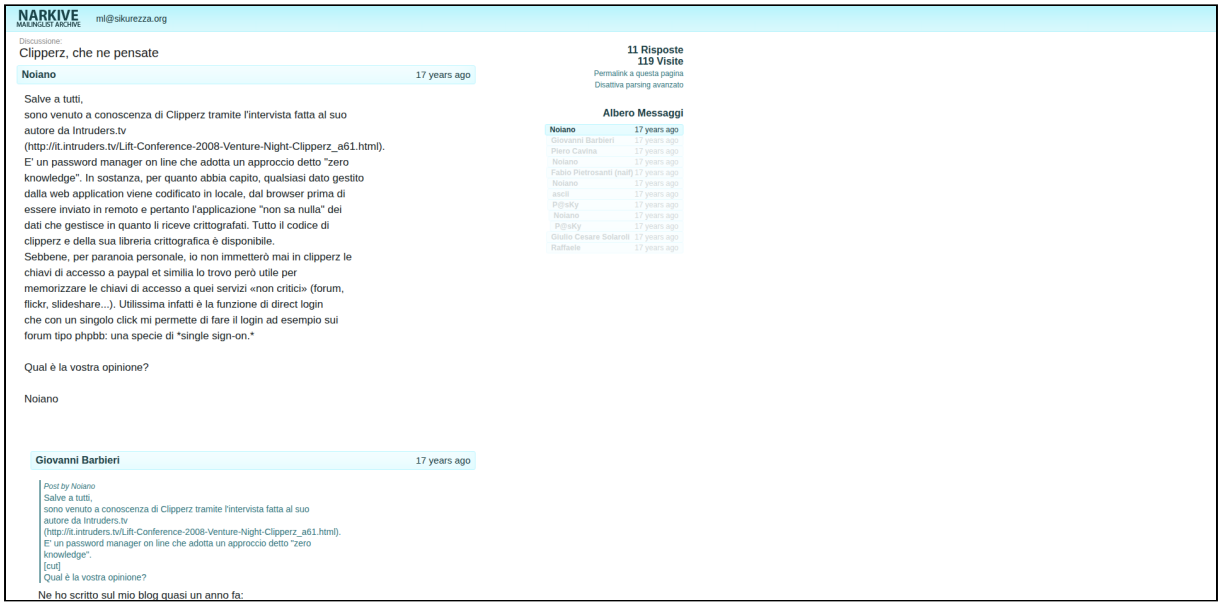
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot



Clipperz, che ne pensate

Noiano 17 years ago

Salve a tutti,
sono venuto a conoscenza di Clipperz tramite l'intervista fatta al suo
autore da Intruders.tv
(http://it.intruders.tv/Lift-Conference-2008-Venture-Night-Clipperz_a61.html).
E' un password manager on line che adotta un approccio detto "zero
knowledge". In sostanza, per quanto abbia capito, qualsiasi dato gestito
dalla web application viene codificato in locale, dal browser prima di
essere inviato in remoto e pertanto l'applicazione "non sa nulla" dei
dati che gestisce in quanto li riceve crittografati. Tutto il codice di
clipperz e della sua libreria crittografica è disponibile.
Sebbene, per paranoia personale, io non immetterò mai in clipperz le
chiavi di accesso a paypal et similia lo trovo però utile per
memorizzare le chiavi di accesso a quei servizi «non critici» (forum,
flickr, slideshare...). Utilissima infatti è la funzione di direct login
che con un singolo click mi permette di fare il login ad esempio sui
forum tipo phpbb: una specie di *single sign-on.*

Qual è la vostra opinione?

Noiano

Giovanni Barbieri 17 years ago

> *Post by Noiano*
> Salve a tutti,
> sono venuto a conoscenza di Clipperz tramite l'intervista fatta al suo
> autore da Intruders.tv
> (http://it.intruders.tv/Lift-Conference-2008-Venture-Night-Clipperz_a61.html).
> E' un password manager on line che adotta un approccio detto "zero
> knowledge".
> [cut]
> Qual è la vostra opinione?

Ne ho scritto sul mio blog quasi un anno fa:
http://www.giovy.it/2007/05/23/clipperz-online-password-manager/, e
l'opinione è che puoi lasciarci tranquillamente anche la password di
PayPal (ed io c'ho anche le info finanziarie, figurati).
Ho conosciuto personalmente il CEO di Clipperz ed ho avuto modo di
seguire una sua presentazione sull'architettura dell'applicazione
durante un BarCamp e... da parte mia c'è un trust totale.
Per buon conto, inoltre, c'è la trasparenza nel rendere visibile i
sorgenti dell'applicazione. Ergo... ;)

Saluti,

--
Giovanni Barbieri aka Giovy - www.giovy.it

Piero Cavina 17 years ago

> *Post by Noiano*
> Salve a tutti,
> sono venuto a conoscenza di Clipperz tramite l'intervista fatta al suo
> autore da Intruders.tv
> Qual è la vostra opinione?

L'impressione è positiva, quello che mi lascia un po' perplesso è che
un servizio del genere è molto utile per un utilizzo "nomade", vale a
dire su computer pubblici, o di altre persone, che però sono fuori dal
nostro controllo.
Inserireste le credenziali per accedere a tutte le vostre password, su
un computer del quale non sapete nulla? Ci sono dei troiani che
inviano al server dell'attaccante i dati di login prima della
cifratura ssl se non ricordo male.
Poi ovviamente dipende dall'uso che se ne fa e dal nostro grado di paranoia...

--
Ciao,
P

Noiano 17 years ago

...

Credo che più preoccupanti dei troiani siano i keylogger che potrebbero
rivelare la passphrase. Un troiano, per quanto ho capito, se anche
riuscisse a sniffare il traffico prima della cifratura SSL ottterrebbe
comunque solo roba cifrata dal browser tramite l'applicativo scritto in
javascript.
Per quanto riguarda l'accesso da postazioni pubbliche io personalmente
sono molto paranoico perchè le pochissime volte che ne ho utilizzata
qualcuna mi sono trovato con gente nel cui vocabolario non vi era
traccia di parole come «sicurezza» o «prevenzione».

Saluti

Noiano

Fabio Pietrosanti (naif) 17 years ago

> *Post by Noiano*
> Sebbene, per paranoia personale, io non immetterò mai in clipperz le chiavi di accesso a paypal et similia lo trovo però utile per memorizzare le chiavi di accesso a quei servizi «non critici» (forum, flickr, slideshare...). Utilissima infatti è la funzione di direct login che con un singolo click mi permette di fare il login ad esempio sui forum tipo phpbb: una specie di *single sign-on.*
> Qual è la vostra opinione?

Che non esiste un meccanismo tecnologico che permetta di validare che il codice javascript caricato sia esente da backdoor o che questa possa essere introdotta dinamicamente su richiesta da parte di "terzi".

Che le mie password non mi sognerei mai di salvarle su di un database diverso dal file cifrato che tengo sul mio computer.

Esporre *tutte* le proprie credenziali di accesso a distanza di "una password" non lo considero un rischio accettabile, sopratutto quando una vulnerabilità potenziale semplice come un XSS le metterebbe a rischio di disclosure.

Saluti

Fabio Pietrosanti

_____
http://www.sikurezza.org - Italian Security Mailing List

Noiano 17 years ago

> *Post by Fabio Pietrosanti (naif)*
> Che non esiste un meccanismo tecnologico che permetta di validare che il codice javascript caricato sia esente da backdoor o che questa possa essere introdotta dinamicamente su richiesta da parte di "terzi".

Per quanto ho potuto notare tutto il sistema di cifratura/decifratura in javascript viene consegnato al client sotto connessione SSL. Il certificato SSL non potrebbe fungere come una specie di validazione nell'ipotesi di fidarsi del sistema (il cui codice è tra l'altro disponibile)? Mi pare di capire che ci vorrebbe una specie di firma digitale come avviene per gli applet java?

> *Post by Fabio Pietrosanti (naif)*
> Che le mie password non mi sognerei mai di salvarle su di un database diverso dal file cifrato che tengo sul mio computer.

Su questo concordo con te: infatti su clipperz ho salvato solo credenziali «low risk» come quelle di alcuni forum per beneficiare del direct login. Il resto lo tengo sotto chiave utilizzando keepassx (linux). A proposito conoscete alternative migliori?

> *Post by Fabio Pietrosanti (naif)*
> Esporre *tutte* le proprie credenziali di accesso a distanza di "una password" non lo considero un rischio accettabile, sopratutto quando una vulnerabilità potenziale semplice come un XSS le metterebbe a rischio di disclosure.

Come sopra :-P

Grazie per le risposte.

Noiano

ascii 17 years ago

> *Post by Fabio Pietrosanti (naif)*
> Che le mie password non mi sognerei mai di salvarle su di un database diverso dal file cifrato che tengo sul mio computer.

non ti credo, more info please

> *Post by Fabio Pietrosanti (naif)*
> Esporre *tutte* le proprie credenziali di accesso a distanza di "una password" non lo considero un rischio accettabile, sopratutto quando una vulnerabilità potenziale semplice come un XSS le metterebbe a rischio di disclosure.

ho dato un occhio al source, ci sono degli accorgimenti meritevoli ma penso anche io che un browser non sia lo strumento adatto per gestire informazioni a cui teniamo molto (cosa? succede gia'?)

ad ogni modo il payload di tale fantomatico xss dovrebbe fare qualcosa di simile a

---

```
alert(document.domain);

function ohmy(searchClass) {
var classElements = new Array();
node = document;
```

```
tag = 'input';
var els = node.getElementsByTagName(tag);
var elsLen = els.length;
var pattern = new RegExp("(^|\\\\s)"+searchClass+"(\\\\s|$)");
for (i = 0, j = 0; i < elsLen; i++) {
if ( pattern.test(els[i].className) ) {
classElements[j] = els[i];
alert(els[i].value);
j++;
}
}
}

ohmy("scrambledField");
```

---

http://tinyurl.com/preview.php?num=2j54av (solo per facilitarvi il copia/incolla, se lo cliccate verra' eseguito nel dominio sbagliato e non funzionera')

aprite il link, clicco destro su "Proceed to this site", copy url destination, aprite clipperz, incollate nella barra degli indirizzi, fatto (testato con ff, se usate qualcosa di diverso tipo amaya potrebbe non funzionare)

ora questo codice potrebbe finire dentro la same origin giusta in vari modi

- un xss su clipperz.com reflected o stored che sia
- un xss sulla componente "clientside" su clipperz.com (dom xss)
- un xss sulla componente "clientside" su file:// nel caso si usi la versione "scaricabile" (dom xss)

e fino a qui sarebbe responsabilita' di clipperz

- grazie a qualche vulnerabilita' client del browser
- grazie a qualche uxss di un plugin (vedi uxss sui pdf di Wisec)
- grazie a qualche xss dom o xul di un plugin

e sarebbe responsabilita' del vostro browser/estensioni/plugin ma anche vostra nel caso in cui vi siate dimenticati di aggiornare

- tramite un xss di un'applicazione che gira su localhost se un malaugurato giorno gli admin di clipper creassero un record A sfortunato

http://www.securityfocus.com/archive/1/486606

- tramite un xss dom di qualche documento che sta su file:// nel caso della versione scaricabile

e le responsabilita' sarebbero miste

certo un xss e' una vulnerabilita' stupida e semplice da trovare anche sui domini dei singoli account protetti da pass ma la same origin fa si che si debba essere exploitati singolarmente su ogni dominio al posto che una volta per tutti, a meno che ad essere compromesso non sia stato il client

questo rimanendo nell'ambito dell'esecuzione di js "indesiderato" e tralasciando tutti gli altri metodi (troiani, keylogger, whatever, whenether)

riassumendo: per me ci sono troppi "se" e personalmente credo che contro un attaccante remoto sono piu' sicuro con un bel file .txt in chiaro nella home di un utente creato appositamente col giusto chmod

pero' il file txt non ha le features di clipperz e quindi penso che un utente scelga clipperz per queste ultime piuttosto che la sicurezza

scusate se sono stato lungo ma non avevo proprio nulla di meglio da fare :)

ciao,
Francesco `ascii` Ongaro
http://WWW.ush.it/

> *Post by Fabio Pietrosanti (naif)*
> Che le mie password non mi sognerei mai di salvarle su di un database
> diverso dal file cifrato che tengo sul mio computer.

A dire il vero personalmente non le ho neanche salvate in nessun
file cifrato o meno, ho un buon buffer di memoria nel mio cervello
che riesce a contenere password minimo di 16 caratteri alfanumerici
con caratteri speciali e ne imparo sempre di nuove con un buon
generatore di password per tutti i server, router, etc, che gestisco,
piu' sicuro per me, piu' sicuro per tutti, il file cifrato devo
necessariamente salvarlo da qualche altra parte e fare un backup,
be' si certo se perdo la memoria allora perdo tutto, ma a quel
punto credo che non mi serviranno neanche piu', al momento quel
giorno e' ancora molto, ma molto lontano... almeno spero....;)

Concordo sulla scarsa sicurezza del Clipperz in oggetto, poiche'
tra troiani e keyloggers non c'e' molto da starsene tranquilli,
quindi personalmente e' scartato in partenza fosse solo per
la password di un videogame da 2 centesimi, la paranoia e'
sempre una virtu'....

Ciao.
--
***@sKy

Makkinista - Fuokista

GPG/PGP keys available via keyservers http://pgpkeys.mit.edu:11371/
DSA: 6CBE 6982 5C10 CFF0 D676 6420 C1C5 B8EC 8690 0F88
RSA: 40 6B 54 8C 20 A0 F6 0B 4C 96 AA 34 D3 FB DC 8C

_____
http://www.sikurezza.org - Italian Security Mailing List

Noiano 17 years ago

...

Ehm potresti illuminarmi su come fai a memorizzare password siffatte?
Esiste qualche metodo particolare...per quanto ne so io le password non
devono avere senso in nessuna lingua, e non devono essere in alcun modo
riconducibili alla persona...va da se il fatto che devono essere
presenti caratteri speciali etc...

> *Post by ***@sKy*
> Concordo sulla scarsa sicurezza del Clipperz in oggetto, poiche'
> tra troiani e keyloggers non c'e' molto da starsene tranquilli,
> quindi personalmente e' scartato in partenza fosse solo per
> la password di un videogame da 2 centesimi, la paranoia e'
> sempre una virtu'....
> Ciao.

Non vorrei sembrare polemico ma avere troiani o keylogger sul pc non ha
nulla a che vedere, IMHO, con la sicurezza di Clipperz come
applicazione. Avere un pc infetto con quelle diavolerie mette qualsiasi
dato in pericolo sia che si tratti del numero di scarpa che del numero
di conto corrente.
Sono totalmente daccordo, invece, sul fatto che la paranoia sia una
virtù :-)

Noiano

P@sKy 17 years ago

> *Post by Noiano*
> Ehm potresti illuminarmi su come fai a memorizzare password siffatte?
> Esiste qualche metodo particolare...per quanto ne so io le password non
> devono avere senso in nessuna lingua, e non devono essere in alcun modo
> riconducibili alla persona...va da se il fatto che devono essere
> presenti caratteri speciali etc...

Certo le password generate hanno tutte le caratteristiche che
stai elencando, in fondo e' "solo" un semplice esercizio memorico
non servono particolari doti (come quando alle elementari
imparavamo a memoria qualche poesia), magari associare pezzi
di password ad oggetti, spesso utilizzo il dialetto pugliese
del mio borgo natio per le parole e come dire quelle non le
trovi in nessun dizionario ;), certo se si fanno attacchi a
forza bruta non c'e' dialetto che tenga, ma se le cambi ogni
settimana la vedo un bel po' dura, la condizione sufficiente
e' quella di avere una buona memoria ed utilizzare un buon
generatore di password (pwgen) nient'altro, magari usando
combinazioni rispetto a quelle generate in precedenza, il
caos deve avere il suo peso ;)..

Comunque questo e' un esempio di pwgen
[***@kalashnikov ~]# pwgen -s 16
T/*kEuwSasB4,n!0

Per me questa password e' facile da memorizzare, magari la
stravolgo un po' con qualche termine dialettale, la la
robustezza resta intatta....

> *Post by Noiano*
> Non vorrei sembrare polemico ma avere troiani o keylogger sul pc non ha nulla a che vedere, IMHO, con la sicurezza di Clipperz come applicazione. Avere un pc infetto con quelle diavolerie mette qualsiasi dato in pericolo sia che si tratti del numero di scarpa che del numero di conto corrente.

Certo,
questo discorso va al di la' del Clipperz chiaramente, il mio discorso era riferito in generale e non allo specifico....

> *Post by Noiano*
> Sono totalmente daccordo, invece, sul fatto che la paranoia sia una virtù :-)

:)
--
***@sKy

Makkinista - Fuokista

GPG/PGP keys available via keyservers http://pgpkeys.mit.edu:11371/
DSA: 6CBE 6982 5C10 CFF0 D676 6420 C1C5 B8EC 8690 0F88
RSA: 40 6B 54 8C 20 A0 F6 0B 4C 96 AA 34 D3 FB DC 8C

_____
http://www.sikurezza.org - Italian Security Mailing List

Giulio Cesare Solaroli 17 years ago

Salve a tutti,

mi chiamo Giulio Cesare Solaroli, e sono il responsabile tecnologico di Clipperz.

Mi permetto di intervenire nella vostra interessante discussione per cerare di completare alcune osservazioni che sono state fatte relativamente al nostro servizio.

> *Post by Fabio Pietrosanti (naif)*
> Che non esiste un meccanismo tecnologico che permetta di validare che il codice javascript caricato sia esente da backdoor o che questa possa essere introdotta dinamicamente su richiesta da parte di "terzi".

Questa affermazione è assolutamente corretta, ma noi abbiamo compiuto tutti gli sforzi che al momento riuscivamo a sostenere per intraprendere un cammino che porti alla risoluzione definitiva di questo problema. Mi permetto di dettagliare le soluzioni che abbiamo già messo in opera per alleviare il problema:

Il codice della nostra applicazione viene caricato tutto in un unico file; html, javascript, css e anche immagini (per i browser che le riescono a gestire) sono codificate nell'unico file che viene scaricato dal browser. I sorgenti dell'applicazione nessi a disposizione sul sito per la verifica del codice, contengono anche uno script in grado di generare lo stesso identico file che viene scaricato dal browser nell'applicazione online; la fase finale del processo di build termina con il calcolo dei checksum della pagina generata che devono corrispondere con quelli pubblicati online.

E' vero che il browser al momento non e' in grado di verificare il checksum della pagina (stiamo lavorando anche a questo aspetto, ma le questioni in ballo per risolverlo sono ancora troppo grandi per riuscirle a gestire da parte nostra), pero' abbiamo messo a disposizione di tutti i nostri utenti un piccolo script PHP che permette di effettuare il controllo prima di accedere all'applicazione vera e propria. Io, ad esempio, accedo sempre all'applicazione passando dall'url che ho memorizzato qui:
http://del.icio.us/gcsolaroli/clipperz

E' ovvio che questo tipo di controllo non e' ideale, dato che il checksum viene verificato su una pagina inviata ad uno script, e non su quella finale che verra' eseguita dal browser, ma mostra in modo abbastanza preciso come potrebbe funzionare una validazione della pagina da parte del browser stesso.

Relativamente poi alla possibilita' di caricare codice dinamicamente, anche questa e' una possibilita' assolutamente reale, ma che noi abbiamo accuratamente evitato e resa inerte con qualche semplice accorgimento:
- non viene mai caricato del codice html dal server, ma solo dati che vengono processati dall'applicazione;
- non viene mai eseguita l'istruzione "eval" sui dati caricati dal server, per impedire di alterare dinamicamente la struttura dell'applicazione.

E' possibile verificare nell'applicazione di cui distribuiamo i sorgenti che questi due accorgimenti sono stati assolutamente rispettati, ed e' quindi impossibile alterare il funzionamento

dell'applicazione in esecuzione sul browser costruendo opportunamente
i dati restituiti dal server.

> *Post by Fabio Pietrosanti (naif)*
> Che le mie password non mi sognerei mai di salvarle su di un database
> diverso dal file cifrato che tengo sul mio computer.

Clipperz offre la possibilita' a tutti di scaricare agevolmente una
versione Offline della nostra applicazione; quello che viene scaricato
e' un file HTML che, oltre a tutta l'applicazione, contiene anche i
dati dell'utente criptati, esattamente come sono memorizzati sul
nostro DB.

Questo file offre un grossissimo vantaggio rispetto a tutti i vari
metodi alternativi di memorizzazione delle password in locale: tiene
legati dati ed applicazione d'accesso ai dati stessi, in modo da
renderli utilizzabili ovunque, a prescindere dal software installato
sul computer che si usa. Ovviamente serve avere accesso ad un browser
"moderno", ma questa e' una richiesta quasi scontata si computer
odierni.

> *Post by Fabio Pietrosanti (naif)*
> Esporre *tutte* le proprie credenziali di accesso a distanza di "una password"
> non lo considero un rischio accettabile, ...

Non e' la stessa condizione in cui sei quando salvi tutti i tuoi dati
su un file memorizzato sul tuo computer?
Se qualcuno riesce ad avere accesso a quel file, ha accesso a tutte le
tue credenziali.

> *Post by Fabio Pietrosanti (naif)*
> ... sopratutto quando una vulnerabilità
> potenziale semplice come un XSS le metterebbe a rischio di disclosure.

Le vulnerabilita' XSS sono reali, ma possibili solo quando il sito ha
certe caratteristiche. La nostra applicazione non ha nessuno dei
requisiti perche' un attacco di tipo XSS possa essere perpetrato. La
nostra applicazione (in tutti i browser tranne IE, che non supporta il
protocollo data://) non carica nemmeno le immagini dal server,
rendendo assolutamente impossibile il contaminamento dell'applicazione
da parte di qualsiasi agente esterno, anche con il controllo del
server stesso di Clipperz.

...

Il problema di troian e keylogger e' assolutamente reale; e c'e' una
sola opzione efficace per contrastarli: one time password.

Ovvero password che, una volta usate, non permettono piu' l'accesso all'account.

Supponendo che tu debba accedere alla tua posta (o qualsiasi altro
servizio web) da un internet cafe', quello che noi cosigliamo di fare
e' il seguente:
- avere a disposizione sempre un paio di One Time Password scritte su
un foglietto nel portafogli;
- usare la OTP per accedere all'account Clipperz;
- usare i direct login per accedere ai servizi.

Qualsiasi informazione riesca a raccogliere un keylogger, non sara'
mai in grado di accedere nuovamente all'account Clipperz, ne tanto
meno al servizio terzo che si vuole utilizzare, dato che nessun tasto
e' stato premuto per inserire le credenziali.

Questo presuppone che nessuno abbiamo volutamente sovvertito il
browser stesso per raccogliere informazioni in modo specifico, ma al
momento ritengo questa ipotesi troppo remota per essere presa in seria
considerazione.

Spero di avere aiutato a rendere un po' piu' chiaro il funzionamento
di Clipperz.

Per qualsiasi ulteriore dubbio potete rivolgervi direttamente a me,
oppure fare tutte le domande del caso (possibilmente in Inglese) nel
nostro forum:
http://www.clipperz.com/forum

Grazie a tutti per l'attenzione.

Saluti,

Giulio Cesare Solaroli

Raffaele 17 years ago

> *Post by Noiano*
> Su questo concordo con te: infatti su clipperz ho salvato solo
> credenziali «low risk» come quelle di alcuni forum per beneficiare del
> direct login. Il resto lo tengo sotto chiave utilizzando keepassx
> (linux). A proposito conoscete alternative migliori?

Se non migliore altrettanto valida:
http://passwordsafe.sourceforge.net

Ciao
Raffaele