Report

Report McAfee sulle minacce: primo trimestre 2009

McAfee® Avert® Labs

Indice dei contenuti

Lo spam: una preoccupazione a livello globale 3
Quale recessione? 3
Nuovi zombie alzano il volume della linea di produzione 4
Gli spammer non rispettano alcuna sovranità, inclusa la loro 6

Web: nuovi siti con reputazioni malevole fanno la loro comparsa quotidianamente 7
Attività degli anonymizer 11
Tendenze generali del web 11

Malware: la montatura di Conficker contro la realtà degli AutoRun 13

Aggiornamento delle previsioni 13
Feriti da fuoco amico 13
World Wide Web inaffidabile 14
Le minacce parlano la tua lingua 14

Blog McAfee Avert Labs 14
Google e l'abuso dei motori di ricerca 14
L'economia e la paura 15

I McAfee Avert Labs 15

Informazioni su McAfee, Inc. 15

Il *Report McAfee sulle minacce* fornisce le statistiche e le analisi più recenti relativamente alle minacce email e web. Questo report trimestrale è stato creato dai ricercatori di McAfee Avert Labs, il cui staff mondiale fornisce una prospettiva unica sul panorama delle minacce, indirizzate a consumatori e aziende, e relative agli Stati Uniti e a tutte le nazioni del mondo. Unisciti a noi in questa disamina delle principali problematiche di sicurezza degli ultimi tre mesi. Una volta finito di leggere, potrai trovare maggiori informazioni sul McAfee Threat Center: http://www.mcafee.com/us/threat_center/default.asp, o www.trustedsource.org.

Nel primo trimestre del 2009, abbiamo rilevato molti cambiamenti significativi nel panorama delle minacce rispetto all'anno precedente o addirittura a qualche mese fa. Nessuno avrebbe previsto 12 mesi fa che i volumi di spam sarebbero diminuiti, ma con la chiusura di McColo nel Novembre 2008, è esattamente ciò che si è verificato. I livelli di spam sono inferiori del 30% rispetto ai livelli di punta, e non abbiamo assistito a quell'aumento che storicamente si verifica nel mese di Marzo. Il punto non è *se* lo spam ritornerà ai livelli precedenti, piuttosto *quando* accadrà. Esistono dati relativi alla creazione di nuovi zombie e botnet che suggeriscono che non dovremo aspettare molto.

La creazione di siti web malevoli sta aumentando, così come i siti che ospitano il malware: sono infatti migliaia i nuovi siti che fanno la loro apparizione quotidianamente. Ogni giorno vengono create nuove forme di malware, e questo report dettaglia quelle che hanno raggiunto i livelli più elevati di diffusione.

Il worm Conficker, ufficialmente W32/Conficker.worm, ha ricevuto un elevato livello di attenzione rispetto ad altre minacce per la sicurezza nel recente passato. Questo report fornirà alcuni punti di vista per verificare se tale attenzione è solo una trovata pubblicitaria o una realtà. Ci focalizzeremo inoltre sulle minacce che non hanno ricevuto lo stesso livello di attenzione dai media, ma che potrebbero in concreto essere più pericolose della loro controparte più famosa.

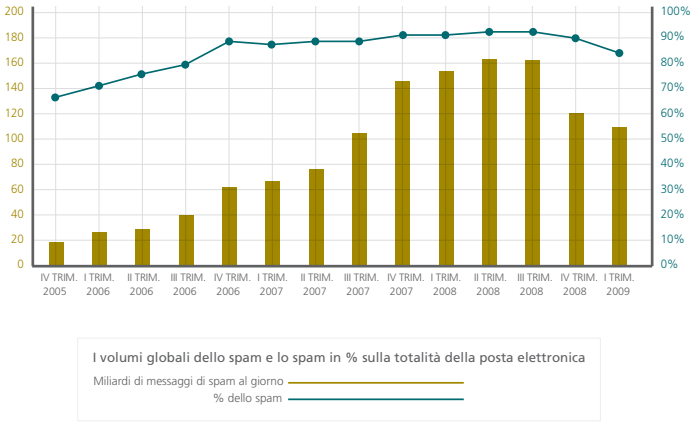
La geografia del panorama delle minacce è in costante evoluzione. Questo report analizza le principali aree geografiche in termini di minacce, inclusi dati quali l'origine dello spam, creazione di zombie e ubicazione del malware, e identifica i protagonisti emergenti nel business di creazione delle minacce. Il report offre inoltre alcuni dettagli interessanti che suggeriscono che le nazioni che creano le minacce non si preoccupano di utilizzarle contro entità all'interno dei loro confini.

Infine, punteremo i riflettori su noi stessi e analizzeremo alcune delle previsioni che avevamo effettuato nel nostro report *2009 Threat Predictions (Report sulle previsioni delle minacce nel 2009)* pubblicato in Gennaio, per verificare se e come si stanno concretizzando. Gli highlight includono l'utilizzo di eventi attuali e siti di social networking utilizzati per diffondere le minacce tra utenti ignari.

Lo spam: una preoccupazione a livello globale

Quale recessione?

I volumi complessivi di email e spam per il primo trimestre 2009 hanno raggiunto livelli mai visti almeno negli ultimi due anni. Anche gli spammer hanno seguito l'andamento del resto del mercato e sono entrati in una fase economica difficile? Non è questo il vero problema. Ciò che sta effettivamente accadendo è che i livelli di spam non si sono ancora ripresi appieno dalla chiusura di McColo, avvenuta lo scorso Novembre 2008. Rispetto allo stesso trimestre dello scorso anno, i volumi sono inferiori del 20% nel 2009 e del 30% rispetto al terzo trimestre del 2008, che aveva registrato i più elevati volumi trimestrali. I volumi di spam hanno recuperato del 70% da quando il "distributore" di spam è stato chiuso, ma non hanno ancora raggiunto i livelli precedenti.



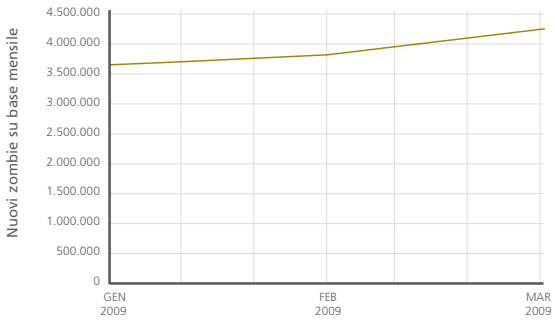
Il mese di Marzo negli anni recenti di solito registra volumi di spam record, ma questo Marzo siamo molto indietro. Lo scorso anno abbiamo registrato una media di 153 miliardi di messaggi al giorno, mentre questo Marzo la media si è attestata a circa 100 miliardi di messaggi al giorno.

Lo spam in termini percentuali sulla posta complessiva è diminuito al di sotto del 90%; non si raggiungeva tale livello dal 2006. Per l'intero 2008 lo spam ha rappresentato il 90% del volume complessivo della posta, mentre il trimestre più recente si è attestato all'86%. Sebbene gli account email e l'attività correlata variano enormemente, stimiamo che i singoli ricevono 6-12 email al giorno in meno rispetto allo scorso anno.

Prevediamo che i volumi di spam raggiungeranno ancora gli stessi livelli del 2008, ma la capacità degli spammer di riorganizzare i propri centri di comando e le botnet dopo la chiusura di McColo sta prendendo più tempo di quanto previsto dall'inizio. Fondamentalmente, per gli spammer questo è un problema di ritorno sull'investimento, come per ogni azienda.

Nuovi zombie alzano il volume della linea di produzione

In questo trimestre, abbiamo rilevato 12 milioni di nuovi indirizzi IP che operano come "zombie", ovvero computer controllati da spammer e altri. Si tratta di un aumento significativo rispetto ai livelli dello scorso trimestre del 2008, con un aumento di circa il 50%. Il terzo trimestre del 2008 ha inoltre registrato un numero record di nuovi zombie, ma è stato superato in questo trimestre di un milione. E sebbene i volumi di spam non abbiano ancora recuperato dalla chiusura di McColo, il livello di attività dei nuovi zombie indica che gli spammer stanno lavorando alacremente per recuperare l'infrastruttura persa, e che i volumi torneranno presto ai livelli precedenti.



Possiamo ripartire i sistemi infetti per nazione. Per il trimestre più recente il 63% dei nuovi zombie appartenevano alle principali dieci nazioni. Questa cifra rappresenta una lieve diminuzione rispetto ai due trimestri precedenti. Sembra che gli spammer raggiungano macchine in più nazioni per alimentare la propria attività.

I TRIM. 2009		IV TRIM. 2009		III TRIM. 2009	
Nazione	**Percentuale di IP**	**Nazione**	**Percentuale di IP**	**Nazione**	**Percentuale di IP**
Stati Uniti	18,0	Cina	15,8	Cina	20,4
Cina	13,4	Stati Uniti	15,4	Stati Uniti	16,5
Australia	6,3	Germania	6,5	Germania	6,8
Germania	5,3	Regno Unito	6,0	Regno Unito	6,0
Regno Unito	4,7	Brasile	4,9	Brasile	4,8
Brasile	4,0	Spagna	4,3	Spagna	3,7
India	3,1	Australia	4,1	India	2,5
Spagna	3,0	Italia	3,5	Russia	2,4
Corea del sud	2,8	Russia	3,1	Corea del sud	2,4
Russia	2,5	Corea del sud	2,4	Italia	2,2
Totale	**63,3**	**Totale**	**66,0**	**Totale**	**67,5**

Cina e Stati Uniti hanno lottato per il primo posto negli ultimi tre trimestri e hanno dominato per il numero di macchine zombie sotto il controllo degli spammer. Un famoso "traslocatore" è l'Australia, che non è riuscito a salire al primo posto nella top 10 nel terzo trimestre del 2008. Nel corso di due trimestri è schizzato al terzo posto, rappresentando il 6% di tutti i nuovi zombie. L'Australia sta dimostrando di essere terreno fertile per il reclutamento degli zombie.

I TRIM. 2009		IV TRIM. 2009	
Nazione	**% del totale**	**Nazione**	**% del totale**
Stati Uniti	35,0	Stati Uniti	34,3
Brasile	7,3	Brasile	6,5
India	6,9	Cina	4,8
Corea del sud	4,7	India	4,2
Cina	3,6	Russia	4,2
Russia	3,4	Turchia	3,8
Turchia	3,2	Corea del sud	3,7
Tailandia	2,1	Spagna	2,4
Romania	2,0	Regno Unito	2,3
Polonia	1,8	Colombia	2,0
	70,0		**68,3**

Lo spam suddiviso per nazione: gli Stati Uniti ancora una volta sono leader mondiali

Le case automobilistiche statunitensi avranno problemi di produzione e vendita, ma la produzione di spam proveniente dagli Stati Uniti continua ad essere al primo posto nel mondo, rappresentando il 35% della produzione di spam mondiale Sebbene le operazioni spam cosiddette "command-and-control" siano un'infrastruttura internazionale, gli spammer continuano a preferire l'utilizzo di computer negli Stati Uniti per produrre. Le dieci principali nazioni dominano nella produzione dello spam, contribuendo per il 70% del totale e distanziando notevolmente le altre oltre 200 nazioni nel mondo.

Analizzando gli ultimi due trimestri, l'India ha mostrato la crescita percentuale maggiore, contribuendo ora per circa il 7% dello spam complessivo. La loro produzione di spam è raddoppiata rispetto al trimestre precedente. Forse lo spam è l'ultima industria a cercare di fare qualcosa in outsourcing in India.

Fanno inoltre il loro ingresso nella top ten Tailandia, Romania e Polonia. Questi dati sostengono l'idea che gli spammer stiano cercando in lungo e in largo nuove fonti di energia per i loro motori spam

	I TRIM. 2009		IV TRIM. 2009		III TRIM. 2009
Farmaci da vendersi su ricetta medica	25,0	Farmaci da vendersi su ricetta medica	37,0	Viagra e simili	31,2
Pubblicità	21,9	Pubblicità	19,3	Pubblicità:	19,3
Prodotti contraffatti	18,8	Viagra e simili	16,8	Medicinali da vendersi su ricetta medica	10,7
Viagra e simili	17,5	DSN	9,5	Storm	8,0
DSN	7,1	Appuntamenti	3,9	DSN	7,7
Storm	1,6	Prodotti contraffatti	2,6	Ultime notizie	6,7
Diploma	1,1	Lavoro	1,7	Prodotti contraffatti	6,0
Software	1,1	Software	1,5	Prestiti	1,6
Prestiti	1,0	Prestiti	1,2	Attività bancaria	1,1
Altro	4,9	Altro	6,5	Altro	7,7
	100,0		**100,0**		**100,0**

Lo spam per tipo: sesso, droga e molto altro

Spam pubblicizzante viagra e simili, farmaci da vendersi su ricetta medica e pubblicità in generale continuano a mantenere i primi posti tra le tipologie di spam inviato. Questi tre tipi da soli rappresentano circa il 60% dello spam inviato durante gli ultimi tre trimestri. Sembra quasi che lo slogan "sesso, droga e rock'n'roll" sia ancora attuale attraverso lo spam. Bene, quasi. Forse siamo un po' cresciuti; oggi la frase potrebbe essere "sesso, droga ed economia".

Lo spam di prodotti contraffatti (principalmente orologi contraffatti) ha fatto un enorme salto questo trimestre, contribuendo per circa il 19% al totale dello spam. Questo tipo di spam di imitazioni contraffatte è stato piuttosto popolare lo scorso anno, ma ha dimostrato una crescita significativa anche questo trimestre. Ciò suggerisce che in momenti di crisi economica gli spammer ci aiutano a ampliare il nostro potere d'acquisto trovando alcune occasioni carine di imitazioni a buon mercato.

Lo spam di notifica dello stato di consegna continua a rappresentare circa l'8% dello spam totale. Questi messaggi sono quasi sempre associati ad attacchi di phishing e si verificano come una notifica legittima di email respinta dopo che l'email indirizzata della vittima è stata camuffata. Chiaramente il phishing è ancora vivo e vegeto. Molti di questi messaggi hanno fini finanziari e sono un tentativo di ottenere le informazioni personali di un individuo.

Gli spammer non rispettano alcuna sovranità, inclusa la loro

Esiste la leggenda nella comunità della sicurezza cibernetica che i criminali online, un numero significativo dei quali si pensa risiedano nell'Europa dell'Est, preferiscano concentrarsi su obiettivi nell'Europa occidentale e evitino di attaccare persone o aziende all'interno della loro giurisdizione. Stiamo iniziando a raccogliere dati che smentiscono tale leggenda. Internet non conosce confini geografici. Ora è evidente che i cibercriminali attaccheranno qualsiasi possibile obiettivo possano trovare. Abbiamo prove che i truffatori cibernetici hanno compromesso gravemente alcune delle principali agenzie governative e aziende Russe e dell'Europa dell'Est, oltre a importanti funzionari di tali entità.

McAfee TrustedSource™ ha recentemente rilevato email e spam carichi di malware provenienti da una serie di agenzie governative e istituzioni bancarie in Russia. Secondo la nostra analisi, le banche compromesse in Russia includono:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

I nostri dati suggeriscono inoltre che sistemi informatici nei seguenti uffici governativi russi sono controllati da gang di criminali cibernetici:

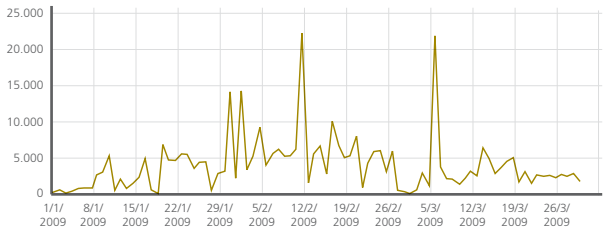
- Ministero delle Tasse, regione del Nazran
- La rete internet dello Stato Russo
- L'Istituto Regionale delle Finanze e dell'Economia
- L'Istituto Comune per la Ricerca Nucleare
- Il Centro Medico del Dipartimento del Presidente della Federazione Russa
- Il Fondo Pensione della Federazione Russa
- La Rete Personale della Giustizia della Federazione Russa
- Comunicazioni Cellulari Cecene JSC

Questi dati relativi alla Russia indicano che i criminali online non fanno assolutamente distinzioni tra i loro obiettivi e che attaccheranno qualsiasi organizzazione di interesse finanziario o altro per loro. Sebbene la Russia chiaramente sia in testa a questo tipo di attività (e il valore assoluto dello spam prodotto), la nostra analisi mostra lo stesso tipo di attività in altre nazioni dell'ex Unione Sovietica, tra cui Ucraina, Bielorussia, Armenia, Azerbaigian, Georgia, Kazakistan, Kirghizistan, Moldavia, Tajikistan, Turkmenistan e Uzbekistan.

Web: nuovi siti con reputazioni malevole fanno la loro comparsa quotidianamente

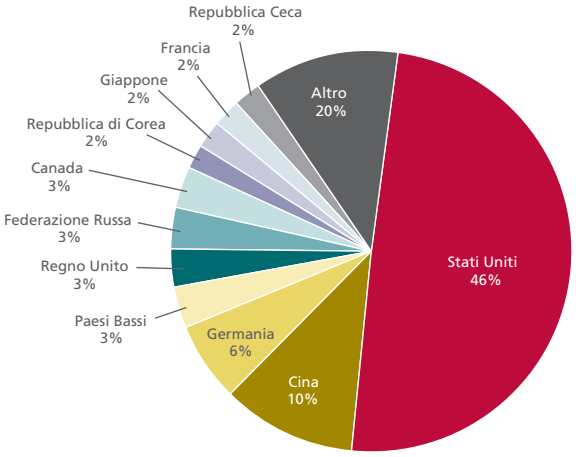
Nel corso di questo trimestre abbiamo visto proseguire molte delle minacce che si erano presentate nell'ultimo trimestre del 2008, ma con una maggiore intensità. Sebbene la maggior parte del battage pubblicitario e dell'attenzione dei media si sia concentrata su Conficker, questa non è stata assolutamente l'unica minaccia molto diffusa in questo trimestre. Anche se non consideriamo l'attività di Conficker, continuiamo a vedere un leggero aumento nell'attività anno su anno e un incremente netto rispetto ai trimestri precedenti. Quello delle applicazioni antivirus inaffidabili o "rogue" è stato un problema che ha causato preoccupazione sul web oltre a un aumento delle truffe e dell'attività di phishing.

I domini malevoli che Conficker contattava non sono inclusi in alcuna delle tabelle o dei dati presenti in questa sezione, tranne che all'interno della tabella "Distribuzione dei siti web con reputazioni malevole". Sebbene i dati di Conficker rappresentino una parte importante per inquadrare le minacce, stemperano la storia complessiva dell'attività maligna. Esistono molte altre minacce che sono sempre più diffuse. Gli autori di malware e i truffatori stanno traendo vantaggio dalla situazione economica e dalle nostre preoccupazioni per spingere una varietà di siti di truffe. Le loro tecniche di adescamento includono come evitare il pignoramento dei mutui e i siti di phishing su qualunque cosa possibile; offrono inoltre tessere fedeltà di negozi. Siti di antivirus "rogue" continuano a sfruttare utenti ignari. E i metodi per attirare utenti sui siti web continuano a evolvere. Anche non tenendo conto di tutta l'attività di Conficker, gli URL che superano il limite verso livelli di reputazione "malevola" (o “rosso”) sono aumentati sensibilmente rispetto agli ultimi due trimestri del 2008.



Nuovi siti web quotidiani con reputazioni malevole

Dove si trovano questi URL con una reputazione web negativa? Non dove la maggior parte della gente immagina.



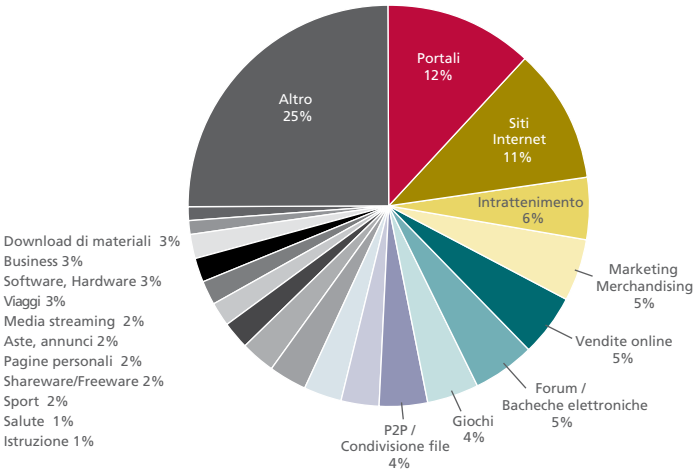
Distribuzione di siti web con reputazioni malevole

Perché l'improvviso cambiamento in ciò che molti hanno considerato essere diventata la "norma" (Stati Uniti, Russia, Cina) rispetto all'attività web malevole?[1] Ciò non significa che alcune di queste nazioni abbiano meno URL con una reputazione malevole. Piuttosto, si tratta più di un riflesso dell'aumentata crescita all'interno di altre nazioni. Buona parte di tale crescita ha a che fare con dove Conficker ha ospitato alcuni dei domini che ha in previsione di contattare, o che ha già contattato In effetti, il contributo di Conficker da solo ha portato l'Olanda al quarto posto. Sebbene l'Olanda sia stata a lungo una scelta diffusa per ospitare URL di phishing, Conficker ha contribuito in modo significativo per i siti web infettati dal malware e altri contenuti malevoli. Comunque, tale cambiamento non può essere attribuito in toto a Conficker. Il Canada è entrato nella Top 10 dei server web malevoli, che è principalmente focalizzata su quali malware e spyware sono stati rilasciati da questi siti.

Un'importante lezione è che queste stesse nazioni si fanno vedere rispetto a vari vettori d'attacco: siti web malevoli , siti che ospitano spyware/adware, phishing e spam. Le prime 7 nazioni che ospitano siti web con una reputazione malevole sono anche nella Top 10 tra i siti che ospitano phishing, spam, e malware/spyware.

1. Nel terzo trimestre del 2008, la classifica era la seguente: Stati Uniti con il 41%, la Cina con il 12%, la Russia con il 7%, la Germania e l'Olanda con il 5%, la Corea con il 4%, Hong Kong con il 3%, Taiwan, Canada e Repubblica Ceca con il 2%, gli altri con il 17%.

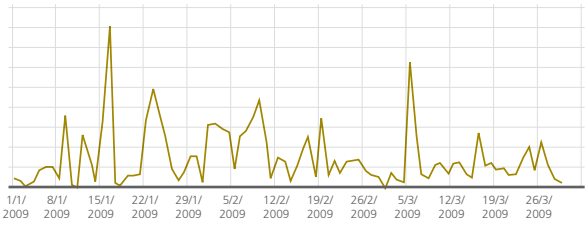
I siti con una reputazione malevole hanno scopi considerevolmente differenti, che siano legittimi, loschi o truffaldini. Si correrà comunque un rischio elevato quando si visita un sito pornografico o di gioco d'azzardo che non è associato ad un'azienda riconosciuta e legittima. Comunque, qualsiasi sito è vulnerabile, e qualsiasi tipo di contenuto che un utente desidera consultare rappresenta un'opportunità da sfruttare per coloro che diffondono il malware.



Le principali 20 categorie legittime che si sono guadagnate la reputazione di 'sito web malevolo' da Trusted Source

Questo trimestre, i server di contenuti hanno registrato un aumento in termini di popolarità con coloro che diffondono il malware come uno strumento per contenuti malevoli e illegali. Abbiamo rilevato questa tendenza su siti che sono ubicati e gestiti da provider affidabili e rispettati così come coloro che sono meno conosciuti e più discutibili. Combinando questa minaccia con l'utilizzo diffuso di blog e ottimizzazione dei motori di ricerca, è più critico che mai per qualsiasi computer disporre di una protezione web completa.

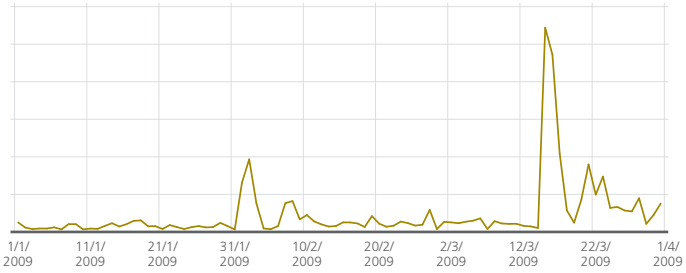
Abbiamo discusso del *dove*, ora parliamo dei *tipi* di minaccia di cui preoccuparsi. Oltre a Conficker, si è trattato di un trimestre intenso in termini di attività legate a nuovo malware e exploit disponibili sul web.



Nuovi siti web che distribuiscono malware e PUP

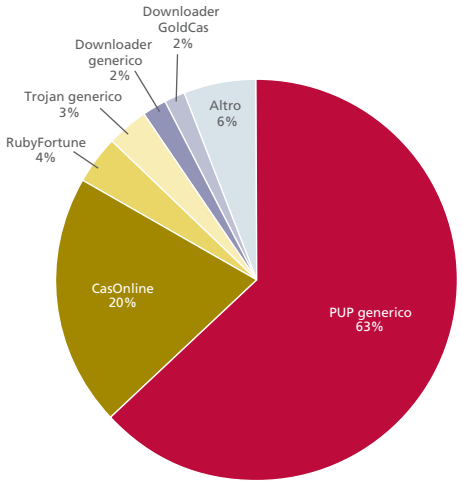
La tabella qui sopra offre un quadro del numero di siti web che rilasciano malware e programmi indesiderati (PUP) che sono stati rilevati in questo trimestre dalla rete McAfee TrustedSource. (La tabella mostra i siti che effettivamente ospitano malware e riflette il traffico utente su quei siti. La tabella non include siti legittimi che vengono sfruttati per indirizzare gli utenti su siti malevoli. Inoltre, da questa tabella abbiamo rimosso la nostra ricerca proattiva per fornire un quadro reale delle nuove minacce uniche disponibili durante l'attività di navigazione standard, a scuola, al lavoro o a casa.)

Per contro, le tabelle qui sotto illustrano cosa la nostra metodologia proattiva ha individuato in termini di nuovi download unici di malware da vari siti web. Abbiamo alcuni picchi interessanti da dove sono stati individuate "miniere d'oro" di download malevoli e PUP.



Download di malware e PUP, identificati proattivamente, per giorno

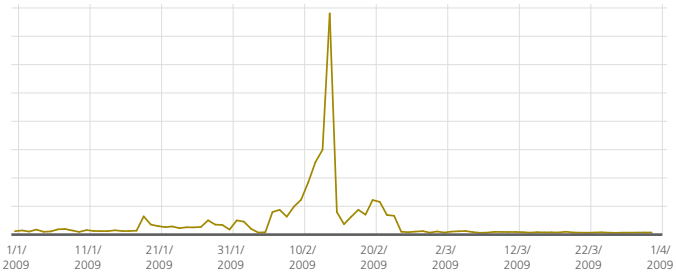
Le nostre attività di osservazione proattiva - navigazione abituale e verifica di siti web insieme a metodi unici per estrarre ulteriori informazioni malevole - hanno mostrato un picco elevato di nuovi download malware legati ai casinò verso la fine di Gennaio e l'inizio di Febbraio, oltre a un picco nei PUP generici verso la fine del trimestre. Quest'attività ha rappresentato i quattro principali tipi di download durante il trimestre. (Consultare la tabella successiva). Un altro malware interessante è la presenza costante del Trojan Vundo, che è diventato più attivo negli ultimi tre mesi.



Predominanza dei download di malware e PUP, per tipo

Una delle minacce web amorfe è *l'exploit*, un termine che può avere significati vari, e spesso diversi, per i ricercatori e gli utenti. Avert Labs tiene traccia di nuove pagine che ospitano exploit del browser dal momento che navighiamo e monitoriamo il web, e identifichiamo con regolarità nuove vulnerabilità per la sicurezza dei browser. Quando i browser (e i loro plug in) non vengono mantenuti aggiornati, questi "sandbox o recinti digitali" possono diventare facilmente un campogiochi per gli autori di malware. Una volta che quest'autore assume il controllo, il computer dell'utente potrebbe ricevere codice di programmazione che permette infezioni adware, spionaggio dei keystroke e altre attività malevole.

Quando i browser (e i loro plug in) non vengono mantenuti aggiornati, questi "sandbox o recinti digitali" possono diventare facilmente un campo giochi per gli autori di malware.

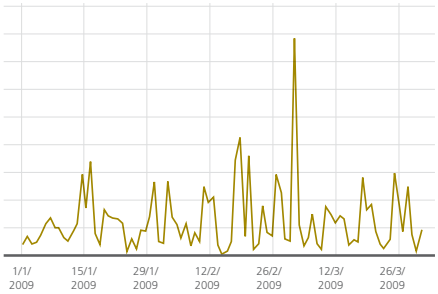


Rilevamento di siti contenenti exploit del browser

Attività degli anonymizer

Gli autori di malware stanno incrementando il loro utilizzo di attacchi di reindirizzamento degli URL, sia tramite un anonymizer (un servizio che consente di navigare in modo anonimo) o un'interfaccia Web 2.0 utilizzando un server di contenuti. Ciò potrebbe essere per evitare il rilevamento standard (comportandosi come un URL incorporato invece di un URL sorgente) o per trarre vantaggio dalla reputazione del sito che sembra distribuire malware.

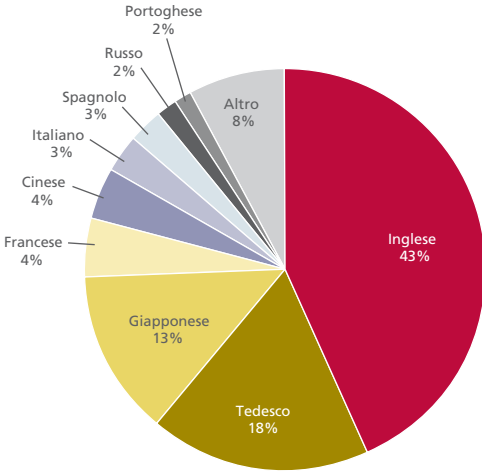
Un anonymizer è uno strumento che nasconde l'identità dell'utente quando si collega online. La maggior parte degli anonymizer non sono malevoli e perciò non sono inclusi nelle nostre precedenti discussioni sui rischi di sicurezza. Comunque, l'utilizzo di uno di questi strumenti potrebbe aprire la porta a un attacco "man in the middle (uomo nel mezzo)", nel quale un anonymizer malevolo o dirottato inietta codice all'interno dei messaggi che viaggiano, in entrambe le direzioni, tra l'utente e il server. Ciò non solo mette in pericolo l'utente, ma mette a repentaglio host e reti che sarebbero altrimenti protetti. Complessivamente, l'attività degli anonymizer in questo trimestre è aumentata rispetto al trimestre precedente. Si è inoltre verificato un leggero aumento nell'attività anno su anno per questo trimestre.



Nuovi Anonymizer su base quotidiana

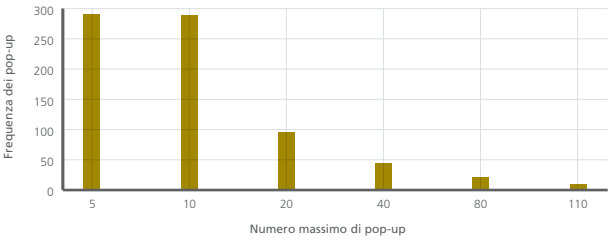
Tendenze generali del web

Il web è una comunità globale. Prendiamo in considerazione le connessioni tra qualsiasi sito professionale o di social networking. Le pagine web continuano a supportare più lingue a ritmo continuo. Gli stessi attacchi blog verificatisi su siti di alto profilo negli Stati Uniti vengono inoltre distribuiti tramite blog cinesi, brasiliani e molti altri. E gli attacchi odierni utilizzano una rete estesa. Inoltre, poiché coloro che distribuiscono malware traggono vantaggio dalla brand awareness (come eventi sportivi di rilievo e l'utilizzo di malware incorporato in categorie o riproduttori JPG), utilizzano marchi noti a livello globale per colpire audience in tutte le lingue.



Ripartizione delle diverse lingue nei contenuti web

Anche il fenomeno dei noiosi pop-up non è diminuito. E' interessante il fatto che, nonostante la disponibilità di programmi che bloccano i popup e altri strumenti a supporto, la maggior parte dei siti web non li utilizzi. Il numero massimo di popup in partenza da un sito web è stato pari a 116.



Distribuzione dei pop-up nei siti con un minimo di 5

Le aziende sul web devono essere esaminate con la stessa minuzia con cui si esaminerebbe un venditore porta a porta.

Continuiamo a rilevare un utilizzo diffuso di URL Web 2.0 e aziendali legittimi per diffondere il malware. Dieci o più anni fa, si pensava di poter rimanere al sicuro semplicemente evitando alcuni contenuti, ma oggi le minacce sembrano trovarci indipendentemente dalle attività che svolgiamo online. Qualsiasi sito web che possa essere sfruttato (tramite una qualsiasi delle numerose vulnerabilità disponibili) sarà colpito. Gli amministratori dei siti web possono rilevare scansioni che cercano di eseguire l'exploit dei propri server. Ciò che è interessante è l'elevata diffusione di queste scansioni in arrivo da siti e server associati a software illegale, siti malevoli e attraverso anonymizer. Se un sito web ad elevato traffico è vulnerabile, la questione non è se verrà sfruttato, ma quando.

Abbiamo registrato un marcato aumento delle truffe sul web. Prevediamo aumenteranno dal momento che gli artisti della truffa si alimentano delle preoccupazioni della popolazione mondiale tramite posta spam e il web. Spesso è molto difficile capire se un'organizzazione è legittima. Le aziende sul web devono essere esaminate con la stessa minuzia con cui si esaminerebbe un venditore porta a porta. Gli utenti devono sapere che una volta che forniscono a un truffatore le informazioni sulle carte di credito per una donazione online o un servizio fasullo, quei dati sono persi.

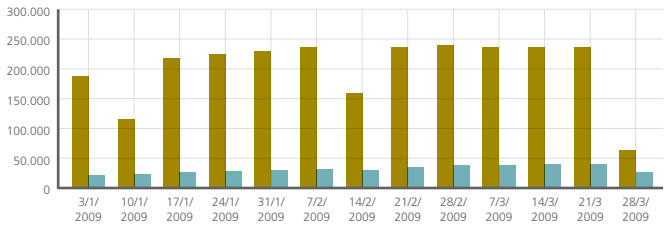
Comunque, la nostra ricerca dà un po' di speranza all'economia. I siti di beni immobiliari hanno mostrato un marcato aumento in termini di crescita questo trimestre, forzando le principali 10 categorie dei contenuti disponibili agli utenti (e spingendo lo sport fuori dal gruppo di testa).

Malware: la montatura di Conficker contro la realtà degli AutoRun

Gli ultimi mesi sono stati ricchi di articoli relativi a Conficker. Avrete pensato che si trattasse dell'unica minaccia di cui valesse la pena preoccuparsi. Comunque, quando analizziamo i numeri, il quadro della situazione è differente. Conficker non corrisponde esattamente al giorno del giudizio.

Conficker è infatti un tassello importante del malware per molte ragioni. Ha infettato numerosi host. E' stato attivamente sviluppato, mantenuto e discusso. Ma i rilevamenti reali non sono così eccezionali come si potrebbe pensare di un malware che ha ricevuto così tanta attenzione.

D'altro canto, quest'anno abbiamo rilevato malware preoccupante. Si tratta di una questione diversa per il malware basato su AutoRun, che utilizza prevalentemente drive USB o flash memory per autoreplicarsi ed è stato individuato in quantità molto maggiori rispetto a Conficker durante questo trimestre. Analizziamoli entrambi fianco a fianco:



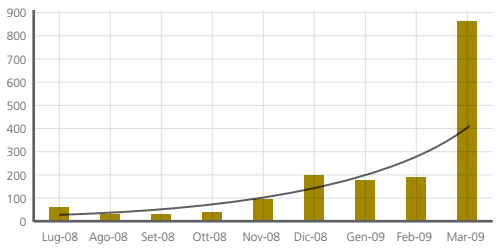
Negli ultimi 30 giorni, meno del 10% di tutte i rilevamenti segnalati è rappresentato dai worm AutoRun. Conficker è partito con un 1% ed è cresciuto di 12 volte, ma rappresenta ancora meno del 15% del totale dei rilevamenti di worm AutoRun al picco più recente.

Aggiornamento delle previsioni

All'inizio del 2009, McAfee Avert Labs ha rilasciato le proprie *previsioni delle minacce 2009*.[2] Molte delle nostre ipotesi si sono materializzate in questo trimestre.

Feriti da fuoco amico

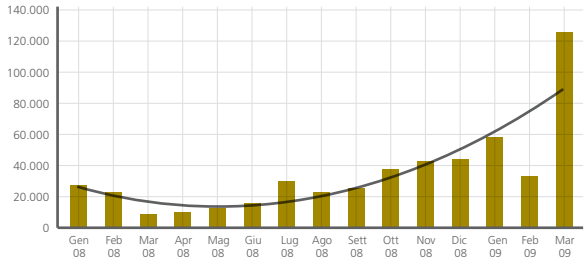
Nell'ultimo decennio un vettore di minacce primario, la ricezione di virus dai propri amici, ha ampiamente fallito. Il Web 2.0 ha rivitalizzato questo metodo d'attacco della vecchia scuola. Durante questo trimestre, molte varianti di Koobface hanno colto di sorpresa migliaia di utenti, quando hanno ricevuto il virus dai propri amici su Facebook. All'insaputa delle vittime, i link associati ai messaggi che hanno inviato i virus conducevano a siti web che avevano distribuito il worm. Poco dopo i loro computer contrassero il virus e inviarono messaggi infettanti alla loro cerchia di amici. I social network continuano a offrire agli aggressori un vettore per gli attacchi di social engineering.



2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_it.pdf

World Wide Web inaffidabile

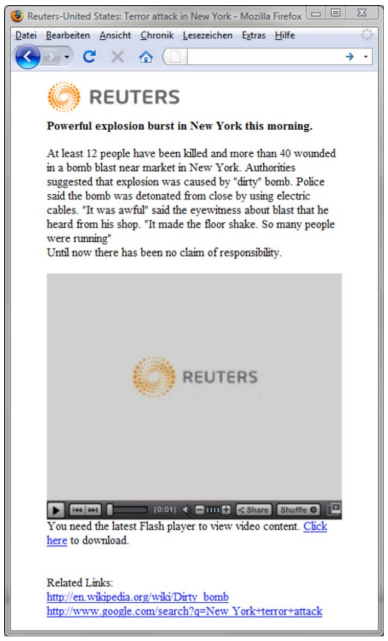
A Febbraio, Facebook è stato sfruttato da aggressori che hanno creato applicazioni rogue o inaffidabili utilizzando la piattaforma di Facebook. Molti utenti hanno abboccato e installato queste applicazioni. Questi eventi hanno attirato l'attenzione dei media, il che ha portato McAfee Avert Labs a scoprire un'enorme cerchia di ottimizzazione dei motori di ricerca che stabilivano come obiettivo i principali termini di ricerca Google. Gli aggressori non solo hanno rubato materiali coperti da copyright da siti popolari, ma hanno anche abusato di altri siti conosciuti come Democrats.org per far aumentare le loro graduatorie in Google. L'obiettivo degli aggressori nell'ttimizzazione dei risultati di ricerca era quello di installare software antivirus inaffidabile. Questo è stato un caso di applicazione inaffidabile di Facebook, che porta a risultati di ricerca e software di sicurezza inaffidabili. Questi incidenti esemplificano l'esigenza di navigare in modo sicuro per gli utenti.



Rilevamenti di codice binario unito di antivirus inaffidabili

Le minacce parlano la tua lingua

Gli aggressori sanno che più un attacco è rilevante e contestualizzato, più probabilmente una persona agirà di conseguenza: cliccando su un link, inserendo un nome utente/password, installando un'applicazione. Racconti di eventi che accadono a casa nostra attirano di più l'attenzione degli stessi eventi verificatisi dall'altra parte del mondo. A Febbraio e Marzo le gang criminali che stavano dietro al virus Waledac hanno sfruttato questo concetto. Vittime ignare sono state attirate su siti web che erano stati personalizzati sulla base della loro ubicazione, aggiungendo un senso di autenticità. Mentre gli utenti leggevano le "news locali", il sito web tentava di installare di nascosto il virus tramite codice exploit drive-by.



Blog McAfee Avert Labs

Google e l'abuso dei motori di ricerca

Google. Il nome da solo ha molti significati per molte persone. Per coloro che sono alla ricerca di un lavoro rappresenta un modo per trovare gli annunci più recenti. Per i datori di lavoro è un modo per trovare persone qualificate online. Per gli acquirenti è uno strumento efficace per individuare prezzi allettanti per i beni di cui hanno bisogno. Per gli autori di malware e i cibercriminali è uno strumento sempre più efficace per distribuire malware e impegnarsi in attività cibercriminali. Se si considera che i motori di ricerca rappresentano oggi la maggior parte dell'attività Internet sembra logico che gli autori di malware tentino di sfruttare la sua potenza come modo per distribuire i propri articoli. Per un esempio dei nostri blog su quest'argomento, date un'occhiata a questi passaggi del blog McAfee Avert:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Considerando la potenza combinata di indicizzazione e parole chiave popolari con l'incentivo dato da denaro facile per i cibercriminali, prevediamo che questo tipo di abuso continuerà.

L'economia e la paura

I problemi economici globali continuano a preoccupare molte persone. Problemi di sicurezza e terrore continuano a tormentarne altre. Gli autori di malware e i cibercriminali possono trasformare facilmente queste paure in guadagni. Questa tendenza, che era una delle nostre previsioni delle minacce per il 2009, è sicuramente stata sfruttata durante questo trimestre in molti modi preoccupanti. La paura è un potente elemento motivante quando viene utilizzata come un'esca di social engineering dai cibercriminali:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Truffe, spam e phishing funzionano abbastanza bene quando le cose vanno bene figuriamoci quando vanno male. Ricordiamo sempre che i cattivi leggono le stesse notizie che leggiamo noi e utilizzeranno i titoli e gli eventi per colpirci a meno che non rimaniamo vigili.

I McAfee Avert Labs

McAfee Avert Labs è il gruppo di ricerca mondiale di McAfee, Inc. Con gruppi di ricerca focalizzati su malware, programmi indesiderati (PUP), intrusioni su sistemi e reti, malware mobile e divulgazione etica delle vulnerabilità Avert Labs gode di un'ampia visione della sicurezza. Questa estesa visione permette ai ricercatori McAfee di migliorare costantemente le tecnologie di sicurezza e proteggere al meglio il pubblico.

Informazioni su McAfee, Inc.

Con sede principale a Santa Clara, California, McAfee Inc. è la principale azienda focalizzata sulle tecnologie di sicurezza. McAfee è costantemente impegnata a affrontare le problematiche di sicurezza più difficili nel mondo. Offre soluzioni e servizi proattivi e collaudati per la sicurezza di sistemi e reti in tutto il mondo, permettendo agli utenti di collegarsi a Internet, navigare e fare acquisti sul web in piena sicurezza. Supportata da un premiato team di ricerca, McAfee mette a disposizione di utenti consumer, aziende, pubblica amministrazione e service provider, la propria approfondita competenza, impegno e innovazione per aiutarli a dimostrare conformità con le normative, proteggere i dati, evitare interruzioni delle attività, identificare le vulnerabilità, tracciare e migliorare costantemente la loro sicurezza. http://www.mcafee.com/it.

McAfee Srl
Via Fantoli 7
20138 Milano
02.554171
www.mcafee.com/it

McAfee e /o altri marchi McAfee citati nel presente documento sono marchi o marchi registrati di McAfee, Inc. e/o sue affiliate negli Stati Uniti e/o altri paesi. Il rosso McAfee utilizzato con riferimento alla sicurezza è una caratteristica distintiva dei prodotti con marchio McAfee. Tutti prodotti non relativi a Mcafee, gli altri marchi registrati o non registrati citati nel presente documento sono di proprietà esclusiva dei rispettivi titolari. © 2009 McAfee, Inc. Tutti i diritti riservati.
5395rpt_avert_quarterly-threat_0409