Your reply has been sent.

Conversation

5/7/2010 9:35 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

... sette, sei, cinque...

5/3/2010 10:08 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Hello? Is there anybody out there :-(?

Vedo che siete molto rapidi a chiedere risposte, molto meno a darle. Comodo. Mettiamola così: io inizio un conto alla rovescia: dieci, nove, otto...

4/28/2010 9:54 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Ho fatto i test richiesti con le tre ore concesse dalla versione demo di Little Snitch a anche giocando un po' con i dump di Watershark (la versione corrente di Ethereal). Al limite, se mi pagate, posso anche mandarvi un dump di tcpdump. Ma il risultato sarà sempre lo stesso: non c'è nessuna applicazione sospetta sulla mia macchina che "telefona a casa", tranne le due o tre che ho esplicitamente abilitato (update di prodotti Adobe e Google). Dunque, siamo al punto di partenza, e la palla è di nuovo nel vostro campo. Dopo aver fatto tutti questo sforzi, adesso mi piacerebbe vederne qualcuno anche da parte vostra. Ritorno dunque alle domande di sempre a cui ancora non avete risposto:

1) Avete nei log degli accessi FTP da IP sospetti intorno alle date incriminate? Posso vedere la lista di questi IP per dirvi se riconosco macchine o reti a cui posso essere stato connesso?

2) Come spiegate spiega i picchi di presenza di malware su siti ospitati su vostre macchine del 22 marzo e del 1 aprile in questo grafico:

http://www.stopbadware.org/reports/asn/31034/

Ci hanno rubato le credenziali a tutti nello stesso momento? E solo ad utenti Aruba?

M.

4/27/2010 10:14 AM - Daniele Maggini (daniele.maggini)

Subject: Codice malware in index.php

Gentile cliente,

in merito al suo nuovo Post ammetto di averle allegato il Link non corretto .. Non ho problemi ad ammetere di aver confuso i Link come da lei indicato il giusto programma da indicarle era Little Snitch :

http://www.versiontracker.com/dyn/moreinfo/macos/17642

Vengo a ribadirle il fatto che è nostra intenzione risolvere il problema in tempi brevi , nessuno vuole prenderla in giro o farle perdere del tempo.

Le posso garantire che i suoi consigli e i suoi suggerimenti non muoiono in questi post .

Mi scuso nuovamente per l'inconveniente.

Rimaniamo a disposizione.

Distinti saluti.
==========
Daniele Maggini
Help Desk
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/862000
==========

4/27/2010 9:43 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Per qualche ora ho creduto che foste delle persone serie.

Poi sono andato al link che lei mi ha fornito, quello che punta verso ZoneAlarm, immaginando che negli anni (l'ultima volta che ho usato quel software è veramente troppo tempo fa) avessero fatto una versione per Mac OS X. Macché, ZA continua a essere un prodotto per Windows solamente. Poco male, potrei sempre usare la demo di Little Snitch, mi sono detto. Ma perché dovrei farlo? Per darvi delle informazioni che non sapreste nemmeno come usare?

Daniele, ho l'impressione che lei stia cercando di spacciarmi come soluzioni le prime pagine web che trova facendo delle ricerche idiote so Google per "Mac firewall" o "Linux antivirus", senza nemmeno prendersi la briga di verificare il contenuto delle pagine che mi propone. Se questa strategia funziona con gli altri clienti che "aiuta", facendola passare per un esperto, beh, in questo invece sta facendo una pessima figura. Non solo sembra incompetente, ma anche arrogante e fastidioso nella sua presunzione. Forse farebbe bene a andare a cercare il baco dal vostro lato.

Quanto a me, il mio tempo è troppo prezioso per sprecarlo in questa caccia al tesoro casuale. Forse farò quello scan con Little Snitch, giusto per gusto personale. Quello che è certo, è che da adesso inizio a cercarmi un altro hosting. Ah, e credo che potrei mettere online questa conversazione, che ne pensa? Mi sembra un ottimo biglietto da visita per la vostra pretesa professionalità.

4/26/2010 9:34 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Daniele,

Sorvolerò sulle "spiccate conoscenze informatiche" che sembra una vaga presa in giro. Venendo ai punti specifici:

a) I codici di accesso ai domini sono controllati solo da me. Nei passati tre anni ho usato macchine diverse da quelle attuali per i trasferimenti FTP, ma tutte queste macchine era sottoposte a procedure di sicurezza piuttosto strette. Come ho cercato di spiegarle al telefono, il centro di ricerca per cui lavoro che mi fornisce l'hardware che uso anche per gestire i siti da voi ospitati è piuttosto "stretto" in termini di sicurezza. Nel caso volesse farsene un'idea, la prego di dare un'occhiata qui: http://security.web.cern.ch/security/

v) Vedi sopra. Certo potrei aver usato un computer infetto. ma è piuttosto improbabile, e in ogni caso non ho mai avuto nessun tipo di problema prima di questo episodio.

c) Non ho bisogno che mi ricordi che i virus non sono un'esclusiva Windows. Sul portatile Mac da cui sto scrivendo gira comunque un antivirus, l'unica porta aperta è la 22, e c'è un solo utente nella lista 'sudo'. Delle macchine Linux che uso non le dico nemmeno, a volte fatico persino a lavorare per quanto sono chiuse.

d) Ah, il buon vecchio ZoneAlarm. Se proprio insiste farò una prova, ma raramente ho usato un firewall più fastidioso e intrusivo di quello. Qui lo abbiamo abbandonato da tempo, Ma l'accontenterò, la tengo al corrente. Quanto alla proposta per Linux, non la capisco: a cosa dovrebbe servirmi un software di recupero dati da una partizione difettosa? Non mi sembra proprio che nessuno dei dischi condivisi che uso abbia quel problema. Ah, e comunque sono partizioni AFS, ergo quel software non andrebbe comunque bene.

Quanto alle sue domande:

1) Indirizzo Ip delle sue macchine: da casa sono in DHCP sotto la maschera 82.253.216.xx, dall'ufficio 137.138.xx.xx
2) Le rare modifiche fatte con FTP (per la gestione giornaliera uso l'interfaccia web del CMS) uso Cyberduck per Mac OS X 3.4.2, oppure ftp-0.17-23.el4_6.1 da linea di comando sulle macchine Linux che uso.
3) Wordpress 2.9.2. Vuole la lista e le versioni dei plugin?
4) Data precisa dell'infezione: ovviamente non la conosco, posso solo dirle quando l'infezione è stata notata per la prima volta, da Google o dai miei utenti. Si tratta del 30 marzo 2010.

Adesso tocca a me farle delle domande:

- Al di la della perdita delle credenziali FTP da parte degli utenti, avete qualche altra teoria o traccia?
- Come me lo spiega il picco del 22 marzo e del 1 aprile di questo grafico: http://www.stopbadware.org/reports/asn/31034/ Ci hanno rubato le credenziali a tutti nello stesso momento? E solo ad utenti Aruba?

M.

4/26/2010 5:00 PM - Daniele Maggini (daniele.maggini)

Subject: Codice malware in index.php

Gentile cliente, .

al fine di poterle essere di supporto per i problemi da lei riscontrati le chiediamo, visto le sue spiccate conoscenze informatiche, la collaborazione nell'eseguire i test e le prove indicate di seguito :

- si accerti di essere l'unico utilizzatore dei codici inerenti ai due domini , se lei avesse fornito (anche in passato) tali credenziali a terze persone tutte le verifiche e controlli effettuati possono risultare Inutili

-- Lei ha effettuato un cambio password dopo quasi tre anni . Le credenziali potrebbero essere state ricevute o fornite da terze persone con Pc infetto . Lei in passato potrebbe aver utilizzato un Pc infetto .

-- Tuttavia il Fatto di utilizzare un Mac / Linux non esclude a priori il fatto di essere infetti come può vedere di seguito alcuni articoli:

http://www.danieleargento.net/blog/?p=408

http://www.oneitsecurity.it/01/04/2010/professione-malware-analyst-intervista-a-giuseppe-bonfa/

-- In merito al software erroneamente fornito le invio due link dove può trovare lo strumento adatto alla sua postazione:

http://www.mac-net.com/386482.page

http://www.linuxdatarecovery.in/linux-data-recovery

--Infine le chiedo alcune informazioni :

1-- Indirizzo Ip delle sue macchine
2-- Le modifiche al portale vengono apportate con client ftp ? Se si mi può indicare per favore nome e versione ..
3 --Se le fosse possibile , può fornirci la versione del Cms installato al momento dell'Infezione ..
4 -- Data precisa dell'infezione

Ringraziandola per la collaborazione rimaniamo a disposizione.

Distinti saluti.

==========
Daniele Maggini
Help Desk
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/862000
==========

4/26/2010 11:03 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Buongiorno,

Pur rimanendo scettico sulla teoria del virus locale che avrebbe rubato le mie credenziali FTP, ho deciso di tentare la soluzione proposta da voi per telefono venerdì mattina. Nel tentativo, mi trovo purtroppo a dover di nuovo constatare la vostra ormai desolante incompetenza.

Al telefono mi avete infatti detto che sospettate il malware "Zeus" che sarebbe entrato in azione in una sua varante non riconosciuta dagli antivirus intorno alla fine di Marzo. Avete anche affermato che, tra i clienti che cooperano con voi nel indagini, avete trovato svariati computer Windows infettati, ma anche (cito!) "una macchina Mac", sulla quale - dopo mia richiesta di spiegazioni sulla modalità di infezione - "il malware gira come un demone", per poi "collegarsi a un database MySQL", e che avrei facilmente scoperto la presenza di questo virus sul mio portatile Mac installando il firewall Comodo, come suggerito nel vostro ultimo messaggio.

Con una rapida ricerca in rete ho purtroppo dovuto imparare che:

1) Non esistono varianti si Zeus per architetture *nix, né per Mac né per Linux. Inventatevi una teoria migliore.
2) Comodo propone prodotti per architetture Windows. E dire che ve l'ho chiesto varie volte al telefono! Vi è forse sfuggito il fatto che lavoro solo con macchine Mac e Linux?

Risultato dell'esperienza: ho l'impressione che non sappiate dove andare a parare e spariate a caso, tanto nel 95% i vostri clienti sono utenti Windows con nessuna attenzione alla sicurezza. Purtroppo nel mio caso entrambe le affermazioni non sono valide (non uso Win da anni, e ne so qualcosina di sicurezza), dunque non tentate di abbindolarmi.

Che facciamo adesso?

M.D. (sempre più esasperato)

4/23/2010 9:10 AM - Daniele Maggini (daniele.maggini)

Subject: Codice malware in index.php

Gentile cliente,

come d'accordi telefonici le invio il link :

http://personalfirewall.comodo.com/

Ringraziandola per la collaborazione rimaniamo a disposizione.

Distinti saluti.

==========
Daniele Maggini
Help Desk
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/862000
==========

4/20/2010 4:21 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Non male: 8 giorni per rispondere e chiedere un numero di telefono. E una quarta persona. Mmm, sono sempre più soddisfatto del vostro servizio.
In ogni caso: +41 76 487 86 90 (si, è un numero svizzero: lavoro all'estero). Vediamo quanto ci mettete a chiamare.
M.D.

4/20/2010 4:05 PM - Daniele Maggini (daniele.maggini)

Subject: Codice malware in index.php

Gentile cliente,

in merito alla sua segnalazione la invito a fornirci un recapito telefonico dove poterla contattare.

Rimaniamo a disposizione.

Distinti saluti.
==========
Daniele Maggini
Help Desk
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/862000
==========

4/12/2010 10:40 AM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

D'accordo, capisco. Allo stesso tempo però penso che a voi questo genere di controllo potrebbe interessare, perché vi permetterebbe di sapere subito se il malware è stato veramente piazzato con un accesso FTP usando le mie credenziali (cosa che io dubito fortemente) o sfruttando invece un qualche altro genere di vulnerabilità lato server (come sospetto). Posso dunque fornirvi la lista degli IP da qui mi collego, o perlomeno le maschere generali (a volte sono in DHCP), degli ISP che uso, e potrete verificare al volo se nell'ultimo mese ci sono connessioni da "altrove". Cerchiamo di fare qualche passo avanti, oppure sperate semplicemente che mi dimentichi dell'accaduto?

E, a proposito, a che punto sono i vostri controlli? Il ticket è stato aperto due settimane fa, mi sembra che abbiate avuto sufficiente tempo per verificare se avete un buco o se invece c'è stato un pattern di accessi con le mie credenziali da IP sospetti.

Attendo nuove, spero in tempi non biblici. M.D.

4/12/2010 10:25 AM - Marialisa Menoncin (marialisa.menoncin)

Subject: Codice malware in index.php

Gentile cliente,
la informiamo che, come da Contratto, non ci è possibile fornirle i log richiesti.

Le comunichiamo che tali Log possono essere richiesti solo ed esclusivamente dalle Autorià Giudiziarie.

Restiamo a disposizione per eventuali chiarimenti.

Distinti saluti.
==========
Marialisa Menoncin
Technical Department
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/862000
==========

4/9/2010 3:33 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Buongiorno,

non dubito dell'esistenza di questo genere di virus, semplicemente mi sento di escludere questo genere di problema da parte mia.

È possibile avere i log di accesso FTP al server su cui sono ospitato, con gli IP di provenienza delle connessioni? Sarebbe piuttosto semplice verificare se c'è qualche connessione sospetta (conosco piuttosto bene gli IP delle macchine da cui lavoro) oppure no.

E mi interesserebbe anche avere una history del file incriminato (index.php), che non dovrebbe essere troppo complessa da ricostruire visto che ho sottoscritto l'opzione di backup.

Attendo notizie. M.D.

4/9/2010 3:14 PM - Paolo Dolci (paolo.dolci)

Subject: Codice malware in index.php

Gentile cliente,

ci scusiamo per la risposta e la informiamo che sono state effettuate tutte le verifiche del caso e sono ancora in corso ulteriori controlli al fine di individuare la causa di tale problematica.

I consigli forniti nella precedente risposta sono comunque validi e la informiamo che anche altri provider hanno avuto problematiche simili scaturite da virus che "rubano" le credenziali di accesso dai Client Ftp dei Clienti.

Non appena saranno ultimati tali controlli provvederemo ad aggiornare i nostri Clienti in merito a tale situazione.

Restiamo a disposizione per eventuali chiarimenti.

Distinti saluti.
==========
Paolo Dolci
Technical Department
http://www.aruba.it
http://assistenza.aruba.it
n° centralino: 0575/0505
n° fax: 0575/862000
==========

4/8/2010 5:50 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Buongiorno,

Non so perché ma mi sento vagamente trattato da imbecille.

Gestisco il mo sito alternativamente da un portatile che gira Mac OS X un desktop che gira Linux. Se vi interessano i dettagli di entrambe posso farveli avere, ma credo il concetto di base sia chiaro: non me ne faccio nulla del vostro programmino antivirus. E continuo fortemente a dubitare che il problema possa essere "lato Client".

Insisto, verificate meglio, perché la rete dice chiaramente che a fine marzo decine di siti ospitati da voi hanno avuto lo stesso problema. Scaricare la responsabilità gratuitamente sul cliente non vi sta facendo fare una bella figura.

M,

P.S. se proprio insistete posso mandarvi uno screenshot di un antivirus per Mac of per Linux girato sulle macchine che uso, ma lo sapere già che cosa vi dirà, vero?

4/6/2010 4:22 PM - Paolo Dolci (paolo.dolci)

Subject: Codice malware in index.php

Gentile cliente,

ci scusiamo per il ritardo nel risponderle.

In merito alla sua segnalazione la invitiamo ad effettuare una scansione della postazione dalla quale gestisce il suo sito con il software da noi indicato nella precedente risposta.

La preghiamo di effettuare una scansione completa ed indicarci se vengono individuati virus/trojan o similari nella sua postazione in quanto dalle nostre verifiche riteniamo che il problema sia lato Client.

Qualora così fosse la invitiamo ad fornirci lo screenshot dei risultati della scansione dal quale poter vedere quali virus erano presenti.

Restiamo a disposizione per eventuali chiarimenti.

Distinti saluti.
==========
Paolo Dolci
Technical Department
http://www.aruba.it
http://assistenza.aruba.it
n° centralino: 0575/0505
n° fax: 0575/862000
==========

4/1/2010 12:30 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php

Buongiorno.

La vostra (decisamente insoddisfacente!) risposta segnalerebbe che avrei ancora "alcuni file nei quali è stato inserito un Javascript malevolo". Di grazia, quali file? Li avete ripuliti voi? Mi dite quali sono perché possa farlo io? Perché l'unico che ho trovato è stato pulito da me, se ce ne fossero altri che mi sono sfuggiti mi piacerebbe sapere quali sono. O avete semplicemente fatto un copia-e-incolla della risposta standard?

Quanto al resto, dite "invitiamo a verificare di non avere script non aggiornati all'interno del suo dominio". Grazie per la banalità, mi sembra di aver scritto esplicitamente di non aver nessun CMS non aggiornato che gira su questo dominio! Ergo, o qualcuno ha uno 0-day exploit, o qualcuno mi ha soffiato la password FTP, o avete un problema voi! Siccome da quello che leggo in rete non sono il solo ospitato sulle vostre macchine ad avere subito questo attacco, ritengo improbabile che le credenziali di svariati clienti siano state acquisite tutte nello stesso momento. Come la mettiamo?

Attendo notizie. M.D.

4/1/2010 12:14 PM - Aldo Giusto (aldo.giusto)

Subject: Codice malware in index.php

Gentile Cliente,

in merito alla sua segnalazione abbiamo effettuato le opportune verifiche individuando alcuni file nei quali è stato inserito un Javascript malevolo.

Abbiamo effettuato dei controlli approfonditi presso il Server dove è ospitato il suo sito senza rilevare la presenza di eventuali problemi o accessi non autorizzati e pertanto la invitiamo a verificare di non avere script non aggiornati all'interno del suo dominio assicurandosi di avere sempre installate le ultime versioni degli script usati in modo che terze persone non possano usare eventuali buchi di sicurezza delle applicazioni per accedere al suo spazio web.

Si assicuri inoltre di non avere nel sito dei Form non "protetti" che possano essere usati sempre da terzi per accedere al suo spazio web, ecc. ecc..

Al fine di evitare il ripresentarsi di tali situazioni la invitiamo a consultare periodicamente siti di sicurezza quali

www.secunia.com
www.securityfocus.com

dove vengono rese note le nuove vulnerabilità scoperte per gli script da lei utilizzati nel suo sito.

Per una sua maggiore sicurezza la invitiamo ad effettuare un cambio della password di gestione inerente la login@aruba.it accedendo presso il nostro sito on line all'indirizzo

http://hosting.aruba.it/areaclienti/CambioPassword/CambioPassword_Richiesta.asp

La nuova Password deve mantenere i seguenti criteri:
- lunghezza compresa fra 8 e 13 caratteri;
- formato alfanumerico (deve quindi contenere sia lettere che numeri)
- diversa dalle password utilizzate in precedenza

Per cambiare le credenziali del MySQL, invece, faccia riferimento al seguente link:

http://kb.aruba.it/KB/a1111/cambio-password-database-mysql-e-ms-sql.aspx?KBSearchID=0

Le consigliamo caldamente di effettuare un controllo del suo PC per assicurarsi che non vi siano Trojan, Keylogger, Malware i quali, una volta che ha effettuato il cambio della password, possano "rubarle" i dati di gestione del suo dominio ed altri dati sensibili presenti nel suo PC causando spiacevoli situazioni. A tale scopo le consigliamo di utilizzare il software MalwareBytes reperibile in versione Free al seguente link:

http://majorgeeks.com/download.php?det=5756

Una volta effettuate tali operazioni le basterà ripubblicare tutte le pagine web che compongono il suo dominio per ripristinare correttamente la visibilità del suo sito.

Al fine di far rimuovere l'avviso di "Sito potenzialmente pericoloso" da Google è necessario che richieda un nuovo controllo da parte di Google. Per richiedere ciò la invito a consultare il seguente link che indica come eseguire tale richiesta:

http://www.google.com/support/webmasters/bin/answer.py?answer=45432

Restiamo a disposizione per eventuali chiarimenti.

Distinti saluti.
==========
Aldo Giusto
Help Desk
http://www.aruba.it
http://assistenza.aruba.it
Call center: 0575/0505
Fax: 0575/515790
==========

3/31/2010 4:47 PM - marco.delmastro@gmail.com

Subject: Codice malware in index.php
Attachments: index.hacked.php

Buongiorno,

il file index.php nella root di www.borborigmi.org e di www.stornellidesilio.it sono stati entrambi recentemente infettati con una riga di malicious code (che trovate in attachment). Me ne sono accorto perché entrambi i siti hanno triggerato i controlli anti-malware di Google.

Ho provveduto a eliminare il frammento di codice incriminato. Nessun altro file sui due domini risulta compromesso, ma ho comunque re-installato una versione fresca di Wordpress. Ho già anche cambiato la password FTP.

Ho l'impressione che il problema non sia legato a una cattiva amministrazione da parte mia (i permessi dei file erano a posto, Wordpress updatato all'ultima versione), e leggo in giro che molti altri siti ospitati sui vostri server condivisi hanno avuto recentemente problemi simili. Potete per favore farmi sapere come state affrontando la situazione, e se il problema rischia di ripresentarsi in futuro.

Grazie, cordialmente, Marco Delmastro