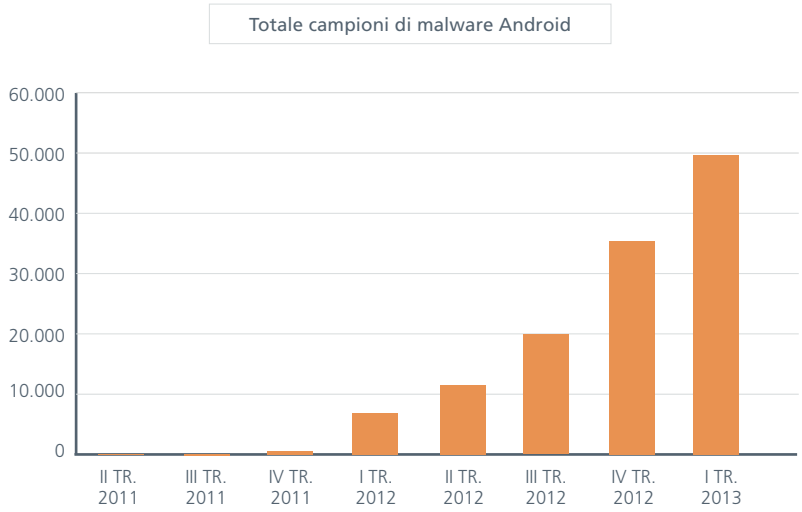
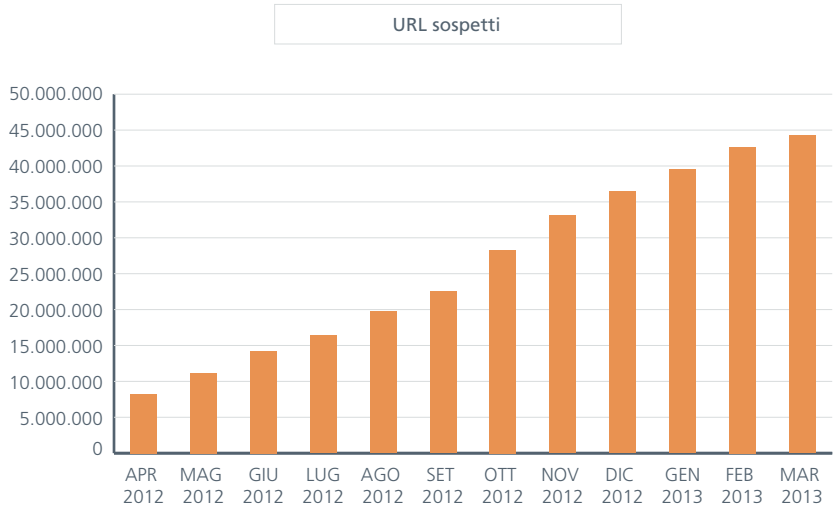
Nel primo trimestre del 2013 la comunità globale del crimine informatico ha effettuato un "Ritorno al Futuro" nella propria incessante ricerca di vittime e guadagni. Molte delle tendenze più significative osservate da McAfee Labs nei tre trimestri precedenti sono in realtà andate scemando, mentre tipologie più obsolete di attacchi e ciò che può solo essere definito "retro-malware" hanno mostrato una nuova crescita importante.

Alcuni esempi di tendenze di minacce precedenti che si sono placate nel corso del primo trimestre 2013 includono:

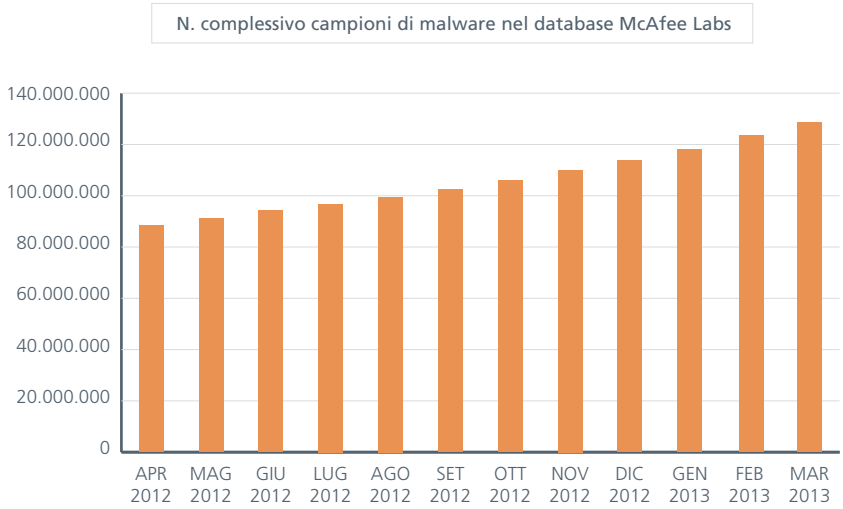
Rallentamento nella comparsa di nuovo malware (Android) mobile. Sebbene il conteggio assoluto dei nuovi campioni di malware Android sia salito del 40%, ciò rappresenta un calo di solo il 10% del tasso di crescita rispetto al quarto trimestre del 2012.



Analogamente, il numero di URL web malevoli rilevati è cresciuto del 12% nel primo trimestre, ma il tasso di crescita, che era superiore dell'80% nel quarto trimestre, è sceso di circa 40 punti percentuali.



Anche la crescita dei campioni di malware noto è scesa un poco nel primo trimestre - al 28% - rispetto al 38% nel quarto trimestre 2012. Nel primo trimestre, McAfee Labs ha aggiunto oltre 14 milioni di nuovi campioni di malware al proprio "Zoo".



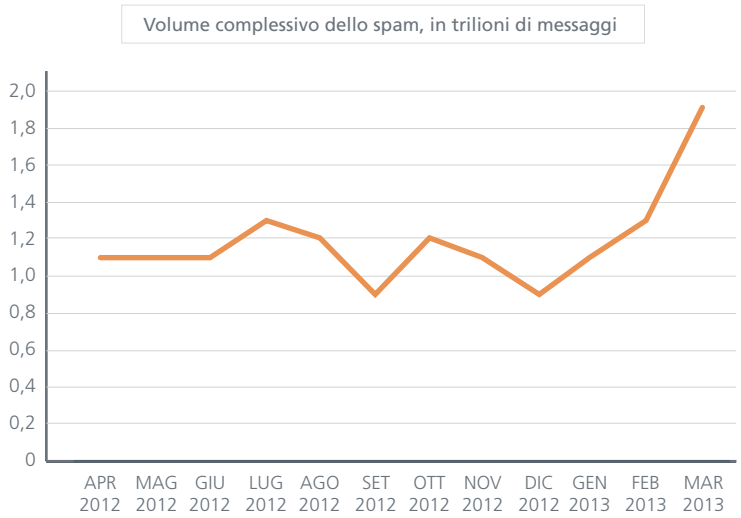
Infine, il tasso di crescita nel volume assoluto di password stealer, ransomware, antivirus fasulli e rootkit scoperti è stato relativamente stabile nel primo trimestre. Tutte queste minacce continuano ad aumentare in numero assoluto, sebbene i loro tassi di crescita siano scesi moderatamente.

Questi tassi di crescita rallentati, tuttavia, non significano che il ciberspazio stia diventando più sicuro. Al contrario, quando combinati con altre tendenze che abbiamo osservato nel primo trimestre, sembrerebbe che la comunità dei criminali informatici stia diventando più furba e disciplinata dal momento che sviluppa una preferenza per gli attacchi mirati volti a colpire comunità o aree geografiche specifiche. Come tutte le aziende, le associazioni del crimine informatico desiderano ottimizzare la loro efficienza e i loro guadagni. La tendenza osservata verso gli attacchi mirati sembrerebbe indicare che il panorama globale delle minacce stia andando verso una nuova e pericolosa direzione.

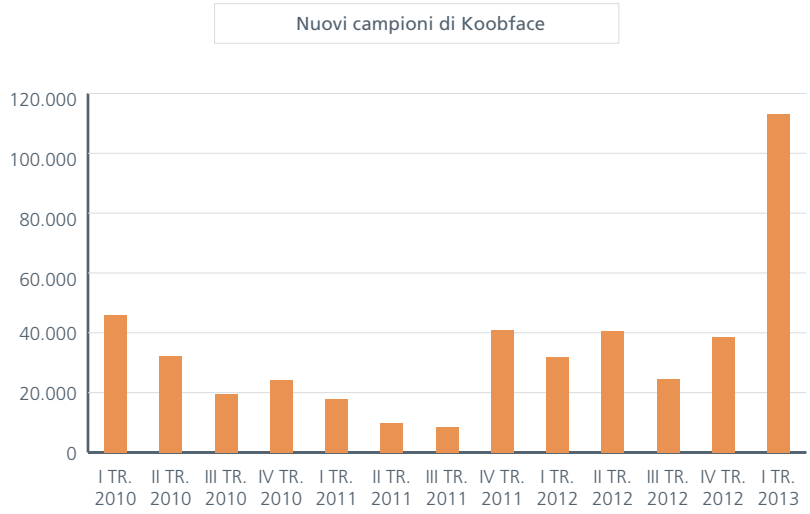
Un importante esempio di questa tendenza agli attacchi mirati è il trojan Citadel. Originariamente progettato per sottrarre valuta da banche specifiche, Citadel è stato "aggiornato" in modo che ora possa essere utilizzato per estrarre informazioni personali dalle vittime prese di mira dall'aggressore.

Altre tendenze delle minacce nel primo trimestre che riportano indietro nel tempo, ma vengono ora distribuite in attacchi mirati e più pericolosi, includono le seguenti:

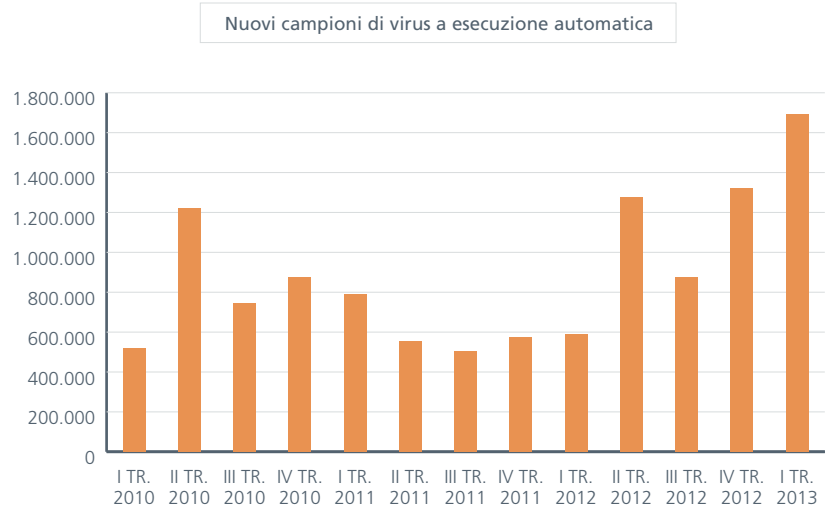
McAfee Labs ha rilevato il primo aumento nel volume globale dello spam in più di tre anni. E non si è trattato di una rinascita contenuta, poiché il volume complessivo dello spam è quasi raddoppiato nel primo trimestre 2013. Tuttavia, il numero complessivo è un po' fuorviante poiché McAfee Labs ha osservato differenze significative nella crescita dello spam a livello regionale. Ancora una volta, gli aggressori sembrano prendere di mira regioni specifiche con truffe specifiche nella speranza di frodare nuove vittime. Tra le truffe più popolari nel primo trimestre vi è un ritorno delle truffe azionarie pump-and-dump e offerte di un farmaco per una presunta crescita ormonale.



I rilevamenti di Koobface, un worm rilevato la prima volta nel 2008, sono stati relativamente stabili nell'ultimo anno ma *sono triplicati* nel primo trimestre del 2013 a livelli mai osservati prima. La comunità dei criminali informatici ritiene ovviamente che gli utenti dei social media rappresentino un ambiente ricco di potenziali vittime.



L'altra retro-minaccia che è aumentata nel primo trimestre è relativa ai campioni di malware ad esecuzione automatica. Per tradizione, i worm ad esecuzione automatica venivano distribuiti tramite chiavette USB o CD. Sono particolarmente utili ai criminali informatici perché i worm ad esecuzione automatica possono essere utilizzati per installare backdoor o password stealer sulle macchine infette. Il picco nei rilevamenti di minacce a esecuzione automatica sembra essere guidato dalla popolarità dei servizi di file sharing basati su cloud.



Oltre a questi attacchi da "Ritorno al Futuro", McAfee Labs ha osservato un aumento significativo relativamente alla nuova tecnica di attacchi "storage stack". Comunemente noti come attacchi del record di avvio principale (Master Boot Record - MBR), il loro obiettivo è di infettare il sistema di storage del computer e da lì assumere il controllo dell'intero dispositivo. La comparsa dei campioni MBR è salita di oltre il 30% nel primo trimestre.

Queste tendenze che significato nel momento in cui le aziende cercano di ottimizzare lo stato della loro sicurezza? Per quanto riguarda la protezione degli endpoint, quest'evoluzione del panorama delle minacce richiede l'utilizzo di protezioni multi-livello che includono non solo antivirus di base, ma anche sistemi di prevenzione delle intrusioni e filtraggio web. Dato il crescente aumento nell'utilizzo dei siti web infetti per distribuire malware, queste ultime due funzioni sono più importanti che mai. In alcuni ambienti, può essere necessaria l'aggiunta di strumenti di sicurezza per i dispositivi e il controllo delle applicazioni per garantire la protezione di informazioni fondamentali che risiedono sui dispositivi dell'utente.

Oltre alla protezione multi-livello per gli endpoint, è necessario fornire agli amministratori di sicurezza strumenti di reazione e reportistica più funzionali. Questo mutevole "cruscotto di sicurezza" sarà sempre più importante per consentire ai professionisti di rispondere rapidamente ed efficacemente ai nuovi attacchi mirati emergenti.

La protezione dell'infrastruttura richiederà inoltre un approccio multi-livello che affronti minacce web, e-mail e di rete. Il modo migliore per proteggersi contro le muove minacce è bloccarle prima che entrino nell'infrastruttura dell'azienda. Ma, oltre ai piani di protezione perimetrale standard, il crescente utilizzo di servizi cloud richiede che lo stato di sicurezza dell'azienda sia esteso al cloud e implementato in modo coerente indipendentemente da dove i dati e le applicazioni critiche vengono distribuite.

Una copia del report completo è disponibile all'indirizzo:
http://www.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2013.pdf.

McAfee
An Intel Company

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

60298exs_qtr-q1_0513_ETMG