TREND MICRO™

Si scatenano le minacce ai dispositivi mobili

Le falle dei dispositivi aprono le porte ai rischi

Sommario

Introduzione

Dalla Relazione annuale sulla sicurezza TrendLabs 2012 è emerso che è iniziata lo scorso anno l'era post-PC in cui i criminali informatici hanno iniziato a creare minacce informatiche specifiche per i dispositivi mobili.[1] Le minacce informatiche rimangono un grande problema per gli utenti in questo trimestre, sebbene le maggiori preoccupazioni vadano al di là dei semplici numeri. La scoperta della minaccia OBAD e la vulnerabilità della "master key" hanno evidenziato la capacità dei criminali informatici di trovare modi per sfruttare le falle dell'ecosistema Android™. Abbiamo notato che queste minacce sono state progettate per superare le misure di sicurezza e come mezzo per permettere ai criminali informatici di acquisire il controllo dei dispositivi.

In questo trimestre sono apparse nuove minacce bancarie online in diversi paesi e in particolare in Brasile, Corea del Sud e Giappone. Queste hanno evidenziato la necessità di una maggiore consapevolezza sulla sicurezza bancaria online. Per attuare i loro piani di danneggiamento, i criminali informatici hanno inoltre elaborato attacchi diversificati che sfruttano le esche del social engineering, l'accesso singolo (SSO), i servizi multiprotocollo e le piattaforme di creazione dei blog. La scoperta delle vulnerabilità è diventata uno degli argomenti principali di questo trimestre in risposta all'ondata di incidenti di tipo zero-day sopraggiunta a inizio anno.

Le aziende di grandi dimensioni hanno continuato a fronteggiare gli attacchi mirati. La campagna Naikon è apparsa per la prima volta in Asia e Pacifico, mentre la nostra ricerca sulla campagna Safe ha rivelato che gli indirizzi IP vittima della campagna si sono diffusi in oltre 100 paesi in tutto il mondo. Tutto ciò evidenzia la necessità di rafforzare le difese aziendali contro gli attacchi mirati e di elaborare delle soluzioni proattive in grado di proteggere le reti aziendali.

MOBILE

Per riuscire a superare le misure di sicurezza, le minacce diventano sempre più sofisticate

Nel 2012 abbiamo visto un rapidissimo aumento del numero di minacce informatiche per i dispositivi mobili: in un solo anno sono aumentate quanto le minacce per PC in dieci anni. Il numero di app Android dannose e ad alto rischio ha raggiunto le 718.000 unità nel secondo trimestre, quando erano solo 509.000 nel primo trimestre di quest'anno. In appena sei mesi, queste app sono aumentate di oltre 350.000 unità, un valore che in passato avevano raggiunto in tre anni. La maggior parte di queste minacce informatiche viene ancora veicolata tramite finte versioni di app comuni mascherate o contenenti cavalli di Troia. Anche in questo trimestre, come nel precedente, è emerso che circa un quarto delle minacce informatiche scoperte è progettato per iscrivere gli ignari utenti a costosi servizi a pagamento.

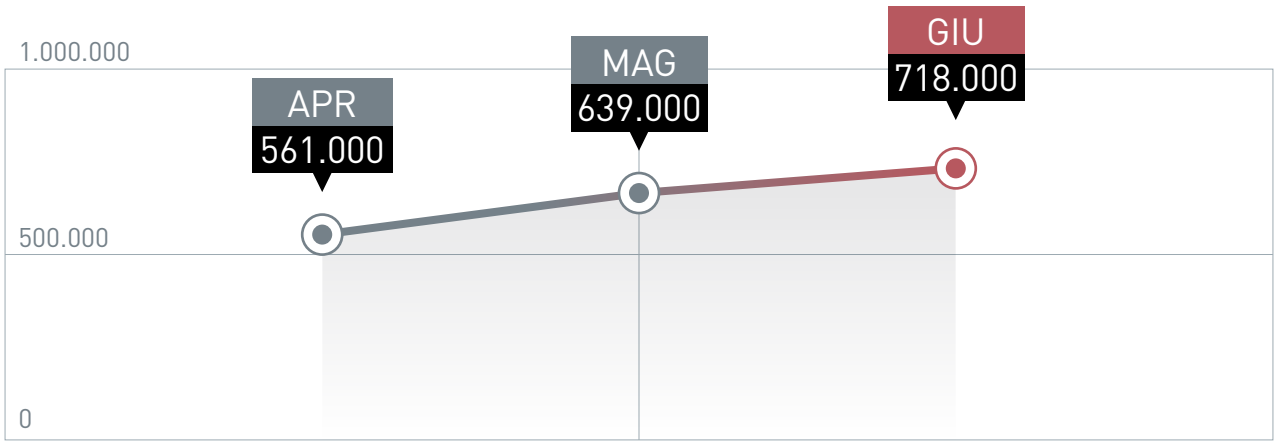
Tuttavia la scoperta della vulnerabilità della master key di Android è stato l'evento di gran lunga più significativo, in quanto quasi il 99% dei dispositivi Android si è rivelato essere vulnerabile.[2] La vulnerabilità consente la modifica delle app installate senza il consenso dell'utente. Questo ha fatto aumentare i dubbi sull'affidabilità delle app di scansione ai fini della protezione e sulla frammentazione esistente nell'ecosistema Android.

Anche la minaccia OBAD (ANDROIDOS_OBAD.A) sfrutta una vulnerabilità di Android.[3] Dopo l'installazione, OBAD richiede i privilegi di root e di amministrazione del dispositivo; questo consente alla minaccia di assumere il completo controllo del dispositivo infettato. Questa routine è simile a quella utilizzata dalle backdoor e dai rootkit in azione sui PC.[4] OBAD mostra continuamente delle notifiche a comparsa per convincere gli utenti a concedere i permessi. Utilizza inoltre una nuova tecnica di offuscamento che rende difficili le operazioni di rilevamento e pulizia.

La minaccia FAKEBANK individuata questo trimestre, invece, si maschera da app legittima. Contiene file dei pacchetti specifici delle applicazioni Android (APK), che copia sulla scheda Secure Digital (SD) del dispositivo.[5] Tramite i file APK, questa minaccia visualizza le icone e un'interfaccia utente che imita un'app bancaria legittima. Questa tecnica somiglia ai cavalli di Troia per PC che monitorano i comportamenti di navigazione dell'utente e simulano i siti delle banche.[6]

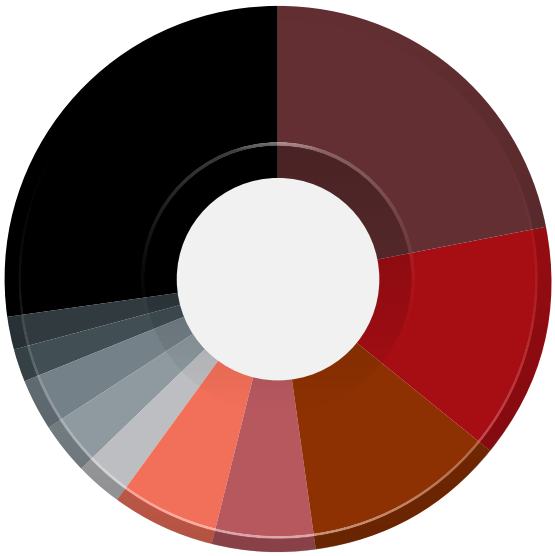
In questo trimestre abbiamo rilevato inoltre dei finti antivirus (FAKEAV) che assomigliano in modo sempre maggiore a quelli legittimi.[7] Gli attacchi mirati raggiungono ora i dispositivi mobili anche nella forma di minacce CHULI, che arrivano come allegati di e-mail di tipo spear-phishing.[8]

Aumento del volume delle minacce Android



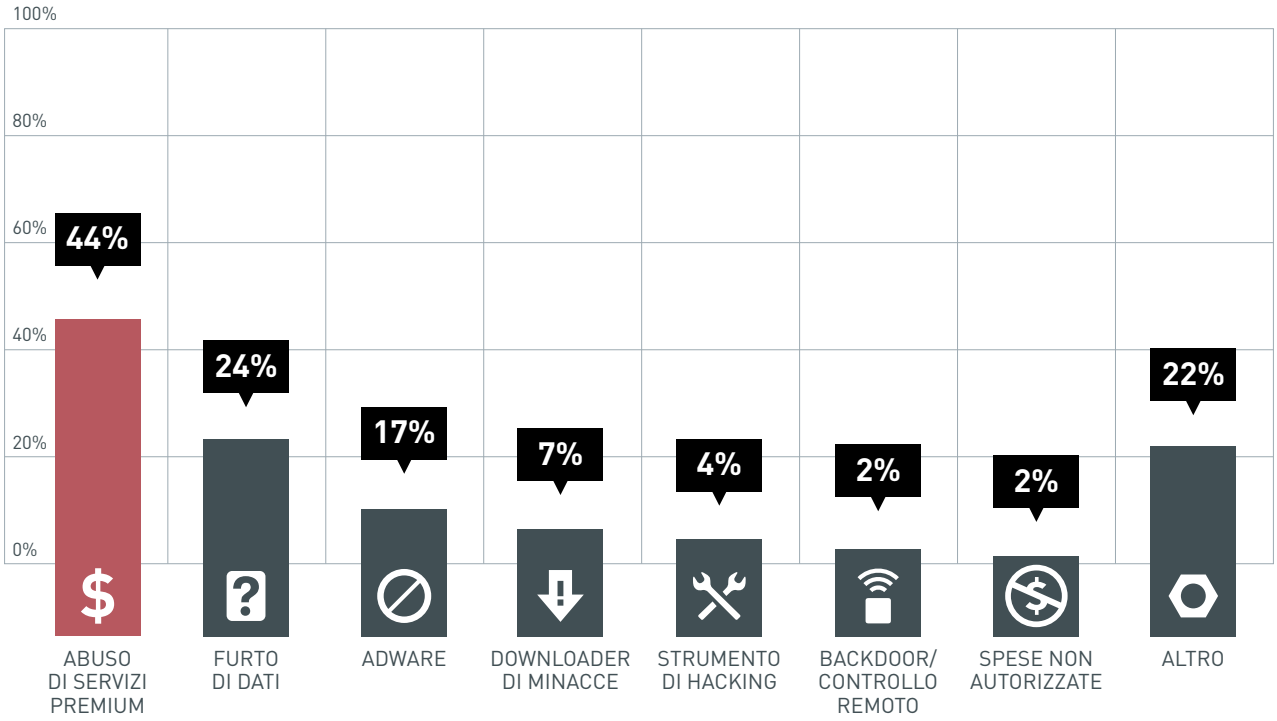
Il numero di app Android dannose e ad alto rischio è aumentato rapidamente fino a giugno 2013. Il numero di app dannose e ad alto rischio ha impiegato tre anni a raggiungere le 350.000 unità; questo numero è raddoppiato in appena sei mesi (da gennaio a giugno 2013).

Principali famiglie di minacce Android



1	FAKEINST	22%
2	OPFAKE	14%
3	SNDAPPS	12%
4	BOXER	6%
5	GINMASTER	6%
6	VDLOADER	3%
7	FAKEDOLPHIN	3%
8	KUNGFU	3%
9	JIFAKE	2%
10	BASEBRIDGE	2%
	Altro	27%

Distribuzione dei principali tipi di minacce



Le minacce che praticano un abuso di servizi premium sono le minacce prevalenti per i dispositivi mobili. Sebbene le percentuali dei tipi di minacce siano invariate rispetto al trimestre precedente, abbiamo notato un aumento nel volume dei furti di dati, il che potrebbe suggerire che questo tipo di minacce stia diventando sempre più sofisticato.

I dati di distribuzione si basano sulle prime 20 famiglie di minacce informatiche e adware; queste coprono l'88% di tutte le minacce rilevate dalla tecnologia Mobile App Reputation nel periodo aprile-giugno 2013. Si noti che una famiglia di minacce potrebbe avere comportamenti tipici di più tipi di minacce.

Paesi con i maggiori volumi di download di app Android dannose

1	★ Emirati Arabi Uniti	13,79%
2	⬇ Myanmar (Birmania)	5,05%
3	★ Vietnam	4,94%
4	★ Messico	4,23%
5	⬇ Russia	4,17%
6	⬇ India	3,74%
7	★ Cina	3,57%
8	★ Venezuela	3,11%
9	⬇ Malesia	2,97%
10	★ Singapore	2,84%

★ NEW ENTRY ⬆ È SALITO ⬇ È SCESO

Gli Emirati Arabi Uniti hanno visto il maggior volume di download di app Android dannose e hanno superato Myanmar, che era al primo posto nel trimestre precedente. Tra i primi 10 paesi sotto attacco, sei sono nuovi; questo potrebbe indicare un aumento dei dispositivi mobili e/o un aumento degli attacchi in quel particolare paese.

La classifica si basa sulla percentuale di app valutata come "dannosa" rispetto al numero totale di app analizzate per il paese. La classifica si limita ai paesi con almeno 10.000 scansioni. Le classifiche si basano sull'analisi trimestrale del rilevamento delle minacce in tempo reale tramite Trend Micro™ Mobile Security Personal Edition.

Paesi più a rischio di esposizione della privacy a causa dell'uso delle app

1	⬆ Arabia Saudita	11,49%
2	★ Vietnam	8,87%
3	⬆ Indonesia	8,82%
4	★ Brasile	7,98%
5	⬇ India	7,87%
6	⬆ Malesia	7,57%
7	★ Sud Africa	6,52%
8	⬇ Russia	5,64%
9	★ Algeria	5,55%
10	⬆ Filippine	5,19%

Come nell'ultimo trimestre, gli utenti di dispositivi mobili in Arabia Saudita hanno scaricato il maggior numero di app ad alto rischio. Il Vietnam si è posizionato al secondo posto per via dell'uso sempre più diffuso dei dispositivi mobili nel paese.[9]

La classifica si basa sulla percentuale di app categorizzate come "privacy risk inducers" (app che spingono verso un rischio per la privacy) rispetto al numero totale di app analizzato nel paese. La classifica si limita ai paesi con almeno 10.000 scansioni. Le classifiche si basano sull'analisi trimestrale del rilevamento delle minacce in tempo reale tramite Trend Micro Mobile Security Personal Edition.

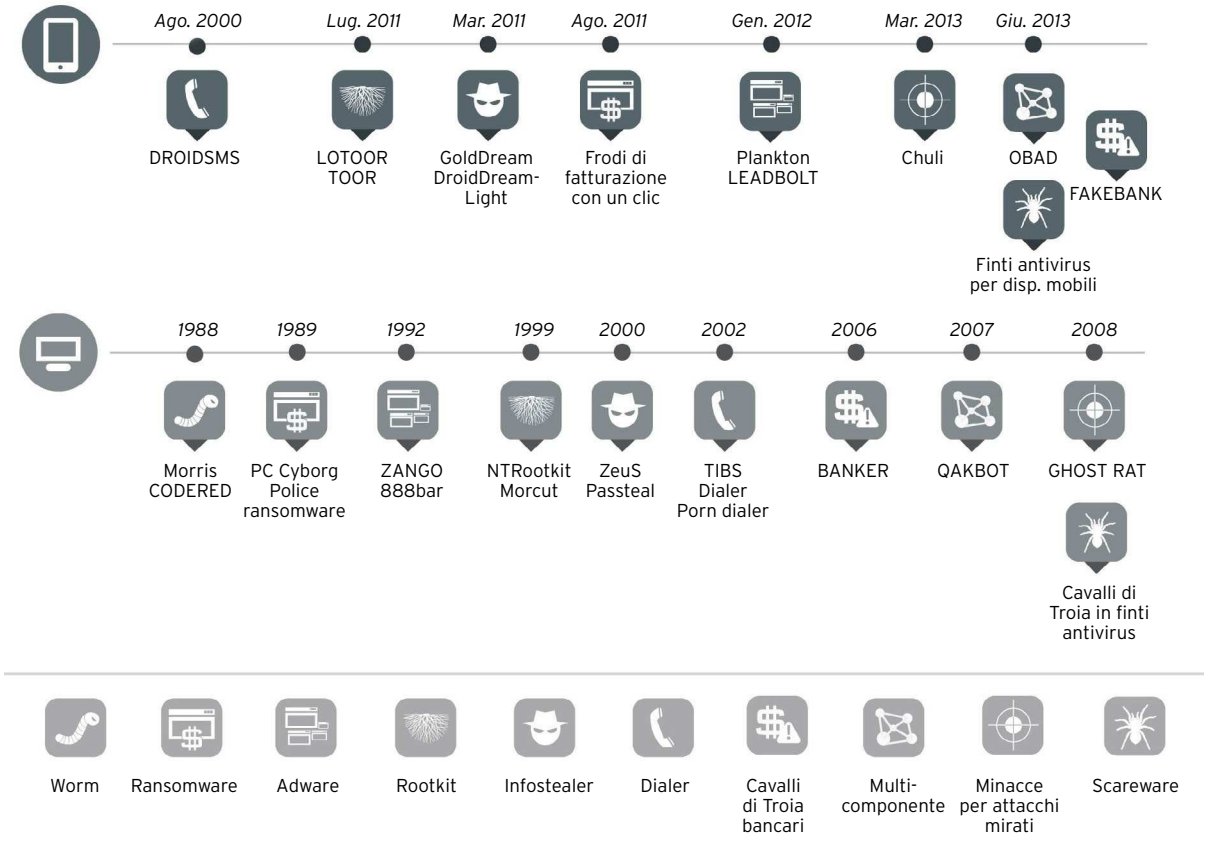
Prezzi pagati sul mercato nero per i numeri raccolti dagli operatori di rete mobile russi

DATI DEI DISP. MOBILI	PREZZO
1 milione di numeri	70 dollari
10.000 numeri	10 dollari
Database personalizzato con dati personali	35 dollari per 1.000 numeri

La complessità in continuo aumento delle minacce per i dispositivi mobili può essere attribuita alla crescente domanda di informazioni collegate ai messaggi di testo (SMS) sul mercato nero. I database SMS sono tra i set di dati più pagati sul mercato nero.

Funzionamento del processo di aggiornamento di Android

Confronto cronologico tra i tipi di minaccia Android e quelli per PC

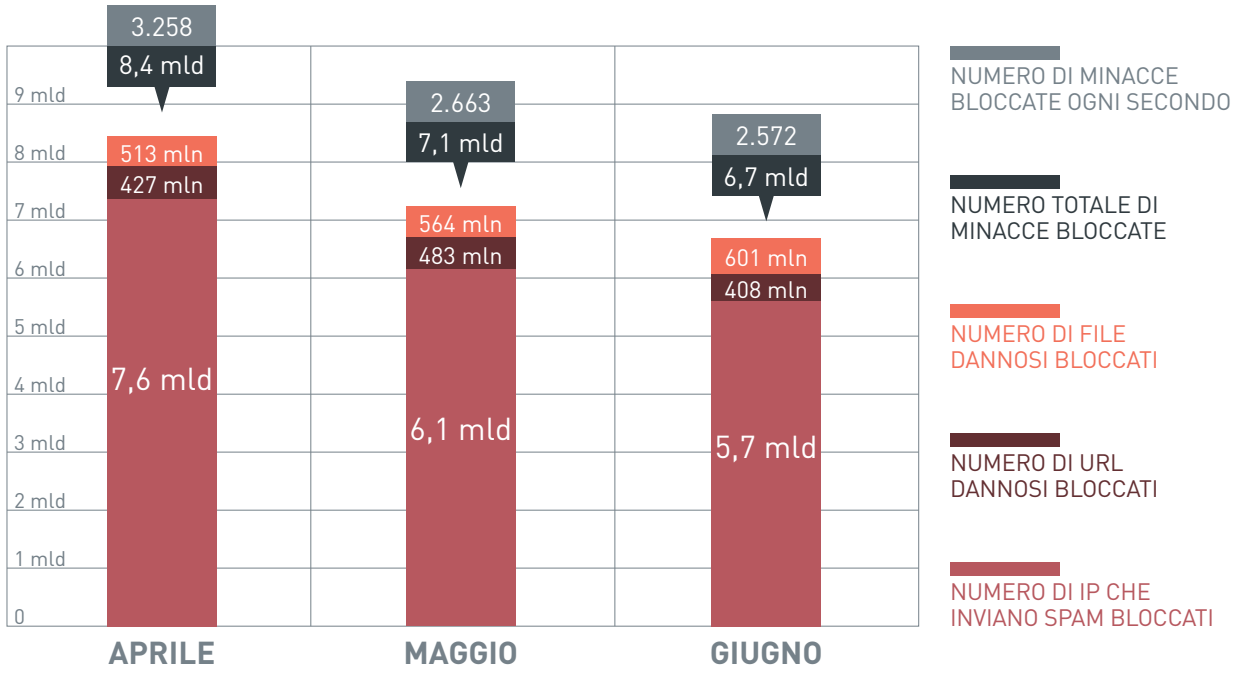


CRIMINALITÀ INFORMATICA

Le minacce informatiche bancarie si regionalizzano, le vecchie minacce rifioriscono

Il numero complessivo di minacce bloccate da Trend Micro™ Smart Protection Network™ è aumentato del 13% rispetto all'ultimo trimestre. Il worm DOWNAD/Conficker è rimasto la minaccia principale, mentre il volume di adware è sensibilmente aumentato man mano che più utenti nei diversi segmenti sono stati indotti a scaricarli nell'ambito di software gratuito.

Numeri complessivi dell'azione di Trend Micro Smart Protection Network



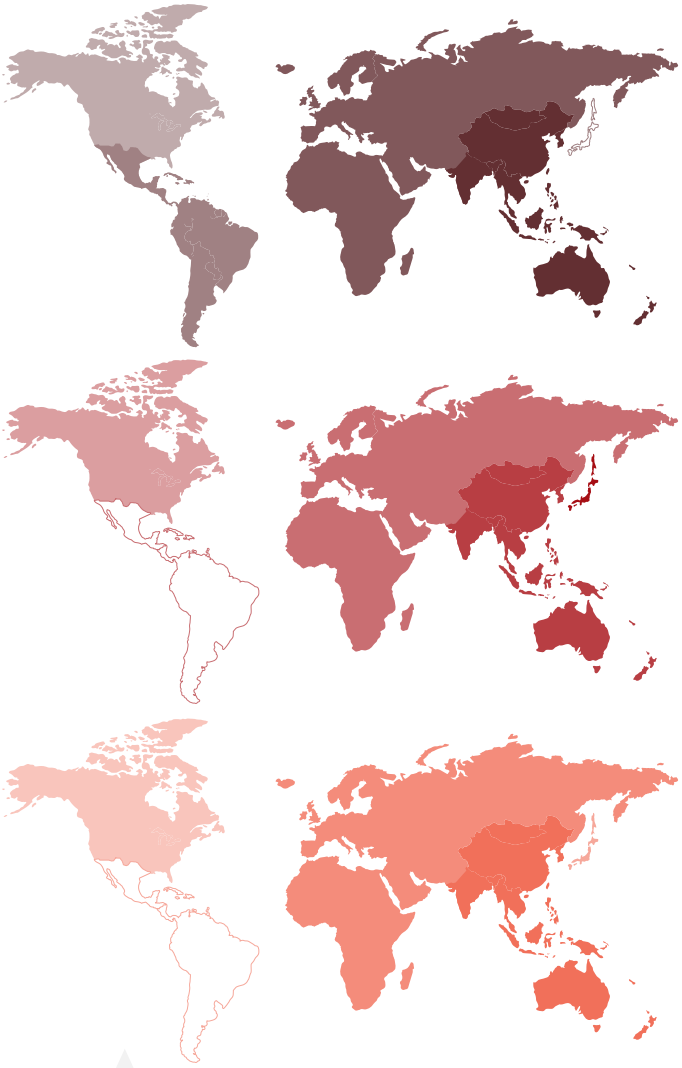
In questo trimestre, siamo riusciti a proteggere i clienti Trend Micro da quasi 3.000 minacce al secondo rispetto alle 2.400 del primo trimestre.

Le prime 3 minacce informatiche

WORM_DOWNAD.KK	509.000
APAC	51%
EMEA	19%
AMERICA LATINA	15%
NORD AMERICA	9%
GIAPPONE	6%

ADW_BHO	448.000
GIAPPONE	34%
APAC	26%
EMEA	19%
NORD AMERICA	17%
AMERICA LATINA	4%

ADW_BPROTECT	311.000
APAC	28%
EMEA	28%
GIAPPONE	20%
NORD AMERICA	15%
AMERICA LATINA	9%



La vulnerabilità del servizio server è stata corretta nel 2008 ma DOWNAD/Conficker, che sfrutta proprio questa vulnerabilità, è risultato essere una delle prime 3 minacce di questo trimestre. La maggior parte delle prime 50 minacce è composta da adware. ZACCESS/SIREFEF e SALITY sono rimaste tra le prime 10.

Le prime 3 minacce per segmento

GRANDI AZIENDE	
NOME	VOLUME
WORM_DOWNAD.AD	360.000
ADW_BPROTECT	53.000
ADW_BHO	28.000

PMI	
NOME	VOLUME
WORM_DOWNAD.AD	58.000
ADW_BPROTECT	9.000
ADW_BHO	8.000

PRIVATI	
NOME	VOLUME
ADW_BHO	370.000
ADW_BPROTECT	215.000
BKDR_BIFROSE.BMC	208.000

I privati sono più inclini a fare clic sugli annunci veicolati dalle minacce informatiche, mentre DOWNAD/Conficker rappresenta un problema per le aziende di tutte le dimensioni.

Primi 10 domini dannosi bloccati

DOMINIO	MOTIVO
trafficconverter.biz	Ospita minacce informatiche, in particolare le varianti DOWNAD
ads.alpha00001.com	Ospita minacce informatiche che modificano le impostazioni predefinite del browser in modo da compromettere i risultati delle ricerche
www.ody.cc	Ha delle pagine che ospitano BKDR_HPGN.B-CN e altri script sospetti
pu.plugrush.com	È collegato a una campagna Blackhole Exploit Kit
c.rvzrjs.info	È collegato ad attività di spam e ad altre attività dannose
adsgangsta.com	È collegato a minacce informatiche ed attacchi di phishing
vjlvchretllifcsgynuq.com	Ospita minacce informatiche; è utilizzato anche per diffondere minacce informatiche tramite Skype
strongvault02.safe-copy.com	Ospita minacce informatiche
www.polaris-software.com	Ospita minacce informatiche
promos.fling.com	Ospita minacce informatiche

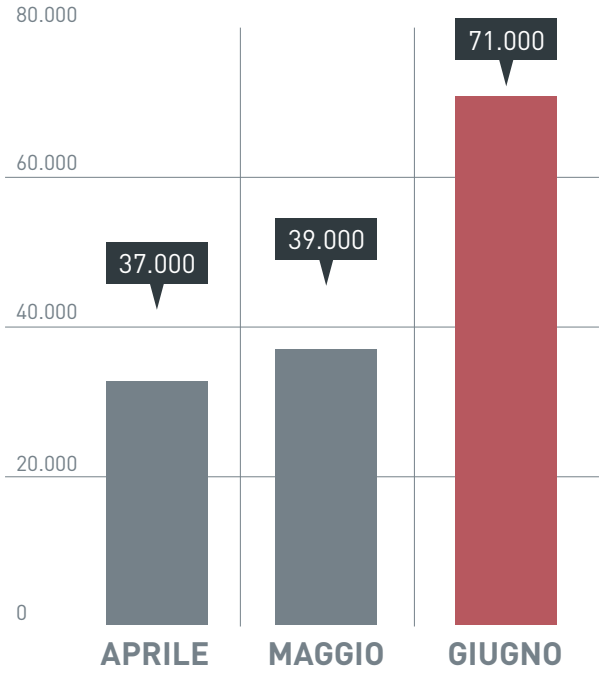
Uno dei principali domini bloccati è collegato a una campagna Blackhole Exploit Kit. Il dominio trafficconverter.biz ospita delle varianti di DOWNAD/Conficker, che è risultato essere la minaccia informatica più importante della prima metà del 2013.

Come previsto, i criminali informatici non hanno creato da zero delle nuove minacce ma hanno riconfezionato delle minacce preesistenti.[10] In questo trimestre abbiamo osservato delle tendenze interessanti in fatto di minacce bancarie; questo tipo di minacce informatiche è aumentato del 29%.

Infezioni riguardante il banking online

	1° TRIM.	2° TRIM.
2013	113.000	146.000

Infezioni incentrate sul banking online



Principali paesi vittima di minacce bancarie

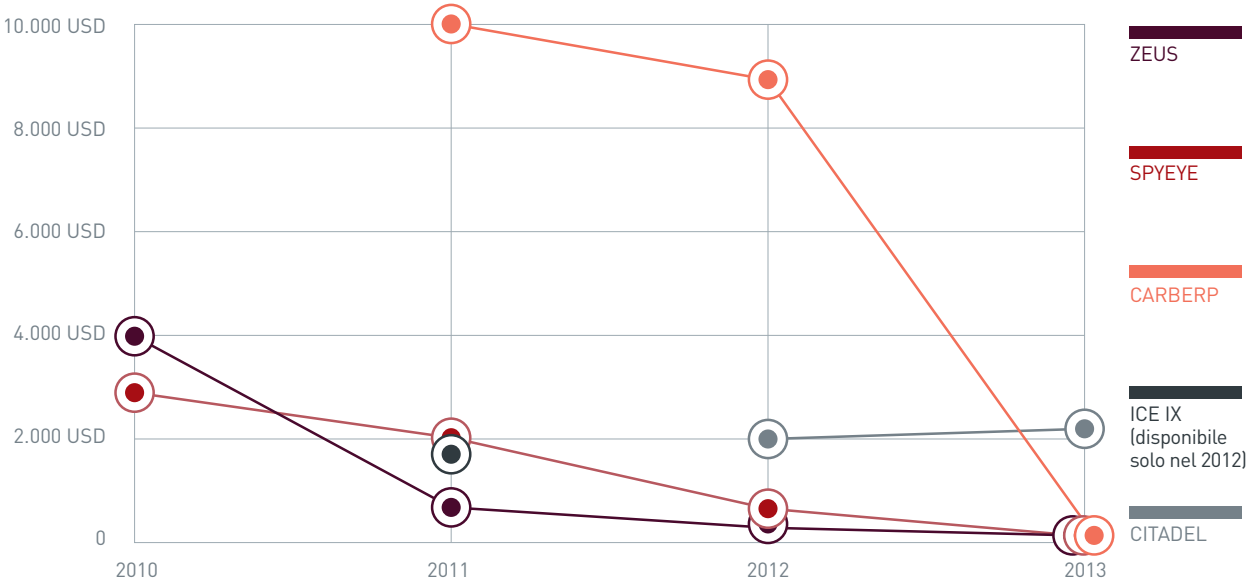
PAESI	PERCENTUALE
Stati Uniti	28%
Brasile	22%
Australia	5%
Francia	5%
Giappone	4%
Taiwan	4%
Vietnam	3%
India	2%
Germania	2%
Canada	2%
Altri	23%

Il volume di minacce informatiche focalizzate sul banking online è aumentato significativamente in questo trimestre, in parte per via dell'aumento del volume della minaccia ZeuS/ZBOT. Le minacce di tipo bancario si stanno diffondendo in tutto il mondo e non si concentrano più su poche aree come l'Europa o le Americhe. Gli Stati Uniti sono stati il paese più colpito dalle minacce bancarie online con circa il 28% del numero mondiale totale di infezioni.

Il Brasile, un'area particolarmente esposta alle minacce, è stato aggredito in questo trimestre da due tipi di minaccia. La prima è la minaccia BANKER mascherata da aggiornamento di Adobe® Flash® Player, in hosting su siti colpiti.[11] L'altra minaccia è mascherata da "browser proprietario" e colpisce gli utenti del Banco do Brasil.[12]

Nel mondo dei criminali informatici, la divulgazione del codice sorgente CARBERP ha reso la creazione di cavalli di Troia bancari molto più semplice. Altri kit di strumenti per cavalli di Troia, come ZeuS, SpyEye e Ice IX, sono invece disponibili gratuitamente e i loro codici sorgente possono essere facilmente utilizzati da hacker capaci.

Cambiamento dei prezzi dei kit di strumenti online di base sul mercato nero



Prezzi attuali stimati.
ZeuS e SpyEye sono stati diffusi prima del 2010.

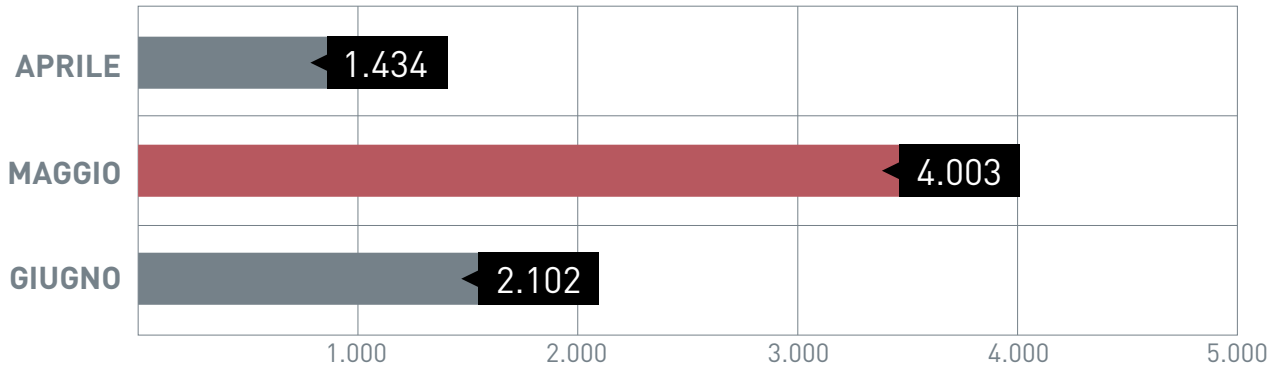
Abbiamo rilevato una minaccia informatica centrata sul banking online che modifica il file HOSTS del computer infettato in modo da reindirizzare i clienti di determinate banche sudcoreane su dei siti di phishing.[13] Abbiamo rilevato inoltre diverse varianti Citadel (rilevate come ZBOT) focalizzate su diversi istituti finanziari giapponesi. Queste minacce informatiche non colpiscono solo le grandi banche giapponesi, ma anche quelle piccole, comprese quelle che si rivolgono esclusivamente ai clienti del banking online.

Come detto in precedenza, i criminali informatici hanno sviluppato la distribuzione delle minacce informatiche e hanno migliorato gli strumenti esistenti. Le nuove tattiche di sviluppo ZeuS/ZBOT includono una routine di propagazione.[14] Abbiamo rilevato che il worm PIZZER è in grado di diffondersi e di autocopiarsi su file di archivio protetti da password, utilizzando una tecnica simile a quella della minaccia PROLACO.[15]

Anche diversi servizi cloud sono stati colpiti in questo trimestre. La backdoor VERNOT, la prima minaccia a sfruttare un diffuso servizio di presa di appunti, ha colpito una nota piattaforma per blog giapponese, utilizzandola come server C&C. Diverse varianti della minaccia GAMARUE sono in hosting su SourceForge, un diffuso archivio di codice. I criminali informatici colpiscono solitamente dei servizi legittimi di hosting gratuito e inducono gli utenti a fidarsi di collegamenti dannosi che sembrano appartenere a nomi famosi.

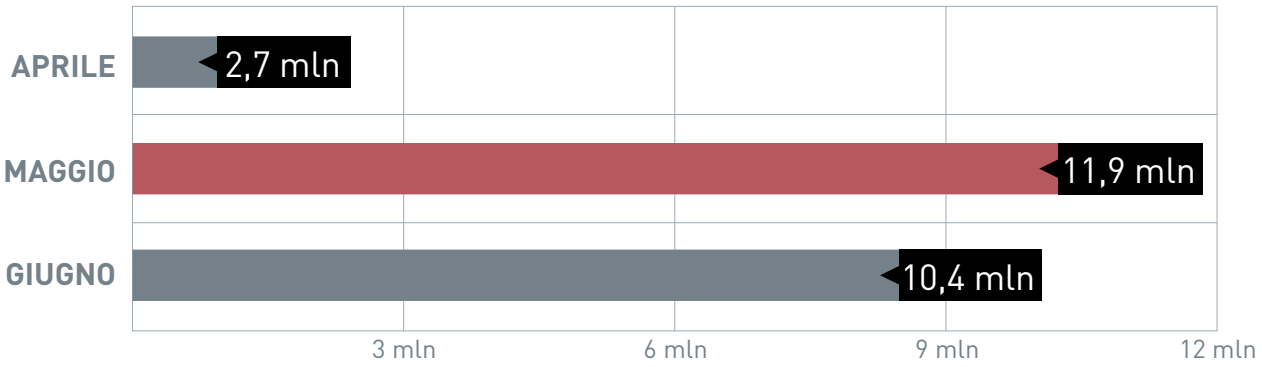
In questo trimestre, altri sviluppi della criminalità informatica hanno contribuito all'aumento dell'attività di spam e dei botnet. Tra queste attività segnaliamo l'attacco ai siti WordPress di aprile, la nascita di Stealrat e il suo uso di host colpiti per inviare spam e infine il rilevamento di picchi di attività spam.[16]

Numero di server C&C botnet rilevati ogni mese



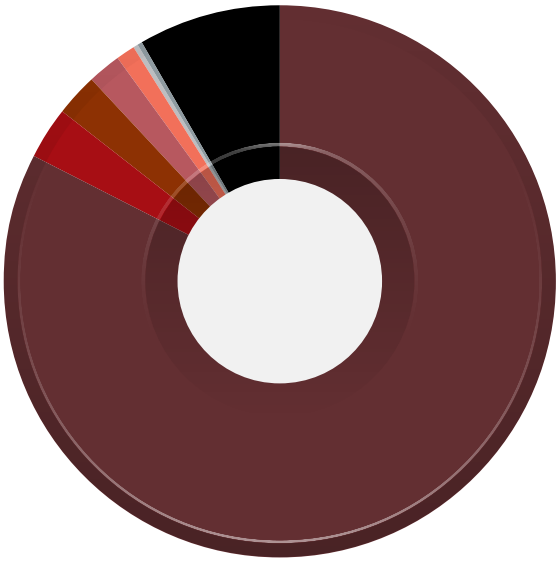
Il mese di maggio ha mostrato il numero maggiore di server C&C rilevati quest'anno.

Numero di collegamenti botnet al mese



A causa dell'aumento del numero di botnet attivi in maggio, abbiamo notato un aumento significativo del numero di collegamenti botnet in questo mese.

Prime 10 lingue usate per lo spam

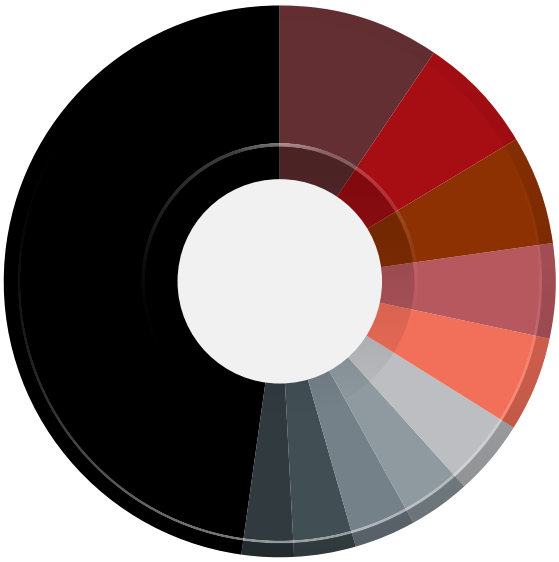


1	⬆ Inglese	82,56%
2	⬆ Cinese	3,26%
3	⬆ Russo	2,49%
4	⬆ Giapponese	1,94%
5	⬇ Tedesco	0,86%
6	⬇ Portoghese	0,29%
7	⬇ Spagnolo	0,20%
8	★ Islandese	0,16%
9	⬇ Francese	0,07%
10	★ Turco	0,07%
	Altre	8,10%

★ NEW ENTRY ⬆ È SALITO ⬇ È SCESO

Sebbene l'inglese sia rimasta la lingua preferita dagli spammer, abbiamo notato un aumento generale del volume di spam in lingue diverse dall'inglese.

Primi 10 paesi mittenti di messaggi spam



1	⬇ Stati Uniti	9,47%
2	⬆ Spagna	6,97%
3	⬇ India	6,36%
4	⬆ Taiwan	5,68%
5	★ Argentina	5,49%
6	★ Italia	4,52%
7	⬆ Colombia	3,70%
8	★ Messico	3,56%
9	⬆ Bielorussia	3,55%
10	★ Turchia	3,08%
	Altri	47,62%

★ NEW ENTRY ⬆ È SALITO ⬇ È SCESO

I criminali informatici stanno cercando altri paese nei quali impiantare le loro attività dannose: questo ha causato l'aumento dell'attività di spam in paesi come l'Argentina, l'Italia, il Messico e la Turchia.

PROBLEMI DI SICUREZZA DELLA VITA DIGITALE

Le minacce dei social network colpiscono piattaforme diverse

Poiché gli utenti gestiscono un numero sempre maggiore di account online, i criminali informatici escogitano modi diversi per sfruttare tale tendenza a loro vantaggio. Colpiscono ad esempio diversi siti di blogging famosi come Tumblr, WordPress e Blogger per realizzare siti di finti streaming di film famosi come L'uomo d'acciaio, Fast and Furious 6 e Iron Man 3.[17] Anche l'ID Apple e alcune famose piattaforme multiprotocollo di messaggistica istantanea (IM) come Digsby sono state prese di mira dagli attacchi.[18] Questi attacchi hanno colpito l'uso dell'approccio ad accesso singolo (SSO), che è pensato come promemoria per proteggere gli account online ed evitare l'uso di password deboli.

Gli utenti sono stati inoltre sottoposti nuovamente a vecchie tattiche di social engineering in quanto molti attacchi utilizzano come esca notizie diverse come l'attentato alla maratona di Boston, il tornado dell'Oklahoma, l'esplosione dell'impianto di fertilizzanti in Texas e il periodo della dichiarazione dei redditi.[19]

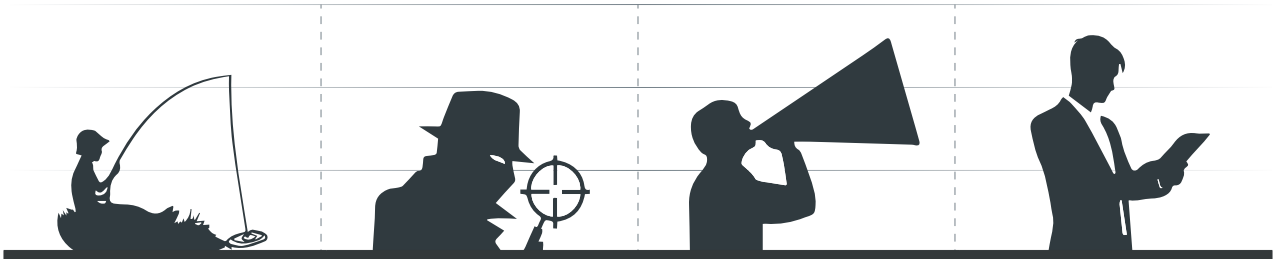
Alcune esche di social engineering utilizzate

Poiché un numero sempre maggiore di utenti in diversi settori utilizza Instagram, questo strumento è ora diventato un obiettivo idoneo per i criminali informatici.

In risposta ad alcuni incidenti di danneggiamento, LinkedIn, Evernote e Twitter hanno sviluppato delle misure di sicurezza aggiuntive, che includono meritoriamente delle misure di verifica dell'identità a due fattori.[20] L'attacco a Twitter rappresenta un interessante studio di caso per capire in che modo i social media possono essere utilizzati per diffondere false notizie, che possono causare gravi problemi.[21]

Le frodi via Instagram hanno mostrato che i criminali informatici mirano alle piccole e medie imprese e a quei professionisti del marketing che desiderano aumentare la loro presenza online. Queste frodi offrono dei "follower gratuiti" o utilizzano dei siti con aspetto professionale che offrono l'acquisto di follower in massa.[22] Tuttavia la tattica di vendere follower non è nuova. I criminali informatici si stanno semplicemente allargando anche ad altre piattaforme oltre a Twitter e Facebook. L'aspetto interessante e che queste minacce sono apparse nel momento in cui i social media hanno trovato dei modi per monetizzare i servizi offerti.[23]

Modalità utilizzate dai criminali informatici per indurre gli utenti a divulgare i loro dati[24]



SITI DI SPAM E PHISHING	MOTORI DI RICERCA	SOCIAL MEDIA	DISPOSITIVI MOBILI
2000-2009	2009–2011	DA FINE 2009 A OGGI	DAL 2011 A OGGI
Le frodi dei primi anni del 2000 riguardavano il settore farmaceutico, la notifica di account e frodi di tipo nigeriano, che solitamente rimandavano le vittime a siti di phishing.	I criminali informatici attaccano i motori di ricerca tramite l'ottimizzazione dei motori di ricerca (SEO) con blackhat. Questa tecnica sfrutta le parole chiave legate a notizie e/o eventi significativi per scopi illegali.	I social media si presentano come piattaforme attraenti per i criminali informatici per via del loro ampio bacino di utenti. Tra le piattaforme preferite dai criminali informatici vi sono Facebook, Twitter, Tumblr e Pinterest.	Oggi, gli smartphone e gli altri dispositivi mobili consentono ai criminali informatici di raggiungere nuovi obiettivi. L'adware mobile e le app dannose sono tra i mezzi preferiti per attuare piani illegali.

Con l'introduzione di nuove piattaforme, i criminali informatici hanno modificati i loro piani. Dalle truffe di tipo nigeriano inviate come spam, i criminali si sono ora estesi a nuove piattaforme e con nuovi obiettivi come i social media e i dispositivi mobili.

EXPLOIT E VULNERABILITÀ

I fornitori di software provano a correggere il tiro

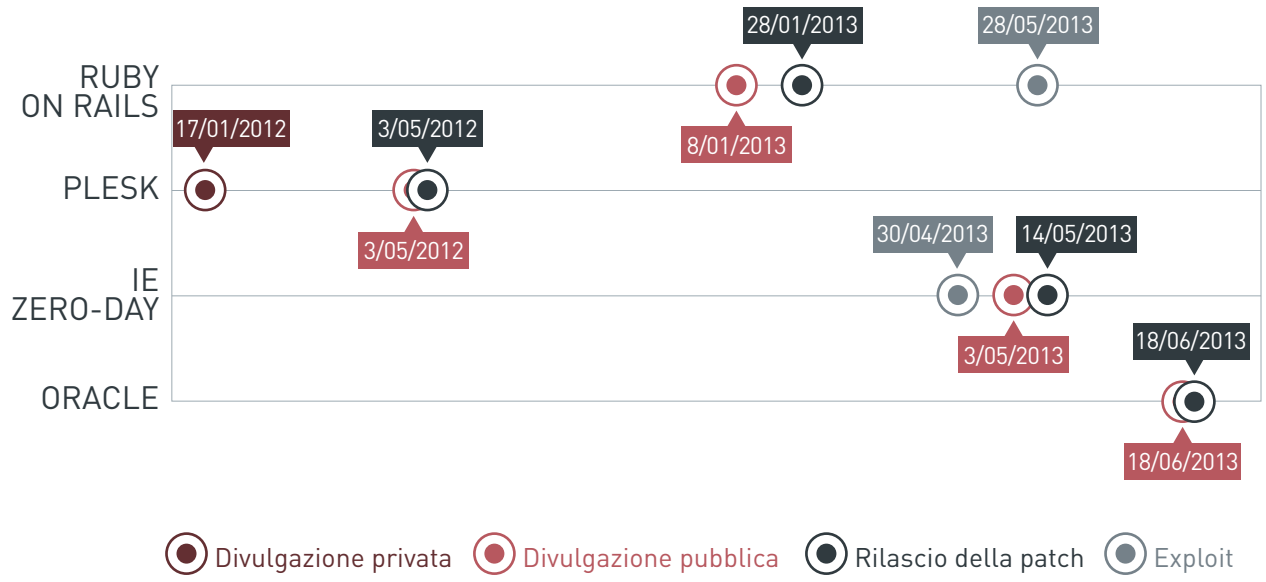
Dopo l'elevato volume di vulnerabilità zero-day del precedente trimestre, Oracle ha implementato diverse azioni volte a migliorare la sicurezza di Java. Tra queste il rilascio di aggiornamenti mensili, i test di sicurezza automatici e il divieto della firma automatica o di app non firmate all'interno del software Java presente nei browser.

Sebbene in questo trimestre siano stati rilevati meno incidenti di tipo zero-day, gli exploit hanno comunque rappresentato una minaccia seria per gli utenti. L'exploit zero-day Internet Explorer® (IE) rilevato sulla pagina del dipartimento del lavoro degli Stati Uniti ha dimostrato che anche siti affidabili possono essere compromessi.[25] Anche gli exploit che hanno colpito Plesk e ColdFusion® hanno evidenziato l'importanza di proteggere i server Web e hanno dimostrato in che modo le grandi aziende proteggono i loro siti.[26]

Come detto in precedenza, era solo questione di tempo prima che i criminali cominciassero a sfruttare la grave vulnerabilità Ruby on Rails rilevata a gennaio.[27] Questo trimestre abbiamo registrato degli exploit indirizzarti a falle del software, a seguito della divulgazione del codice della vulnerabilità.

La correzione delle vulnerabilità è stato uno tra gli argomenti più importanti del trimestre, soprattutto per via dell'annuncio di Google della sua politica di divulgazione dei sette giorni. Molti esperti di sicurezza considerano l'annuncio una proposta nobile ma non pratica. Tuttavia, come ha evidenziato il nostro CTO Raimund Genes, il problema più importante da affrontare è il modo in cui le vulnerabilità vengono descritte.

Linea temporale degli attacchi basati su vulnerabilità



In che modo Oracle pensa di proteggere Java

				
Rilasciando tre patch ogni tre mesi a partire da ottobre 2013	Utilizzando strumenti di verifica della sicurezza automatici contro le regressioni e i bug	Supportando i criteri di protezione Windows® in modo che gli amministratori di sistema possano impostare dei criteri di rete sull'uso di Java	Impedendo l'esecuzione di app non firmate o autofirmate	Rendendo flessibile il processo di revoca delle firme

CAMPAGNE DI ATTACCHI MIRATI, ATTACCHI DDoS E VIOLAZIONI DEI DATI

I problemi della sicurezza aziendale aumentano

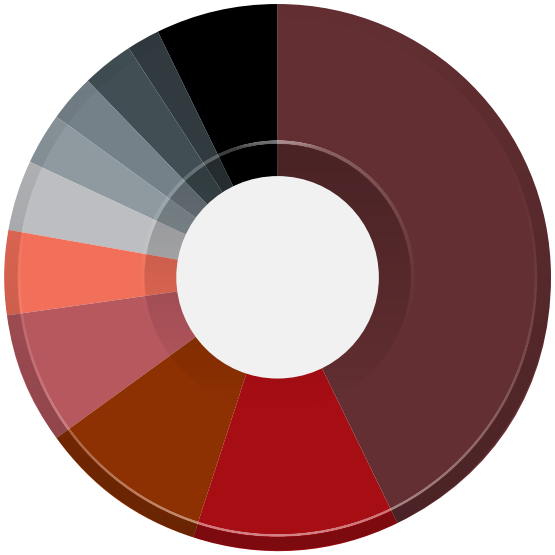
Attacchi mirati

Le campagne di attacchi mirati continuano a essere un problema per le organizzazioni: continuiamo a scoprire campagne attive e in corso. La campagna Naikon utilizza l'accesso remoto del cavallo di Troia (RAT), RARSTONE ed è stata rilevata principalmente in paesi dell'area Asia e Pacifico.[28] Questa campagna ha colpito diversi settori come le telecomunicazioni, l'industria di petrolio e gas, gli enti pubblici, i media e altri. Comincia solitamente con attacchi di spear-phishing mirati a una determinata vulnerabilità, utilizzata anche in un'altra campagna conosciuta come "Safe".[29]

Le nostre ricerche sulla campagna Safe, nel frattempo, hanno rivelato che gli indirizzi IP vittima sono diffusi in 100 paesi in tutto il mondo.

In questo trimestre, inoltre, gli attacchi mirati hanno sfruttato degli eventi tragici per infiltrarsi nelle reti aziendali. Abbiamo rilevato e-mail che hanno sfruttato l'attentato alla maratona di Boston come esca di social engineering per indurre gli utenti a scaricare una minaccia informatica in grado di comunicare tramite il Secure Sockets Layer (SSL).[30]

Tipi di file utilizzati negli attacchi spear-phishing collegati ad attacchi mirati



1	EXE/DLL	43%
2	PDF	12%
3	DOC	10%
4	JPG	8%
5	TXT/HTML	5%
6	RTF	4%
7	ZIP	3%
8	XLS	3%
9	RAR	3%
10	PPS/PPT	2%
	Altri	7%

Gli autori della minaccia modellano l'attacco a seconda del loro obiettivo. Utilizzano qualsiasi tipo di file pur di avvicinarsi al loro obiettivo: infiltrarsi in una rete.

Attacchi DDoS

Molti enti sudcoreani hanno subiti diverse violazioni di sicurezza che hanno causato la distribuzione di attacchi di tipo denial-of-service (DDoS) e blocchi dei siti. Un incidente in particolare ha reso inaccessibili diversi siti. Come nel caso del cavallo di Troia che cancellava l'MBR di marzo, questo attacco è stato progettato in modo da attivarsi in un momento specifico. L'incidente ha dimostrato che i criminali informatici continuano a perseguire obiettivi di alto valore e che sono in grado di infliggere il massimo danno in un periodo di tempo ridottissimo.

Violazione dei dati

In questo trimestre aziende come Yahoo! Japan, LivingSocial, Twitter e Name.com hanno subito violazioni di sicurezza. Anche Opera ha subito una violazione che ha condotto al furto di certificati digitali obsoleti.

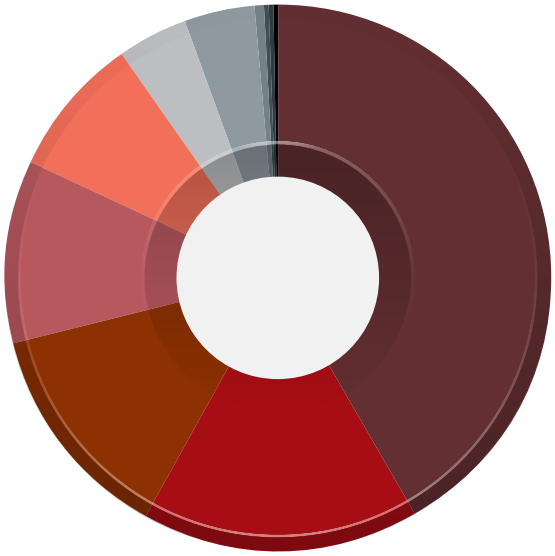
Attacchi mirati ad aziende molto conosciute[31]

AZIENDA	RISULTATO
Goo	Blocco di 100.000 account per impedire accessi non autorizzati
Yahoo! Japan	I criminali informatici hanno cercato di estrarre dati appartenenti a 1,27 milioni di utenti
Associated Press (AP)	I criminali informatici hanno manomesso l'account Twitter di AP e hanno causato un danno in borsa di 200 milioni di dollari
LivingSocial	Accesso non autorizzato agli account di 50 milioni di utenti
Diversi enti sudcoreani	Diversi siti web sono stati bloccati e hanno subito attacchi DDoS

Poiché gli attacchi contro le aziende ad alto profilo causano danni ingenti, è sempre più importante consolidare le difese dell'organizzazione.

Appendice

Prime 10 famiglie di adware per Android



1	ARPUSH	41,79%
2	ADSWO	16,50%
3	PLANKTON	12,84%
4	LEADBLT	11,02%
5	IZP	8,17%
6	WAPSX	4,25%
7	OQX	4,10%
8	WBOO	0,67%
9	YOUMI	0,27%
10	UAPSH	0,13%
	Altri	0,26%

URL dannosi per paese di origine

	PAESE	PERCENTUALE
1	Stati Uniti	25,90%
2	Germania	3,24%
3	Cina	3,16%
4	Paesi Bassi	3,13%
5	Corea del Sud	2,60%
6	Francia	1,94%
7	Giappone	1,93%
8	Russia	1,64%
9	Canada	0,81%
10	Regno Unito	0,77%
	Altri	54,88%

Non è stato rilevato alcun cambiamento significativo tra i paesi dell'elenco. Gli Stati Uniti hanno la maggiore percentuale del volume di URL dannosi, seguita dalla Germania.

Primi 10 paesi con il maggior numero di server C&C botnet

	PAESE	PERCENTUALE
1	Stati Uniti	24,05%
2	Australia	5,15%
3	Corea del Sud	3,38%
4	Cina	3,02%
5	Germania	2,87%
6	Taiwan	2,10%
7	Francia	1,88%
8	Regno Unito	1,72%
9	Brasile	1,47%
10	Canada	1,18%
	Altri	53,18%

Come nel trimestre precedente, gli Stati Uniti hanno il maggior numero di server C&C botnet mentre l'Australia ha superato la Corea del Sud.

Primi 10 paesi con il maggior numero di collegamenti ai botnet

	PAESE	CONDIVISIONE
1	Malesia	28,39%
2	Stati Uniti	14,14%
3	Francia	11,63%
4	Germania	5,64%
5	Canada	5,29%
6	Corea del Sud	4,13%
7	Regno Unito	3,84%
8	Thailandia	3,22%
9	Hong Kong	3,07%
10	Italia	2,53%
	Altri	18,12%

Gli attacchi DDoS in Malesia sono stati collegati alle elezioni e hanno contribuito all'aumento del volume del paese di collegamenti dannosi.

Bibliografia

1. Trend Micro Incorporated. (2013). "TrendLabs 2012 Annual Security Roundup: Evolved.Threats.in.a.'Post-PC'.World." Ultimo accesso 30 luglio 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf.

2. Jonathan Leopando. (10 luglio 2013). *TrendLabs Security Intelligence Blog*. "Android Vulnerability Affects 99% of Devices—Trend Micro Users Protected.". Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-solution-for-vulnerability-affecting-nearly-all-android-devices/.

3. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "ANDROIDOS_OBAD.A." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_OBAD.A.

4. Leo Zhang. (13 luglio 2013). *TrendLabs Security Intelligence Blog*. "Cybercriminals Improve Android Malware Stealth Routines with OBAD." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/.

5. Trend Micro Incorporated. (2013): *Threat Encyclopedia*. "ANDROIDOS_FAKEBANK.A." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_FAKEBANK.A.

6. Weichao Sun. (14 maggio 2013). *TrendLabs Security Intelligence Blog*. "Mobile Ads Pushed by Android Apps Lead to Scam Sites." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-ads-pushed-by-android-apps-lead-to-scam-sites/.

7. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "ANDROIDOS_FAKEAV.F." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_FAKEAV.F.

8. Iain Thomson. (27 marzo 2013). *The Register*. "Tibetan and Uyghur Activists Targeted with Android Malware." Ultimo accesso 30 luglio 2013, http://www.theregister.co.uk/2013/03/27/android_malware_targeting_tibetan/.

9. Ericsson ConsumerLab. (6 agosto 2012). *Ericsson.com*. "Vietnamese Consumers Show Increasing Demand for Smartphones and Tablets." Ultimo accesso 30 luglio 2013, http://www.ericsson.com/vn/news/2012_vn_smartphone_demands_254740123_c.

10. Trend Micro Incorporated. (2012). "Security Threats to Business, the Digital Lifestyle, and the Cloud: Trend Micro Predictions for 2013 and Beyond." Ultimo accesso 30 luglio 2013, http://www.trendmicro.ca/cloud-content/us/pdfs/security-intelligence/spotlightarticles/sp-trend-micro-predictions-for-2013-and-beyond.pdf.

11. Roddell Santos. (28 maggio 2013). *TrendLabs Security Intelligence Blog*. "BANKER Malware Hosted in Compromised Brazilian Government Sites." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/banker-malware-hosted-in-compromised-brazilian-government-sites/.

12. Ranieri Romera. (7 maggio 2013). *TrendLabs Security Intelligence Blog*. "Homemade Browser Targeting 'Banco do Brasil' Users." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/homemade-browser-targeting-banco-do-brasil-users/.

13. Roddell Santos. (14 giugno 2013). *TrendLabs Security Intelligence Blog*. "Malware Redirects South Korean Users to Phishing Sites." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/malware-redirects-south-korean-users-to-phishing-sites/.

14. Abigail Pichel. (10 giugno 2013). *TrendLabs Security Intelligence Blog*. "Going Solo: Self-Propagating ZBOT Malware Spotted." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/going-solo-self-propagating-zbot-malware-spotted/.

15. Lenart Bermejo. (24 maggio 2013). *TrendLabs Security Intelligence Blog*. "Worm Creates Copies in Password-Protected Archived Files." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/worm-creates-copies-in-password-protected-archived-files/.

16. Jessa Dela Torre. (16 aprile 2013). *TrendLabs Security Intelligence Blog*. "Compromised Sites Conceal Stealrat Botnet Operations." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-sites-conceal-stealrat-botnet-operations/.

17. Paul Pajares. (8 luglio 2013). *TrendLabs Security Intelligence Blog*. "Man of Steel, Fast and Furious 6 Among Online Fraudsters' Most Used Lures.". Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/man-of-steel-fast-and-furious-6-among-online-fraudsters-most-used-lures/; Gelo Abendan. (2 maggio 2013). *TrendLabs Security Intelligence Blog*. "Fake Iron Man 3 Streaming Sites Sprout on Social Media." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/fake-iron-man-3-streaming-sites-sprout-on-social-media/.

18. Anthony Melgarejo. (2 maggio 2013). *TrendLabs Security Intelligence Blog*. "Backdoor Leads to Facebook and Multiprotocol Instant-Messaging Worm." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-leads-to-facebook-and-multi-protocol-instant-messaging-worm/; Paul Pajares. (30 aprile 2013). *TrendLabs Security Intelligence Blog*. "Hackers to Manage Your Apple ID, If Caught from Phishing

Bait." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/hackers-to-manage-your-apple-id-if-caught-from-phishing-bait/.

19. Aisa Escober. (16 aprile 2013). *TrendLabs Security Intelligence Blog.* "KELIHOS Worm Emerges, Takes Advantage of Boston Marathon Blast." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/kelihos-worm-emerges-takes-advantage-of-boston-marathon-blast/; Trend Micro Incorporated. (2013). *Threat Encyclopedia.* "Spam Attack Leverages Oklahoma Tornado Disaster." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/spam/494/Spam+Attack+Leverages+Oklahoma+Tornado+Disaster; Ryan Certeza. (19 aprile 2013). *TrendLabs Security Intelligence Blog.* "Cybercriminals Quickly Take Advantage of Texas Fertilizer Plant Blast, MIT Shooting." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-quickly-take-advantage-of-texas-fertilizer-plant-blast-mit-shooting/; Gelo Abendan. (4 aprile 2013). *TrendLabs Security Intelligence Blog.* "Cybercriminals Threaten Tax Day Once Again." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-threaten-tax-day-once-again/.

20. Jim Finkle. (31 maggio 2013). *NBC News Technology.* "LinkedIn Improves Security with Two-Factor Authentication." Ultimo accesso 30 luglio 2013, http://www.nbcnews.com/technology/linkedin-improves-security-two-factor-authentication-6C10141010; Seth Hitchings. (30 maggio 2013). *The Evernote Blog.* "Evernote's Three New Security Features." Ultimo accesso 30 luglio 2013, http://blog.evernote.com/blog/2013/05/30/evernotes-three-new-security-features/; Jim O'Leary. (22 maggio 2013). *Twitter Blog.* "Getting Started with Login Verification." Ultimo accesso 30 luglio 2013, https://blog.twitter.com/2013/getting-started-login-verification.

21. David Jackson. (23 aprile 2013). *USA Today News.* "AP Twitter Feed Hacked; No Attack at White House." Ultimo accesso 30 luglio 2013, http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/.

22. Karla Agregado. (16 maggio 2013). *TrendLabs Security Intelligence Blog.* "Get Free Followers! on Instagram? Get Free Malware, Survey Scams Instead." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/get-free-followers-on-instagram-get-free-malware-survey-scams-instead/.

23. Zachary Seward. (20 maggio 2013). *Quartz.* "How Yahoo Plans to Make Money on Tumblr: Ads That Don't Feel Like Ads." Ultimo accesso 30 luglio 2013, http://qz.com/86437/how-yahoo-plans-to-make-money-on-tumblr-ads-that-dont-feel-like-ads/.

24. Jay Alabaster. (4 aprile 2013). *Computerworld.* "Japanese Web Portals Hacked, Up to 100,000 Accounts Compromised." Ultimo accesso 30 luglio 2013, http://www.computerworld.com.au/article/458079/japanese_web_portals_hacked_up_100_000_accounts_compromised/; *LivingSocial.* "LivingSocial Security Notice." Ultimo accesso 30 luglio 2013, https://www.livingsocial.com/createpassword; Kadim Shubber. (20 maggio 2013). *Wired UK.* "Millions of Users' Data Hacked in Yahoo Japan Security Breach." Ultimo accesso 30 luglio 2013, http://www.wired.co.uk/news/archive/2013-05/20/yahoo-japan-hacked; Erin Madigan White. (23 aprile 2013). *AP Blog, The Definitive Source.* "AP Responds to Hacking of Twitter Account." Ultimo accesso 30 luglio 2013, http://blog.ap.org/2013/04/23/hackers-compromise-ap-twitter-account/.

25. Dexter To. (5 maggio 2013). *TrendLabs Security Intelligence Blog. "Compromised U.S. Government Web Page Used Zero-Day Exploit." Ultimo accesso 30 luglio 2013,* http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-us-government-webpage-used-zero-day-exploit/.

26. Sooraj K.S. (6 giugno 2013). *TrendLabs Security Intelligence Blog.* "Plesk Zero-Day Exploit Results in Compromised Web Server." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/plesk-zero-day-exploit-results-in-compromised-webserver/.

27. Gelo Abendan. (30 maggio 2013). *TrendLabs Security Intelligence Blog.* "Trend Micro Deep Security Guards Users from Ruby on Rails Exploit." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-deep-security-guards-users-from-ruby-on-rails-exploit/.

28. Maharlito Aquino. (13 giugno 2013). *TrendLabs Security Intelligence Blog.* "RARSTONE Found in Targeted Attacks." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/.

29. Kyle Wilhoit. (17 maggio 2013). *TrendLabs Security Intelligence Blog.* "Hiding in Plain Sight: A New Targeted Attack Campaign." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-sight-a-new-apt-campaign/.

30. Nart Villeneuve. (25 aprile 2013). *TrendLabs Security Intelligence Blog.* "Targeted Attack Campaign Hides Behind SSL Communication." Ultimo accesso luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-campaign-hides-behind-ssl-communication/.

31. Gelo Abendan. (3 marzo 2012). *Threat Encyclopedia.* "Mobile Apps: New Frontier for Cybercrime." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/webattack/119/mobile apps new frontier for cybercrime; Marco Dela Vega. (23 novembre 2010). *TrendLabs Security Intelligence Blog.* "With Holiday Wishes Come Poisoned Searches." Ultimo accesso 30 luglio 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/with-holiday-wishes-come-poisoned-searches/; Dianne Kristine Lagrimas. (13 novembre 2011). *Threat Encyclopedia.* "Sports as Bait: Cybercriminals Play to Win." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/webattack/99/sports as bait cybercriminals play to win; Valerie Ria Rivera. (29 marzo 2011). *Threat Encyclopedia.* "Spam, Scams, and Other Social Media Threats." Ultimo accesso 30 luglio 2013, http://about-threats.trendmicro.com/us/webattack/75/spam scams and other social media threats.

Realizzato da:

TrendLabs

Supporto tecnico globale e ricerca e sviluppo di **TREND MICRO**

DECLINAZIONE DI RESPONSABILITÀ TREND MICRO

Le informazioni riportate nel presente documento hanno finalità esclusivamente informative e di divulgazione. Non vengono fornite e non devono essere interpretate come consulenza legale. Le informazioni contenute nel presente documento potrebbero non essere applicabili a tutte le situazioni e potrebbero non riflettere la situazione attuale. Le informazioni del presente documento non devono essere considerate come base affidabile o come fondamento per intraprendere azioni, senza essere accompagnate da un'adeguata consulenza legale basata su fatti specifici; le circostanze e le altre informazioni qui contenute non possono essere interpretate diversamente. Trend Micro si riserva il diritto di modificare il contenuto del presente documento in qualsiasi momento senza preavviso.

La traduzione del presente materiale in lingue diverse dalla lingua di origine è da intendersi esclusivamente come supporto. L'accuratezza della traduzione non è garantita e non è implicita. Per qualsiasi domanda relativa all'accuratezza della traduzione, fare riferimento alla versione in lingua originale del documento. Qualsiasi discrepanza o differenza presente nella traduzione non è vincolante e non ha alcun effetto ai fini della conformità o dell'esecuzione.

Sebbene Trend Micro si impegni in modo ragionevole a inserire nel presente documento informazioni accurate e aggiornate, Trend Micro non rilascia alcuna garanzia o dichiarazione di qualsiasi tipo in relazione all'accuratezza, alla validità corrente o alla completezza delle informazioni. L'utente accetta di accedere, utilizzare e fare affidamento sul presente documento e sul suo contenuto a proprio rischio. Trend Micro esclude espressamente ogni garanzia, espressa o implicita, di qualsiasi tipo. Trend Micro ed eventuali terzi coinvolti nella creazione, produzione o fornitura del presente documento escludono qualsiasi responsabilità per qualsiasi tipo di conseguenza, perdita o danno, incluse perdite dirette, indirette, speciali, consequenziali di profitti aziendali, nonché danni speciali di qualsiasi tipo derivanti dall'accesso, l'utilizzo, l'impossibilità di utilizzo del presente documento ovvero da errori o omissioni nel contenuto del presente documento. L'uso delle presenti informazioni costituisce accettazione all'uso delle informazioni "così come sono".

Trend Micro Incorporated, leader globale di software e soluzioni di protezione, vuole rendere il mondo sicuro per lo scambio di informazioni digitali. Per ulteriori informazioni, visitare il sito www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud