

Report



# Report McAfee Labs sulle minacce

Maggio 2015





Nel primo trimestre McAfee Labs ha osservato quasi il **doppio dei campioni di ransomware** rispetto a qualsiasi altro periodo analogo.

## Informazioni su McAfee Labs

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

McAfee è ora una divisione di Intel Security.

[www.mcafee.com/it/mcafee-labs.aspx](http://www.mcafee.com/it/mcafee-labs.aspx)



Segui McAfee Labs

## Introduzione

Questo report sulle minacce rappresenta la nostra prima disamina degli attacchi basati sul firmware. Nel nostro argomento principale di apertura offriamo nuovi dettagli sul malware proveniente dall'organizzazione segreta **Equation Group**. Questa minaccia è capace di riprogrammare il firmware dell'unità disco rigido. La nostra analisi mostra che il firmware riprogrammato è in grado di ricaricare il malware associato ogni volta che il sistema infettato si avvia. Il malware persiste anche se il disco rigido viene riformattato o si reinstalla il sistema operativo. Abbiamo la sensazione che questo tipo di minaccia sarà quest'anno un argomento scottante durantegli eventi Black Hat e DefCon.

Ci soffermiamo inoltre su due soliti noti, il ransomware e gli exploit di Adobe Flash, dato che in questo trimestre McAfee Labs ha riscontrato un massiccio aumento di nuovi esempi di entrambi i tipi di minaccia. Per quanto riguarda il ransomware, ne attribuiamo gran parte dell'aumento a CTB-Locker, una nuova famiglia di difficile rilevamento che utilizza un programma "affiliato" per inondare rapidamente il mercato di campagne di phishing e condurre alle infezioni di CTB-Locker. Per quanto concerne invece gli exploit di Flash, la crescita è imputabile al numero di istanze di Flash su numerose piattaforme (soprattutto i dispositivi mobili), al numero di vulnerabilità note e non coperte da patch, oltre che alla difficoltà nel rilevamento di alcuni exploit basati su Flash.

Altri punti importanti:

- Nel momento in cui questo report sarà stato pubblicato, la **Conferenza RSA 2015** sarà storia. Speriamo che chi ha partecipato abbia avuto la possibilità di seguire **l'evento principale di Intel Security** presentato da **Chris Young, General Manager di Intel Security Group**. Per chi non ha potuto partecipare, la registrazione è disponibile **qui**. Young ha delineato la visione di Intel Security per cambiare il modo di pensare del settore della sicurezza e della relativa clientela, in merito alle informazioni sulle minacce e ai dati in tempo reale su eventi di sicurezza e attacchi. Ha sottolineato la necessità di andare oltre la mera raccolta ed elaborazione di una maggiore quantità di dati. Bisogna trovare maggior valore nei dati analizzandoli in modi nuovi e creativi. Vale la pena di ascoltarlo.
- Oltre a compiere una ricerca eccellente sulle minacce fornendo informazioni su di esse e autorevolezza nel campo della sicurezza informatica, McAfee Labs sviluppa le fondamentali tecnologie incorporate nei prodotti Intel Security. Di recente, alcune di queste tecnologie hanno compiuto dei progressi notevoli.
  - Il **servizio McAfee Global Threat Intelligence** invia informazioni sulla reputazione di file, web, IP, certificati e posta elettronica ai prodotti di Intel Security. Gestisce decine di miliardi di interrogazioni al giorno, proteggendo milioni di sistemi ogni ora.
  - Di recente, la soggiacente infrastruttura cloud di McAfee GTI è stata rinnovata – un po' come se si sostituisse il motore di un'auto che viaggia a 100 all'ora – per gestire molte più interrogazioni, più dati sulle minacce e un maggior numero di tipi di reputazione. Ne è stata inoltre rifatta l'architettura in modo che sia più veloce, più sicura, più resiliente e più facile da gestire.
  - Verso la fine dell'anno scorso Intel Security ha iniziato a rendere disponibili i prodotti per endpoint che includono la tecnologia "DAT reputation". McAfee Labs sottopone i file delle firme a lunghi test prima della pubblicazione, ma possono esserci delle rare circostanze in cui un DAT ha un impatto sui clienti. Ora molti dei nostri prodotti per endpoint rilevano, contengono e mitigano molto rapidamente i problemi derivanti dai DAT, diventando così molto più affidabili. Maggiori informazioni sulla nostra tecnologia per la reputazione DAT sono reperibili **qui**.
- Continuiamo a ricevere indicazioni preziose dai lettori tramite i sondaggi fra gli utenti dei Report sulle minacce. Se desideri farci conoscere la tua opinione in merito a questo report sulle minacce, **fai clic qui** per partecipare a un sondaggio di soli cinque minuti.

*Vincent Weafer, Senior Vice President, McAfee Labs*

Condividi questo report



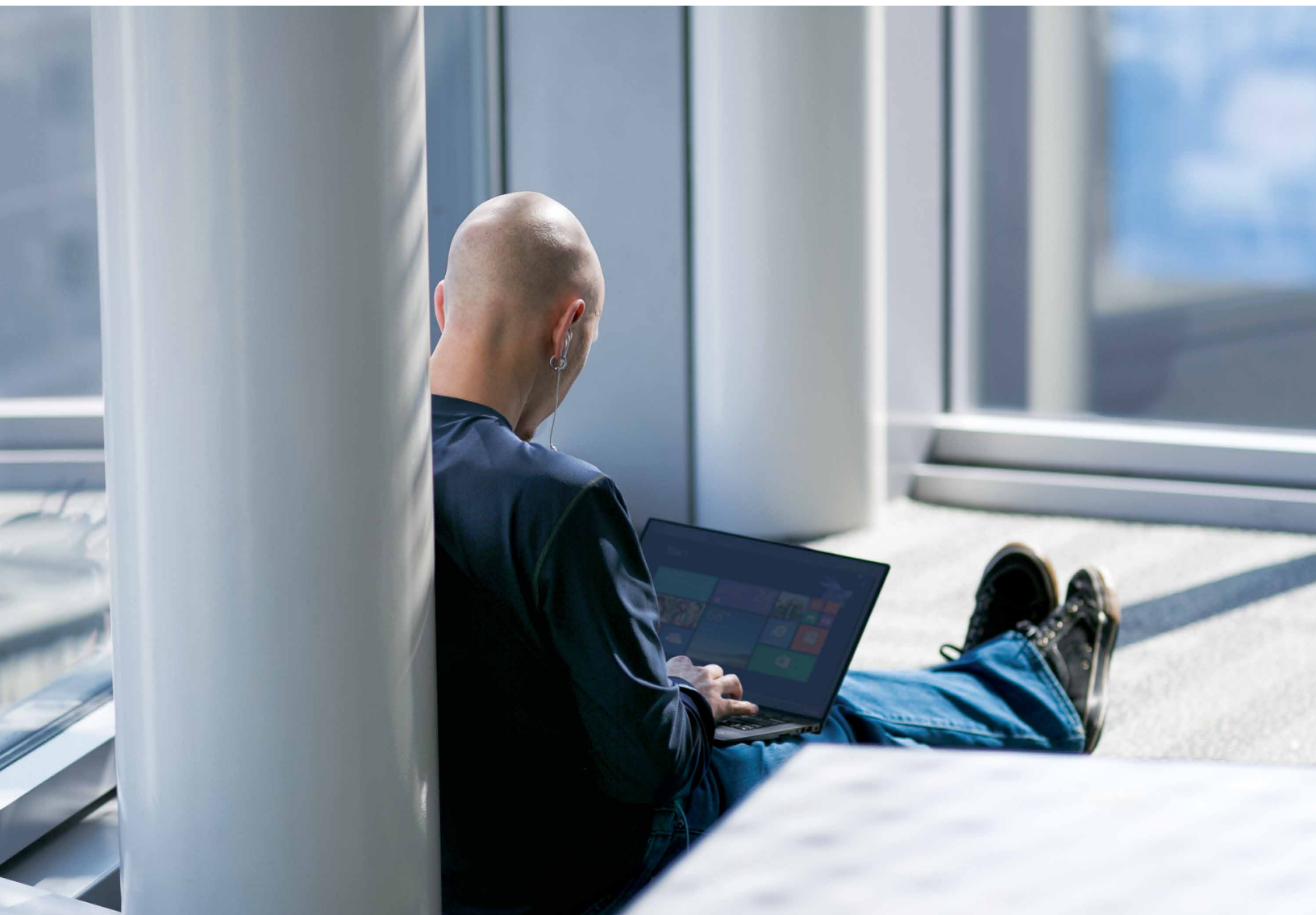
# Sommario

**Report McAfee Labs sulle Minacce**  
Maggio 2015

Rapporto preparato e redatto da:

Christiaan Beek  
Alexander Matrosov  
François Paget  
Eric Peterson  
Arun Pradeep  
Craig Schmugar  
Rick Simon  
Dan Sommer  
Bing Sun  
Santosh Surgihalli  
James Walter  
Adam Wosotowsky

Sintesi	5
Argomenti principali	6
Equation Group: lo sfruttamento del firmware delle unità a disco rigido e a stato solido	7
Il ritorno del ransomware: la vendetta delle nuove famiglie	14
Adobe Flash: il più amato da sviluppatori e criminali informatici	24
Statistiche sulle minacce	34



# Sintesi

## Equation Group: lo sfruttamento del firmware delle unità a disco rigido e a stato solido

---

I sistemi compromessi dall'Equation Group rimangono infettati anche se il disco rigido viene riformattato o il sistema operativo viene reinstallato. Si tratta del malware più sofisticato mai visto.

A febbraio è salita alla ribalta delle cronache una campagna di attacchi rari ma estremamente sofisticati. Si ritiene che la mente degli attacchi fosse l'"Equation Group", così denominato per la sua affinità con gli schemi crittografici più complessi. La scoperta più allarmante è stata che il malware dell'Equation Group include dei moduli per la riprogrammazione delle unità a disco rigido e a stato solido. Una volta riprogrammato, un sistema compromesso rimane infettato anche se il disco rigido viene riformattato o il sistema operativo viene reinstallato. Inoltre il firmware riprogrammato e il malware associato non sono rilevabili da parte del software di sicurezza. Questo report sulle minacce marca la prima disamina di McAfee Labs degli attacchi basati sul firmware.

## Il ritorno del ransomware: la vendetta delle nuove famiglie

---

Nel primo trimestre McAfee Labs ha osservato un forte aumento del ransomware, la maggior parte proveniente dalla nuova famiglia CTB-Locker e dal suo programma di "affiliazione" che hanno rapidamente inondato il mercato con le campagne di phishing.

Nel **Report McAfee Labs sulle minacce: novembre 2014** abbiamo fatto la seguente previsione per il 2015: "Il ransomware evolverà i suoi metodi di propagazione e crittografia e i bersagli perseguiti." Come volevasi dimostrare è emersa una nuova famiglia di ransomware: CTB-Locker. Questa famiglia si è diffusa in molti modi: IRC (Internet Relay Chat), reti peer-to-peer, post nei newsgroup, spam tramite email e altri. È stata inoltre ampiamente localizzata per ridurre al minimo i sospetti da parte dei destinatari della posta elettronica. Per eludere i prodotti di sicurezza, il downloader è occultato in un file .zip che contiene un altro file .zip che infine si decompone in un file salvaschermo. In più gli autori hanno creato un programma clandestino di "affiliazione" per inondare rapidamente il mercato con le campagne di phishing che conducono alle infezioni di CTB-Locker. Il risultato è che il primo trimestre ha visto un massiccio aumento nel numero di esempi di ransomware, soprattutto a causa di questa nuova famiglia.

## Adobe Flash: il più amato da sviluppatori e criminali informatici

---

Sempre nel primo trimestre gli exploit di Adobe Flash sono cresciuti del 317%. Flash è un vettore di attacco allettante perché viene ampiamente installato su molte piattaforme, presenta molte vulnerabilità note e non corrette e gli exploit sono spesso difficili da rilevare.

Adobe Flash è stato a lungo una superficie di attacco attraente per i criminali informatici, perché viene diffusamente installato su numerose piattaforme, presenta molte vulnerabilità note e non corrette e gli exploit sono spesso difficili da rilevare. Basta aggiungere a questi elementi l'aumento del kit di exploit Angler – descritto nel **Rapporto McAfee Labs sulle minacce: febbraio 2015** – e si ottiene la ricetta per la riuscita di un attacco informatico. Anzi, il numero di nuovi esempi di malware di Adobe Flash rilevato da McAfee Labs è schizzato a quasi 200.000 nel primo trimestre, un aumento del 317% rispetto ai 47.000 esempi rilevati nell'ultimo trimestre del 2014. In questo argomento principale esaminiamo Adobe Flash: come funziona, il crescente numero di vulnerabilità ed exploit, il modo in cui i criminali informatici li sfruttano e ciò che possono fare le aziende per proteggersi da questi exploit.

Condividi questo report







# Argomenti principali

Equation Group: lo sfruttamento del firmware delle unità a disco rigido e a stato solido

Il ritorno del ransomware: la vendetta delle nuove famiglie

Adobe Flash: il più amato da sviluppatori e criminali informatici

Inviaci la tua opinione



## Equation Group: lo sfruttamento del firmware delle unità a disco rigido e a stato solido

James Walter e Alexander Matrossov

A febbraio, la **notizia** della scoperta di una nuova campagna di attacchi (inverso di durata molto lunga) si è diffusa rapidissimamente. L'"Equation Group", così chiamato per la sua predilezione per gli schemi di crittografia ultrasofisticati e il malware associato, costituisce ora una delle minacce più sofisticate mai osservate.

```

u4byte l_key[44]; /* storage for the key schedule
/* initialise the key schedule from the user supplied key */
u4byte *set_key(const u4byte in_key[], const u4byte key_len)
{
    u4byte i, j, k, a, b, t;
    l_key[0] = 0xb7e15163;
    for(k = 1; k < 44; ++k)
        l_key[k] = l_key[k - 1] + 0x9e3779b9;
    for(k = 0; k < key_len / 32; ++k)
        l[k] = in_key[k];
    t = (key_len / 32) - 1; // t = (key_len / 32);
    a = b = i = j = 0;
    for(k = 0; k < 132; ++k)
    {
        a = rotl(l_key[i] + a + b, 3); b += a;
        b = rotl(l[j] + b, b);
        l_key[i] = a; l[j] = b;
        i = (i == 43 ? 0 : i + 1); // i = (i + 1) % 44;
        j = (j == t ? 0 : j + 1); // j = (j + 1) % t;
    }
    return l_key;
/* encrypt a block of text */
void encrypt(const u4byte in_blk[4], u4byte out_blk[4])
{
    u4byte a,b,c,d,t,u;
    a = in_blk[0]; b = in_blk[1] + l_key[0];
    c = in_blk[2]; d = in_blk[3] + l_key[1];
    f_rnd( 2,a,b,c,d); f_rnd( 4,b,c,d,a);
    f_rnd( 6,c,d,a,b); f_rnd( 8,d,a,b,c);
    f_rnd(10,a,b,c,d); f_rnd(12,b,c,d,a);
    f_rnd(14,c,d,a,b); f_rnd(16,d,a,b,c);
    f_rnd(18,a,b,c,d); f_rnd(20,b,c,d,a);
    f_rnd(22,c,d,a,b); f_rnd(24,d,a,b,c);
    f_rnd(26,a,b,c,d); f_rnd(28,b,c,d,a);
    f_rnd(30,c,d,a,b); f_rnd(32,d,a,b,c);
    f_rnd(34,a,b,c,d); f_rnd(36,b,c,d,a);
    f_rnd(38,c,d,a,b); f_rnd(40,d,a,b,c);
    out_blk[0] = a + l_key[42]; out_blk[1] = b;

```

Il codice dell'algoritmo di crittografia RC6 usato da Equation Group.

Una delle scoperte più significative compiute dal gruppo di ricerca sulle minacce d Intel Security riguarda i moduli di riprogrammazione del firmware delle unità a disco rigido (HDD) e a stato solido (SSD). Le unità HDD/SSD il cui firmware è stato riprogrammato possono ricaricare il malware associato ogni volta che i sistemi infettati si avviano. La minaccia poi persiste anche se le unità vengono riformattate o il sistema operativo reinstallato. Inoltre, dopo che hanno infettato l'unità, il firmware riprogrammato e il malware associato non sono rilevabili da parte del software di sicurezza.

I campioni specifici di Equation Group scoperti possono ora essere considerati come alcuni degli esempi di attacco firmware più visibili e avanzati mai osservati.

Negli ultimi anni, Intel Security ha osservato molti esempi di malware con capacità di manipolazione del firmware o del BIOS. Abbiamo visto sia proof-of-concept accademici che casi reali, fra i quali **CIH/Chernobyl**, Mebromi e **BIOSkit**. Abbiamo inoltre previsto questo specifico tipo di attacco nel report **Previsioni sulle minacce nel 2012** (Le principali minacce per il 2012 secondo McAfee Labs). I campioni specifici dell'Equation Group scoperti possono ora essere considerati come alcuni degli esempi di attacco firmware più visibili e avanzati mai osservati.

### I moduli di riprogrammazione del firmware HDD/SSD dell'Equation Group

Il malware dell'Equation Group si compone di numerosi moduli o "piattaforme", ognuna con una specifica funzionalità.

Modulo di Equation Group	Funzione del modulo
DoubleFantasy	Conferma del bersaglio, convalida della ricognizione, responsabile degli upgrade di modulo e piattaforma.
EquationDrug	Modulo completo e robusta piattaforma di attacco. Uno dei componenti primari e persistenti. Contiene il o i moduli di riprogrammazione del firmware HDD.
EquationLaser	Modulo compatibile con i sistemi operativi legacy (Windows 95/98)
Equestre	Nome intercambiabile associato a EquationDrug.
Fanny	Componente worm. Colpisce soprattutto regioni specifiche.
GrayFish	Piattaforma di attacco residente nel registro. Include un bootkit. Contiene il o i moduli di riprogrammazione del firmware HDD.
TripleFantasy	Backdoor, trojan di convalida del bersaglio.

Alcuni moduli dell'Equation Group risalgono al 2001, quindi sono piuttosto vecchi per essere dei malware. Ciononostante, sono una delle piattaforme di attacco più sofisticate che abbiamo mai visto. I ricercatori delle minacce continuano a individuare nuovi comportamenti ogni anno.

I moduli di riprogrammazione del firmware HDD/SSD scoperti più di recente sono stati compilati dal 2010 in poi. Sono state trovate versioni del plug-in sia a 32 sia a 64 bit. Anche se i campioni analizzati colpiscono solo i sistemi Microsoft Windows, ci sono indizi dell'esistenza di versioni anche per i sistemi Apple iOS e OS X. I nuovi moduli che puntano a Windows sfruttano i vecchi moduli dell'Equation Group, ancora molto efficaci, che compiono due azioni.

Condividi questo report





Un modulo riprogramma il firmware HDD/SSD con il codice appositamente scritto per la marca e modello dell'unità HDD/SSD. Il secondo modulo inserisce un'API in un'area nascosta dell'unità HDD o SSD. Tramite l'API il firmware riprogrammato è in grado di memorizzare e caricare lo specifico codice payload che esegue varie funzioni, pur rimanendo invisibile al sistema operativo. Nonostante questi nuovi moduli siano simili per sofisticazione agli altri moduli dell'Equation Group, i ricercatori delle minacce continueranno a scoprire nuovi comportamenti per molti anni.

Queste funzioni apportano grossi e importanti vantaggi all'Equation Group.

Una volta infettata l'unità, i moduli di riprogrammazione del firmware HDD/SSD dell'Equation Group persistono anche dopo la riformattazione del disco o la reinstallazione del sistema operativo, nascondono dello spazio sul disco dalla visibilità del sistema e non possono essere rilevati dal software di sicurezza.

- **Persistenza:** il firmware riprogrammato può sopravvivere alla riformattazione del disco e alla reinstallazione o alla creazione della nuova immagine del sistema operativo.
- **Invisibilità:** l'area di memorizzazione occulta è nota solo al firmware e rimane intatta anche se l'unità HDD/SSD viene riformattata.
- **Firmware persistente:** in alcuni casi gli elementi chiave del firmware riprogrammato sopravvivono alla sostituzione (reflashing) del firmware HDD o SSD.
- **Non rilevabilità:** il firmware riprogrammato e il malware associato non sono rilevabili da parte del software di sicurezza dopo che hanno infettato l'unità.

**File Name:** nls\_933w.dll\_11FB08B9126CDB4668B3F5135CF7A6C5  
**MD5 Hash Identifier:** 11FB08B9126CDB4668B3F5135CF7A6C5  
**SHA-1 Hash Identifier:** FF2B50F371EB26F22EB8A2118E9AB0E015081500  
**File Size:** 212480  
**File Type:** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Questa DLL contiene del codice che comunica direttamente con i dischi rigidi tramite l'interfaccia di comando ATA.

Come già detto, il codice di riprogrammazione del firmware è specifico per i diversi produttori di HDD/SSD, fra cui Western Digital, Samsung, Maxtor, Toshiba, IBM e Seagate. La sezione delle risorse del modulo (nls\_933w.dll) che abbiamo analizzato contiene un piccolo driver in modalità kernel x86 (circa 20 kB) in grado di comunicare con le unità disco rigido infette tramite l'interfaccia di comando ATA.<sup>1</sup> Il processo di aggiornamento del firmware richiede che l'unità interessata abbia dei comandi ATA non documentati. Tali serie di comandi sono già pronte<sup>2</sup> e sono usate spesso, sia per scopi leciti (per esempio indagini giudiziarie, analisi forensi) sia illeciti.

I comandi ATA sono comunemente usati per controllare e manipolare il comportamento meccanico ed elettrico delle unità. Possono inoltre controllare oppure attivare/disattivare funzioni specifiche.

Esempi di comandi di Maxtor:

- Check power mode
- Download microcode
- Flush cache
- Device configuration identify
- Security erase unit
- Security unlock
- Smart write log

Condividi questo report



Molti comandi ATA sono comuni a diversi produttori, quindi il modulo di riprogrammazione del firmware ne trae vantaggio ogni volta che è possibile.

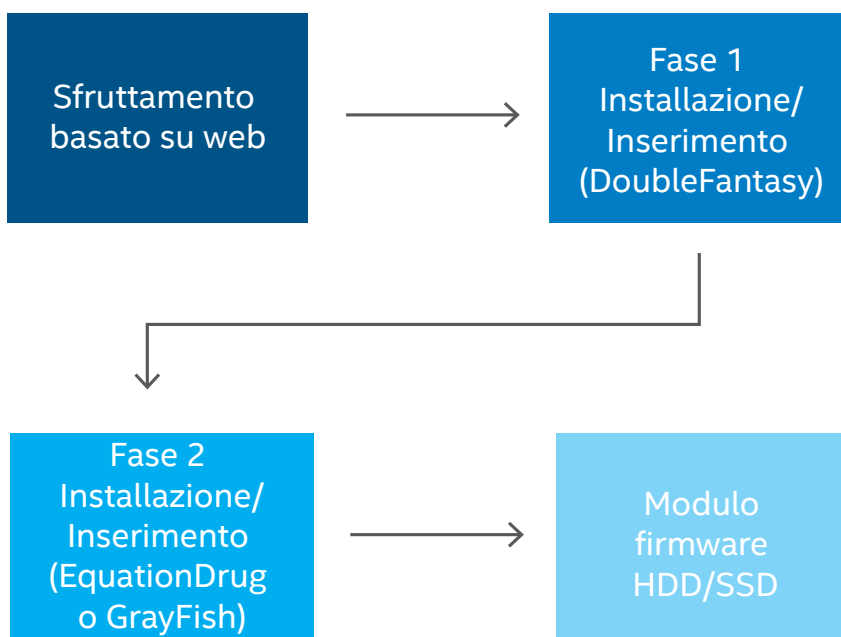
Il file nls\_933w.dll è stato compilato nel 2010. Tuttavia, inserisce un driver aggiuntivo (win32m.sys—MD5: 2b444ac5209a8b4140dd6b747a996653) nel sistema, che era stato compilato nel 2001. Il driver infettato viene memorizzato nella directory %WINDIR%\System32\drivers\win32m.sys dei computer delle vittime. Nonostante esistano esempi più recenti dei moduli HDD, questo sembra essere la versione 3.0.1.

### Meccanismo di infezione dei moduli firmware HDD/SSD

L'impatto e le metodologie dell'infezione sono diversi a seconda delle varie piattaforme dell'Equation Group. Tuttavia, sussistono delle modalità specifiche e ripetitive nell'invio dei moduli firmware HDD/SSD.

Il vettore iniziale dell'infezione è un exploit basato su web. L'Equation Group impiega un attacco di tipo "watering hole" (abbeveratoio), con il quale infetta i siti web frequentati dalle vittime. Quando la vittima visita uno di questi siti, il sistema bersaglio viene infettato dal malware della prima fase DoubleFantasy. DoubleFantasy conferma il bersaglio, esegue varie attività di ricognizione e (dopo la conferma) invia il malware della seconda fase: EquationDrug oppure il più recente GrayFish. La piattaforma della seconda fase gestisce poi l'installazione e la manutenzione dei moduli di riprogrammazione del firmware HDD/SSD.

### Fasi dell'attacco Equation Group HDD/SSD



## Attribuzione

Chi c'è dietro l'Equation Group e quali altri attacchi ha appoggiato? L'Equation Group è stato associato a **Flame**, **Duqu**, **Stuxnet** e **Gauss**. La nostra analisi mostra delle somiglianze nello stile di scrittura e nell'uso di specifiche strutture e metodologie nel codice e nelle modalità di infezione di questi attacchi. Esistono inoltre delle analogie nell'uso della crittografia RC5 o RC6. In alcuni casi, la crittografia è identica a quella di altri attacchi.

Inoltre, gli algoritmi di codifica delle stringhe sembrano basati sulla stessa idea di base o lo stesso codice sorgente. Confrontando il codice attribuito all'Equation Group con quello di Flame e TripleFantasy si nota l'utilizzo di primitive simmetriche per la codifica/decodifica:

```
char *__cdecl string_decrypt(char *str, int len)
{
    unsigned int str_size; // edi@1
    char v3; // dl@1
    signed int counter; // ecx@1
    char *result; // eax@3

    str_size = *(len + 1);
    v3 = *(len + 3);
    counter = 1;
    if ( str_size < 1u )
    {
        result = str;
    }
    else
    {
        do
        {
            str[counter - 1] = v3 ^ counter ^ *(len + counter + 3) ^ 0x47;
            v3 += *(len + counter++ + 3);
        }
        while ( counter <= str_size );
        result = str;
    }
    return result;
}
```

Decifrazione della stringa di malware dell'Equation Group.

```

char *__usercall string_decrypt@eax(char *str@eax, int Length@edx)
{
    char *v2; // esi@1
    char *key; // edi@2

    v2 = str;
    if ( Length )
    {
        key = (11 - str);
        do
        {
            str = (IV + &v2[key] * &v2[key + 12]);
            *v2 -= str ^ ((IV + (key + v2) * (key + v2 + 12)) >> 8) ^ ((IV + &v2[key] * &v2[key + 12]) >> 16) ^ ((IV + &v2[key] * &v2[key + 12]) >> 24);
            ++v2;
            --Length;
        }
        while ( Length );
    }
    return str;
}

```

Decifratura della stringa di Flame.

```

BYTE *__cdecl string_decrypt(int a1, _BYTE *a2, int a3, char a4)
{
    _BYTE *result; // eax@2
    int v5; // edi@3
    char v6; // dl@3
    _BYTE *v7; // ecx@4

    if ( a1 )
    {
        v5 = a3;
        v6 = a4 - 57;
        if ( a3 > 0 )
        {
            v7 = a2;
            while ( 1 )
            {
                *v7 = ((v6 - 33 * v7[a1 - a2]) << 6) | ((v6 - 33 * v7[a1 - a2]) >> 6) | (v6 - 33 * v7[a1 - a2]) & 0x3C;
                ++v7;
                if ( !--v5 )
                    break;
                v6 += a4;
            }
            result = a2;
        }
        else
        {
            result = 0;
        }
    }
    return result;
}

```

Decifratura della stringa di TripleFantasy.

Le somiglianze mostrate in queste schermate corroborano la possibilità di una relazione con altri attacchi contemporanei, sponsorizzati dagli stati.

Condividi questo rapporto







Scopri in che modo Intel Security può proteggerti contro questa minaccia.

## Protegersi dalla manipolazione di firmware e BIOS

Come detto in precedenza, un'unità HDD o SSD il cui firmware è stato riprogrammato da un modulo dell'Equation Group, può ricaricare il malware associato ogni volta che il sistema infettato si avvia, così il malware persiste anche se il disco rigido viene riformattato o il sistema operativo reinstallato. Inoltre, il firmware riprogrammato e il malware associato non sono rilevabili da parte del software di sicurezza dopo che si sono installati.

Intel Security e altri gruppi di ricerca ritengono che questo modulo di riprogrammazione del firmware sia molto raro e che sia stato impiegato solo in attacchi mirati a bersagli di altissimo livello. Di conseguenza, la maggior parte delle imprese non dovrebbe risentire di questa minaccia.

Nondimeno, la protezione contro gli attacchi di manipolazione di firmware e BIOS dovrebbe far parte del sistema di sicurezza di ogni azienda. Le aree principali su cui concentrarsi sono due:

- Stabilire delle modalità di rilevamento dell'iniziale invio del malware dell'Equation Group. I vettori di attacco noti sono phishing, CD e unità USB, quindi è a questi che va posta particolare attenzione.
- Tutelare i sistemi dalle sottrazioni di dati. Anche se tuttora non è possibile rilevare il modulo di riprogrammazione del firmware, l'obiettivo complessivo di un attacco è molto probabilmente la ricognizione. Dato che quest'ultima dipende dalla comunicazione e sottrazione sistematiche dei dati con un server di controllo, bloccare questa fase è di fondamentale importanza.

Policy e procedure raccomandate	
Generali	<ul style="list-style-type: none"> <li>▪ Defense-in-depth: protezione integrata e multilivello</li> <li>▪ Software di sicurezza in tutti gli endpoint</li> <li>▪ Attivare gli aggiornamenti automatici del sistema operativo oppure scaricare gli aggiornamenti regolarmente per mantenere il sistema coperto dalle patch per le vulnerabilità note</li> <li>▪ Installare le patch degli altri produttori software non appena vengono rese disponibili</li> <li>▪ Cifrare dati e dischi rigidi importanti</li> </ul>
Phishing	<ul style="list-style-type: none"> <li>▪ Eliminare le campagne di phishing di massa con il filtraggio dei messaggi email tramite gateway protetti</li> <li>▪ Implementare la verifica dell'identità dei mittenti per ridurre il rischio di scambiare criminali informatici per mittenti affidabili</li> <li>▪ Rilevare ed eliminare gli allegati pericolosi con strumenti antimalware avanzati</li> <li>▪ Eseguire la scansione degli URL presenti nei messaggi alla ricezione, e nuovamente al clic di un utente</li> <li>▪ Eseguire la scansione del traffico web alla ricerca del malware quando il phishing induce un utente a fare clic più volte e a infettarsi</li> <li>▪ Educare gli utenti ad adottare pratiche ottimali per sapere come riconoscere e come trattare i messaggi email sospetti</li> </ul>
Sottrazione dei dati	<ul style="list-style-type: none"> <li>▪ Implementare la prevenzione delle perdite di dati per arrestare la diffusione in caso di violazione</li> </ul>

Condividi questo report



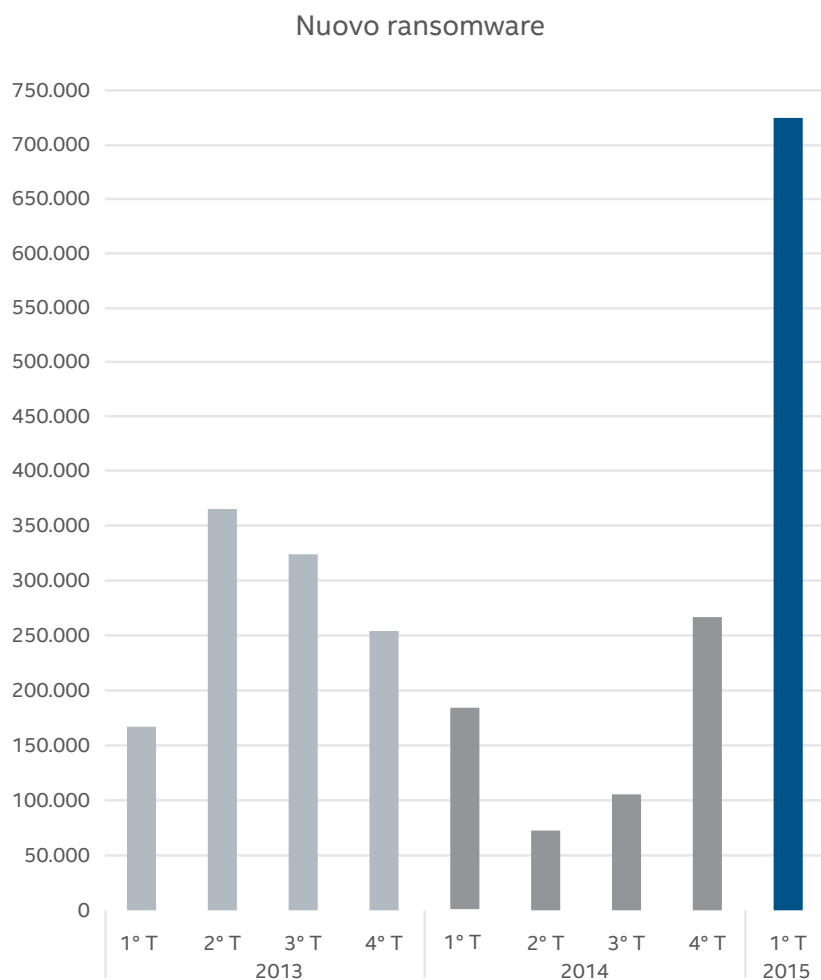
# Il ritorno del ransomware: la vendetta delle nuove famiglie

Christiaan Beek

Nel **Report McAfee Labs sulle minacce: novembre 2014** abbiamo previsto le nove principali minacce del 2015. Riguardo al ransomware, abbiamo scritto: "Il ransomware evolverà i suoi metodi di propagazione e crittografia e i bersagli perseguiti."

E quasi subito abbiamo cominciato a vedere un enorme aumento del ransomware, soprattutto con la nuova famiglia CTB-Locker, seguito dalle nuove versioni di CryptoWall, TorrentLocker e dai picchi di BandarChor. Nel primo trimestre abbiamo inoltre osservato l'emergere della nuova famiglia **Teslacrypt**.

Nel primo trimestre McAfee Labs ha osservato un aumento del 165% nel ransomware, specialmente con la famiglia CTB-Locker, oltre a nuove versioni di CryptoWall, TorrentLocker e a picchi di BandarChor. Nello stesso periodo abbiamo inoltre osservato l'emergere della nuova famiglia TeslaCrypt.



Fonte: McAfee Labs, 2015

Queste campagne di ransomware puntano principalmente a vittime che si trovano in paesi relativamente ricchi, per la loro maggiore inclinazione a pagare i riscatti. Ciò è emerso dalle affermazioni fatte nei forum clandestini che ospitano discussioni sull'efficacia delle campagne.

Condividi questo report



Gli argomenti delle email di phishing che portano alle infestazioni di ransomware sono molto specifici. Non solo i nomi del modello di email e dell'allegato compaiono nella lingua locale, ma fingono di provenire da aziende reali dei paesi presi di mira. Per esempio, a marzo abbiamo visto una campagna di ransomware in Turchia che inviava finte email, apparentemente provenienti da aziende postali e telefoniche, contenenti la richiesta di modificare o verificare i propri indirizzi, di compilare un modulo per una nuova consegna di merci oppure di controllare le bollette:

## Ptt posta hizmetleri

**EA273182901BE** takip numaralı kargonuz **09 Mart 2015** adresinize teslim edilememiştir. Lütfen adres bilgilerinizi güncelleyerek kargonuzu teslim alınız.

Teslimat adresi değiştirmek için [PTT Adres Değişikliği Formu](#) indirip dikkatlice ve eksiksiz olarak doldurmanız gerekmektedir.

[Adres Değişikliği Formu İndir](#)

**Dikkat**

Kargonuz 15 iş günü içinde almanız gerekmektedir. Fazladan her gün için PTT sizden 25TL/günlük tazminat talep etme hakkına sahip olacaktır.

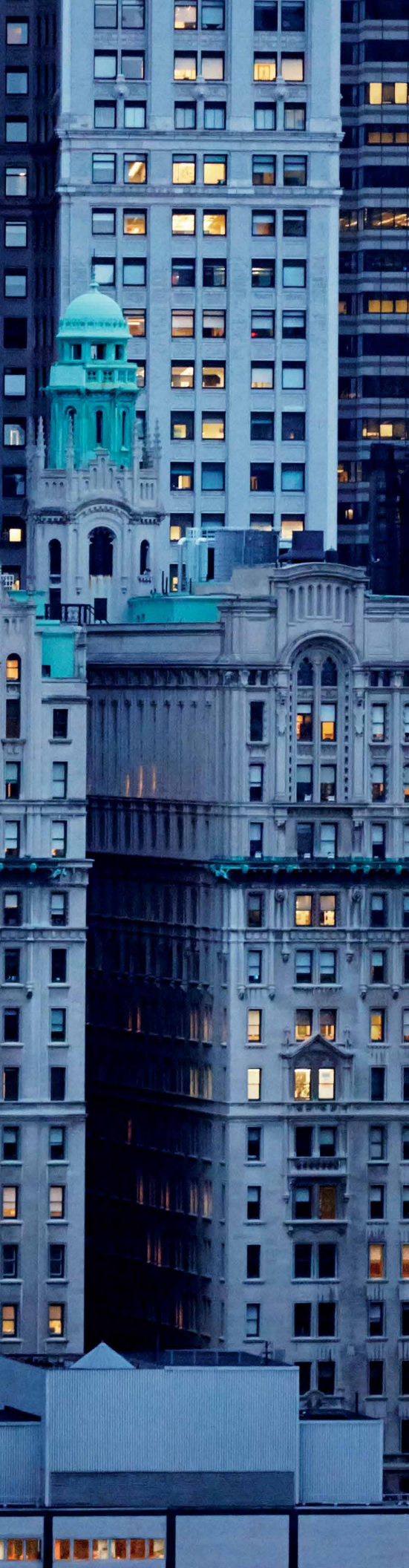
**Gizlilik Politikası**

PTT olarak ilgili kuralların tarafımızca tümü ile eksiksiz bir şekilde yerine getirileceğini teyit etmekteyiz. Böylelikle, aşağıda belirtilen kişisel bilgi toplama ilkelerine bağlı olarak, tüm gayretimizi tarafımızca toplanmış olan her türlü bilgiyi ekibimizce alınan sıkı güvenlik ve gizlilik önlemleri ile saklama hususunda özen göstermekteyiz. Kişisel bilgi toplama ve kullanımını en aza indirgeyerek, toplanan kişisel bilgileri sadece işlemlerin gerçekleştirilmesi için gerekli olan süre kadar tutmakta, öte yandan size en kaliteli hizmeti ve birbirinden güzel fırsatları sunmaktayız. Web sitemiz, gizlilik konusunda yeterince duyarlı olduğunu gösterebilen ve standartlarımıza uygun olan sitelere bağlantılar içermektedir. Ancak ilgili sitelerin içeriği ya da gizlilik uygulamalarından PTT sorumlu tutulamaz.

Bu e-posta [REDACTED] için gönderilmiştir. Eğer artık ilgilenmiyorsanız haber grubu üyeliğinizi [iptal edebilirsiniz](#)

PTT Posta Hizmetleri  
Posta ve Telgraf Teşilatı A.Ş. 2015

Questa email apparentemente legittima conteneva un collegamento per reindirizzare le vittime a un sito web contenente il ransomware.



## Storia del ransomware

Nel maggio 1996, Adam Young della Columbia University, presentò al IEEE Symposium on Security and Privacy il lavoro **Cryptovirology—extortion-based security threats and countermeasures** (Criptovirologia: minacce a scopo di estorsione e relative contromisure). Young descrisse lo sviluppo dei primi prototipi di ransomware, che usavano il processo di crittografia asimmetrica.

Nella crittografia asimmetrica, per cifrare e decifrare un file si usa una coppia di chiavi. Applicata al ransomware, la coppia di chiavi pubblica-privata viene generata in maniera univoca dall'aggressore per la sua vittima. La chiave privata per decifrare i file viene memorizzata nel server dell'aggressore e messa a disposizione della vittima solo dopo il pagamento di un riscatto. Aggiungendo il danno alla beffa, alcuni aggressori non forniscono le chiavi private neanche dopo il pagamento del riscatto, lasciando le vittime senza soldi e senza file. Con una chiave asimmetrica, l'autore del ransomware è in possesso di una chiave (privata) che non è accessibile agli analisti del malware. Senza l'accesso alla chiave, decifrare i file tenuti in ostaggio è pressoché impossibile.

Dopo quello studio illuminante del 1996 i ricercatori hanno descritto molti scenari, sia in dibattiti che in letteratura. Una delle prime famiglie di ransomware note in circolazione –Gpcode.ak – è comparsa nel 2008. Questo malware ha all'attivo una lunga serie di cifratura di file nei computer delle vittime. La famiglia di ransomware più famigerata – CryptoLocker – è comparsa nel settembre 2013. La forma di CryptoLocker allora attuale è stata bloccata nel maggio 2014, disattivando uno dei suoi vettori di distribuzione principali, la rete GameOver Zeus. Al momento le principali famiglie di ransomware sono CryptoWall (versioni 2 e 3), TorrentLocker versione 2 e CTB-Locker (McAfee Labs ha esaminato CryptoLocker, GameOver Zeus e la loro neutralizzazione nel **Rapporto McAfee Labs sulle Minacce: agosto 2014**).

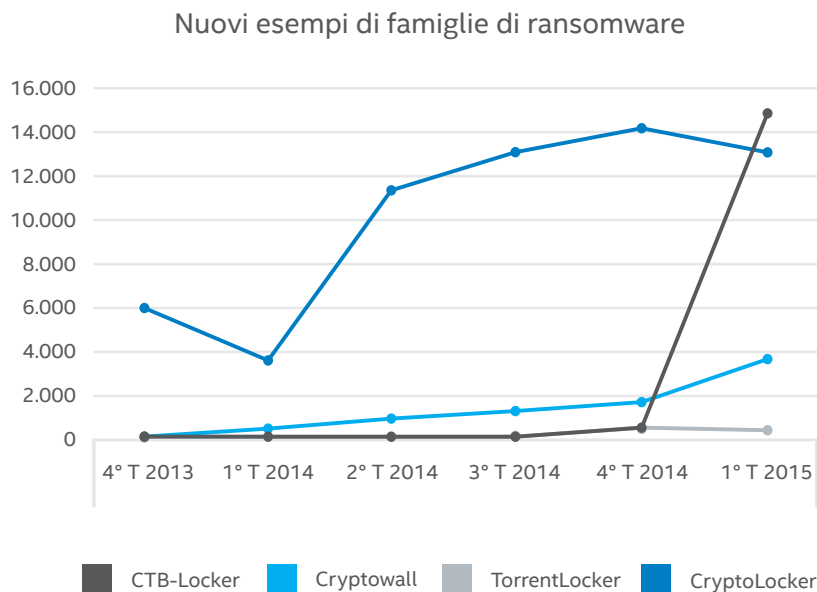
Nel corso degli anni le nuove tecnologie sono state adattate per rendere il ransomware più efficace:

- Valuta virtuale: usando la **valuta virtuale** come mezzo per far pagare i riscatti, gli aggressori non si espongono ai controlli del banking tradizionale e alla possibilità di tracciatura dei bonifici.
- La rete Tor: utilizzando la **rete Tor** gli aggressori possono occultare più facilmente l'ubicazione dei propri server di controllo che detengono le chiavi private delle vittime. Tor rende possibile il mantenere a lungo un'infrastruttura criminale, che può anche essere affittata ad altri autori di attacco per svolgere le campagne affiliate.
- Lo spostamento ai dispositivi mobili: nel giugno 2014 i ricercatori hanno scoperto la prima famiglia di ransomware che cifra i dati dei dispositivi Android. Pletor utilizza la crittografia AES, cifra i dati nella scheda di memoria del telefono e poi utilizza Tor, gli SMS oppure il protocollo HTTP per connettersi con gli autori dell'attacco.
- La presa di mira dei dispositivi di archiviazione di massa: nell'agosto 2014 Synolocker ha cominciato a colpire i dischi NAS (Network Attached Storage) e le stazioni su rack di Synology. Il malware sfrutta una vulnerabilità nelle versioni non coperte da patch dei server NAS, per cifrare in remoto tutti i dati dei server con le chiavi RSA a 2048 bit o a 256 bit.



## Statistiche

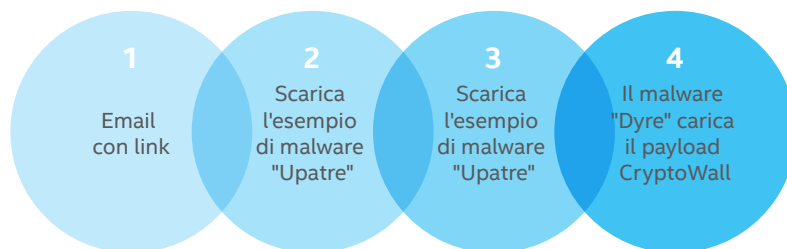
Nella tabella seguente possiamo osservare la proliferazione dei nuovi esempi unici di alcune delle principali famiglie di ransomware:



Fonte: McAfee Labs, 2015

CTB-Locker ha fatto la sua comparsa nel dicembre 2014. Mentre scriviamo è ancora molto attivo. Nonostante il numero di esempi di CryptoWall versione 1 e 2 sia relativamente stabile, la versione 3 ha cominciato a diffondersi tramite la rete Dyre nel settembre 2014.

## Fasi dell'attacco di rete Dyre



Per infettare i sistemi, la rete Dyre esegue questi passaggi.

## Curve-Tor-Bitcoin-Locker, noto anche come CTB-Locker

In questo trimestre è stato molto attivo CTB-Locker. Il significato del nome è questo:

- Curve indica l'uso, da parte del malware, della **crittografia persistente basata sulle curve ellittiche**, che cifra i file con una chiave RSA univoca.
- Tor deriva dal fatto che gli aggressori piazzano i propri server di controllo sulla rete Tor, che li rende difficili da individuare e disattivare.
- Bitcoin fa riferimento a un metodo di pagamento con valuta virtuale, che evita di lasciare quelle tracce che potrebbero far risalire agli aggressori.
- Locker indica che i file vengono tenuti bloccati o cifrati finché non viene pagato il riscatto.

CTB-Locker ha successo perché usa delle astute tecniche evasive per eludere il software di sicurezza, le sue email di phishing sono più credibili di altre, mentre il programma di affiliazione gli ha consentito di inondare il mercato molto rapidamente.

Perché CTB-Locker ha tanto successo? Innanzitutto perché usa delle astute tecniche di evasione per eludere il software di sicurezza. In secondo luogo perché le email di phishing usate nelle campagne di CTB-Locker sono più credibili rispetto a quelle di altre campagne di ransomware. Per esempio, questo malware usa dei nomi file con riferimenti ad aziende locali. Infine, la presenza di un programma di affiliazione ha consentito a CTB-Locker di inondare molto rapidamente il mercato con le campagne di phishing, prima che i sistemi venissero aggiornati con il software di sicurezza in grado di rilevare e contenere gli attacchi.

CTB-Locker viene distribuito in molti modi: IRC (Internet relay chat), reti peer-to-peer, post nei newsgroup, spam tramite email e altri. In questo trimestre abbiamo osservato un nuovo interessante metodo: l'utilizzo del ben noto downloader Dalexis. Per eludere gli strumenti antispam, il downloader è occultato in un file .zip, che contiene un altro file .zip, che infine si decompone in un file .scr (salvaschermo).

Dopo la sua esecuzione, CTB-Locker visualizza questa inquietante immagine:



Molte vittime di CTB-Locker vedono inizialmente questa immagine.

Condividi questo report



In una delle schermate successive, CTB-Locker offre gratuitamente la decrittografia di cinque file. Purtroppo, per ottenere le chiavi private e decifrarli, non si collega al proprio server di controllo. Se lo facesse, i ricercatori antimalware sarebbero in grado di appropriarsi delle chiavi e di studiarne i criteri. Invece, CTB-Locker memorizza le cinque chiavi private in un file di 600 byte dal nome casuale, situato nel disco del computer della vittima. Questa tecnica elimina la necessità di collegarsi al server che ospita la chiave privata della vittima.

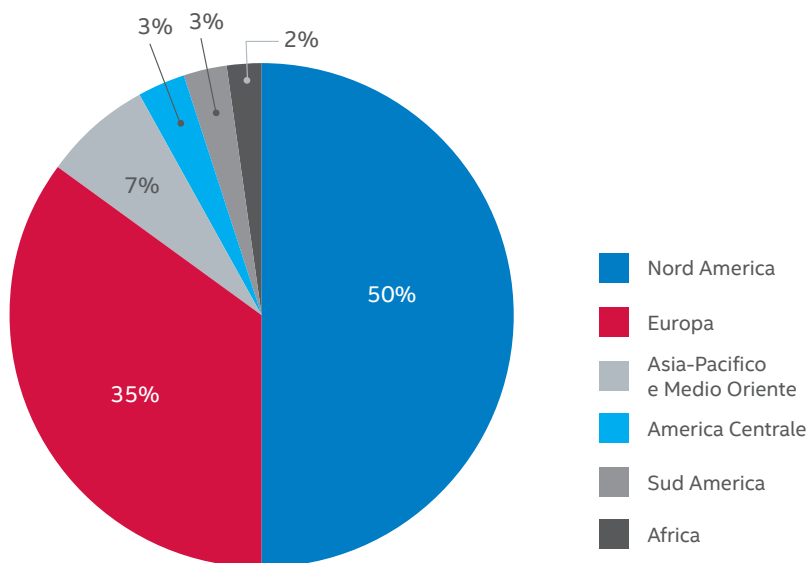
### L'escalation delle campagne di CTB-Locker

Le campagne che utilizzano CTB-Locker sono cominciate ai primi di dicembre 2014, ma gli attacchi di massa sono stati sferrati a partire dal gennaio 2015. CTB-Locker è stato rilevato in inglese, olandese, tedesco, francese e italiano. Le opzioni linguistiche si estendono agli allegati, il che fa sembrare la email di phishing più autentiche. Anche i nomi dei file sono stati localizzati:

- a\_la\_clinique\_vtrinaire\_lavalle.scr
- aliments\_universelles\_lolivier.scr
- alte\_poststr\_25\_72250\_freudenstadt.scr
- an\_der\_wassermhle\_3\_28816\_stuhr.scr
- andros\_consultants\_limited.scr
- b\_n\_r\_roofing\_2000\_ltd.scr
- b\_van\_brouwershaven\_and\_zn\_bv.scr
- bill39C6113.scr
- fairview\_rehab\_and\_sports\_injury\_clinic.scr
- fashioncrest\_ltd.scr
- feedback\_instruments\_ltd914.scr

Nonostante il multilinguismo del malware, la maggior parte delle vittime di CTB-Locker riscontrate da McAfee Labs si trova in Nord America:

Posizione delle vittime di CTB-Locker



Fonte: McAfee Labs, 2015

Condividi questo report



## I programmi di affiliazione di CTB-Locker

Nell'agosto 2014, il o gli autori di CTB-Locker hanno presentato il loro prodotto su diversi forum russi. Il programma di affiliazione fa parte di una vera e propria strategia commerciale.

L'autore ha offerto l'uso dell'infrastruttura di CTB-Locker per includere gli affiliati che utilizzano le loro botnet per inviare spam alle potenziali vittime. Per ogni infezione riuscita, con il pagamento del riscatto, l'affiliato riceve una percentuale.

In un forum clandestino, uno di essi ha spiegato le sue motivazioni. È entrato nel mondo ransomware semplicemente perché si tratta di un modo facile per lucrare denaro con un basso rischio di arresto. "La natura dell'infrastruttura di CTB-Locker ospitata da altri, l'utilizzo di Tor e i pagamenti con Bitcoin ne fanno un programma di cui far parte con sufficiente sicurezza. L'affiliato afferma di estorcere 15.000–18.000 dollari al mese, con un utile netto di 8.000–10.000 dollari. I suoi profitti dipendono dal numero di vittime che pagano, ma anche dal costo del kit di exploit, dai criptatori personalizzati e dal reindirizzamento del traffico. I paesi più redditizi sono Stati Uniti, Regno Unito, Australia e vari paesi europei. Secondo l'affiliato, le vittime che pagano il riscatto sono circa il 7 per cento del totale.

## La funzionalità di CryptoWall versione 3

Dal CryptoWall originale all'ultimo rilascio, la versione 3, sono cambiate molte funzioni. Il malware ora utilizza per i pagamenti esclusivamente Tor, ma comunica in diversi modi: tramite gli URL dei server di controllo codificati in modo fisso e occultati oppure attraverso una rete peer-to-peer basata sul protocollo I2P. Molte altre famiglie di ransomware hanno usato il nome CryptoLocker per fuorviare le vittime e l'industria della sicurezza. Anche CryptoWall lo ha fatto, ma dopo un po' di tempo ha cominciato a usare il proprio nome.

Come CTB-Locker, le ultime campagne di CryptoWall tentano inoltre di eludere i meccanismi di protezione utilizzando un allegato in JavaScript alle email, anche se CryptoWall scarica dei file .jpeg anziché .zip. Comunque non sono presenti immagini per ingannare le vittime, ma solo gli eseguibili del ransomware.

## Una nuova famiglia di ransomware: Teslacrypt



Nel primo trimestre è emerso Teslacrypt, che ha aggiunto i salvataggi dei videogiochi ai potenziali bersagli.



Nel febbraio 2015 è comparsa la nuova famiglia Teslacrypt. Nonostante si basi sul codice di CryptoLocker e ne presenti tutte le funzioni tipiche, fra cui l'utilizzo di Tor per occultarsi e di Bitcoin per i pagamenti, Teslacrypt possiede delle nuove funzionalità. Un membro della famiglia di Teslacrypt punta ai contenuti salvati dai videogiochi e ad altri file di contenuto aggiuntivo scaricabili. Vengono cifrati i file correlati a oltre cinquanta videogiochi, fra i quali:



Alcuni dei giochi colpiti da Teslacrypt.

Teslacrypt inoltre aggiunge l'opzione di pagare con PayPal My Cash Card. Per un'analisi più dettagliata di Teslacrypt, leggi [questo recente blog di McAfee Labs](#).

## Recupero dei dati

La domanda posta più di frequente sul ransomware è: "Si possono recuperare i dati cifrati?". La risposta è generalmente "No", a meno che si paghi il riscatto e i ladri forniscano la chiave privata. Le chiavi private del ransomware sono memorizzate nei server dei criminali e non si possono ottenere in nessun altro modo, a meno che si abbia accesso a tali server o a una copia.

Occasionalmente, un'agenzia governativa incaricata delle disattivazioni è in grado di sequestrare il server di controllo della campagna di ransomware. Se riesce ad accedere al database contenente le chiavi private di decrittografia, può poi compilare uno strumento per il recupero del file cifrato. Recentemente, il Centro Nazionale Olandese Contro il Crimine Tecnologico ha sequestrato il server di controllo della famiglia di ransomware CoinVault. In collaborazione con Kaspersky ha poi realizzato uno **strumento di recupero**.

Nel caso di CTB-Locker ci sono dei casi in cui i file possono essere recuperati. Se l'opzione Ripristino configurazione di sistema di Windows è stata attivata (nella maggior parte dei sistemi lo è per impostazione predefinita), i file si possono recuperare dalle copie shadow del volume. Il Servizio Copia Shadow del volume, detto anche VSS, è una tecnologia che esegue il backup manuale o automatico dei file, anche quando questi sono in uso. Da Windows XP fino a Windows 7 e Windows Server 2008 era implementata nel Servizio Copia Shadow del volume. A partire da Windows 8 non è più possibile sfogliare, cercare o ripristinare le vecchie versioni dei file tramite la scheda Versioni precedenti della finestra di dialogo Proprietà.

In Windows 8, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 e Windows Server 2012, le copie disponibili di un dato volume vengono elencate dal comando incorporato "Vssadmin list shadows". Per montare una copia di VSS dalla riga di comando e cercarne i file sono possibili vari metodi. Per sfogliare le copie shadow del volume sono a disposizione svariati strumenti open source. Con uno di essi può essere possibile ripristinare i file cifrati dal ransomware.

Condividi questo report



Questo metodo funziona con tutte le famiglie di ransomware? Sfortunatamente no. Con CryptoWall versione 3, Crypto-Fortress e Teslacrypt, gli autori del ransomware hanno aggiunto il seguente comando durante l'esecuzione del malware:

- `vssadmin delete shadows /all /quiet`

Ciò significa che tutte le copie shadow del volume vengono silenziosamente eliminate. Tuttavia, con il software di ripristino e conoscendo i valori di offset utilizzati, potrebbe essere possibile recuperare i volumi eliminati.

### Cosa ci riserva il futuro?

Compariranno nuove varianti e famiglie, oltre a diverse tecniche e funzionalità. All'inizio di quest'anno, per esempio, i ricercatori svizzeri hanno scoperto una nuova tecnica utilizzando riscatto e crittografia, che hanno battezzato RansomWeb. Con essa, gli aggressori infettano gli script dei server web e i campi dei database, poi attendono finché tali valori non vengono memorizzati per qualche settimana o mese nei backup e infine rimuovono la chiave dal server o dalla posizione remota. L'applicazione web e il database cominciano a funzionare male e vengono infettati anche i backup. A questo punto gli autori dell'attacco inviano la richiesta di riscatto.

### Pratiche sicure per proteggersi dal ransomware

Con l'attento monitoraggio dei feed di informazioni, McAfee Labs rimane più avanti delle campagne di ransomware. In tal modo può rilevare e bloccare la maggior parte del ransomware ancor prima che venga eseguito. E nessun pagamento in Bitcoins raggiungerà le tasche dei criminali.

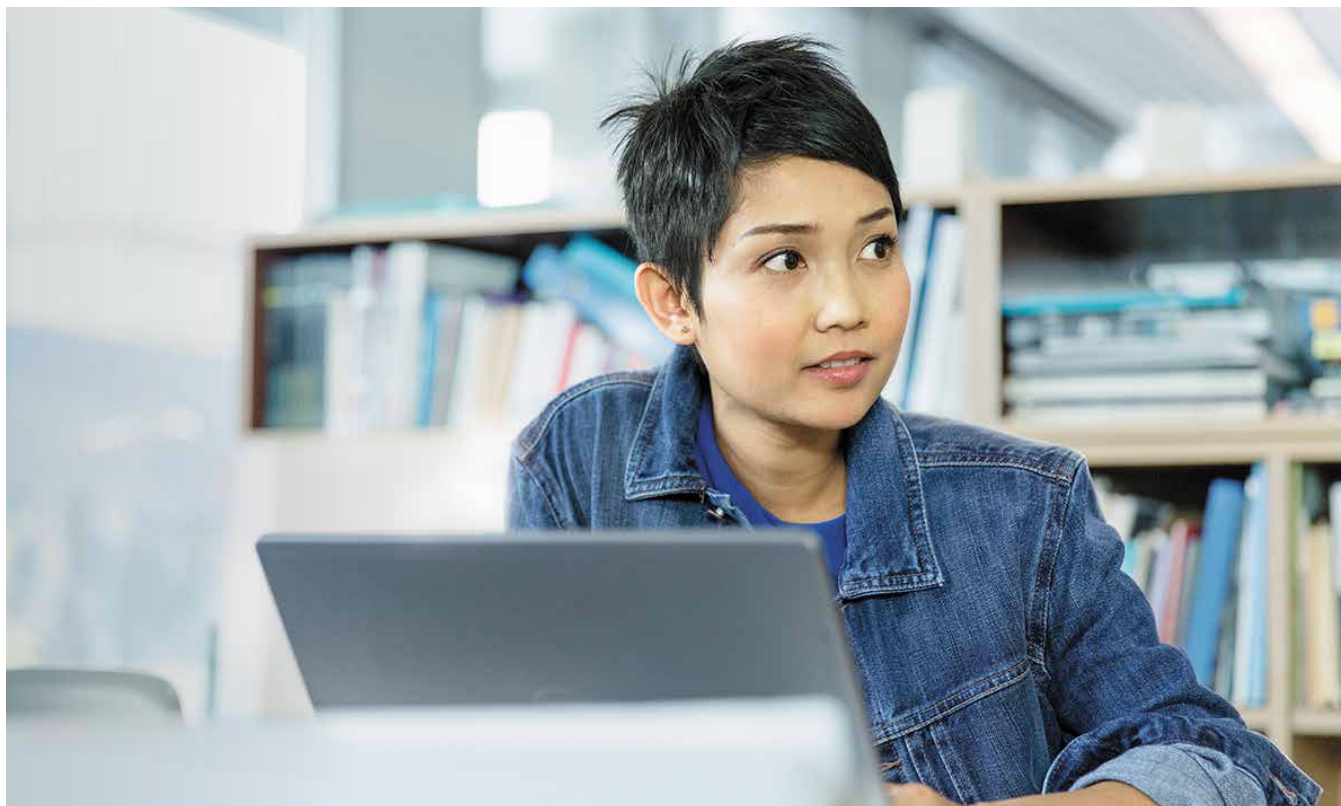
Policy e procedure adeguate includono:

- Eseguire il backup dei dati. Sembrerebbe un'ovvietà e invece troppo spesso non è previsto alcun backup oppure la relativa procedura non ha funzionato perché non era stata mai provata. I supporti di archiviazione removibili sono ampiamente diffusi, hanno un costo accessibile e sono facili da utilizzare. Gli utenti domestici dovrebbero eseguire il backup e poi scollegare il dispositivo e conservarlo in un luogo sicuro. Per i servizi di backup nel cloud, bisogna tenere presente che l'endpoint della vittima potrebbe subire la copia dei file cifrati nel cloud stesso. Alcuni servizi di backup basati sul cloud offrono la possibilità di ripristinare le versioni più recenti dei file.
- Sensibilizzare continuamente gli utenti. Dato che la maggior parte degli attacchi di ransomware inizia con un'email di phishing, la sensibilizzazione degli utenti è necessaria e di fondamentale importanza. Le statistiche indicano che, per ogni dieci email inviate dagli aggressori, almeno una ha successo. Non aprire le email o gli allegati provenienti da mittenti non verificati o sconosciuti.



Scopri in che modo Intel Security può proteggerti contro questa minaccia.

- Bloccare i programmi e il traffico indesiderati o non necessari. Se non c'è bisogno di usare Tor, l'applicazione e il suo traffico nella rete vanno bloccati. Bloccando Tor si impedisce spesso al ransomware di ottenere la chiave pubblica RSA dal server di controllo, fermando così il processo di cifratura del ransomware.
- Mantenere aggiornate le patch di sistema. Molte vulnerabilità comunemente sfruttate dal ransomware possono essere coperte dalle patch. Mantenere aggiornati con le patch i sistemi operativi, Java, Adobe Reader, Flash e le applicazioni. Implementare una procedura di applicazione delle patch e verifica che siano state applicate correttamente.
- Utilizzare un antispam. La maggior parte delle campagne di ransomware inizia con un'email di phishing contenente un collegamento o un determinato tipo di allegato. Nel caso delle campagne di phishing che comprimono il ransomware in un file .scr o in qualche altro formato di file poco comune è facile impostare una regola antispam per bloccare tali allegati. Se i file .zip riescono a passare, va eseguita la scansione di almeno due livelli di ogni file .zip per cercare i possibili contenuti nocivi.
- Proteggere gli endpoint. Usa la protezione per gli endpoint e le sue funzioni avanzate. In molti casi, il client è installato con abilitate le sole funzionalità predefinite. Utilizzando alcune funzioni avanzate, come ad esempio "Blocca gli eseguibili della cartella Temp", si può rilevare e bloccare un maggior numero di malware.



# Adobe Flash: il più amato da sviluppatori e criminali informatici

*Arun Pradeep e Santosh Surgihalli*

Una definizione del popolare programma Adobe Flash è "piattaforma software e multimediale usata per creare grafica vettoriale, animazioni, giochi e applicazioni Internet ricche di funzionalità [...] che possono essere visualizzate, riprodotte ed eseguite in Adobe Flash Player".<sup>3</sup>

Un'altra ugualmente accurata definizione potrebbe descrivere Adobe Flash come "piattaforma software e multimediale usata con molto successo dai criminali informatici per colpire le vittime con un crescente numero di dispositivi che eseguono vecchie versioni di Flash".

In questo argomento principale esaminiamo Adobe Flash (chiamato in precedenza Macromedia Flash e Shockwave Flash): come funziona, il crescente numero di vulnerabilità ed exploit, il modo in cui i criminali informatici li sfruttano e ciò che possono fare le organizzazioni per proteggersi da questi exploit di Flash.

## La piattaforma Adobe Flash

Il nucleo della piattaforma Adobe Flash è composto di tre elementi.

- Il linguaggio di programmazione orientata agli oggetti ActionScript, open source e indipendente dalla piattaforma, che può essere utilizzato per descrivere azioni multimediali fra cui le animazioni, la gestione di eventi interattivi (in primo luogo per gli sviluppatori di videogiochi) e lo streaming audio e video.
- Lo strumento autoriale Adobe Flash Professional, usato per creare applicazioni multimediali in linguaggio ActionScript. I file del codice sorgente hanno l'estensione .fla. Le applicazioni multimediali compilate, ovvero i file dei filmati Flash, hanno l'estensione .swf.
- Il motore di runtime Adobe Flash Player, che esegue i file .swf. Differenti versioni funzionano autonomamente o all'interno dei browser web come plug-in su svariati endpoint: computer desktop, portatili, tablet e smartphone.

Gli strumenti di terze parti aiutano a creare, eseguire o gestire i file .swf.

L'uso della grafica vettoriale, combinata con il codice programma, consente una dimensione ridotta dei file dei filmati Flash e pertanto lo streaming usa meno larghezza di banda rispetto agli analoghi file bitmap o ai video clip. Il risultato è che Flash Player è diventato una delle applicazioni più installate per la visualizzazione dei contenuti multimediali.

Ovviamente la sua popolarità ha attirato anche gli autori del malware.



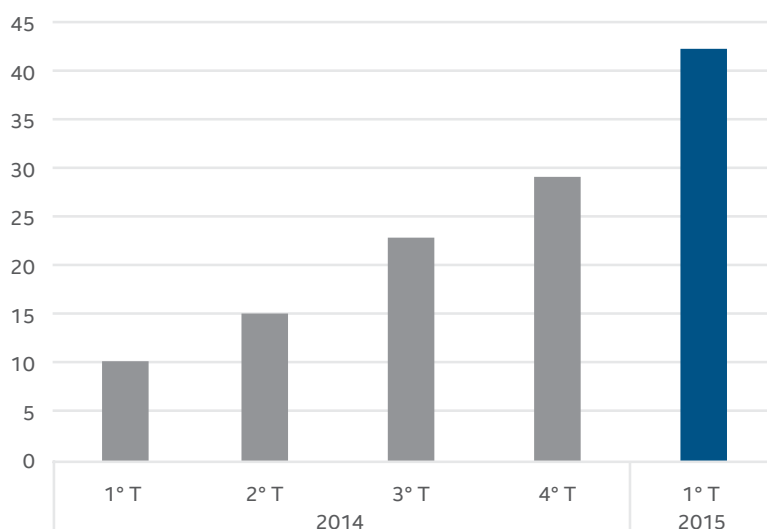
## Gli exploit in Flash

Le vulnerabilità del software vengono solitamente segnalate al National Vulnerability Database, un archivio mantenuto dal National Institute of Standards and Technology, e ivi monitorate. Una vulnerabilità riconosciuta viene monitorata tramite il suo codice **CVE (Common Vulnerabilities and Exposures, Vulnerabilità ed esposizioni comuni)**.

Nel primo trimestre, al database sono state aggiunte 42 nuove CVE di Flash, un aumento del 50% rispetto alle 28 vulnerabilità Flash riscontrate nel quarto trimestre del 2014. Anzi, dall'inizio del 2014 c'è stato un aumento costante nel numero di vulnerabilità Flash. L'ultimo periodo ha visto il più alto numero di vulnerabilità mai segnalato in un trimestre.

Nel primo trimestre sono state individuate 42 nuove vulnerabilità di Flash, un aumento del 50% rispetto alle 28 riscontrate nel quarto trimestre del 2014. È il più alto numero di vulnerabilità di Flash segnalato in un singolo trimestre.

Nuove vulnerabilità



Fonte: National Vulnerability Database

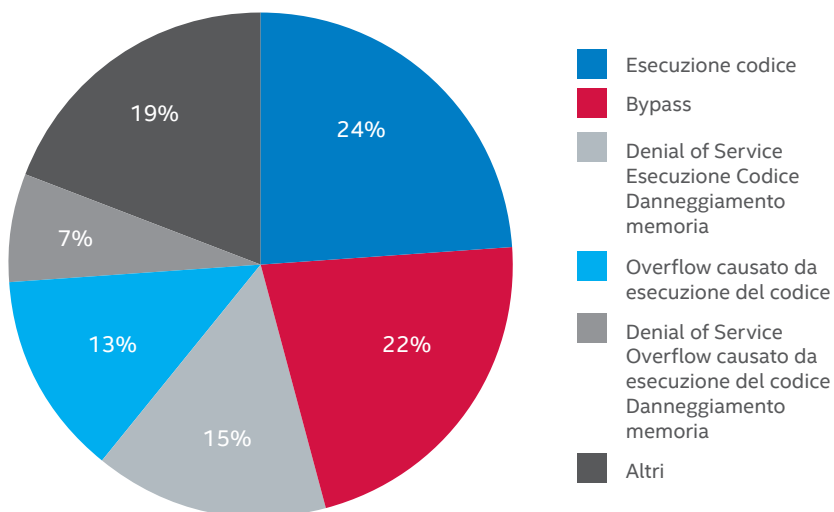
Alcune delle vulnerabilità Flash più recenti sono probabilmente il risultato del **programma di divulgazione delle vulnerabilità** creato da Adobe alla fine del 2014 per coordinare la divulgazione e correzione con patch delle vulnerabilità delle applicazioni web di Adobe. Non solo, Adobe ha messo a disposizione le correzioni iniziali per tutte le 42 nuove vulnerabilità Flash scoperte nel primo trimestre lo stesso giorno in cui venivano registrate le CVE.

Le informazioni sulle attuali correzioni per le vulnerabilità di Flash sono reperibili **qui**. Inoltre, Adobe fornisce delle indicazioni sulla rapidità con la quale i clienti dovrebbero aggiornare i rispettivi prodotti Adobe, in base alla gravità delle vulnerabilità. Le indicazioni sono reperibili **qui**.

Le vulnerabilità .swf in Flash sono di vari tipi:

- Bypass: Flash Player non limita correttamente la scoperta degli indirizzi di memoria, il che permette agli aggressori di bypassare in Windows il meccanismo di protezione della funzionalità ASLR (Address Space Layout Randomization).
- Denial of service codice eseguibile danneggiamento della memoria: queste vulnerabilità permettono agli aggressori di eseguire un codice arbitrario o di causare un denial of service (danneggiamento della memoria) tramite vettori non specificati.
- Denial of service: queste vulnerabilità consentono all'autore dell'attacco di causare un denial of service (dereferenziazione puntatore NULL) o magari di creare altri impatti non specificati tramite vettori sconosciuti.
- Overflow causato da esecuzione del codice: le vulnerabilità da overflow del buffer consentono agli aggressori di eseguire del codice arbitrario tramite dei vettori non specificati.
- Esecuzione codice: le vulnerabilità "use-after-free" consentono agli aggressori di eseguire del codice arbitrario tramite vettori non specificati.

Vulnerabilità mirate Adobe Flash



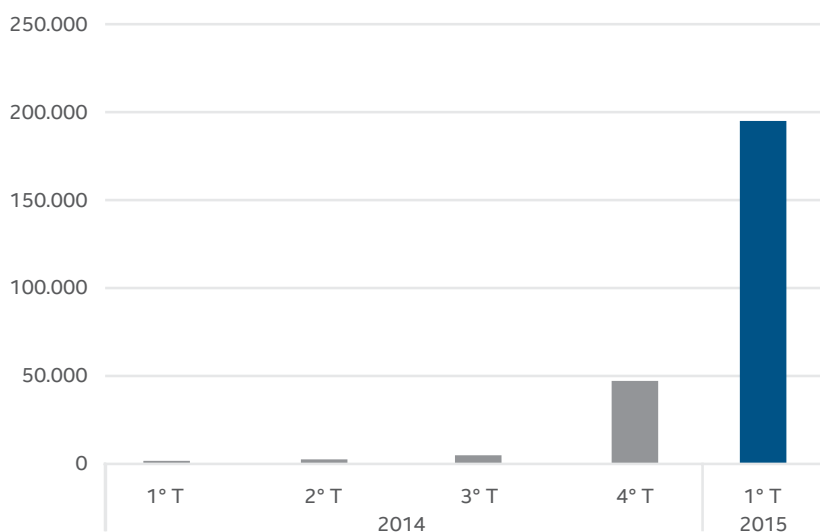
Fonte: McAfee Labs, 2015

## Prevalenza degli exploit di Flash

Gli exploit di Flash hanno cominciato ad aumentare drasticamente nell'ultimo trimestre del 2014. Le vulnerabilità Flash sono fra i principali bersagli degli autori degli exploit. McAfee Labs attribuisce questo fatto a diversi fattori: il costante aumento delle vulnerabilità Flash; il ritardo degli utenti nell'applicare le patch software disponibili che eliminano le vulnerabilità Flash; nuovi e creativi metodi per sfruttare tali vulnerabilità; il notevole aumento nel numero di dispositivi mobili in grado di riprodurre i file .swf e la difficoltà nel rilevare gli exploit di Flash.

Nel primo trimestre il numero di nuovi campioni .swf di Adobe Flash è aumentato del 317%. I campioni includono file puliti, file infetti o con malware e file sconosciuti.

Nuovi esempi .swf di Adobe Flash



Fonte: McAfee Labs, 2015

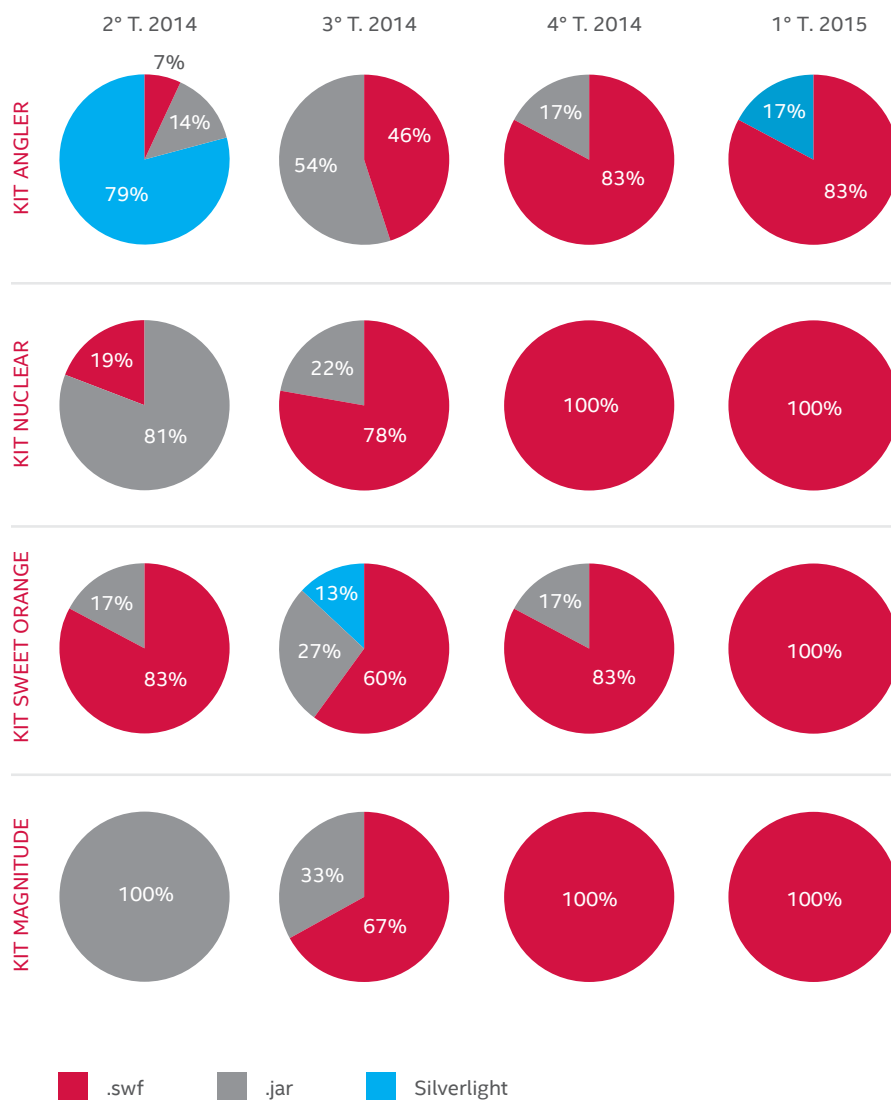
Condividi questo report



Fra i kit di exploit per Flash, Angler è quello più diffuso. Questo potente kit, descritto dettagliatamente nel **Report McAfee Labs sulle minacce: febbraio 2015**, è un toolkit già pronto e di facile utilizzo che può inviare svariati payload tramite lo sfruttamento delle vulnerabilità. Come mostrato nei seguenti grafici, Angler e gli altri principali kit di exploit hanno spostato la loro attenzione dalle vulnerabilità .jar (archivi Java) e Microsoft Silverlight a quelle di Flash.

I kit di exploit hanno spostato la loro attenzione dalle vulnerabilità degli archivi Java e di Microsoft Silverlight a quelle di Adobe Flash.

### Kit di exploit prendono di mira le vulnerabilità

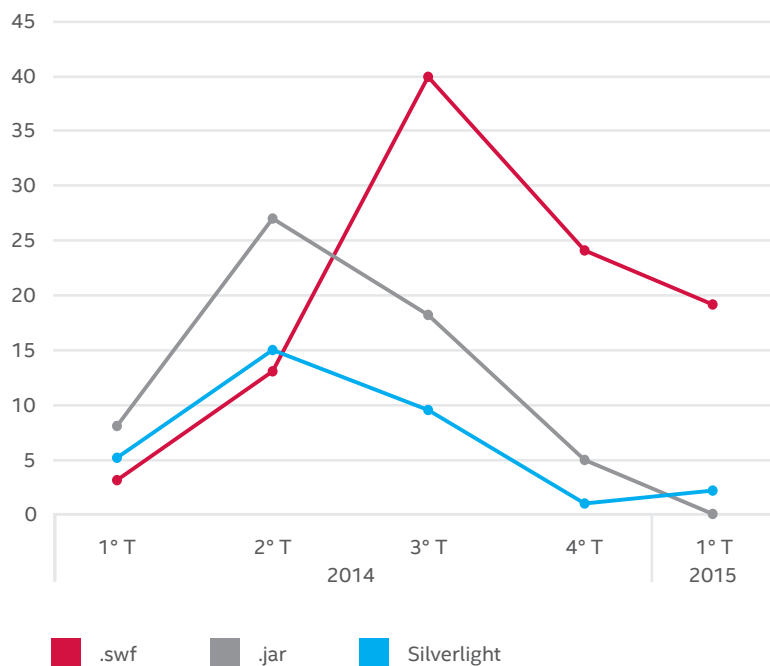


I quattro exploit principali ora si concentrano quasi esclusivamente sullo sfruttamento delle vulnerabilità di Flash.



Il grafico seguente illustra la tendenza delle vulnerabilità colpite dai vari kit di exploit:

Vulnerabilità di Adobe Flash prese di mira dai kit di exploit



Fonte: McAfee Labs, 2015

### Perché gli autori del malware colpiscono Flash?

Una delle ragioni per le quali gli autori degli attacchi puntano a Flash è il costante aumento del numero di vulnerabilità, unito al ritardo con il quale gli utenti applicano le relative patch software. Le maggiori opportunità ne rendono facile lo sfruttamento.

Un'altra ragione è il rapido aumento del numero di dispositivi mobili. La maggior parte di essi include la tecnologia per eseguire i file .swf, che aumenta notevolmente la popolarità di Flash come vettore dell'attacco.

Prendiamo in considerazione altri due motivi della popolarità di questa forma di attacco.

## Le ultime vulnerabilità Flash scoperte

Nell'esempio seguente, tratto da CVE-2014-0497, un file .swf artefatto per scopi illeciti offre un ActionScript di facile lettura, contenente funzioni e operazioni per l'esecuzione del codice shell.

Possiamo vedere che l'autore del malware usa un algoritmo per verificare la versione di Flash Player e assemblare una catena ROP correlata. Il malware quindi genera un codice shell per sfruttare la vulnerabilità.

```
if("win 11,7,700,202" !== _loc7_)
{
    if("win 11,7,700,224" !== _loc7_)
    {
        return null;
    }
    _loc5_ = _loc5_ - 10450228;
    _loc6_ = _loc5_ + 13082624;
    _loc4_.writeUnsignedInt(_loc5_ + 4646881);
    _loc4_.position = 64;
    _loc4_.writeUnsignedInt(_loc5_ + 52090);
    _loc4_.position = 76;
    _loc4_.writeUnsignedInt(_loc5_ + 4293);
    _loc4_.writeUnsignedInt(_loc5_ + 9376924);
    _loc4_.writeUnsignedInt(_loc5_ + 93510);
    _loc4_.writeUnsignedInt(_loc5_ + 1145378);
    _loc4_.writeUnsignedInt(_loc5_ + 1909483);
    _loc4_.writeUnsignedInt(param2);
    _loc4_.writeUnsignedInt(4096);
    _loc4_.writeUnsignedInt(64);
    _loc4_.writeUnsignedInt(param2 - 4);
}
```

Codice che crea una programmazione orientata all'istruzione return (ROP).

Ora vediamo una schermata di codice tratta dal famoso exploit Pixel Bender del 2014:

```
public function sadad(param1:int) : *
{
    if(param1 == 1)
    {
        return "A501-0-000-00A-4-0B-003-17279-7-37-4616C6C6-9-7-A32A0-0-C6-E-6-16D-657-3706163-65-0-0317-2797374-6-16-C6C697A-3-22-0627-9-205065-747-28-9-2";
    }
    if(param1 == 2)
    {
        return "EB4-89-090-9-09090-90-9-090909-090-90-90-9090-909-0-9-0909090-9-09-09090-90-909090-90909090-909-090-90909-0-9-09090909-0-909090-90-9090";
    }
}

function read_memory(param1:Vector.<int>, param2:uint, param3:uint) : uint
{
    if(param3 >= param2)
    {
        return param1[(param3 - param2) / 4];
    }
    return param1[1073741824 - (param2 - param3) / 4];
}
```

Codice shell inserito a codifica fissa nell'exploit Pixel Bender.

Il codice ActionScript decompilato possiede due comandi di codice shell (in rosso) a codifica fissa. Dopo lo smascheramento possiamo vedere il codice per lo sfruttamento della vulnerabilità.

Condividi questo report





## Nuovi metodi per sfruttare Flash

Gli exploit tramite pubblicità contraffatte su siti legittimi usano l'algoritmo RC4 per occultare il codice nocivo. I recenti exploit CVE-2015-0311, CVE-2015-0312 e CVE-2015-0313 usano questa tecnica per occultare exploit e codice shell.

```
private function InitEx() : void
{
    ggew = jtyk.xxfrh();
    var _loc1_* = kryuje.wecy();
    var _loc2_* = new RegExp("[3892754016]+", "g");
    var _loc3_* = "15814670395a839d024B304y549t110e672s730".replace(_loc2_, "");
    _loc1_[_loc3_] (ggew);
    stage.addChild(_loc1_);
}
```

Cifratura della funzione loadBytes.

Nella precedente funzione principale, la variabile `_loc3_` contiene il dato cifrato 15814670395a839d024B304y549t110e672s730. Eliminando le cifre si legge "loadBytes", comando che carica in Flash Player una matrice di byte (probabilmente contenente i tipi di file .swf, .gif, .jpeg o .png).

La variabile `_loc1_` chiama un'altra funzione privata che restituisce la stringa `new Loader()`, come segue:

```
public function kryuje()
{
    super();
}

public static function wecy() : Loader
{
    var _loc1_* = new Loader();
    return _loc1_;
}
```

Assegnazione della funzione `new Loader` a una variabile.

L'array di byte o i dati binari per il carico si trova nella variabile `ggew`, che chiama la funzione `jytk`. Questa funzione pubblica include i dati binari che è decrittografato e caricato utilizzando il caricatore. Circa 60 kB di dati binari devono essere decrittografati, utilizzando l'algoritmo RC4, come mostrato qui:

```
public static function xxfrh() : *
{
    var _loc1:* = wigr(ejtey.ybe);
    var _loc2:* = kyte();
    var _loc3:* = new ejtey.vree();
    var _loc4:* = 0;
    var _loc5:* = 0;
    var _loc6:* = 0;
    var _loc7:* = 0;
    var _loc8:* = 0;
    var _loc9:* = 0;
    var _loc10:* = 0;
    _loc4_ = 0;
    while(_loc4_ < 256)
    {
        _loc3[_loc4_] = _loc4_;
        _loc4_++;
    }
    _loc3[ejtey.fhrw] = 0;
    _loc4_ = 0;
    while(_loc4_ < 256)
    {
        _loc8_ = (_loc2[_loc7_] & 255) + (_loc3[_loc4_] & 255) + _loc8_ & 255;
        _loc10_ = _loc3[_loc4_];
        _loc3[_loc4_] = _loc3[_loc8_];
        _loc3[_loc8_] = _loc10_;
        _loc7_ = (_loc7_ + 1) % _loc2[ejtey.weruji];
        _loc4_++;
    }
    _loc3[ejtey.fhrw] = 0;
    _loc4_ = 0;
    while(_loc4_ < _loc1[ejtey.weruji])
    {
        _loc5_ = _loc5_ + 1 & 255;
        _loc6_ = (_loc3[_loc5_] & 255) + _loc6_ & 255;
        _loc10_ = _loc3[_loc5_];
        _loc3[_loc5_] = _loc3[_loc6_];
        _loc3[_loc6_] = _loc10_;
        _loc9_ = (_loc3[_loc5_] & 255) + (_loc3[_loc6_] & 255) & 255;
        _loc1[_loc4_] = _loc1[_loc4_] ^ _loc3[_loc9_];
        _loc4_++;
    }
}
```

L'algoritmo RC4 nel dettaglio.

Dopo lo smascheramento del codice otteniamo:

```
"Loader.LoadBytes(RC4_decode(RC4_encrypted_data))"
```

Questo comando carica i dati decifrati, che generano la catena ROP dalle DLL di Flash per caricare in maniera dinamica il codice shell ed eseguire l'exploit.



Scopri in che modo Intel Security può proteggerti contro questa minaccia.

Diversamente dai precedenti attacchi basati su Flash, nei quali il codice di exploit o il codice shell erano facilmente rilevati dai prodotti antimalware, questi nuovi attacchi includono più livelli anti-rilevamento che nascondono efficacemente i comportamenti anche ai prodotti di sicurezza più sofisticati. La creatività di tale metodo dimostra chiaramente il livello di sofisticazione e complessità raggiunto da questi exploit.

### Protegersi contro gli exploit delle vulnerabilità Flash

McAfee Labs raccomanda diversi modi con cui proteggere i sistemi contro gli attacchi basati su Flash:

- Installare le patch per Flash non appena vengono distribuite. Solitamente le patch sono disponibili lo stesso giorno in cui viene riportata una CVE di Flash. Le informazioni sugli attuali aggiornamenti per Flash sono reperibili qui. Un computer pienamente coperto dalle patch è una difesa robusta contro gli attacchi informatici.
- Attivare gli aggiornamenti automatici del sistema operativo oppure scaricarli regolarmente per mantenere il sistema coperto con le patch per le vulnerabilità note.
- Configurare il software antivirus per la scansione automatica di tutti gli allegati di email e i messaggi istantanei. Accertarsi che i programmi di posta elettronica non aprano automaticamente gli allegati o eseguano automaticamente il rendering della grafica; disattivare il riquadro di anteprima.
- Configurare il software antivirus per bloccare gli allegati contenenti l'estensione .swf.
- Configurare le impostazioni di sicurezza del browser al livello medio o superiore.
- Usare un plug-in del browser per bloccare l'esecuzione di script e di iframe.
- Non installare plug-in browser non attendibili.
- Usare estrema cautela durante l'apertura degli allegati, soprattutto quelli con l'estensione .swf.
- Non aprire mai le email indesiderate o gli allegati inattesi, anche se provenienti da persone conosciute.
- Fare attenzione al phishing basato sullo spam: evitare di fare clic sui link presenti nelle email o nei messaggi immediati.
- Digitare gli URL oppure copiarli nella barra degli indirizzi del browser per verificarli, anziché fare clic sulle pubblicità nel web.
- Non fare clic sui filmati in Flash o sui siti web non attendibili.



# Statistiche sulle minacce

Malware mobile  
Malware  
Minacce web

Minacce per reti  
e messaggistica

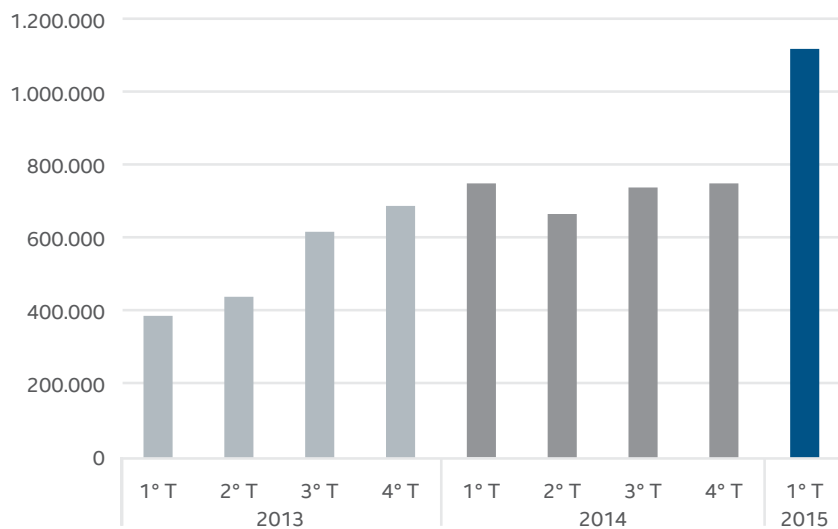
Inviaci la tua opinione



## Malware mobile

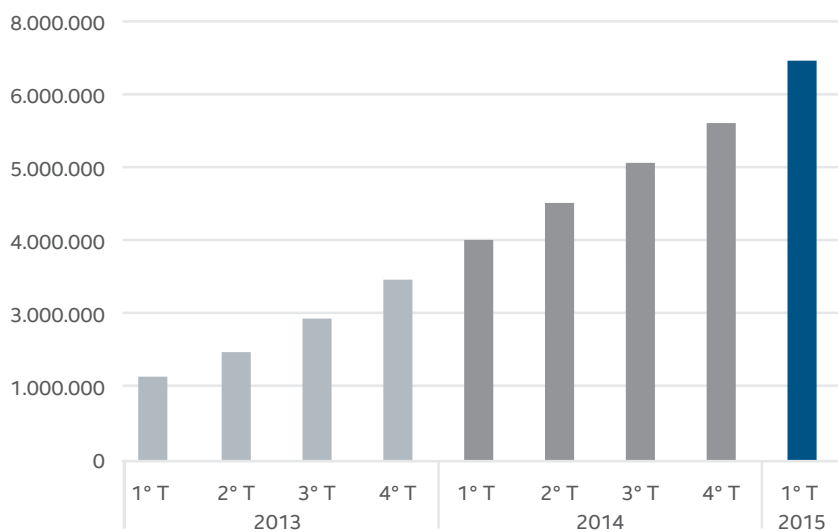
Il numero di nuovi esempi di malware mobile ha compiuto un balzo del 49% dal quarto trimestre 2014 al primo trimestre 2015.

Nuovo malware mobile



Fonte: McAfee Labs, 2015

Malware mobile complessivo



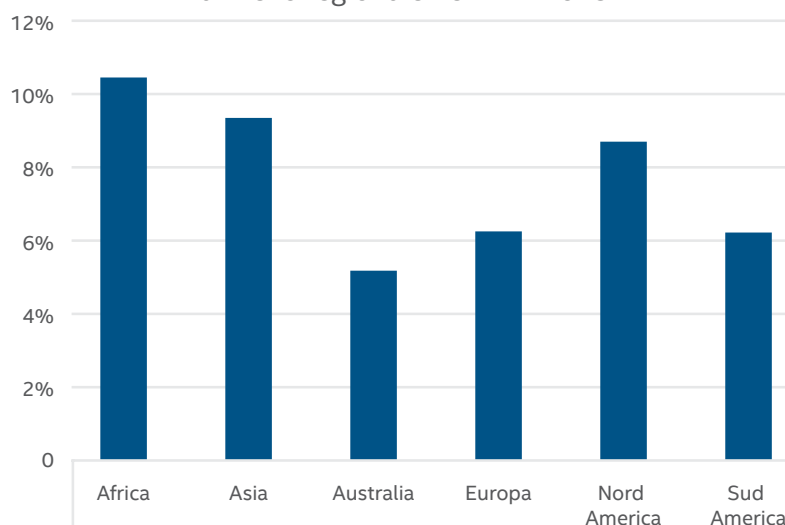
Fonte: McAfee Labs, 2015

Condividi questo report



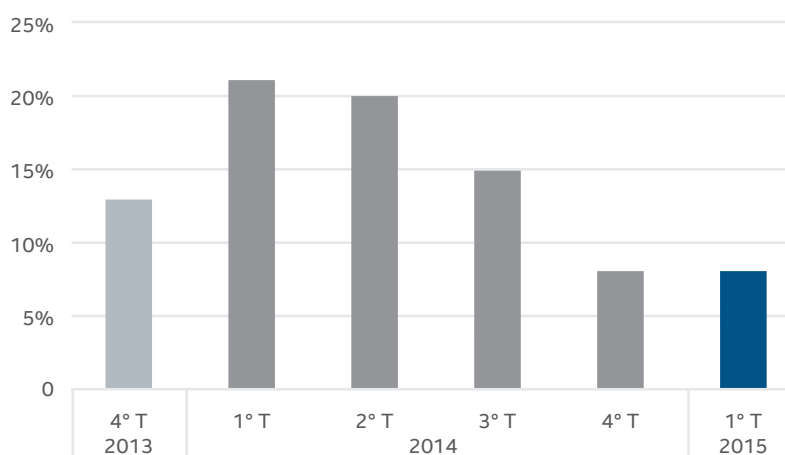


Percentuali di infezione da malware mobile  
a livello regionale nel 1° T. 2015



Fonte: McAfee Labs, 2015

Percentuale di infezione da malware mobile a livello mondiale

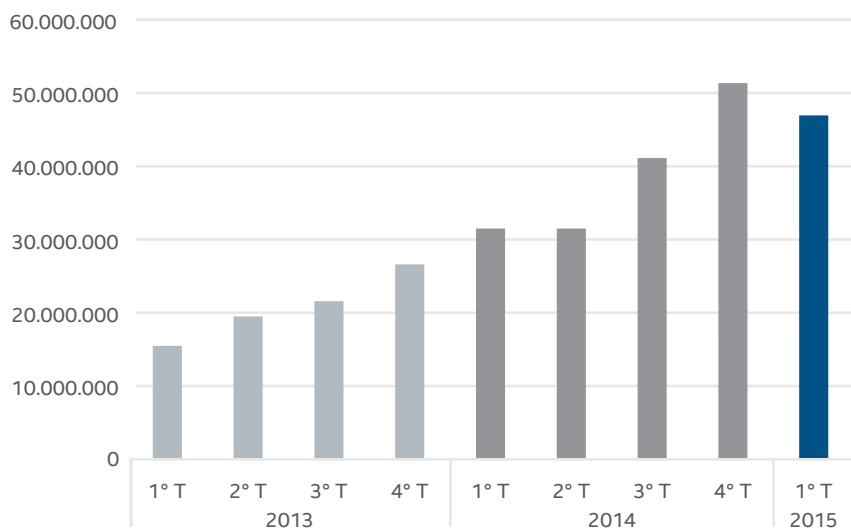


Fonte: McAfee Labs, 2015

## Malware

Il declino del nuovo malware in questo trimestre è dovuto principalmente a una famiglia di adware, SoftPulse, che nel primo trimestre è tornata ai livelli normali dopo il picco del quarto trimestre.

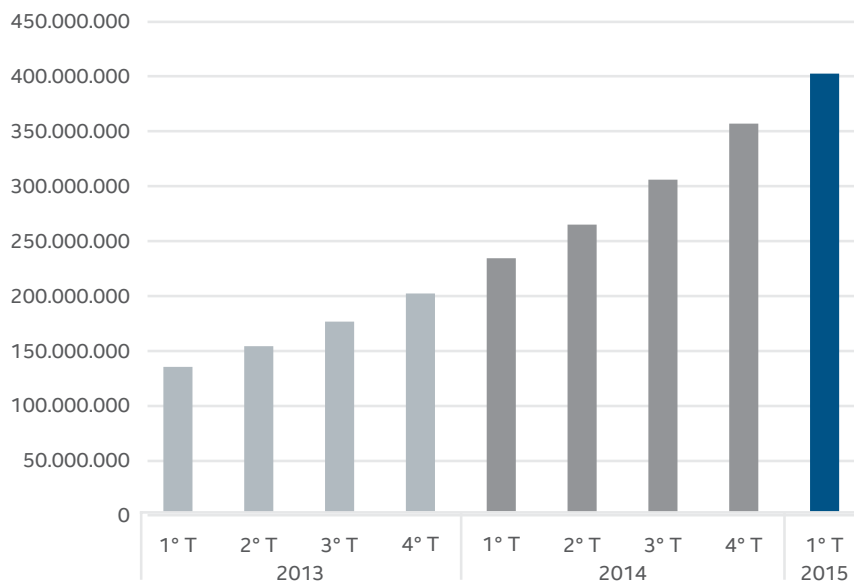
Nuovo malware



Fonte: McAfee Labs, 2015

Il campionario di malware di McAfee Labs è cresciuto del 13% dal quarto trimestre 2014 al primo trimestre 2015. Ora contiene 400 milioni di campioni.

Malware complessivo

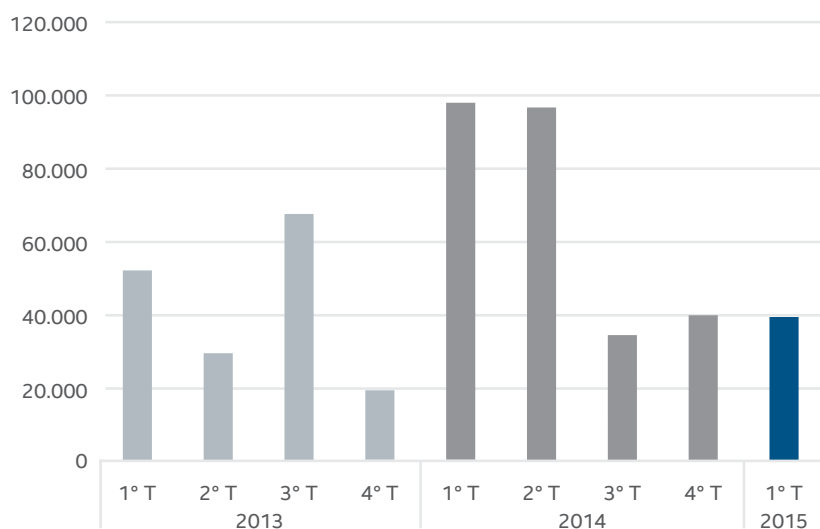


Fonte: McAfee Labs, 2015

Condividi questo report

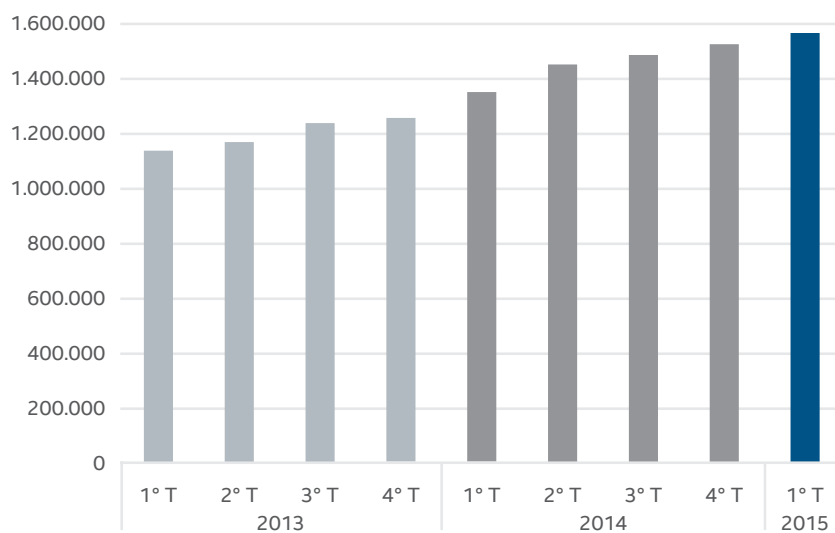


### Nuovo malware rootkit



Fonte: McAfee Labs, 2015

### Malware rootkit complessivo

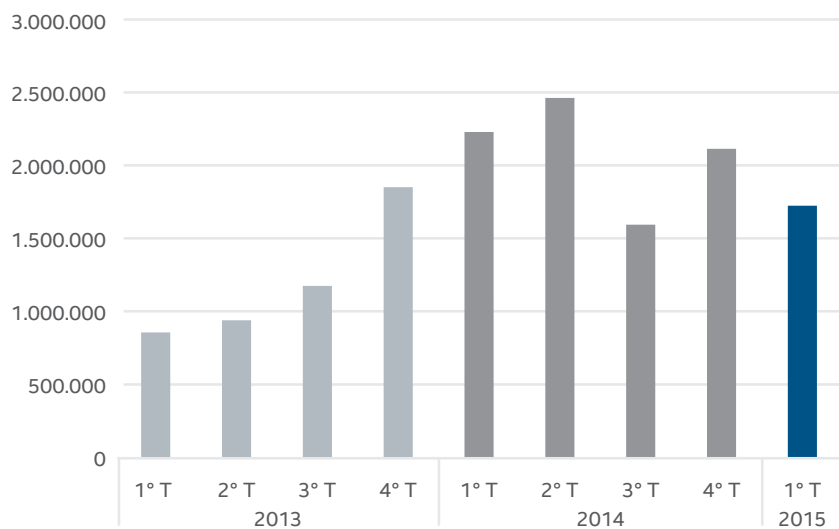


Fonte: McAfee Labs, 2015

Condividi questo report

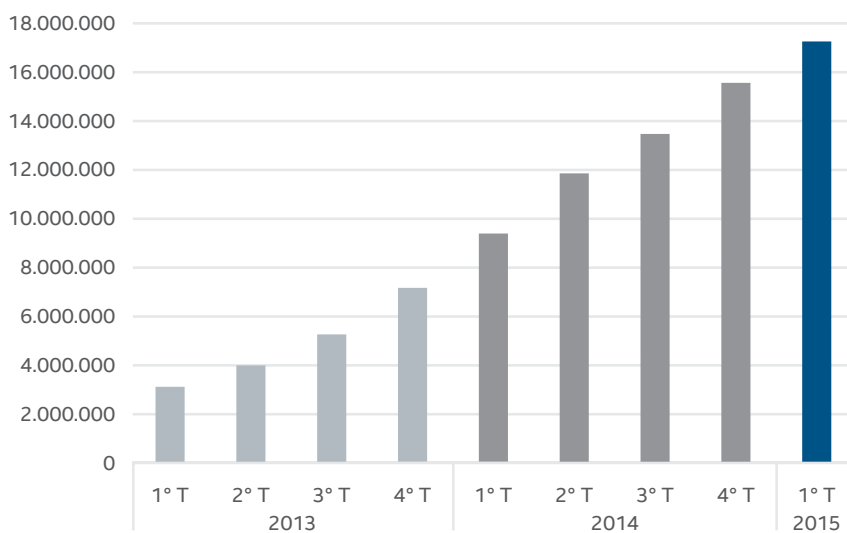


### Nuovi numeri binari firmati pericolosi



Fonte: McAfee Labs, 2015

### N. complessivo di file binari certificati pericolosi



Fonte: McAfee Labs, 2015

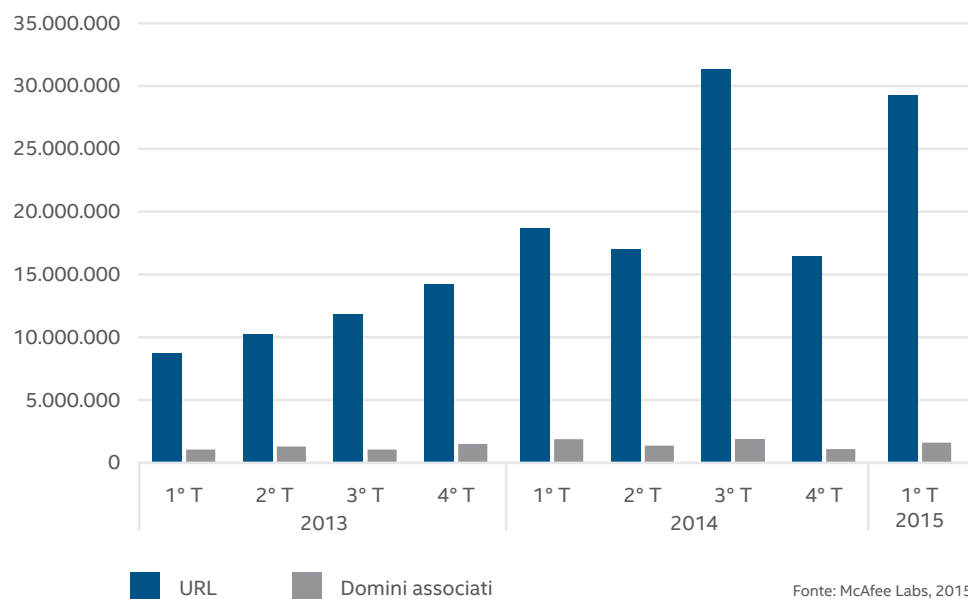
Condividi questo report



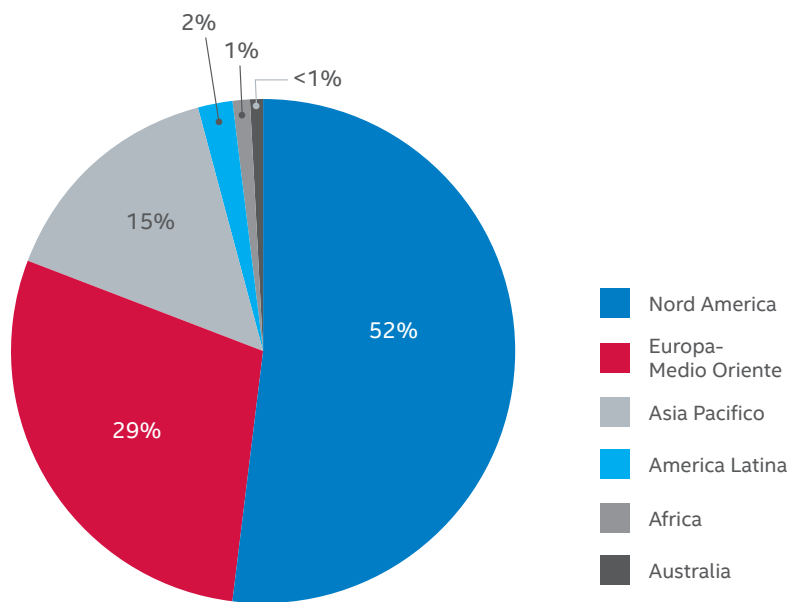
## Minacce web

Nel terzo trimestre 2014 abbiamo spiegato il forte aumento di nuovi URL sospetti con un aumento negli URL abbreviati malevoli. Nel primo trimestre 2015 abbiamo osservato lo stesso aumento, ma non a causa degli URL abbreviati malevoli. Non ne conosciamo ancora la causa.

Nuovi URL sospetti



Posizione dei server che ospitano contenuti sospetti

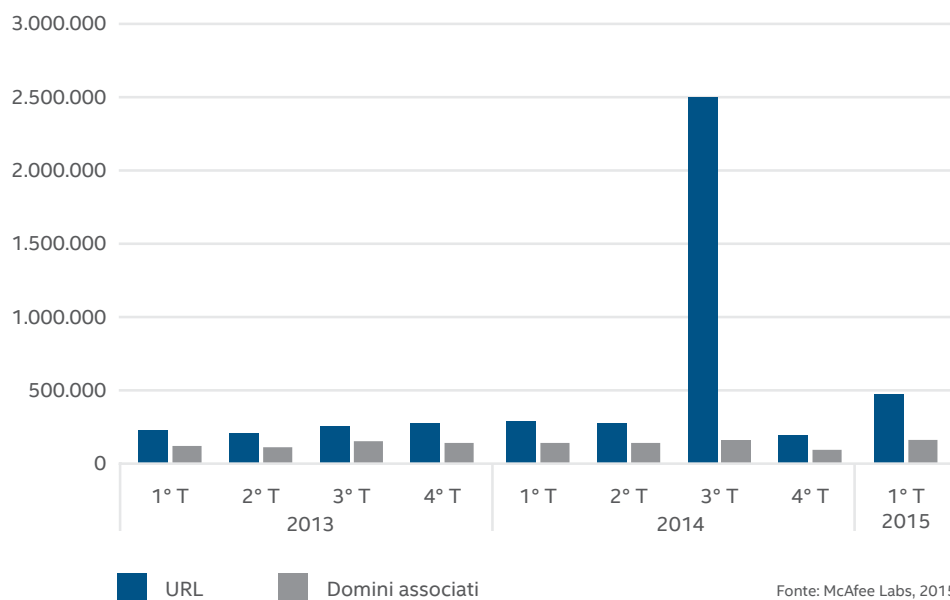


Condividi questo report

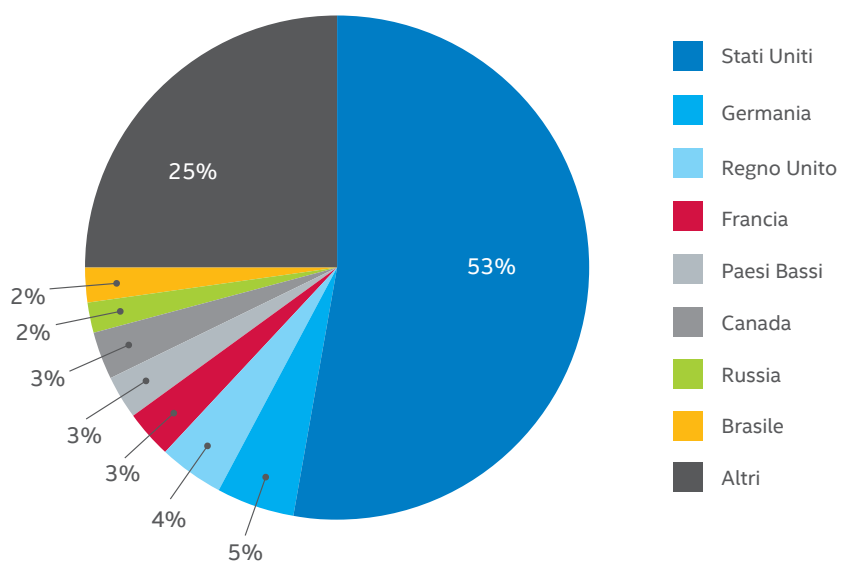




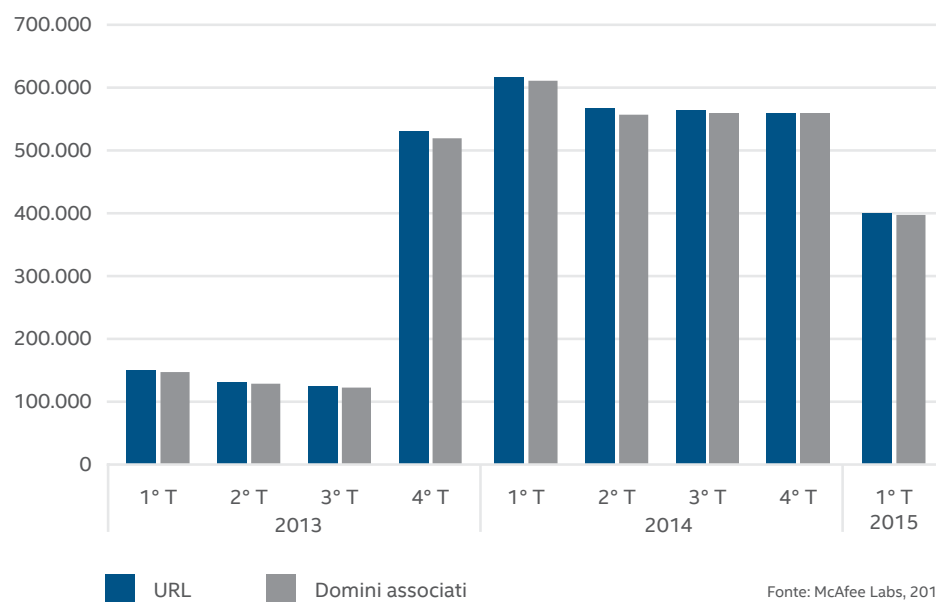
### Nuovi URL di phishing



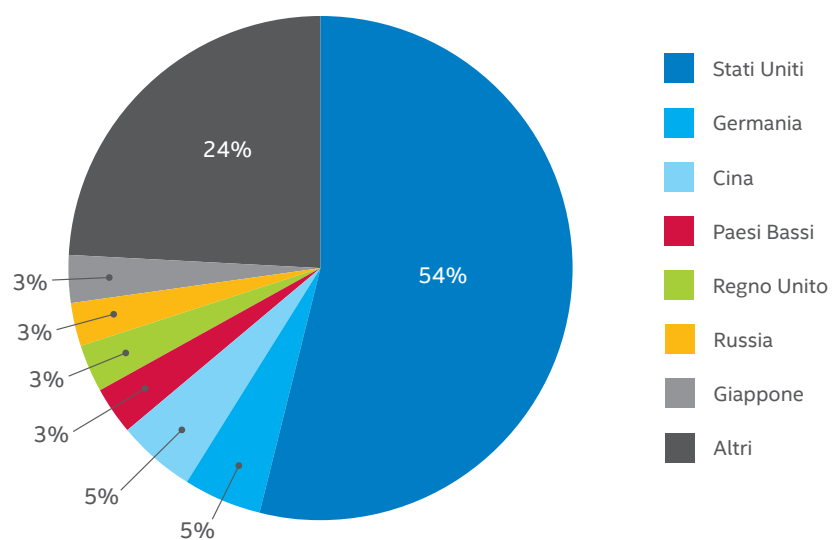
### Principali nazioni che ospitano domini di phishing



### Nuovi URL di spam

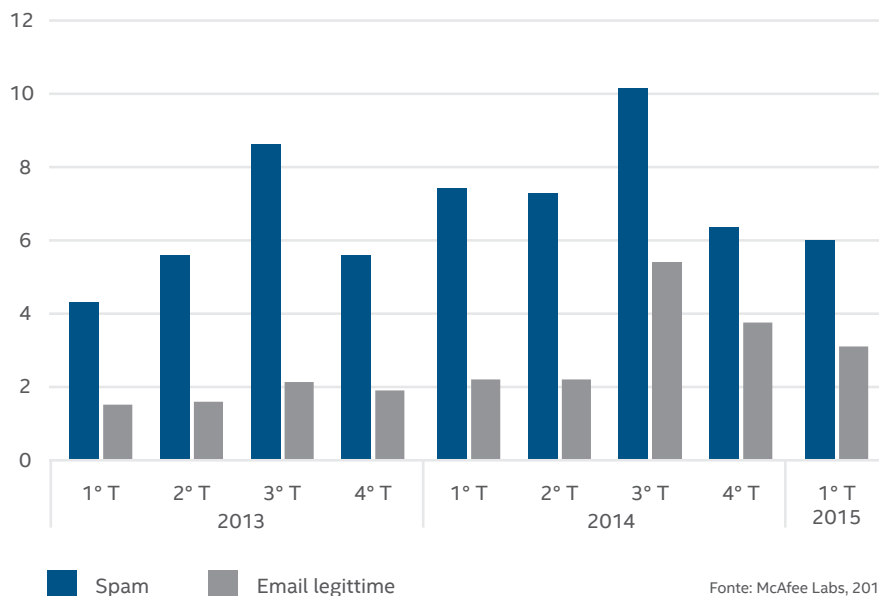


### Principali nazioni che ospitano domini di spam



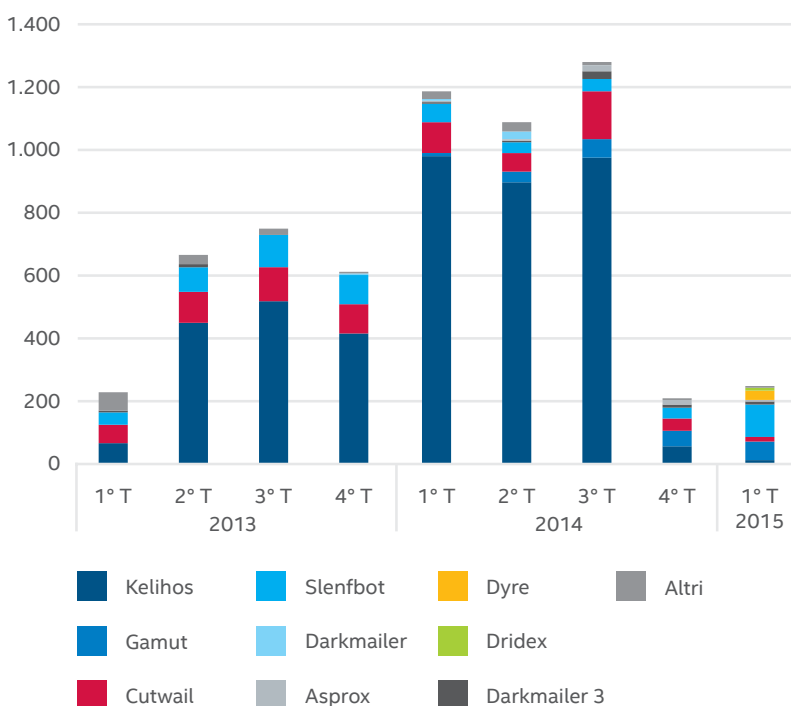
## Minacce per reti e messaggistica

Volume complessivo di spam ed email  
(bilioni di messaggi)



Nel primo trimestre i botnet Snowshoe, Festi e Darkmailer2 sono stati spodestati da Dyre, Dridex e Darkmailer3. Slenfbot, che invia lo spam in modo costantemente pervasivo, ha raggiunto la prima posizione durante il primo trimestre grazie alle sue campagne relative a farmaci, carte di credito rubate e strumenti ambigui per il marketing sulle reti sociali.

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

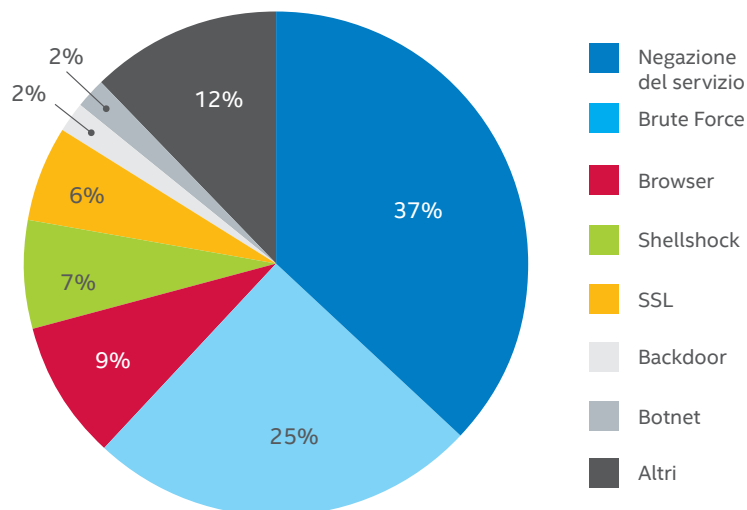


Condividi questo report



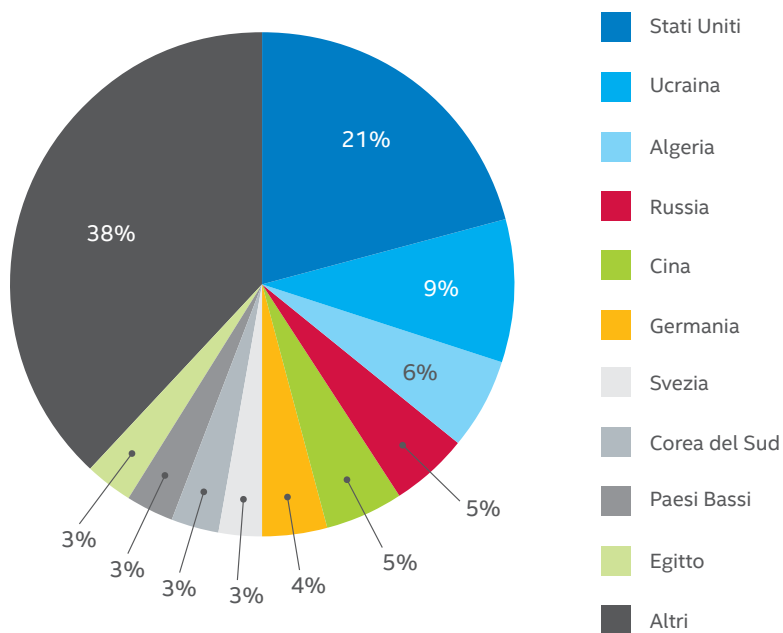
Gli attacchi correlati a SSL continuano, anche se rispetto al quarto trimestre 2014 sono calati in una certa misura. Tale riduzione è probabilmente il risultato degli aggiornamenti alla libreria SSL che hanno eliminato molte delle vulnerabilità sfruttate nei trimestri precedenti. Gli attacchi di Shellshock sono ancora piuttosto prevalenti, dopo la sua comparsa alla fine dell'anno scorso.

Principali attacchi di rete



Fonte: McAfee Labs, 2015

Principali sedi dei server di controllo delle botnet



Fonte: McAfee Labs, 2015

Condividi questo report





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

Segui McAfee Labs



## A proposito di Intel Security

McAfee è ora parte di Intel Security. Con la propria strategia Security Connected, l'approccio innovativo alla sicurezza potenziata dall'hardware e l'ineguagliato servizio Global Threat Intelligence, Intel Security è impegnata senza sosta nello sviluppo di soluzioni e servizi di sicurezza proattiva comprovati che proteggono sistemi, reti e dispositivi portatili per l'utilizzo aziendale e personale a livello mondiale. Intel Security combina l'esperienza e la competenza di McAfee con l'innovazione e le prestazioni comprovate di Intel per rendere la sicurezza un ingrediente essenziale di ogni architettura e di ogni piattaforma di elaborazione. La missione di Intel Security è di assicurare a chiunque la tranquillità di vivere e lavorare in modo sicuro e protetto nel mondo digitale.

[www.intelsecurity.com](http://www.intelsecurity.com)

1. <https://msdn.microsoft.com/en-us/library/windows/hardware/ff559309%28v=vs.85%29.aspx>.
2. [http://www.cse.scu.edu/~tschwarz/coen252\\_07/Resources/foi-computer-forensics.pdf](http://www.cse.scu.edu/~tschwarz/coen252_07/Resources/foi-computer-forensics.pdf).
3. [http://en.wikipedia.org/wiki/Adobe\\_Flash](http://en.wikipedia.org/wiki/Adobe_Flash).



**McAfee. Part of Intel Security.**

Via Fantoli, 7  
20138 Milano  
Italia  
(+39) 02 554171  
[www.intelsecurity.com](http://www.intelsecurity.com)

Le informazioni contenute nel presente documento sono fornite solo a scopo didattico e destinate ai clienti McAfee. Le informazioni qui contenute sono soggette a modifica senza preavviso e vengono fornite "COME SONO" senza garanzia o assicurazione relativamente all'accuratezza o all'applicabilità delle informazioni a situazioni o a circostanze specifiche.

Intel e il logo Intel sono marchi registrati di Intel Corporation negli Stati Uniti e/o in altri Paesi. McAfee e il logo McAfee sono marchi registrati o marchi di McAfee, Inc. o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. I piani, le specifiche e le descrizioni dei prodotti contenuti nel presente documento hanno unicamente scopo informativo, sono soggetti a variazioni senza preavviso e sono forniti senza alcun tipo di garanzia, esplicita o implicita. Copyright © 2015 McAfee, Inc. 61956rpt\_qtr-q1\_0615