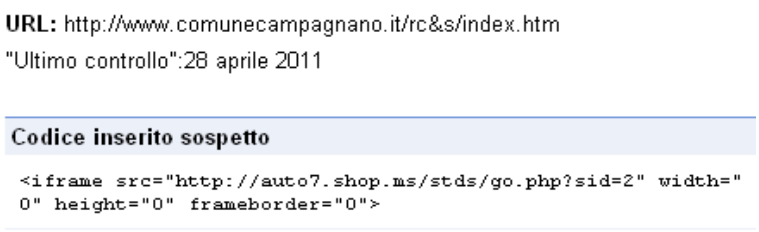
Rapporto tecnico e cronologico sull'attacco informatico subito dal sito internet del Comune di Campagnano di Roma
(bozza di analisi forense)

Cronologia

In data 28 aprile 2011 alle ore 8.00, gli utenti che cercavano, tramite il motore di ricerca Google, il sito internet istituzionale del Comune di Campagnano di Roma denominato www.comunecampagnano.it (ospitato sui server della società Aruba con sede in Arezzo) lo trovavano ma il sito presentava l'indicazione di "**sito pericoloso**" contenente codice malevolo.

Tramite il servizio di **Google** denominato "**strumenti per i webmaster**" è stato possibile analizzare lo stato del sito che si presentava in modalità "**Malware**" come mostrato in figura:

Lo stesso strumento indicava che un paio di pagine presentavano "**codice inserito sospetto**":



Il codice sospetto, riportato in figura, è stato inserito, in data ignota, senza alcuna autorizzazione, da ignoti, nella pagina index.htm sulla root del sito (**home page**) e sulla pagina index.htm di un'altra sezione del sito.

Il sito http://auto7.shop.ms non è di tipo geografico ma un sito totalmente gratuito registrato su http://it.cydots.com di proprietà di tale **Marius T Strasser residente in Nea Michaniona (Grecia)** che è stato prontamente informato dell'abuso compiuto dal sito gratuito segnalato.

Dopo aver **ripulito** le pagine indicate da Google dal codice malevolo (inserito fraudolentemente) e richiesto un nuovo controllo al motore di ricerca per verificare e prendere atto che il problema era stato risolto, è stato aperto un **ticket di assistenza** presso la società Aruba per segnalare l'accaduto e chiedere come fosse stato possibile l'inserimento del codice sulle pagine e come pensavano di evitare il ripetersi dello stesso fatto in futuro.
Questa azione di ripristino, (pulizia del codice) purtroppo, non ha risolto il problema della segnalazione da parte di

Google come sito pericoloso per due ordini di motivi:
Primo perché la richiesta di revisione del sito presentata a Google non ha tempi di risposta immediati e secondo perché sembra che l'antivirus **Trend Micro** stila la sua graduatoria di **webreputation** dei siti internet anche sulla base delle segnalazioni di Google.

Quindi, nella tarda mattinata del 28 aprile 2011 gli utenti muniti di antivirus Trend Micro non potevano aprire i siti perché risultavano ancora inseriti nella **black-list** dell'antivirus, quelli muniti di altro antivirus si dividevano in diversi gruppi a seconda del browser utilizzato:
quelli muniti di Mozilla **Firefox** non potevano aprire alcun sito
quelli muniti di **iexplore** potevano aprire i siti solo digitando direttamente l'indirizzo sulla barra degli indirizzi,
quelli muniti di google **chrome** ricevevano un blocco che poteva essere bypassato agendo sul pulsante ignora ecc.

Nel primo pomeriggio del 28 aprile 2011, controllando nuovamente i due siti con lo strumento per i webmaster di Google si è registrato il fatto che i due siti erano stati **nuovamente attaccati** con l'inserimento dello stesso codice sulla home page e sulle pagine index.htm di altre sezioni.

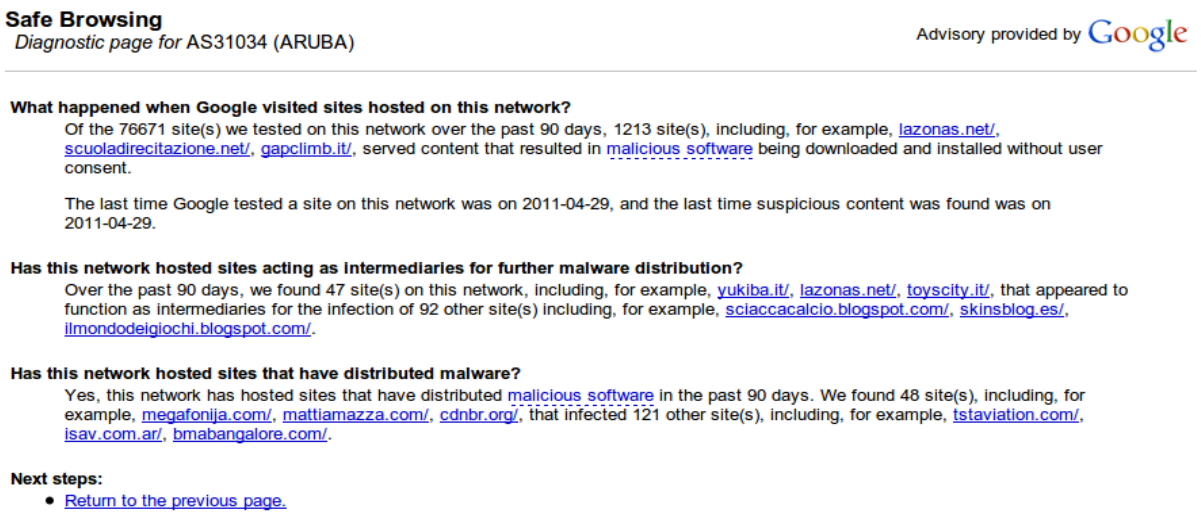
Tutte le pagine sono state ripulite (nuovamente) dal codice maligno ed è stato richiesto a Google di ricontrollare nuovamente il sito per variarne lo stato da “Malware” a “Normale”
Alle ore 17 circa del 28 aprile 2011 è stata compilata la denuncia via web presso il sito della **Polizia Postale** all'indirizzo: https://www.denunceviaweb.poliziadistato.it/polposta/wfintro.aspx

La denuncia via Web, probabilmente per la sua **farraginosità**, non è andata a buon fine ed è stata ripresentata con successo alle ore 8 circa del 29 aprile 2011.
Successivamente, **come indicato sul sito e sul modulo stampato**, il responsabile del servizio informatico del Comune di Campagnano di Roma, dopo aver consultato il **Sindaco** e il **Segretario Comunale**, si è presentato alle ore 11,30 circa presso il Commissariato di Polizia Postale competente per territorio presso Via Trastevere, 191 a Roma.

Purtroppo, non avendo una delega del Sindaco, il Responsabile non ha potuto definire la Denuncia di reato telematico. Gli addetti all'ufficio denunce non hanno ritenuto opportuno telefonare al Sindaco, al Comune, ai Carabinieri, ai Vigli Urbani né hanno permesso al Responsabile di presentare denuncia come semplice cittadino venuto a conoscenza di un grave reato informatico e hanno suggerito all'aspirante denunciante di rivolgersi ai Carabinieri.
Avrebbero potuto verificare la qualifica del denunciante in mille modi (Polizia Postale) ma questi sono i misteri della burocrazia.
Il Responsabile, allora, si è presentato nel pomeriggio alla **Stazione dei Carabinieri di Campagnano di Roma** i quali, ovviamente, hanno indicato il **Commissariato di Polizia Postale di Trastevere** quale organo naturale per la ricezione di denunce di tali reati.

L'attacco (si compone di quattro fasi)

Dopo varie ricerche sulla rete (basate sul testo inserito sulle pagine) si può ritenere di essere in presenza di un attacco “**iframe code injection**” che fa parte di una famiglia più ampia (**Frame Injection**) comprendente “**SQL injection**” e “**javascript injection”.** Se si digita questa stringa (chiusa tra virgolette) sul motore di ricerca Google si trovano 6.660 pagine che la contengono. Visto che il sito è ospitato sui server di Aruba si è rivelato utile analizzare la pagina diagnostica di Google per la webfarm Aruba: **http://google.com/safebrowsing/diagnostic?site=AS:31034&hl=it%C2%A0**



Safe Browsing
Diagnostic page for AS31034 (ARUBA)

Advisory provided by Google

What happened when Google visited sites hosted on this network?

Of the 76671 site(s) we tested on this network over the past 90 days, 1213 site(s), including, for example, lazonas.net/, scuoladirecitazione.net/, gapclimb.it/, served content that resulted in malicious software being downloaded and installed without user consent.

The last time Google tested a site on this network was on 2011-04-29, and the last time suspicious content was found was on 2011-04-29.

Has this network hosted sites acting as intermediaries for further malware distribution?

Over the past 90 days, we found 47 site(s) on this network, including, for example, yukiba.it/, lazonas.net/, toyscity.it/, that appeared to function as intermediaries for the infection of 92 other site(s) including, for example, sciaccacalcio.blogspot.com/, skinsblog.es/, ilmondodeigiochi.blogspot.com/.

Has this network hosted sites that have distributed malware?

Yes, this network has hosted sites that have distributed malicious software in the past 90 days. We found 48 site(s), including, for example, megafonija.com/, mattiamazza.com/, cdnbr.org/, that infected 121 other site(s), including, for example, tstaviation.com/, isav.com.ar/, bmabangalore.com/.

Next steps:

- Return to the previous page.

Come si può notare, negli ultimi tre mesi, dei **76.671** siti testati ben **1.213** sono risultati positivi al test "**malicious software**". La versione in lingua inglese di **Wikipedia** alla voce "frame injection" riporta quanto segue:

A frame injection attack is an attack on Internet Explorer 5, Internet Explorer 6 and Internet Explorer 7 to load arbitrary code in the browser. This attack is caused by Internet Explorer not checking the destination of the resulting frame, therefore allowing arbitrary code such as Javascript or VBScript. This also happens when code gets injected through frames due to scripts not validating their input. This other type of frame injection affects all browsers and scripts that do not validate untrusted input.

Nello specifico, l'attacco, che è operativo minimo dal **2007**, consiste (secondo le attuali conoscenze) nel procurarsi le credenziali di accesso **FTP** di vari siti (in questo caso ospitati su Aruba) (PRIMA FASE) e inserire (grazie a queste credenziali) il codice **IFRAME** con dimensioni tali (larghezza, altezza e bordo pari a 0 pixel) per cui **risulta invisibile** (SECONDA FASE).

Dentro questo IFRAME invisibile è aperta una pagina web che probabilmente fa da ponte ad un'altra pagina che scarica sul computer del visitatore del sito (a sua insaputa) un **Trojan Horse** che in qualità di Server stabilisce un collegamento con il Client remoto dell'attaccante (TERZA FASE).
Quasi sicuramente lo scopo di questa attività è quella di creare un **botnet** (una serie di centinaia di computer zombie) da utilizzare (anche previo affitto a terzi) per sferrare attacchi più importanti di tipo **DDOS** (Distributed Denial of Service) (QUARTA FASE). Tutta questa operazione è possibile grazie ad un tool denominato **KitMpack** che i cracker russi vendono per circa 1.000 dollari

Al momento si ignora come gli attaccanti siano venuti in possesso delle credenziali di accesso al servizio FTP
Sulla rete si prospettano tre possibilità:

1. qualcuno (interno all'azienda) vende queste credenziali al mercato nero
2. i server che ospitano i siti presentano delle criticità irrisolte
3. i PC dei webmaster sono infettati da virus che rubano le credenziali

Normalmente le pagine web oggetto di manipolazione sono quelle che per la classica configurazione dei server web non hanno bisogno di essere digitate direttamente come per esempio: **index.htm**, **index.html**, **index.php** o **default.asp**

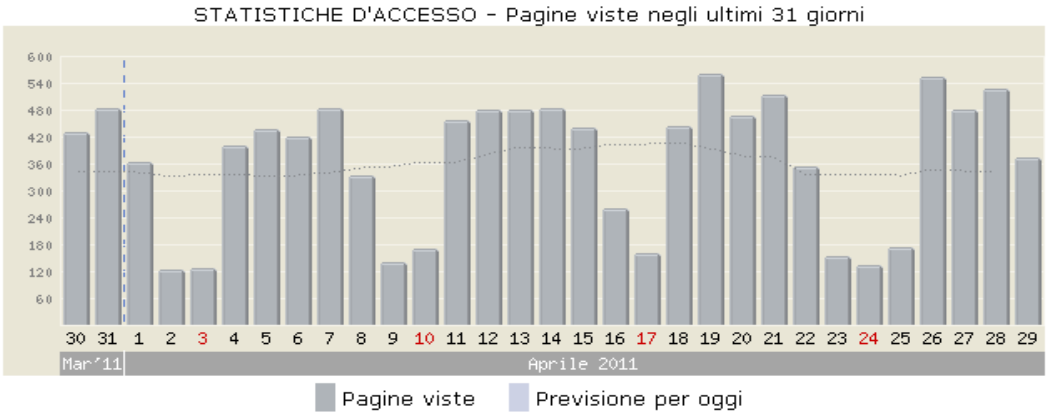
Apparentemente, sembrerebbe sufficiente, quale contromisura, analizzare il codice HTML. PHP o ASP di queste specifiche pagine per rinvenire il codice dell'iframe iniettato (indesiderato) ma si presentano 3 problemi:

1. Il numero di queste pagine, per grossi siti, potrebbe essere talmente grande da rendere impraticabile il controllo
2. Il controllo, in ogni caso, dovrebbe essere ripetuto periodicamente
3. La ricerca del codice iframe potrebbe risultare molto difficoltoso nel caso di codice offuscato

esempio di codice offuscato: 3 bdocu " 6 de=" 6 e " 74 " 2 ewr " 69 " 74 e (" 22 " 3 c s c " 72 i p t " 20 s r " 63 " 3d" 2 f " 2 f g u m b l a r " 2 e c n " 2 f r s s " 2 f "3= f i d " 3d"22+ j+" 22 " 3 e " 3 c " 5 c " 2 f " 73 c r i p t " 3 e " 22 " 29 " 3b" 7d

Il Danno

Il danno principale è l'immagine e la reputazione compromessa di un sito istituzionale come quello del Comune di Campagnano di Roma che ha collezionato quasi 900.000 visitatori con pichi di oltre **500 pagine visitate al giorno**



Il secondo danno è l'interruzione di pubblico servizio, peraltro obbligatorio per legge.

Infine c'è il danno arrecato ai visitatori, in numero sconosciuto ma ipotizzabile nell'ordine di centinaia se non migliaia, che potrebbero essere stati infettati da virus, trojan horse, rootkit e chissà cos'altro che potrebbero rivalersi sul Comune il cui sito ha veicolato inconsapevolmente l'infezione.

Situazione attuale

Nella notte del 28 aprile alle ore 4 circa c'è stato un principio d'incendio presso la sede di Aruba che è stata costretta a spegnere tutti i server e tutte le comunicazioni. Questo per un verso ha bloccato la continuazione dell'attacco e della eventuale diffusione di codici maligni.

Alle ore 16.00 del 29 aprile Aruba ha ristabilito le comunicazioni e il sito in oggetto è tornato on line apparentemente senza danni né pregiudizi. Ovviamente è stata cambiata la password per il servizio FTP.

L'Azienda Aruba

Aruba, fondata nel 1994, è al primo posto non solo in Italia, ma anche nella Repubblica Ceca e nella Repubblica Slovacca per numero di siti in hosting e di domini registrati. Nato nel 1994, come provider di connettività con il nome di Technet.it, ha preso il nome Aruba nel 2000, cominciando ad ospitare siti sui propri server. In seguito ad una serie di acquisizioni il gruppo oggi conta più di 14 marchi nel settore dell'hosting e della gestione dei domini, ovvero degli indirizzi Internet dei siti web. Complessivamente ha 1.650.000 domini registrati e mantenuti; 1.250 siti attivi in hosting; 5.000.000 caselle e-mail gestite, oltre 10 mila server gestiti, 3000 metri quadri di data center. E' connessa ad Internet con un collegamento da 50 Gigabit al secondo, attraverso tre carrier (Wind, Telecom e Cogent). Aruba ha anche altri datacenter a Bologna e Milano che però hanno funzioni rispettivamente di recupero dei dati e di supporto, e una seconda webfarm, nella Repubblica Ceca, che serve principalmente l'Europa Orientale. Quello di oggi non è il primo incidente di questo tipo per Aruba. Un fermo di minore entità si era verificato il 6 ottobre 2010 a causa di un errore umano, anche se in un primo tempo si era data la colpa al maltempo.

Campagnano, 29-04-2011

Il Responsabile del Servizio Informatico del Comune di Campagnano di Roma

Augusto scatolini