



Cisco 2018  
Report annuale sulla cybersecurity

# Sommario

## **Sintesi ..... 3**

## **Parte I: il panorama degli attacchi ..... 6**

L'evoluzione del malware .....	6
Traffico Web dannoso criptato .....	9
Minacce e-mail .....	14
Tattiche di evasione della sandbox .....	22
Abuso dei servizi cloud e di altre risorse legittime .....	24
Attacchi IoT e DDoS .....	31
Vulnerabilità e patching .....	38

## **Parte II: il panorama della difesa ..... 46**

Il costo degli attacchi .....	46
Sfide e ostacoli .....	47
Orchestrazione complessa a causa dei fornitori .....	48
Impatto: esposizione al pubblico in seguito a violazioni e maggior rischio di perdite .....	50
Servizi: occuparsi di persone e policy, non solo di tecnologia .....	53
Aspettative: investire in tecnologia e formazione .....	54

## **Conclusioni ..... 57**

## **Informazioni su Cisco ..... 60**

## **Appendice ..... 65**

# Sintesi

E se i responsabili della sicurezza potessero prevedere il futuro? Se sapessero che un attacco è imminente, potrebbero bloccarlo o almeno mitigarne l'impatto e si adopererebbero per mettere in sicurezza le risorse che più necessitano protezione. In effetti gli addetti alla sicurezza sono *in grado* di vedere cosa si profila all'orizzonte: gli indizi sono molti (ed evidenti).

Gli autori degli attacchi e gli stati nazionali hanno già le competenze e gli strumenti necessari per bloccare infrastrutture e sistemi critici e paralizzare intere regioni. Ma, anche quando vengono alla luce attacchi informatici destabilizzanti e devastanti, come quelli sferrati in Ucraina o in altre parti del mondo, partendo dal presupposto l'obiettivo non era il mercato, la regione o la tecnologia della loro azienda, parte dei professionisti della sicurezza tendono a credere di non essere a rischio.

Ad ogni modo, non dedicando la dovuta attenzione a campagne apparentemente distanti o lasciandosi totalmente assorbire dal caos delle schermaglie quotidiane con i criminali informatici, i responsabili della sicurezza non riescono a rendersi conto della portata e della velocità con cui i criminali accumulano e affinano le proprie armi informatiche.

Da anni Cisco mette in guardia gli addetti alla sicurezza sull'escalation del crimine informatico nel mondo. In questo ultimo report annuale sulla cybersecurity, vengono presentati dati e analisi dei ricercatori sulle minacce di Cisco e di molti altri partner tecnologici sul comportamento degli autori di attacchi osservato negli ultimi 12-18 mesi. In linea generale, gli argomenti esaminati nel report possono essere ricondotti a tre temi generali:

## 1. I criminali informatici stanno portando il malware a livelli di sofisticatezza e impatto senza precedenti.

Nel 2017 l'evoluzione del malware (pagina 6) ha segnato uno degli sviluppi più significativi nel panorama degli attacchi. L'avvento di cryptoworm ransomware basati sulla rete rende superfluo il fattore umano nel lancio di campagne ransomware. Inoltre, una parte degli autori degli attacchi non ambisce al riscatto, ma punta a distruggere sistemi e dati, come dimostrato da Nyetya, un wiper malware mascherato da ransomware (vedere pagina 6). Il malware auto-propagante è pericoloso e ha il potenziale di bloccare completamente Internet, secondo quanto indicano i ricercatori sulle minacce di Cisco.

## 2. I criminali informatici sono sempre più abili a evadere e a sfruttare come armi servizi cloud e altre tecnologie usati per scopi legittimi.

Oltre a sviluppare minacce in grado di **sfuggire ad ambienti di sandboxing sempre più sofisticati** (pagina 22), gli autori degli attacchi hanno ampliato **l'applicazione della crittografia per eludere il rilevamento** (pagina 9). La crittografia ha lo scopo di aumentare la sicurezza, ma per i criminali informatici rappresenta anche uno strumento potente per nascondere attività di command-and-control (C2), poiché offre loro più tempo per agire e provocare danni.

I criminali informatici ora adottano anche **canali di C2 che si basano su servizi Internet legittimi** come Google, Dropbox e GitHub (vedere pagina 24). In questo modo è quasi impossibile identificare il traffico malware.

Inoltre, molti criminali informatici **lanciano campagne multiple da un singolo dominio** (pagina 26) per ottenere il massimo ritorno possibile sui propri investimenti. Riutilizzano anche risorse infrastrutturali, indirizzi e-mail degli iscritti, ASN (Autonomous System Number) e nameserver.

## 3. Gli autori degli attacchi sfruttano le lacune nella sicurezza, molte delle quali derivano dall'espansione di Internet of Things (IoT) e dall'uso di servizi cloud.

I responsabili della sicurezza implementano i dispositivi IoT a un ritmo sostenuto, ma spesso prestano scarsa attenzione alla sicurezza di questi sistemi. **I dispositivi IoT privi di patch e di controllo** offrono ai criminali informatici numerose opportunità per infiltrarsi nelle reti (pagina 34). La ricerca indica anche che le aziende con dispositivi IoT passibili di attacchi non sembrano neanche **motivate ad accelerare la risoluzione del problema**, (pagina 42). Oltretutto queste aziende probabilmente hanno molti più dispositivi IoT vulnerabili nei loro ambienti IT di quanto credono.

Nel frattempo, **le botnet IoT si stanno espandendo** di pari passo con IoT e stanno diventando più mature e automatizzate. Parallelamente a questa crescita, i criminali informatici le utilizzano per lanciare attacchi DDoS (Distributed Denial-of-Service) più avanzati ([pagina 31](#)).

Gli hacker approfittano anche del fatto che per i team di sicurezza è **difficile difendere gli ambienti sia cloud che IoT**. Uno dei motivi è dovuto alla mancanza di chiarezza riguardo a chi precisamente sia responsabile della protezione di tali ambienti (vedere a [pagina 42](#)).

### Consigli per i responsabili della sicurezza

Quando inevitabilmente i criminali informatici colpiranno le loro aziende, i responsabili della sicurezza saranno preparati? E quanto velocemente riusciranno ad effettuare il ripristino? Stando allo **Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018**, che offre approfondimenti sulle procedure di sicurezza attuate da oltre 3600 intervistati in 26 paesi, i responsabili della sicurezza devono superare moltissime sfide (vedere a [pagina 46](#)).

Ciò nonostante, essi scopriranno che l'attuazione di miglioramenti strategici alla sicurezza e l'adesione alle principali migliori prassi possono ridurre l'esposizione ai rischi emergenti, rallentare l'avanzamento dei criminali informatici e fornire maggiore visibilità sul panorama delle minacce. Devono prendere in considerazione le seguenti azioni:

- Implementare strumenti di difesa di prima linea caratterizzati da scalabilità, come le piattaforme di sicurezza cloud.
- Garantire la conformità a policy e procedure aziendali per il patching di applicazioni, sistemi e appliance.

- Impiegare la segmentazione della rete per ridurre l'esposizione agli attacchi.
- Adottare strumenti di nuova generazione per il monitoraggio dei processi degli endpoint.
- Accedere a dati e processi di intelligence sulle minacce puntuali e accurati che consentano di integrare tali informazioni nel monitoraggio della sicurezza e nella gestione degli eventi.
- Svolgere analisi più approfondite e più avanzate.
- Rivedere le procedure di risposta di sicurezza ed esercitarsi a utilizzarle.
- Eseguire spesso il backup dei dati e testare le procedure di ripristino (processi che sono fondamentali in un mondo caratterizzato da worm ransomware veloci e basati sulla rete e armi informatiche distruttive).
- Rivedere i test di terze parti sull'efficacia delle tecnologie di sicurezza per ridurre il rischio di attacchi alla filiera di approvvigionamento.
- Svolgere l'analisi della sicurezza dei sistemi di amministrazione di microservizi, servizi cloud e applicazioni.
- Rivedere i sistemi di sicurezza e considerare l'uso dell'analisi SSL e, se possibile, della decrittografia SSL.

I responsabili della sicurezza dovrebbero anche pensare di adottare tecnologie di sicurezza avanzata che includano funzionalità di machine learning e di artificial intelligence. Dato che il malware nasconde le sue comunicazioni all'interno del traffico Web criptato e i criminali inviano dati sensibili attraverso i sistemi cloud aziendali, i team di sicurezza hanno bisogno di strumenti efficaci per prevenire o rilevare l'utilizzo della crittografia atto a nascondere attività dannose.

### i Il report

Il **report annuale di Cisco sulla cybersecurity 2018** presenta gli ultimi progressi nel settore della sicurezza allo scopo di aiutare le aziende e gli utenti a difendersi dagli attacchi. Inoltre vengono esaminate le tecniche e le strategie di cui i criminali informatici si avvalgono per aggirare le difese ed eludere il rilevamento.

Nel report vengono inoltre illustrati i risultati principali dello **Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018**, che analizza la postura della sicurezza delle aziende e la percezione della preparazione nella difesa dagli attacchi.

# Parte I: il panorama degli attacchi

# Parte I: il panorama degli attacchi

I criminali informatici stanno portando il malware a livelli di sofisticatezza e impatto senza precedenti. Il crescente numero e la varietà di tipi e famiglie di malware perpetuano il caos nel panorama degli attacchi, minando le azioni che i responsabili della sicurezza mettono in atto per guadagnare terreno e mantenere la propria posizione in relazione alle minacce.

## L'EVOLUZIONE DEL MALWARE

*Nel 2017 uno degli sviluppi più importanti nel panorama degli attacchi è stata l'evoluzione del ransomware. L'avvento di worm ransomware basati sulle reti rende superflua la presenza dell'elemento umano per lanciare le campagne. Inoltre, alcuni criminali informatici non ambiscono al riscatto, ma puntano alla distruzione di dati e sistemi. Questa attività è destinata ad aumentare nel prossimo anno.*

Sono lì in agguato e, nel 2018, gli addetti alla sicurezza dovranno prepararsi ad affrontare nuove minacce basate sulla rete e autopropaganti

Nel 2017 i criminali informatici hanno portato il ransomware a un nuovo livello, come da previsioni. Dopo la campagna di SamSam del marzo 2016<sup>1</sup> - il primo attacco su larga scala in cui la rete è stata usata come vettore per diffondere il ransomware, estromettendo in tal modo l'utente dal processo di infezione - gli esperti di minacce Cisco sapevano che sarebbe stata solo questione di tempo prima che gli autori delle minacce trovassero il modo per automatizzare questa tecnica. I criminali informatici hanno reso il loro malware ancora più potente abbinandolo a funzionalità "quasi-worm" per causare danni ancora più diffusi.

Questa evoluzione del malware è stata veloce. Nel maggio 2017 ha fatto la sua comparsa WannaCry, un cryptoworm ransomware che si è diffuso a macchia d'olio attraverso Internet.<sup>2</sup> Per propagarsi, ha approfittato di una vulnerabilità della sicurezza di Microsoft Windows chiamata **EternalBlue**, rivelata dal gruppo di hacker Shadow Brokers a metà aprile 2017.

Una volta incassati i portafogli, WannaCry ha raccolto oltre 143.000 dollari con pagamenti in bitcoin. Considerate le tempistiche e calcolando il valore dei bitcoin originariamente versati nei portafogli a 93.531 dollari, secondo le stime degli esperti delle minacce di Cisco, sarebbero stati pagati circa 312 riscatti. Come termine di paragone, l'exploit kit Angler, quando era attivo, guadagnava circa 100 milioni di dollari all'anno a livello globale.

WannaCry non ha tracciato i danni procurati tramite la crittografia, né i pagamenti eseguiti dagli utenti colpiti ed è altresì sconosciuto il numero di utenti che hanno ricevuto le chiavi di decifrazione dopo avere effettuato il versamento. (WannaCry si sta ancora propagando e gli utenti continuano a pagare il riscatto, invano). A causa delle scarse prestazioni di WannaCry come ransomware, il governo degli Stati Uniti e molti esperti della sicurezza credono che la componente di riscatto sia in realtà una copertura che nasconde il vero scopo di WannaCry: la cancellazione dei dati.

<sup>1</sup> SamSam: The Doctor Will See You, After He Pays the Ransom, blog di Cisco Talos, marzo 2016: [blog.talosintelligence.com/2016/03/samsam-ransomware.html](http://blog.talosintelligence.com/2016/03/samsam-ransomware.html).

<sup>2</sup> Player 3 Has Entered the Game: Say Hello to 'WannaCry,' blog di Cisco Talos, maggio 2017: [blog.talosintelligence.com/2017/05/wannacry.html](http://blog.talosintelligence.com/2017/05/wannacry.html).

Nyetya (noto anche come NotPetya) è comparso nel giugno 2017.<sup>3</sup> Anche questo wiper malware si è camuffato da ransomware e ha utilizzato le vulnerabilità nell'esecuzione del codice remoto soprannominate "EternalBlue" ed "EternalRomance" (anche quest'ultima resa nota da Shadow Brokers) e altri vettori che comportano la raccolta di credenziali a prescindere dalle rivelazioni di Shadow Brokers.<sup>4</sup> Nyetya è stato distribuito attraverso gli aggiornamenti di un pacchetto software fiscale utilizzato da oltre l'80% delle aziende in Ucraina e installato in più di un milione di computer.<sup>5</sup> La polizia informatica ucraina ha confermato che sono state colpite oltre 2000 aziende ucraine.<sup>6</sup>

Prima della diffusione del ransomware autopropagante, il malware veniva distribuito in tre modi: download drive-by, e-mail o supporti fisici come memorie USB dannose. Tutti questi metodi richiedevano qualche tipo di interazione umana per infettare un dispositivo o un sistema con il ransomware. Con l'utilizzo di questi nuovi vettori da parte degli hacker, basta solo disporre di una postazione di lavoro attiva e priva di patch per lanciare una campagna di ransomware basata sulla rete.

Gli esperti della sicurezza possono considerare i worm come un "vecchio" tipo di minaccia, poiché il numero di CVE (Common Vulnerabilities and Exposures) simili ai worm è diminuito di pari passo al miglioramento degli standard di sicurezza dei prodotti. Però, il malware autopropagante non rappresenta solo una minaccia considerevole: secondo i ricercatori Cisco, può potenzialmente impedire il funzionamento di Internet. WannaCry e Nyetya sono solo un assaggio di ciò che verrà, quindi gli addetti alla sicurezza dovrebbero prepararsi.

La diffusione di WannaCry e Nyetya avrebbe potuto essere evitata o resa priva di conseguenze, se più aziende avessero applicato le migliori prassi elementari in fatto di sicurezza, ad esempio eseguire il patching delle vulnerabilità, istituire processi e policy appropriati per reagire agli incidenti e adottare la segmentazione della rete.

Per ulteriori suggerimenti su come affrontare la minaccia dei worm ransomware automatici basati sulla rete, leggere **Back to Basics: Worm Defense in the Ransomware Age** nel blog di Cisco Talos.

## Il punto debole della sicurezza: la filiera di approvvigionamento

La campagna di Nyetya è stata anche un attacco alla filiera di approvvigionamento, uno dei molti osservati nel 2017 dai ricercatori Cisco. Una delle ragioni per cui Nyetya è riuscito a infettare così tante macchine così rapidamente è che gli utenti non hanno considerato un aggiornamento software automatico come un rischio per la sicurezza e, in qualche caso, non si sono nemmeno accorti che stavano ricevendo aggiornamenti dannosi.

Un altro attacco alla filiera di approvvigionamento, che si è verificato nel settembre 2017, ha coinvolto i server di download utilizzati da un fornitore di software per distribuire un pacchetto legittimo noto come CCleaner.<sup>7</sup> I file binari di CCleaner, che contenevano una backdoor trojan, sono stati firmati con un certificato valido, inducendo gli utenti a ritenere che il software che stavano usando fosse sicuro. I fautori di questa campagna erano a caccia di grandi aziende tecnologiche che utilizzavano questo software, legittimamente o nell'ambito di una struttura IT fantasma.

Gli attacchi alle filiere di approvvigionamento sembrano aumentare in termini di velocità e complessità, possono esercitare un impatto su larga scala sui computer e i danni che producono possono persistere per mesi o addirittura anni. Gli addetti alla sicurezza devono essere informati del potenziale rischio legato all'utilizzo di software o hardware proveniente da aziende che non dispongono di una postura della sicurezza responsabile e devono selezionare fornitori che emettono CVE, risolvono velocemente le vulnerabilità e si impegnano costantemente per assicurare che i sistemi di build che realizzano siano inviolabili. Inoltre, gli utenti dovrebbero prendersi il tempo necessario per analizzare il nuovo software prima di scaricarlo in modo da verificare che non contenga malware.

Nel caso di software non supportati da prassi di sicurezza esaustive, la segmentazione della rete può contribuire a contenere i danni dagli attacchi alle filiere di approvvigionamento, impedendo loro di diffondersi all'interno di intere aziende.

3 New Ransomware Variant 'Nyetya' Compromises Systems Worldwide, blog di Cisco Talos, giugno 2017: [blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html](http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html).

4 Ibid.

5 Ukraine scrambles to contain new cyber threat after 'NotPetya' attack, di Jack Stubbs e Matthias Williams, Reuters, luglio 2017: [reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P](http://reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P).

6 The MeDoc Connection, blog di Cisco Talos, luglio 2017: [blog.talosintelligence.com/2017/07/the-medoc-connection.html](http://blog.talosintelligence.com/2017/07/the-medoc-connection.html).

7 CCleaner Command and Control Causes Concern, blog di Cisco Talos, settembre 2017: [blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html](http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html).

## ● Perché è importante l'integrità nei report dell'intelligence sulle minacce

Tutte le aziende che condividono informazioni sulle minacce con i clienti o il pubblico attraverso un qualsiasi canale dovrebbero adottare linee guida che le aiutino a garantire l'accuratezza dei loro report. Anche se non tutti i dati sono chiari, le aziende possono comunque comunicare quello che sanno, evitando pericolose congetture. Meglio avere una visione appropriata che cercare a tutti i costi di arrivare primi.

Ad esempio, quando si è verificato l'attacco di WannaCry nel maggio 2017, c'è stata una confusione iniziale all'interno della community degli esperti di sicurezza su come il worm ransomware si infiltrasse nei sistemi. Diverse aziende sia del settore pubblico che privato sostenevano che l'attacco derivasse da una campagna di phishing e da un allegato e-mail dannoso. Ma la minaccia basata sulla rete, in realtà, andava alla ricerca di porte SMB (Server Message Block) di Microsoft Windows Server vulnerabili e rivolte al pubblico e le infettava.

I ricercatori sulle minacce di Cisco hanno avvisato tempestivamente la community degli esperti della sicurezza

che le e-mail che pensavano fossero collegate alla campagna di WannaCry erano probabilmente e-mail di spam del bot Necurs che stavano diffondendo il ransomware "Jaff". Ciò è successo parecchi giorni prima che la community degli esperti della sicurezza convenisse che le e-mail sospette contenevano Jaff e non WannaCry. Nel frattempo gli utenti agivano sulla base di informazioni che non potevano aiutarli a evitare la rapida campagna di WannaCry.

Il caos seguito all'avvento della campagna di WannaCry serve a ricordare che la community degli esperti della sicurezza deve evitare di comunicare dati inesatti circa l'origine e la natura degli attacchi informatici. Nelle prime ore di una campagna, nella frenesia di dover bloccare rapidamente gli hacker e proteggere gli utenti, si tendono a pubblicare, soprattutto sui social media, informazioni che possono creare confusione e impedire agli utenti di difendere i loro sistemi.

Per ulteriori informazioni su questo argomento, leggere il post *On Conveying Doubt* sul blog di Cisco Talos.

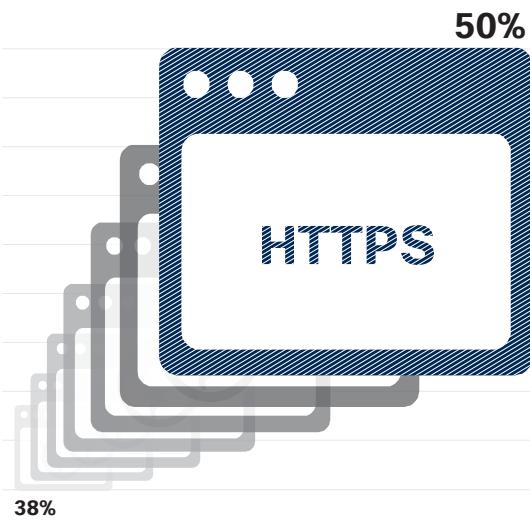
## TRAFFICO WEB DANNOSO CRIPTATO

L'espansione del volume del traffico Web criptato, legittimo o dannoso, genera ancora più difficoltà e confusione tra gli addetti alla sicurezza che devono identificare e monitorare le potenziali minacce. La crittografia ha lo scopo di aumentare la sicurezza, ma per i criminali informatici rappresenta anche uno strumento potente per nascondere attività di command-and-control (C2), poiché offre loro più tempo per agire e provocare danni. I ricercatori Cisco che si occupano di minacce prevedono che i criminali informatici ricorreranno di più alla crittografia nel 2018. Per tenere il passo, i responsabili della sicurezza dovranno adottare in misura maggiore l'automazione e strumenti evoluti, quali machine learning e artificial intelligence, per integrare le attuali soluzioni per la prevenzione, il rilevamento e la risoluzione delle minacce.

### Un angolo buio per gli addetti alla sicurezza: il traffico Web dannoso criptato

Gli esperti di minacce di Cisco riferiscono che, nell'ottobre 2017, il 50% del traffico Web globale è stato criptato. Si tratta di un aumento di 12 punti rispetto ai volumi rilevati a novembre 2016 (vedere la Figura 1). Uno dei fattori alla base di questo incremento è la disponibilità di certificati SSL gratuiti o a basso costo. Un altro è la prassi, sempre più frequente, di Google Chrome di contrassegnare come "non protetti" i siti Web non criptati che gestiscono informazioni sensibili, come quelle sulle carte di credito dei clienti. Le aziende sono motivate a rispettare i requisiti di crittografia HTTPS di Google, altrimenti rischierebbero di subire potenzialmente significativo del posizionamento nelle pagine di ricerca di Google.

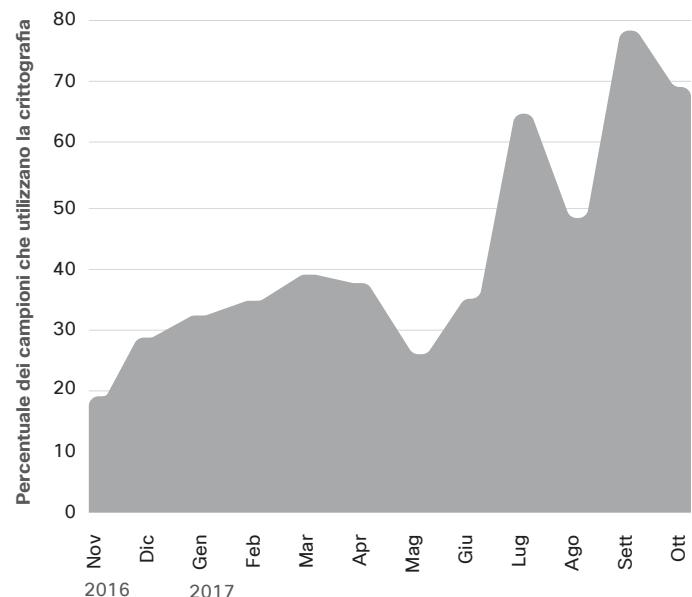
**Figura 1** Aumento del volume del traffico Web globale criptato



Fonte: Cisco Security Research

Con l'aumento del traffico Web criptato a livello globale, i fattori degli attacchi sembrano ampliare l'uso della crittografia come strumento per nascondere le loro attività di C2. I ricercatori di Cisco hanno rilevato che le comunicazioni di rete criptate, utilizzate dai campioni di malware osservati nell'arco di 12 mesi, sono più che triplicate (vedere la Figura 2). L'analisi condotta su oltre 400.000 file binari dannosi ha rilevato che, a partire da ottobre 2017, circa il 70% aveva usato un qualche tecnica crittografica.

**Figura 2** Aumento del volume dei file binari dannosi che sfruttano la comunicazione di rete criptata



Fonte: Cisco Security Research

 Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## Applicazione del machine learning allo spettro delle minacce

Per sopperire alla mancanza di visibilità creata dalla crittografia e ridurre il tempo d'azione dei criminali informatici, sempre più aziende si interessano all'uso delle tecniche di machine learning e artificial intelligence. Queste funzionalità avanzate permettono di migliorare le difese orientate alla sicurezza delle reti e, nel corso del tempo, "apprendere" come rilevare automaticamente comportamenti insoliti nel traffico Web che potrebbero indicare attività dannose.

Il machine learning è utile per rilevare automaticamente le minacce "conosciute-conosciute", ossia quei tipi di infezioni rilevate in precedenza (vedere la Figura 3). Ma il suo valore reale, soprattutto nel monitoraggio del traffico Web criptato, deriva dalla capacità di rilevare minacce "conosciute-

sconosciute" (varianti inedite di minacce note, sottofamiglie di malware o nuove minacce correlate) e "sconosciute-sconosciute" (malware assolutamente nuovo). La tecnologia può imparare a identificare percorsi insoliti in grandi volumi di traffico Web criptato e avvisare automaticamente i team di sicurezza circa la necessità di ulteriori indagini.

Quest'ultimo punto è particolarmente importante, dato che la mancanza di personale specializzato è un ostacolo al rafforzamento delle difese in molte aziende, come emerge dallo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018 (vedere a pagina 35). L'automazione e gli strumenti intelligenti, come machine learning e artificial intelligence, possono aiutare i responsabili della sicurezza a superare le difficoltà in termini di competenze e risorse, aumentando l'efficacia nell'identificazione delle minacce note ed emergenti e nella successiva reazione.

**Figura 3** Machine learning nella sicurezza della rete: tassonomia



Fonte: Cisco Security Research

 Scaricare il grafico del 2018 al link seguente: cisco.com/go/acr2018graphics

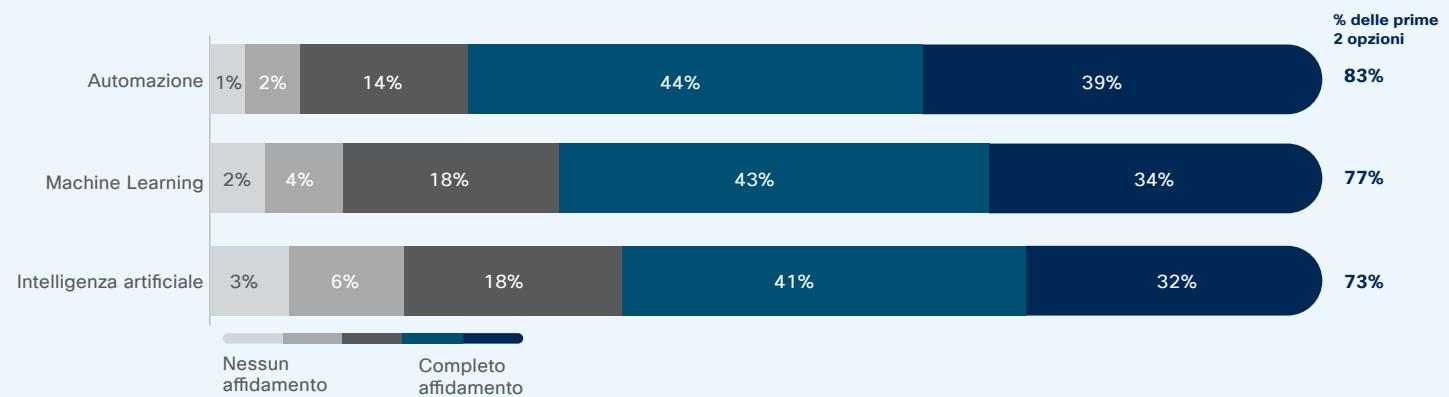
## i Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018: i responsabili della sicurezza fanno più affidamento su machine automation e artificial intelligence

I Chief Information Security Officer (CISO) intervistati per lo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018 affermano di essere impazienti di aggiungere strumenti che utilizzano artificial intelligence e machine learning e indicano che la propria infrastruttura di sicurezza si sta espandendo in termini di sofisticatezza e intelligence. D'altro canto, lamentano una certa frustrazione per il numero di falsi positivi generati da tali sistemi, poiché in questo modo aumenta il carico di lavoro del team di sicurezza. Queste preoccupazioni dovrebbero ridursi nel corso del tempo perché le tecnologie di machine learning e di artificial intelligence maturano e imparano a distinguere l'attività "normale" negli ambienti di rete che monitorano.

Quando è stato chiesto a quali tecnologie automatizzate si affidassero maggiormente le proprie aziende, il 39% degli esperti della sicurezza ha dichiarato di fare completamente affidamento sull'automazione, il 34% sul machine learning e il 32% sull'artificial intelligence (Figura 4).

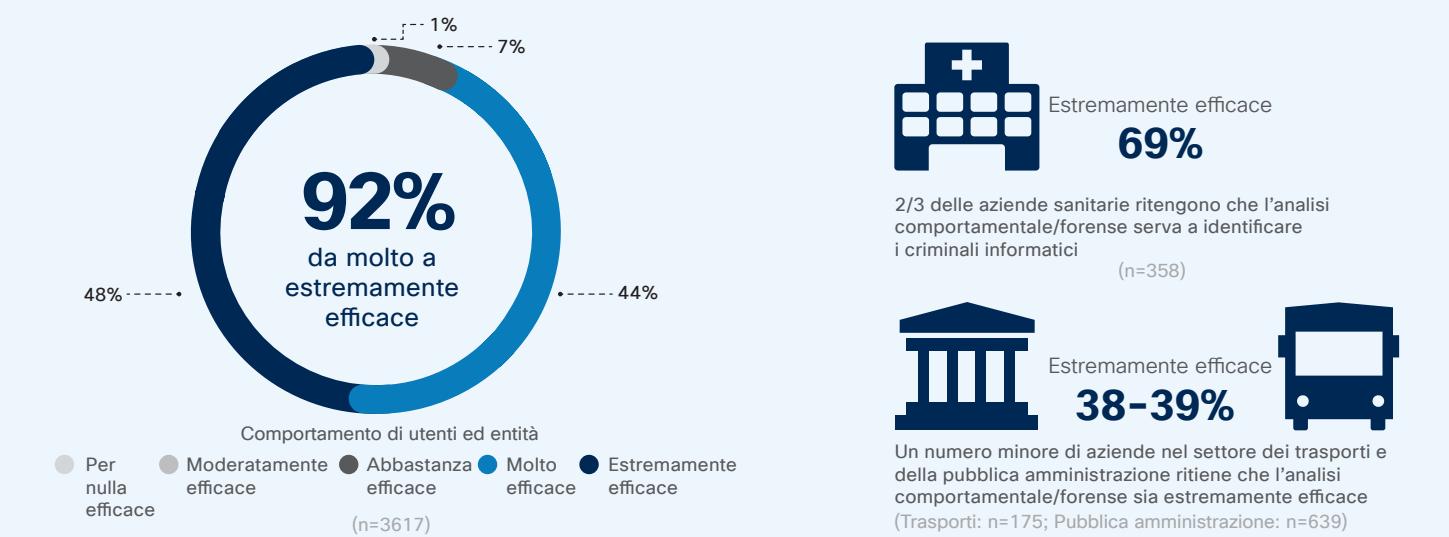
Anche gli strumenti di analisi comportamentale sono considerati utili per individuare gli hacker nelle reti: per il 92% degli esperti della sicurezza questi strumenti funzionano da molto a estremamente bene (Figura 5).

**Figura 4** Le aziende si affidano massicciamente ad automazione, machine learning e artificial intelligence



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 5** La maggior parte degli esperti della sicurezza ritiene validi gli strumenti di analisi comportamentale



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

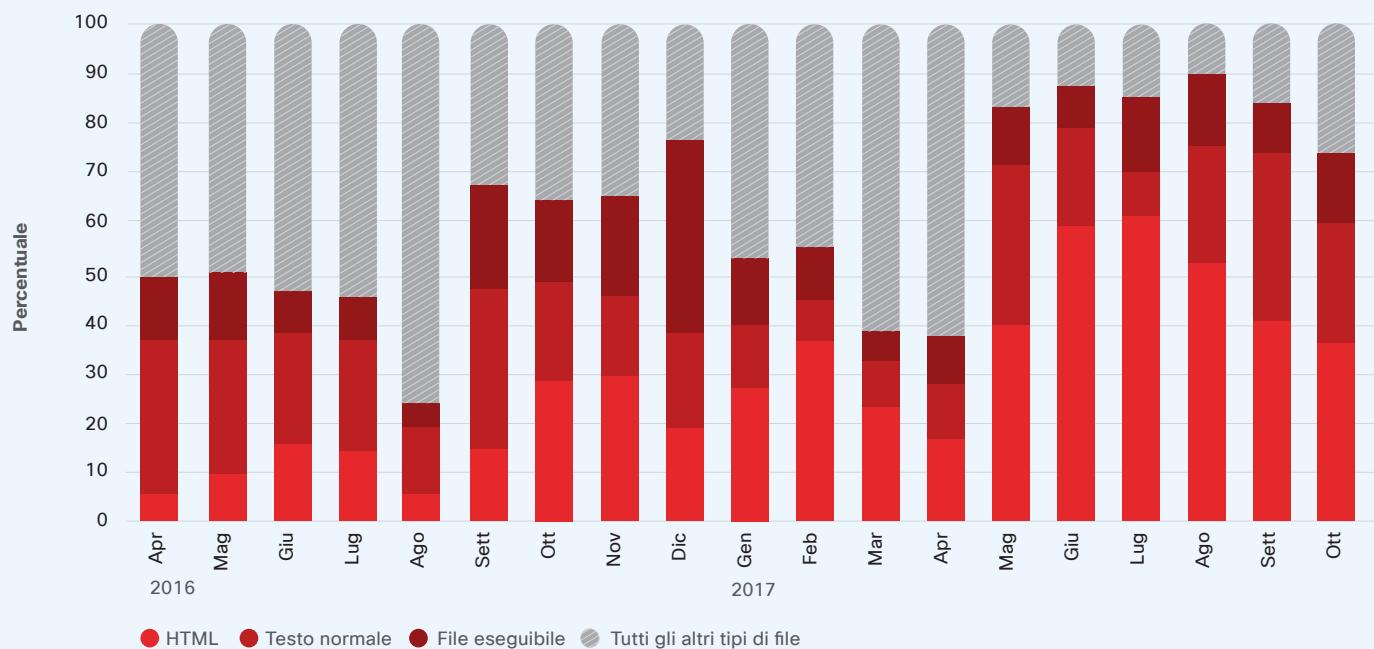
Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## i I metodi di attacco nel Web mostrano l'attenzione che i criminali informatici rivolgono alla compromissione dei browser

Un'analisi dei metodi di attacco nel Web, condotta su un periodo di 18 mesi, da aprile 2016 a ottobre 2017, mostra un aumento dell'uso, da parte dei criminali informatici, di contenuti Web dannosi (Figura 6). Questa tendenza è in linea con gli attacchi aggressivi al browser Web Microsoft Internet Explorer da parte di exploit kit ancora attivi.

I ricercatori sulle minacce di Cisco hanno osservato che il numero di rilevamenti di contenuti Web JavaScript dannosi in questo periodo è stato significativo e costante. Ciò sottolinea l'efficacia della strategia nell'infettare i browser vulnerabili per facilitare altre attività nefaste, come il reindirizzamento dei browser o il download di trojan.

**Figura 6** Attività di blocco basate su malware per tipo di contenuto, aprile 2016 – ottobre 2017



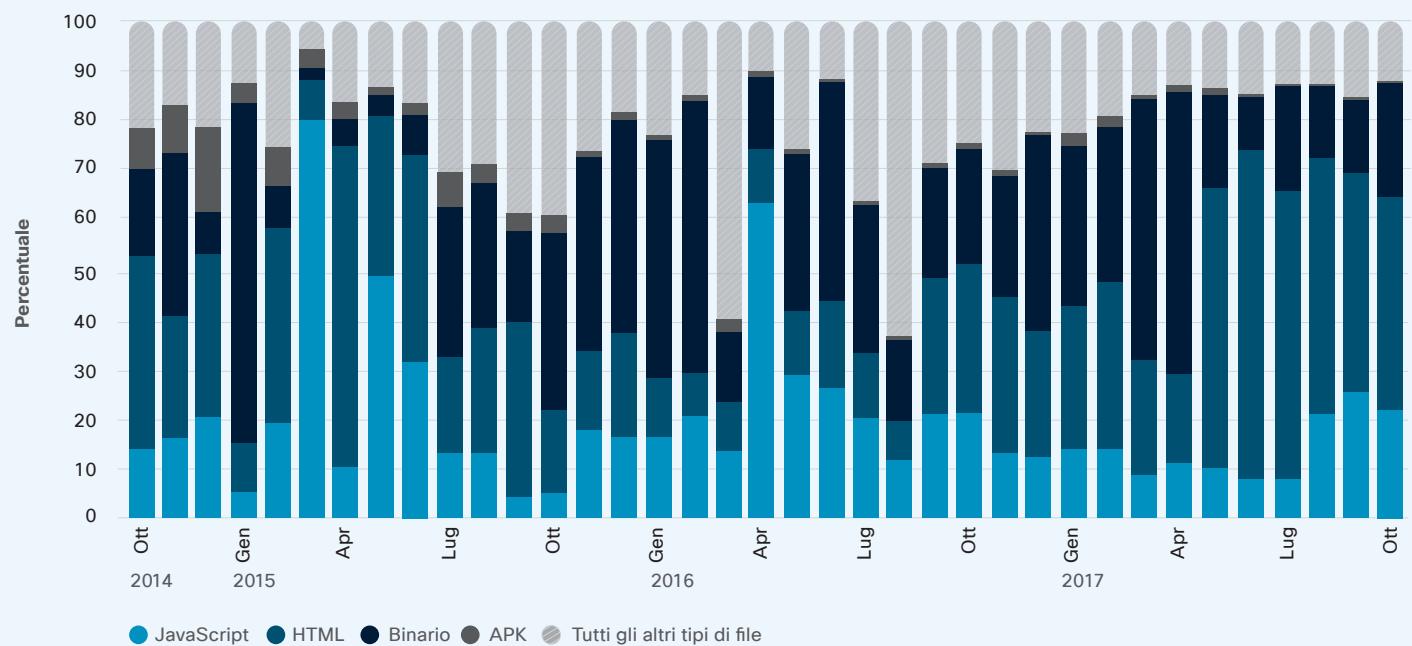
Fonte: Cisco Security Research

La Figura 7 mostra una panoramica dei metodi di attacco nel Web rilevati in un periodo di tre anni, da ottobre 2014 a ottobre 2017. In cui gli autori degli attacchi hanno impiegato costantemente file binari sospetti, principalmente per diffondere adware e spyware. Come illustrato nel *Report semestrale di Cisco sulla cybersecurity 2017*, questi tipi di applicazioni potenzialmente indesiderate (PUA) possono presentare rischi per la sicurezza quali l'aumento delle

infezioni da malware e il furto di informazioni relative a utenti o aziende.<sup>8</sup>

La panoramica di tre anni della Figura 7 mostra anche che il volume dei contenuti Web dannosi varia nel tempo, in quanto, nell'implementazione delle loro campagne, i criminali informatici modificano le tattiche impiegate per eludere il rilevamento.

**Figura 7** Attività di blocco basate su malware per tipo di contenuto, ottobre 2014 – ottobre 2017



Fonte: Cisco Security Research

 Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

<sup>8</sup> Report semestrale di Cisco sulla cybersecurity 2017: [cisco.com/c/m/en\\_au/products/security/offers/cybersecurity-reports.html](http://cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html).

## MINACCE E-MAIL

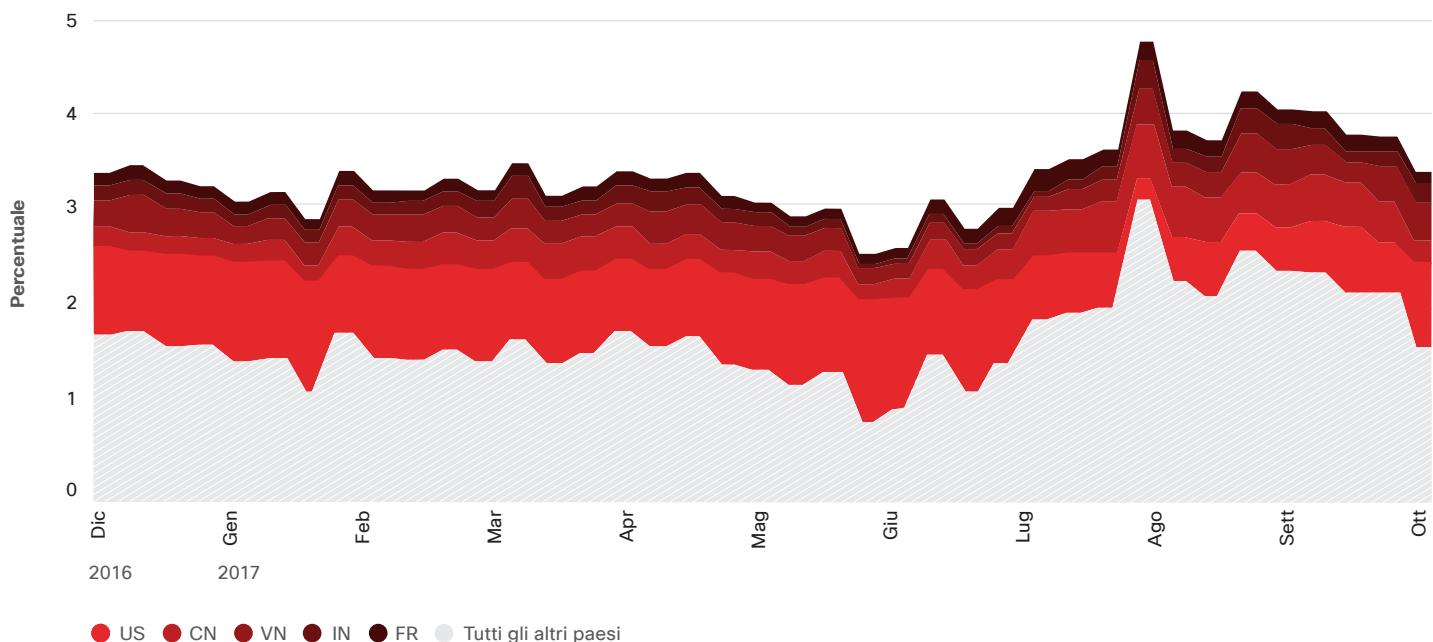
A prescindere dai mutamenti del panorama delle minacce, spam ed e-mail dannose restano strumenti indispensabili per la distribuzione di malware da parte degli hacker, perché portano le minacce direttamente all'endpoint. Applicando il giusto mix di tecniche di social engineering, come phishing e allegati e link dannosi, i criminali informatici devono solamente aspettare che gli utenti, ignari, attivino i loro exploit.

### Le oscillazioni nell'attività di botnet spam influiscono sul volume complessivo

A fine 2016 i ricercatori sulle minacce di Cisco hanno osservato un notevole aumento nell'attività delle campagne di spam, concomitante con un declino nell'attività degli exploit kit. Quando alcuni tra i principali exploit kit, come Angler, sono scomparsi improvvisamente dal mercato, molti dei loro utilizzatori si sono rivolti, o sono tornati, al vettore costituito dalle e-mail per

continuare a garantirsi dei profitti.<sup>9</sup> Tuttavia, dopo quella corsa iniziale di ritorno alle e-mail, il volume di spam globale è diminuito e si è stabilizzato nella prima metà del 2017. Successivamente, tra a fine maggio e inizio giugno 2017, il volume di spam globale è crollato prima di impennare bruscamente nella seconda metà dell'estate (vedere la Figura 8).

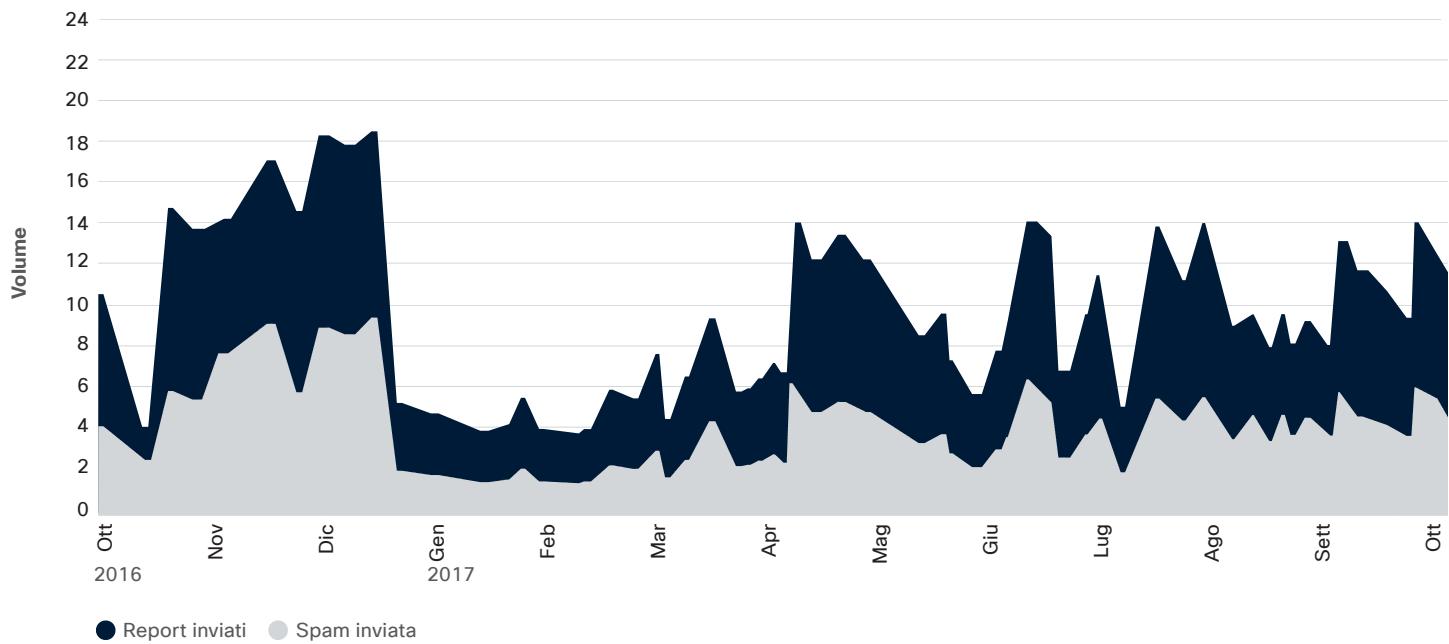
**Figura 8** Blocchi di reputazione IP per paese, dicembre 2016 – ottobre 2017



Fonte: Cisco Security Research

<sup>9</sup> Vedere "Il declino dell'attività degli exploit kit potrà verosimilmente influenzare i trend dello spam a livello globale", p. 18, Report semestrale di Cisco sulla cybersecurity 2017: [cisco.com/c/m/en\\_au/products/security/offers/cybersecurity-reports.html](http://cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html).

**Figura 9** Attività di botnet spam, ottobre 2016 – ottobre 2017



Fonte: Cisco SpamCop



Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

La riduzione del volume di spam da gennaio ad aprile 2017 coincide con una pausa nell’attività dei botnet spam, come mostrato nel grafico interno generato dal servizio Cisco® SpamCop (Figura 9).

I ricercatori sulle minacce di Cisco riferiscono che, tra gennaio e aprile, la botnet Necurs, uno dei principali contributori al volume di spam a livello mondiale, era attiva, ma distribuiva meno spam. Nel mese di maggio la botnet ha diffuso il ransomware Jaff attraverso massicce campagne di spam. Le

campagne presentavano un file PDF con un documento Microsoft Office dannoso incorporato e il downloader iniziale per il ransomware Jaff.<sup>10</sup> I ricercatori della sicurezza hanno scoperto una vulnerabilità in Jaff che ha permesso loro di creare un decriptatore, costringendo gli operatori di Necurs a tornare rapidamente alla distribuzione della loro solita minaccia, il ransomware Locky.<sup>11</sup> Il tempo che è servito agli autori di Necurs per tornare a Locky coincide con la diminuzione significativa nel volume di spam globale osservata nelle prime due settimane di giugno (Figura 9).

<sup>10</sup> *Jaff Ransomware: Player 2 Has Entered the Game*, di Nick Biasini, Edmund Brumaghin e Warren Mercer, con contributi di Colin Grady, blog di Cisco Talos, maggio 2017: [blog.talosintelligence.com/2017/05/jaff-ransomware.html](http://blog.talosintelligence.com/2017/05/jaff-ransomware.html).

<sup>11</sup> *Player 1 Limpers Back Into the Ring—Hello Again, Locky!* di Alex Chiu, Warren Mercer e Jaeson Schultz, con contributi di Sean Baird e Matthew Molyett, blog di Cisco Talos, giugno 2017: [blog.talosintelligence.com/2017/06/necurs-locky-campaign.html](http://blog.talosintelligence.com/2017/06/necurs-locky-campaign.html).

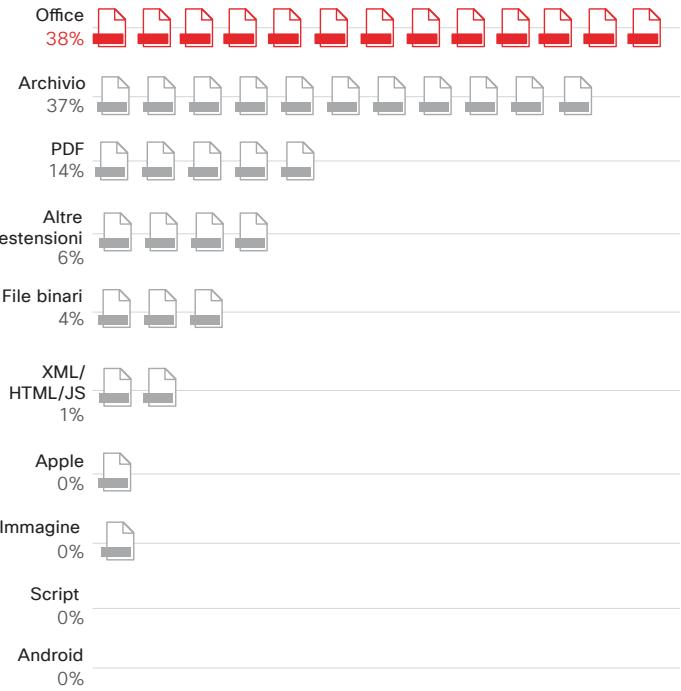
## Estensioni di file dannosi nelle e-mail: i 10 principali strumenti delle famiglie di malware più comuni

I ricercatori sulle minacce di Cisco hanno analizzato la telemetria delle e-mail da gennaio a settembre 2017 per identificare i tipi di estensioni di file dannosi contenuti nei documenti allegati alle e-mail impiegati più spesso dalle famiglie di malware più diffuse. L'analisi ha prodotto una "top 10" da cui è emerso che il gruppo prevalente di estensioni di file dannosi (38%) è quello dei formati di Microsoft Office come Word, PowerPoint ed Excel (vedere la Figura 10).

I file di archiviazione come .zip e .jar rappresentano circa il 37% delle estensioni di file dannosi osservate nello studio. Non stupisce che i criminali informatici impieghino diffusamente i file di archiviazione, poiché questi file da tempo sono il nascondiglio preferito per il malware. Gli utenti devono aprire i file di archiviazione per visualizzare il contenuto, il che, per molte minacce, costituisce un passo importante nella catena delle infezioni. Inoltre, i file di archiviazione dannosi spesso riescono a ingannare gli strumenti di analisi automatica, specialmente quando contengono minacce che richiedono l'interazione dell'utente per l'attivazione. Per eludere il rilevamento, gli autori degli attacchi utilizzano anche tipi di file meno noti, ad esempio .7z e .rar.

Le estensioni di file PDF dannosi si attestano alle prime tre posizioni, totalizzando quasi il 14% sulle estensioni di file dannosi. (Nota: la categoria "Altre estensioni" si riferisce a estensioni osservate nello studio, che non è stato possibile associare facilmente a tipi di file conosciuti. È noto che alcuni tipi di malware utilizzano estensioni di file casuali).

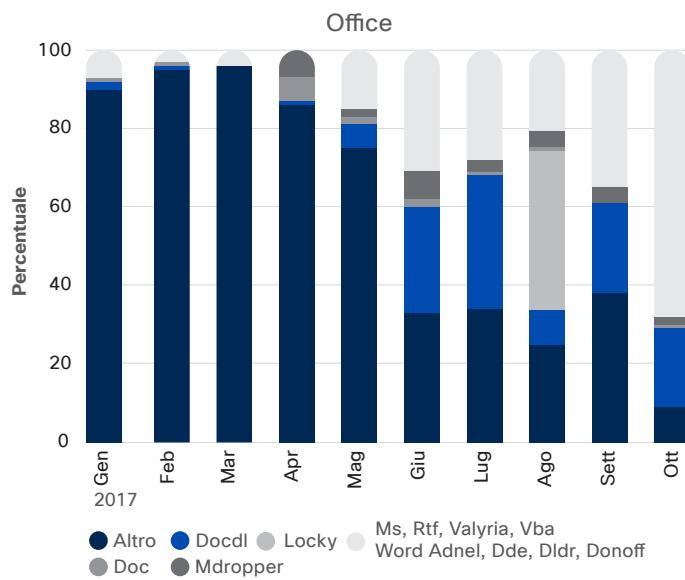
**Figura 10** Le prime 10 estensioni di file dannosi, gennaio – settembre 2017



Fonte: Cisco Security Research

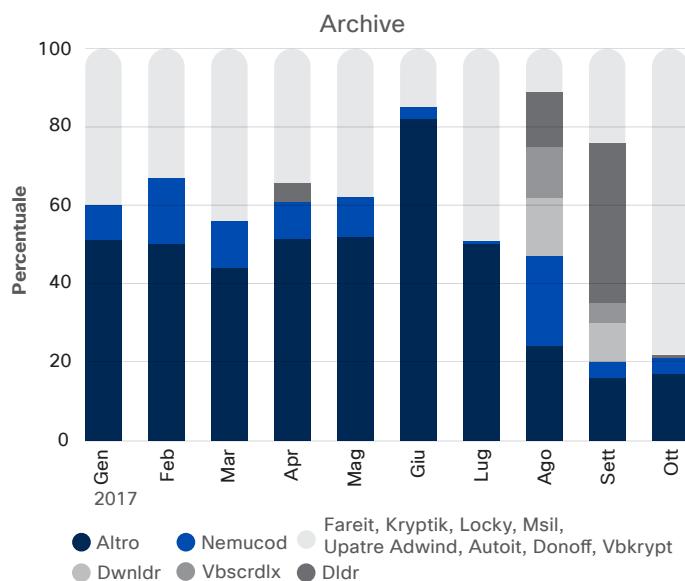
Le Figure 11a-c mostrano una panoramica delle famiglie di malware considerate nell'indagine che sono state associate ai primi tre tipi di estensioni di file dannosi: file di MS Office, archivi e file PDF. La Figura 12 riporta la percentuale di rilevamenti delle estensioni di file con payload dannoso per singola famiglia di malware. I picchi nell'attività sono in linea con le campagne di spam osservate durante quei mesi, secondo i ricercatori sulle minacce di Cisco. Ad esempio,

**Figura 11a** Primi tre tipi di estensioni di file dannosi e rapporti con le famiglie di malware



Fonte: Cisco Security Research

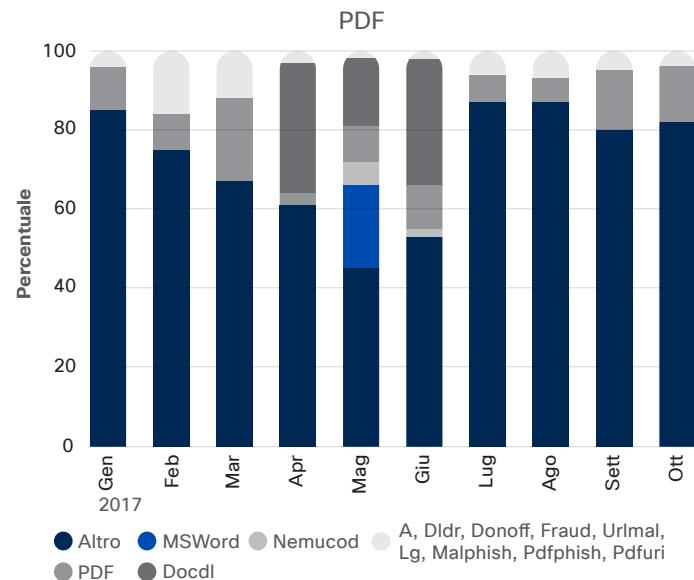
**Figura 11c** Primi tre tipi di estensioni di file dannosi e rapporti con le famiglie di malware



Fonte: Cisco Security Research

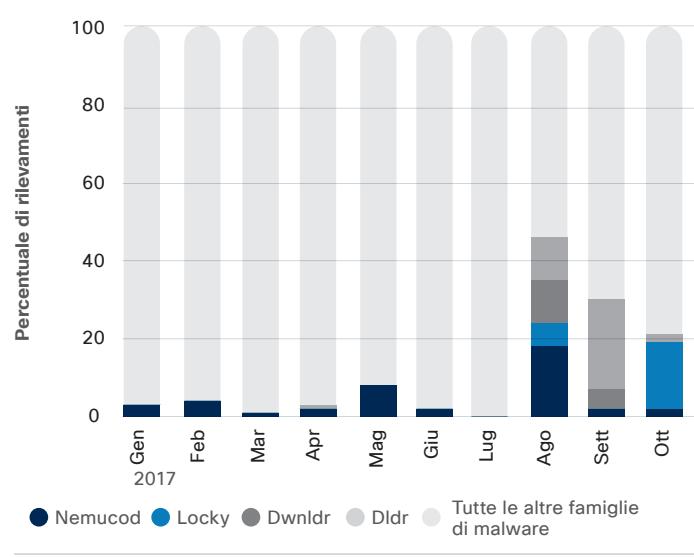
nella tarda estate, vi sono state importanti campagne di distribuzione di Nemucod e Locky, due minacce che spesso operano congiuntamente. Notoriamente Nemucod invia payload dannosi nei file di archiviazione come .zip che contengono script dannoso, ma sembrano normali file con estensione .doc. (“Dwnldr”, mostrato anch’esso nella Figura 12, è una probabile variante di Nemucod).

**Figura 11b** Primi tre tipi di estensioni di file dannosi e rapporti con le famiglie di malware



Fonte: Cisco Security Research

**Figura 12** Andamento delle principali famiglie di malware, gennaio – ottobre 2017



Fonte: Cisco Security Research

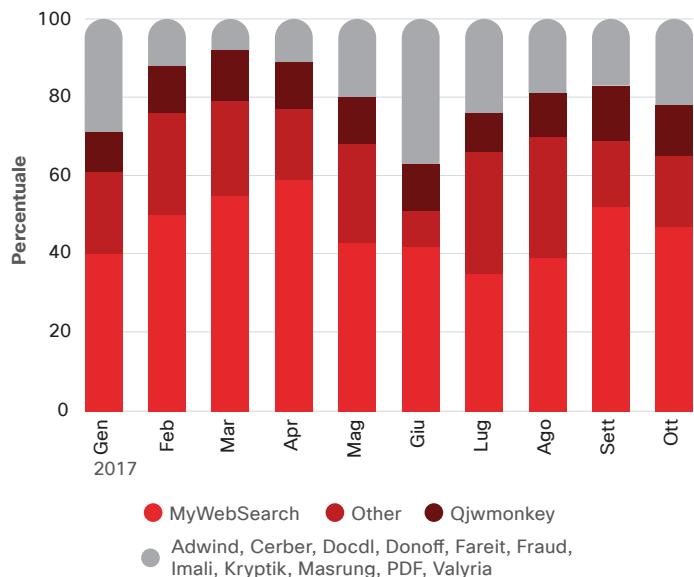
### Lo spyware MyWebSearch è l'utente più attivo del gruppo “altre estensioni”

Il gruppo “altre estensioni” dello studio comprende diversi tipi di malware ben conosciuti. Ma MyWebSearch, un software adware e hijacker di browser dannoso che si finge un’utile barra degli strumenti, è il malware più attivo (vedere la Figura 13). Utilizza unicamente le estensioni di file .exe, a volte solo un tipo al mese. Questa applicazione potenzialmente indesiderata (PUA) è in circolazione da anni e infetta diversi tipi di browser. Spesso è abbinata a software fraudolenti e può esporre gli utenti a malvertising.

L’analisi delle estensioni di file dannosi dimostra che, anche nell’attuale panorama delle minacce, sofisticato e complesso, le e-mail rimangono un canale vitale per la distribuzione di malware. Per le aziende, le strategie di difesa di base sono costituite da:

- Implementazione di difese potenti e complete per la sicurezza dei sistemi e-mail.
- Formazione degli utenti circa la minaccia di allegati e link dannosi nelle e-mail di phishing e spam.

**Figura 13** MyWebSearch è l’utente più attivo del gruppo “altre estensioni”



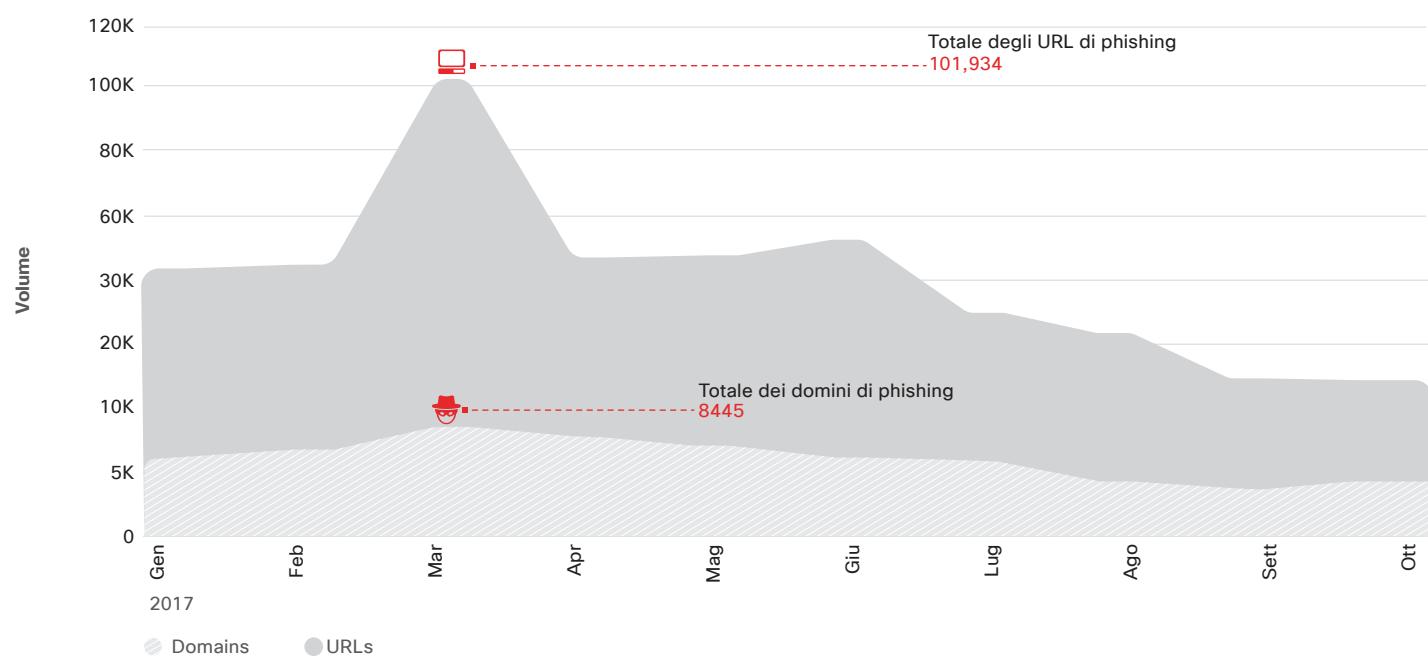
Fonte: Cisco Security Research

## Il social engineering è ancora un trampolino di lancio fondamentale per gli attacchi tramite e-mail

Phishing e spear phishing sono tattiche ben congegnate per trarre vantaggio delle credenziali degli utenti e altre informazioni sensibili, poiché sono molto efficaci. Infatti, le e-mail di phishing e spear phishing sono state alla base di alcune delle più importanti e pubblicate violazioni degli ultimi anni. Due esempi del 2017 includono un attacco diffuso che ha avuto per obiettivo gli utenti Gmail<sup>12</sup> e un caso di hackeraggio dei sistemi energetici irlandesi.<sup>13</sup>

Per valutare i principali URL e i domini di phishing in Internet, gli esperti di minacce di Cisco hanno esaminato i dati provenienti da fonti che indagano su e-mail potenzialmente "fasulle" inviate dagli utenti attraverso l'intelligence sulle minacce anti-phishing basata sulla community. La Figura 14 mostra il numero di URL e domini di phishing osservati tra gennaio e ottobre 2017.

**Figura 14** Numero di URL e domini di phishing osservati per mese



Fonte: Cisco Security Research

I picchi osservati a marzo e giugno possono essere attribuiti a due diverse campagne. La prima sembra avere avuto per oggetto gli utenti di uno dei principali provider di servizi di telecomunicazioni. La campagna:

- Ha coinvolto 59.651 URL contenenti sottodomini sotto aaaainfomation[punto]org.
- Presentava sottodomini che contenevano stringhe casuali costituite da 50-62 lettere.

Ogni lunghezza di sottodominio (50-62) conteneva circa 3500 URL, il che ha permesso di utilizzare i sottodomini a livello di codice (esempio: Cewekonuxyksowegulukozapojygepuqybyteqe johofopefogu[punto]aaaainfomation[punto]org).

Gli hacker hanno utilizzato un servizio di privacy poco costoso per registrare i domini osservati in questa campagna.

12 Massive Phishing Attack Targets Gmail Users, di Alex Johnson, NBC News, maggio 2017: [nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501](http://nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501).

13 Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure, di Lizzie Deardon, The Independent, luglio 2017: [independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html](http://independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html).

Nella seconda campagna, che è stata più attiva nel mese di giugno, i criminali informatici hanno utilizzato il nome di un'agenzia fiscale del Regno Unito per mascherare le loro azioni. Essi hanno impiegato 12 domini di primo livello (TLD): undici erano URL con sei stringhe casuali di sei caratteri (esempio: jyzwyp[punto]top) e nove sono stati associati con più di 1600 siti di phishing ciascuno.

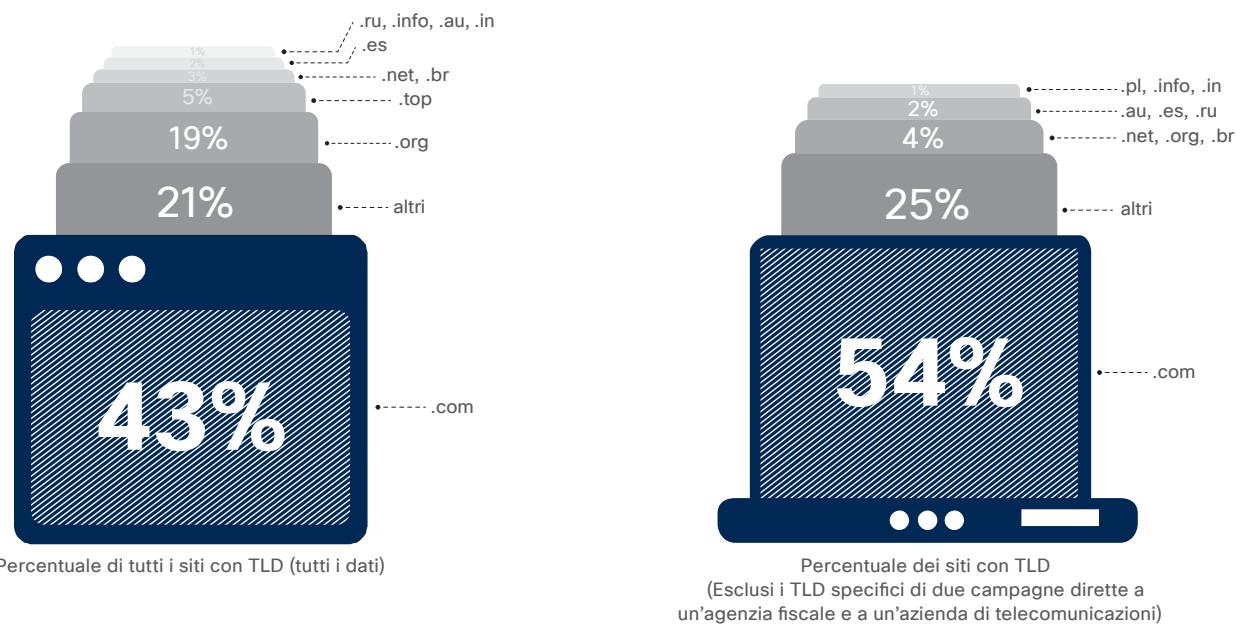
Come nella campagna di marzo, gli hacker hanno utilizzato un servizio di privacy per nascondere le informazioni di registrazione dei domini e hanno completato la registrazione in un periodo di due giorni. Il secondo giorno sono stati osservati quasi 19.000 URL collegati alla campagna e tutti sono stati scoperti all'interno di una finestra di cinque ore (per saperne di più su quanto velocemente gli autori delle minacce

attivino i domini appena registrati, vedere "Utilizzo improprio di risorse legittime per la creazione di backdoor C2", a [pagina 24](#)).

#### Distribuzione di TLD in siti di phishing noti

L'analisi dei siti di phishing nel periodo tra gennaio e agosto 2017 ha rilevato che i criminali informatici avevano impiegato 326 TLD unici per queste attività, tra cui .com, .org, .top (in gran parte nell'ambito della campagna che ha colpito l'Agenzia delle Entrate del Regno Unito) oltre a TLD specifici per paese (vedere la Figura 15). L'uso di TLD meno conosciuti può essere vantaggioso per gli autori di attacchi, poiché questi domini sono generalmente poco costosi e offrono una protezione della privacy a basso costo.

**Figura 15** Distribuzione di TLD in siti di phishing noti



Fonte: Cisco Security Research

## Gli addetti alla sicurezza devono rimanere in guardia e continuare a monitorare questa “vecchia” minaccia

Nel 2017 decine di migliaia di tentativi di phishing sono stati segnalati mensilmente ai servizi anti-phishing di intelligence sulle minacce basati sulla community considerati nell’analisi. Tra le tattiche e gli strumenti comunemente impiegati dagli autori degli attacchi per mettere in atto campagne di phishing figurano:

- **Domain squatting:** ai domini viene assegnato un nome simile a quello di un dominio valido (esempio: cisc0[punto]com).
- **Domain shadowing:** a un dominio valido vengono aggiunti sottodomini senza che il proprietario ne sia a conoscenza (esempio: badstuff[punto]cisco[punto]com).
- **Domini registrati dannosi:** domini creati per scopi dannosi (esempio: viqpbe[punto]top).
- **Abbreviazioni di URL:** URL dannosi camuffati per mezzo di abbreviazioni (esempio: bitly[punto]com/random-string).

Nota: nei dati che sono stati esaminati, Bitly.com è risultato lo strumento per l’abbreviazione di URL più utilizzato dagli autori degli attacchi. Gli URL abbreviati dannosi rappresentano il 2% dei siti di phishing valutati nello studio. Cifra che è salita al 3,1% ad agosto.

- **Servizi di sottodominio:** siti creati in un server di sottodominio (esempio: mybadpage[punto]000 webhost[punto]com).

Gli autori delle minacce che impiegano phishing e spear phishing affinano continuamente i metodi di social engineering per indurre gli utenti a fare clic su link dannosi o a visitare pagine Web fraudolente fornendo le proprie credenziali o altri tipi di informazioni preziose. La formazione e la responsabilizzazione degli utenti, oltre all’applicazione di tecnologie per la sicurezza delle e-mail rimangono strategie essenziali per contrastare queste minacce.

## TATTICHE DI EVASIONE DALLA SANDBOX

Gli autori degli attacchi stanno diventando particolarmente abili nello sviluppo di minacce in grado di eludere ambienti di sandboxing sempre più sofisticati. Nell'analisi di allegati di e-mail dannosi che erano stati dotati di varie tecniche di evasione della sandbox, i ricercatori Cisco hanno scoperto che il numero di campioni dannosi che utilizzavano una particolare tecnica di evasione evidenziava vari picchi e un successivo calo repentino. Questo è l'ennesimo esempio di come gli autori di attacchi aumentino rapidamente il numero di tentativi di violare le difese quando trovano una tecnica efficace.

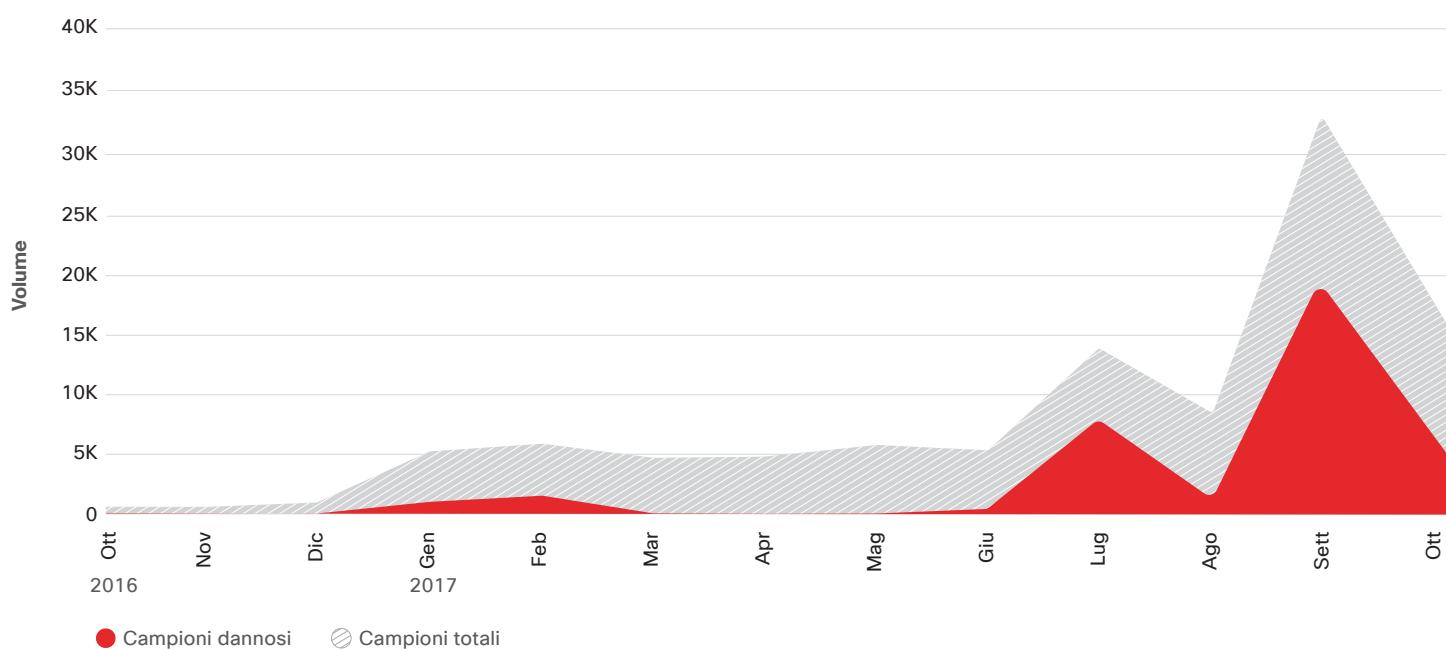
### Gli autori di malware giocano sporco nelle sandbox degli addetti alla sicurezza

Nel settembre 2017 i ricercatori sulle minacce di Cisco hanno notato un numero elevato di casi in cui un payload dannoso viene consegnato dopo la chiusura di un documento (Figura 16), poiché il malware viene attivato mediante l'evento "document\_close". La tecnica funziona perché, in molti casi, i documenti non vengono chiusi dopo essere stati aperti e analizzati nella sandbox. Poiché la sandbox non chiude in modo esplicito i documenti, gli allegati sono ritenuti sicuri dalla sandbox e vengono consegnati ai destinatari previsti. Quando un destinatario apre l'allegato e, poi, lo chiude, il payload

dannoso viene consegnato. Le sandbox che non rilevano correttamente le azioni svolte alla chiusura dei documenti possono essere eluse utilizzando questa tecnica.

L'utilizzo dell'evento "document\_close" è una scelta intelligente per gli autori degli attacchi, poiché sfrutta la funzionalità macro integrata in Microsoft Office, così come la tendenza degli utenti di aprire gli allegati che ritengono essere rilevanti per loro. Una volta che gli utenti si rendono conto che l'allegato non li riguarda, chiudono il documento, innescando le macro in cui è nascosto il malware.

**Figura 16** Elevato volume di documenti Microsoft Word dannosi che utilizzano "le chiamate di funzione chiudi" osservato nel settembre 2017



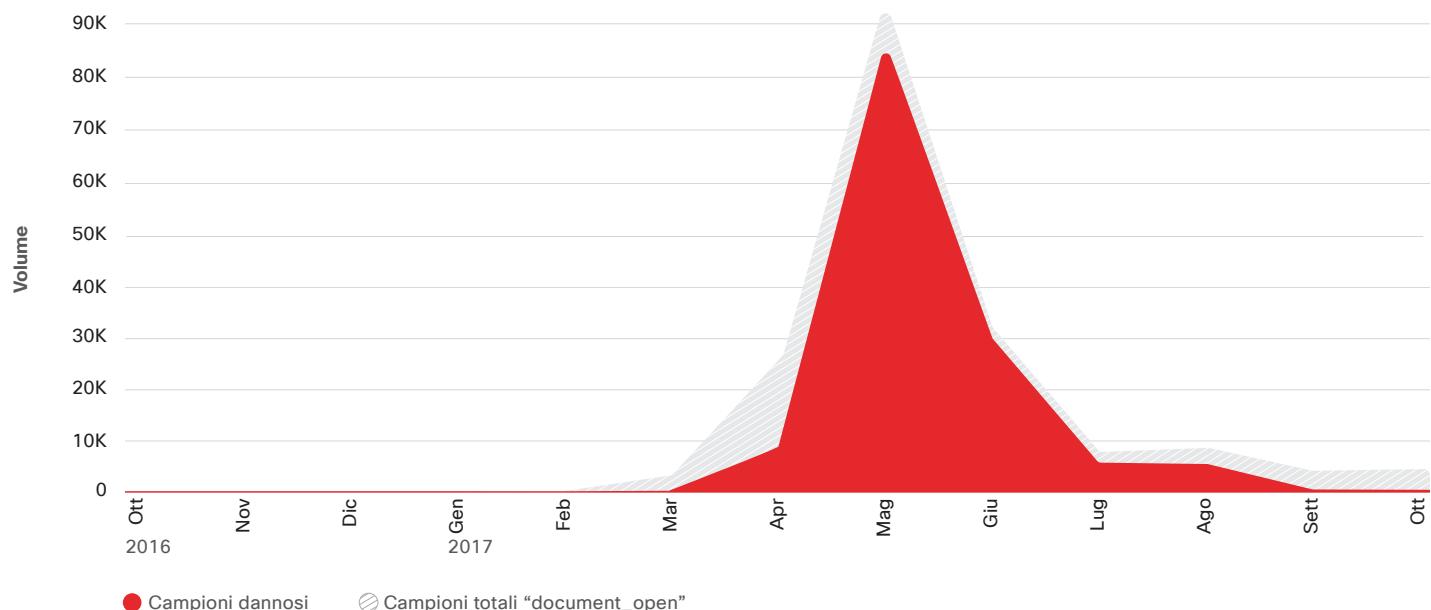
Fonte: Cisco Security Research

Alcuni criminali informatici eludono il sandboxing camuffando il tipo di documento in cui è presente il payload dannoso. Come mostrato nella Figura 17, nel maggio 2017 abbiamo rilevato un attacco significativo che è stato costruito con documenti Word dannosi incorporati all'interno di documenti PDF. I documenti potrebbero aggirare le sandbox che si limitano a rilevare e aprire il file PDF anziché aprire e analizzare anche il documento Word incorporato. Il documento PDF in genere conteneva un invito per l'utente a fare clic e aprire il documento Word, il che faceva scattare il

comportamento malevolo. Le sandbox che non aprono e analizzano i documenti integrati all'interno di file PDF possono essere aggirate utilizzando questa tecnica.

Dopo avere rilevato il picco nei campioni dannosi che coinvolgono questi PDF, i nostri ricercatori hanno affinato l'ambiente delle sandbox per rilevare se i file PDF contenevano azioni o inviti ad aprire documenti Word incorporati.

**Figura 17** Un grande attacco nel maggio 2017 coinvolgeva i PDF con documenti Word dannosi integrati



Fonte: Cisco Security Research

I picchi nei campioni dannosi che utilizzano diverse tecniche di evasione delle sandbox mostrano la volontà degli autori degli attacchi di seguire un metodo che sembra funzionare per sé e per altri criminali informatici. Inoltre, se gli autori degli attacchi si impegnano per creare malware e la relativa infrastruttura, è evidente che ambiscono a un ritorno sui loro investimenti. Se capiscono che il malware può eludere i test delle sandbox, aumentano il numero dei tentativi di attacco e degli utenti interessati.

I ricercatori Cisco consigliano di utilizzare un sandboxing che include funzionalità "sensibili al contenuto" per essere certi che il malware che utilizza queste tattiche non possa aggirare l'analisi delle sandbox. In pratica, la tecnologia di sandboxing dovrebbe mostrare consapevolezza circa le caratteristiche dei metadati dei campioni che sta analizzando, ad esempio per determinare se il campione include un'azione da svolgere alla chiusura del documento.

## ABUSO DEI SERVIZI CLOUD E DI ALTRE RISORSE LEGITTIME

Con lo spostamento di applicazioni, dati e identità nel cloud, i team di sicurezza devono gestire il rischio derivante dalla perdita del controllo sul perimetro della rete tradizionale. Gli autori degli attacchi approfittano delle difficoltà dei team di sicurezza nella difesa degli ambienti cloud e IoT che sono in continua evoluzione ed espansione. Una ragione è la mancanza di chiarezza su chi esattamente sia responsabile della protezione di tali ambienti.

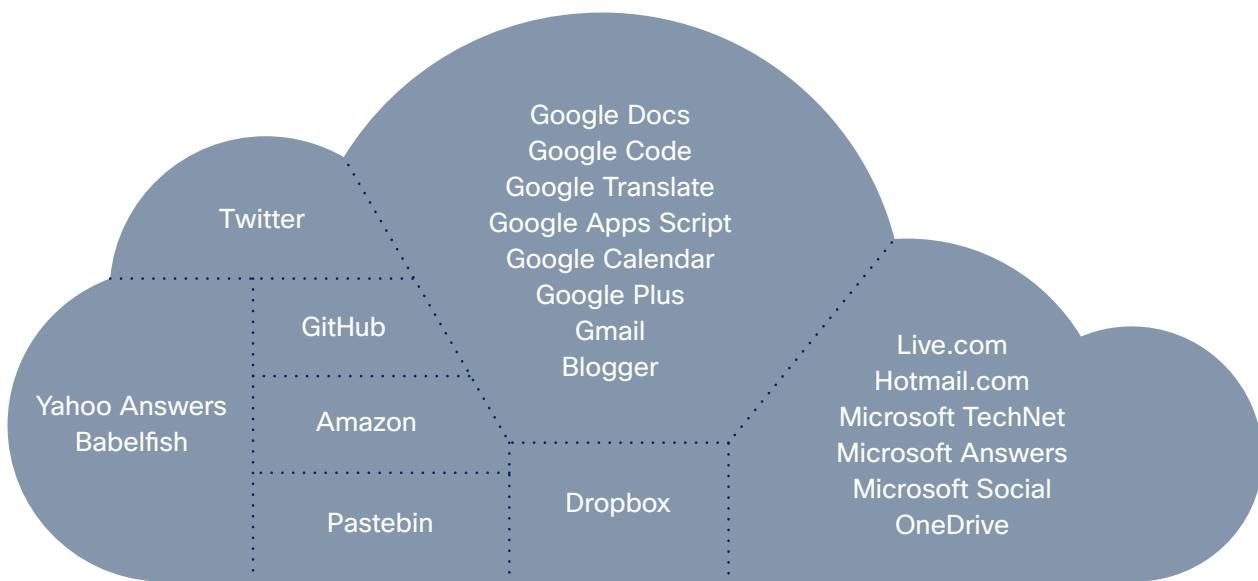
Per affrontare questa sfida, le aziende potrebbero trovarsi nella necessità di applicare una combinazione di migliori prassi, tecnologie di sicurezza avanzate, come il machine learning e, perfino, alcune metodologie sperimentali in base ai servizi utilizzati e al modo in cui le minacce si evolvono in questo spazio.

### Utilizzo dannoso di risorse legittime per la creazione di backdoor C2

Quando gli autori delle minacce utilizzano servizi legittimi per le attività di command-and-control (C2), per i team di sicurezza diventa quasi impossibile identificare il traffico di rete prodotto dal malware, perché esso imita il comportamento del traffico di rete legittimo. I criminali informatici dispongono di una grande quantità di "rumore" prodotto da Internet da utilizzare come copertura, perché molti oggi si affidano a servizi come Google Docs e Dropbox per il loro lavoro, indipendentemente dal fatto che questi servizi siano offerti o avallati a livello di sistema dai loro datori di lavoro.

La Figura 18 mostra molti servizi legittimi ben noti che i ricercatori e Anomali, un partner Cisco e provider di intelligence sulle minacce, hanno rilevato, in quanto sono utilizzati negli schemi di malware backdoor C2<sup>14</sup> negli ultimi anni. (Nota: questi tipi di servizi si trovano di fronte a un dilemma nella lotta contro gli abusi, poiché se rendono più difficile per gli utenti l'impostazione degli account e l'utilizzo, potrebbe essere compromessa la loro capacità di generare profitti).

**Figura 18** Esempi di servizi legittimi violati dal malware per il C2



Fonte: Anomali

<sup>14</sup> Anomali definisce uno schema di C2 come "la totalità di indirizzi IP, domini, servizi legittimi e tutti i sistemi remoti che fanno parte della... architettura di comunicazione" del malware.

Secondo una ricerca di Anomali, gli autori di minacce persistenti avanzate (APT) e i gruppi sponsorizzati dagli Stati sono stati fra i primi a utilizzare servizi legittimi per attività di C2. Però, la tecnica ora è adottata da una più ampia gamma di sofisticati criminali informatici che operano nell'economia sommersa. L'uso di servizi legittimi per attività di C2 si rivela interessante per i criminali informatici, perché è semplice:

- Registrare nuovi account per questi servizi.
- Impostare una pagina Web sull'Internet accessibile al pubblico.
- Usurpare la crittografia per i protocolli di C2. (Anziché impostare i server di C2 con crittografia o introdurre quest'ultima nel malware, gli autori degli attacchi possono semplicemente adottare il certificato SSL di un servizio legittimo).
- Adattare e trasformare le risorse in tempo reale. (Per esempio, gli hacker possono riutilizzare gli impianti per più attacchi senza riutilizzare i DNS o gli indirizzi IP).
- Ridurre il rischio di “bruciare” l'infrastruttura. (I criminali informatici che utilizzano servizi legittimi per il C2 non hanno bisogno di codificare indirizzi IP o domini nel malware e, al termine delle operazioni, possono limitarsi a disattivare le loro pagine di servizi legittime senza che nessuno possa mai conoscere gli indirizzi IP).
- Gli autori degli attacchi sfruttano questa tecnica, perché permette loro di ridurre le spese generali e migliorare il ritorno sugli investimenti.

Per gli addetti alla sicurezza, l'uso di servizi legittimi per il C2 da parte dei criminali informatici pone alcune sfide significative:

#### I servizi legittimi sono difficili da bloccare

Le imprese, da una prospettiva puramente aziendale, possono anche solo pensare di bloccare parti di servizi Internet legittimi come Twitter o Google?

#### I servizi legittimi sono spesso criptati e intrinsecamente difficili da ispezionare

La decriptografia SSL è costosa e non sempre possibile su scala aziendale. Così, il malware nasconde le proprie comunicazioni all'interno del traffico crittografato rendendo difficile, se non impossibile, per i team di sicurezza individuare quello dannoso.

#### L'uso di servizi legittimi sovverte l'intelligence relativa a domini e certificati e complica l'attribuzione

Gli autori degli attacchi non hanno bisogno di registrare i domini, perché l'account del servizio legittimo viene considerato l'indirizzo iniziale di C2. Inoltre, è improbabile che essi continuino a registrare certificati SSL o a utilizzare certificati SSL autofirmati per gli schemi di C2. Entrambe le tendenze ovviamente sono destinate ad avere un impatto negativo sui feed degli indicatori per i filtri reputazione e il blacklisting, che sono basati su domini appena generati e registrati e sui certificati e gli indirizzi IP a essi collegati.

È difficile rilevare l'uso di servizi legittimi per le attività di C2. Tuttavia, i ricercatori di Anomali consigliano agli addetti alla sicurezza di considerare l'ipotesi di adottare alcune metodologie sperimentali. Ad esempio, gli addetti alla difesa potrebbero identificare il malware che utilizza servizi legittimi per le attività di C2 cercando:

- Connessioni a servizi legittimi non generate da browser, né da app
- Dimensioni di risposta delle pagine uniche o limitate provenienti da servizi legittimi
- Elevata frequenza di scambio di certificati con servizi legittimi
- Campioni di sandboxing globali per individuare le chiamate DNS sospette a servizi legittimi

Tutti questi comportamenti singolari meritano ulteriori indagini sui programmi e i processi di origine.<sup>15</sup>

<sup>15</sup> Per ulteriori informazioni su queste metodologie sperimentali nonché per capire come gli autori degli attacchi usano servizi legittimi per il C2, scaricare la ricerca di Anomali, *Rise of Legitimate Services for Backdoor Command and Control*, disponibile all'indirizzo: [anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf](http://anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf).

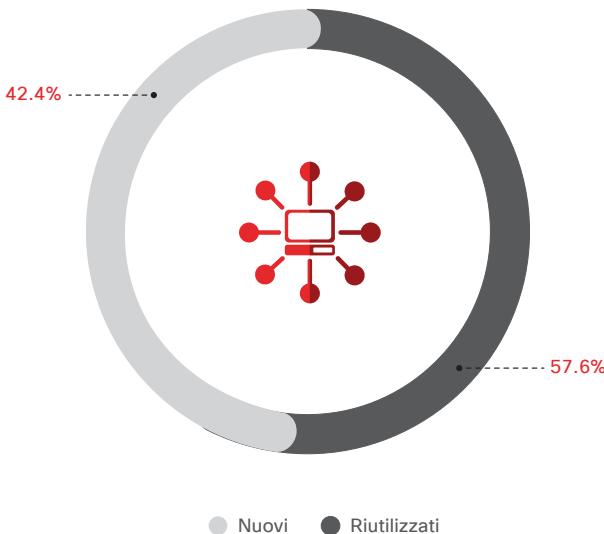
## Estrazione di valore ottimale dalle risorse

I ricercatori sulla sicurezza di Cisco hanno analizzato nomi unici mai visti prima (domini) associati alle query DNS fatte in un periodo di sette giorni nell'agosto 2017. Si noti che l'espressione "mai visto prima", in questo contesto, non ha nulla a che vedere con la data di creazione di un dominio, ma si riferisce a quando esso è stato "visto" per la prima volta dalla tecnologia di sicurezza del cloud di Cisco nel periodo di osservazione.

Questa ricerca aveva lo scopo di ottenere maggiori informazioni dettagliate sul modo in cui spesso gli autori degli attacchi usano e riutilizzano domini di livello registrato (RLD, Registered-Level Domain) nei loro attacchi. Capire i comportamenti degli autori delle minacce a livello di dominio può aiutare gli addetti alla sicurezza a identificare i domini dannosi, insieme ai relativi sottodomini, che devono essere bloccati con strumenti di difesa di prima linea, come le piattaforme di sicurezza cloud.

Affinché i ricercatori potessero concentrarsi esclusivamente sul nucleo di RLD unici, circa 4 milioni in totale, i sottodomini sono stati esclusi dal campione di domini appena visti. Solo una piccola percentuale di RLD del campione è stata categorizzata come dannosa. Degli RLD dannosi, più della metà (circa il 58%) è stata riutilizzata, come mostrato dalla Figura 19.

**Figura 19** Percentuale di domini nuovi e riutilizzati



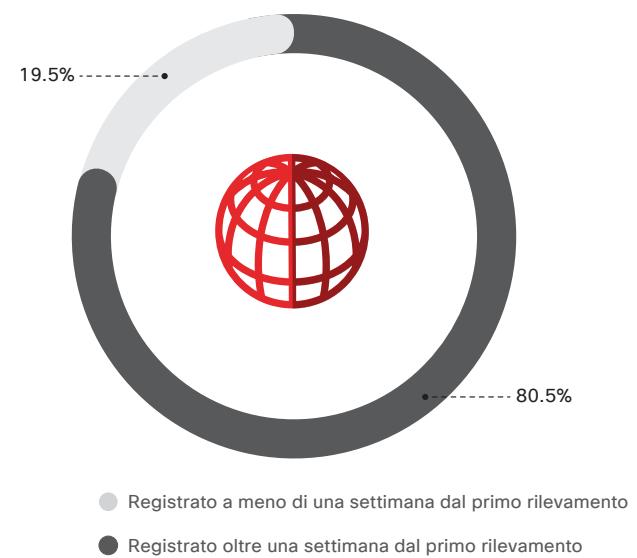
Fonte: Cisco Security Research

Da questa scoperta si evince che, mentre la maggior parte degli autori di attacchi costruisce nuovi domini per le proprie campagne, molti tentano di ottenere il massimo ritorno sull'investimento lanciando più campagne da un singolo dominio. La registrazione dei domini può essere costosa, soprattutto per la massa critica che in genere serve agli autori degli attacchi per mettere in atto le proprie campagne ed eludere il rilevamento.

### 1/5 dei domini dannosi messo rapidamente in uso

I criminali informatici possono aspettare giorni, mesi o anche anni dopo la registrazione dei domini in attesa del momento giusto per usarli. Tuttavia, i ricercatori sulle minacce di Cisco hanno osservato che una percentuale significativa di domini dannosi, circa il 20%, è stata utilizzata nelle campagne entro una settimana dalla registrazione (vedere la Figura 20).

**Figura 20** Tempi di registrazione di RLD

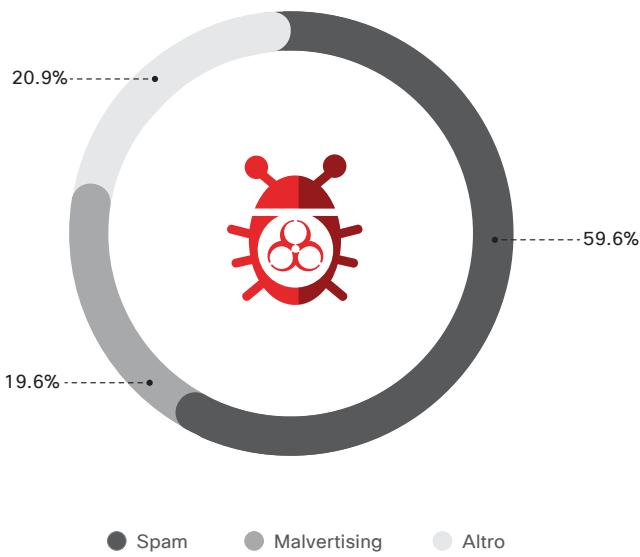


Fonte: Cisco Security Research

## Molti nuovi domini legati a campagne di malvertising

La maggior parte dei domini dannosi analizzati, circa il 60%, è stata associata a campagne di spam. Quasi un quinto dei domini era collegato a campagne di malvertising (vedere la Figura 21). Il malvertising è diventato uno strumento essenziale per indirizzare gli utenti verso gli exploit kit, tra cui quelli che distribuiscono ransomware.

**Figura 21** Catalogazioni dannose



Fonte: Cisco Security Research

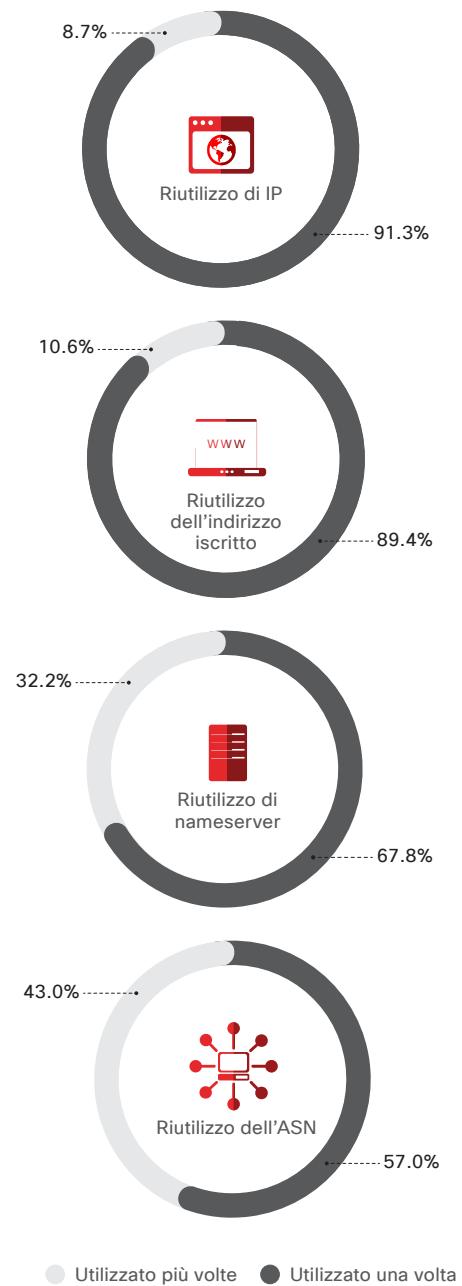
Le tecniche meglio costruite per la creazione di campagne di malvertising legate ai domini comprendono il domain shadowing. Con questa tecnica i criminali informatici rubano le credenziali dell'account di dominio legittimo per creare sottodomini che puntano a server dannosi. Un'altra tattica consiste nell'abuso di servizi DNS dinamici gratuiti per generare domini e sottodomini dannosi. In questo modo, gli autori di attacchi riescono a distribuire payload dannosi da IP host (computer infetti o siti Web pubblici violati) sempre diversi.

## I domini riutilizzano le risorse delle infrastrutture

Gli RLD dannosi del campione hanno anche riutilizzato le risorse delle infrastrutture come indirizzi e-mail iscritti, indirizzi IP, ASN (Autonomous System Number) e nameserver (vedere la Figura 22). Secondo i ricercatori, questa è un'ulteriore prova che i criminali informatici puntano sempre a ottenere il massimo dagli investimenti nei nuovi domini, preservando le

proprie risorse. Ad esempio, un indirizzo IP può essere utilizzato da più di un dominio. Quindi, un autore di attacchi che getta le basi per una campagna potrebbe decidere di investire in alcuni indirizzi IP e una serie di nomi di dominio anziché nei server, che costano di più.

**Figura 22** Riutilizzo delle infrastrutture da parte di RLD dannosi



Fonte: Cisco Security Research

Le risorse riutilizzate dagli RLD forniscono indizi sulla possibilità che un determinato dominio sia dannoso. Ad esempio, è raro che siano riutilizzati degli indirizzi e-mail o degli indirizzi IP iscritti, quindi uno schema di riutilizzo su l'uno o l'altro fronte suggerisce un comportamento sospetto. I responsabili della sicurezza confidano molto nel blocco di questi domini, sapendo che questa operazione probabilmente non comporta un impatto negativo sulle attività aziendali.

Nella maggior parte dei casi è improbabile che il blocco statico di ASN e nameserver sia fattibile. Però, i modelli di riutilizzo degli RLD meritano ulteriori indagini per determinare se alcuni domini debbano essere bloccati.

L'uso di strumenti di sicurezza del cloud intelligenti per la difesa in prima linea per identificare e analizzare domini e sottodomini potenzialmente dannosi può aiutare i team di sicurezza a seguire le tracce di un hacker e a rispondere a domande come:

- In quale indirizzo IP viene risolto il dominio?
- Quale ASN è associato a quell'indirizzo IP?
- Chi ha registrato il dominio?
- Quali altri domini sono associati a quel dominio?

Le risposte possono aiutare gli addetti alla difesa non solo a perfezionare le policy di sicurezza e a bloccare gli attacchi, ma anche a impedire agli utenti di connettersi a destinazioni Internet dannose mentre si trovano nella rete aziendale.

## Le tecnologie DevOps a rischio di attacchi ransomware

Nel 2017 si è assistito all'avvento di attacchi ransomware alle DevOps, iniziati a gennaio con una campagna ransomware che aveva per obiettivo MongoDB, una piattaforma di database open-source.<sup>16</sup> I criminali informatici hanno criptato le istanze pubbliche di MongoDB e hanno chiesto il pagamento di riscatti per le chiavi e il software di decrittografia. Subito dopo, si sono concentrati sulla violazione di database, come CouchDB ed Elasticsearch, con un ransomware orientato ai server.

Rapid7 è un partner Cisco nonché fornitore di dati di sicurezza e soluzioni di analisi. Come hanno spiegato i ricercatori di Rapid7 nel nostro *Report semestrale di Cisco sulla cybersecurity 2017*, i servizi DevOps spesso vengono implementati in modo non corretto o lasciati intenzionalmente aperti per consentire un facile accesso da parte di utenti legittimi, il che li espone agli attacchi.

Rapid7 esegue ispezioni periodiche in Internet alla ricerca di tecnologie DevOps e cataloga sia le istanze aperte sia le istanze colpite da ransomware. In base ai nomi delle tabelle esposti in

internet, alcuni dei servizi DevOps che osservano nelle ispezioni possono contenere informazioni di identificazione personale (PII).

Per ridurre il rischio di esposizione agli attacchi di ransomware alle DevOps, le aziende che utilizzano istanze Internet pubbliche di tecnologie DevOps devono:

- Sviluppare solidi standard per l'implementazione sicura delle tecnologie DevOps
- Mantenere un'attiva consapevolezza delle infrastrutture pubbliche utilizzate dall'azienda
- Mantenere aggiornate le tecnologie DevOps e applicare le patch
- Condurre analisi delle vulnerabilità

**Per ulteriori dettagli sulla ricerca di Rapid7, vedere “Bisogna evitare che le tecnologie DevOps lascino esposta l'azienda” nel Report semestrale di Cisco sulla cybersecurity 2017.**

<sup>16</sup> After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters, di Lucian Constantin, IDG News Service, 13 gennaio 2017: [pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html](http://pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html).

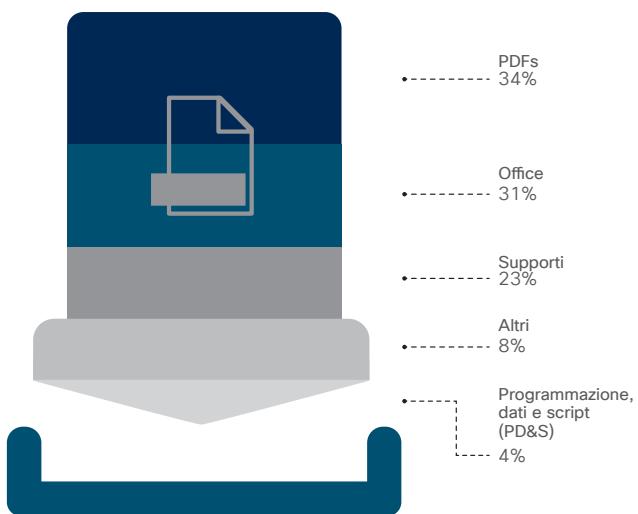
## Minacce interne attraverso il cloud

In report sulla sicurezza precedenti è stato esaminato il valore delle autorizzazioni OAuth e dei privilegi di super-utente per determinare chi può avere accesso alle reti e come questi utenti possono accedere ai dati.<sup>17</sup> Per valutare in modo più approfondito l'impatto dell'utente sulla sicurezza, i ricercatori sulle minacce di Cisco hanno recentemente analizzato le tendenze dell'esfiltrazione dei dati. Mediante un algoritmo di machine learning hanno definito il profilo di 150.000 utenti in 34 paesi che si avvalevano di provider di servizi cloud nel periodo da gennaio a giugno 2017. L'algoritmo teneva conto non solo del volume di documenti scaricati, ma anche di variabili quali l'ora dei download, gli indirizzi IP e le posizioni.

Dopo un'attività di definizione di profili durata sei mesi, i ricercatori hanno dedicato un mese e mezzo allo studio delle anomalie, segnalando lo 0,5% degli utenti per download sospetti. La percentuale è esigua, ma questi utenti hanno scaricato in totale oltre 3,9 milioni di documenti da sistemi cloud aziendali o una media di 5200 documenti per utente nel corso di un mese e mezzo. Dei download sospetti, il 62% si è verificato al di fuori del normale orario di lavoro e il 40% nel fine settimana.

I ricercatori di Cisco hanno altresì condotto un'analisi di text mining sui titoli dei 3,9 milioni di documenti interessati dai download sospetti.

**Figura 23** Documenti scaricati più di frequente



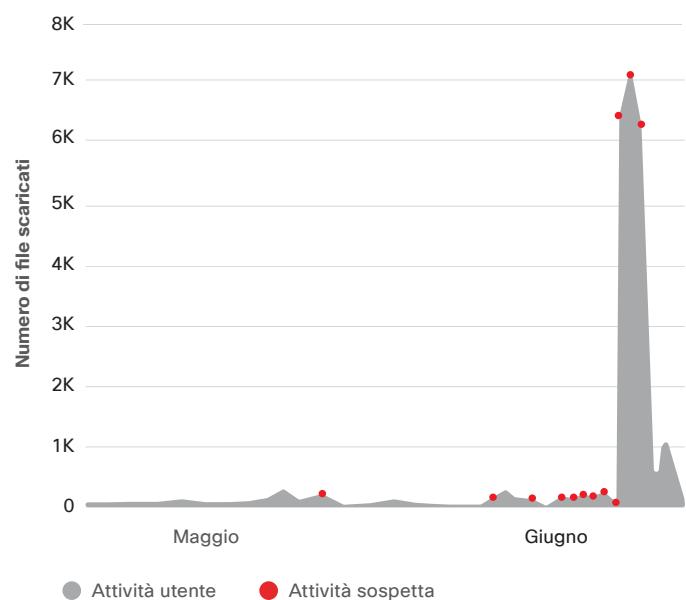
Fonte: Cisco Security Research

Una delle parole chiave più diffuse nei titoli dei documenti era "dati". Le parole chiave che comparivano più comunemente insieme alla parola "dati" erano "dipendente" e "cliente". Dei tipi di documenti scaricati, il 34% erano PDF e il 31% documenti di Microsoft Office (vedere la Figura 23).

L'applicazione di algoritmi di machine learning offre una visione più sfaccettata dell'attività degli utenti sul cloud che non si limita al numero di download. Nella nostra analisi, il 23% degli utenti è stato segnalato più di tre volte per download sospetti, solitamente iniziando con un piccolo numero di documenti. Il volume aumentava lievemente ogni volta e alla fine questi utenti hanno evidenziato picchi improvvisi e significativi di download (Figura 24).

Gli algoritmi di machine learning riescono a fornire una maggiore visibilità sul cloud e il comportamento degli utenti. Se gli addetti alla sicurezza possono iniziare a prevedere il comportamento degli utenti in merito ai download, possono risparmiare il tempo eventualmente necessario per eseguire indagini sul comportamento legittimo. Possono anche intervenire per fermare un potenziale attacco o incidente di esfiltrazione dei dati prima che si verifichi.

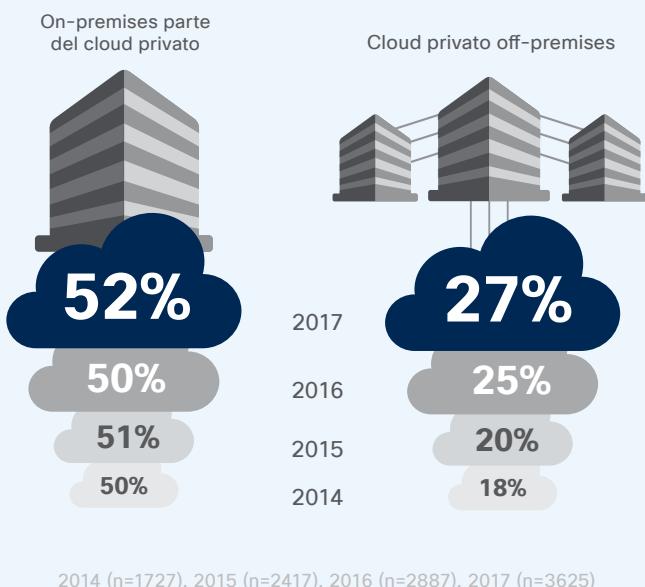
**Figura 24** Gli algoritmi di machine learning fotografano il comportamento di download degli utenti sospetti



## i Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018: la sicurezza vista come un vantaggio chiave delle reti in hosting nel cloud

Secondo lo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018, l'uso di infrastrutture cloud on-premise e pubbliche è in crescita, anche se molte aziende hanno ancora reti on-premise. Nello studio del 2017, il 27% degli esperti della sicurezza ha affermato di utilizzare cloud privati off-premises rispetto al 25% nel 2016 e al 20% nel 2015 (Figura 25). Per il 52% le reti sono on-premise su cloud privato.

**Figura 25** Un maggior numero di aziende utilizza cloud privati



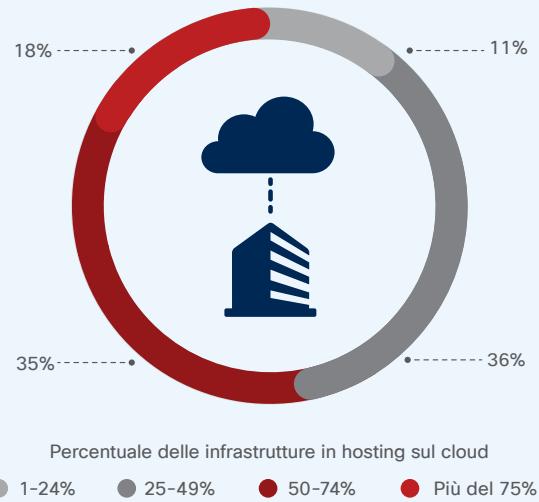
Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Delle aziende che utilizzano il cloud, il 36% ospita tra il 25 e il 49% della propria infrastruttura nel cloud, mentre il 35% ne ospita tra il 50 e il 74% (Figura 26).

Il vantaggio più diffuso offerto dalle reti in hosting nel cloud è la sicurezza, come indicano gli intervistati tra gli addetti alla sicurezza. Fra questi, il 57% ha dichiarato di ospitare reti nel cloud per la maggiore sicurezza dei dati, il 48% per la scalabilità e il 46% per la facilità di utilizzo (vedere la Figura 27).

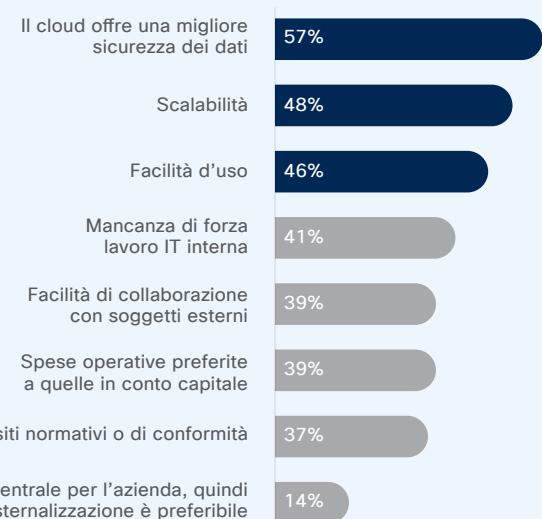
Gli intervistati hanno anche affermato che, con il trasferimento di un numero sempre più elevato di infrastrutture sul cloud, potrebbero decidere di investire in Cloud Access Security Broker (CASB) per aggiungere maggiore sicurezza agli ambienti cloud.

**Figura 26** Il 53% delle aziende ospita almeno la metà delle infrastrutture nel cloud



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 27** Il 57% ritiene che il cloud offre una maggiore sicurezza dei dati



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## ATTACCHI IoT E DDoS

*IoT è ancora in evoluzione, ma i criminali informatici stanno già sfruttando i punti deboli nella sicurezza dei dispositivi IoT per accedere ai sistemi, compresi quelli di controllo industriale che supportano infrastrutture critiche. Inoltre le botnet IoT crescono in termini di dimensioni e potenza e sono sempre più efficaci nello scatenare potenti attacchi che potrebbero compromettere gravemente Internet. Ed è proprio questo il loro scopo, come dimostra il fatto che gli autori di attacchi sfruttano sempre più il livello applicativo. Ma molti esperti della sicurezza non sono consapevoli o ignorano la minaccia rappresentata dalle botnet IoT. Le aziende continuano ad aggiungere dispositivi IoT ai loro ambienti IT, non considerando minimamente o per nulla la sicurezza, o peggio, non valutando quanti dispositivi IoT entrano in contatto con le reti. In questo modo consentono ai criminali informatici di prendere facilmente il comando di IoT.*

Poche aziende vedono le botnet IoT come una minaccia imminente, ma in effetti lo sono

Insieme a IoT, si espandono e si evolvono anche le botnet IoT. E a mano a mano che le botnet crescono e maturano, i criminali informatici le utilizzano per lanciare attacchi DDoS di portata e intensità crescenti. Radware, un partner Cisco, ha svolto un'analisi di tre delle più grandi botnet IoT, ovvero Mirai, Brickerbot e Hajime, nel *Report semestrale di Cisco sulla cybersecurity 2017* e rivisita l'argomento delle botnet IoT nel nostro ultimo report per sottolineare la gravità di questa minaccia.<sup>18</sup> La ricerca mostra che solo il 13% delle aziende ritiene che le botnet IoT rappresentino una grave minaccia per la propria attività nel 2018.

Le botnet IoT prosperano perché aziende e utenti implementano rapidamente dispositivi IoT a basso costo senza curarsi quasi per nulla della sicurezza. I dispositivi IoT sono sistemi basati su Linux e Unix, quindi sono spesso obiettivi di file binari in formato eseguibile e collegabile (ELF, Executable and Linkable Format). È anche meno impegnativo prenderne il

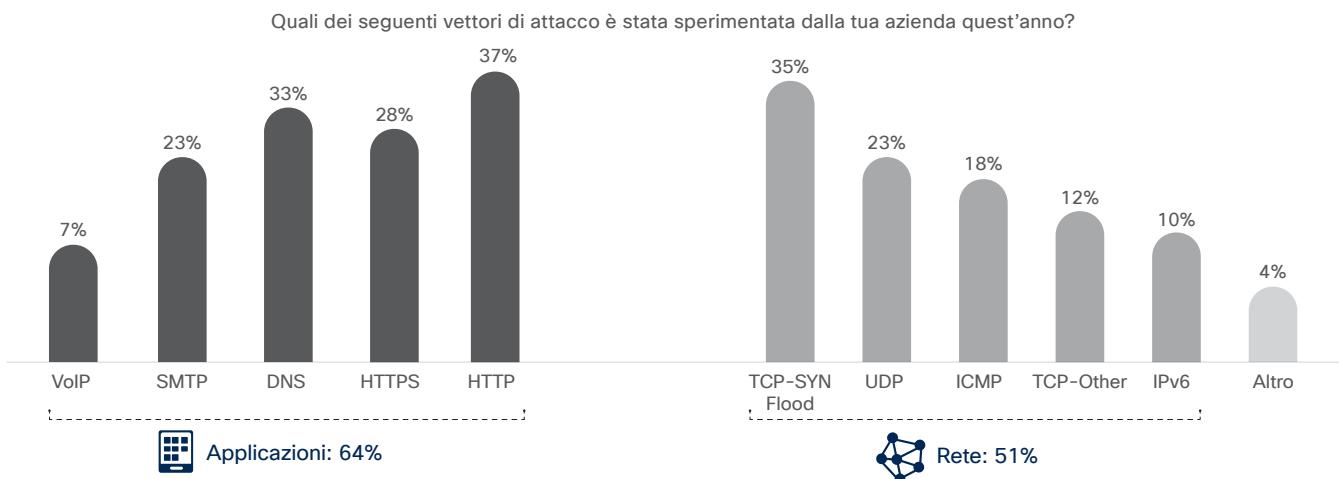
controllo rispetto a un PC, perciò per i criminali informatici è facile mettere insieme un grande esercito in poco tempo.

I dispositivi IoT operano 24 ore su 24 e possono essere chiamati in azione praticamente all'istante. E mentre gli hacker aumentano le dimensioni delle botnet IoT, investono in codice e malware sempre più sofisticato perpetrando attacchi DDoS sempre più avanzati.

### Gli attacchi DDoS alle applicazioni superano gli attacchi DDoS alla rete

Gli attacchi a livello delle applicazioni sono in aumento, mentre sono in calo gli attacchi a livello di rete (vedere la Figura 28). I ricercatori di Radware sospettano che questo cambiamento possa essere attribuito alla crescita delle botnet IoT. La tendenza è preoccupante perché il livello applicativo è molto diversificato e presenta numerosi dispositivi al suo interno, perciò questo genere di attacchi potrebbero potenzialmente arrestare grandi porzioni di Internet.

**Figura 28** Gli attacchi DDoS alle applicazioni sono aumentati nel 2017



Fonte: Radware

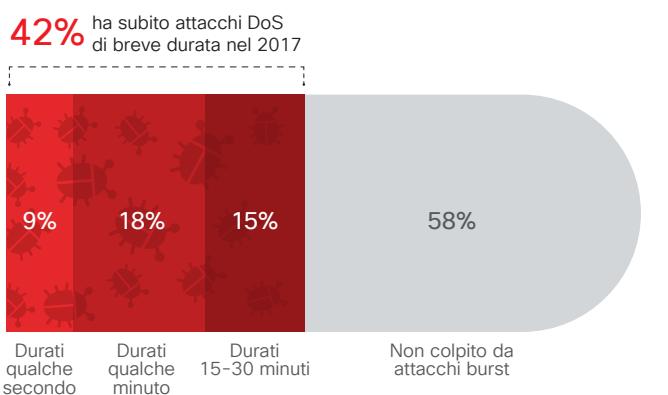
<sup>18</sup> Per maggiori dettagli sulla ricerca relativa alle botnet IoT di Radware, vedere "IoT: non fa in tempo a nascere, che le botnet IoT sono già arrivate", p. 39, *Report semestrale di Cisco sulla cybersecurity 2017*: [cisco.com/c/m/en\\_au/products/security/offers/cybersecurity-reports.html](http://cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html).

Secondo i ricercatori di Radware, un numero sempre maggiore di autori di attacchi colpisce il livello applicativo perché le opportunità di violazione nel livello di rete si sono ridotte. La creazione di botnet IoT richiede anche meno risorse rispetto alle botnet PC. In questo modo, gli hacker possono investire maggiori risorse nello sviluppo di codice e malware avanzato. Gli operatori della botnet multivettoriale Mirai, che è nota per gli attacchi avanzati al livello applicativo, sono tra quelli che fanno questo tipo di investimento.

### Gli “attacchi burst” crescono in termini di complessità, frequenza e durata

Una delle più significative tendenze degli attacchi DDoS che Radware ha osservato nel 2017 si è esplicata in un aumento degli attacchi burst brevi che stanno diventando sempre più complessi, frequenti e persistenti. Il 42% delle aziende oggetto dell’indagine di Radware ha subito questo tipo di attacco DDoS nel 2017 (Figura 29). Nella maggior parte degli attacchi, i burst ricorrenti sono durati solo alcuni minuti.

**Figura 29** Esperienza con attacchi DDoS in burst ricorrenti



Fonte: Radware

Le tattiche burst vengono usate in genere contro i siti Web e i provider di servizi di giochi, a causa della sensibilità dei loro utenti alla disponibilità del servizio e della loro incapacità di fronteggiare tali manovre di attacco. In questi attacchi burst puntuali o casuali che provocano raffiche di traffico elevato con una durata di giorni o addirittura settimane le aziende potrebbero non avere il tempo di reagire, quindi si possono verificare gravi interruzioni del servizio.

I ricercatori di Radware affermano che gli attacchi burst:

- Sono composti da più vettori mutevoli. Sono distribuiti geograficamente e si manifestano come una serie continua di SYN flood, ACK flood e User Datagram Protocol (UDP) flood precisi e ad alto volume su più porte.

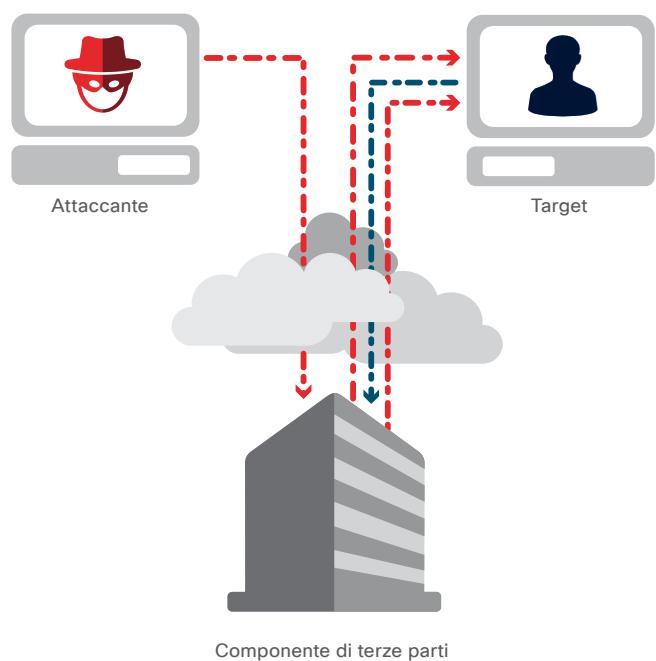
- Combinano attacchi ad alto volume con durata variabile: da 2 a 50 secondi di elevato traffico con intervalli di circa 5-15 minuti.
- Sono spesso combinati con altri attacchi DDoS di lunga durata.

### Crescita negli attacchi a riflessione e amplificazione

Un’altra tendenza degli attacchi DDoS che Radware ha osservato nel 2017 è la crescita degli attacchi DDoS a riflessione e amplificazione che si configurano come un vettore importante contro un ampio spettro di servizi. Secondo Radware, 2 imprese su 5 hanno subito un attacco a riflessione e amplificazione nel 2017. Un terzo di queste aziende ha riferito di non essere riuscita a mitigare questi attacchi.

Un attacco a riflessione e amplificazione utilizza un componente di terze parti potenzialmente legittimo per inviare traffico a un obiettivo, celando l’identità dell’hacker. Gli autori di attacchi inviano pacchetti ai server riflettori con l’indirizzo IP di origine impostato sull’IP dell’utente obiettivo. Questo consente di sovraccaricare indirettamente l’obiettivo dell’attacco di pacchetti di risposta, facendogli superare il limite di utilizzo delle risorse (vedere la Figura 30).

**Figura 30** Attacco a riflessione e amplificazione



Fonte: Radware

Affinché un attacco a riflessione e amplificazione vada a buon fine, i criminali informatici devono avere una capacità di larghezza di banda maggiore rispetto ai loro obiettivi. Con i server riflettori è possibile: l'autore dell'attacco riflette semplicemente il traffico da una o più macchine di terze parti. Poiché si tratta di server ordinari, questo tipo di attacco è particolarmente difficile da mitigare. Ecco alcuni esempi:

#### Attacchi DNS a riflessione e amplificazione

Questo sofisticato attacco denial of service sfrutta il comportamento di un server DNS per amplificare l'attacco. La richiesta DNS standard è più piccola della risposta DNS. In un attacco DNS a riflessione e amplificazione, l'autore dell'attacco sceglie con cura una query DNS che si traduce in una risposta lunga fino a 80 volte più della richiesta (ad esempio "ANY"). Invia questa query utilizzando una botnet ai server DNS di terze parti, falsificando l'indirizzo IP di origine con l'indirizzo IP dell'utente obiettivo. I server DNS di terze parti inviano la propria risposta all'indirizzo IP obiettivo. Con questa tecnica di attacco, una botnet relativamente piccola può generare un volume massiccio di risposte di grandi dimensioni verso l'obiettivo dell'attacco.

#### Riflessione NTP

Questo tipo di attacco ad amplificazione sfrutta server Network Time Protocol (NTP) pubblicamente accessibili per sovraccaricare di traffico UDP e rendere impotenti i responsabili della sicurezza. NTP è un vecchio protocollo di rete per la sincronizzazione dell'ora tra sistemi di computer su reti a commutazione di pacchetto. È ancora ampiamente usato in tutta Internet da computer desktop, server e persino telefoni per sincronizzare l'ora. Molte vecchie versioni di server NTP contengono un comando chiamato monlist che invia al richiedente un elenco che contiene fino a 600 voci degli ultimi host che si sono connessi al server interrogato.

Nello scenario più elementare l'autore dell'attacco invia ripetutamente la richiesta "get monlist" a un server NTP casuale e falsifica l'indirizzo IP di origine del server richiedente con quello del server obiettivo. Le risposte del server NTP vengono quindi indirizzate al server obiettivo causando un notevole aumento nel traffico UDP dalla porta di origine 123.

#### Riflessione SSDP

Questo attacco sfrutta il Simple Service Discovery Protocol (SSDP), che viene utilizzato per consentire ai dispositivi Universal-Plug-and-Play (UPnP) di trasmettere la loro esistenza. È utile anche per consentire il rilevamento e il controllo dei dispositivi e dei servizi collegati in rete, quali fotocamere, stampanti collegate in rete e molti altri tipi di apparecchiature elettroniche.

Una volta che un dispositivo UPnP è connesso a una rete e ha ricevuto un indirizzo IP, è in grado di comunicare i propri servizi ad altri computer nella rete inviando un messaggio in un IP multicast. Quando un computer riceve il messaggio di rilevamento relativo al dispositivo, invia una richiesta per una descrizione completa dei servizi del dispositivo. Il dispositivo UPnP quindi risponde direttamente al computer con un elenco completo di tutti i servizi che può offrire.

Come per gli attacchi DDoS NTP e DNS ad amplificazione, l'autore dell'attacco può utilizzare una piccola botnet per eseguire la richiesta finale relativa ai servizi. Dopodiché falsifica l'indirizzo IP di origine con l'indirizzo IP dell'utente obiettivo e indirizza le risposte direttamente alla vittima.

## Gli addetti alla sicurezza devono risolvere i “percorsi di falla”

Un “percorso di falla”, come definito dal partner Cisco Lumeta, è una violazione di policy o segmentazione oppure una connessione non autorizzata o non configurata correttamente creata verso Internet su una rete aziendale, anche dal cloud, che consente l'inoltro del traffico a una posizione su Internet, ad esempio un sito Web dannoso. Queste connessioni inaspettate possono verificarsi anche internamente tra due segmenti di rete diversi che non devono comunicare fra loro. Ad esempio, negli ambienti con infrastrutture critiche, un percorso di falla imprevisto tra i sistemi IT del reparto produttivo e della gestione potrebbe indicare attività dannose. Percorsi di falla possono derivare anche da router e switch configurati in modo improprio.

I dispositivi con autorizzazioni impostate in modo non corretto o che sono lasciati aperti e non gestiti sono vulnerabili agli attacchi. I dispositivi e le reti correlate ai sistemi IT fantasma o non autorizzati sono anch'essi terreno fertile per i criminali informatici per stabilire percorsi di falla perché tendono a essere non gestiti e privi di patch. Lumeta stima che circa il

40% di reti dinamiche, endpoint e infrastrutture cloud nelle aziende stia portando a significativi punti ciechi nelle infrastrutture e alla mancanza di riconoscimento in tempo reale per i team responsabili della sicurezza.

Il rilevamento dei percorsi di falla esistenti è fondamentale, in quanto tali percorsi possono essere sfruttati in qualsiasi momento. Tuttavia, è importante individuare in tempo reale i nuovi percorsi di falla che vengono creati perché sono indicatori immediati di compromissione e sono associati con gli attacchi più avanzati, tra cui il ransomware.

La recente analisi di Lumeta sull'infrastruttura IT di oltre 200 aziende in diversi settori sottolinea la carenza di visibilità degli endpoint. Mostra inoltre che numerose aziende sottostimano sensibilmente il numero di endpoint nei propri ambienti IT (vedere la Figura 31). La mancanza di consapevolezza circa il numero di dispositivi IoT abilitati per IP che sono connessi alla rete è spesso uno dei motivi principali della sottostima degli endpoint.

**Figura 31** Panoramica dei punti ciechi delle infrastrutture in vari settori

Clienti attuali di Lumeta	Pubblica amministrazione	Sanità	Ottimizzazione	Contabilità
Endpoint presunti	150.000	60.000	8000	600.000
Endpoint scoperti	170.000	89.860	14.000	1.200.000
Lacuna di visibilità degli endpoint	12%	33%	43%	50%
Reti non gestite	3278	24	5	771
Dispositivi di inoltro non autorizzati o non protetti	520	75	2026	420
Reti conosciute ma non raggiungibili	33.256	4	16.828	45
Percorsi di falla verso Internet identificati al momento dell'implementazione	3000	120	9400	220

Fonte: Lumeta

I ricercatori di Lumeta indicano che i percorsi di falla sono in aumento, soprattutto negli ambienti cloud, dove è minore la visibilità sulla rete e sono previsti meno controlli di sicurezza.

I malintenzionati non sempre utilizzano immediatamente i percorsi di falla che creano o trovano. Ritornano a questi canali in un secondo momento e li usano per installare malware o ransomware, trarre informazioni e molto altro. I ricercatori di Lumeta affermano che una delle ragioni per cui spesso i percorsi di falla non vengono rilevati è che i malintenzionati sono abili a crittografare e a nascondere la loro attività, ad esempio mediante TOR. Inoltre sono attenti e utilizzano i percorsi di falla con accortezza, in modo da non creare sospetti nei team addetti alla sicurezza.

I ricercatori di Lumeta affermano che le carenze nelle competenze dei team di sicurezza, ossia la mancanza di conoscenze fondamentali sulle reti, possono interferire con la capacità delle aziende di eseguire indagini e risolvere i problemi relativi ai percorsi di falla in modo tempestivo. Una migliore collaborazione tra i team di rete e sicurezza consente di accelerare le indagini e la risoluzione dei percorsi di falla.

Gli strumenti per l'automazione che forniscono il contesto di rete possono anche offrire indizi agli analisti della sicurezza su potenziali percorsi di falla. Inoltre l'attuazione di policy di segmentazione appropriate può aiutare i team responsabili della sicurezza a determinare rapidamente se una specifica comunicazione inaspettata tra reti o dispositivi sia dannosa.

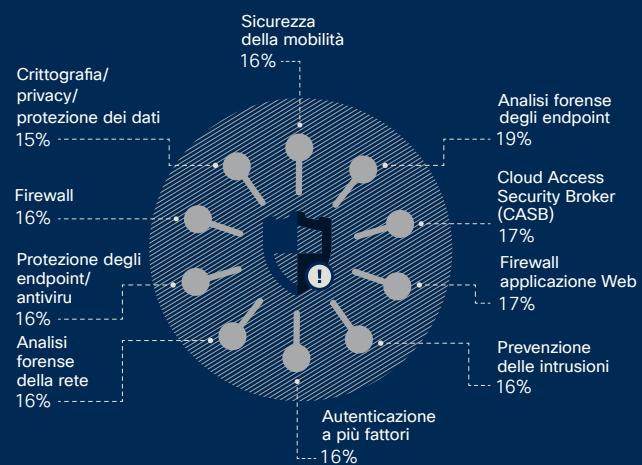
### Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018: la mancanza di personale addetto alla sicurezza impedisce a molte aziende di implementare nuove funzionalità informatiche

Gravi carenze di personale continuano a rappresentare un problema fondamentale per i responsabili della sicurezza. Come indicato in precedenza, la mancanza di competenze può interferire con la capacità di un'azienda di analizzare e risolvere certi tipi di minacce.

Inoltre, senza avere a disposizione i giusti esperti, gli addetti alla sicurezza non possono implementare nuove tecnologie e processi che potrebbero contribuire a rafforzare la loro postura della sicurezza (Figura 32).

Molti esperti della sicurezza intervistati per lo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018 hanno affermato che, idealmente, vorrebbero automatizzare o esternalizzare un numero maggiore delle loro attività di routine, in modo da reindirizzare il personale verso attività di più alto valore.

**Figura 32** Funzionalità chiave che verrebbero aggiunte dai responsabili della sicurezza se il livello dell'organismo migliorasse



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## Le vulnerabilità dei sistemi di controllo industriale mettono a rischio le infrastrutture critiche

I sistemi di controllo industriale (ICS) sono il cuore di ogni sistema di produzione e di controllo dei processi. I sistemi ICS si connettono ad altri sistemi elettronici che fanno parte del processo di controllo, creando un ecosistema altamente collegato di dispositivi vulnerabili che molti criminali informatici puntano a violare.

I malintenzionati che vogliono colpire i sistemi ICS per paralizzare le infrastrutture critiche s' impegnano attivamente nella ricerca e nella creazione di punti di accesso backdoor per facilitare futuri attacchi, come indica TrapX Security, un partner Cisco che sviluppa difese di cybersecurity basate su tecniche di inganno. Tra i potenziali autori di attacchi informatici ci sono esperti con conoscenze avanzate sui sistemi IT, le architetture ICS e i processi che supportano. Alcuni sanno anche programmare controller e sottosistemi di gestione del ciclo di vita dei prodotti (PLM, Product Lifecycle Management).

I ricercatori delle minacce di TrapX hanno recentemente condotto indagini su diversi attacchi informatici mirati ai sistemi ICS dei clienti evidenziando problemi imprevisti relativi alla difesa informatica dei sistemi ICS. Due degli incidenti descritti di seguito hanno avuto luogo nel 2017 e le relative indagini sono tuttora in corso.

### Obiettivo: grande azienda internazionale di trattamento acque e rifiuti

I criminali informatici hanno utilizzato il server demilitarized zone (DMZ) dell'azienda come punto di accesso per violare la rete interna. Il team dedicato alla gestione operativa della sicurezza ha ricevuto avvisi dalla tecnologia integrata nella rete DMZ che rileva le tecniche di inganno. Questa sotto-rete fisica o logica collega le reti interne alle reti non attendibili, come Internet, proteggendo altre infrastrutture interne. L'indagine ha rilevato che:

- Il server DMZ era stato violato a causa di un errore di configurazione che consentiva le connessioni RDP.
- Il server era stato violato ed era controllato da diversi indirizzi IP, collegati ad hacktivist politici ostili allo stabilimento.

- I criminali informatici erano riusciti a lanciare numerosi attacchi importanti contro molti altri stabilimenti dell'azienda dalla rete interna violata.

### Obiettivo: impianto elettrico

Le risorse critiche di questo impianto elettrico comprendono un'infrastruttura ICS molto grande e i necessari componenti SCADA (Supervisory Control And Data Acquisition) che gestiscono ed eseguono i processi. L'impianto è considerato infrastruttura nazionale critica e soggetto a controllo e vigilanza da parte dell'agenzia di sicurezza nazionale responsabile. È perciò considerato un impianto ad alta sicurezza.

Il CISO aveva optato per l'implementazione di una tecnologia di protezione da tecniche di inganno per tutelare le risorse IT standard dell'impianto da attacchi ransomware. La tecnologia è stata distribuita anche all'interno dell'infrastruttura ICS. Poco dopo, il team dedicato alla gestione operativa della sicurezza ha ricevuto diversi avvisi che indicavano una violazione dei sistemi operativi dell'impianto dell'infrastruttura critica. Dall'indagine che il team ha immediatamente svolto è emerso che:

- Un dispositivo presente nella rete di controllo dei processi stava tentando di interagire con trappole che erano camuffate da controller PLM. Si trattava di un tentativo concreto di mappare e comprendere l'esatta natura di ogni controller PLM della rete.
- Il dispositivo compromesso normalmente avrebbe dovuto essere chiuso, ma un fornitore di manutenzione non aveva chiuso la connessione al termine del suo intervento. Questa svista aveva lasciato la rete di controllo dei processi vulnerabile agli attacchi.
- Le informazioni che i criminali informatici stavano raccogliendo erano esattamente il tipo richiesto per interrompere l'attività dell'impianto e potenzialmente causare gravi danni alla continuità operativa dell'impianto stesso.

## Suggerimenti

Molte violazioni del sistema ICS iniziano con la compromissione di server e risorse di elaborazione vulnerabili all'interno della rete IT aziendale. I ricercatori delle minacce di TrapX raccomandano alle aziende di mettere in atto le seguenti azioni per ridurre i rischi e garantire l'integrità operativa all'interno dei loro stabilimenti:

- Controllare i fornitori e i sistemi e verificare che tutti gli aggiornamenti e le patch siano applicati immediatamente (se le patch non sono disponibili, considerare la migrazione a una nuova tecnologia).
- Ridurre l'uso di chiavette di memoria USB e unità DVD.
- Isolare i sistemi ICS dalle reti IT non consentendo alcuna connessione diretta tra i due, il che include connessioni di rete, laptop e chiavette di memoria.

- Implementare policy che limitino fortemente l'uso delle reti ICS per tutte le attività diverse dalle operazioni essenziali. Ridurre l'accessibilità alle postazioni di lavoro e ai monitor ICS con accesso a un browser Internet esterno. Tenere conto che queste policy falliranno e definire una pianificazione alternativa.
- Ricercare ed eliminare tutte le password integrate o predefinite nella rete di produzione. Inoltre, ove possibile, implementare l'autenticazione a due fattori.
- Rivedere i piani di disaster recovery dopo un attacco informatico importante.

Per ulteriori case study, vedere la ricerca di TrapX Security, *Anatomy of an Attack: Industrial Control Systems Under Siege*.

## i Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018: più attacchi OT e IoT all'orizzonte

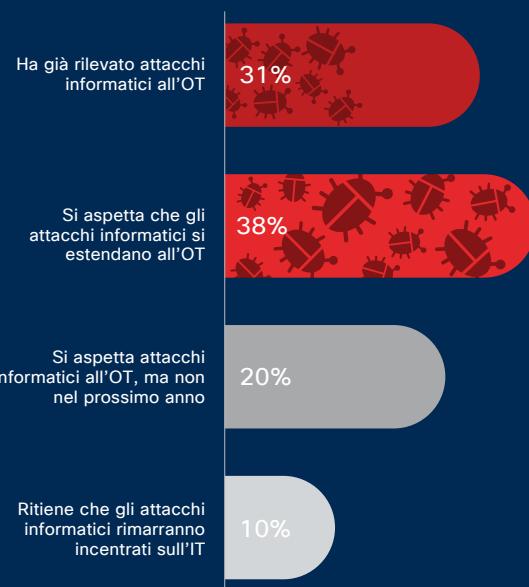
Gli attacchi diretti alla tecnologia operativa (OT), come i dispositivi ICS e IoT, sono ancora abbastanza inconsueti, tanto che molti esperti della sicurezza non li hanno ancora sperimentati in prima persona. Ma secondo la ricerca condotta per lo **Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018**, gli esperti della sicurezza si aspettano senza dubbio di subire tali attacchi e stanno cercando di capire come reagire.

Sono consapevoli che spesso questi sistemi hanno poche protezioni e software senza patch e non aggiornati, il che li rende vulnerabili agli attacchi.

“Usiamo ancora dispositivi OT che hanno 25 anni e compressori e macchine che ne hanno 40”, ha affermato un intervistato. “I professionisti IT vengono consultati quando bisogna pianificare. [Dicono:] ‘Dimmi quando Windows X non sarà più supportato’ oppure ‘Ehi, questa versione di Oracle è vicina alla fine del ciclo di vita [EOL]’. Niente di simile è possibile nell'ambiente OT”.

Pochi esperti della sicurezza possono parlare con certezza di questioni relative alla protezione di OT nelle proprie aziende. Ciò in parte deriva dal fatto che non hanno o non prevedono di aggiungere molta OT, oppure perché le implementazioni di IoT sono nuove. Di questi esperti, il 31% ha dichiarato che le proprie aziende hanno già subito attacchi informatici all'infrastruttura OT, mentre il 38% ha affermato che si aspetta che gli attacchi si estenderanno dall'IT all'OT nel corso del prossimo anno (Figura 33).

**Figura 33** Il 31% delle aziende ha subito attacchi informatici all'infrastruttura OT



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## VULNERABILITÀ E PATCHING

*Nel caos dei problemi di sicurezza, i responsabili della sicurezza possono perdere di vista le vulnerabilità che interessano la loro tecnologia. Ma si può stare certi che i criminali informatici sono sempre attentissimi a calcolare come sfruttare questi potenziali punti deboli per lanciare attacchi.*

*Un tempo applicare le patch per le vulnerabilità note entro 30 giorni era considerata una best-practice. Adesso, se si attende così tanto, potrebbe aumentare il rischio di attacco per l'azienda, perché i criminali informatici si muovono più velocemente nel divulgare e utilizzare exploit di vulnerabilità attivi. Le aziende inoltre non devono assolutamente trascurare lacune della sicurezza esigue ma significative, che gli hacker potrebbero sfruttare, soprattutto nella fase di riconoscimento in vista di un attacco quando sono alla ricerca di vie di accesso ai sistemi.*

Fra le principali vulnerabilità del 2017 ci sono gli errori di overflow del buffer e Apache Struts

Gli errori di overflow del buffer sono in cima alla lista delle vulnerabilità Common Weakness Enumeration (CWE) rilevate da Cisco nel 2017, seppur altre categorie abbiano mostrato

aumenti e diminuzioni. Le vulnerabilità di convalida dell'input sono aumentate, mentre sono diminuiti gli errori di buffer (Figura 34).

**Figura 34** Attività per categoria di minacce CWE

Categoria della minaccia	Gen.-Sett. 2016	Gen.-Sett. 2017	Modifica
CWE-119: errori di buffer	493	403	(-22%)
CWE-20: convalida dell'input	227	268	+15%
CWE-264: autorizzazioni, privilegi e accesso	137	163	+18%
CWE-200: perdita/divulgazione di informazioni	125	250	+100%
CWE-310: problemi di crittografia	27	17	(-37%)
CWE-78: inserimento di comandi del sistema operativo	7	15	+114%
CWE-59: visita di collegamenti	5	0	

Fonte: Cisco Security Research

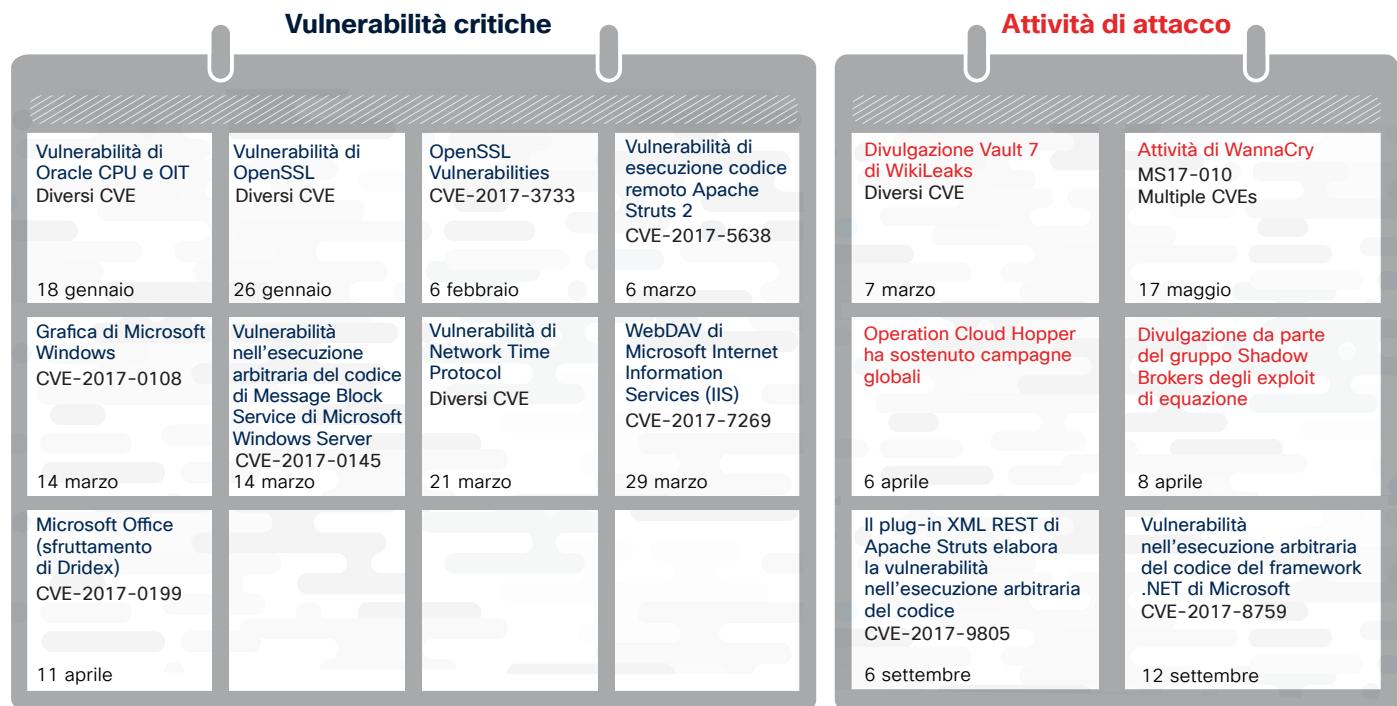
Nell'esame degli avvisi critici (Figura 35), le vulnerabilità di Apache Struts sono risultate ancora prevalenti nel 2017. Apache Struts è un framework open source molto diffuso per la creazione di applicazioni Java. Le vulnerabilità di Apache Struts sono state implicate in violazioni della sicurezza verificatesi nel 2017 che hanno coinvolto importanti broker di dati.

Mentre Apache tende a identificare le vulnerabilità e a fornire le patch rapidamente, può essere impegnativo applicare patch a soluzioni di infrastruttura quali Apache Struts senza

compromettere le prestazioni di rete. Come è stato indicato in precedenti report di Cisco sulla sicurezza,<sup>19</sup> le vulnerabilità del software open source o di terze parti possono richiedere patch manuali, non applicabili con la stessa frequenza delle patch automatizzate dei fornitori di software standard. In questo contesto i malintenzionati hanno più tempo per per lanciare i loro attacchi.

La scansione approfondita dei sistemi operativi fino a livello della libreria o del singoli file può fornire alle aziende gli inventari dei componenti delle soluzioni open source.

**Figura 35** Avvisi critici e attività di attacco



Fonte: Cisco Security Research



Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

19 Report semestrale di Cisco sulla cybersecurity 2017: [cisco.com/c/m/en\\_au/products/security/offers/cybersecurity-reports.html](http://cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html).

## Le vulnerabilità di IoT e libreria si sono fatte più minacciose nel 2017

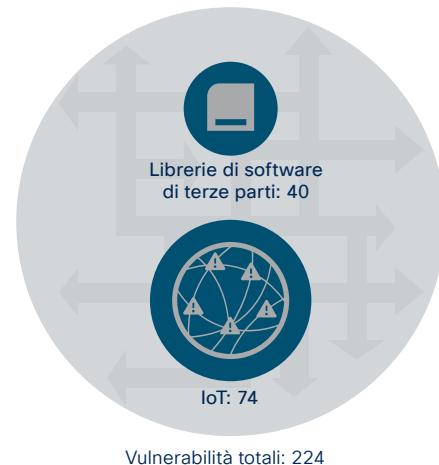
Tra il 1° ottobre 2016 e il 30 settembre 2017, i ricercatori delle minacce di Cisco hanno scoperto 224 nuove vulnerabilità in prodotti non-Cisco, di cui 40 sono state collegate con le librerie software di terze parti incluse in questi prodotti e 74 con dispositivi IoT (Figura 36).

Il numero relativamente elevato di vulnerabilità nelle librerie evidenzia la necessità di esaminare in modo più approfondito le soluzioni di terze parti che forniscono il framework per molte reti aziendali. Gli addetti alla sicurezza devono presupporre che le librerie software di terze parti possono essere obiettivi per i criminali informatici: non è sufficiente assicurarsi di utilizzare l'ultima versione del software o che non siano state segnalate CVE (vulnerabilità comuni) aperte. I team di sicurezza devono controllare frequentemente se sono state rilasciate patch e rivedere le procedure di sicurezza dei fornitori terzi. I team possono, ad esempio, richiedere che i fornitori offrano dichiarazioni sul ciclo di vita di sviluppo sicuro.

Un'altra best-practice per vagliare i software di terze parti è assicurarsi che le funzioni di aggiornamento automatico o di controllo degli aggiornamenti siano eseguite in modo sicuro. Ad esempio, quando viene avviato un aggiornamento, gli esperti della sicurezza devono essere certi che la comunicazione per tale software avvenga su un canale sicuro (ad esempio SSL) e che il software sia provvisto di firma

digitale. Entrambe queste condizioni sono imprescindibili: se vengono utilizzate solo le firme digitali, senza un canale protetto, l'autore dell'attacco potrebbe intercettare il traffico e sostituire un aggiornamento con una versione precedente del software provvista di firma digitale ma contenente vulnerabilità; se invece ci si limita a utilizzare un canale sicuro, l'hacker potrebbe compromettere il server di aggiornamento del fornitore e sostituire l'aggiornamento con malware.

**Figura 36** Vulnerabilità di IoT e libreria di terze parti



Fonte: Cisco Security Research

### i Vulnerabilità Spectre e Meltdown: la preparazione proattiva può accelerare la risoluzione

L'annuncio di gennaio 2018 sulle vulnerabilità Spectre e Meltdown, che permetterebbero ai criminali informatici di compromettere i dati su piattaforme che eseguono processori di computer di nuova generazione, ha sollevato preoccupazioni riguardo alla capacità degli esperti della sicurezza di proteggere i dati dagli attacchi. Le vulnerabilità consentirebbero agli autori degli attacchi di visualizzare i dati delle applicazioni in memoria sul chipset, con il potenziale di un danno diffuso, poiché i microprocessori colpiti si trovano dappertutto, dai cellulari all'hardware dei server.

Le minacce presentate dalle vulnerabilità Spectre e Meltdown evidenziano l'importanza di comunicare alle aziende di sicurezza le possibili soluzioni, come le patch, e di accertarsi che i fornitori terzi, ad esempio i vendor di cloud e della filiera di approvvigionamento, aderiscano alle migliori prassi per porre rimedio alle lacune nella sicurezza poste da tali vulnerabilità. I team di Product Security Incident Response, detti PSIRT (come Cisco PSIRT), sono pensati per rispondere rapidamente agli annunci di vulnerabilità, fornire le patch e dare consigli ai clienti su come evitare rischi.

Le aziende devono avere un piano per affrontare vulnerabilità come Spectre e Meltdown, invece che sperare che non accadano. La chiave è essere pronti per tali annunci e disporre di sistemi in grado di mitigare il potenziale danno. Ad esempio, i team di sicurezza devono inventariare in modo proattivo i dispositivi in loro controllo e documentare le configurazioni delle funzionalità in uso, poiché alcune vulnerabilità dipendono dalle configurazioni e hanno un impatto sulla sicurezza solo quando vengono attivate determinate funzionalità.

I team di sicurezza dovrebbero anche chiedere ai fornitori terzi, come i provider di servizi cloud, di informarli sui loro processi di aggiornamento e patching. Le aziende devono pretendere trasparenza dai provider di servizi cloud relativamente a come pongono rimedio a tali vulnerabilità, e a quanto velocemente rispondono agli avvisi. Ma indefinitiva, la responsabilità della rapidità di intervento ricade sulle aziende stesse: devono comunicare con le organizzazioni PSIRT e stabilire processi per rispondere rapidamente alle vulnerabilità.

**Per ulteriori informazioni, leggere il post del blog di Talos su Spectre e Meltdown.**

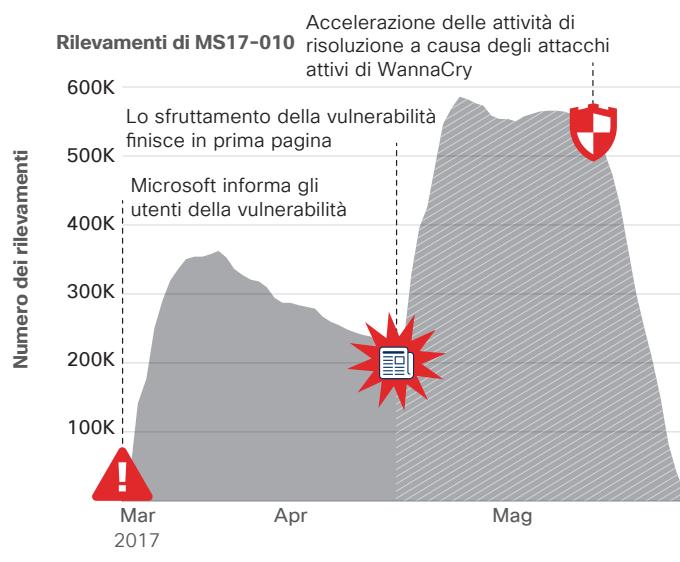
## Gli exploit attivi accelerano la corsa alla risoluzione, ad esclusione dei dispositivi IoT

Qualys, Inc., un partner di Cisco e fornitore di soluzioni di sicurezza e conformità basate su cloud, ha esaminato retrospettivamente il comportamento di gestione delle patch da parte delle aziende prima e dopo la campagna WannaCry che ha colpito molte società in tutto il mondo nel maggio 2017.

Il cryptoworm ransomware WannaCry, che molti esperti di sicurezza credono sia stato progettato per cancellare dati, ha approfittato di una vulnerabilità di sicurezza di Microsoft Windows chiamata EternalBlue, che è stata individuata dal gruppo di hacker Shadow Brokers a metà aprile 2017. (Per ulteriori informazioni su questo argomento, vedere "Sono lì in agguato e, nel 2018, gli addetti alla sicurezza dovranno prepararsi ad affrontare nuove minacce basate sulla rete e autopropaganti", a pagina 6.)

Il 14 marzo 2017 Microsoft ha rilasciato un aggiornamento di sicurezza (MS17-010) avvisando gli utenti di una vulnerabilità critica nel suo Microsoft Windows SMB Server. La Figura 37 mostra che il numero di dispositivi rilevati che presentano la vulnerabilità raggiunge il picco e poi diminuisce gradualmente tra metà marzo e metà aprile, mano a mano che le aziende analizzano i loro sistemi e applicano la patch.

**Figura 37** Il comportamento di patching prima e dopo la campagna di WannaCry



Fonte: Qualys

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](https://cisco.com/go/acr2018graphics)

Però, un numero significativo di dispositivi era ancora senza patch a metà aprile. Successivamente, il 14 aprile, Shadow Brokers ha rilasciato l'exploit per colpire la vulnerabilità nota in varie versioni di Microsoft Windows. La Figura 37 mostra che, poco dopo, il numero di dispositivi rilevati con quella vulnerabilità è quasi raddoppiato. Questo è successo quando le aziende hanno appreso dell'exploit e del suo potenziale impatto sia sulle versioni supportate che non supportate di Windows attraverso un controllo remoto di Qualys che ha utilizzato una porzione del codice di exploit.

Ma anche dopo il rilascio dell'exploit, il patching non è stato eseguito diffusamente fino a metà maggio, quando l'attacco WannaCry ha fatto notizia in tutto il mondo. La Figura 37 mostra la curva di risoluzione ripida dopo quella campagna. A fine maggio erano pochi i dispositivi senza la patch.

La ricerca di Qualys sul comportamento di patching dei suoi clienti indica che ci vuole un grande evento per motivare molte aziende ad applicare patch per vulnerabilità critiche: la consapevolezza di un exploit attivo non è sufficiente per accelerare la risoluzione. Nel caso della campagna di WannaCry le imprese avevano accesso alla patch per la vulnerabilità di Microsoft già da due mesi prima che gli attacchi ransomware si verificassero.

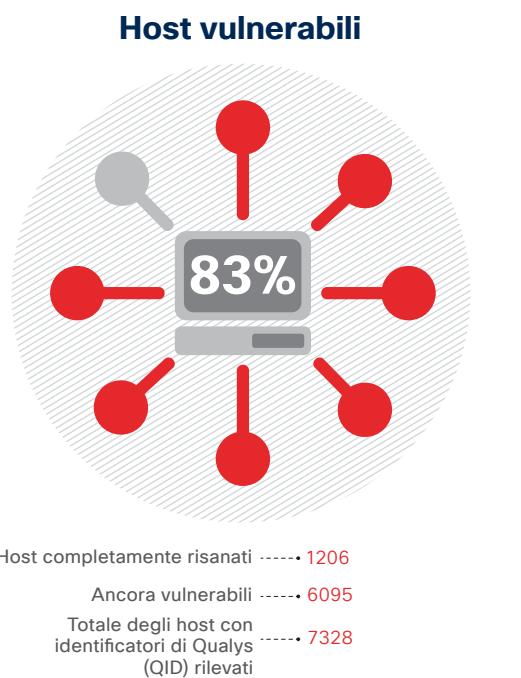
Un altro fattore, secondo quanto descritto dai ricercatori di Lumeta, partner di Cisco e Qualys, era che gli endpoint IT sconosciuti, non gestiti, non autorizzati e fantasma sono stati lasciati senza patch e i criminali informatici sono riusciti a sfruttare questi punti ciechi. Non conoscendo questi sistemi, la scansione delle vulnerabilità non è riuscita a valutare e raccomandare le patch, lasciandoli vulnerabili a WannaCry.

## Il patching è ancora più lento, o del tutto assente, per i dispositivi IoT

Qualys ha esaminato anche le tendenze di patching per i dispositivi IoT. I dispositivi del campione includevano serrature di porte, pannelli di allarme antincendio, lettori di schede e sistemi HVAC basati su IP.

I ricercatori hanno esaminato in modo specifico dispositivi IoT vulnerabili a diverse minacce note, tra cui il malware Devil's Ivy che sfrutta una vulnerabilità in una porzione di codice chiamata gSOAP, molto usata in prodotti di sicurezza fisici, e Mirai, una botnet IoT che si connette alle macchine obiettivo attraverso attacchi brute force contro server Telnet.

**Figura 38** Tendenze nel patching dei dispositivi IoT



Fonte: Qualys

Qualys ha rilevato 7328 dispositivi in totale, ma solo 1206 sono stati corretti (vedere la Figura 38). Pertanto, si può concludere che l'83% dei dispositivi IoT del campione ha ancora vulnerabilità critiche. Se Qualys non ha rinvenuto alcuna evidenza di malintenzionati intenti a colpire attivamente tali vulnerabilità, le aziende erano ancora passibili di attacchi. Tuttavia, esse non sembrano motivate ad accelerare il processo di risoluzione.

Secondo Qualys, sono diversi i motivi che soggiacciono all'inerzia nell'applicazione delle patch. Ad esempio, alcuni dispositivi potrebbero non essere aggiornabili. Altri potrebbero richiedere il supporto diretto da parte del fornitore. Inoltre, non è sempre chiaro chi all'interno dell'azienda sia tenuto a occuparsi della manutenzione dei dispositivi IoT. Ad esempio, un team di progettazione che si occupa del sistema HVAC dell'azienda può non essere consapevole dei rischi IT che potrebbero interessare tale sistema o persino che il sistema è basato su IP.

Più preoccupante, tuttavia, è il numero esiguo di dispositivi IoT che Qualys ha rilevato. Verosimilmente il numero effettivo è molto più elevato, perché le aziende semplicemente non sanno quanti dispositivi IoT sono connessi alla loro rete. Questa mancanza di visibilità mette tali dispositivi a serio rischio di compromissione (per ulteriori informazioni su questo argomento, vedere a [pagina 34](#)).

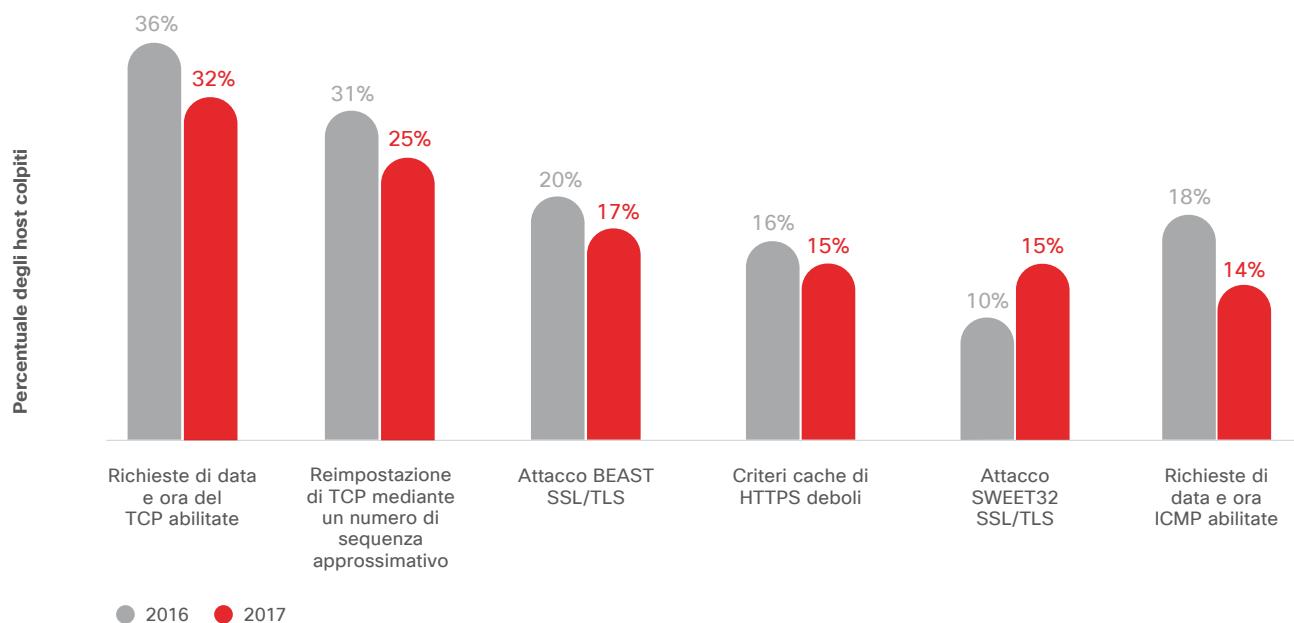
Un primo passo per affrontare il problema è inventariare tutti i dispositivi IoT sulla rete. Le aziende possono quindi determinare se i dispositivi sono analizzabili e ancora supportati dai fornitori e quali dipendenti della società li possiedono e li usano. Le aziende possono anche migliorare la sicurezza IoT trattando tutti i dispositivi IoT come gli altri dispositivi di elaborazione in modo da garantire che ricevano gli aggiornamenti firmware e la regolare applicazione delle patch.

## Le vulnerabilità più comuni sono a bassa gravità ma ad alto rischio

Spesso le aziende lasciano irrisolte le vulnerabilità a bassa gravità per anni perché non sanno che esistono o non le considerano rischi significativi, come indicano gli esperti di sicurezza di SAINT Corporation, società di soluzioni di sicurezza partner di Cisco. Tuttavia, queste lacune della sicurezza, esigue ma significative, potrebbero fornire vie di accesso al sistema agli autori degli attacchi.

I ricercatori di SAINT hanno esaminato i dati di esposizione a vulnerabilità raccolti da oltre 10.000 host nel 2016 e nel 2017. La società ha sviluppato un elenco delle principali vulnerabilità individuate più frequentemente in tutte le aziende dello studio, rilevando che le vulnerabilità di bassa gravità si verificano più spesso (vedere la Figura 39). (Nota: alcune aziende incluse nella ricerca avevano più di un host).

**Figura 39** Vulnerabilità a basso rischio rilevate più spesso, 2016-2017



Fonte: SAINT Corporation

Di seguito viene presentato un approfondimento sulle vulnerabilità di bassa gravità presentate nella Figura 39 e sui motivi per cui potrebbero essere preziose per i malintenzionati:

#### **Richieste di data e ora del TCP abilitate**

Le informazioni su data e ora del TCP permettono di sapere da quanto tempo una macchina è in esecuzione o quando è stata riavviata l'ultima volta, il che potrebbe aiutare gli autori degli attacchi a capire quali tipi di vulnerabilità risolvibili con patch potrebbero essere sfruttate. Inoltre, i programmi software possono utilizzare data e ora del sistema come valore di inizializzazione di un generatore di numeri casuali per la creazione di chiavi di crittografia.

#### **Reimpostazione di TCP mediante un numero di sequenza approssimativo**

Gli autori di attacchi remoti possono indovinare i numeri di sequenza e causare un attacco denial of service alle connessioni TCP persistenti iniettando ripetutamente un pacchetto TCP RST, soprattutto nei protocolli che utilizzano connessioni longeve, come il Border Gateway Protocol.

#### **Attacco “BEAST”**

I criminali informatici possono utilizzare la vulnerabilità Browser Exploit Against SSL/TLS (BEAST) per lanciare un attacco man-in-the-middle (MiTM) essenzialmente finalizzato a “leggere” contenuto protetto che viene scambiato tra le parti. (Nota: questo è un attacco complicato da eseguire, perché l'hacker deve anche avere il controllo del browser sul lato client per leggere e inserire i pacchetti di dati molto rapidamente).

I ricercatori di sicurezza di SAINT non hanno rilevato hacker che sfruttavano attivamente queste vulnerabilità di bassa gravità nella loro analisi.

Le vulnerabilità illustrate nella Figura 39 sono note alla community degli esperti di sicurezza, ma alcune di esse non sarebbero in genere individuate o segnalate automaticamente come errore nel controllo di conformità di routine, ad esempio un controllo PCI DSS (Payment Card Industry Data Security Standard). Non sono infatti vulnerabilità critiche secondo gli standard di quel settore e ogni settore valuta la criticità delle vulnerabilità in modo diverso.

Inoltre, la maggior parte delle vulnerabilità frequenti a bassa gravità mostrate nella Figura 39 non possono essere corrette facilmente o non possono essere affatto corrette attraverso la gestione delle patch, perché derivano da problemi di configurazione o problemi di certificato di sicurezza (ad esempio cifrature SSL deboli o un certificato SSL autofirmato).

Le aziende devono agire prontamente per risolvere le vulnerabilità di bassa gravità che possono presentare rischi. Devono valutare e identificare le priorità di risoluzione a seconda della propria percezione del rischio, piuttosto che basarsi su valutazioni di terze parti o sull'uso parziale di un sistema di punteggio, ad esempio un punteggio su base CVSS, o una determinata valutazione di conformità. Solo le aziende conoscono i propri ambienti specifici e le proprie strategie di gestione dei rischi.

# Parte II: il panorama della difesa

## Parte II: il panorama della difesa

Sappiamo che gli autori di attacchi sviluppano e adattano le loro tecniche a un ritmo più veloce rispetto a quello dei responsabili della sicurezza. Usano anche come armi e testando sul campo gli exploit, le strategie di evasione e le proprie competenze in modo da lanciare attacchi di portata sempre maggiore. Quando inevitabilmente i criminali informatici colpiranno le loro aziende, i responsabili della sicurezza saranno preparati? E quanto velocemente riusciranno ad effettuare il ripristino? Ciò dipende in gran parte dalle azioni che stanno adottando adesso per rafforzare la propria postura della sicurezza.

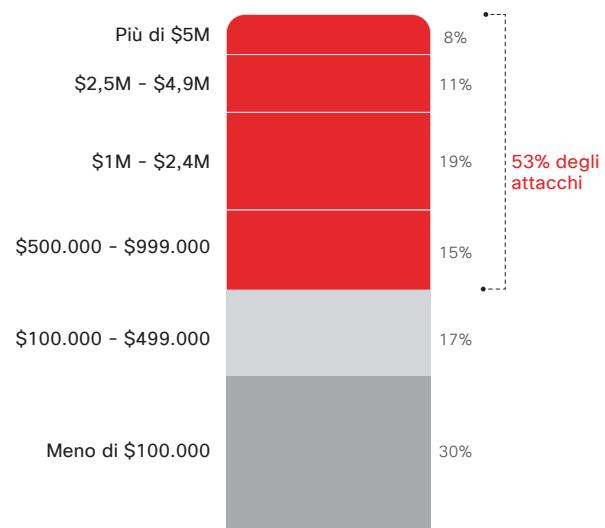
*Dalla ricerca per lo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018 è emerso che gli addetti alla sicurezza hanno molto lavoro da fare e molte sfide da superare. Per valutare le opinioni degli addetti alla difesa sullo stato della sicurezza nelle rispettive aziende, abbiamo chiesto a CISO (Chief Information Security Officer) e manager delle operazioni di sicurezza (SecOps), in molti paesi e in aziende di varie dimensioni, di illustrare le risorse e le procedure di sicurezza di cui dispongono.*

*Lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2018 offre informazioni dettagliate sulle procedure di sicurezza attualmente in uso e una comparazione di questi risultati con quelli riportati negli studi del 2017, 2016 e 2015. La ricerca ha coinvolto più di 3600 intervistati in 26 paesi.*

### Il costo degli attacchi

Il timore di violazioni si fonda sul costo economico degli attacchi, che non è più una cifra ipotetica. Le violazioni causano veri e propri danni economici alle aziende e ci possono volere mesi o anni per porvi rimedio. Secondo gli intervistati dello studio, più della metà (53%) degli attacchi ha causato danni finanziari superiori a 500.000 dollari, comprese, tra l'altro, perdite di entrate, clienti, opportunità e costi vivi (Figura 40).

**Figura 40** Il 53% degli attacchi provoca danni pari ad almeno \$500.000



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

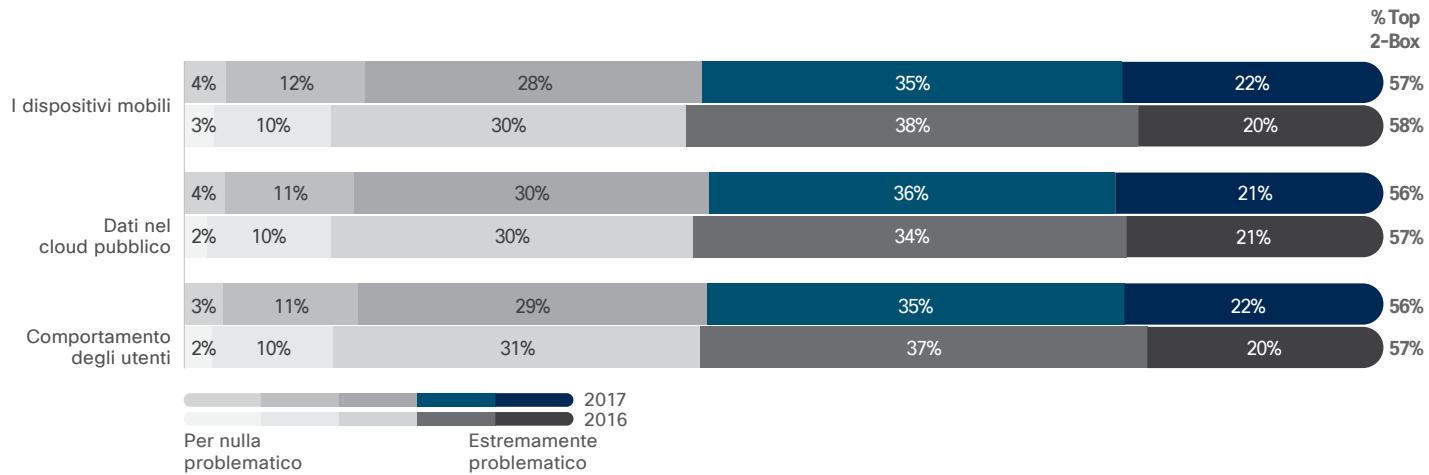
Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](https://cisco.com/go/acr2018graphics)

## Sfide e ostacoli

Nelle azioni dispiegate a protezione delle proprie aziende, i team di sicurezza si trovano dinanzi a molti ostacoli. Le aziende devono difendere diverse aree e funzioni, un aspetto che rende ancor più difficili le sfide della sicurezza. Le aree e

le funzioni più impegnative da difendere sono i dispositivi mobili, i dati nel cloud pubblico e il comportamento degli utenti (Figura 41).

**Figura 41** Aree più impegnative da difendere: dispositivi mobili e dati nel cloud



Fonente: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

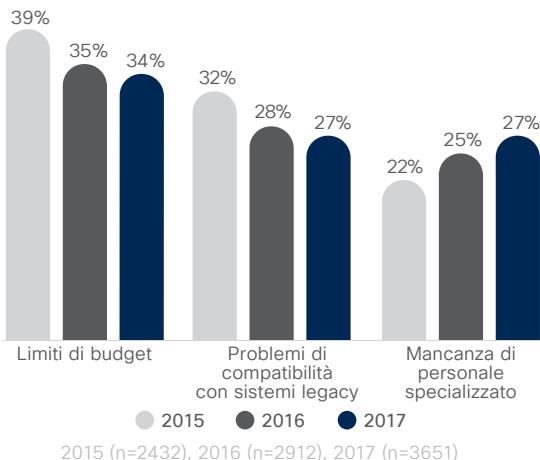


Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

Gli esperti della sicurezza citano il budget, l'interoperabilità e il personale come vincoli fondamentali nella gestione della sicurezza (Figura 42). Tra le sfide per l'adozione di tecnologia e processi di sicurezza avanzata viene menzionata anche la mancanza di personale specializzato: nel 2017 il 27% ha indicato la mancanza di risorse qualificate come un ostacolo, rispetto al 25% nel 2016 e al 22% nel 2015.

La mancanza di esperti è indicata come ostacolo principale in tutti i settori e in tutte le aree. "Se avessi una bacchetta magica e potessi impiegare il 10% in più di persone per alleviare in parte il carico di coloro che sono davvero sotto pressione a causa della forte domanda nelle loro particolari aree di servizio, sarei molto, molto felice", ha dichiarato un CISO di una grande società di servizi professionali.

## **Figura 42** Il più grande ostacolo alla sicurezza: i limiti di budget



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Mentre la mancanza di personale specializzato rappresenta una sfida continua, le aziende riferiscono che stanno cercando e assumendo più risorse per i team di sicurezza. Nel 2017 il numero medio di esperti della sicurezza nelle aziende era pari a 40; questo dato segna un aumento significativo rispetto al 2016, quando si attestava a 33 (Figura 43).

**Figura 43** Le aziende assumono più esperti della sicurezza



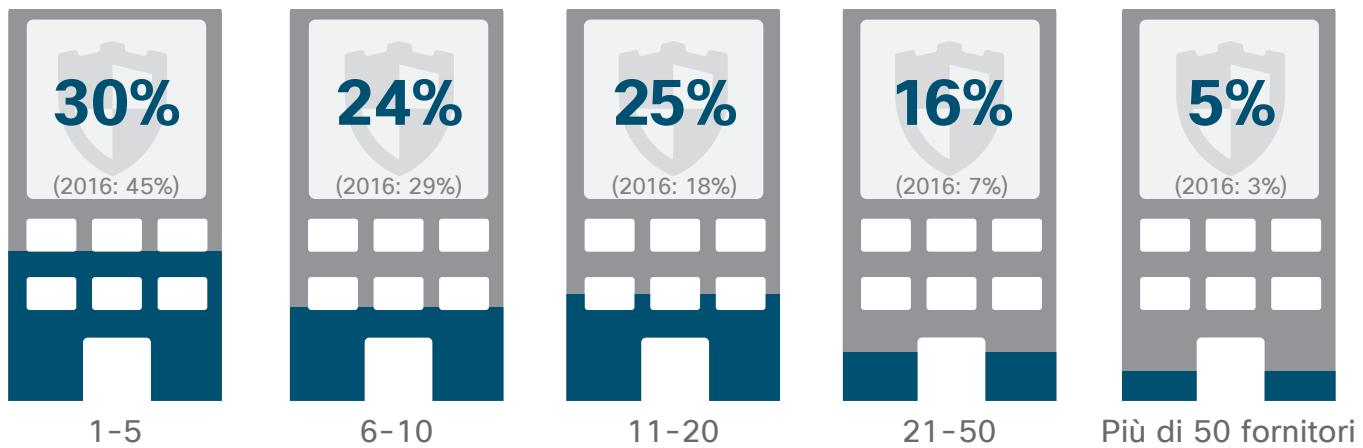
---

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

## Orchestrazione complessa a causa dei fornitori

I responsabili della sicurezza stanno implementando un mix complesso di prodotti di una grande varietà di fornitori: un arsenale di strumenti che possono offuscare anziché razionalizzare il panorama della sicurezza. Questa complessità genera molti effetti a cascata sulla capacità di un'azienda di difendersi dagli attacchi, per esempio un maggior rischio di perdite.

**Figura 44** Le aziende hanno utilizzato più fornitori di soluzioni di sicurezza nel 2017

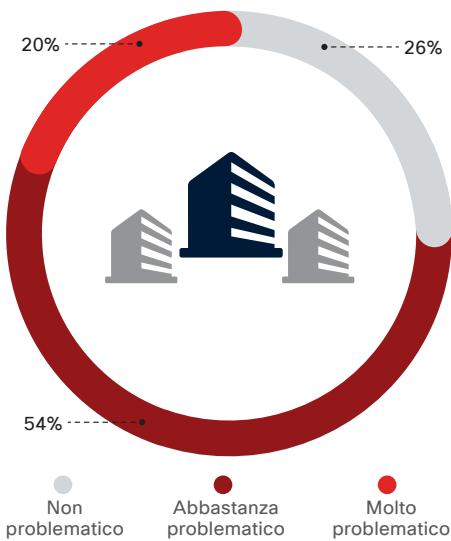


Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](https://cisco.com/go/acr2018graphics)

Aumentando il numero di fornitori, aumenta anche la difficoltà di orchestrare gli avvisi delle diverse soluzioni. Come mostrato nella Figura 45, il 54% degli esperti della sicurezza indica che la gestione di avvisi di fornitori diversi è piuttosto impegnativa, mentre il 20% la reputa molto impegnativa.

**Figura 45** La difficoltà di orchestrare gli avvisi



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

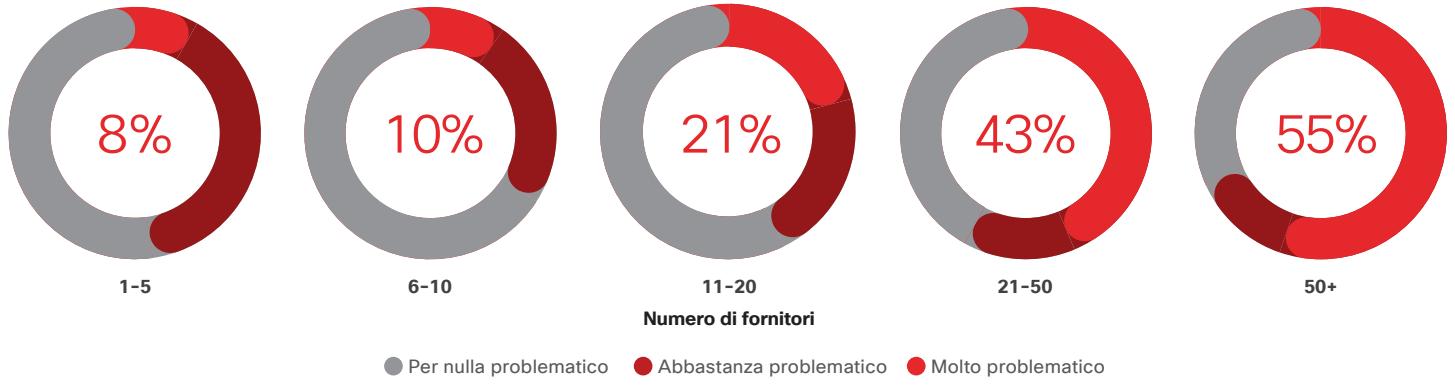
## I team di sicurezza si trovano dinanzi a molte sfide per orchestrare gli avvisi di fornitori diversi

Come mostrato nella Figura 46, tra le aziende che hanno solo da 1 a 5 fornitori, l'8% ha dichiarato che orchestrare gli avvisi è molto impegnativo. Al contrario, tra le aziende che usano più

di 50 fornitori, il 55% ha affermato che tale orchestrazione è molto impegnativa.

Quando le aziende non sono in grado di orchestrare e capire gli avvisi che ricevono, alcune minacce effettive possono passare inosservate.

**Figura 46** Con l'aumento dei fornitori, cresce anche la difficoltà di orchestrare gli avvisi di sicurezza



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

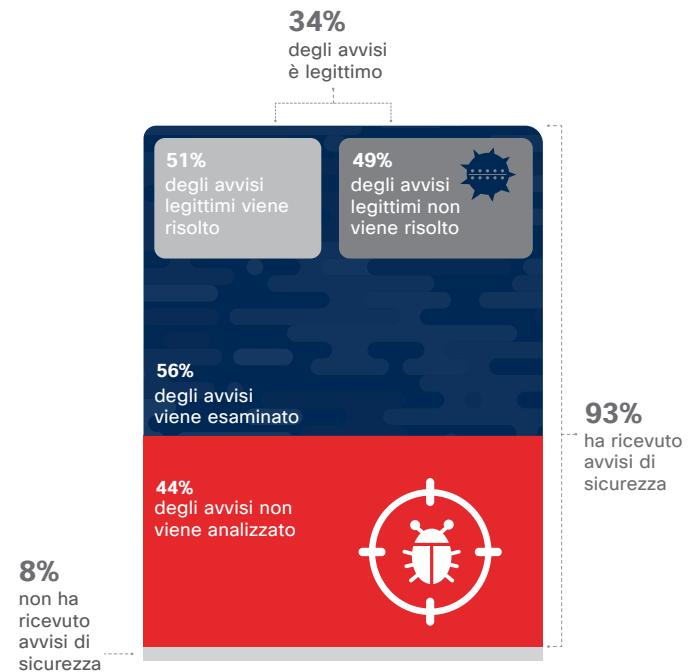
Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](https://cisco.com/go/acr2018graphics)

I dati forniti dagli intervistati indicano che persistono lacune tra gli avvisi generati, quelli che vengono analizzati e quelli a cui alla fine viene posto rimedio. Come mostrato nella Figura 47:

- Nelle aziende che ricevono avvisi di sicurezza quotidiani, in media il 44% di tali avvisi non viene analizzato.
- Degli avvisi analizzati, il 34% viene considerato legittimo.
- Tra gli avvisi considerati legittimi, il 51% viene risolto.
- A quasi la metà (49%) degli avvisi legittimi non viene posto rimedio.

Questo processo lascia irrisolti molti avvisi legittimi: una ragione sembra essere la mancanza di organico e personale specializzato che potrebbe far fronte alla necessità di analizzare tutti gli avvisi.

**Figura 47** Molti avvisi sulle minacce non vengono analizzati o risolti

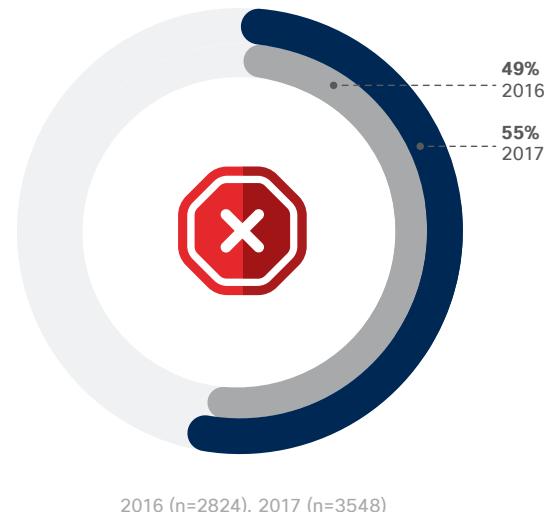


Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

## Impatto: esposizione al pubblico in seguito a violazioni e maggior rischio di perdite

“Ci sono due tipi di aziende: quelle che hanno subito violazioni e quelle che non sanno di averle subite” ha affermato un intervistato dello studio comparativo. (La risposta riprende una famosa citazione dell'ex CEO di Cisco John Chambers: “Ci sono due tipi di aziende: quelle che sono state hackerate e quelle che non sanno di essere state hackerate”). Sebbene le aziende stiano cercando di affrontare le future sfide della sicurezza con una preparazione adeguata, gli esperti della sicurezza sanno che le violazioni che comportano un danno reputazionale sono ormai inevitabili. Il 55% degli intervistati ha affermato che nel corso dell’ultimo anno la loro azienda ha dovuto gestire un’esposizione esterna suscettibile di provocare un danno reputazionale in seguito a una violazione (Figura 48).

**Figura 48** Il 55% delle aziende ha dovuto gestire l’esposizione al pubblico in seguito a una violazione



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](https://cisco.com/go/acr2018graphics)



*“Praticamente quasi tutte le aziende Fortune 500 sono state attaccate negli ultimi 2 anni. Bisogna essere preparati, soprattutto da una prospettiva di marketing o PR”.*

– Intervistato dello studio comparativo

Le aziende hanno riscontrato un numero notevolmente più alto di violazioni della sicurezza che hanno colpito oltre il 50% dei sistemi (Figura 49) rispetto all'anno scorso. Infatti, nel 2017 il 32% degli esperti della sicurezza ha affermato che le violazioni hanno riguardato più della metà dei loro sistemi, rispetto al 15% nel 2016. Le funzioni aziendali più comunemente colpite dalle violazioni sono: operazioni, finanza, proprietà intellettuale e reputazione del marchio (Figura 50).

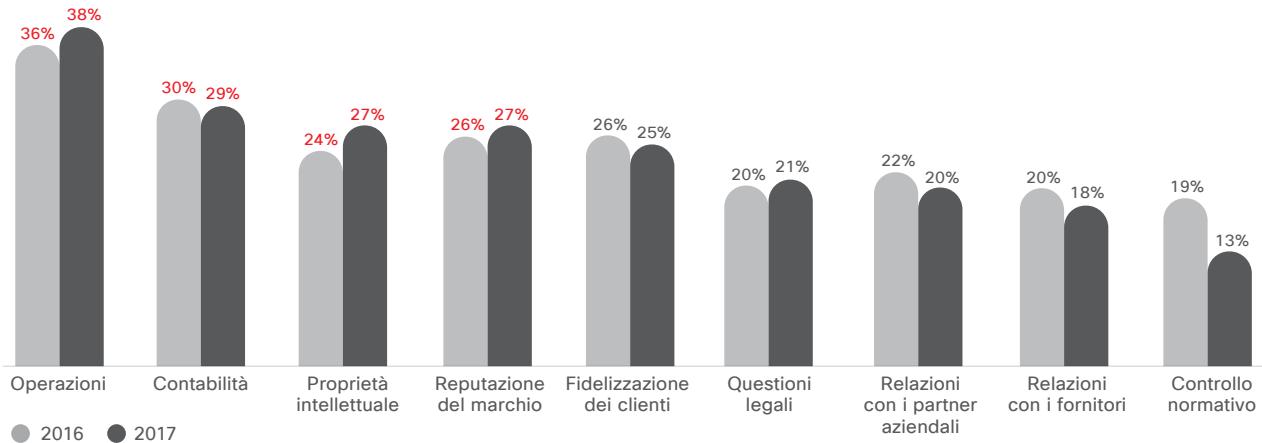
In ambienti di sicurezza complessi aumenta la probabilità di violazioni. Tra le aziende che utilizzano tra 1 e 5 fornitori, il 28% ha dovuto gestire un'esposizione esterna suscettibile di provocare un danno reputazionale a seguito di una violazione; questo dato sale all'80% per le aziende che hanno oltre 50 fornitori (Figura 51), probabilmente a causa della maggiore visibilità sulle minacce generate da più prodotti.

**Figura 49** Notevole aumento delle violazioni della sicurezza che interessano più del 50% dei sistemi



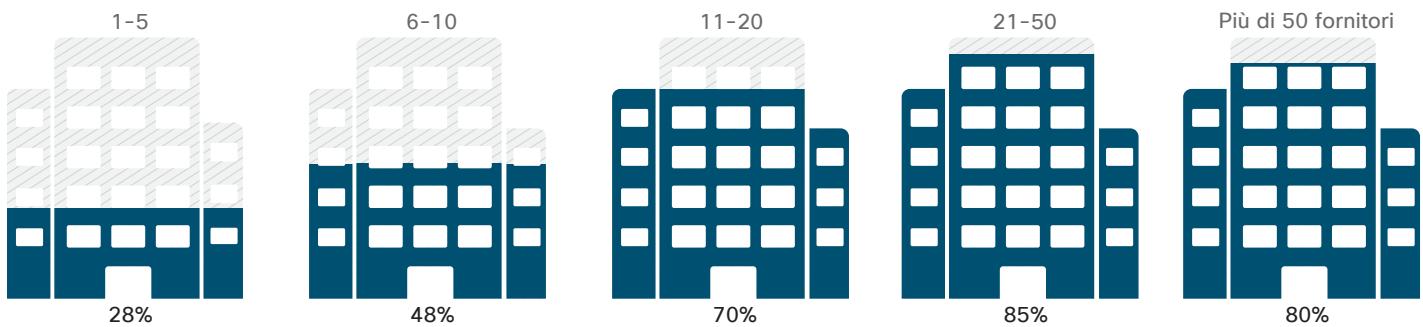
Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 50** Operazioni e finanza hanno più probabilità di essere colpiti da violazioni della sicurezza



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 51** L'80% delle aziende che utilizza più di 50 fornitori si è ritrovata sotto i riflettori a causa di violazioni che provocano danni reputazionali



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

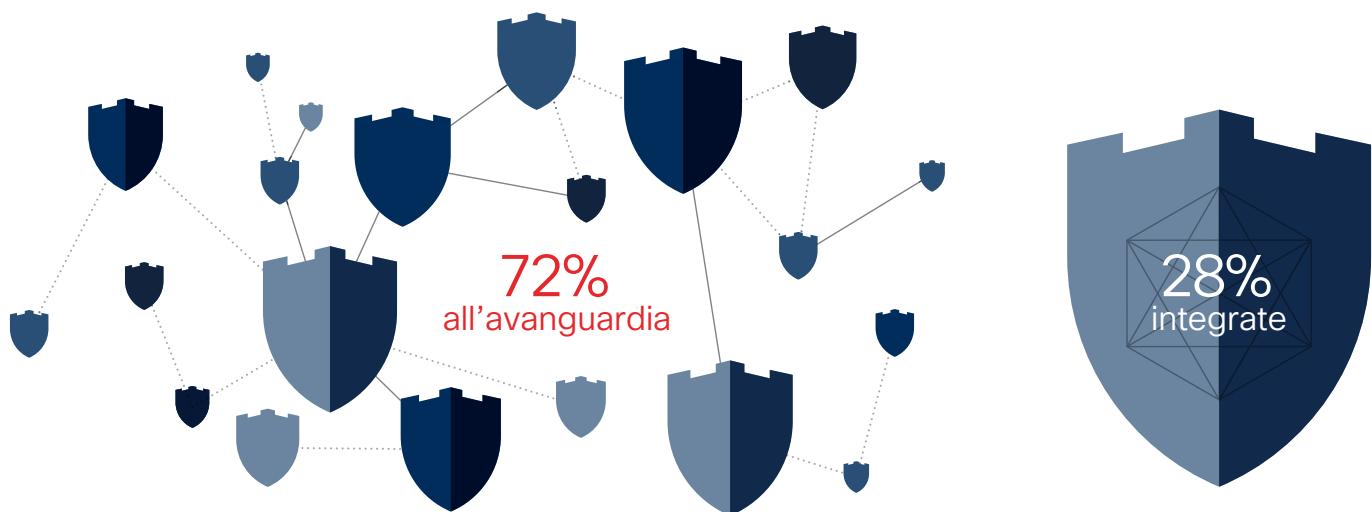
Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## Il valore di un framework integrato

Perché usare una moltitudine di prodotti di diversi fornitori, se l'ambiente che si crea è difficile da gestire? Uno dei motivi principali è l'approccio per la scelta della soluzione migliore che i team di sicurezza applicano per le proprie esigenze. Coloro che adottano questo approccio credono anche che sia più conveniente, secondo quanto emerge dalla ricerca effettuata per lo studio comparativo.

Raffrontando le soluzioni migliori con quelle integrate, il 72% degli esperti della sicurezza opta per le migliori soluzioni puntuale per soddisfare esigenze specifiche, rispetto al 28% che acquista prodotti pensati per interagire come soluzione integrata (vedere la Figura 52). Delle aziende che adottano l'approccio sulla scelta della soluzione migliore, il 57% ne cita la convenienza, mentre il 39% ha indicato la facilità di implementazione.

**Figura 52** Il 72% acquista soluzioni all'avanguardia perché rispondono a esigenze specifiche



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

È interessante notare che le aziende che adottano un approccio integrato alla sicurezza citano ragioni simili per giustificare la loro scelta. Il 56% afferma che un approccio integrato sia più conveniente, mentre il 47% indica che queste soluzioni sono più facili da implementare.

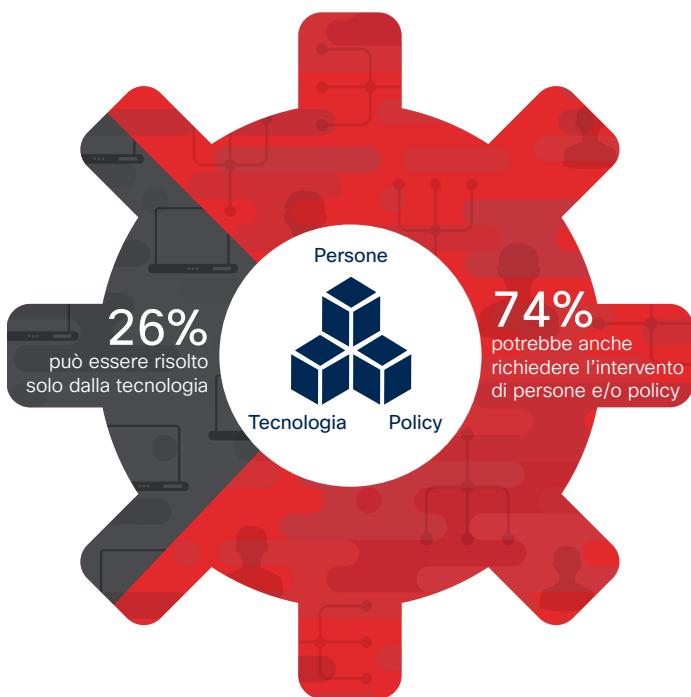
La facilità di implementazione è un fattore sempre più citato per giustificare un approccio di architettura integrata: nel 2016 solo il 33% delle aziende affermava che la facilità di implementazione fosse un motivo per scegliere un approccio integrato rispetto al 47% del 2017. Mentre le soluzioni di un unico fornitore potrebbero non essere funzionali per tutte le aziende, gli acquirenti delle soluzioni di sicurezza devono accertarsi che le soluzioni siano integrate per ridurre i rischi e aumentarne l'efficacia.

## Servizi: occuparsi di persone e policy, non solo di tecnologia

Di fronte alle potenziali perdite e agli impatti negativi sui sistemi, le aziende non possono più affidarsi solamente alla tecnologia per la difesa. Devono esaminare altre opzioni per migliorare la sicurezza, come l'applicazione di policy o la formazione degli utenti. Questo approccio olistico alla sicurezza è evidente nei problemi identificati nelle azioni di Intelligence Lead Security Assurance, noto anche come valutazione del “Red Team”, ad opera del Cisco Advanced Services Security Advisory Team.

Esaminando i dati con le raccomandazioni presenti in diverse valutazioni del Red Team effettuate nel 2017, i membri dei team dei servizi hanno identificato tre capacità difensive fondamentali: persone, policy e tecnologia. Se un'azienda utilizzasse solo la tecnologia per porre rimedio alle vulnerabilità della sicurezza, risolverebbe solo il 26% dei problemi identificati nelle simulazioni di attacco del Red Team, il che lascerebbe irrisolto il 74% dei problemi (vedere la Figura 53). Allo stesso modo, se le aziende utilizzassero solo le policy per affrontare i problemi di sicurezza, risolverebbero solo il 10% dei problemi; mentre con la formazione degli utenti solo il 4%. Le tre aree di difesa devono essere affrontate insieme.

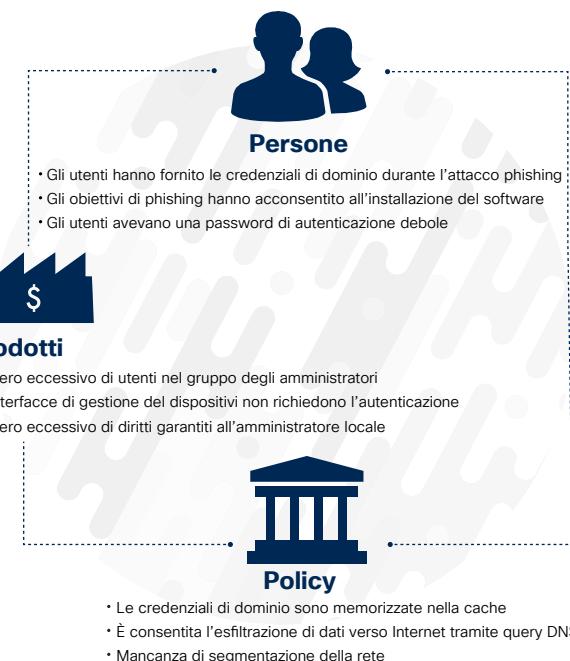
**Figura 53** Solo il 26% dei problemi di sicurezza può essere affrontato esclusivamente dai prodotti



Fonte: Cisco Security Research

La Figura 54 presenta degli esempi di problemi identificati durante le simulazioni suddivisi per categoria. Alcuni problemi, come le password deboli, riguardano tutte e tre le categorie. Il rafforzamento delle password può richiedere miglioramenti nell'ambito delle persone (formazione degli utenti), dei prodotti (configurazione dei server per password più complesse) e delle policy (impostazione di requisiti più stringenti per le password).

**Figura 54** Tipi di problemi rilevati nelle simulazioni di attacco categorizzati in base ai requisiti per la risoluzione



Fonte: Cisco Security Research

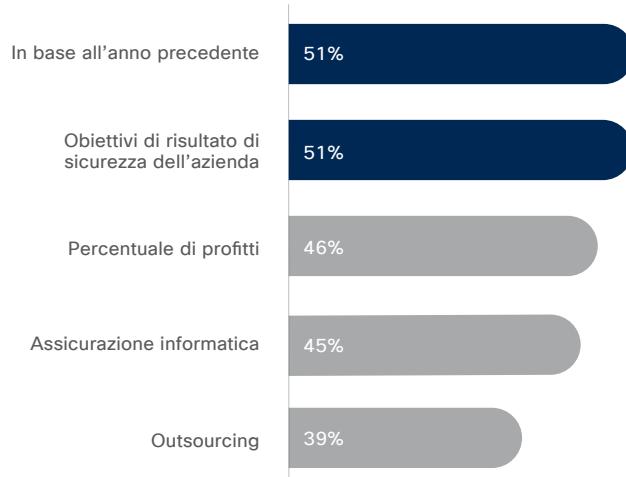
Le aziende possono avere più probabilità di gestire con successo tutti e tre i fattori, garantendo che la sicurezza sia integrata in ogni livello dell'azienda, non aggiunta in maniera frammentaria. Dovrebbero anche evitare di affidarsi esclusivamente a prodotti o miglioramenti tecnici per correggere la sicurezza. Affinché i prodotti funzionino correttamente, le aziende devono comprendere e implementare policy e processi adeguati per la tecnologia.

## Aspettative: investire in tecnologia e formazione

I professionisti della sicurezza sono unanimi nel ritenere che le minacce per le loro aziende rimarranno complesse e impegnative. Sanno che gli autori di attacchi svilupperanno modi più sofisticati e dannosi per violare le reti. Sono anche consapevoli del fatto che il luogo di lavoro moderno crea condizioni ideali per i criminali informatici: la mobilità dei dipendenti e l'adozione di dispositivi IoT offrono infatti nuove opportunità agli autori degli attacchi. Insieme alle minacce crescenti, molti esperti della sicurezza si aspettano di essere oggetto di ulteriori esami da parte di normatori, dirigenti, interlocutori, partner e clienti.

Per ridurre le probabilità di rischio e perdite, i responsabili della sicurezza devono individuare le aree in cui investire le loro risorse limitate. In genere, i budget per la sicurezza rimangono relativamente stabili, salvo nei casi in cui si sia verificata una grave violazione che comporta un danno reputazionale e che quindi porta a spendere di più per processi e tecnologia. Per il 51% la spesa per la sicurezza si basa sui budget degli anni precedenti, mentre per una percentuale equivalente di intervistati sono gli obiettivi di risultato a determinare il budget (Figura 55). La maggior parte dei responsabili della sicurezza ritiene che la spesa per la sicurezza delle loro aziende sia adeguata.

**Figura 55** Il 51% ha dichiarato che la spesa per la sicurezza è determinata dai budget degli anni precedenti



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Quando pianificano i budget, molte aziende esaminano sistematicamente le liste di richieste sviluppate nell'ambito di piani di sicurezza completi, assegnando priorità agli investimenti quando le risorse si rendono disponibili. Gli investimenti possono essere ridistribuiti a fronte di nuove vulnerabilità, per un incidente interno, una violazione ad elevata visibilità o una valutazione periodica dei rischi eseguita da terze parti.

I fattori principali che guidano gli investimenti futuri, e quindi i miglioramenti nella tecnologia e nei processi, sembrano essere le violazioni. Nel 2017, per il 41% degli esperti della sicurezza, le violazioni spingono verso maggiori investimenti nelle tecnologie e soluzioni per la sicurezza, tendenza che è cresciuta rispetto al 37% del 2016 (Figura 56). Per il 40% le violazioni favoriscono un aumento degli investimenti nella formazione del personale di sicurezza contro il 37% del 2016.

**Figura 56** Le violazioni della sicurezza stanno guidando gli investimenti in tecnologia e formazione



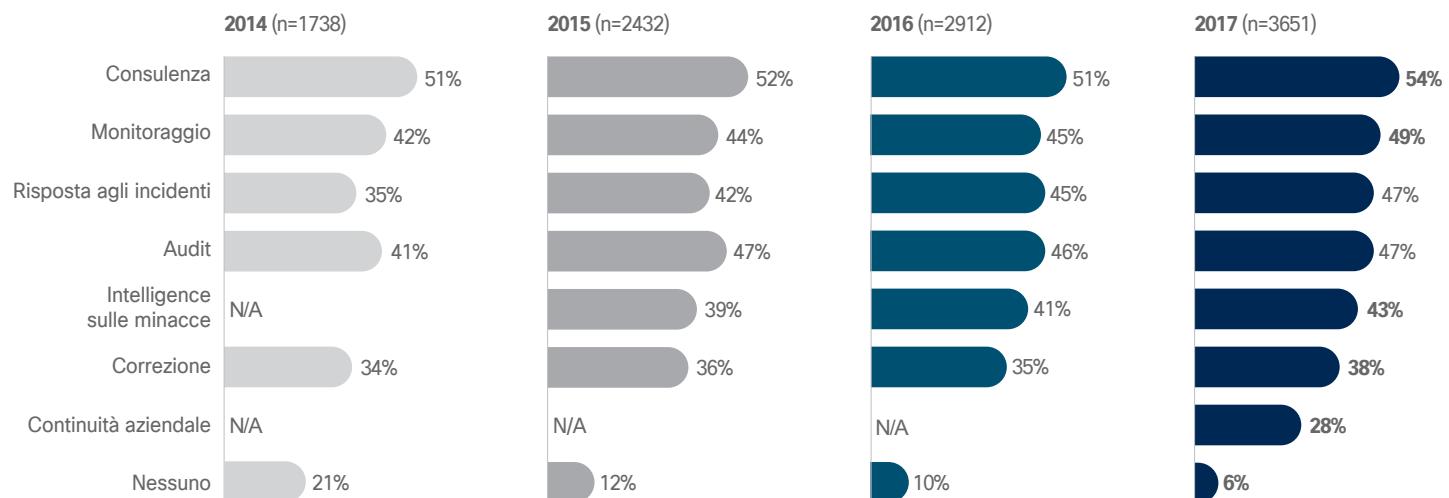
Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

Gli esperti della sicurezza prevedono di spendere di più per strumenti che utilizzano artificial intelligence e machine learning allo scopo di migliorare le difese e trasferirvi parte del carico di lavoro. Inoltre, hanno in programma di investire in strumenti che forniscono protezioni per i sistemi critici, come i servizi per infrastrutture critiche.

Per ampliare le risorse e rafforzare le difese, le aziende si affidano sempre più all'outsourcing. Nel 2017 il 49% degli esperti della sicurezza ha affermato di esternalizzare i servizi di monitoraggio, rispetto al 44% del 2015. Sempre nel 2017, il 47% ha invece esternalizzato le attività di reazione agli incidenti contro il 42% del 2015 (Figura 57).

**Figura 57** L'uso dell'outsourcing per il monitoraggio e la reazione agli incidenti cresce di anno in anno



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

 Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

**i** Per ulteriori risultati dello Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018, vedere l'Appendice a pagina 64.

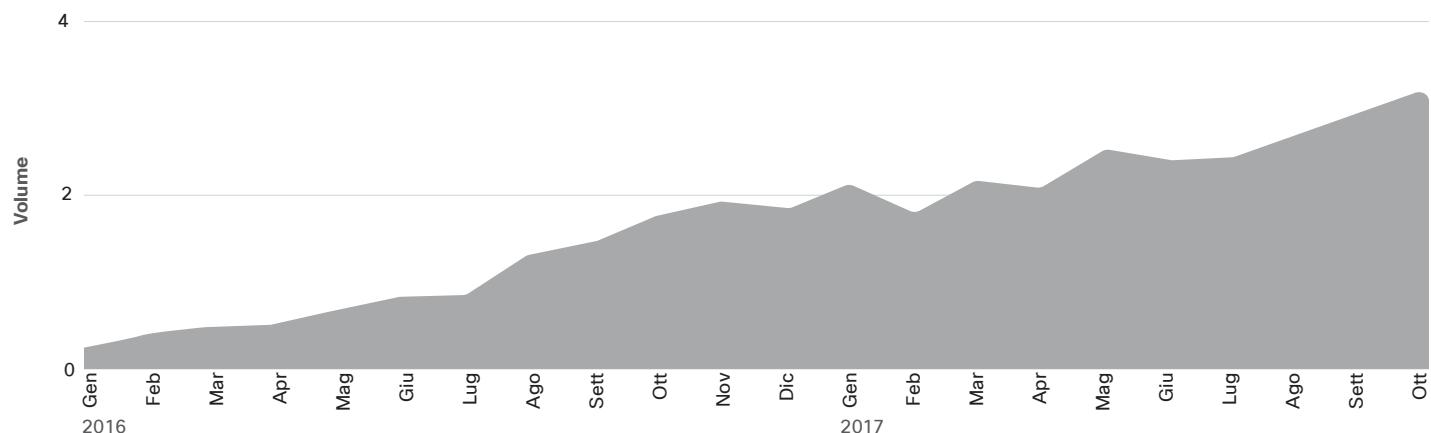
# Conclusioni

## Conclusioni

Nel moderno panorama delle minacce i criminali informatici sono abili a eludere il rilevamento. Sfruttano strumenti più efficaci, come la crittografia, e tattiche più avanzate e intelligenti, come l'abuso di servizi Internet legittimi, per nascondere le loro attività e pregiudicare le tecnologie per la sicurezza tradizionali. Inoltre, sviluppano costantemente le loro tattiche per mantenere il malware aggiornato ed efficace. Può servire molto tempo persino per identificare le minacce note alla community degli esperti di sicurezza.

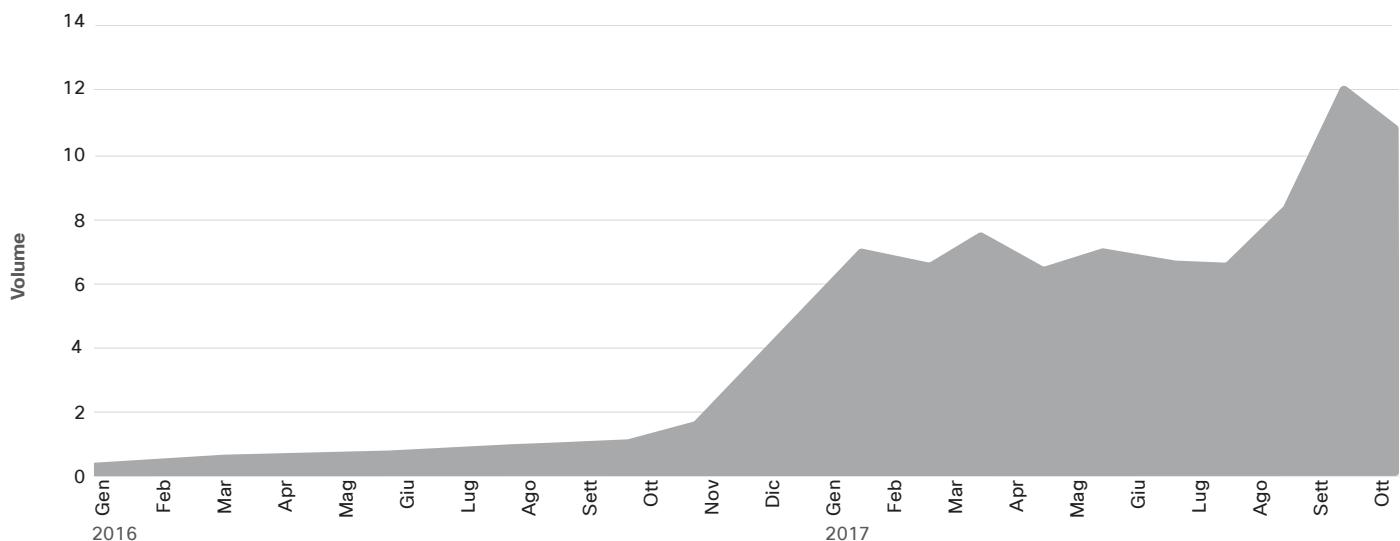
Una ragione per cui i responsabili della sicurezza faticano ad avere la meglio nel caos della guerra con i criminali informatici, e a vedere e capire davvero cosa sta succedendo nel panorama delle minacce, è l'enorme volume di traffico potenzialmente dannoso che devono affrontare. La ricerca mostra che il volume totale degli eventi totali registrato dai prodotti di sicurezza per endpoint basati su cloud di Cisco è quadruplicato da gennaio 2016 a ottobre 2017 (vedere la Figura 58). Il “totale degli eventi” è la somma di tutti gli eventi, innocui o dannosi, registrati dai nostri prodotti di sicurezza per endpoint basati su cloud nel periodo della ricerca.

**Figura 58** Volume totale di eventi



Fonte: Cisco Security Research

**Figura 59** Volume complessivo di malware



Fonte: Cisco Security Research

I nostri prodotti di sicurezza hanno inoltre rilevato un aumento di undici volte del volume complessivo di malware nello stesso periodo, come mostra la Figura 59.

Le tendenze nel volume di malware si ripercuotono sui tempi di rilevamento (TTD) dei responsabili della sicurezza, una metrica importante per qualsiasi azienda al fine di capire quanto siano efficaci le proprie difese dinanzi alla pressione esercitata dalla raffica costante di malware implementato dai criminali informatici.

La mediana TTD di Cisco, pari a circa 4,6 ore nel periodo che va da novembre 2016 a ottobre 2017, permette di illustrare la sfida continua della rapida identificazione delle minacce in questo caotico panorama. Eppure, tale cifra è ben al di sotto della mediana TTD di 39 ore che è stata registrata nel

novembre 2015, ossia all'avvio del monitoraggio del TTD, e alla mediana di 14 ore riportata nel *Report annuale di Cisco sulla cybersecurity 2017* relativa al periodo da novembre 2015 a ottobre 2016.<sup>20</sup>

L'uso della tecnologia di sicurezza basata su cloud è stato un fattore chiave che ha consentito a Cisco di portare e mantenere la mediana TTD a un livello basso. Il cloud permette di scalare e assicurare le prestazioni di pari passo con l'aumento del volume totale degli eventi e malware che colpiscono gli endpoint. Difficilmente le soluzioni di sicurezza on-premise riuscirebbero a offrire la stessa flessibilità. Sarebbe molto impegnativo e costoso per qualsiasi impresa progettarne una su scala in grado di gestire un volume 10 volte superiore di eventi dannosi in un periodo di due anni, mantenendo e accelerando i tempi di risposta.



In Cisco usiamo il termine tecnico “time to detection” (tempi di rilevamento) o “TTD” per indicare il periodo di tempo che intercorre fra una compromissione e l’identificazione della minaccia. Questo lasso di tempo viene determinato utilizzando dati telemetrici di sicurezza opt-in, raccolti da prodotti di sicurezza Cisco distribuiti in tutto il mondo. Sfruttando la nostra visibilità globale e un modello di analisi continua, siamo in grado di misurare il tempo che intercorre dal momento in cui un file dannoso viene scaricato su un endpoint al momento in cui si determina che si tratta di una minaccia che risultava non classificata al momento del rilevamento.

La “mediana TTD” corrisponde alla media dei valori medi mensili riferiti al periodo osservato.

20 Report annuale di Cisco sulla cybersecurity 2017: [cisco.com/c/m/en\\_au/products/security/offers/annual-cybersecurity-report-2017.html](http://cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html).

# Informazioni su Cisco

# Informazioni su Cisco

Cisco realizza sicurezza informatica intelligente con una gamma di soluzioni di protezione avanzata tra le più complete del settore e in grado di difendere contro una grande varietà di vettori di attacco. Il nostro approccio alla sicurezza altamente operativo e incentrato sulle minacce riduce la complessità e la frammentazione, garantendo al tempo stesso livelli di visibilità superiori, controlli coerenti e protezione avanzata dalle minacce, prima, durante e dopo l'attacco.

I ricercatori dell'ecosistema Cisco Collective Security Intelligence (CSI) hanno riunito in una singola soluzione le funzioni di analisi delle minacce leader del settore, utilizzando dati telemetrici ottenuti da una vasta gamma di dispositivi, sensori, feed pubblici e privati, oltre che dalla community open source. Ogni giorno vengono elaborati miliardi di richieste Web e milioni di e-mail, campioni di malware e intrusioni nelle reti.

I nostri sofisticati sistemi e infrastrutture utilizzano questi dati telemetrici, aiutando i ricercatori e i sistemi di machine learning a monitorare le minacce in più reti, data center,

endpoint, dispositivi mobili, sistemi virtuali, siti Web, e-mail e cloud per identificare le cause profonde e l'ambito delle infezioni. Le informazioni dettagliate così ottenute si traducono in una protezione in tempo reale per i nostri prodotti e servizi, che viene immediatamente fornita ai clienti Cisco di tutto il mondo.

**Per ulteriori informazioni sul nostro approccio alla sicurezza incentrato sulle minacce, visitare il sito [cisco.com/go/security](http://cisco.com/go/security).**

# CONTRIBUTI AL REPORT ANNUALE DI CISCO SULLA CYBERSECURITY 2018

Si ringraziano i team di ricercatori sulle minacce e gli altri esperti specializzati di Cisco nonché i partner tecnologici, che hanno contribuito al **Report annuale di Cisco sulla cybersecurity 2018**. Le loro ricerche e i loro punti di vista sono essenziali per aiutare Cisco a fornire alla community degli esperti di sicurezza, alle aziende e agli utenti informazioni rilevanti sulla complessità e la vastità del moderno e globale panorama delle minacce informatiche e presentare le migliori prassi e le conoscenze per migliorare le proprie difese.

I partner tecnologici svolgono un ruolo fondamentale aiutando la nostra azienda a sviluppare una sicurezza semplice, aperta e automatizzata che consenta alle aziende di integrare le soluzioni di cui hanno bisogno per proteggere i propri ambienti.

## Cisco Advanced Malware Protection (AMP) for Endpoints

Cisco AMP for Endpoints offre funzionalità automatiche di prevenzione, rilevamento e risposta in un'unica soluzione. Monitora e analizza costantemente la rete alla ricerca di segnali di attività dannosa per scoprire le minacce che oltrepassano la sicurezza di prima linea e rappresentano il rischio maggiore per le aziende. Usa molte tecniche di rilevamento, tra cui sandboxing avanzato, prevenzione degli exploit e machine learning per rilevare e mitigare rapidamente le minacce. Con Cisco AMP for Endpoints le aziende sono protette: è infatti l'unica soluzione che offre sicurezza retrospettiva per rispondere velocemente alle minacce e determinarne la portata, il punto di origine e per trovare il modo di contenerle.

## Cisco Cloudlock

Cisco Cloudlock fornisce soluzioni Cloud Access Security Broker (CASB) che aiutano le aziende a utilizzare il cloud in modo sicuro. Offre visibilità e controllo per ambienti Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) e Infrastructure-as-a-Service (IaaS) per tutti gli utenti, i dati e le applicazioni. Fornisce inoltre intelligence utilizzabile sulla cybersecurity attraverso l'analisi della sicurezza fornita da tutta la community e dal CyberLab, che è guidato da esperti nell'analisi dei dati.

## Cisco Cognitive Threat Analytics

Cisco Cognitive Threat Analytics è un servizio basato su cloud che rileva le violazioni, il malware operante all'interno di reti protette e altre minacce alla sicurezza mediante un'analisi statistica dei dati sul traffico di rete. Gestisce le vulnerabilità nelle difese perimetrali identificando i sintomi della diffusione di malware o della violazione dei dati tramite l'analisi comportamentale e il rilevamento delle anomalie. Cisco Cognitive Threat Analytics si basa su modelli statistici avanzati e sull'apprendimento automatizzato per identificare in modo autonomo le nuove minacce, apprendere dal contesto e adattarsi nel tempo.

## Cisco Product Security Incident Response Team (PSIRT)

Cisco Product Security Incident Response Team (PSIRT) è un'organizzazione globale dedicata che gestisce la ricezione, l'indagine e la divulgazione pubblica di informazioni sulle vulnerabilità e i problemi di sicurezza correlati ai prodotti e alle reti Cisco. PSIRT riceve report da ricercatori indipendenti, organizzazioni di settore, fornitori, clienti e altre fonti che si occupano di sicurezza delle reti o dei prodotti.

## Cisco Security Incident Response Services (CSIRS)

Il team Cisco Security Incident Response Service (CSIRS) comprende responsabili è composto da addetti di altissimo livello per la risposta agli incidenti, che assistono i clienti Cisco prima, durante e dopo un incidente. CSIRS si avvale del personale migliore, di soluzioni di sicurezza di livello enterprise, tecniche di risposta all'avanguardia e best-practice apprese nell'esperienza pluriennale di lotta contro il crimine informatico per garantire che i clienti siano in grado di difendersi in modo più proattivo contro ogni attacco, di reagire e approntare il ripristino velocemente.

## Cisco Talos Intelligence Group

Cisco Talos Intelligence Group è uno dei più grandi team commerciali di intelligence sulle minacce al mondo: è composto da ricercatori, analisti e tecnici di prim'ordine. Questi team, supportati da una telemetria impareggiabile e da sistemi sofisticati, creano un'intelligence sulle minacce accurata, rapida e fruibile per i clienti, i prodotti e i servizi Cisco. Talos Group difende i clienti Cisco dalle minacce note ed emergenti, scopre nuove vulnerabilità nei software comuni e blocca le minacce in rete prima che possano danneggiare ulteriormente Internet per esteso. L'intelligence di Talos è alla base dei prodotti Cisco che rilevano, analizzano e proteggono dalle minacce note ed emergenti. Talos ottempera alle norme ufficiali di Snort.org, ClamAV e SpamCop, oltre a rilasciare molti strumenti di analisi e di ricerca open source.

## Cisco Threat Grid

Cisco Threat Grid è una piattaforma di analisi dei malware e di intelligence sulle minacce. Threat Grid esegue analisi statiche e dinamiche su campioni di malware sospetti che provengono da clienti e da integrazioni di prodotti in tutto il mondo. Centinaia di migliaia di campioni di file, in una vasta gamma di tipologie, vengono inviati quotidianamente a Threat Grid Cloud per mezzo dell'interfaccia utente del portale Threat Grid Cloud, o dall'API di Threat Grid. Threat Grid può anche essere implementato come appliance on-site.

## Cisco Umbrella

Cisco Umbrella è un gateway Internet sicuro che agisce come prima linea di difesa contro le minacce su Internet, dovunque si trovino gli utenti. Poiché si basa su Internet, Umbrella offre visibilità completa delle attività in tutte le posizioni, dispositivi e utenti. Analizzando e apprendendo da questa attività, Umbrella scopre automaticamente l'infrastruttura allestita dai criminali informatici per le minacce note ed emergenti e blocca in modo proattivo le richieste prima che venga stabilita una connessione.

## Security Research and Operations (SR&O)

Security Research and Operations (SR&O) è responsabile della gestione di vulnerabilità e minacce di tutti i prodotti e

servizi Cisco, incluso il team leader di settore Cisco PSIRT. SR&O aiuta i clienti a comprendere il panorama delle minacce nel corso di eventi come Cisco Live e Black Hat, nonché tramite la collaborazione con altre organizzazioni di Cisco e del settore. SR&O offre inoltre nuovi servizi come Custom Threat Intelligence (CTI) di Cisco, che è in grado di identificare gli indicatori di compromissione che non sono stati rilevati o mitigati dalle infrastrutture di sicurezza esistenti.

## Security and Trust Organization

Cisco Security and Trust Organization sottolinea il nostro impegno nei confronti di due principi importanti che sono anche priorità assolute per vertici aziendali e leader mondiali. I principali obiettivi dell'organizzazione includono la protezione dei clienti pubblici e privati di Cisco, l'implementazione e la sicurezza del Secure Development Lifecycle e dell'impegno di Trustworthy Systems sulla gamma di prodotti e servizi Cisco, oltre alla protezione dell'impresa Cisco dalle minacce in continua evoluzione. Cisco adotta un approccio olistico per la sicurezza e la fiducia che include persone, policy, processi e tecnologia. Security and Trust Organization guida l'eccellenza operativa attraverso InfoSec, Trustworthy Engineering, Data Protection and Privacy, Cloud Security, Transparency and Validation e Advanced Security Research and Government. Per ulteriori informazioni, visitare [trust.cisco.com](http://trust.cisco.com).

## Partner tecnologici del Report annuale di Cisco sulla cybersecurity 2018

### ANOMALI<sup>®</sup>

La suite Anomali di soluzioni di intelligence sulle minacce consente alle aziende di rilevare, analizzare e rispondere alle minacce di cybersecurity attive. La pluripremiata piattaforma di intelligence sulle minacce ThreatStream aggrega e ottimizza milioni di indicatori di minaccia, creando una "no-fly list informatica". Anomali si integra con l'infrastruttura interna per identificare i nuovi attacchi, esegue analisi forensi nell'ultimo anno per scoprire violazioni esistenti e consente ai team di sicurezza di comprendere e contenere velocemente le minacce. Anomali offre anche STAXX, uno strumento gratuito per raccogliere e condividere l'intelligence sulle minacce; inoltre fornisce un feed di intelligence gratuito e pronto per l'uso, Anomali Limo. Per ulteriori informazioni visitare [anomali.com](http://anomali.com) e seguire Anomali su Twitter: @anomali.

### LUMETA

DETECT WITH A HIGHER SENSE<sup>™</sup>

Lumeta permette di riconoscere le situazioni critiche in ambito informatico consentendo ai team che gestiscono la sicurezza e la rete di prevenire le violazioni. Lumeta offre un livello di conoscenza impareggiabile delle infrastrutture di rete note, sconosciute, fantasma e non autorizzate al di sopra di ogni altra soluzione sul mercato, così come il monitoraggio di rete ed endpoint in tempo reale per rilevare modifiche non autorizzate, prevenire i percorsi di falla, garantire una corretta segmentazione della rete e rilevare i comportamenti sospetti su tutti gli elementi di rete dinamici, endpoint, macchine virtuali e infrastrutture basate su cloud. Per ulteriori informazioni, visitare [lumeta.com](http://lumeta.com).



Qualys, Inc. (NASDAQ: QLYS) è pioniere e fornitore leader di soluzioni di conformità e di sicurezza basata su cloud con oltre 9300 clienti in più di 100 paesi, tra cui gran parte dei Forbes Global 100 e dei Fortune 100. La piattaforma cloud di Qualys e la suite integrata di soluzioni aiutano le aziende a semplificare la gestione operativa della sicurezza e ad abbassare i costi della conformità fornendo, su richiesta, intelligence sulla sicurezza basilare, e automatizzando l'intera gamma di controlli, conformità e protezione per i sistemi IT e le applicazioni Web. Fondata nel 1999, Qualys ha costruito partnership strategiche con i principali provider di servizi gestiti e aziende di consulenza in tutto il mondo. Per ulteriori informazioni, visitare [qualys.com](http://qualys.com).



Radware (NASDAQ: RDWR) è un leader globale nella distribuzione delle applicazioni e nelle soluzioni di cybersecurity per i data center virtuali, su cloud e software-defined. Le sue soluzioni pluripremiate garantiscono assurance a livello del servizio per più di 10.000 aziende e vettori in tutto il mondo. Per ulteriori informazioni e risorse di sicurezza specializzate, visitare il centro di sicurezza online di Radware, che offre un'analisi completa degli strumenti di attacco DDoS, delle tendenze e delle minacce: [security.radware.com](http://security.radware.com).



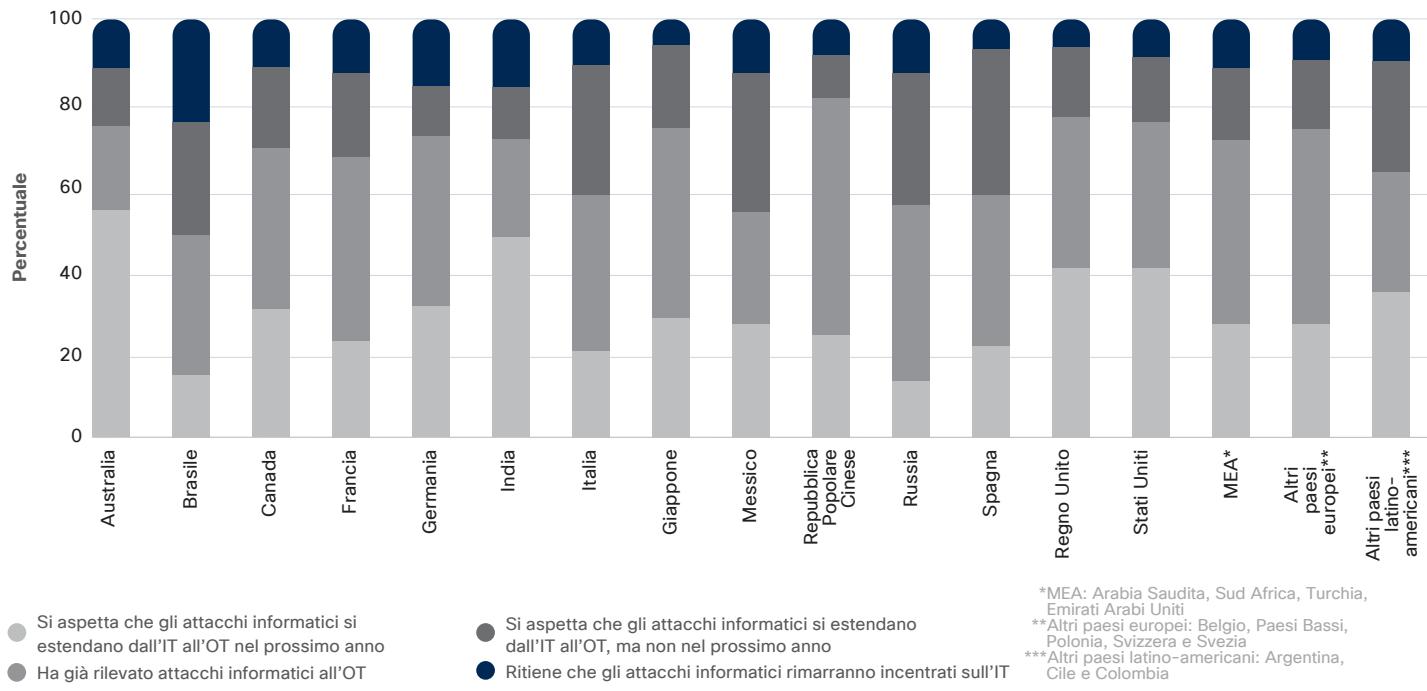
SAINT Corporation, leader nelle soluzioni integrate di nuova generazione di gestione delle vulnerabilità, aiuta le aziende e le istituzioni della pubblica amministrazione a individuare le esposizioni al rischio a tutti i livelli dell'azienda. SAINT interviene in modo che accesso, sicurezza e privacy possano coesistere a beneficio di tutti. SAINT permette inoltre ai clienti di rafforzare le difese di InfoSec riducendo allo stesso tempo il TCO. Per ulteriori informazioni, visitare [saintcorporation.com](http://saintcorporation.com).



TrapX Security fornisce una rete di sicurezza automatizzata per l'inganno e la difesa adattivi che intercetta le minacce in tempo reale fornendo contemporaneamente l'intelligence utilizzabile per bloccare i criminali informatici. TrapX DeceptionGrid™ consente alle aziende di rilevare, acquisire e analizzare i malware zero-day in uso dalle organizzazioni di minaccia persistente avanzata (APT) più efficaci al mondo. Aziende di diversi settori si affidano a TrapX per rafforzare i propri ecosistemi IT e ridurre il rischio di incorrere in compromissioni costose e dannose nonché in violazioni dei dati e della conformità. Le difese di TrapX sono integrate nel cuore della rete e nelle infrastrutture mission-critical senza il bisogno di configurazione o di far intervenire degli operatori. Racchiudendo il rilevamento di malware all'avanguardia, l'intelligence sulle minacce, l'analisi forense e il rimedio in un'unica piattaforma, si contribuisce ad abbattere la complessità e i costi. Per ulteriori informazioni, visitare [trapx.com](http://trapx.com).

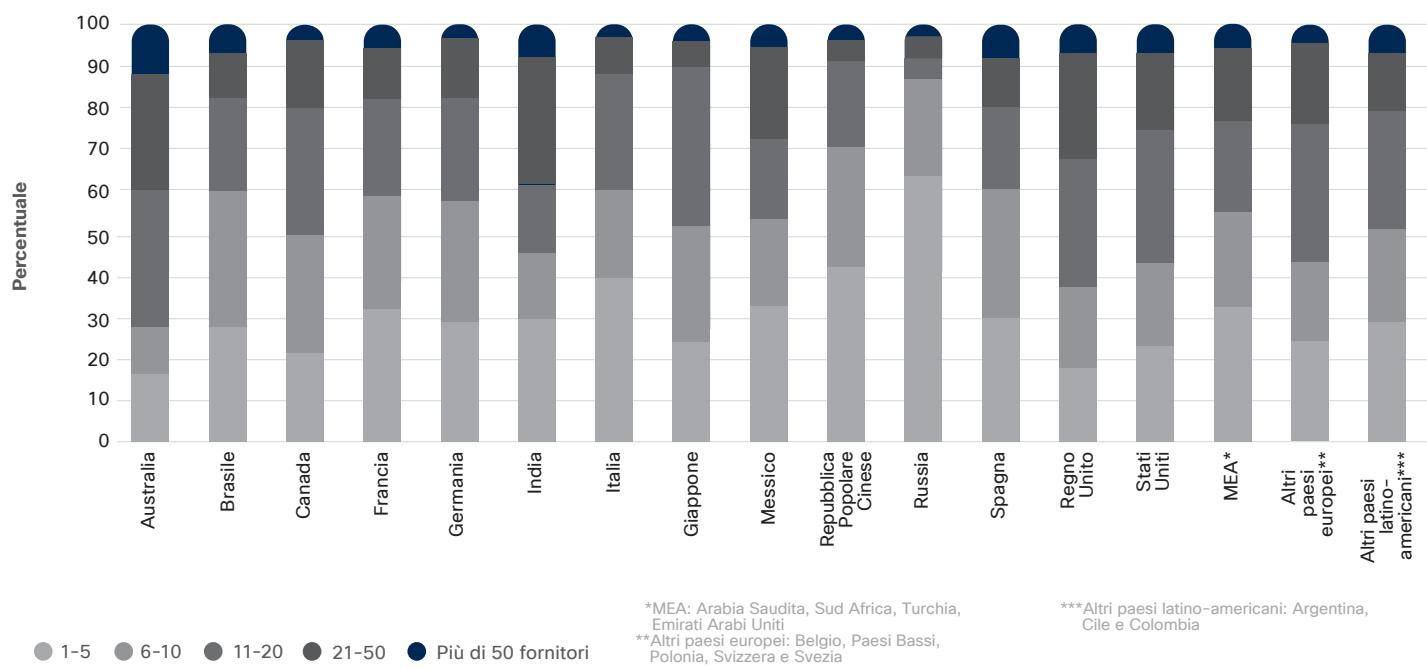
# Appendice

**Figura 60** Previsioni di attacchi informatici a OT e IT per paese o per area



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

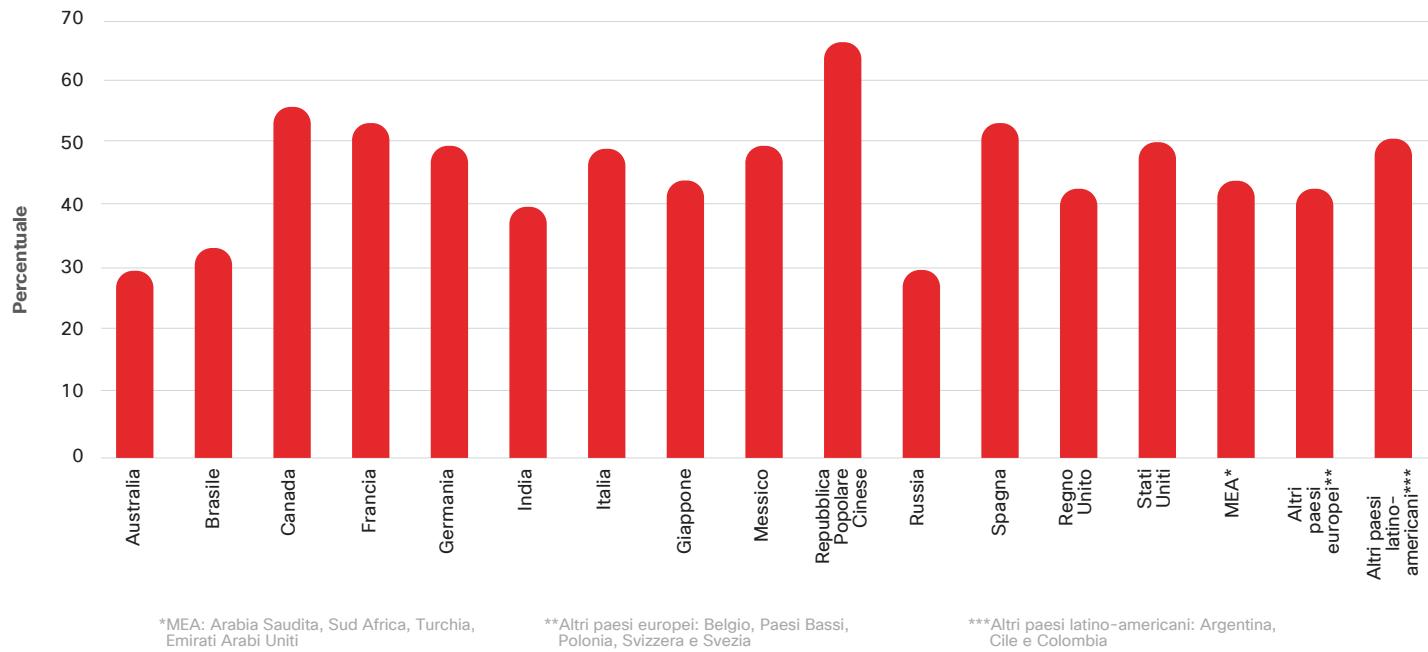
**Figura 61** Numero di fornitori di sicurezza nell'ambiente per paese o per area



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: cisco.com/go/acr2018graphics

**Figura 62** Percentuale di avvisi non analizzati per paese o per area



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 63** Ostacoli all'adozione di processi e tecnologie di sicurezza avanzata per paese o per area

Quale dei seguenti fattori è secondo te l'ostacolo maggiore per l'adozione di processi e tecnologie di sicurezza avanzata?

	Australia	Brasile	Canada	Francia	Germania	India	Italia	Giappone	Messico	Repubblica Popolare Cinese	Russia	Spagna	Regno Unito	USA	MEA*	Altri paesi europei**	Altri paesi latino-americani***
Limitazioni di budget	23%	35%	29%	33%	25%	36%	38%	31%	31%	38%	60%	33%	27%	34%	36%	37%	35%
Conflitti di priorità	28%	11%	29%	27%	28%	26%	24%	27%	16%	27%	20%	18%	32%	32%	25%	18%	24%
Mancanza di personale specializzato	25%	28%	19%	22%	24%	31%	24%	28%	30%	25%	35%	33%	31%	26%	25%	23%	26%
Mancanza di informazioni sui processi e le tecnologie di sicurezza avanzata	26%	26%	24%	21%	22%	24%	21%	26%	23%	29%	18%	21%	27%	22%	22%	17%	21%
Problemi di compatibilità con sistemi legali	27%	19%	30%	27%	30%	30%	22%	23%	32%	40%	25%	25%	24%	28%	30%	25%	28%
Requisiti di certificazione	33%	27%	29%	29%	24%	27%	27%	22%	27%	23%	22%	27%	27%	30%	24%	33%	21%
Atteggiamento e cultura aziendale sulla sicurezza	30%	23%	25%	20%	16%	26%	17%	21%	26%	17%	19%	24%	28%	25%	20%	20%	27%
Riluttanza ad acquistare strumenti prima della conferma del mercato	19%	20%	23%	26%	25%	29%	20%	28%	15%	16%	17%	20%	21%	22%	22%	21%	25%
Carico di lavoro attuale eccessivo per poter assumere nuove responsabilità	22%	16%	28%	18%	28%	28%	26%	27%	23%	21%	15%	28%	22%	22%	20%	17%	19%
L'azienda non è un bersaglio ambito per gli attacchi	25%	18%	21%	22%	24%	17%	14%	20%	12%	16%	11%	13%	21%	21%	21%	20%	16%
La sicurezza non è una priorità a livello dirigenziale	22%	10%	17%	17%	20%	13%	13%	23%	15%	18%	11%	11%	19%	19%	17%	19%	21%

\*MEA: Arabia Saudita, Sud Africa, Turchia, Emirati Arabi Uniti

\*\*Altri paesi europei: Belgio, Paesi Bassi, Polonia, Svizzera e Svezia

\*\*\*Altri paesi latino-americani: Argentina, Cile e Colombia

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018



Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

**Figura 64** Acquisto di soluzioni di difesa dalle minacce alla sicurezza per paese o per area

Quale opzione descrive meglio la modalità con la quale la tua azienda acquista soluzioni di difesa dalle minacce alla sicurezza?

Paese	N=	In genere acquista prodotti puntuali all'avanguardia per soddisfare esigenze specifiche	In genere acquista prodotti progettati per integrarsi
Australia	203	86	14
Brasile	197	72	28
Canada	185	67	33
Francia	191	59	41
Germania	195	69	31
India	199	78	22
Italia	201	71	29
Giappone	223	72	28
Messico	198	77	23
Repubblica Popolare Cinese	205	63	37
Russia	196	58	42
Spagna	148	70	30
Regno Unito	194	76	24
Stati Uniti	393	81	19
MEA*	249	69	31
Altri paesi europei**	199	73	27
Altri paesi latino-americani***	196	71	29

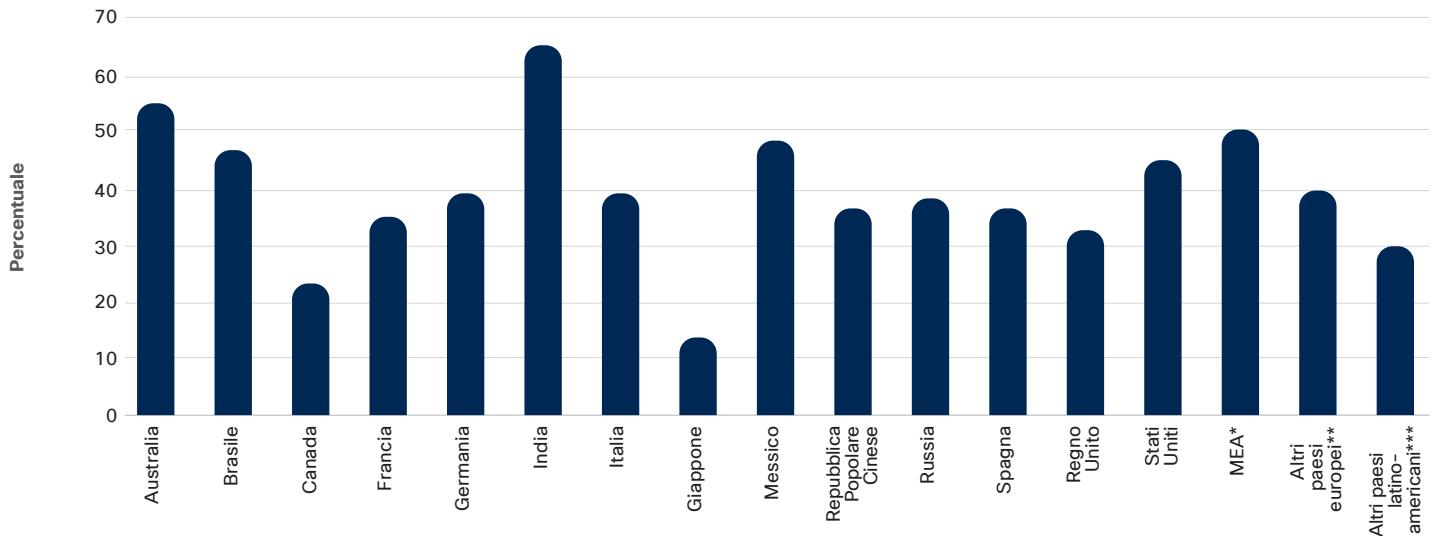
\*MEA: Arabia Saudita, Sud Africa, Turchia, Emirati Arabi Uniti

\*\*Altri paesi europei: Belgio, Paesi Bassi, Polonia, Svizzera e Svezia

\*\*\*Altri paesi latino-americani: Argentina, Cile e Colombia

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

**Figura 65** Percentuale delle aziende che ritengono di aderire molto bene al framework standardizzato InfoSec, per paese o area



\*MEA: Arabia Saudita, Sud Africa, Turchia, Emirati Arabi Uniti

\*\*Altri paesi europei: Belgio, Paesi Bassi, Polonia, Svizzera e Svezia

\*\*\*Altri paesi latino-americani: Argentina, Cile e Colombia

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Scaricare il grafico del 2018 al link seguente: [cisco.com/go/acr2018graphics](http://cisco.com/go/acr2018graphics)

## Download dei grafici

Tutti i grafici di questo report possono essere scaricati all'indirizzo: [cisco.com/go/mcr2018graphics](http://cisco.com/go/mcr2018graphics).

## Aggiornamenti e correzioni

Per vedere gli aggiornamenti e le correzioni delle informazioni di questo progetto, visitare [cisco.com/go/errata](http://cisco.com/go/errata).



**Sede centrale Americhe**  
Cisco Systems, Inc.  
San Jose, California (USA)

**Sede centrale Asia Pacifica**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Sede centrale Europa**  
Cisco Systems International BV Amsterdam  
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e di fax delle sedi italiane sono disponibili nel sito Web Cisco all'indirizzo [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Pubblicato nel febbraio 2018

---

© 2018 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati.

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per visualizzare l'elenco di marchi Cisco, visitare il sito Web all'indirizzo: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'utilizzo del termine partner non implica una relazione di partnership tra Cisco e altre aziende. (1110R)

Adobe, Acrobat e Flash sono marchi registrati o marchi di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.