



(ALLEGATO N°2)

Informativa Protezione Dati GDPR

Informativa Protezione Dati - SOPHOS – GDPR 679/2017- Rev. 2k18.1

04 Giugno 2018

Sistemìa di Leone Stefano Fabio

P.IVA 03404430872

R.E.A. 0232517

Via F.Pensavalle,21 – 95128 Catania (Italy)

Tel. 095.7169500

Fax. 095.7286819

E-Mail: mbox@sistemìa.com

Web: www.sistemìa.com



Introduzione – GDPR 679/2017

Che cos'è?

Il Regolamento Generale sulla protezione dei dati (General Data Protection Regulation, GDPR) dell'UE incrementa i requisiti di protezione dei dati personali dei cittadini dell'UE.

Chi riguarda?

Tutte le organizzazioni in possesso di dati che possono portare all'identificazione personale di cittadini dell'UE (ad es. indirizzi e-mail, foto o informazioni cliniche).

Quali sono le tempistiche?

Termine ultimo: Maggio 2018 (anche se in diversi paesi l'implementazione è stata anticipata).

Quali sono i motivi di preoccupazione?

Sanzioni che possono raggiungere i 20 milioni di EUR o il 4% del fatturato annuo globale (a seconda di quale sia più elevato), in caso di violazione dei dati personali.

Violazioni dei dati

57% Quantità causata da hacker o malware.

23% Quantità causata da divulgazione non intenzionale.

2016 Data Breaches – Privacy Rights Clearinghouse

Bloccare le principali cause di perdita dei dati

Malware e hacker

Furto/smarrimento di un dispositivo

Bloccare le minacce alla soglia del perimetro di rete

Blocco degli attacchi volti al furto dei dati prima ancora che colpiscano la rete

Impedire gli errori umani

Sicurezza dei dati, anche all'esterno della rete/dei dispositivi



LE AZIENDE DEVONO

- + Proteggere i dati personali dei clienti da accessi non autorizzati (breach);
- + Istruire tutto il personale dipendente in merito alla nuova normativa;
- + Adottare una politica di governance e data protection adeguata in modo proporzionale al rischio in caso di breach;
- + Introdurre la figura del DPO, il Data Protection Officer, che può essere interno o esterno all'azienda a seconda dei casi;
- + Dotarsi di strumenti tecnologici necessari a monitorare e prevenire gli attacchi informatici.



COME MANTENERE LA GIUSTA PROTEZIONE CONTRO IL RANSOMWARE

Tutte le aziende, tanto quelle di grandi dimensioni quanto quelle più piccole, sono esposte a minacce provenienti da aggressivi e spietati attacchi di ransomware. L'impossibilità di accedere a file di vitale importanza, seguita dalla richiesta di pagamento, può causare enormi problemi di produttività per un'organizzazione.

Come si svolge un tipico attacco? E quali soluzioni occorre implementare per garantire la migliore protezione disponibile?

Questo documento analizza le tecniche più frequentemente utilizzate per inviare ransomware, analizza i motivi per cui questi attacchi vanno a segno, e offre nove consigli di sicurezza per aiutarvi a rimanere protetti. Inoltre, mette in luce le tecnologie di sicurezza essenziali, che dovrebbero essere incluse in qualsiasi sistema informatico.

Il ransomware: una breve introduzione

Il ransomware è una delle minacce più diffuse e più pericolose per gli utenti di Internet. Dalla prima comparsa del famigerato CryptoLocker nel 2013, si è notata una nuova epoca di varianti di ransomware che agiscono cifrando i file, e che si diffondono tramite messaggi di spam e kit di exploit, allo scopo di estorcere denaro sia dagli utenti privati che dalle aziende.

L'origine dell'attuale afflusso di famiglie di ransomware risale ai primissimi Fake AV, per poi passare alle varianti "Locker", e giungere infine alle specie che cifrano i file, che sono attualmente quelli più diffusi. Tutte le categorie di malware hanno un obiettivo comune: estorcere denaro alle vittime tramite persino attacchi intimidatori. Le richieste di denaro diventano sempre più minacciose con ciascuna iterazione.

E le conseguenze finanziarie possono essere disastrose. Secondo quanto riferito, l'Hollywood Presbyterian Medical Center avrebbe pagato 40 Bitcoin (\$17.000) per ottenere nuovamente accesso ai propri file, mentre il Kansas Heart Hospital, nonostante il versamento di una somma non divulgata, si sarebbe visto presentare una seconda richiesta di riscatto, senza ricevere accesso a tutti i file.

Perché gli attacchi di ransomware hanno un tasso di successo così elevato?

La maggior parte delle aziende adotta comunque qualche sistema di sicurezza IT. Ma allora perché esistono attacchi di ransomware che riescono a superare queste difese?

1. Tecniche di attacco sofisticate e costante innovazione

- I programmi di 'Malware as a Service' (MaaS) stanno diventando sempre più diffusi, semplificando l'avvio e il completamento di un attacco, e rendendone facile l'uso a scopo di lucro anche da parte di criminali dotati di competenze tecniche limitate. Quello che segue è un programma di MaaS disponibile per l'acquisto.



The image shows a screenshot of a webpage for 'RIG EXPLOIT KIT v3'. The page features a header with the product name, a price of \$499.00, and a 'Buy Now' button. Below the header, there are several sections: 'Description', 'Additional information', and 'Reviews'. The 'Description' section includes a list of features and a 'Why do we need to use exploit?' section. Annotations with arrows point to specific parts of the page:

- An annotation box on the right side of the page states: "Include tecniche per rate ed endpoint, dall'infezione di un sito web fino alla distribuzione di un payload per endpoint e alla vendita dei risultati." (Includes techniques for rate and endpoint, from the infection of a website to the distribution of a payload for endpoint and the sale of the results).
- An annotation box at the bottom right states: "Multiplatforma & con sviluppo agile." (Multiplatform & with agile development).
- An annotation box at the bottom right states: "Exploit inclusi automaticamente." (Exploits included automatically).



- Vengono adoperate tecniche predefinite per indurre l'utente a eseguire la routine di installazione del ransomware. Ad esempio, è possibile che la vittima riceva un'e-mail con le seguenti istruzioni:

"I requisiti della mia azienda sono elencati nel file in allegato, si prega cortesemente di inviare un preventivo".

- Gli autori del ransomware agiscono in maniera molto professionale. Possono, ad esempio, proporre uno strumento di decifratura funzionante, che inviano dopo aver ricevuto il pagamento del riscatto.

2. Falle nei sistemi di sicurezza delle aziende coinvolte

- Strategie di backup inadeguate (nessun backup in tempo reale, backup non off-line/off-site).
- Aggiornamenti e patch per sistemi operativi e applicazioni non vengono implementati con la dovuta tempestività.
- Utenti pericolosi/autorizzazioni con troppi diritti (gli utenti sono amministratori e/o possiedono più file nelle unità di rete di quanto realmente necessario per lo svolgimento del proprio lavoro).
- Mancanza di formazione sulla sicurezza ("Quali documenti posso aprire, e da chi devono provenire?", "Qual è la procedura da seguire quando un documento sembra avere un aspetto malevolo?", "Come posso fare per riconoscere le e-mail di phishing?").
- Sistemi di sicurezza (scansioni antivirus, firewall, IPS, gateway di posta/web) non implementati, oppure non configurati correttamente. Anche un'inadeguata segmentazione della rete può essere inclusa in questo elenco (server e workstation nella stessa rete).
- Mancanza di conoscenze tecniche sulla sicurezza informatica da parte degli amministratori (è possibile che per le e-mail siano stati bloccati i file .exe, ma non le macro di Office o altri contenuti attivi).
- Conflitto di priorità ("Sappiamo che questo metodo non è sicuro, ma i dipendenti devono pur lavorare...").

3. Mancanza di tecnologie di prevenzione avanzate

- Molte aziende adottano soluzioni di protezione generica.
- Il ransomware subisce aggiornamenti costanti, mirati a colpire ed eludere questo tipo di protezione.

Ad esempio, dopo aver cifrato i file, si eliminano automaticamente con una rapidità tale che ne impedisce l'analisi.

- Le soluzioni devono essere realizzate appositamente per poter contrastare le tecniche adottate dal ransomware.

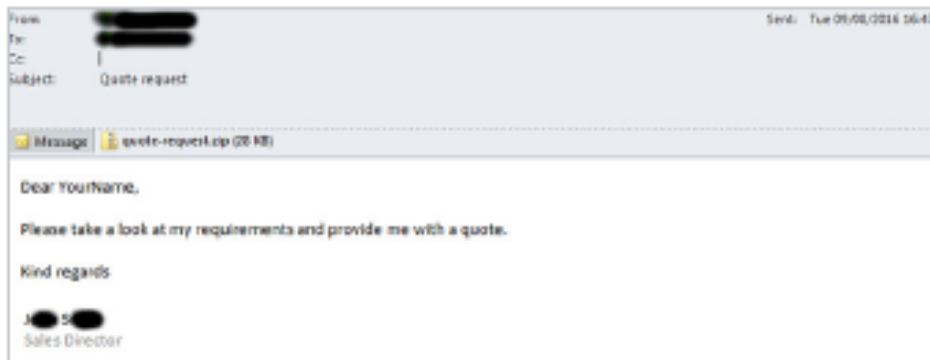


Come avviene un attacco di ransomware?

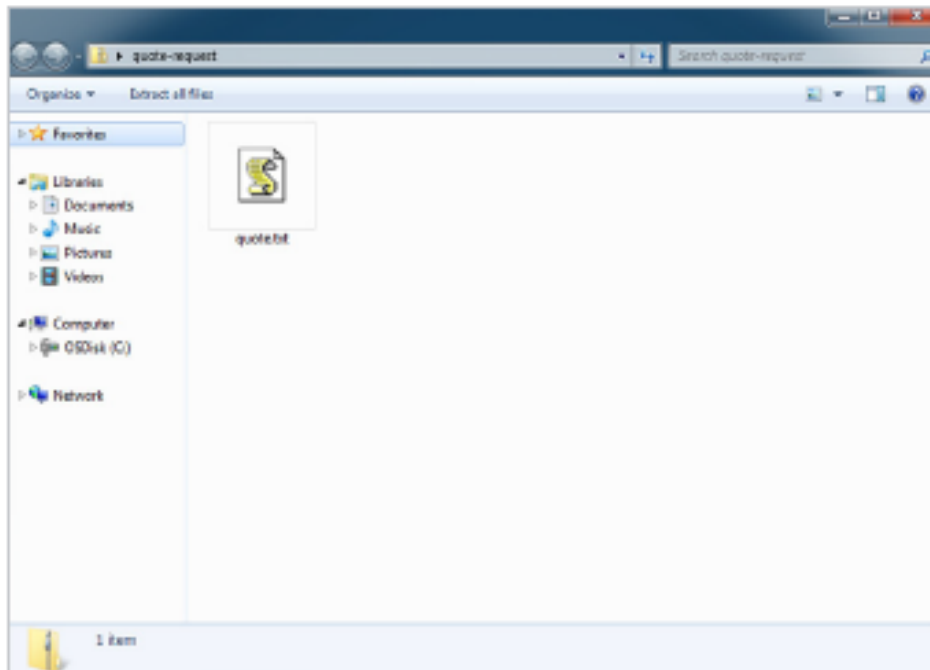
Gli attacchi di ransomware possono cominciare principalmente in due modi. Tramite messaggio e-mail contenente un allegato malevolo, oppure visitando un sito web compromesso (spesso legittimo e importante).

E-mail malevole

Oggi come oggi i criminali creano messaggi e-mail che è impossibile distinguere da quelli "buoni". Grammaticalmente corretti, senza errori di battitura, e spesso scritti in maniera da essere pertinenti a voi o alla vostra azienda.



Una volta aperto, il file zip sembra contenere un normale file .txt.



Tuttavia, quando si esegue il file, viene scaricato il ransomware, che si installa nel computer. In questo esempio, il trojan è in realtà un file JavaScript camuffato da file .txt, ma sono presenti moltissime variazioni dell'approccio e-mail, come ad es. documenti Word con macro e file di collegamento (.lnk).



Siti web malevoli

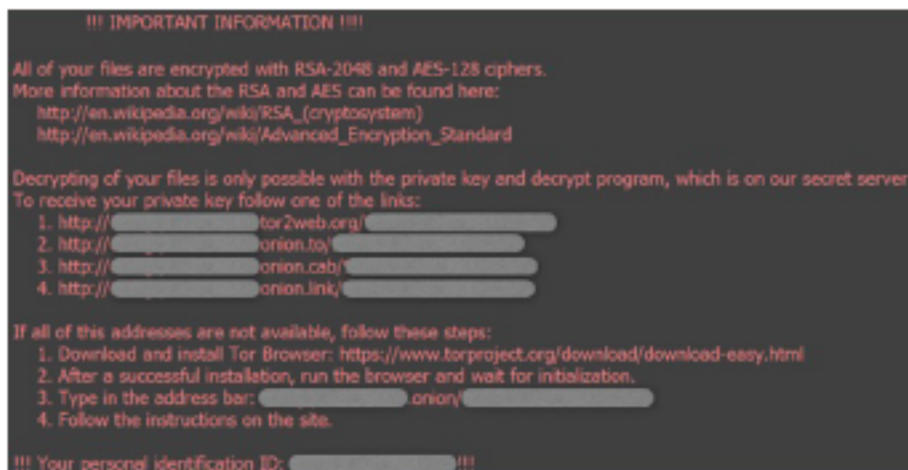
Un altro modo tipico in cui si può cadere vittima di un attacco è visitando un sito web legittimo che è stato infettato da un kit di exploit. Anche i siti web più famosi e importanti possono venire temporaneamente compromessi. I kit di exploit sono strumenti disponibili sul mercato nero che vengono utilizzati dagli hacker per sfruttare vulnerabilità note o sconosciute (ad es. exploit del giorno zero).

Si visita il sito compromesso, si clicca su un link dall'aspetto innocuo, ci si passa sopra il mouse, o a volte ci si limita soltanto a guardare la pagina. E ciò basta per scaricare ed eseguire il file di ransomware sul computer, spesso senza alcun indizio prima che il danno sia ormai compiuto.

E dopo?

Dopo l'esposizione iniziale, ad es. tramite e-mail e web come indicato negli esempi, il ransomware procede con le sue azioni:

- Contatta il server di comando e controllo dell'autore dell'attacco, inviando informazioni sul computer infettato e scaricando una chiave pubblica individuale per il suddetto computer.
- Alcuni tipi di file specifici (che variano a seconda del tipo di ransomware), come ad es. documenti Office, file di database, PDF, documenti CAD, HTML, XML, ecc., vengono cifrati su computer locale, dispositivi mobili e tutte le unità di rete accessibili.
- Spesso vengono eliminati anche i backup automatici del sistema operativo Windows (copie shadow), per impedire le attività di recupero dei dati.
- Viene quindi visualizzato un messaggio sul desktop che indica come effettuare il pagamento del riscatto (ransom), solitamente in Bitcoin, entro un limite di tempo specifico.



- Infine, il ransomware si elimina automaticamente, lasciandosi alle spalle solamente i file cifrati e la nota di riscatto.



Epidemia di ransomware Wanna DecryptOr 2.0

Wanna (noto anche come WannaCry, WCry, WanaCrypt, WanaCryptOr e Wana DeCryptOr) è un ransomware a rapida diffusione che ha cominciato a generare scompiglio il 12 maggio 2017.

Le analisi sembrano aver confermato che l'attacco è stato lanciato utilizzando codice NSA sospetto, finito in mano a un gruppo di hacker noto come Shadow Brokers. Adopera una variante dell'exploit ShadowBrokers APT EternalBlue (CC-1353), cifrando in maniera impenetrabile vari tipi di file, inclusi documenti, immagini e video.

A differenza di altri attacchi, Wanna è stato in grado di sfruttare una vulnerabilità del codice di esecuzione remota (Remote Code Execution, RCE) che gli ha consentito di infettare computer privi di patch senza alcuna interazione da parte degli utenti. Questo stratagemma ha permesso a Wanna di diffondersi rapidamente, in maniera analoga a quella osservata una decina di anni fa durante le epidemie di worm quali Slammer e Conficker.

La vulnerabilità dell'RCE vittima dell'exploit era un difetto del servizio Windows Server Message Block (SMB), che viene utilizzato dal computer Windows per condividere file e stampanti sulle reti locali. Microsoft ha risolto questa vulnerabilità con il bollettino MS17-010 a marzo 2017, ma i sistemi che non avevano installato l'aggiornamento o che eseguivano versioni di Windows obsolete e non più supportate erano rimasti vulnerabili.

Per contrastare l'epidemia, Microsoft ha adottato una misura straordinaria, rilasciando l'aggiornamento di sicurezza per le piattaforme in supporto personalizzato (come ad es. Windows XP) e mettendolo a disposizione di tutti. Si consiglia vivamente di installare questo aggiornamento il prima possibile.

Per ulteriori informazioni consultare il seguente articolo della knowledgebase di Sophos: www.sophos.com/kb/126733

Nove regole di sicurezza

Difendersi dal ransomware non significa solamente avere a disposizione le soluzioni di sicurezza più moderne. Anche ottime di sicurezza IT, che includano corsi di formazione regolari per i dipendenti, sono elementi essenziali per qualsiasi sistema di sicurezza. Accertatevi di seguire le seguenti nove regole di sicurezza:

1. Effettuare backup frequentemente, e conservare una copia off-line e off-site di un backup recente

Vi sono decine di modi diversi, oltre al ransomware, in cui si rischia improvvisamente di perdere i file, ad es: incendi, allagamenti, furto, laptop caduti per terra, o persino eliminazione involontaria. Se il backup viene cifrato, si eviterà il rischio che il dispositivo di backup finisca nelle mani sbagliate.

2. Abilitare le estensioni dei file

Per impostazione predefinita, Windows disattiva le estensioni dei file, il che significa che per identificarli ci si basa sull'icona del file. Abilitando le estensioni, diventa molto più facile individuare i tipi di file che non verrebbero normalmente inviati da voi o dai vostri utenti, come ad es. JavaScript.

3. Aprire i file JavaScript (.JS) nel Blocco note

Aprendo un file JavaScript nel Blocco note, è possibile prevenire l'esecuzione di eventuali script malevoli e analizzare i contenuti del file.

4. Non abilitare le macro nei documenti ricevuti come allegato e-mail

Microsoft ha deliberatamente disattivato l'esecuzione automatica delle macro per impostazione predefinita diversi anni fa, come misura di sicurezza. Molte infezioni cercano di persuadere gli utenti a riattivare le macro, per cui non fatele!



5. Prestare la dovuta cautela quando si ricevono allegati non richiesti

I malintenzionati giocano molto sul dilemma del dover evitare di aprire un documento se non si è sicuri che sia quello giusto, ma del non sapere se sia il documento giusto sino a quando non lo si apre. In caso di dubbio, meglio lasciar perdere.

6. Non concedersi diritti di accesso superiori a quelli effettivamente richiesti

Evitare di mantenere attivo l'accesso con privilegi di amministrazione per più tempo di quanto strettamente necessario, ed evitare di navigare, aprire documenti, o svolgere altre "normali attività lavorative" con diritti di amministrazione.

7. Prendere in considerazione l'installazione di visualizzatori Microsoft Office

Queste applicazioni consentono di visualizzare i contenuti dei documenti senza aprirli in Word o Excel. Inoltre, i software di visualizzazione non supportano le macro, per cui non vi è il rischio di abilitarle per errore!

8. Applicare le patch presto, spesso e volentieri

Spesso il malware che non si diffonde tramite documenti approfitta del bug di sicurezza delle applicazioni più comunemente usate, inclusi Office, Flash, browser, e altri. Prima si applicano le patch, meno falle di sicurezza restano disponibili per gli exploit.

9. Rimanere aggiornati sulle nuove funzionalità di sicurezza presenti nelle applicazioni aziendali

Ad esempio, Office 2016 include ora un'opzione che si chiama "Blocca l'esecuzione delle macro nei file di Office provenienti da Internet", e che serve a proteggere il sistema contro contenuti esterni malevoli, senza impedire l'uso interno delle macro.



Tecnologie di sicurezza che aiutano a mantenersi protetti contro il ransomware

Per bloccare il ransomware, occorre implementare una protezione che sia avanzata ed efficace in tutte le fasi di attacco.

Protezione degli endpoint

Intercept X si serve dell'esclusiva tecnologia CryptoGuard per stroncare sul nascere qualsiasi attacco di ransomware. Agisce rilevando il ransomware, inclusa la recente epidemia di ransomware Wanna, e impedendone l'azione di cifratura dei file. Intercept X può essere utilizzata insieme alla soluzione di sicurezza attuale, per bloccare i processi che cercano di effettuare modifiche non autorizzate dei dati.

Blocco delle minacce e-mail

La principale difesa contro e-mail piene di trappole è il gateway di posta. Le tecnologie antispam bloccano le e-mail di ransomware, mentre le scansioni antivirus individuano e bloccano le minacce in circolazione. Bloccare le e-mail contenenti allegati macro può aiutarvi a evitare un'altra comunissima tecnica di ransomware. La tecnologia Time-of-Click impedisce a voi e ai vostri utenti di cliccare sugli elementi di un sito infetto – anche se magari era sicuro nel momento in cui l'e-mail è giunta nella vostra casella di posta.

Blocco delle minacce e-mail

Le minacce web vengono neutralizzate a livello di firewall e gateway web. Il filtraggio degli URL blocca sia i siti che ospitano ransomware, che i loro server di comando e controllo. Inoltre, implementando controlli severi, è possibile persino impedire il download dei file associati al malware.

Il sandboxing nel cloud sia a livello di gateway di posta che web, blocca le minacce avanzate del giorno zero, incluso il ransomware. È come avere a disposizione un laboratorio antimailware personale, che esegue i file sospetti per determinarne il comportamento.

Protezione dei server

Il whitelisting e il lockdown dei server mantengono i server protetti, in quanto inseriscono in una whitelist le applicazioni autorizzate, identificando gli elementi che queste ultime possono modificare e aggiornare; qualsiasi altro tentativo di effettuare modifiche viene automaticamente bloccato, impedendo al ransomware di entrare in azione. Il rilevamento del traffico malevolo impedisce al ransomware di contattare i server di comando e controllo e di scaricarne il payload. Sophos Server Protection include anche la tecnologia CryptoGuard, che impedisce al ransomware di cifrare i file.

Security Heartbeat

Individualmente, i singoli prodotti di sicurezza sono straordinari, ma lo sono ancora di più quando interagiscono l'uno con l'altro. Abilitando la condivisione di informazioni di sicurezza tra endpoint e firewall, e rispondendo in maniera proattiva alle minacce, potrete contare su una protezione senza eguali contro le minacce avanzate.



Una strategia di protezione dei dati a prova di bomba

I dati sono tutto

1. Come avviene il processo di entrata e uscita dei dati nella vostra azienda?
2. Come vengono utilizzati i dati dagli utenti finali?
3. Chi ha diritto di accedere ai dati aziendali?





Prevenzione delle violazioni

5 passi per evitare che i dati finiscano nelle mani sbagliate

- 1. Mantenere aggiornate le patch**
Spesso il malware per il furto di dati sfrutta vulnerabilità già note.
- 2. Applicare una protezione a strati multipli sui punti di accesso**
Difesa contro vettori di attacco multipli mediante protezione Web, E-mail e Antimalware a livello di gateway.
- 3. Utilizzare la Protezione avanzata contro le minacce (ATP)**
Scegliere un next-generation firewall che rilevi e blocchi gli attacchi direttamente sulla rete.
- 4. Adoperare il Sandboxing selettivo**
Per la protezione contro minacce lente o "a scoppio ritardato".
- 5. Limitare la divulgazione dei dati di natura sensibile**
Utilizzare Application Control e Data Control



Come garantire la conformità al Regolamento

La chiave è la cifratura

Il Regolamento imporrà alle organizzazioni di:

1. Implementare "adeguate misure di sicurezza" per proteggere i dati personali

→ La cifratura viene generalmente considerata la migliore misura di sicurezza dei dati disponibile

2. Avvertire i diretti interessati in caso di violazione dei dati personali

→ Se si è in grado di dimostrare che i dati erano cifrati, non vi è l'obbligo di avvisare i diretti interessati

3. Essere sottoposte a sanzioni in caso di violazione dei dati personali

→ Se i dati erano cifrati, è molto probabile che non venga imposta alcuna sanzione

Ma cosa, dove e quando cifrare?



Dispositivi smarriti o rubati



Non cifrato



Cifrato



- I dispositivi accidentalmente smarriti o rubati sono una situazione comune.
- Solamente gli utenti autorizzati devono poter accedere ai dispositivi.
- Quanti dispositivi avete smarrito?



Copia dei file sui supporti rimovibili



- Pur essendo piccolissimi, questi dispositivi possono contenere quantità enormi di dati ed essere facilmente smarriti.
- Vietare o proteggere?
- Dove si trova ora e cosa conteneva la vostra prima chiavetta USB?

Copia dei file su una condivisione di rete



- I moderni sistemi operativi semplificano notevolmente la condivisione dei dati in rete.
- Protezione contro le minacce interne.
- Chi è autorizzato ad accedere ai dati aziendali/degli utenti?

Copia dei file in-the-cloud



- I servizi di Cloud storage hanno rivoluzionato il modo in cui i dati vengono condivisi fra utenti e dispositivi.
- Che cosa avete salvato nel Cloud, e cosa accadrebbe se qualcuno se ne appropriasse illecitamente?
- Cifrare i dati prima di caricarli nel Cloud.



Sistemìa vi può aiutare, ecco come

Le nostre pluripremiate soluzioni di cifratura costituiscono **adequate misure di sicurezza** per la protezione dei dati personali

SafeGuard Enterprise Encryption

- Cifra i dati su dispositivi e sistemi operativi multipli
- Non è d'impaccio – è realizzata per adattarsi al flusso di lavoro e ai processi della vostra azienda
- Include la gestione centralizzata di Microsoft BitLocker e Apple FileVault
- Offre numerose opzioni di reportistica, per fornire prove di conformità alle normative

SafeGuard garantisce la protezione dei dati personali in caso di violazione





SPX Email Encryption

- Una soluzione di cifratura delle e-mail e di DLP che protegge la privacy, la riservatezza e l'integrità delle vostre e-mail di natura sensibile.
- Rileva automaticamente le informazioni sensibili che lasciano il perimetro di rete aziendale tramite e-mail, bloccandole o cifrandole
- Solleva i dipendenti dalla responsabilità di gestire la sicurezza, occupandosene per conto loro.
- Disponibile in **Sophos UTM** e nella **Sophos Email Appliance**



Possiamo aiutarvi a creare un
criterio di protezione dei dati

E possiamo aiutarvi a
**bloccare sul nascere i tentativi di
violazione**



Protezione contro hacker e perdita accidentale

Sophos Endpoint Protection

- Patch Assessment, per individuare e attribuire priorità alle patch mancanti
- Application Control
- Data Control
- Funzionalità avanzate di protezione Web

Sophos UTM

- Funzionalità di protezione avanzata contro le minacce (ATP)
- Sandboxing selettivo
- Funzionalità avanzate di protezione Web
- SPX Email Encryption (opzionale)





PHISHING: NON ABBOCCATE ALL'AMMO

Il phishing si verifica quando gli hacker inviano e-mail malevole allo scopo di prelevare illecitamente i dati personali di un utente (ad es. la password del laptop).

Prestate attenzione a questi comuni indizi che denotano la presenza di phishing, ed evitate di cadere nella trappola:

- Insistenza forzata/simulata, per sollecitare una risposta prima che abbiate tempo per pensare
- Offerta di un premio o una ricompensa, per indurvi a cliccare su un link
- Richiesta di fornire una password o altri dati di natura riservata, per motivi di sicurezza
- Indirizzi web simili, ma non identici, a quelli autentici, ad es.
www.g00gle.com anziché www.google.com
www.twiter.com anziché www.twitter.com
- Uso di link "mascherati" che hanno l'aspetto di essere siti web attendibili, ma che portano a una pagina diversa una volta aperti
 - Consiglio pratico: passando il mouse sul link, viene visualizzato l'indirizzo effettivo
- E-mail che sembrano provenire da uno dei dirigenti della vostra azienda
- Errori grammaticali/di battitura

LE VOSTRE PASSWORD SI MERITANO IL RED CARPET

La password rappresenta la vostra prima linea di difesa contro gli hacker. Non dimenticate di dedicarle l'attenzione che merita.

PASSWORD SICURE

Contengono un minimo di 14 caratteri

Sono una frase, e non una singola parola, ad es: "AdØro qVest4 P4sswØrd!"

Contengono sia lettere maiuscole che minuscole e caratteri di punteggiatura

Non sono singole parole in qualsiasi lingua, gergo o dialetto

Non si basano su informazioni di natura personale, nomi di parenti, ecc.

PASSWORD DEBOLI

Contengono meno di 10 caratteri

Si trovano in un dizionario (di qualsiasi lingua)

Sono prevedibili: nomi di parenti, animali domestici, amici, compleanni, ecc.

Utilizzano parole o serie di numeri (no alla sequenza di Fibonacci!)

SOCIAL MEDIA SICURI



I social media sono un ottimo strumento per mantenersi in contatto con amici e parenti. Ma non dimenticate che niente rimane veramente privato, per cui vi invitiamo a seguire questi consigli pratici:

- Se non lo direste di persona, non ditelo on-line
- Non pubblicate alcuna informazione relativa al vostro lavoro o alcun dato personale di natura sensibile
- Modificate le impostazioni sulla privacy in modo da selezionare le opzioni più sicure, per essere sicuri che solamente chi conoscete bene e gode della vostra fiducia possa visualizzare quello che pubblicate
- Chiudete la sessione una volta che avete finito (se doveste smarrire il dispositivo, per lo meno i vostri account non saranno facilmente accessibili)
- Utilizzate password diverse per ciascun account (ad es. Facebook, Twitter)



La storia	
Bloccare le principali cause di perdita dei dati Malware e hacker Furto/smarrimento di un dispositivo Bloccare le minacce alla soglia del perimetro di rete Blocco degli attacchi volti al furto dei dati prima ancora che colpiscano la rete Impedire gli errori umani Sicurezza dei dati, anche all'esterno della rete/dei dispositivi	Prodotti disponibili per la vendita Quando proporre questa soluzione: opportunità iniziale. È essenziale per tutti Central Device Encryption, Central Mobile, Intercept X Central Device Encryption e Central Mobile mantengono protetti i dati situati nel dispositivo in caso di furto/smarrimento. Intercept X blocca il malware volto al furto dei dati. Quando proporre questa soluzione: alto interesse iniziale/cross-selling in un secondo momento XG Firewall, Sophos Email Appliance XG Firewall protegge i dispositivi di rete bloccando ai limiti del perimetro di rete gli attacchi volti al furto dei dati. SEA blocca le e-mail sospette prima che possano raggiungere gli utenti; inoltre, è in grado di bloccare o cifrare e-mail e allegati di natura sensibile. Quando proporre questa soluzione: il cliente cerca una soluzione completa SafeGuard La cifratura a livello dei singoli file protegge i dati ovunque si trovino: nel cloud, oppure all'esterno di dispositivi o rete.

SOPHOS

Copyright © 2017 Sophos Ltd. Tutti i diritti riservati.



INTERCEPT – Soluzione Anti-Ransomware & Minacce Zero Day





Le minacce sono sconosciute e quindi più difficili da individuare

400.000

I SophosLabs ricevono ed elaborano
400.000 campioni al giorno di
malware precedentemente inedito.



Il **75%** dei file malevoli rilevati
dai SophosLabs proviene da
un'unica organizzazione.



Fonte: SophosLabs

La protezione endpoint è sempre più completa



**PROTEZIONE
CONTRO L'IGNOTO**



**BLOCCO DEL
RANSOMWARE**



**BLOCCO DEI
CYBERCRIMINALI**

SOPHOS

Funzionalità del rilevamento antimalware con tecnologie di Deep Learning di Sophos

- Prevenzione sia del malware complesso che di quello inedito
- Blocco del malware prima che riesca a eseguirsi
- Rilevamento indipendente dalle firme
- Classificazione dei file come malevoli, app potenzialmente indesiderate (PUA) o innocui
- Impatto minimo (meno di 20 MB) con aggiornamenti poco frequenti
- Rilevamento del malware in circa 20 millisecondi
- Protezione anche in caso di host off-line
- Subito pronto per l'uso, senza bisogno di ulteriore training



SOPHOS

Il Deep Learning rispetto ad altri tipi di Machine Learning



Modello più intelligente



Più scalabile

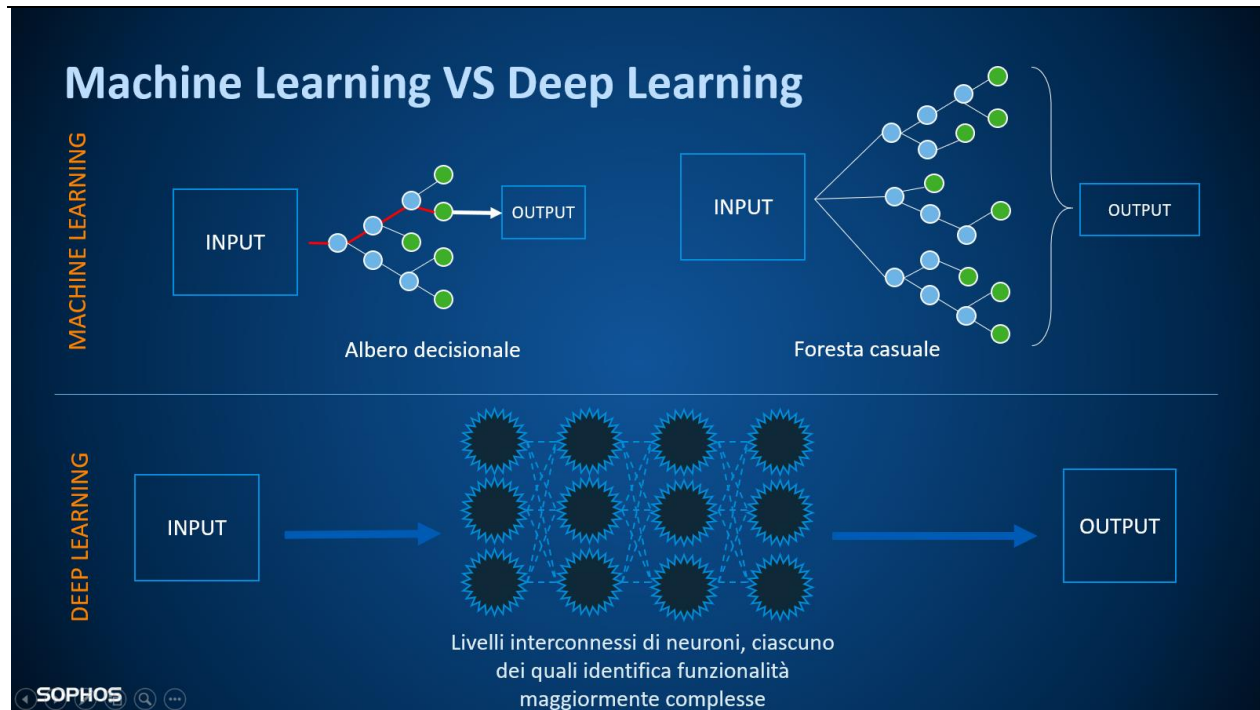


Impatto più leggero

“Intercept X sfrutta una rete neurale di Deep Learning che agisce in maniera simile al cervello umano... I risultati sono un migliore tasso di precisione sia per il malware attuale che per quello del giorno zero, nonché una percentuale minore di falsi positivi.”

- ESG Lab Report, dicembre 2017

SOPHOS



I vantaggi del Deep Learning di Sophos

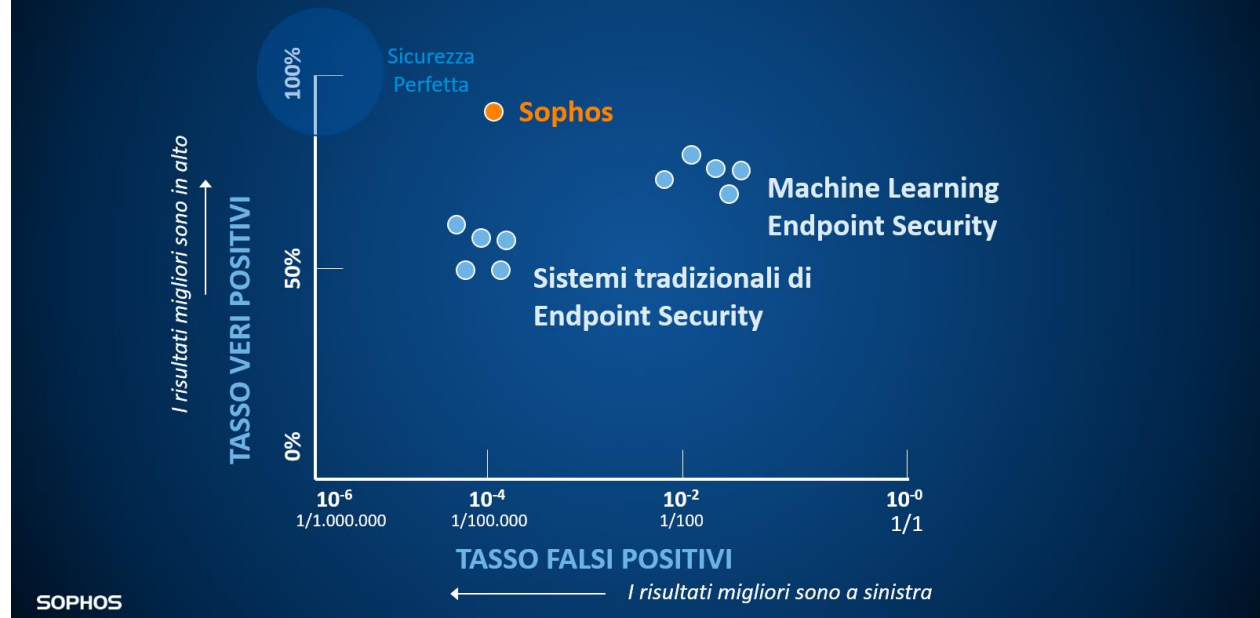
- **Affidabile**
 - Il miglior tasso di rilevamento antimalware del settore
 - Efficacia comprovata da VirusTotal fin da agosto 2016, con una recensione imparziale
- **Performance**
 - Blocco del malware inedito, indipendentemente dalle firme
 - Rilevamento e blocco delle minacce nel giro di 20 millisecondi
- **Esperienza**
 - Sviluppo cominciato nel 2010
 - Realizzato dagli esperti di data science dei SophosLabs, con tecnologia DARPA
- **SophosLabs**: Training basato su centinaia di milioni di campioni

“ Uno dei **migliori punteggi in termini di performance** che abbiamo mai osservato nei nostri test ”

Maik Morgenstern, CTO, AV-TEST



Sicurezza predittiva: rilevamento del malware inedito



Viviamo all'ombra del ransomware

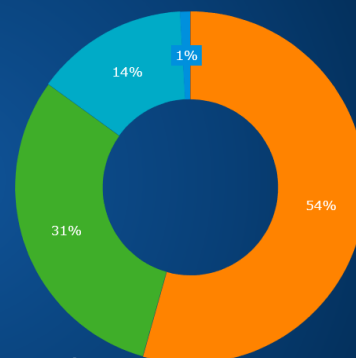
La vostra organizzazione è stata colpita dal ransomware?

54%

Percentuale di organizzazioni colpita dal ransomware negli ultimi 12 mesi

85%

Percentuale di organizzazioni che sono state colpite o che prevedono saranno colpite dal ransomware



- Sì
- No, ma prevediamo che accadrà in futuro
- No e non pensiamo possa accadere
- Non lo so

Fonte: sondaggio sullo stato attuale della sicurezza endpoint

SOPHOS



Il ransomware in breve

2

Media degli attacchi di ransomware tra le vittime[^]

77%

Vittime di ransomware che utilizzano sistemi di protezione endpoint aggiornati[^]

2.500 \$

Media dei pagamenti per il ransomware^{*}

133 mila \$

Costo medio di un attacco di ransomware[^] (USD)

[^]Fonte: sondaggio sullo stato attuale della sicurezza endpoint

^{*} Fonte: Ponemon Institute



Protezione antiransomware basata sul comportamento



CryptoGuard: protezione dei file

- Effettua copie cache just-in-time dei file
- Identifica comportamenti relativi alla cifratura malevola dei file
- Isola i processi malevoli
- Ripristina automaticamente allo stato originale i file colpiti

WipeGuard: protezione del disco e dell'avvio

- Previene il sabotaggio malevolo delle aree di sistema del disco
- Blocca i processi malevoli
- Efficacia comprovata contro NotPetya

SOPHOS



I vantaggi dell'antiransomware Intercept X

Massima efficacia

- Individuazione basata sul comportamento
- Blocco della cifratura non autorizzata
- Rilevamento di file, dischi e ransomware di avvio
- Preparazione dei sistemi per le sfide del futuro, con protezione contro le nuove varianti

Ripristino automatico

- Ripristino a uno stato conosciuto
- Tecnologia proprietaria con snapshot
- Sicurezza e produttività degli utenti finali

Analisi della catena di attacco

- Identificazione del punto di origine
- Mappatura visiva di livello forense
- Cattura tutti i file attaccati



È essenziale bloccare gli attacchi indipendenti dai file e gli exploit

- Le funzionalità antiexploit di Intercept X bloccano sia gli attacchi basati sull'invio di file eseguibili malevoli prima che possano essere distribuiti, che gli attacchi che non inviano malware
- I file eseguibili malevoli ammontano solamente al 41% del malware che viene inviato a un endpoint[^]
- Molte tecniche non richiedono un file per poter raggiungere la memoria del computer
- Il 26% degli attacchi basati sul malware utilizza file di Office come armi

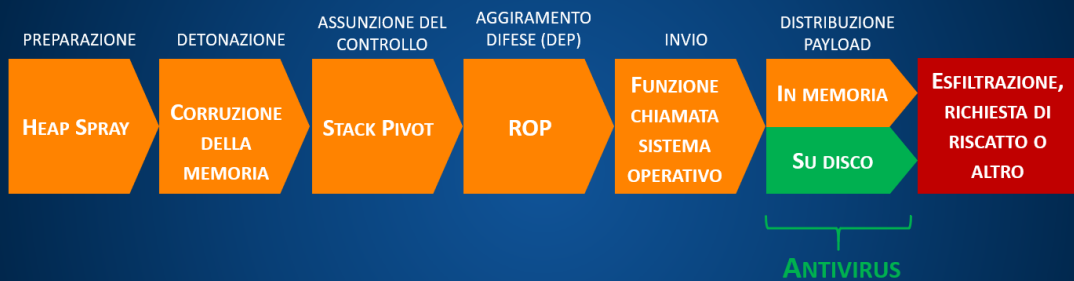
[^]In base alle segnalazioni di VirusTotal (31/12/17 – 06/01/18)

* Verizon Data Breach Investigations Report 2017





La catena di attacco



- La maggior parte degli attacchi basati sugli exploit fa uso di 2 o più tecniche
- Le tecniche di exploit non cambiano e sono passaggi obbligatori per poter sfruttare vulnerabilità dei software già esistenti e future
- Bloccare gli exploit significa bloccare l'attacco

SOPHOS

Tecniche degli hacker per gli active adversary



SOPHOS

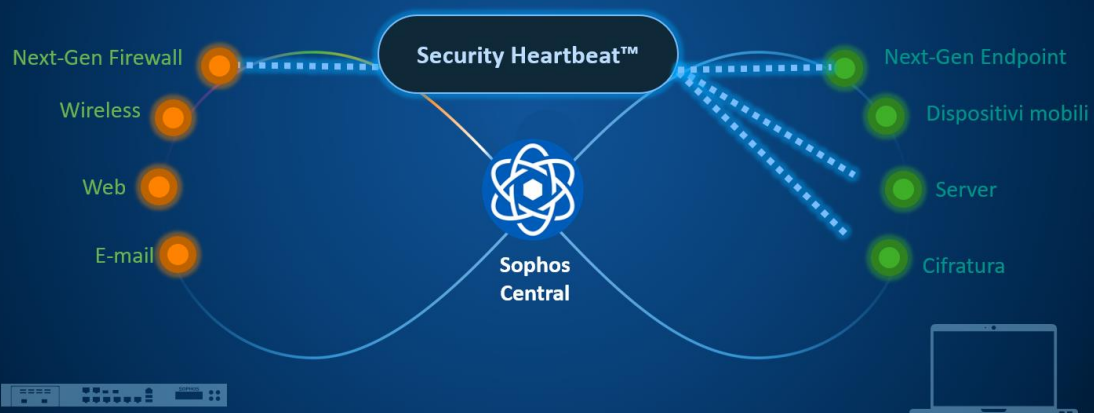


Alcune delle tecniche di exploit e active adversary bloccate da Intercept X

Implementazione della Protezione esecuzione programmi (DEP)	Uso obbligatorio di ASLR (Address Space Layout Randomization)	ASLR dal basso verso l'alto	Null page dereference	Allocazione di disseminazione nell'heap	Dynamic Heap Spray	Stack pivot e stack exec (protezione della memoria)
Attacchi ROP basati su stack (chiamante)	Protezione strutturata contro la sovrascrittura del gestore eccezioni (Structured Exception Handler Overwrite Protection, SEHOP)	Filtraggio importazione della tabella indirizzi (Import Address Table Filtering, IAF)	Libreria di caricamento	Reflective DLL Injection	Shellcode malevolo	VBScript God Mode
WOW64	Syscall	Hollow Process	DLL Hijacking	Squiblydoo AppLocker Bypass	Protezione contro le APC (Double Pulsar / Atom Bombing)	Privilege escalation dei processi
	Protezione contro il furto di credenziali	Mitigazione di code cave	Protezione contro MITB (navigazione sicura)	Rilevamento del traffico malevolo	Rilevamento shell Meterpreter	

SOPHOS

Sophos Synchronized Security



SOPHOS

Sophos Synchronized Security

Condivisione dei dati di intelligence in tempo reale tra endpoint e firewall

“**Nessun'altra azienda** riesce neppure ad avvicinarsi a questo livello di comunicazione tra **endpoint e prodotti di sicurezza della rete**”

Chris Christianson, Vice President di Security Programs, **IDC**



Sophos Central

Gestione di diversi prodotti
Sophos da un'unica
dashboard



SOPHOS



SOPHOS INTERCEPT X: IL POTERE DEL PIÙ



SOPHOS

La migliore protezione endpoint in assoluto

Blocco delle minacce sconosciute con il Deep Learning

Rilevamento di malware nuovo e ignoto con il Machine Learning avanzato

Prevenzione antiransomware con CryptoGuard

Blocco del ransomware e ripristino dei file a uno stato sicuro

Blocco degli autori degli attacchi con la prevenzione antiexploit

Blocco delle tecniche di exploit utilizzate dagli hacker durante i loro attacchi

“ Uno dei **migliori punteggi in termini di performance** che siano mai stati raggiunti nei nostri test. ”
Maik Morgenstern, CTO, AV-TEST

“ Intercept X ha bloccato **tutti gli attacchi di ransomware** dei nostri test nel giro di pochi secondi. ”
ESG Labs

“ Intercept X ha bloccato tutti gli attacchi complessi e avanzati che le abbiamo lanciato contro. ”
ESG Labs

SOPHOS



Livelli di difesa multipli: esempio di ransomware



“Installare Sophos Intercept X insieme a prodotti di protezione endpoint già esistenti è un processo semplice ed efficace. Abbiamo notato che blocca più rapidamente le minacce, offrendo un’analisi semplice e comprensibile degli attacchi.”

- Bob Appleby, Partner, PA, Computer Connections

SOPHOS



IN BREVE



EU General Data Protection Regulation [GDPR] – Reference Card

The EU GDPR will be enforced from 25 May 2018, and it is the culmination of years of work by the EU to reform Data Protection regulation into a Union-wide framework instead of a patchwork of country-specific legislations. The GDPR affects all organizations that hold personal data on EU citizens, regardless of where the organization is based in the world. The maximum fines for non-compliance are the higher of €20m and 4% of the organization's worldwide turnover.

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
Stop the top causes of data loss		
Stop malware and ransomware	 Intercept X	Keeps your endpoints secure from the latest malware and ransomware.
Keep your data secure if devices are lost or stolen	 Sophos Central Device Encryption	The easiest way to manage full disk encryption on PCs and Macs that secures your devices so data on the disk is always safe even if lost or stolen.
	 Sophos Mobile	Protects data on mobile devices and includes comprehensive anti-theft and loss prevention.
Stop threats at network perimeter		
Stop data-stealing attacks at your network perimeter	 XG Firewall	Synchronized Security working with endpoint protection to automatically identify and isolate compromised systems.
Automatically encrypt or block sensitive data in emails	 Secure Email Appliance Gateway	Automatically blocks malicious emails and encrypts sensitive email attachments.



EU General Data Protection Regulation [GDPR] – Reference Card

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
Stop human error		
Keep individual files secure wherever they go	 SafeGuard Encryption	Next-gen file encryption keeps your data safe even when it leaves your corporate network and devices.
Protect sensitive data in the cloud	 SafeGuard Encryption	Automatically and seamlessly encrypt and decrypt files as they are uploaded or downloaded from public cloud storage services like Dropbox and OneDrive.
Prevent unintentional disclosure	 SafeGuard Encryption	Synchronized Encryption that is always on makes sure all files are always encrypted everywhere.