Report sulla sicurezza del primo semestre 2011

Blue Coat Systems, Inc.

30 giugno 2011

Panoramica Generale

L'innovazione produce opportunità, anche per il cosiddetto "sommerso". Le innovazioni per il web e la mobilità si concentrano sulla facilità di utilizzo, la disponibilità e la creazione di un vasto pubblico di utenti ma non mancano di offire opportunità al cibercrimine. La sicurezza come al solito arriva tardi, dopo un periodo di infrazioni e dopo che i problemi della sicurezza pongono l'emergenza in prima linea. A metà 2011, ci troviamo nel bel mezzo di questo periodo di sicurezza.

La maggior parte delle minacce sul web vengono ora inviate da siti web diffusi e fidati, oggetti di attacco del cibercrimine. Per tale motivo, le difese della reputazione sono diventate meno efficaci. Quello che una volta era un link farm oscuro per il search engine poisoning, risiede ora all'interno di siti web diffusi. L'eccezione per i link farm è ora un dominio maligno o un sito web remoto. Gli attacchi di phishing provengono in massa da siti web diffusi e fidati, attaccati dal cibercrimine. L'accumulo recente di identità utenti e degli ID di posta elettronica in vasta scala da parte del cibercrimine incrementano la preoccupazione per gli attacchi di phishing e di APT (Advanced Persistent Threats) che mirano a utenti e organizzazioni specifiche.

SEP (Search engine poisoning) è salito al posto numero uno come metodo di propagazione delle minacce web in questo periodo dell'anno. Per essere più specifici, le ricerche di immagini hanno superato le ricerche di testo e sono ora il vettore principale per la propagazione di malware. I film e i giochi pirata, oltre ai contenuti per adulti, sono l'esca principale contando sui nuovi dispositivi che forniscono agli utenti un panorama di intrattenimento ad alta definizione . Le pagine web vengono spesso create in modo dinamico per gli attacchi SEP, sottolineando il valore di una difesa in tempo reale attraverso il rating dei siti web e l'analisi delle minacce . Inoltre, si è ripresentato lo spam relativo ai film e i giochi pirata, distribuendo falsi codec o warez che conducono direttamente al malware in modo dinamico.

I siti web di cui ci fidiamo sono punti di ingresso del cibercrimine. Dal momento che i siti web al giorno d'oggi contengono migliaia di link web dinamici a diverse fonti e tipi di contenuto, le innovazioni come il malvertising vengono considerate ora il secondo metodo di distribuzione delle minacce web più diffuso a metà 2011. Il cibercrimine risiede pazientemente nelle reti delle campagne pubblicitarie multilivello e sceglie in modo selettivo gli obiettivi, oltre a valutare exploit e vulnerabilità. Ogni qualvolta si presenta l'opportunità, colpisce. Un'analisi paziente e selettiva fornisce un miglior ritorno sugli investimenti rispetto agli attacchi di immissione di massa degli anni passati.

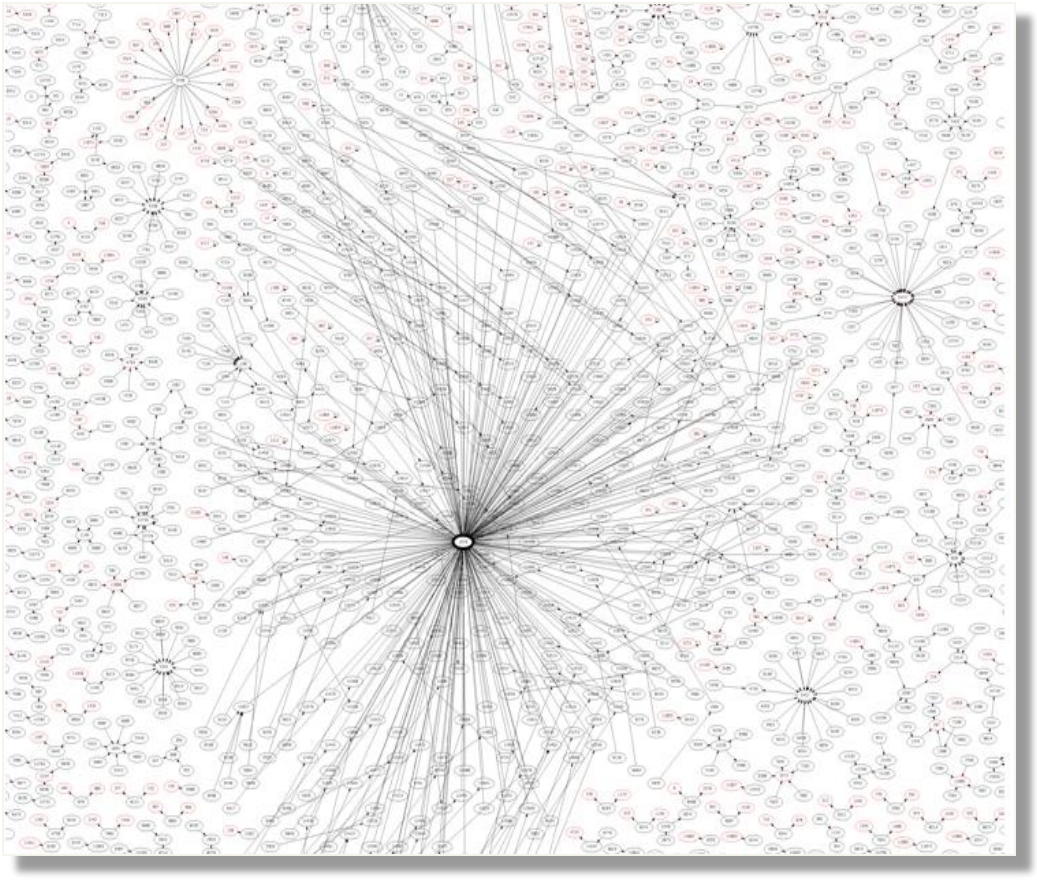
L'analisi svolta in queste settimane mostra la SEP a un volume stabile, con un "effetto marea" di alti e bassi. A causa del malvertising, i grafici sono pieni di picchi e curve, in quanto il volume di attacco cambia drasticamente giorno dopo giorno e spesso entro un lasso di tempo di 24 ore. La ricerca sui link web dinamici mostra come il cibercrimine si stia muovendo velocemente verso nuovi domini e indirizzi IP—più rapidamente rispetto agli anni passati. Mentre alcuni siti di cibercrimine di lunga vita esistono ancora, la tendenza odierna è la velocità di trasferimento verso nuove identità e postazioni per evitare di essere scoperti.

Dalla prospettiva di un user agent, alcuni utenti Mac sono alla ricerca di prodotti e immagini pirata e incorrono nei vettori di consegna malware conosciuti. Mentre i kit di exploit odierni si concentrano sugli utenti Windows, molti utenti Mac sono in apprensione per i possibili attacchi da parte del cibercrimine. Quando gli utenti Mac saranno l'obiettivo del cibercrimine, si troveranno privi di protezione. Prima della fine del 2011, non sarà una sorpresa vedere gli utenti Mac far fronte ai problemi delle minacce.

Seguire la pista delle reti malware

Le esche sono dinamiche e così i carichi utili. D'altra parte, l'infrastruttura delle reti di propagazione malware richiede tempo e sforzo per la manutenzione e il funzionamento. Quando un avvenimento o un evento che coinvolge celebrità cattura la nostra attenzione, l'utilizzo di questi come esche richiede una rete malware pronta a raccogliere utenti web in modo efficace. Qui sotto è riportata un'immagine dalla difesa cloud Blue Coat WebPulse™, gestita da Blue Coat Security Labs, dei siti web noti per distribuire minacce sul web e per le correlazioni tra di essi. Le reti di propagazione malware sono sparse in diversi siti web—molti di essi fidati e diffusi—per evitare di essere scoperte tramite l'analisi della reputazione. Nascondersi all'interno di siti web che godono di buona reputazione è diventata una modalità comune per la distribuzione di minacce sul web e per gli attacchi di phishing. Raramente tutti gli elementi di attacco si trovano in un unico sito web.

Immagine 1: Reti di propagazione malware e siti web ad esse correlati

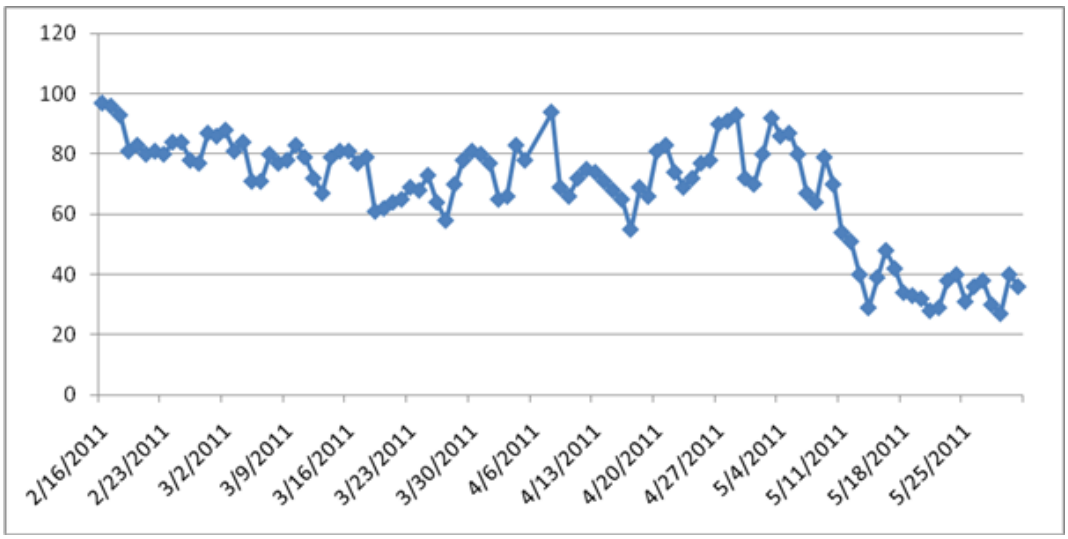


Fonte: Blue Coat Security Labs

Il software per la mappatura grafica consente di vedere in modo chiaro come la grande rete di malvertising, al centro dell'immagine sopra, trascina gli utenti nell'attacco in modo del tutto inaspettato. Inoltre è possibile vedere molte altre correlazioni di cerchi più piccoli di siti web collegati che lavorano insieme in modo dinamico per raccogliere utenti e distribuire minacce sul web. Le linee verticali delle ellissi (siti web) nella parte superiore centrale sono scale pornografiche.

Ogni giorno, il numero delle reti malware esistenti varia. Nella prima metà del 2011, le reti malware sono variate da poco meno di 100 operative in un solo giorno a meno di 25.

Grafico 1: Reti di consegna malware esistenti al giorno



Fonte: Blue Coat Security Labs

Il grafico 1 rappresenta il numero delle reti malware univoche visualizzate ogni giorno, con un calo a metà maggio, in conseguenza di trasferimenti e consolidamenti. In tutto, a partire dalla fine di maggio sono state sotto osservazione 395 reti malware univoche. Negli ultimi 30 giorni rappresentati nel grafico, ogni giorno sono state visualizzate in media 50 reti malware univoche.

La tabella 1 classifica le reti di propagazione malware in base al numero di host sotto attacco. La tabella mostra sia il numero medio che il numero massimo e minimo di nodi nella prima metà dell'anno. Ciò dimostra la natura dinamica di queste reti.

Tabella 1: la Top 10 delle reti di consegna malware in base al numero di nomi host univoci

Rete di consegna malware	Numero di host			Attività maligne principali
	Media	Min	Max	

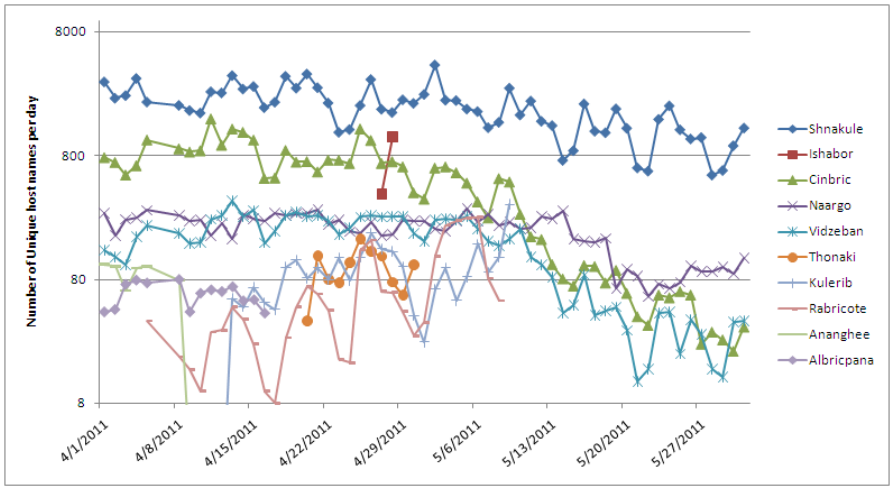
Shnakule	2001	560	4357	Drive-by download, finti antivirus (AV), finti codec, finti aggiornamenti flash, warez finti, aggiornamenti Firefoz finti e botnet / controlli CnC NOTA: le attività correlate includono pornografia, gioco d'azzardo, prodotti farmaceutici, link farming e scam di tipo "work-at-home" (lavoro da casa).
Ishabor	766	393	1140	AV falso
Cinbric	505	21	1602	Ransomware a sfondo pornografico
Naargo	199	58	299	Rete a sfondo pornografico NOTA: non rappresenta categoricamente una rete malware ma la sua natura sospetta deve essere costantemente seguita e indagata.
Vidzeban	156	12	347	Warez falso NOTA: questa rete presenta pagine in russo.
Thonaki	99	37	169	AV falso
Kulerib	96	1	325	Malware drive-by download e sul gioco d'azzardo NOTA: le attività correlate includono pornografia, gioco d'azzardo, prodotti farmaceutici e scam di tipo "work-at-home" (lavoro da casa).
Rabricote	72	8	254	Link farming sospetto
Ananghee	62	1	106	AV falso
Albircpana	61	43	80	AV drive-by download falsi

Fonte: Blue Coat Security Labs

Inizialmente si pensava che Ishabor, Kulerib, Rabricote e Albircpana fossero reti self-contained (autocontenute), ora sono state identificate come componenti della più grande rete di propagazione malware Shnakule.

Per una prospettiva su come oscilla la dimensione delle reti di propagazione malware su base giornaliera, il grafico 2 mostra il numero dei nomi host univoci (o degli host sotto attacco univoci) generati ogni giorno nei mesi di aprile e maggio.

Grafico 2: nomi host univoci al giorno nella Top 10 delle reti di consegna malware



Fonte: Blue Coat Security Labs

Shnakule è stata la rete di propagazione malware dominante, mentre Cinbric e Vidzeban hanno subito un declino. Ishabor ha avuto vita breve; tuttavia, in due giorni ha prodotto 1.500 nomi host univoci prima di entrare a far parte di Shnakule e creare una rete di propagazione malware più ampia.

La natura dinamica degli attacchi sul web emerge nelle tabelle e nei grafici molto velocemente. Mentre Google Earth visualizza le città, le strade e gli edifici, la difesa cloud Blue Coat WebPulse effettua il mapping delle reti di consegna malware. A differenza degli indirizzi degli edifici, però, i nomi degli host cambiano molto rapidamente.

La tabella 2 classifica le reti malware in base al numero di richieste iniziali al giorno, su un periodo di tempo superiore ai 60 giorni, effettuate automaticamente ai server di rating WebPulse dalle appliance Blue Coat ProxySG. Mentre la tabella 1 classificava le reti di propagazione malware per dimensione, la tabella presente considera la loro efficacia nell'indirizzare gli utenti verso le reti stesse.

Tabella 2: la Top 10 delle reti di consegna malware in base alle richieste iniziali del server di rating

Rete di consegna malware	Numero di richieste			Attività maligne principali
	Media	Min	Max	
Shnakule	21263	4555	51539	Vedere la tabella 1
Ishabor	4303	2717	5888	Vedere la tabella 1
Shangvos	2899	0	5892	Download maligni
Tonenuro	2105	1766	2444	AV falso
Ostroka	1832	0	11636	Scam e sondaggi di Facebook sospetti

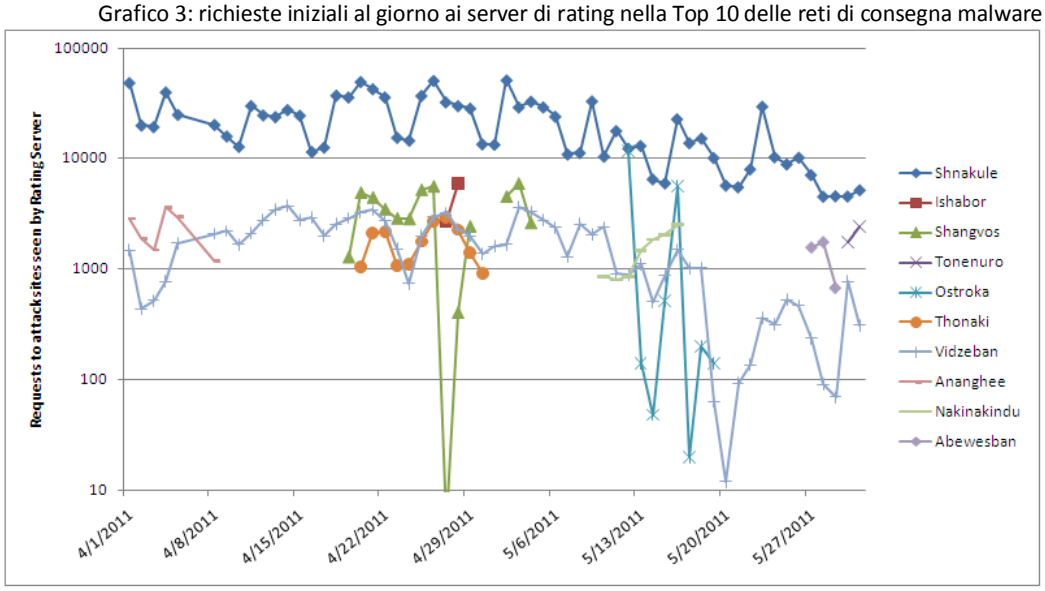
Thonaki	1768	911	2919	Vedere la tabella 1
Vidzeban	1637	12	3741	Vedere la tabella 1
Ananghee	1557	0	3613	Vedere la tabella 1
Nakinakindu	1486	799	2507	Drive-by download NOTA: si pensa sia un componente di Shnakule
Abewesban	1330	669	1755	AV falso

Fonte: Blue Coat Security Labs

Nelle tabelle 1 e 2 sono state evidenziate quindici reti di propagazione malware univoche. Questo rappresenta solo un piccolo esempio delle quasi 400 reti di propagazione malware univoche sotto il controllo di Blue Coat Security Labs nella prima metà del 2011.

Nel grafico riportato qui sotto, le reti di propagazione malware sono state considerate in base al numero di richieste iniziali ai server di rating. Il grafico delle reti di propagazione malware eseguibile con comando sh viene mostrato nel grafico 3 riportato di seguito.

Grafico 3: richieste iniziali al giorno ai server di rating nella Top 10 delle reti di consegna malware



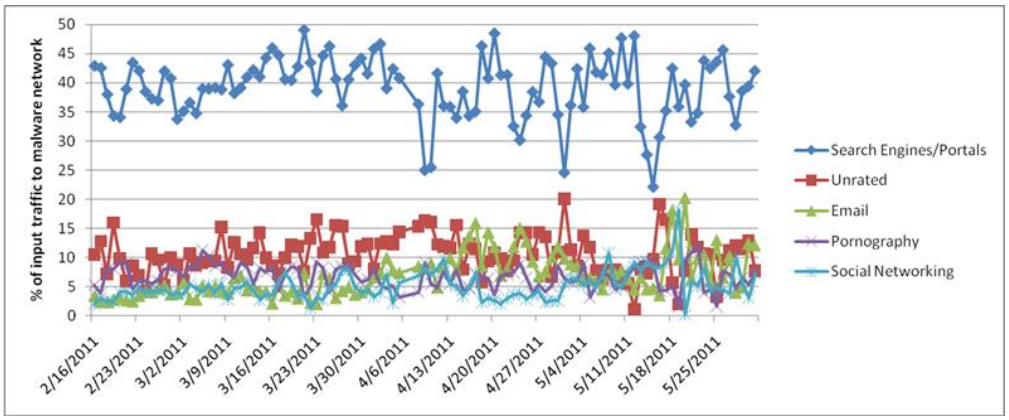
Fonte: Blue Coat Security Labs

Il grafico mostra il numero di richieste web iniziali per i siti malware classificate dai server di rating ospitati dal cloud WebPulse. Il rating viene fornito in tempo reale, quindi memorizzato all'interno dei dispositivi ProxySG distribuiti. Le successive richieste web vengono classificate localmente presso i siti del cliente da ProxySG utilizzando la cache per il rating dell'URL. In questo modo il numero reale di richieste web per queste reti malware da parte degli utenti con dispositivi ProxySG risulta di gran lunga maggiore.

Mentre le descrizioni delle reti di propagazione malware, delle tabelle e dei grafici sono interessanti e mostrano la natura dinamica e il volume delle minacce sul web, la questione su quali utenti cadranno in

queste reti malware rimane aperta. Il grafico 4 mostra le cinque categorie (o fonti) principali attraverso le quali utenti ignari entrano nelle reti di propagazione malware sotto osservazione.

Grafico 5: la Top 5 delle categorie di ingresso nelle reti di consegna malware



Fonte: Blue Coat Security Labs

Search engine poisoning è il principale vettore di propagazione malware della prima metà del 2011. Il malvertising non rappresenta una categoria specifica e non viene rappresentato nel grafico 5. Nonostante ciò, viene classificato come il numero due tra i vettori di propagazione malware in base all'analisi delle ricerche. Le reti tradizionali o ad alta sicurezza potrebbero scegliere di bloccare le richieste web non classificate, consapevoli di risultare terze in classifica per aver condotto gli utenti su reti di propagazione malware. I social network, la pornografia e la posta elettronica sono in parità al quarto posto. La tabella 3 riportata qui sotto mostra i paragoni tra le categorie in quanto punti d'ingresso per le reti di propagazione malware sotto osservazione.

Tabella 3: la Top 5 delle categorie per ingresso in reti malware, in base alla percentuale di richieste

	Media	Min	Max
Motori di ricerca/Portali	39.20	22.07	49.11
Non classificato	10.53	1.16	20.10
E-mail	6.90	2.04	20.19
Pornografia	6.70	1.59	11.85
Social Network	5.16	0.21	18.19

Fonte: Blue Coat Security Labs

La correlazione di questi argomenti dimostra che le ricerche di immagini per adulti o pornografiche siano classificate come richieste web il cui blocco è importante. Alle persone piace guardare gli altri, e questo fatto fa parte della natura umana. Come già notato nel report sulla sicurezza web Blue Coat del 2011 (febbraio 2011), la pornografia era al terzo posto per quanto riguarda la propagazione dei malware e le

minacce web. Inoltre, il report ha evidenziato dei picchi di 110.000 nuovi siti pornografici in un solo giorno. Queste impennate sottolineano l'importanza di una difesa web in tempo reale in grado di classificare i nuovi contenuti web e di scoprire i link web dinamici, in modo tale da conoscere le reti di propagazione malware o le minacce web inedite.

Analisi delle botnet: prova della condivisione

Nella prima metà del 2011, le notizie di numerose infrazioni, come anche la sottrazione di identità e di possibili codici sorgenti, oltre a frodi finanziarie, hanno portato sotto i riflettori i problemi relativi alla sicurezza, e porteranno cambiamenti alle difese, alle politiche e ai profili di rischio. Le tendenze verso le risorse condivise tra cibercriminali e i malware del mercato di massa rappresentano dei gravi sviluppi che portano ad un'evoluzione della protezione web.

Nei primi cinque mesi del 2011 i botnet, le reti CnC (command and control), i trojan e i worm più individuati sono rappresentati nella tabella 4. ZEUS è molto noto nei casi di frode finanziaria in quanto intercetta le credenziali di accesso degli account finanziari online. SALITY è stato associato al worm Daprosy, uno dei virus più distruttivi dell'ultimo decennio. KOOBFACE (un anagramma di Facebook) è diffuso all'interno dei siti di social network e infetta i sistemi Windows e Mac e perfino i sistemi Linux, sia pure in misura limitata.

Tabella 4: Botnet / reti C&C / Trojan / Worm più prolifici

1.	TROJAN-REGISTRY-DISABLER/Gen:Trojan.Heur.VB.dm0@gWscL@gi
2.	ZEUS/MUROFET/SPYEYE
3.	SALITY
4.	Trojan-Downloader.Win32.Agent.eckq
5.	Uno spam Trojan sospetto particolare (determinato tramite la reputazione online)
6.	WALEDAC*
7.	MEBROOT/SINOWAL/TORPIG
8.	DELSNIF
9.	HILOTI
10.	TROJAN-PROXY/Trojan.Win32.Agent.didu/Win32/SpamTool
11	KOOBFACE
12	TDSS
13	PUSHDO/CUTWAIL/PANDEX
14	CARBERP
15	KAZY*
16	BREDOLAB*

Fonte: Blue Coat Security Labs

**Molti di questi nodi infetti delle botnet condividono uno "spazio di botnet" simile. (Vale a dire che i sistemi di utenti finali appaiono infettati dai diversi trojan che producono botnet. Ogni exploit effettua richieste phone-home in relazione alle proprie funzionalità). Il quid pro quo, la condivisione dello spazio di botnet, esiste.*

Molte botnet sono note per incrociare e condividere i nodi compromessi in una relazione simbiotica (con altri malware monetizzabili, come ransomware, spam farmaceutici, scam e

un'ampia gamma di altri exploit). Gli esempi analizzati, sottoposti ad un ambiente di test, documentati e studiati da Blue Coat Security Labs manifestano questa caratteristica.

È una buona idea validare i siti web controllando i certificati e avvertendo gli utenti in merito a siti privi di certificati autorizzati. VirusTotal, utilizzato da molti professionisti e utenti finali per controllare i file o gli URL rispetto a oltre 40 motori anti-malware per le minacce, ha avuto un sito falso a partire da giugno 2011, secondo Kaspersky Lab. Il finto sito fornisce un worm in grado di reclutare i sistemi utente in una botnet per attacchi DDoS (distributed denial of service). Inoltre, comunica con i server CnC (command-and-control) con le caratteristiche dell'host, secondo i report dalla Net-security.org pubblicati a fine maggio. Secondo quanto riportato nei report, a febbraio 2010 VirusTotal è stato imitato per distribuire "scareware" ai visitatori.

Analisi di categoria per il filtraggio web

Nel primo semestre del 2011, l'analisi delle 20 categorie più richieste, basata sull'esame della comunità WebPulse (oltre 75 milioni di utenti), mostra che la maggior parte delle graduatorie sono simili a quelle del 2010, con qualche eccezione.

Tabella 5: la Top 20 delle categorie web più richieste

Gennaio-maggio 2011	2010
1. Motori di ricerca/Portali	Motori di ricerca/Portali
2. Computer/Internet	Pubblicità sul web
3. Social Network	Computer/Internet
4. Pubblicità sul web	Social Network
5. Server di contenuti	Server di contenuti
6. Audio/Videoclip	Audio/Videoclip
7. Contenuto misto/aperto	Notizie/Multimedia
8. Notizie/Multimedia	Acquisti
9. Non visualizzabile	Riferimento
10. Acquisti	Contenuto misto/aperto
11. Riferimento	Affari/Economia
12. Affari/Economia	Chat/Messaggistica istantanea
13. Intrattenimento	Intrattenimento

14. Pagine personali/Blog	Non visualizzabile
15. Chat/Messaggistica istantanea	Pagine personali/Blog

Fonte: Blue Coat Security Labs

I social network rappresentano la prima eccezione, e hanno scalato le classifiche fino a estromettere la pubblicità sul web dal terzo posto. Non è certo cosa da poco, visto che le tre categorie principali richieste rappresentano i pilastri della categorizzazione del traffico web, richiedono volume e raramente cambiano.

I social network stanno diventando un ecosistema di comunicazione a sé stante. Blue Coat WebFilter fornisce fino a quattro rating di categoria per richiesta web e più di 45 rating di categoria secondari all'interno della categoria "Social network". Ciò consente i controlli della policy su giochi, IM/chat, posta elettronica e altre categorie all'interno del social network o su specifici domini di social network come Facebook.com. Le nuove applicazioni web e i controlli sulle operazioni costituiscono un passo avanti e abilitano i controlli della policy tramite nomi e operazioni di applicazioni web specifiche. Caricare un video o una foto, caricare o scaricare degli allegati, pubblicare un messaggio o inviare un'e-mail sono esempi di operazioni.

Altra eccezione interessante della prima metà del 2011 è la scalata di tre posizioni dei contenuti misti/aperti, che si attestano alla settima posizione. Il problema qui è che i contenuti misti/aperti hanno avuto il più elevato tasso di crescita nell'ospitare i malware—fino al 29% su base annuale dall'analisi del 2010. Alcuni esempi di siti web di contenuto misto/aperto sono i siti di immagini (ad esempio: istockphoto.com, fotosearch.com, imagebarn.com) oltre ai siti che ospitano i video (ad esempio: google.video.com e youtube.com). In generale, i siti di contenuto misto/aperto ospitano contenuti non offensivi a caso, non organizzati, che devono essere posizionati in una categoria specifica. Tuttavia, potrebbero ospitare contenuti discutibili.

K9 Web Protection è un prodotto di difesa web gratuito per uso domestico fornito da Blue Coat. Mentre la popolazione degli utenti è inferiore al 5% della comunità totale WebPulse, la popolazione K9 fornisce oltre il 15% di minacce web ed esempi di contenuti non classificati per WebPulse, ed è di gran lunga la più interessante popolazione di utenti per finalità di analisi.

Tabella 6: la Top 20 delle categorie web più richieste per gli utenti di K9 Web Protection

Gennaio-maggio 2011	2010
1. Computer/Internet	Computer/Internet
2. Download di software	Motori di ricerca/Portali
3. Non visualizzabile	Audio/Videoclip
4. Archiviazione online	Archiviazione online
5. Motori di ricerca/Portali	Download di software

6. Social Network	Non visualizzabile
7. Chat/Messaggistica istantanea	Istruzione
8. Pubblicità sul web	Riferimento
9. Server di contenuti	Contenuto misto/aperto
10. Non classificato	Acquisti
11. Contenuto misto/aperto	Social Network
12. Notizie/Multimedia	Server di contenuti
13. Audio/Videoclip	Notizie/Multimedia
14. Giochi online	Pornografia
15. Acquisti	Servizi finanziari

Fonte: Blue Coat Security Labs

Risulta interessante vedere come il download di software e l'archiviazione online siano la seconda e la quarta categoria più richiesta tra i consumatori K9 e gli utenti privati. L'archiviazione online ha visto una crescita del 13% su base annuale nell'hosting dei malware, in base all'analisi dei dati del 2010. I siti non visualizzabili sono spesso tracciati e l'analitica web si colloca con un contenuto non visualizzabile nel browser web. Queste richieste web vengono tracciate da WebPulse.

In media, gli utenti al lavoro sono più interessati alle categorie notizie/comunicazione, affari/economia e riferimento rispetto ai consumatori K9 o agli utenti privati e ciò non sorprende affatto. È interessante notare che la pornografia risalta nella top 20 delle categorie per l'analisi degli utenti aziendali ma non per gli utenti privati di K9. Sicuramente K9 Web Protection potrebbe essere stato utilizzato per bloccare la pornografia a casa, così da portare gli utenti a visualizzarla al lavoro.

È possibile scaricare K9 Web Protection alla pagina web www.k9webprotection.com ed eseguirlo sui dispositivi iOS (iPad, iPhone), sistemi Mac e Windows (PC o tablet).

Siti web che ospitano malware

Come già accennato, le reti di propagazione malware sono ora nascoste in siti legittimi, tipicamente autorizzati da politiche d'uso accettabili. La tabella 6 rappresenta le categorie principali dei siti web che ospitano malware (rispetto alle reti di consegna) nella prima metà del 2011.

Tabella 6: Top 10 delle categorie di siti web che ospitano malware

	Gennaio-maggio 2011	2010
1.	Archiviazione online	Sospetti

2.	Download di software	Archiviazione online
3.	Pornografia*	Pornografia*
4.	Contenuto misto/aperto	Computer/Internet
5.	Computer/Internet	Motori di ricerca/Portali
6.	Segnaposto*	Contenuto misto/aperto
7.	Phishing*	Personali/Incontri
8.	Attacchi*	Servizi di web hosting
9.	Giochi online*	Download di software
10.	Illegale/Discutibile*	Phishing*

È necessario bloccare le categorie segnate da un asterisco per seguire le best practice finalizzate al filtraggio e alla protezione del web.

Per quattro delle cinque categorie principali l'utilizzo è considerato accettabile ed è concesso dalla maggior parte delle politiche aziendali sull'IT. La crescita su base annuale nelle categorie di contenuto misto/aperto e di archiviazione online è la preoccupazione maggiore, come riportato nel report sulla sicurezza web Blue Coat del 2011.

Riepilogo

È possibile riassumere i risultati in alcuni punti fondamentali:

L'hosting del malware si trova spesso all'interno di categorie a cui gli utenti possono accedere.

- SEP è il No. 1 nella propagazione malware, seguito dal malvertising e dai siti non classificati. Siti di social network, pornografia e posta elettronica sono a pari merito.

La pornografia si conferma come l'ultima esca "vecchia scuola". Ogni giorno vengono creati nuovi siti web per adulti, rendendo l'analisi dei contenuti web in tempo reale e il rilevamento delle minacce altrettanti requisiti.

- Gli utenti alla ricerca di immagini e materiale multimediale pirata costituiscono una fonte di preoccupazione primaria. La loro attività si colloca in cima alla lista delle possibili propagazioni malware. Le identità sottratte agli utenti pongono il phishing in posizione di assoluto rilievo, oltre allo spam per i rich media, gli aggiornamenti dei codec e i warez falsi.

Si arriva alla conclusione principale secondo la quale un singolo livello di difesa non è sufficiente, ma sono necessarie difese web in tempo reale. L'analogia con Google Earth afferma: fornisce mappe delle città, delle strade e degli edifici, mentre una difesa web in tempo reale esegue il mapping delle reti di

propagazione malware e mette in correlazione le esche dinamiche con i percorsi di propagazione e i payloads dinamici.

È noto che gli utenti spesso affrontano il web con non più di un software antivirus o un semplice filtraggio URL di siti statici conosciuti. Nel contesto di alcuni dei più importanti cibercrimini della storia, è necessario integrare difese web in tempo reale a uno schema composto da più livelli. Le difese ospitate nel cloud sono in grado di espandersi e adattarsi più velocemente alle nuove minacce web rispetto a quelle on-box e si avvalgono dei contributi degli utenti collaborativi in tempo reale per generare una profonda consapevolezza sulle minacce e i contenuti web di nuova generazione. È possibile aggiungere l'intelligence di sicurezza del cloud ai gateway web e agli utenti in remoto in un'architettura ibrida in tempo reale, o fornita come Cloud Security SaaS.

Basta un solo clic per aprire le porte al cibercrimine. Per un singolo link web dinamico è necessaria un'analisi in tempo reale per proteggere utenti, risorse e reputazione.

Crediti

Questo report è opera di Tom Clare, con la redazione di Craig Kensek.

I contributi in merito alle ricerche sulla sicurezza sono di Roger Harrison, Chris Larsen, Tim van der Horst, Tyler Anderson, Patrick Cummins e Ben Hanks.

Appendice – La nuova minaccia proveniente dal malvertising

Quasi tutti i servizi web gratuiti normalmente utilizzati — dalle ricerche alla posta elettronica, dalle mappe ai social network, compresi i siti con contenuti video o giochi — sono gratuiti, solo in quanto finanziati dalla pubblicità online. La pubblicità online rappresenta un enorme business multimiliardario, supportato da infrastrutture di reti pubblicitarie a più livelli, e funziona in modo efficace non solo per gli inserzionisti legittimi, ma anche per i cibercriminali. In effetti, nel report sulle minacce web 2011 di Blue Coat Systems , il *malvertising* (malware advertising)) è arrivato dal nulla per collocarsi alla posizione No. 3 nella Top 10 dei metodi di attacco web nel 2010. Osserviamo come funziona questo nuovo fenomeno, e proviamo a delineare qualche conclusione su come affrontarlo.

Pubblicità online e malvertising

Le reti pubblicitarie operano su un modello di marketing affiliato, dove gli advertiser collocano le campagne con un vasto numero di publisher – grandi e piccoli — che vengono pagate in commissioni sui contenuti multimediali, con riferimento ad azioni misurabili che tracciano il traffico per l'advertiser. La complessa rete affiliata agisce da intermediario tra i publisher e i programmi affiliati – accordi tra aziende che pagano in base al numero di persone che visitano la pagina contenente le pubblicità online del commerciante, la guardano o effettuano un clic-through per visualizzare una call to action sulla pubblicità stessa.

SIDEBAR

Anatomia di un attacco malware

Quanto segue è un caso tipico di malware osservato da Blue Coat Security Labs che ha recentemente colpito l'India.

- Come la maggior parte dei siti gratuiti d'informazione nel mondo, uno dei principali siti web di questo tipo in India - screenindia.com - è supportato dalla pubblicità.
- Uno dei link di terze parti per le pubblicità conduce a doubleclick.net, un grande dominio pubblicitario conosciuto e rispettabile. La pubblicità in questo caso era una pubblicità affidabile infetta.
- Dal sito doubleclick.net alcuni JavaScript portavano a daniton.com, che sembrava essere una parte affidabile della rete affiliata.
- In una visita iniziale a daniton.com il sito pubblicitario non reagiva, ma a una successiva visita consegnava una parte pesantemente crittografata di JavaScript.
- Il JavaScript proveniente da daniton.com comportava un'immissione di tag iFrame nella pagina host originale.
- L'iFrame richiedeva silenziosamente al browser web dell'utente una chiamata al vero host malware (è interessante notare come l'host malware cambiasse posizione ogni giorno) per scaricare un file exploit PDF.
- Altra cosa interessante: una delle funzioni dell'iFrame era quella di trovare la versione di Acrobat Reader in uso, in modo da sfruttare l'"exploit" corrispondente a quella versione e fornire così la vittoria più facile possibile.

Questa infrastruttura è grande e complessa, presenta grandi numeri di piccole transazioni, di relazioni aziendali, di connessioni collegate tra le pubblicità e le destinazioni dei click-through. Domini più ampi di rete pubblicitarie affidabili e conosciute potrebbero operare in outsourcing a favore di domini pubblicitari più piccoli, nuovi e magari non così affidabili. Grazie a molti livelli di separazione e automazione tra il commerciante che colloca l'annuncio e lo spazio dove la pubblicità finisce con l'essere posizionata, le reputazioni e l'affidabilità sono spesso assunte o ereditate attraverso i livelli delle reti affiliate.

Il cibercrimine adora sfruttare la reputazione e la fiducia di altre persone — così come la loro infrastruttura — per inviare software maligni a più persone possibile. L'immissione di una pubblicità maligna in una rete pubblicitaria legittima consente al cibercriminale di lanciare una rete molto grande senza necessariamente avere quel risalto da essere scoperto.

I cibercriminali sono in grado di:

- creare una nuova pubblicità benigna o un dominio pubblicitario che — una volta considerato affidabile, di buona reputazione e ottenuto il permesso dalla maggior parte delle difese — si trasforma in qualcosa di terribile oppure
- infettare chiunque abbia creduto in una pubblicità web, utilizzando lo stesso tipo di immissione o metodi di avvelenamento usati per infettare siti web affidabili e di buona reputazione

Una campagna di malvertising criminale viene condotta come ogni altra campagna pubblicitaria, ma in entrambi i casi bisogna immediatamente e silenziosamente rifare la pubblicità stessa o i suoi click-through per distribuire un payload del malware. Il payload infetta quindi il computer dell'utente, sottrae i dati di accesso e le password o il denaro e i dati dai datori di lavoro.

Osserviamo come le pubblicità passino da una rete affiliata alla pagina web e come i cibercriminali approfittino dell'infrastruttura a reti affiliate che caratterizza il mondo della pubblicità online.

Normalmente il proprietario di una pagina web offre lo spazio pubblicitario a un fornitore pubblicitario principale – l'unico con il quale il proprietario abbia un qualche rapporto. Avviene tutto in modo automatico e così, quando la pagina viene riempita, supponiamo, da nuovi articoli, le parole chiave nell'articolo sono rese disponibili al software del fornitore pubblicitario principale. Ad esempio, con le parole chiave "Golf" "Florida" e "Lusso", punteremo a persone interessate a una sofisticata vacanza praticando il golf con formula fly and drive nell'arcipelago Florida Keys. Il software "capisce" se ha a disposizione una pubblicità altamente pertinente

da utilizzare. Nel caso in cui il fornitore pubblicitario principale non dovesse disporre di una pubblicità in grado di mirare a queste persone o toccare una certa soglia economica posizionando una pubblicità per conto del suo cliente, è destinato a inserire una pubblicità meno mirata (ad un prezzo inferiore) proveniente da uno dei suoi affiliati. Nel caso l'affiliato non dovesse disporre di una pubblicità appropriata o si rifiutasse di pagare una tariffa secondaria per servire una pubblicità generica, si potrebbe decidere di servire una pubblicità generica/economica da uno dei *loro* affiliati. E così via.

Chiaramente questo groviglio di accordi tra affiliati/partner/sub-affiliati e di responsabilità incoerenti tra le reti pubblicitarie fornisce una grande opportunità alla pubblicità maligna – o a un dominio pubblicitario maligno – per infiltrarsi.

Come tutta la pubblicità sul web, gli annunci di malvertising potrebbero essere mirati (grazie a delle parole chiave come "fornitore di servizi di accesso a terze parti" o "protezione dei dati") per ottimizzare la propria efficacia e creare un tipo di collegamento dinamico ma mirato tra tutti i siti progettati per attrarre un particolare tipo di visitatore.

La tattica del tempismo e della trasformazione per eludere la sicurezza

Una caratteristica fondamentale del malvertising consiste in questo: l'annuncio pubblicitario o il dominio pubblicitario maligno si avvia in modo innocente, consentendo diversi controlli da parte dei software di sicurezza per acquisire dei rating puliti e una buona reputazione.

Come una cellula dormiente in un poliziesco, sa attendere con pazienza. Prendendo tempo per acquisire delle buone reputazioni all'interno delle reti pubblicitarie e sottoponendosi a diverse ricerche di malware, il cibercrimine crea posizioni affidabili e di valore all'interno delle strutture pubblicitarie sul web prima di lanciare degli attacchi che conducono ad una campagna di successo. Quando il dormiente si sveglia, il routing dietro l'annuncio viene trasformato per visualizzare o eseguire il click-through verso un host malware, in modo che le connessioni malware siano in grado di fare del loro peggio nella campagna di destinazione. Finito il lavoro, se ne vanno.

Le tattiche del malvertising messe in atto dal cibercrimine tendono a sferrare attacchi durante il fine settimana quando le risorse IT sono minime, gli aggiornamenti della difesa non sono ancora installati e un attacco verrebbe notato di meno. È bene ricordarsi che le difese web classiche sono mirate agli aggiornamenti – un nuovo database deve essere eseguito prima che i sistemi di sicurezza possano agire sulla nuova minaccia.

Tecnologia e tecniche indispensabili per tenere alla larga la pubblicità dannosa

Spesso il cibercrimine attende mesi interi per stabilire infrastrutture pubblicitarie legittime, attaccare gli utenti in un momento ottimale selezionato ed entrare nelle difese basate sulla precedente reputazione. È quindi chiaro che, quando si ha a che fare con il malvertising, i sistemi di sicurezza non possono contare sulla reputazione per decidere quali annunci bloccare. È necessario invece contare su sistemi di sicurezza avanzati che classificano le proprietà del web e gli annunci pubblicitari su cui fanno affidamento in tempo reale.

Allo stesso modo, non è possibile attendere che gli "aggiornamenti della sicurezza" vengano applicati sul computer dell'utente. Potrebbe essere troppo tardi. Se il sistema di sicurezza richiede regolarmente "Fare clic per aggiornare i file delle definizioni", non sarà in grado di proteggere gli utenti, specialmente durante il fine settimana. La protezione degli utenti , a casa o in viaggio — o anche in ufficio – deve

essere fornita on-demand, e questi ultimi devono contare su sistemi di protezione basati sul tipo di sicurezza basato sul cloud offerto dalla protezione on-demand.

Crediti dell'appendice

L'appendice è opera di Dave Ewart con la collaborazione di Chris Larsen.