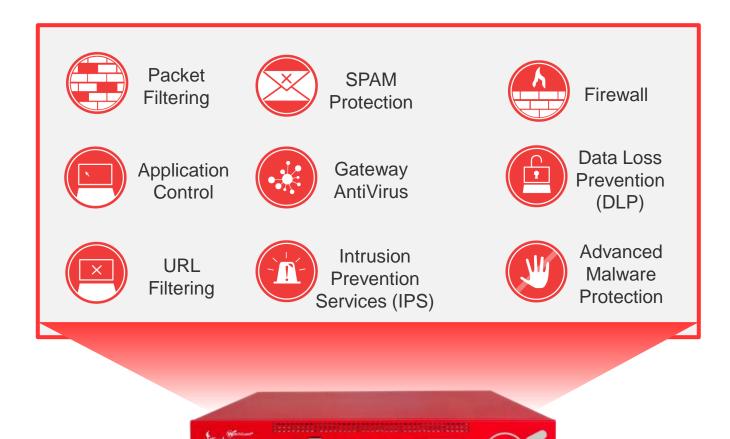
Risposta

Impostare i criteri per automaticamente inviare allarmi e / o rispondere alle minacce



IL VALORE DELL' UTM

La soluzione Unified Threat Management (UTM) Layered Security combina una varieta' di servizi di sicurezza indispensabili, in una soluzione facile da installare e gestire.



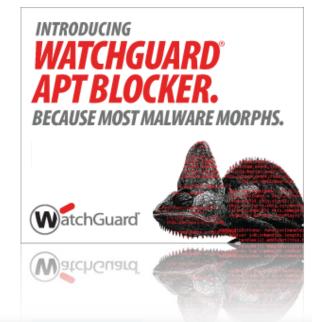
Meno Apparati.

Configurati solo la prima volta. Gestiti Centra mente ard



APT BLOCKER

- Identifica e sottopone file sospetti alla, next-generation, full system emulation sandbox nel cloud
- Fornisce la real-time threat visibility;
 protezione in minuti non ore
- Analizza un vasto insieme di tipi di file (Eseguibili, Doc Office, PDFs & Android APKs)
- Rileva lo Zero Day Malware
- Scalabile; ispeziona milioni di oggetti al giorno
- Not sensibile a tecniche di evasione



APT Malicious Act	ivity	
MD5	beaeaf220881d185b7fd1873bf87ed49	
Threat Level	HIGH	
MIME Type	application/x-pe-app-32bit	
Network	Command&Control traffic observed	•
Autostart	Registering for autostart during Windows boot	
Evasion	Trying to detect analysis virtual environment (HDD detection)	
Network	Using injected code to hide network activity (dns traffic)	
Steal	Reading user's mail server credentials	
Disable	Stopping the Windows Security Center service	
File	Modifying executable in user-shared data directory	
Memory	Writing to the memory of a non-child running process	
Settings	Modifying name server (DNS, DHCP) addresses	
Evasion	Possibly stalling against analysis environment (sleep)	
Evasion	Possibly stalling against analysis em	vironment (loop)

APT BLOCKER: SANDBOX VIRTUALE

Virtualizza il Sistema completo

Esegue I contenuti sconosciuti in un ambiente protetto

Analizza I comportamenti

Rileva tecniche di evasione dalla sandbox

Taccia malware addizionale e server C&C (command e control)



TDR - Threat Detection & Response!

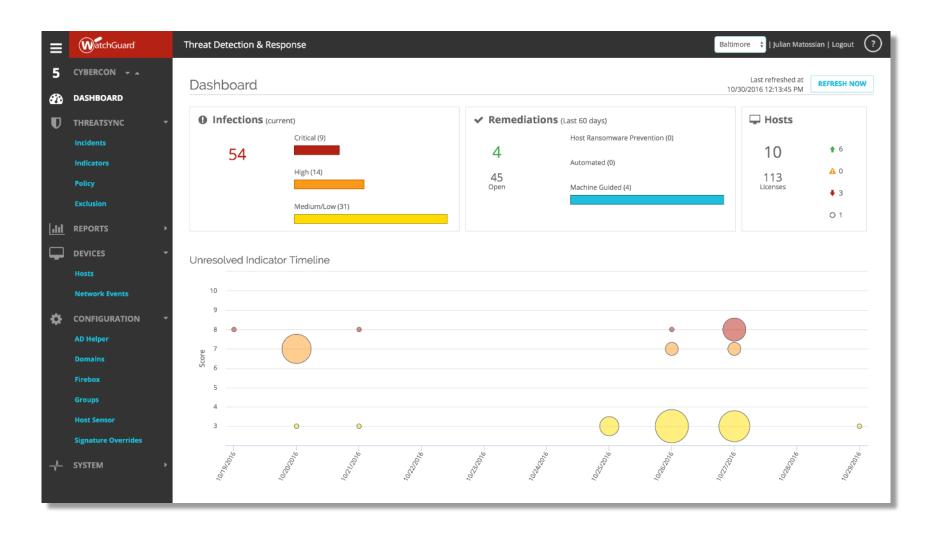
Threat Detection & Response: un'azione immediata contro minacce nuove o nascoste correlando eventi di sicurezza della rete e degli endpoint in una classifica di pericolosita'







INTERFACCIA INTUITIVA





NESSUN ALTRO LO FA!

UTM con capacità di correlazione completamente integrato - rilevamento delle minacce dalla rete all'endpoint in un'unica vista.

UTM per elaborare le informazioni sulle minacce per conto di clienti e partner, trasmettendo solo le prestazioni di sicurezza avanzata senza la complessità e costi.

UTM per fornire risposta agli incidenti automatica ed integrata che lavora in tandem con AV esistenti

UTM per unire prevenzione, l'individuazione, la correlazione e la risposta in un **unico prodotto**





COSA OFFRONO I COMPETITORS?







Product	TOTAL SECURITY			
Stateful Firewall	✓	\checkmark	\checkmark	\checkmark
Mobile VPN	✓	\checkmark	\checkmark	\checkmark
Branch Office VPN	✓	✓	✓	✓
Application Proxies	✓	\checkmark	\checkmark	\checkmark
IPS	✓	✓	✓	✓
App Control	✓	√	✓	✓
WebBlocker	✓	✓	✓	✓
spamBlocker	✓	\checkmark	\checkmark	\checkmark
Gateway AntiVirus	✓	✓	✓	\checkmark
RED	✓	√ *	✓	√ *
Network Discovery	✓			
APT Blocker	✓	✓	√ *	√ *
DLP	✓	\checkmark	\checkmark	\checkmark
Dimension Command	✓			
Threat Detection & Response	✓			
Support	Gold (24x7)			(WatchGuard

E DOPO L'UTM? **EPP TDR EDR** AV Personal Firewall Managed Hunting **Forensics** Anti-Virus Host IPS + Blocking **Advanced Heuristics** Behavioral Analysis Signatures & Threat Intell. Real Time Agent Scoring Host Isolation **Automated Response Network Integration** Correlation **Vulnerability Assessment Endpoint DLP** Disk Encryption Host Sandboxing

Chi fa Cosa?



EPP

Enterprise

KASPERSKY !!





SOPHOS

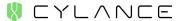






WEBROOT

Malware bytes





TDR

Vendere TDR come completamento di questi servizi

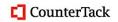
TDR non intende competere in questo spazio

EDR

Enterprise

CARBON BLACK











Per non rischiare:



CONTATTACI

055/456336 3397299492 marco.vannucci@progenit.it

