Report

Report McAfee sulle minacce: secondo trimestre 2011

McAfee® Labs™

Il panorama delle minacce del 2011 sta vivendo un anno di confusione e cambiamento. Osserviamo confusione rispetto alle importanti sfide lanciate da gruppi di cosiddetti hacktivisti come LulzSec e Anonymous, e cambiamenti relativi alle nuove categorie di malware e dispositivi presi di mira.

In questo trimestre McAfee Labs ha rilevato una fervida attività da parte degli hacktivisti, ma in modo molto diverso rispetto al passato. Il gruppo Lulz Security, LulzSec in breve, si differenzia dagli altri gruppi di hacktivisti perché non ha obiettivi specifici. Si sono attivati, come sostengono, per divertimento o "lulz" (una variante di LOL, o loughing out loud, che significa ridere ad alta voce), ma hanno dimostrato una certa bravura nel compromettere reti e server, nonché nel rubare nomi utente, password e altri dati. LulzSec ha perpetrato varie intrusioni contro un certo numero di aziende, oltre ad attacchi contro dipartimenti di polizia e agenzie di intelligence e molte altre azioni dannose. Nonostante alcuni dei risultati e degli utilizzi di queste azioni dannose siano ancora in corso (forniamo un'utile panoramica dell'attività del trimestre) una cosa risulta chiara: molte aziende, di grandi e piccole dimensioni, sono più vulnerabili di quanto abbiano mai pensato. Inoltre, il settore della sicurezza potrebbe dover riconsiderare alcuni dei suoi presupposti fondamentali, tra cui quello che recita "Proteggiamo realmente utenti e aziende?". Sebbene LulzSec possa aver cessato la propria attività durante questo trimestre, le domande che questo e altri gruppi di hacktivisti hanno sollevato verranno discusse a lungo.

Un cambiamento significativo nel primo trimestre del 2011 è stata l'affermazione di Android quale terza piattaforma presa più di mira per il malware mobile. In questo trimestre il nuovo malware specifico per Android è salito per quantità al primo posto, mentre J2ME (Java Micro Edition) è la seconda piattaforma più colpita, con un terzo del malware rilevato su Android. Questo aumento per quanto riguarda le minacce contro una piattaforma così diffusa dovrebbe farci riflettere sul nostro comportamento relativamente ai dispositivi mobile e al livello di preparazione del settore della sicurezza per contrastare questa crescita.

Abbiamo inoltre registrato un aumento del malware mobile a scopo di lucro, tra cui semplici Trojan che inviano SMS e Trojan più complessi che utilizzano gli exploit per compromettere gli smartphone. Forniamo un aggiornamento dei "listini prezzi" del crimine informatico oltre ad alcuni cambiamenti nei prezzi per toolkit e servizi. Le pratiche del "crimeware as a service" e il fiorente "hacktivism as a service" continuano a evolvere man mano che gli interessi e gli obiettivi cambiano. Se guardiamo al lato positivo, in questo trimestre sono state registrate alcune importanti vittorie contro i criminali informatici.

Proseguendo sulla scia del cambiamento, abbiamo osservato un calo considerevole nel malware ad esecuzione automatica (AutoRun) e KoobFace, compensato da un forte aumento del software antivirus confraffatto che colpisce i computer Mac. Il sistema operativo OS X di Apple è stato fondamentalmente ignorato per anni dagli autori di malware, perciò questo fatto rappresenta un cambiamento significativo per i criminali informatici.

Il malware ha proseguito a crescere complessivamente nel corso del trimestre così come il malware rootkit. I rootkit, utilizzati principalmente per le loro azioni furtive e caratteristiche di elasticità, rendono il malware più efficace e persistente e la sua popolarità sta crescendo. Rootkit come Koutodoor e TDSS si manifestano sempre più frequentemente. La quantità di malware che attacca le vulnerabilità nei prodotti di Adobe continua a sopraffare il malware rivolto contro i prodotti Microsoft.

Botnet e minacce contro i programmi di messaggistica, sebbene ancora ai livelli più bassi, hanno iniziato a aumentare nuovamente. Prevedevamo tale ripresa dopo la recente chiusura di alcune botnet. Utenti e aziende devono mettere in conto questa crescita e prepare le proprie difese e reazioni di conseguenza. Prendiamo di nuovo in esame i temi del social engineering per area geografica e argomento e le botnet per area geografica e tipologia.

Nel corso di questo trimestre abbiamo osservato numerosi picchi nell'attività web dannosa oltre a una preoccupante crescita nel numero di blog e wiki con reputazioni pericolose. Sono aumentati anche i siti che rilasciano malware, i programmi PUP e i siti di phishing.

Il secondo trimestre dell'anno è stato chiaramente un periodo di confusione, cambiamenti e nuove sfide.

Indice dei contenuti

Hacktivism

All'inizio di questo trimestre il gruppo Anonymous ha apparentemente litigato e si è diviso. Il 9 maggio, un comunicato stampa di Anonymous affermava che la rete Anonops aveva smesso di funzionare dopo che il co-amministratore del sito web Ryan aveva tentato di organizzare un "colpo di stato". Come rappresaglia, le sue informazioni di contatto sono state immediatamente rese pubbliche sul web.

Intorno al 7 maggio, è apparso un nuovo account Twitter registrato con il nome utente @LulzSec, contrassegnando la nascita di Lulz Security. La sua prima prodezza non ha ottenuto una grande copertura sulla stampa; tuttavia, quando ha preso di mira il mondo dello spettacolo, si è assistito alla vera presentazione di LulzSec al mondo.

Dopo 50 giorni di attività, le avventure di LulzSec sono terminate a causa delle lotte intestine. Questi eventi mostrano un livelo di immaturità in alcuni gruppi etichettati come hacktivisti politici e che affermano di essere parte di Anonymous. Jester (th3j35t3r, un avversario di Anonymous noto per la sua lotta contro i siti web jihadisti e anti Stati Uniti) e altri gruppi (Team Web Ninjas, Backtrace, The A-Team, Teamp0ison, ecc.) hanno considerato importante denunciare i loro ex colleghi. Queste lotte intestine hanno aiutato le autorità a identificare alcuni di questi hacker.

Tra gli altri incidenti segnalati vi è un "grave" attacco contro la Commissione Europea proprio prima di un summit per discutere della struttura futura dell'Unione Europea, della strategia economica e della guerra in Libia[1]. Il Ministero delle finanze francesi ha subito un attacco simile. L'organizzazione australiana di intelligence ASIO (Australian Security Intelligence Organisation) ha rivelato che sta investigando su un attacco che ha compromesso i computer di almeno 10 ministri federali, tra cui il primo ministro, il ministro degli esteri e il ministro della difesa. Il governo tedesco ha segnalato di aver rilevato una media di cinque attacchi mirati al giorno contro gli utenti delle reti governative[2].

Alcuni account pubblicati annoverano le varie operazioni degli hacktivisti, come #antisec, #OpNewBlood, #OpLibya, #OpBrazil, a oltre 4.000 in totale, ma questo numero è difficile da verificare. Queste operazioni hanno portato alla messa offline di alcuni siti web, al furto di grandi quantità di nomi utente e password e al furto e caricamento di documenti riservati. Molte aziende hanno subito attacchi motivati politicamente molto efficaci. Molti osservatori hanno definito questi attacchi semplicistici, anche goffi, ma questi sapientoni non hanno capito il punto: il fenomeno dell'hacktivism riguarda il messaggio non il metodo.

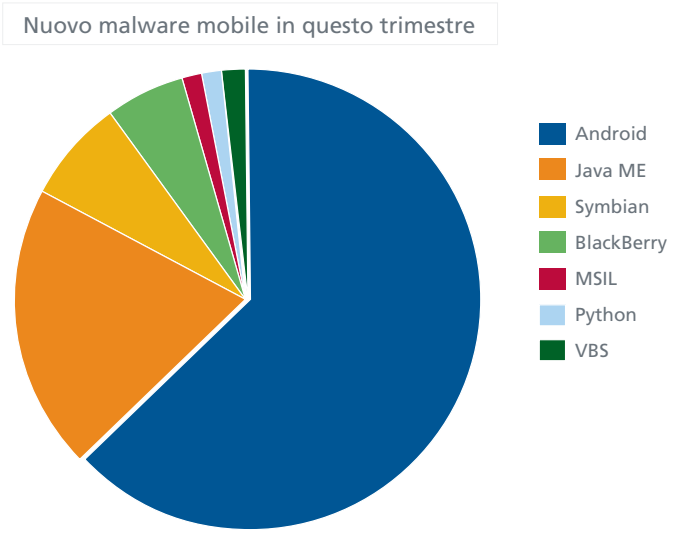
Anche due intrusioni da parte di un hacker rumeno hanno catturato l'attenzione a causa degli obiettivi di alto profilo: le agenzie spaziali di Stati Uniti e Europa.

In un blog di Aprile, questo hacker ha pubblicato informazioni provenienti dal server dell'Agenzia Spaziale Europea che includevano nomi, nomi utente e e-mail di oltre 150 utenti. In maggio, lo stesso hacker ha affermato di aver violato un server del Goddard Space Flight Center della NASA e di aver ottenuto l'accesso a dati satellitari riservati. Aveva pubblicato sul suo blog una schermata di ciò che affermava essere uno dei principali server FTP della NASA.

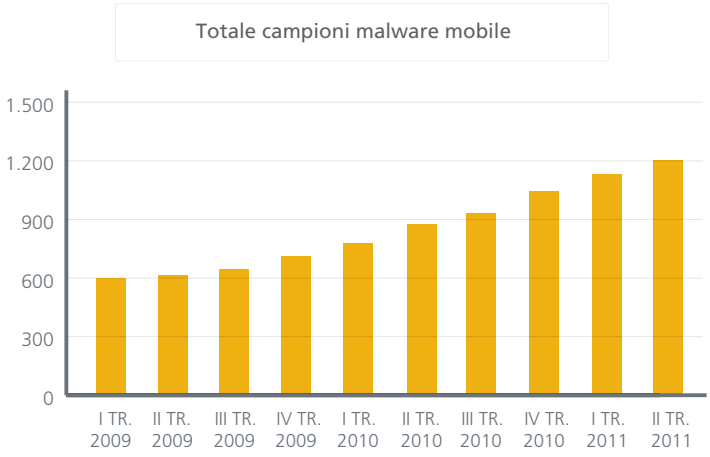
1. http://www.bbc.co.uk/news/world-europe-12840941
2. http://www.bundestag.de/presse/hib/2011_05/2011_201/08.html

Minacce mobile

Questo trimestre il malware basato sul sistema operativo Android è diventato l'obiettivo più popolare per gli sviluppatori di malware mobile. Si tratta di una rapida crescita per Android, che sorpassa tre volte il secondo posto di Java Micro Edition.



Mentre osserviamo una crescita stabile significativa nel panorama delle minacce malware mobili, molte delle stesse funzioni e caratteristiche delle minacce basate su PC fanno già parte della base di codice. Le minacce mobile sfruttano già gli exploit, utilizzano funzionalità botnet e utilizzano anche funzioni rootkit per la loro durata azione furtiva e stabilità.



Le applicazioni modificate malevolmente rappresentano ancora un vettore popolare per infettare i dispositivi: alterano un'applicazione o un gioco legittimo così che gli utenti scaricheranno e installeranno da soli malware sui loro smartphone.

In questo trimestre le applicazioni modificate che si infiltrano sono risultate essere il malware Android/Jmsonez.A, Android/Smsmecap.A e le famiglie Android/DroidKungFu e Android/DrdDreamLite. Analizziamo più attentamente alcuni malware mobile recenti.

Android/Jmsonez.A è una versione di un'applicazione calendario che non funziona esattamente come previsto[3]. Indipendentemente da quando il programma viene lanciato, visualizza il calendario per il mese di gennaio 2011. Se l'utente cerca di modificare il mese in una data futura, il malware inizia a inviare messaggi SMS a un numero a tariffa maggiorata. Inoltre, Android/Jmsonez.A controlla la casella inbox per i messaggi SMS di conferma dal servizio a tariffa maggiorata per evitare di essere rilevato.

Android/Smsmecap.A è una versione modificata di un'applicazione comedy legittima[4]. Il malware invia messaggi SMS divertenti irriverenti a tutti i contatti presenti nella rubrica dell'utente. Dal 21 maggio, la data della presunta "Estasi", ha inviato messaggi in tono beffardo.

La famiglia Android/DroidKungFu è simile a Android/DrdDream; utilizza inoltre un paio di vulnerabilità di tipo root exploits per rimanere su un dispositivo[5]. Gli exploit sono di fatto identici a quelli utilizzati da Android/DrdDream tranne che sono stati cifrati con l'algoritmo AES. Queste varianti possono anche caricare URL e installare software aggiuntivi e aggiornamenti.

La famiglia Android/DrdDreamLite è un avariante meno esperta della famiglia Android/DrdDream originale[6]. La versione Lite utilizza l'algoritmo DES per cifrare i dati che invia all'aggressore. Android/DrdDreamLite non include alcun root exploit per rimanere installato su un dispositivo infetto.

Altri Trojan complessi sono Android/Tcent.A, la famiglia Android/Crusewin.A, Android/J.SMSHider.A e Android/Toplank.A.

Android/Tcent.A è un altro Trojan che invia SMS a tariffa maggiorata, come Android/Jmsonez.A, ma include un'interessante funzione di auto-protezione[7]. Il malware mira a colpire il servizio di messaggistica immediata QQ, che è diffuso in Cina. Il malware cerca di disintallare l'antivirus e altri software di sicurezza incorporati con i client mobile di QQ.

La famiglia Android/Crusewin.A include una serie di Trojan che inviano messaggi a tariffe maggiorate[8]. A differenza di malware più semplice, la famiglia Android/Crusewin.A include alcune funzioni botnet, tra cui l'esecuzione di ordini da parte del command server dell'aggressore. L'aggressore può inviare messaggi SMS da un dispositivo infetto, utile per iscrivere le vittime a servizi di abbonamento a tariffa maggiorata e cercare di disinstallare il software. L'ultima funzione è simile a quella di Android/Tcent.A ma ha un piccolo problema. Android/Crusewin.A utilizza un codice di disinstallazione che funziona solo su smartphone Symbian; non funzionerà correttamente su Android. Ciò suggerisce che l'autore del malware sia in grado di effettuare il porting del codice Trojan/botnet Symbian sulla piattaforma Android.

Android/J.SMSHider.A invia messaggi a tariffa maggiorata[9]. L'autore del malware ha modificato un'app "SMS love analyzer" legittima aggiungendo funzionalità backdoor e la capacità di cancellare i messaggi SMS in arrivo. Android/J.SMSHider.A utiizza la cifratura con algoritmo DES per coprire le comunicazioni con l'aggressore.

Android/Toplank.A simula di essere un aggiornamento multiutente del famoso gioco Angry Birds. Il malware invia informazioni sensibili (identità dell'abbonato al servizio mobile internazionale, l'elenco delle autorizzazioni concesse al malware, ecc.) all'aggressore e può scaricare un'applicazione Android aggiuntiva su un dispositivo infetto. La nuova app fornisce una backdoor all'aggressore, che può poi aggiungere e cancellare bookmark, cronologia del browser e shortcut. L'aggressore può anche scaricare altro software.

Gli autori di crimeware mobile continuano con i loro trucchetti con SymbOS/Zitmo.C e BlackBerry/Zitmo.D, che sono dei semplici programmi che inviano SMS. Gli autori hanno già compromesso i PC delle vittime con malware avanzato, in modo da far sembrare che stiano facendo il minimo indispensabile sulle piattaforme mobile per abilitare i loro attacchi.

3. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501748
4. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=509500
5. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=522281
6. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=518925
7. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501599
8. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501639
9. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=527859

Crimine informatico

Rubriche di indirizzi e-mail in vendita

Tramite le loro botnet o attraverso servizi di noleggio, gli spammer hanno bisogno di elenchi di indirizzi e-mail per inondare il mondo. I prezzi variano per tali imprese, spesso in base alla posizione.

Paese	Prezzi per gli elenchi di indirizzi (tutti in dollari USA)
Russia	400.000 indirizzi a San Pietroburgo: 25 $ 1.000.000 (intero paese): 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 8.000.000: 200 $
Stati Uniti	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 10.000.000: 300 $
Ucraina	2.000.000: 40 $
Germania	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 8.000.000: 200 $
Turchia	1.000.000: 50 $
Portogallo	150.000: 25 $
Australia	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $
Inghilterra	1.500.000: 100 $

Strumenti crimeware

Anche in questo trimestre, abbiamo rilevato nuovi prodotti e aggiornamenti tra i kit exploit. I più ragguardevoli sono stati il rilascio di Eleonore Versione 1.6.5, con due exploit nel 2011 e Best Pack, con un exploit 2011.

Nome	Prezzi (tutti in dollari USA)	Descrizione
Weyland-Yutani BOT Versione 1.0	1.000 $	Offerto sul mercato nero. Il venditore ha rapidamente chiuso l'offerta dopo aver affermato di aver trovato un acquirente.
BlackHole Exploit Kit Versione 1.1.0	Licenza annuale: 1.500 $ 6 mesi: 1.000 $ 3 mesi: 700 $	Questo kit è apparso la prima volta nel settembre 2010. Aggiornato in Aprile, contiene nove exploit, di cui sei del 2010.
Best Pack		Annunciato da ScriptKiddieSec e Kahu Security come il possibile successore di Dragon Pack, questo pacchetto exploit contiene sette vecchi exploit e uno del 2011[10]: • CVE-2011-0611 (colpisce le versioni di Adobe Flash Player precedenti alla versione 10.2.159)
Phoenix Exploit Kit Versione 2.7	2.200 $	Questa versione ha sostituito la Versione 2.5, il cui codice era trapelato in aprile. La release attuale include almeno 15 exploit, di cui sei del 2010.
Eleonore Versione 1.6.5	2.000 $	10 exploit includono due exploit Flash Player del 2011: • CVE-2011-0558 (Flash prima della versione 10.2) • CVE-2011-0611 (Flash prima della versione 10.2.159)
YES Exploit Kit 4.0	400 $	Ha sostituito la Versione 3.0RC dell'aprile 2010. Questa versione contiene circa 20 exploit, di cui sette del 2010.

11. http://www.kahusecurity.com/2011/best-pack/

Azioni contro i criminali informatici

Questo trimestre non è stato del tutto negativo. Tribunali e forze dell'ordine continuano a fare progressi in tutto il mondo contro i criminali informatici.

Paese e data	Descrizione
Regno Unito Aprile	L'unità e-Crime della Polizia Centrale ha arrestato tre uomini - un lituano, un lettone e un altro la cui nazionalità non è stata resa nota - per l'utilizzo del malware SpyEye per rubare dettagli per collegarsi al servizio di online banking[11].
Stati Uniti Aprile	Con l'Operazione Adeona il Dipartimento di Giustizia e l'FBI hanno chiuso la botnet Coreflood, che aveva infettato centinaia di migliaia di PC a partire dal 2002. Durante un periodo di 11 mesi, partito nel marzo 2009, le autorità hanno affermato che Coreflood ha dirottato circa 190 GB di password bancarie e altri dati sensibili da oltre 413.000 sistemi infetti nel momento in cui gli utenti navigavano in Internet[12].
Finlandia Maggio	La polizia ha arrestato 17 persone sospettate di aver preso parte a una frode bancaria online volta contro i titolari di conti Nordea all'inizio di quest'anno. I responsabili hanno cercato di rubare quasi 1,2 milioni di Euro tramite una serie di più di 100 transazioni fasulle[13]. La maggioranza dei sospetti sono sospettati di essere intermediari di phishing. I due sospettati essere le menti dell'operazione provenivano dall'Estonia.
Regno Unito Maggio	Uno studente dell'Università di Salford è stato condannato per una truffa basata su malware che gli ha consentito di intrufolarsi all'interno di computer e account webmail di 100 vittime stimate. La polizia ha chiesto a McAfee di analizzare il malware e ha riconosciuto il contributo di McAfee nel raccogliere le prove che hanno consentito di procedere a un rapido arresto[14].
Stati Uniti, Ucraina, Lettonia Giugno	Il Dipartimento di giustizia e l'FBI hanno annunciato l'Operazione Trident Tribunal, un'azione di forze di polizia internazionale coordinata che ha interrotto le attività di due cerchie di criminali informatici internazionali coinvolti nella vendita di software antivirus fasullo (scareware)[15]. Condotta con i servizi di sicurezza ucraini, l'azione sembra essere la prima a colpire una banda che utilizza Conficker[16]. La seconda azione di polizia era rivolta contro cittadini lettoni accusati di aver creato un'agenzia di pubblicità con scopi fraudolenti.
Russia Giugno	Una delle figure più controverse del mondo online in Russia, il cofondatore e CEO di ChronoPay Pavel Vrublevsky, è stato arrestato perché sospettato di aver ordinato un attacco DDoS (Distributed Denial of Service) contro un'azienda rivale. Vrublevsky, 32, è probabilmente meglio conosciuto come il comproprietario dell'inaffidabile programma di vendita di medicinali online Rx-Promotion. La sua azienda è stata inoltre ripetutamente coinvolta nell'elaborazione di carte di credito - e in molti casi nella creazione di aziende conto terzi - per truffe di scareware o programmi antivirus inaffidabili che utilizzano avvisi di sicurezza ingannevoli per i PC nel tentativo di spaventare le persone e spingerle a acquistare software di "sicurezza" senza valore[17].

Un assaggio di guerra informatica

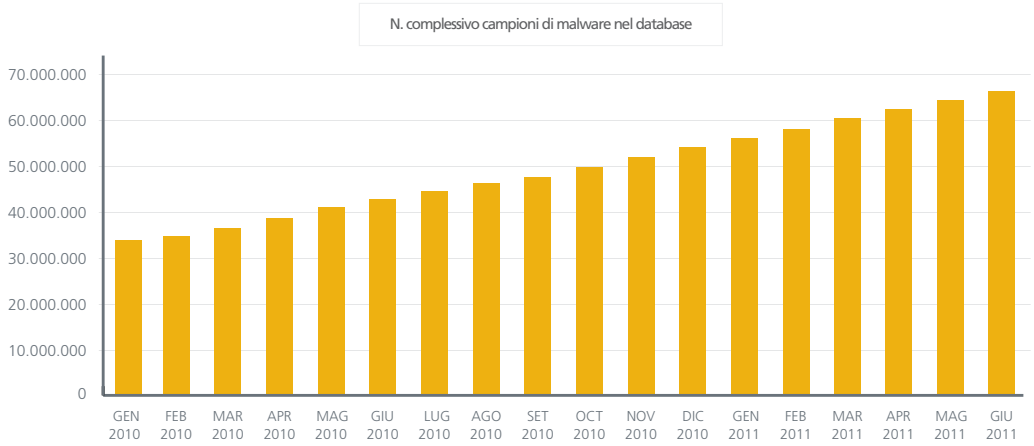
Il solo discutere della definizione di "guerra informatica" può far scattare un acceso dibattito, dal momento che un numero sempre maggiore di nazioni è alle prese con il tentativo di classificare questo conflitto in evoluzione. La discussione si farà ancor più confusa con la diffusione sempre più prevalente del fenomeno dell'hacktivism.

Paese e data	Descrizione
Russia Marzo/Aprile	Dal 24 marzo al 4 aprile sono stati lanciati vari attacchi DDoS contro alcuni blogger su LiveJournal, che ospita oltre 4,7 milioni di blogger russi (incluso il presidente Dmitry Medvedev) che si scambiano informazioni e spesso condividono punti di vista critici che non possono esprimere sulla stampa tradizionale[18].
Stati Uniti Aprile	L'Oak Ridge National Laboratory, che ospita uno dei supercomputer più potenti al mondo, è caduto vittima di un attacco cibernetico sofisticato lanciato attraverso e-mail di phishing inviate a circa 573 dipendenti del laboratorio. Sembra che alcuni di loro abbiano fatto clic su un link contenuto nell'e-mail e scaricato malware che si appropria di informazion[19].
Corea del sud Maggio	Le autorità sudcoreane hanno affermato che i servizi segreti della Corea del nord si sono introdotti illegamente nel sistema informatico della National Agricultural Cooperative Federation (Federazione cooperativa agricola nazionale) che offre servizi di fornitura, elaborazione, marketing e bancari a oltre 4.000 filiali[20].
Norvegia Maggio	Le forze armate norvegesi hanno ammesso di essere state colpite da un attacco cibernetico mirato potenzialmente grave nel mese di marzo. L'attacco si è verificato nel momento in cui 100 militari anziani hanno ricevuto un'e-mail con un allegato che sembrava arrivare da un'altra agenzia governativa[21].

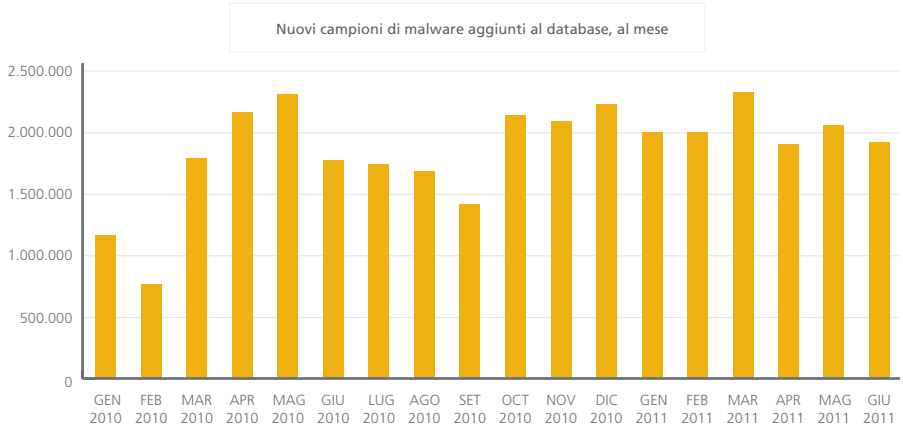
11. http://www.networkworld.com/news/2011/041111-uk-police-arrest-three-men.html
12. http://www.theregister.co.uk/2011/04/13/coreflood_botnet_takedown/
13. http://www.theregister.co.uk/2011/05/10/finnish_banking_trojan_investigation/
14. http://www.zdnet.co.uk/news/security-management/2011/05/18/gamer-sentenced-for-stealing-steam-passwords-40092802/
15. http://www.fbi.gov/news/stories/2011/june/cyber_062211/cyber_062211
16. http://www.zdnet.co.uk/news/security-management/2011/06/24/ukrainian-sting-targets-conficker-fraudsters-40093222/
17. http://krebsonsecurity.com/tag/pavel-vrublevsky/
18. http://uk.reuters.com/article/2011/04/06/oukin-uk-russia-medvedev-cyberattack-idUKTRE7354OV20110406
19. http://www.computerworlduk.com/news/security/3275613/us-government-energy-research-lab-shuts-down-email-and-internet-access-after-phishing-attack/
20. http://www.koreaittimes.com/story/14507/north-korea-behind-cyber-attack-south-korea-bank
21. http://www.cio.com.au/article/387581/norwegian_military_admits_march_cyberattack

Minacce malware

In questo trimestre il panorama del malware ha riservato diverse sorprese. Sebbene in termini numerici non sia stato il periodo più trafficato della storia (solo di poco inferiore al ritmo dello scorso anno), se combinato con il primo trimestre ci troviamo di fronte al primo semestre più animato nella storia per questo vettore. L'aumento corrisponde al 22% rispetto al 2010! McAfee Labs ha identificato quasi sei milioni di campioni di malware unico durante questo trimestre. Questo ci mette sula strada giusta perché la nostra collezione cumulativa dello "zoo" di malware raggiunga i 75 milioni di campioni entro la fine dell'anno.

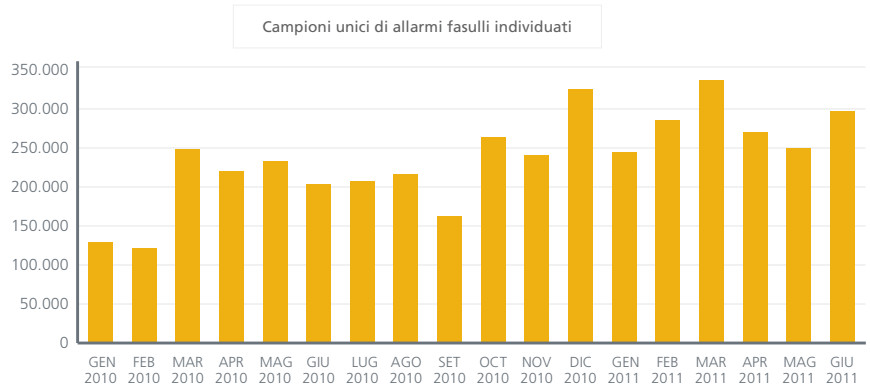


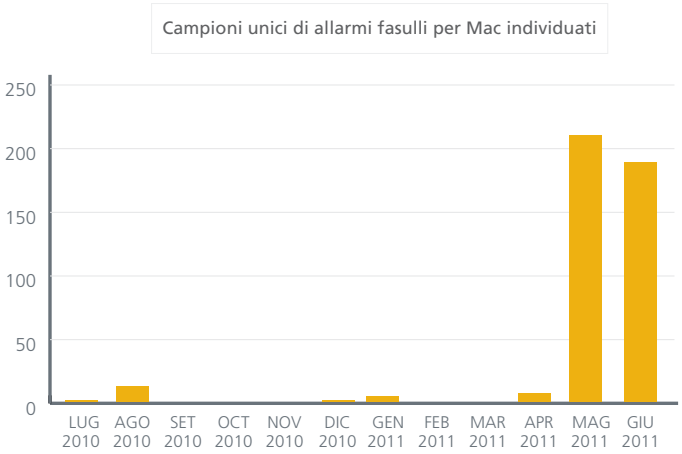
Giusto per sottolineare quanto sia stata significativa la crescita durante gli ultimi anni, diamo uno sguardo alla crescita incrementale mensile di codici binari malware unici:



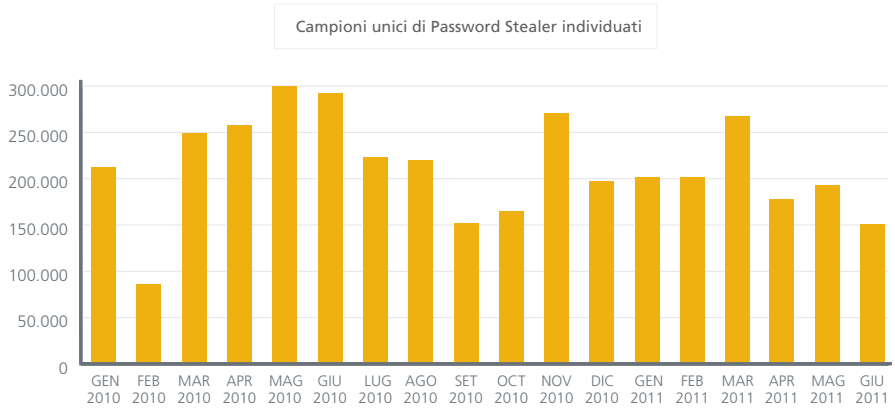
Ad oggi raccogliamo in media quasi due milioni di nuovi campioni ogni mese. Non si tratta certo di uno sviluppo gradito, ma è coerente e prevedibile considerato come le nostre vite lavorative e private sono oggi legate alla tecnologia.

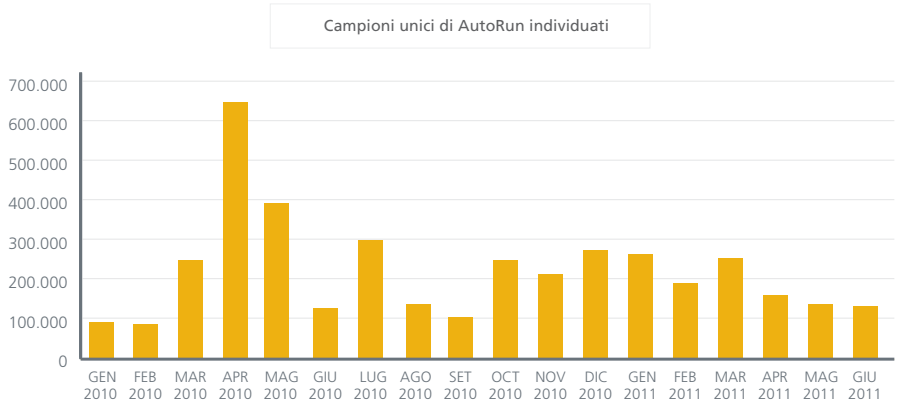
Tra le famigie specifiche di cui seguiamo i movimenti, il software antivirus contraffatto (noto anche come software antivirus inaffidabile o allarmi fasulli) continua a mostrare una crescita costante e ha iniziato anche ad approcciare una nuova piattaforma: i computer Mac. È proprio così: gli antivirus contraffatti per la piattaforma Apple sono oggi una realtà. Questo non sorprende nessuno di noi di McAfee Labs. Oggi ci sono più utenti Mac di quanto sia mai stato ed è in aumento anche la presenza in ambito aziendale. Questo mette le piattaforme Apple esattamente nel mirino degli autori di malware. Sarà interessante vedere se questa tipologia di malware si diffonderà anche su iPhone e iPad. Probabilmente, è più una questione di "quando" piuttosto che di "se".

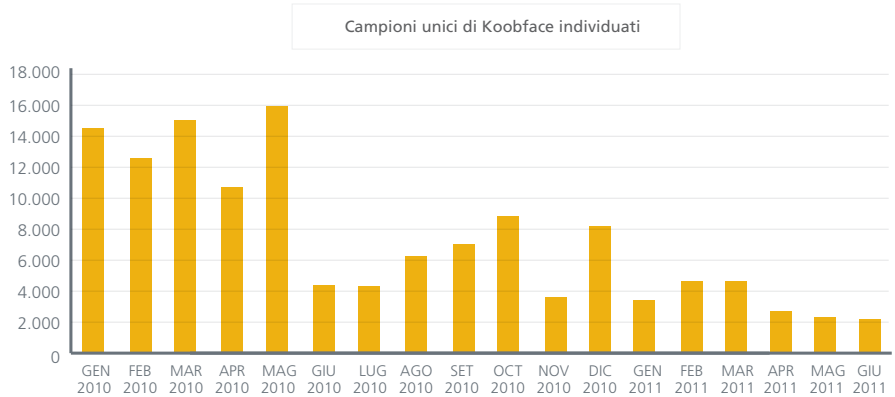




In questo trimestre, i Trojan password-stealing generici sono leggermente calati, mentre il malware ad esecuzione automatica è diminuito in modo significativo. Le minacce Koobface sono scese ai livelli più bassi degli ultimi anni.

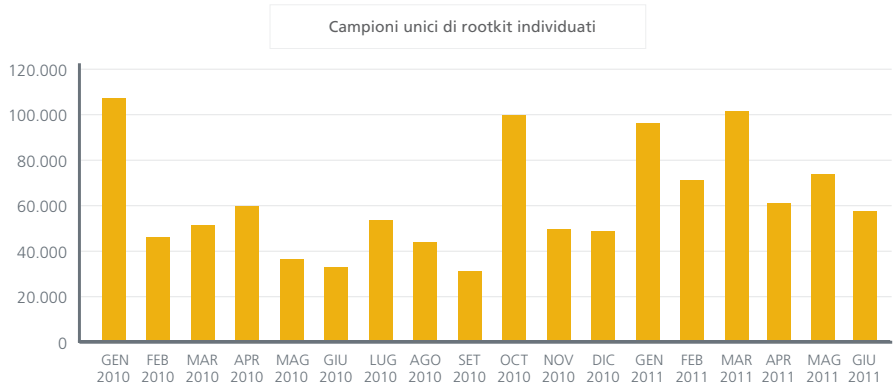






Rootkit e malware stealth

Un'altra categoria di malware che dimostra una crescita progressiva recente è quella dei rootkit. Un rootkit (alcune volte definito malware stealth) è un codice che nasconde i propri elementi dal sistema operativo e dai software di sicurezza. I criminali informatici utilizzano i rootkit per rendere più furtivo e persistente altro malware. Meglio è nascosto il malware, più a lungo permarrà sul sistema e porterà avanti la sua attività dannosa. Come si può evincere dai diagrammi seguenti, i rootkit stanno vivendo una crescita complessiva. La prima metà del 2011 è comparabile al malware nel suo complesso: i rootkit hanno vissuto il loro semestre più attivo, in aumento di quasi il 38% rispetto al 2010! Due tra i rootkit più impegnati in cui ci siamo imbattuti sono Koutodoor e TDSS. Entrambi sono terribili e nascondo malware per impossessarsi di dati.



I numeri globali dei computer infetti

A livello globale e per area geografica singola buona parte del malware che abbiamo acquisito in questo trimestre corrisponde alle stesse varietà del primo trimestre. Abbiamo registrato poche differenze tra i continenti ma complessivamente sono risultati essere più simili che diversi.

Posizione	Top 5 globale del malware
1	Malware AutoRun (ad esecuzione automatica)
2	Adware OpenCandy
3	Malware Hotbar
4	Trojan generici
5	Adware HotBar vF

Posizione	Nord America
1	Malware AutoRun (ad esecuzione automatica)
2	Malware Hotbar
3	Adware OpenCandy
4	Malware Downloader
5	Adware HotBar vF

Posizione	Sud America
1	Malware AutoRun (ad esecuzione automatica)
2	Sfruttamento di Java Runtime
3	Malware AutoRun Conficker
4	Trojan di accesso remoto
5	Malware Downloader

Posizione	Europa e Medio Oriente
1	Adware HotBar vF
2	Malware AutoRun (ad esecuzione automatica)
3	Malware Hotbar
4	Adware OpenCandy
5	Malware AutoRun Conficker

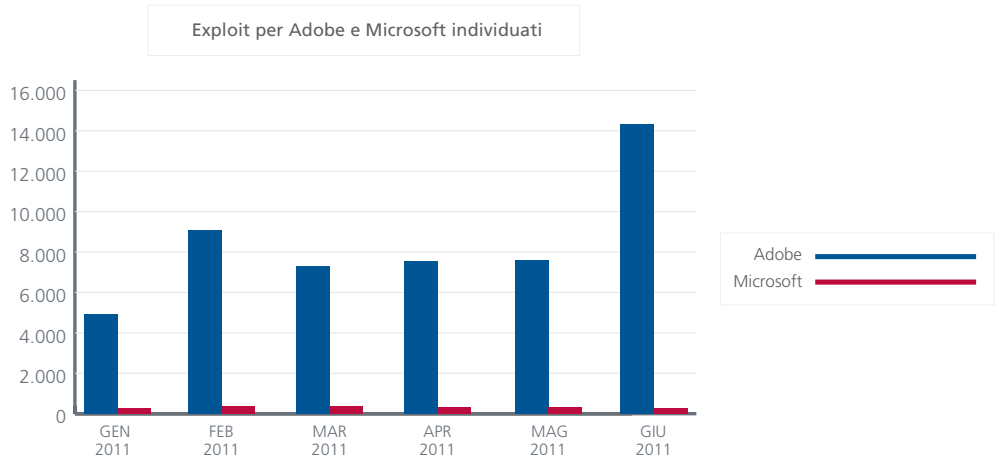
Posizione	Africa
1	Malware AutoRun (ad esecuzione automatica)
2	Malware Downloader
3	Malware Downloader
4	Malware Yahoo Messenger
5	Virus Sality

Posizione	Asia
1	Malware AutoRun (ad esecuzione automatica)
2	Malware Downloader
3	Malware AutoRun Conficker
4	Malware Downloader
5	Sfruttamento del browser

Posizione	Australia
1	Adware OpenCandy
2	Malware Downloader
3	Malware Hotbar
4	Malware Downloader
5	Malware AutoRun (ad esecuzione automatica)

Adobe attira più exploit di Microsoft

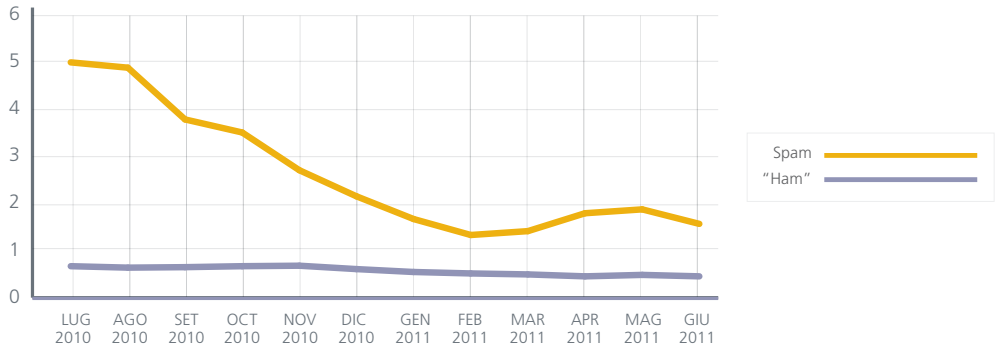
Per vari trimestri, uno dei trend principali cui abbiamo assistito è quello per cui gli autori di malware preferiscono scrivere exploit mirati alle vulnerabilità nei prodotti Adobe rispetto a quelle presenti nei prodotti Microsoft. Questo trend non dimostra che le tecnologie di Adobe siano più vulnerabili o abbiano più bug di codifica rispetto a quelle di Microsoft. Piuttosto, Adobe è uno dei leader indiscussi al mondo per quanto riguarda le applicazioni client, e questa posizione di leadership è proprio ciò che muove gli autori di malware e i criminali informatici: mirano a colpire ciò che è popolare e utilizzato diffusamente. Il diagramma seguente mostra il malware che tenta di sfruttare le vulnerabilità nei prodotti Adobe e Microsoft osservato da McAfee Labs in questo trimestre.



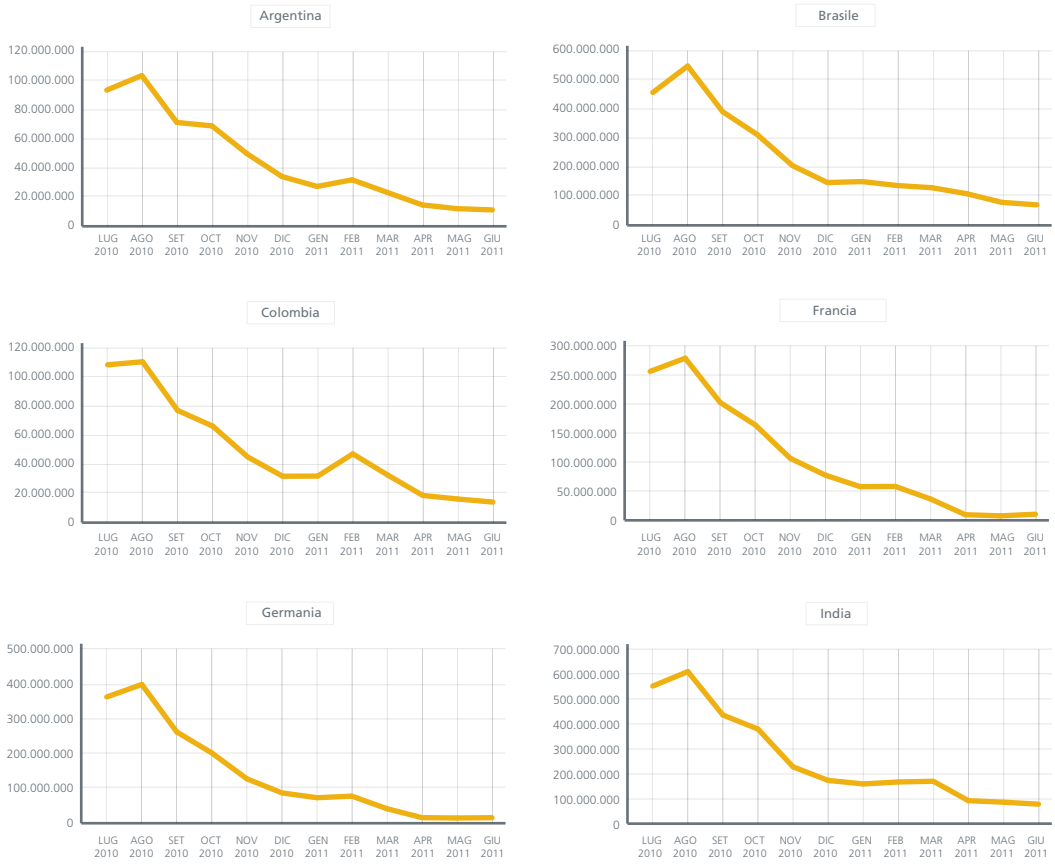
Minacce contro la messaggistica

Le minacce contro i programmi di messaggistica hanno continuato a declinare lievemente rispetto al trimestre precedente, sebbene il calo non sia significativo. Lo scorso trimestre, uno sforzo coordinato tra vari fornitori di sicurezza, forze di polizia e anche i CERT ha permesso di chiudere un gran numero di zombie di botnet e le loro strutture di comando. Questo recente successo potrebbe ancora avere un effetto positivo. Prevediamo di vedere ancora bruschi aumenti per quanto riguarda lo spam; allo stesso tempo, continuiamo a monitorare quest'area con attenzione. Sebbene il volume dello spam rimanga ai livelli storici più bassi, il fenomeno dello spearphishing (una categoria di spam) che osserviamo attualmente è più mirato e efficace che mai. Questo vettore continua a evolvere.

Volume complessivo dello spam, in trilioni di messaggi al giorno

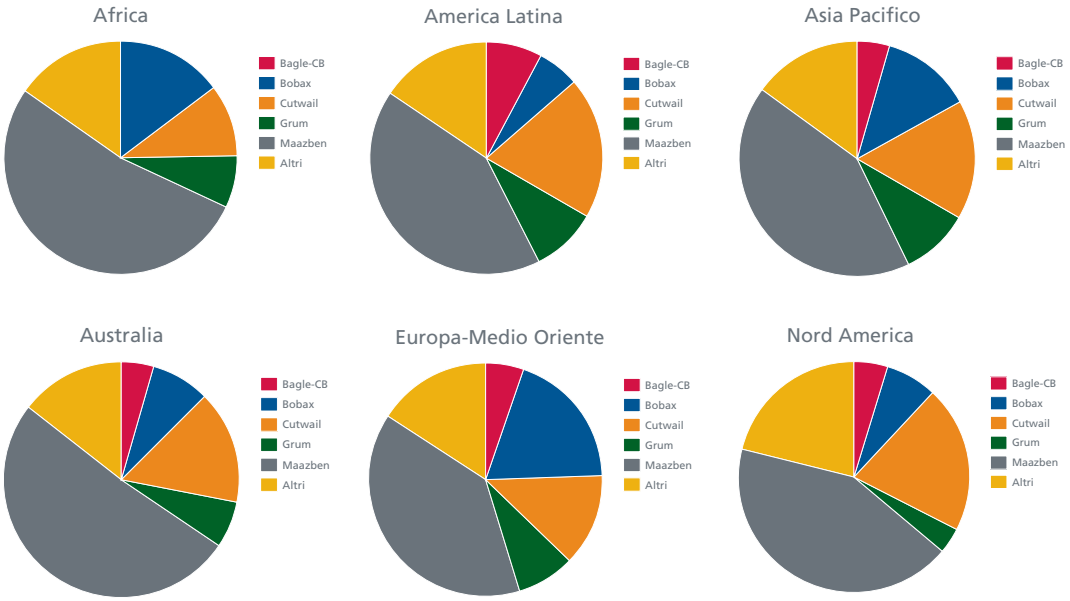


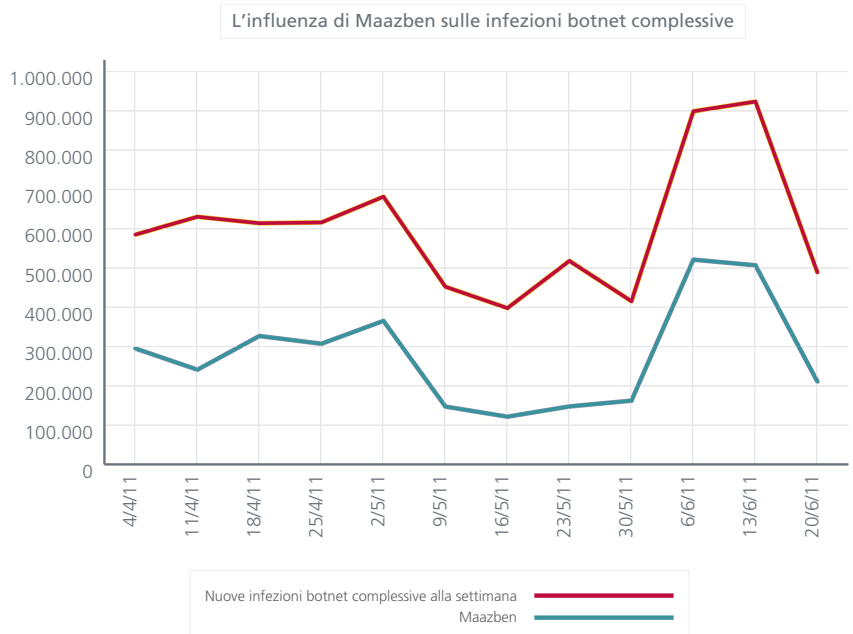
Volume dello spam per nazione

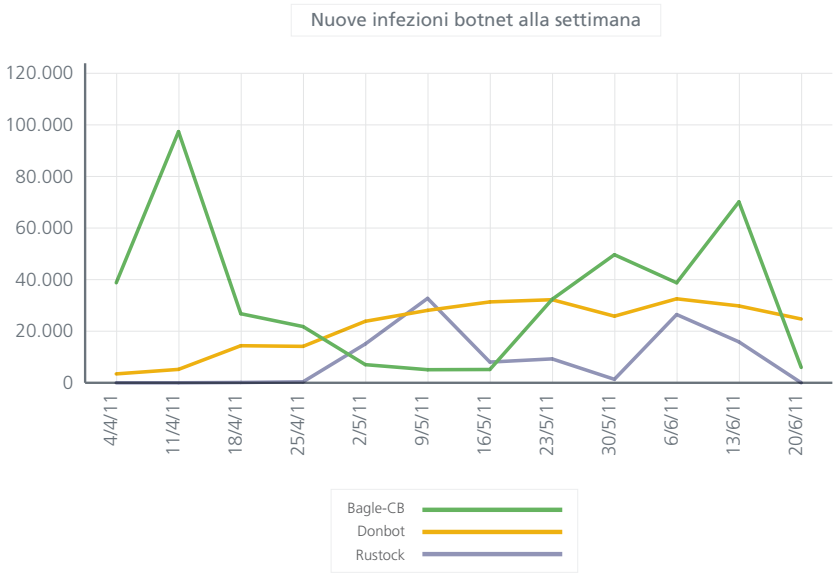


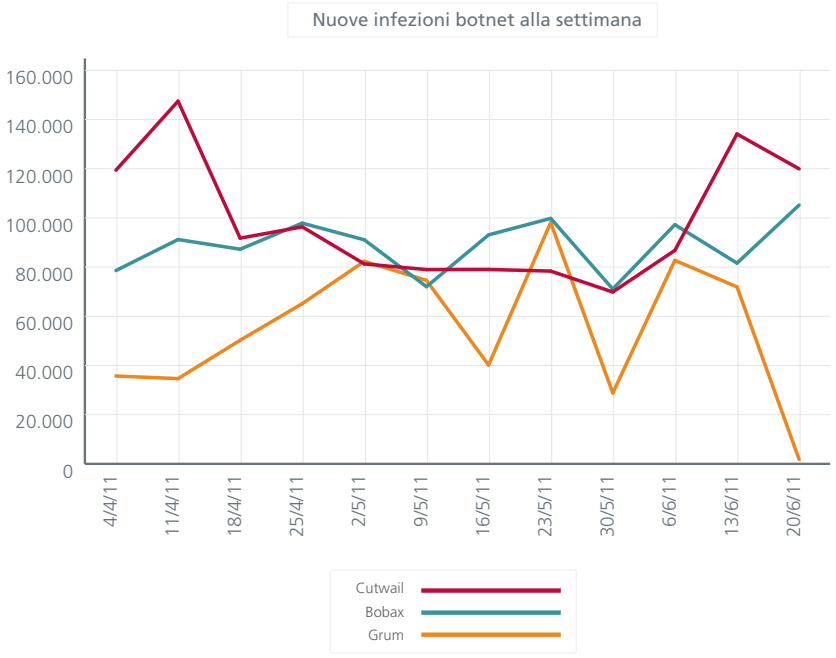

Volume dello spam per nazione
Italia
250.000.000
200.000.000
150.000.000
100.000.000
50.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Giappone
50.000.000
40.000.000
30.000.000
20.000.000
10.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Polonia
200.000.000
150.000.000
100.000.000
50.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Portogallo
100.000.000
80.000.000
60.000.000
40.000.000
20.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Russia
350.000.000
300.000.000
250.000.000
200.000.000
150.000.000
100.000.000
50.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Corea del sud
200.000.000
150.000.000
100.000.000
50.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Spagna
200.000.000
150.000.000
100.000.000
50.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Regno Unito
500.000.000
400.000.000
300.000.000
200.000.000
100.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Stati Uniti
1.500.000.000
1.200.000.000
900.000.000
600.000.000
300.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011
Venezuela
500.000.000
400.000.000
300.000.000
200.000.000
100.000.000
0
LUG 2010 AGO 2010 SET 2010 OCT 2010 NOV 2010 DIC 2010 GEN 2011 FEB 2011 MAR 2011 APR 2011 MAG 2011 GIU 2011

In questo trimestre, McAfee Labs ha assistito all'assottigliarsi costante delle botnet Rustock nonostante possano essere rianimate dai criminali informatici nel corso dei prossimi mesi. Nel frattempo, i responsabili delle botnet Maazben, Cutwail e Bobax hanno incrementato la propria attività. Di queste tre botnet dominanti, Maazben supera chiaramente tutti gli altri in termini di utilizzo e influenza a livello mondiale.

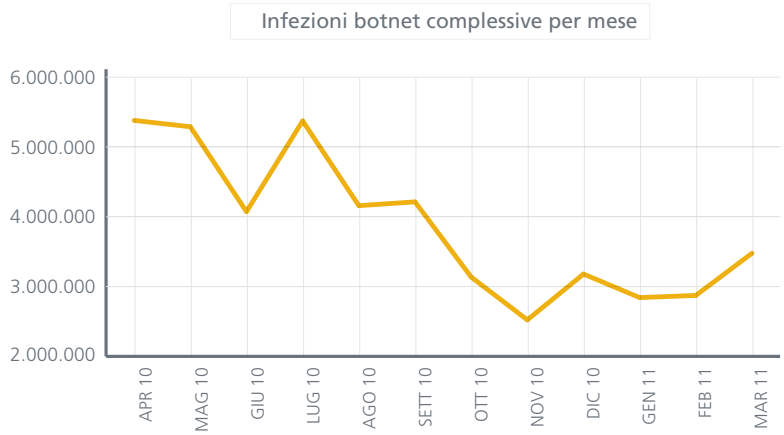




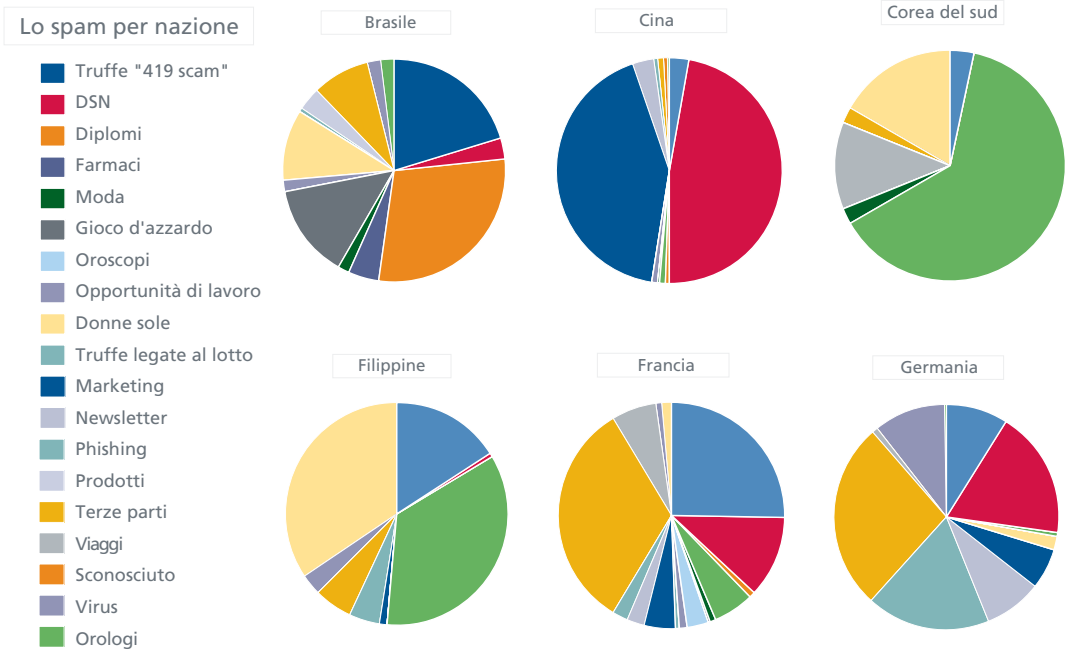

Nuove infezioni botnet alla settimana
120.000
100.000
80.000
60.000
40.000
20.000
0
4/4/11
11/4/11
18/4/11
25/4/11
2/5/11
9/5/11
16/5/11
23/5/11
30/5/11
6/6/11
13/6/11
20/6/11
Bagle-CB
Donbot
Rustock

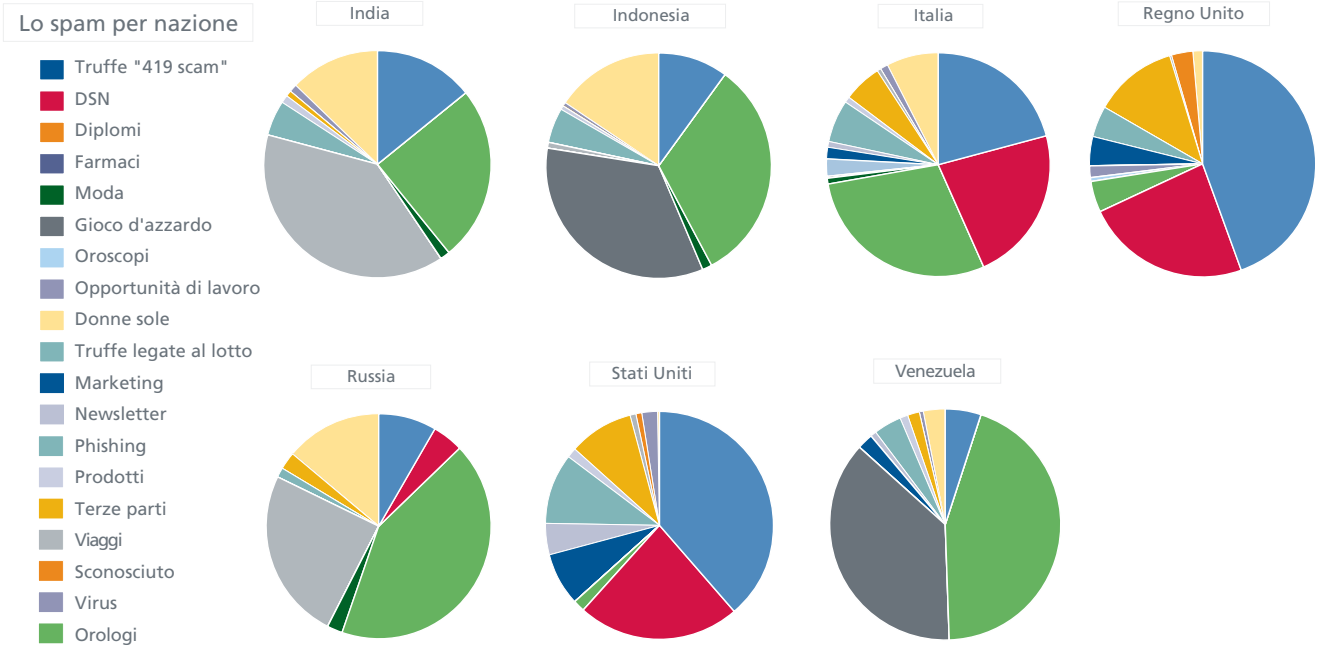

Nuove infezioni botnet alla settimana
160.000
140.000
120.000
100.000
80.000
60.000
40.000
20.000
0
4/4/11
11/4/11
18/4/11
25/4/11
2/5/11
9/5/11
16/5/11
23/5/11
30/5/11
6/6/11
13/6/11
20/6/11
Cutwail
Bobax
Grum

Si è verificata una crescita progressiva nelle infezioni da parte di botnet nel corso del trimestre. Si tratta di un'interessante giustapposizione se prendiamo in considerazione il calo dello spam a livello mondiale. Chiaramente l'utilizzo di botnet sta attraversando un momento di transizione. Data la crescita e gli obiettivi degli hacktivisti, prevediamo di assistere a alcuni cambiamenti importanti nel modo in cui vengono utilizzate le botnet.



Lo spam è allettante e gli argomenti utilizzati nell'oggetto (l'esca di social engineering utiizzata per rendere attraente il messaggio) continuano a essere diversi. Le truffe "Nigerian 419" sembrano essere un po' più diffuse in questo trimestre così come le truffe legate al lotto sono risultate prevalenti in molte parti del mondo, insieme agli argomenti spam di lunga data relativi a DSN (Database Source Name) fasulli e giochi d'azzardo. Le tecniche di social engineering che utilizzano esche in base alla dislocazione geografica proseguiranno di sicuro, dal momento che i truffatori sono ben coscienti delle diversità che caratterizzano il loro pubblico di riferimento globale.

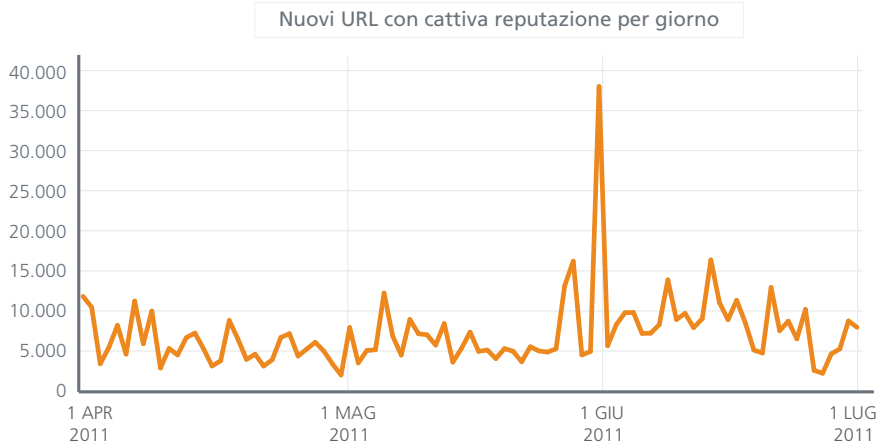




Minacce web

I siti web possono avere reputazioni pericolose o dannose per una varietà di motivi. Le reputazioni possono essere basate su domini completi e qualsiasi quantità di sotto-domini e su indirizzi IP o URL specifici. Le reputazioni nocive sono influenzate dal fatto di ospitare malware, programmi PUP o siti di phishing. Spesso osserviamo una combinazione di codice e funzionalità discutibili. Molti fattori contribuiscono alla valutazione della reputazione di un sito.

Lo scorso trimestre McAfee Labs ha registrato una media di 8.900 nuovi siti pericolosi al giorno; in questo periodo tale cifra è diminuita leggermente a 7.300 elementi, paragonabile allo stesso periodo dello scorso anno.

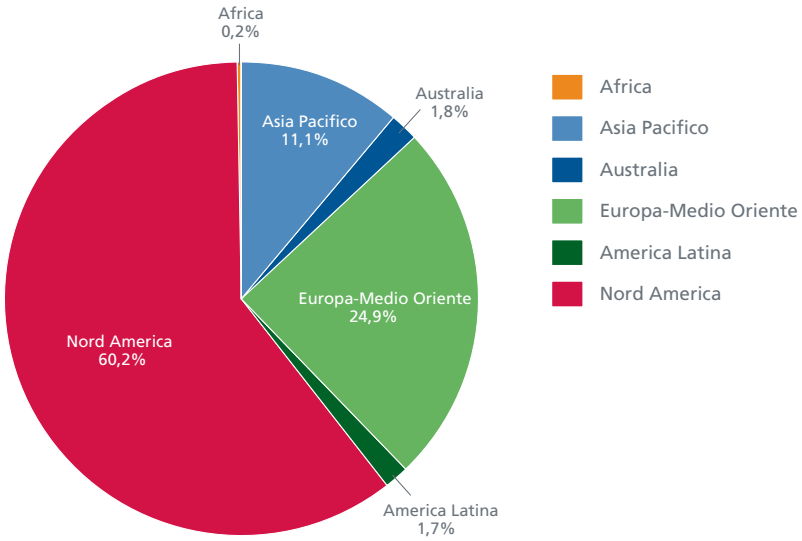


Abbiamo registrato alcuni picchi significativi nei contenuti web malevoli in questo trimestre. Molti di questi picchi corrispondevano a campagne nocive intensive.

Il 31 maggio, campagne di spam - una che promuove siti di incontri online con chat video e un'altra che informa i destinatari di false fatture in sospeso - hanno distribuito URL fraudolenti che ospitavano malware legato a Zeus (Generic FakeAlert.by e Generic PWS.y). Tra questi siti vi erano were undss-syria.org, baranava.com, emajic.net e sturtholdfastmarioncc.com.

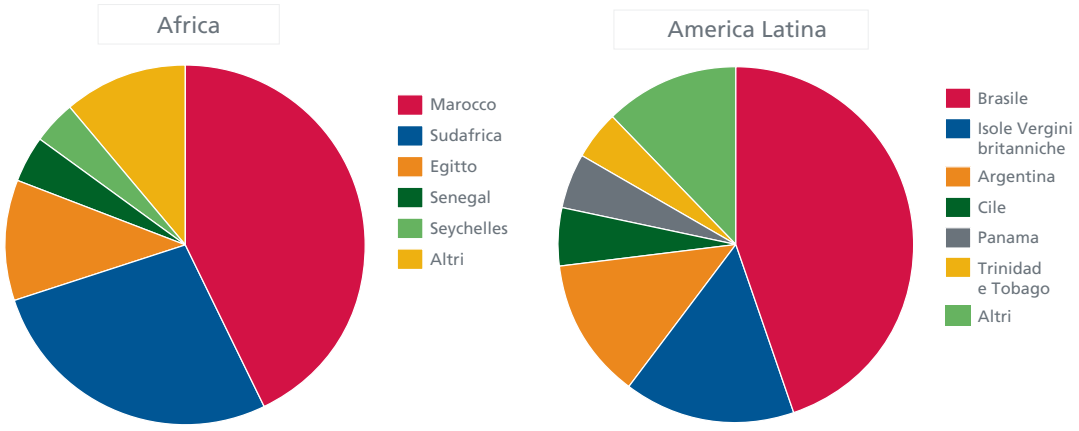
La maggior parte di questi nuovi siti malevoli è dislocata negli Stati Uniti, seguiti da Corea del sud, Olanda, Canada, Regno Unito, Cina e Germania.

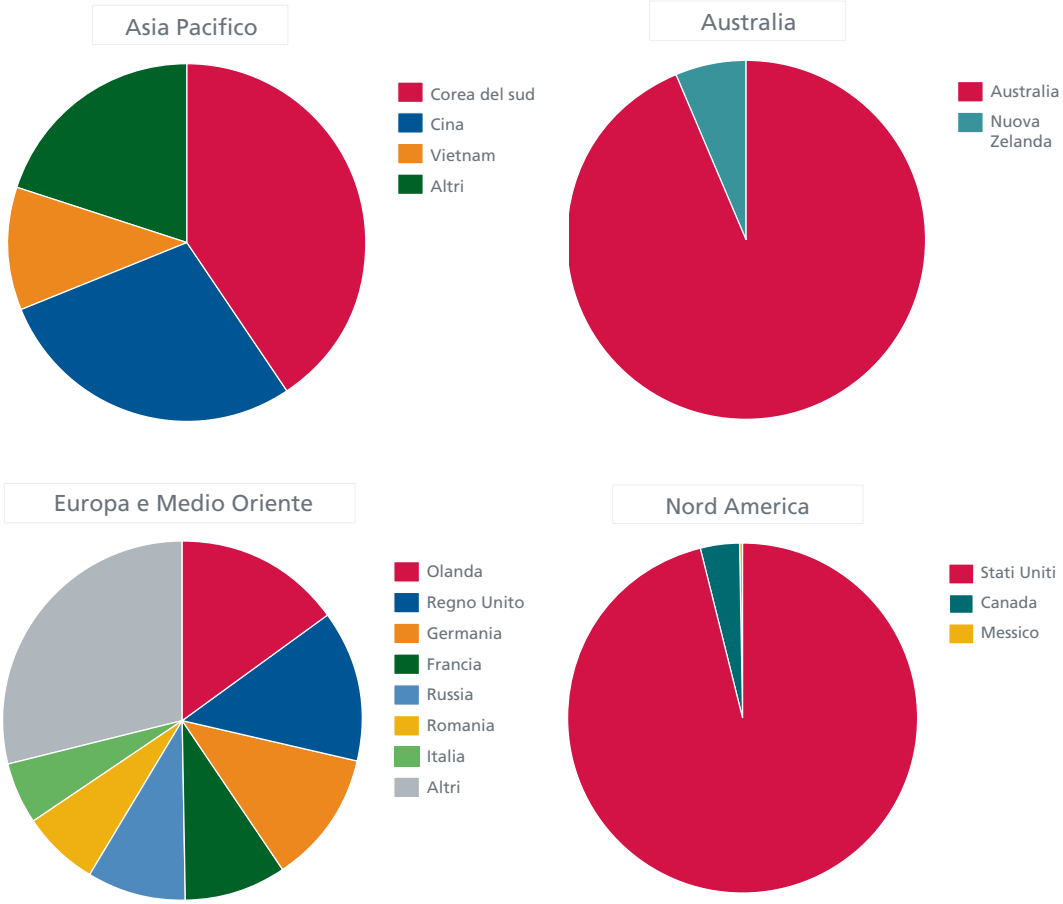
Nel primo trimestre le principali nazioni sono risultate essere Stati Uniti, Coread del sud, Germania e Cina. In questo trimestre, comunque, la situazione è piuttosto diversa. La nostra analisi regionale rivela dove risiedono i server più pericolosi:



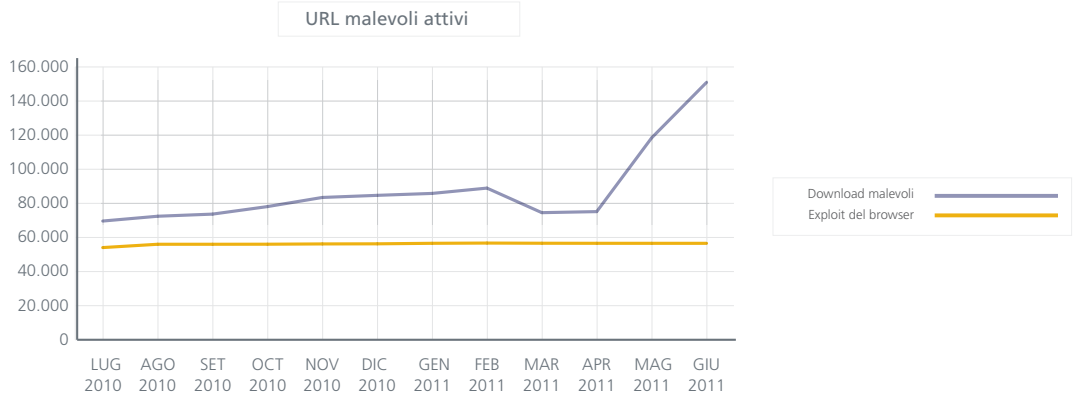
Il Nord America, principalmente gli Stati Uniti, domina ancora, ma la cifra per la regione che riunisce Europa, Medio Oriente e Africa è aumentata al 25% rispetto al 18% nel primo trimestre.

Analizziamo alcune regioni più in dettaglio:





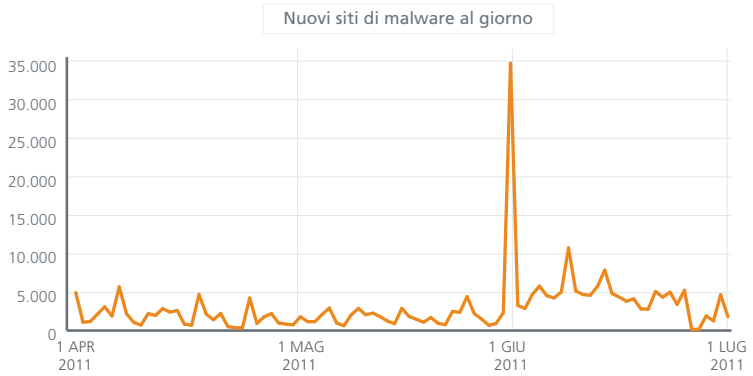
In questo trimestre, il numero di siti web che ospita download dannosi è aumentato ancora, mentre la quantità di siti che ospitano exploit browser è rimasta invariata:



In questo trimestre abbiamo anche osservato un costante aumento di blog e wiki con reputazioni malevole.

Siti web che distribuiscono malware e PUP

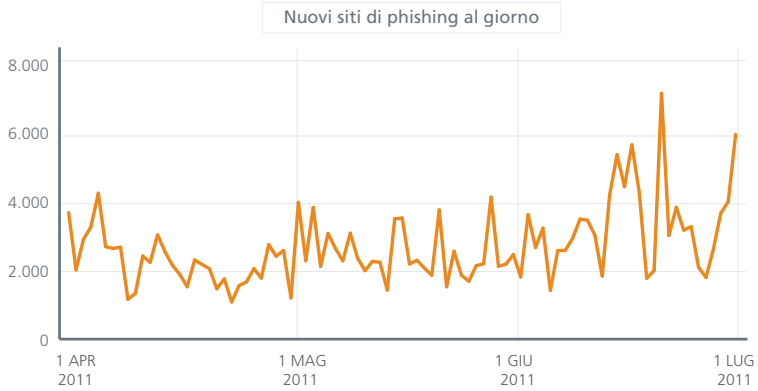
La tabella seguente offre un quadro del numero di siti web che rilasciano malware e programmi indesiderati (PUP) che sono stati rilevati in questo trimestre da McAfee Labs.



Abbiamo osservato un leggero aumento in questo trimestre con circa 3.000 nuovi siti al giorno rispetto ai 2.700 al giorno del primo trimestre.

Siti di phishing

Questo trimestre abbiamo identificato circa 2.700 URL di phishing al giorno, in lieve aumento rispetto ai 2.500 al giorno dello scorso trimestre.



Informazioni sugli autori

Questo report è stato preparato e redatto da Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, François Paget, Craig Schmugar, Jimmy Shah e Adam Wosotowsky di McAfee Labs.

Informazioni su McAfee Labs

McAfee Labs è il gruppo di ricerca globale di McAfee. Con l'unica organizzazione di ricerca focalizzata su tutti i vettori di minaccia, ovvero malware, web, e-mail, rete e vulnerabilità, McAfee Labs raccoglie l'intelligence dai propri milioni di sensori e dal suo servizio McAfee Global Threat Intelligence™ basato su cloud. I 350 ricercatori pluridisciplinari di McAfee Labs in 30 nazioni seguono la gamma completa di minacce in tempo reale, identificando le vulnerabilità delle applicazioni, analizzando e correlando i rischi e attivando rimedi immediati per proteggere aziende e consumatori.

Informazioni su McAfee

McAfee, società interamente controllata da Intel Corporation (NASDAQ:INTC), è la principale azienda focalizzata sulle tecnologie di sicurezza. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di collegarsi a Internet, navigare ed effettuare acquisti sul web in modo sicuro. Supportata dal suo ineguagliato servizio di Global Threat intelligence, McAfee crea prodotti innovativi destinati a utenti consumer, aziende, pubblica amministrazione e service provider che necessitano di conformarsi alle normative, proteggere i dati, prevenire le interruzioni dell'attività, individuare le vulnerabilità e monitorare e migliorare costantemente la propria sicurezza. McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti.
www.mcafee.com/it

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

32000rpt_quarterly-threat-q2_0711_ETMG