TREND MICRO™ Securing Your Journey to the Cloud

Considerando le testimonianze dello scorso trimestre come suggerir

ONDATA CRESCENTE: NUOVI ATTACCHI MINACCIANO LE TECNOLOGIE PUBBLICHE

potremmo intravedere chiaramente l'arrivo di una nuova ondata di minacce che interesserà l persone a un livello più pronunciato e fisico. Gli aggressori hanno individuato ulteriori lacune sicurezza da sfruttare, sia nelle esistenti tecnologie destinate al pubblico sia nei nuovi svilupp dell'Internet delle cose. Un simile aumento di attacchi imminenti comporta anche l'ingresso i di nuovi criminali informatici, operatori indipendenti che utilizzano semplici minacce informat per compiere operazioni regionali su vasta scala. Anche se le forze dell'ordine stanno facendc in avanti nella lotta a favore della sicurezza informatica, le minacce persistono.

La recente violazione delle tecnologie caus l'interruzione dei servizi pubblici

In passato, abbiamo già avuto modo di capire quanto siano sensibili agli attacchi informatici al sistemi di trasporto automatici e attualmente siamo in presenza di possibili minacce nel setto dell'aviazione. Il primo incidente si è verificato quando il ricercatore di sicurezza, Chris Rober inviato un tweet in cui sosteneva di aver manomesso i sistemi di bordo dell'aereo 737/800 su

trovava. A questo episodio ha fatto seguito un attacco DDoS all'aeroporto Okecie di Varsavia provocato ritardi, tenendo a terra oltre 1.400 passeggeri di LOT Polish Airlines.

[Leggete: Attacchi in alta quota: c'è da preoccuparsi? (ingl.)]

I router sono stati il secondo bersaglio degli aggressori. I nostri ricercatori hanno rilevato un aumento degli attacchi che utilizzano le minacce informatiche che modificano il DNS mirati ai router domestici. La maggior parte delle infezioni rilevate ha interessato il Brasile, gli Stati Ur Giappone. Il Brasile è stato il paese maggiormente colpito, con l'81% di infezioni. Questi attac avevano l'obiettivo di impadronirsi delle informazioni personali presenti sui dispositivi connes router domestici utilizzando minacce informatiche.

[Leggete: Le minacce informatiche che modificano il DNS mettono gli occhi sui router domestici (ingl.)]

Questi attacchi avevano l'obiettivo di impadronirsi delle informazioni personali presenti sui dispositivi connessi ai router domestici utilizzando minacce informatiche che modificano il DN Come suggerisce il nome, le minacce informatiche che modificano il DNS cambiano il DNS di u router per fare in modo che tutti i dispositivi ad esso collegati carichino la versione dannosa d Web ai quali tentano di accedere, inclusi i siti Web di home banking. Sebbene le minacce informatiche che modificano il DNS non siano una novità, la loro importanza continua ad aum poiché un numero sempre crescente di privati e aziende si connette a Internet delle cose.

[Leggete: Le minacce informatiche che modificano il DNS mettono gli occhi sui router domestici (ingl.)]

Infine, a inizio aprile, un attacco alla rete televisiva francese TV5 Monde ha paralizzato la rete aziendale, interrompendo tutte le trasmissioni per quattro ore. Gli aggressori inoltre hanno a il controllo degli account di social networking di TV5 Monde e li hanno utilizzati non solo per pubblicare propaganda ma anche per rivelare le informazioni personali dei parenti dei soldati francesi impegnati in operazioni militari.

[Leggete: L'attacco a TV5Monde: quattro ore che hanno cambiato il mondo (ingl.)]

Simili incidenti dimostrano che i criminali informatici stanno andando ben oltre i computer de
e i dispositivi mobili. Stanno ampliando i propri obiettivi tanto da includere infrastrutture e ga
destinati al pubblico e per i quali in genere diamo per scontata la sicurezza.

Come in tutti i sistemi, sono presenti bug anche in questo sistema [aeroplano]; nessun siste
concepito dall'uomo e completamente privo di errori. Spetta ai governi e agli organismi d
regolamentazione imporre ai fornitori (aerei e sistemi IFE) l'obbligo di andare oltre la semplice
sicurezza mediante anonimato, di dimostrare la sicurezza dei sistemi esistenti e di risolvere le
vulnerabilità che emergono. Chissà, forse i sistemi che vengono implementati verrebbero prog
in maniera solida e sicura e svolgerebbero un lavoro impeccabile nel tenere lontani gli aggress
Martin Rösler, Senior Director, ricerca sulle minacce

Gli operatori indipendenti della criminalit informatica si sono esposti in molte regior il ransomware e le minacce informatiche p PoS persistono

Nel secondo trimestre, è stato registrato un numero maggiore di istanze di operazioni di crim
informatici indipendenti. Frapstar, operatore canadese indipendente, ha tratto profitto dalla
di informazioni personali rubate. In Brasile, LordFenix ha fatto un colpaccio con la sua orda di
di Troia per il banking online prodotti artigianalmente, ciascuno del valore di circa 300 dollari
Analogamente, AlejandroV è riuscito a sottrarre 22.000 numeri di carte di credito univoci cor
FighterPoS, la sua minaccia informatica per PoS.

**[Leggete: FighterPoS: contrastare una nuova famiglia di minacce informatiche per Po
(ingl.)]**

MalumPoS è un'altra minaccia informatica per PoS che ha fatto il suo ingresso in scena in que
stesso periodo. Questa minaccia informatica è stata rilevata mentre sottraeva informazioni d
sistemi in esecuzione su Oracle MICROS; ciò significa che 330.000 enti di tutto il mondo sono
vulnerabili a questa minaccia, soprattutto negli Stati Uniti.

**Numero di rilevamenti di minacce informatiche per PoS
(1° trimestre 2014-2° trimestre 2015)**

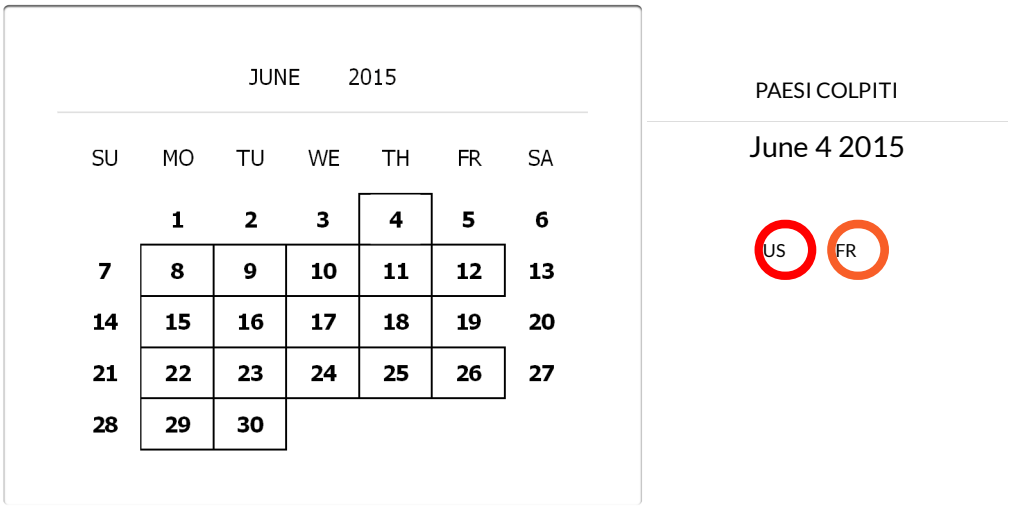
Il lieve declino di rilevamenti di minacce informatiche per PoS potrebbe essere dovuto al fatto che la minaccia ha raggiunto il suo p
saturazione.
Le ultime versioni della minaccia nella prima metà dell'anno potrebbero costituire gli ultimi disperati tentativi di capitalizzare i gu
realizzati.

[Leggete: Trend Micro individua MalumPoS (ingl.)]

Due criminali informatici nigeriani indipendenti hanno utilizzato Hawkeye, un semplice keylo
da 35 dollari, per prendere di mira le piccole imprese di tutto il mondo, in particolare quelle c
sede in India, Egitto, Iran, Pakistan, Taiwan, Hong Kong, Russia, Francia, Germania e Stati Unit

[Leggete: In che modo due criminali informatici hanno guadagnato milioni utilizzando minaccia informatica da 35 dollari (ingl.)]

Infezioni da ransomware a livello regionale (giugno 2015)



Dal calendario riportato qui sopra emerge l'intenzione di distribuire ransomware in paesi specifici.
Questo ransomware include varianti TorrentLocker e CryptoWall.

Nel corso di questo trimestre, l'attività di ransomware è stata consistente. Nel solo mese di gi
abbiamo rilevato infezioni da TorrentLocker e CryptoWall quasi ogni giorno negli Stati Uniti, r
Regno Unito, in Corea del Sud e in Cina. Abbiamo scoperto anche che **in Cina tantissimi adolescenti** (ingl.) guadagnano con il ransomware mobile.

Paesi colpiti da attacchi di minacce informatiche nel 2° trimes 2015

HawkEye | LordFenix | Frapstar | TorrentLocker | Cryptowall 3.

Ransomware mobile cinese

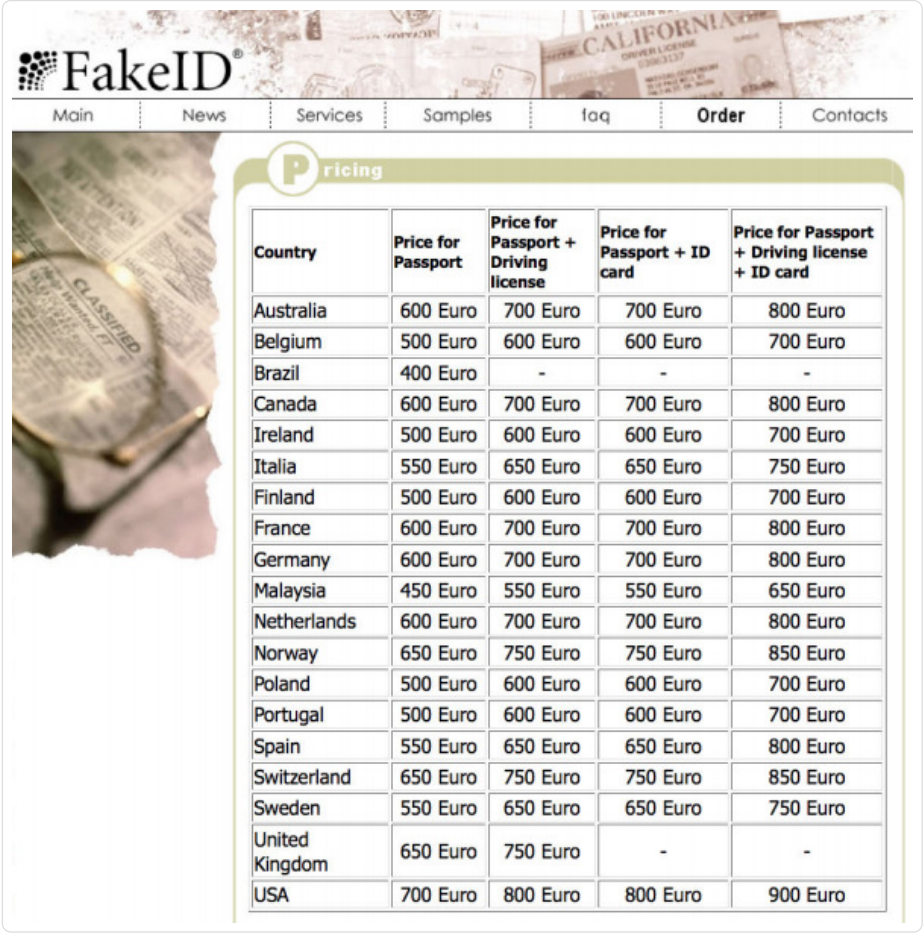
Operazione: HawkEye

Paesi colpiti: India, Egitto, Iran, Pakistan, Taiwan, Stati Uniti, Hong Kong, Russia, Francia, Ger

In futuro, assisteremo a un'integrazione di minacce vecchie e nuove, combinate per raggiun stesso obiettivo. Chi si occupa di protezione deve iniziare a prendere in considerazione le m nuove e imminenti mentre affronta quelle vecchie e controlla i potenziali attacchi mirati. Per combattere le minacce, raccomando di utilizzare una strategia definita chiaramente. Oltre a esaminare gli eventi particolari all'interno di un host, è opportuno assicurarsi anche di poterli mettere in relazione con gli eventi all'interno della rete. **- Jay Yaneza, Threats Analyst**

Le iniziative delle forze dell'ordine hanno dato i loro frutti poiché i governi hanno privilegiato la sicurezza

Alcune delle vittorie ottenute in questo trimestre in materia di sicurezza sono state possibili attraverso le partnership tra pubblico e privato. Trend Micro ha collaborato con l'Interpol e l'Europol per neutralizzare due noti botnet: SIMDA e BEEBONE. "La serie di successi continu affermato a maggio Ross Ulbricht, creatore di Silk Road. Il suo esperimento è servito a fare ulteriormente luce sui mercati del Web invisibile in cui è possibile trovare dai passaporti contraffatti ai contratti di omicidio.



Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

[Leggete: Mondo sommerso: alla scoperta del Web invisibile (ingl.)]

Sono degni di nota alcuni passi da gigante compiuti in materia di legislazione sulla sicurezza e favore della privacy. Le novità più rilevanti sono state introdotte negli Stati Uniti con la firma Freedom Act e con l'obbligo imposto dal governo statunitense di utilizzare HTTPS per tutti i s Web federali.

Uno dei maggiori problemi che la criminalità informatica pone alla legislazione è rappres dalla sua rapida evoluzione. La maggior parte delle leggi impiega dai 3 ai 5 anni per esser approvata. Pertanto, la normativa generale che è in circolazione da più tempo è quella più pert Di conseguenza, come è successo negli Stati Uniti, è stato possibile arrestare persone accusate parte della criminalità organizzata o di racket. Queste leggi non sono specifiche per i crimini "informatici", ma sono risultate utili. In generale, sarebbe necessario standardizzare le leggi de paesi.

In fin dei conti, Internet è globale. Pertanto, anche la criminalità informatica è globale, quindi

sarebbe molto più semplice perseguire le persone se la legge in merito agli attacchi contro i ser fosse esattamente la stessa in Germania, in Irlanda o in Francia. Ci sarebbero meno complicazi occasioni di simili incidenti. Ecco quindi che la cosa più importante è riuscire a semplificare la comunicazione all'interno delle partnership tra pubblico e privato. Se la comunicazione è sem le forze dell'ordine e i ricercatori di sicurezza riescono a scambiarsi agevolmente le informazi

Robert McArdle, Senior Threat Research Manager

La violazione dei dati dell'OPM è, ad oggi, l'incidente di maggiore portata mai avven per l'impatto nazionale e politico che ha avuto

A giugno, le informazioni personali di oltre 21 milioni di dipendenti federali (ex e attuali), nonc membri delle rispettive famiglie e dei candidati esclusi, sono state rese vulnerabili in seguito a serie di violazioni di dati ai danni dell'**Office of Personal Management** degli Stati Uniti. I dat includevano codici fiscali e persino impronte digitali.

[LEGGETE: Violazione dei dati federali: il più prolifico della storia (ingl.)]

Anche l'**IRS** è stato oggetto di una violazione di dati che ha interessato 100.000 contribuenti. aggressori dell'attacco hanno sottratto i dati con un'applicazione Web dell'IRS contraffatta.

Principali violazioni di dati rilevate (2° trimestre 2015)

Japan Pension Service

Data rilevamento: 1 giugno 2015
Settore: rendita
Impatto: 1 milione di vittime (dati personali, tra cui codici fiscali)

OPM, Washington DC

Data rilevamento: 4 giugno 2015
Settore: pubblica amministrazione
Impatto: 21,5 milioni di vittime (codici fiscali)

I principali obiettivi degli attacchi di questo trimestre sono state le pubbliche amministrazioni. La violazione dell'OPM è stato l'incid maggiore portata mai avvenuto finora, in quanto ha reso vulnerabili oltre 20 milioni di dati personali.

Fonte: https://www.privacyrights.org/data-breach

In un certo senso, è più grave se sono le informazioni personali a venire rubate. Posso cambi facilmente la mia carta di credito ma, a meno che non traslochi, non posso cambiare il mio indirizzo. Né posso cambiare la mia data di nascita. Le informazioni di identificazione persona solo identificano gli utenti, ma sono anche spesso difficili, se non impossibili, da cambiare. - **Raimund Genes, Chief Technology Officer**

Gli ultimi attacchi contro le pubbliche amministrazioni hanno evidenziato la presenza di motivazioni politiche dietro al campagne mirate

La Casa Bianca e la NATO sono state le ultime vittime di Operation Pawn Storm, una campagı spionaggio informatico di tipo politico ed economico scoperta lo scorso anno. Al contempo, gli pubblici di Filippine e Taiwan sono state vittime di due altre campagne di attacchi mirati: Trop Trooper e ESILE.

[Leggete: Operation Pawn Storm intensifica la propria attività e prende di mira NATC Casa Bianca (ingl.)]

I paesi che hanno cercato di arrestare le capacità di sviluppo nucleare dell'Iran hanno dovuto fronte agli attacchi **Duqu 2.0** che utilizzavano numerose vulnerabilità zero-day. Contemporaneamente, altri autori di minacce hanno iniziato a utilizzare il **macro malware** n campagne di attacchi mirati, quali GHOLE. Questo spiega la costante crescita del volume di m malware registrata nell'ultimo trimestre.

Rilevamenti di macro malware (2014 - 1° semestre 2015)

Il numero di rilevamenti di macro malware aumenta leggermente trimestre dopo trimestre, molto probabilmente a causa di un mag
negli attacchi di malvertisement che indirizzava sui siti per il download di macro malware.

Generalmente, gli attacchi mirati contro gli obiettivi politici e contro le aziende sono piutt
simili. Tuttavia, si differenziano leggermente per motivazione e risultato finale. Spesso g
attacchi politici utilizzano minacce zero-day in abbinamento ai "tradizionali" vettori di attacc
contro, gli attacchi contro le aziende utilizzano generalmente metodologie "standard" dal mom
che fanno quasi sempre affidamento sull'elemento umano, l'anello più debole della catena. **- K
Wilhoit, Senior Threat Researcher**

Le infezioni secondarie proliferano per via di tre fenomeni infausti. In primo luogo, un nun
sempre maggiore di aggressori prende di mira la catena di approvvigionamento di inform
delle aziende, sfruttando island hopping per compromettere gli host interni. In secondo luogo,
seguito a una compromissione, l'uso della steganografia consente di stabilire un secondo cana
all'interno dei sistemi compromessi, permettendo all'avversario di contrastare con efficacia la
risposta agli incidenti. In terzo luogo, dopo essersi impossessati della proprietà intellettuale o d
informazioni di identificazione personale, i criminali informatici utilizzano il marchio dell'az
per attaccare il relativo bacino di utenti mediante attacchi watering-hole. Questi attacchi sono
aumentati in maniera esponenziale nei primi sei mesi del 2015. **- Tom Kellermann, Chief
Cybersecurity Officer**

Le vulnerabilità hanno minacciato i siti We
e i dispositivi mobili destinati al pubblico

Ad aprile, WordPress, piattaforma di blog, è stata interessata da una vulnerabilità che **ha consentito agli aggressori di inserire codice JavaScript dannoso** nella finestra del brows dell'amministratore. Magento, piattaforma di e-commerce utilizzata da eBay e da più di altri 240.000 siti di shopping online a livello mondiale, è stata sconvolta da una vulnerabilità identi a fine giugno. L'ampio bacino di utenti di queste applicazioni Web dimostra che le vulnerabilità queste piattaforme sono tanto pericolose quanto quelle rilevate nel software tradizionale.

[Leggete: La piattaforma di e-commerce utilizzata da eBay, Magento, è stata attaccat ladri di dati di carte di credito (ingl.)]

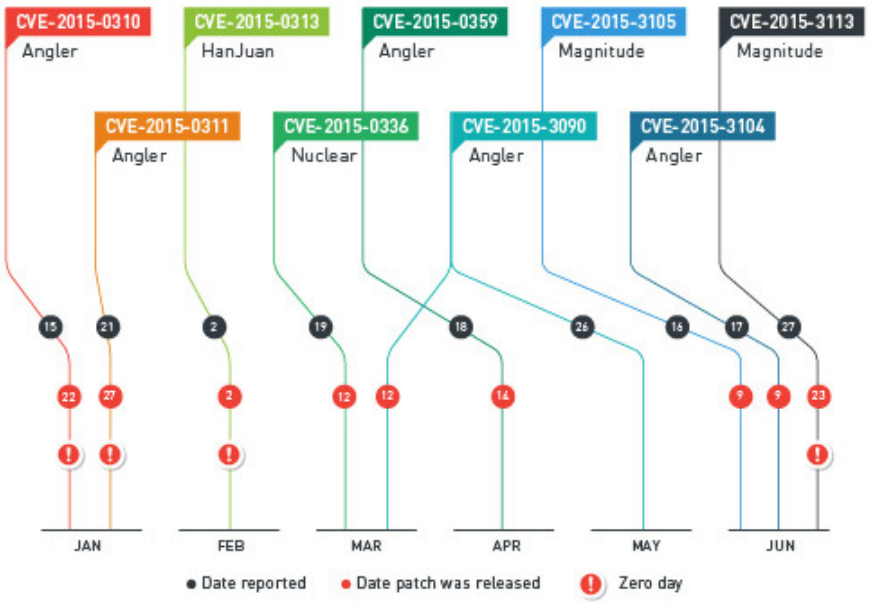
Anche le piattaforme mobili sono state interessate da una discreta quantità di vulnerabilità, c **vulnerabilità SwiftKey Android** (ingl.), che consente agli aggressori di assumere il controllo dispositivi mobili degli utenti. È stata distribuita una patch, ma la frammentazione dei disposit impedisce ancora l'implementazione sui dispositivi colpiti. Sono stati rilevati imponenti difett sicurezza anche nelle sandbox di applicazioni che proteggono i sistemi OSX e iOS.

Gli aggressori sfruttano le vulnerabilità e i punti deboli di tutte le piattaforme. Hanno solo bisogno di trovare il modo di entrare. Le aziende devono prestare molta attenzione alle vulnerabilità dei principali software e plug-in utilizzati. È necessario integrare un programma valutazione delle vulnerabilità mirato e continuo con un programma di valutazione delle configurazioni. Anche se le vulnerabilità del software standard, come Flash, Java, Firefox e Int Explorer®, vengono utilizzate come criteri per tracciare il panorama delle minacce, non dobbi dimenticare che le vulnerabilità delle applicazioni personalizzate (soprattutto applicazioni We sono numerose e che molte non compaiono nell'elenco CVE. Le applicazioni personalizzate van sottoposte a verifiche personalizzate. Un ottimo test di penetrazione da eseguire sulle applicaz personalizzate ripaga sempre. **- Pawan Kinger, Director, Deep Security Labs**

I numeri di accesso di Angler Exploit Kit so triplicati, si tratta dell'integrazione di exploit nei kit più veloce mai avvenuta pri

In seguito all'individuazione di ulteriori vulnerabilità, anche i kit di exploit sono stati rapidame aggiornati affinché le includessero. Angler Exploit Kit è l'esempio lampante di tale comportan Si tratta del primo kit in cui le vulnerabilità sono state integrate quasi contemporaneamente loro individuazione. Questo spiega l'aumento del conteggio delle infezioni dal 1° al 2° trimest 2015, nonché l'incremento del numero di utenti che ha eseguito l'accesso a URL connessi al k exploit tra maggio e giugno. Angler è particolarmente noto perché utilizza vari exploit di Adol Flash Player, insieme ad altri kit di exploit, come Nuclear e Magnitude.

Cronologia delle vulnerabilità di Adobe Flash integrate nei ki exploit, 2° trimestre 2015



Gli exploit per le vulnerabilità di Adobe Flash sono state integrate in un numero sempre crescente di kit di exploit (soprattutto Angler) dell'anno.

Gli sviluppatori di Angler Exploit Kit aggiungono al kit gli exploit di Adobe Flash in modo a aggressivo. Gli sviluppatori dei kit di exploit Magnitude e Nuclear fanno altrettanto. Per proteggere meglio i nostri clienti, dobbiamo continuare a studiare e monitorare questa agilità.
Joseph C. Chen, Threats Analyst

Panorama delle minacce

Trend Micro Smart Protection Network™ ha bloccato oltre 12 miliardi di minacce nell'ultimo trimestre, registrando un calo rispetto ai 14 miliardi di minacce dell'inizio dell'anno. Questo c potrebbe essere dovuto al fatto che adesso i criminali informatici si concentrano sugli attacch piuttosto che sull'uso di un approccio che mira a infettare chiunque.

Numero totale di minacce bloccate

2° trimestre 2015

Livello di rilevamento (numero di minacce bloccate ogni secon

2° trimestre 2015

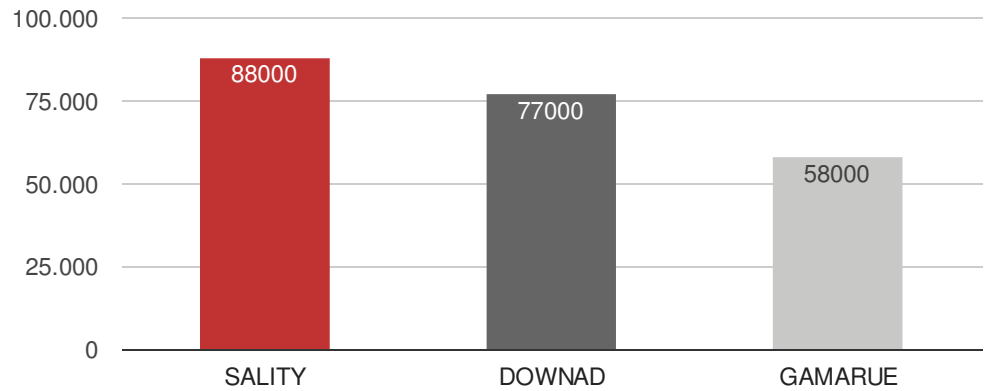
1622

Di queste minacce, le prime tre famiglie di minacce informatiche conteggiate nell'ultimo trim sono state SALITY (88.000), DOWNAD/CONFICKER (77.000) e GAMARUE (58.000). Le vari SALITY sono note per le loro routine dannose che includono la diffusione di file .EXE e .SCR in Le varianti DOWNAD/CONFICKER sono note per la loro persistenza nello sfruttamento dell vulnerabilità e per l'elevata velocità di propagazione. Le varianti GAMARUE sono in grado di sottrarre informazioni e di assumere il controllo di un sistema per sferrare attacchi su altri sis

Principali famiglie di minacce informatiche | **Tipi principali di minacce mobili**

Principali famiglie di minacce informatiche

**sulla base dei rilevamenti su PC*



Il numero totale di applicazioni dannose e ad alto rischio per Android sale a circa 7,1 milioni. S
di un aumento del 31% rispetto al 1° trimestre 2014 (5,4 milioni).

SCARICA IL RAPPORTO COMPLETO