Î.S. CENTRUL DE TELECOMUNICAŢII SPECIALE

CENTRUL PENTRU SECURITATEA CIBERNETICĂ CERT-GOV-MD

FII **INFORMAT**, RĂMÎI **PROTEJAT**.

Octombrie 2014

Buletin Informativ

Dragi colegi,

Centrul pentru Securitate Cibernetică CERT-GOV-MD prezintă buletinul informativ, ca parte a serviciilor sale proactive. Acest buletin compilează articole ce țin de securitatea în sectorul IT pentru luna octombrie 2014 și are drept scop de a vă informa despre cele mai recente știri din domeniul securității informaționale, tendințe, sfaturi și ultimele descoperiri. Sperăm că aceste articole vă vor ajuta în activitatea dumneavoastră de zi cu zi, fie în cazul în care sunteți un specialist tehnic, sau un simplu utilizator de rețea.

FII INFORMAT, RĂMÎI PROTEJAT.
Echipa CERT-GOV-MD

În acest număr:

Sfaturi utile:

Drupageddon - cea mai mare provocare a anului 2014 pentru site-urile Drupal

Drupageddon este numele folosit pentru a desemna vulnerabilitatea severă descoperită recent în site-urile pe bază de Drupal. Termenul a fost obținut prin combinarea cuvintelor "Drupal" și "Armageddon", în scopul demonstrării impactului catastrofal al uneia dintre cele mai periculoase erori a anului curent în sistemul de management al conținutului.

Sunt câțiva factori, în vulnerabilitatea descoperită, care au lăsat mulți administratori de sistem fără de somn zile întregi sau chiar săptămâni:

1) Ușurința creării și automatizării exploit-urilor pentru această eroare;
2) Un timp destul de limitat (~ 3-7 ore) pentru aplicarea patch-ului pe sistemele afectate de această vulnerabilitate înainte ca site-ul Drupal să fie considerat compromis;
3) Procedurile de recuperare site-ului web consumă mult timp - administratorii de sistem ar trebui să recupereze site-ul din copia de rezervă și să restabilească tot conținutul care lipsește, sau - în cazul în care backup-urile lipsesc sau sunt deteriorate - să construiască site-ul afectate de la zero.

Conform datelor publicate pe site-ului oficial Drupal.org se estimează că între 100.000 și 800.000 de site-uri web pe bază de Drupal au devenit compromise ca urmare a atacurilor automate, ceea ce a făcut această vulnerabilitate una din cele mai mari provocări actuale pentru comunitatea Internet.

Experții în domeniul securității cibernetice au participat la Conferința Internațională "Securitatea Cibernetică: Provocări Tendințe și Soluții"

Conferința Internațională organizată de Centrul pentru Securitatea Cibernetică CERT-GOV-MD a avut loc pe data de 15 octombrie 2014, ca parte a Lunii pentru Securitatea Cibernetică în Moldova, inițiată de Guvernul Republicii Moldova.

În cadrul evenimentului, specialiștii, cercetătorii, inginerii, oamenii de știință, dezvoltatorii de soluții și experții au avut ocazia să se întâlnească pentru a discuta situația curentă, tendințele, soluțiile și provocările cu care se confruntă Republica Moldova în domeniul securității cibernetice.

Mai multe detalii despre conferință găsiți în următorul link:
http://cert.gov.md/noutati/international-conference-2014.html

"Noi nu vedem lucrurile așa cum sunt ele, ci le vedem așa cum suntem noi." - Anais Nin

Insiderii - inamicii din interior

Insiderii reprezintă o problemă semnificativă a sectorului TI și în special o problemă majoră pentru echipele de securitate din cadrul organizațiilor. Pentru a lupta cu aceste pericole multe companii au creat o gamă variată de sisteme de securitate și control a rețelei, cum ar fi sistemele de prevenire a pierderilor de date, criptarea, firewall-urile, IDS și pachetele de anti-virus, însă toate acestea nu reușesc să protejeze în totalmente organizația, deoarece insiderii de regulă au scopuri diferite, abilități, cunoștințe, profiluri de risc și drepturi de acces diferite.

Deși nu există o cale sigură pentru a readresa toate scenariile posibile a unui atac, următoarele practici vă pot ajuta să minimizați riscul unei amenințări din partea insiderilor:

- Monitorizați activitățile utilizatorilor. Spre exemplu, dacă un anumit utilizator accesează sute de documente care nu sunt de competența acestuia, atunci alarma ar trebui să fie declanșată imediat, iar amenințarea poate fi tratată mult mai devreme.
- Setați drepturile de acces bazate pe rolurile de utilizator. Asigurați-vă că doar acei angajați care au necesitatea reală de acces la sursa de informație sunt eligibili să o facă.
- Separați responsabilitățile. Separarea responsabilităților previne subversiunea sau coluziunea, precum și evită implicarea personalului în activitățile în care nu au nici un rol.

Citiți mai mult pe:
http://www.information-age.com/technology/security/123458593/cyber-enemy-within-rise-insider-threat

Cum să rămâneți securizat pe net

În timp ce Internetul este o parte esențială a vieții noastre, este foarte important să înțelegem riscurile ce pot surveni din utilizarea tehnologiilor moderne.

Criminalii Cibernetici folosesc diferite metode pentru a pătrunde în calculatorul Dvs. Cu toate acestea, majoritatea criminalilor au un singur scop - de a atrage victima să navigheze spre un site malițios, care găzduiește de obicei un pachet exploit - format dintr-un set de script-uri malițioase care țintesc browser-ul, add-on-ul și software-ul terț încărcat de browser.

Mai jos găsiți tehnicile de atac, utilizate de criminalii cibernetici precum și contramăsurile care vă vor ajuta să evitați infectarea.

Tehnici de atac:

1) ***Mesaje Spam***. Include mesaje transmise prin email, SMS și chat, rețele sociale, mesaje private pe forum și conexiuni în blog. Mesajul periculos poate conține file malițios sau un link spre un site infectat.
2) ***Publicitate Malițioasă***. Publicitate de pe site și anume bannerele ascunse pot redirecționa utilizatorul spre site-ul infectat. La ocazie, aceste bannere malițioase pot chiar pătrunde în rețeaua cu bannere obișnuite. Asemenea cazuri au fost depistate în sistemul de bannere publicitare Yahoo și chiar Youtube.
3) ***Promovarea prin motoare de căutare***. Utilizatorii moderni apelează adesea la motoare de căutare pentru a găsi informația necesară, deci cu cât mai ușor este găsit un anumit site cu atât mai mulți vizitatori el va avea. Criminalii Cibernetici utilizează diferite tehnici pentru a crește poziția site-ului malițios în topul căutărilor.
4) ***Site-uri legitime infectate***. Uneori, infractorii cibernetici pot infecta site-uri populare, în scopul de a răspândi programele sale nocive. În grupul de risc intră site-uri de știri cu trafic ridicat, magazinele online, portalurile sau agregatorii de știri.
5) ***Descărcare directă de către utilizatori***. Destul de des infractorii cibernetici nu au nevoie de instrumente ingenioase și costisitoare pentru ca programele lor malițioase să pătrundă în calculatorul victimei. Utilizatorii pot fi pur și simplu păcăliți în descărcarea și rularea malware-ului.

Contramăsuri:

- Întotdeauna atrageți atenția la activitatea dvs. în Internet: ce site-uri vizitați, ce file-uri descărcați și ce programe instalați pe calculatorul Dvs;
- Fiți prudenți cu mesajele de la utilizatori sau organizații necunoscute, nu accesați link-urile și/sau atașamentele din aceste emailuri;
- Actualizați periodic softurile utilizate frecvent, în mod special necesită actualizare softul care interacționează cu browser-ul Dvs;
- Instalați programe de securitate moderne și păstrați baza de date a antivirusului actualizată.

Citiți mai mult pe:
https://securelist.com/analysis/publications/66347/internet-predators/

Malvertising-ul devine din ce în ce mai răspândit

Cercetătorii din compania de securitate informațională "Proofpoint Inc" au detectat numeroase site-uri afectate de campaniile malvertising. Printre site-urile afectate se află Yahoo!, AOL, Match.com. Astfel, conform unor estimări mai mult de 3 milioane de vizitatori pe zi potențial au putut fi expuși la această amenințare.

Malvertising-ul este un termen utilizat pentru a desemna o varietate malițioasă de publicitate online, folosită pentru a răspândi programe malware prin intermediul rețelelor de publicitate legitime cu scopul de a atrage victimele pe site-uri malware.

Cercetătorii din "Proofpoint Inc" au constatat că, fără a fi nevoie să fie accesat ceva, vizitatorii site-urilor afectate pot fi infectați cu CryptoWall 2.0 Ransomware. Folosind Flashpack Exploit Kit, atacatorii au exploatat o vulnerabilitate în plugin-ul Adobe Flash Player ce le-a permis instalarea CryptoWall 2.0 pe calculatoarele utilizatorilor finali. Similar cu comportamentul altor programe de tip "ransomware", CryptoWall a criptat hard diskul utilizatorilor finali și nu a permis accesul la aceasta până când victima nu a plătit o taxă în valută Bitcoin pentru cheia de decriptare.

Întrucât toate tranzacțiile Bitcoin sunt publice, cercetătorii au putut sa studieze unul din fluxurile de bani și au constatat că timp de 5 zile de când a fost activ acesta a primit 24,35 BTC, care este aproximativ 9.354 dolari USD. Conform estimărilor, zilnic, această campanie genera cel puțin 40 de adrese, deci pentru 30 de zile ale campaniei, atacatorii au putut acumula o cantitate de cel puțin 750.000 dolari USD.

Se recomandă să utilizați următoarele practici în scopul de a vă proteja împotriva infectării cu acest tip de malware:

1) ***Efectuați regulat backup-ul datelor importante și păstrați informația pe dispozitivele de stocare externă***. Aceasta vă permite să curățați sistemul infectat și să recuperați toate datele criptate din backup, fără a plăti bani pentru decriptarea calculatorului dvs;
2) ***Actualizați în mod regulat sistemul de operare, browser-ul web și plugin-urile***;
3) ***Activați funcția "Click to play" în browser-ul dumneavoastră***. Prin activarea acestei opțiuni, conținutul web care necesită plugin-uri, cum ar fi Java, Flash, Silverlight, Adobe Reader, QuickTime, și altele va fi dezactivat în mod implicit. În acest fel utilizatorul va trebui să facă click manual pentru a activa pluginul pe orice pagină web pentru ca conținutul să se încarce. Acest lucru oferă un control util al securității, iar conținutul malițios nu este executat în mod automat de browser.
   - ***Chrome***. Settings -> Show advanced settings -> Privacy -> Content settings -> Plug-ins -> Alegeți opțiunea "Click to play" -> Restartați browser-ul;
   - ***Firefox***. -> Tapați:"config" bara pentru adresă și apasați Enter -> Click pe “I'll be careful, I promise button to proceed” -> În bara de căutare ce apare în partea de sus a paginii tapați "plugins.click_to_play" -> Click drept pe setări de configurare și selectați "Toggle". Valoarea din coloană se va schimba din "false" pe "true" -> Restartați browser-ul.

Citiți mai mult pe:
http://www.proofpoint.com/threatinsight/posts/malware-in-ad-networks-infects-visitors-and-jeopardizes-brands.php

Tor: Anonimitatea nu este egală cu Securitatea

Tor este o rețea de calculatoare care face posibilă navigarea anonimă în mediul online. Procesul de navigare poate fi descris pe scurt în felul următor, un client tor transmite în mod securizat datele sale la rețeaua tor, rețeaua tor alege un drum aleatoriu și retransmite datele, datele trec prin ultimul nod tor (uneori denumit și "nod de ieșire Tor") unde acestea sunt decriptate și trimise la destinația finală.

Cercetătorii de la Leviathan - o companie a cărei activitate ține de securitatea informațională - au găsit un nod de ieșire care în mod silențios infecta cu soft malițios toate binarele care au fost transmise prin acest nod.

Investigația ulterioară a arătat ca autorii de soft malițios au utilizat tehnică sofisticată, care le-a permis să fie evitate de mecanismele simple de auto-verificare a binarului inițial păstrând în același timp originalul intact.

Este recomandat să fie luate următoarele contramăsuri pentru a rămâne securizat în timpul utilizării rețelei Tor:

- ***Verificați în permanență integritatea fișierelor***. Acest control de regulă se efectuează prin compararea hash string-ul a unui fișier de pe pagina unde a fost inițiată descărcarea cu hash string-ul binarului primit;
- ***Verificați semnăturile digitale***. Asigurați-vă că:
  1. Binarele pe care le downloadați sunt semnate;
  2. Titularul semnăturii digitale este de încredere;
  3. Autoritatea de certificare care a emis certificatul digital al semnăturii digitale a titularului este de încredere.
- ***Actualizați aplicațiile în mod regulat***. Nu uitați că nu doar binarele pot fi periculoase, dar și de asemenea fișierele de tip PDF, Word sau Excel.

Aflați mai multe pe:
http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries/

Despre noi

În vederea executării prevederilor Hotărârii Guvernului Nr. 746 din 18.08.2010 "Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat", în cadrul Î.S. "Centrul de telecomunicații speciale" a fost creat Centrul pentru Securitatea Cibernetică CERT-GOV-MD.

Punct centralizat de contact

CERT-GOV-MD este punctul central de raportare și coordonare privind incidentele de securitate în sistemele de comunicații și informatice, aflate în administrarea Centrului de telecomunicații speciale.

Pentru raportarea incidentelor cibernetice:

Trimiteți un e-mail la info@cert.gov.md
sau ne puteți contacta la telefon (+373 22) 820-900 (întrebați de CERT-GOV-MD) doar în zilele lucrătoare de la 8:00 la 17:00.

Găsiți-ne pe web:
www.cert.gov.md

FII **INFORMAT**, RĂMÎI **ROTEJAT**

Sfaturi de securitate WordPress

Chetan Soni, un expert în securitatea cibernetică și tester de penetrare, a publicat o serie de sfaturi de securitate informațională pentru protecția site-urilor web a căror sistem de management al conținutului funcționează în baza platformei WordPress.

Conform acestor sfaturi de securitate, pentru protecția unui site WordPress, administratorul de sistem trebuie să urmeze următoarele sfaturi:

1. ***Securizați fișierul htaccess***. Hackerii pot folosi fișierul *.htaccess* pentru a redirecționa utilizatorii către site-uri malițioase. Pentru a restricționa accesul la acest tip de fișier adăugați următoarele rânduri în fișierul dumneavoastră *htaccess*:

```
<Files .htaccess>
 order allow,deny
 deny from all
</Files>
```

2. ***Dezactivați Theme/Plugin Editor***. Acest pas previne hackeri de a efectuarea unor modificări semnificative pe site-ul WordPress. Pentru aceasta, accesați *wp-config.php* și adăugați următorul cod:

```
define ('DISALLOW_FILE_EDIT ", true);
```

3. ***Securizați fișierul wp-config***. Hackerii încearcă să acceseze acest fișier pentru a distruge site-ul dvs. Schimbați permisiunile de acces a fișierului, astfel încât accesul să fie permis doar de pe un singur web server;
4. ***Schimbați Table Prefix***. Baza de date WordPress este formată din mai multe tabele, care au nume standarde, cum ar fi *wp_users*, *wp_options*, *wp_posts* etc. În cazul în care un hacker știe unde sunt stocate datele de utilizator, el va încerca să exploateze acest lucru. Este recomandat să fie schimbat și prefixul *"wp_"*. Pentru a face acest lucru, deschideți fișierul *wp-config.php*, care este localizat în WordPress root directory și să schimbați prefixul în următorul fel :

```
$ Table_prefix = 'wp_chetansoni123_';
```

5. ***Utilizați plugin-uri de securitate WordPress.*** Sunt disponibile mai multe plugin-uri de securitate, care adresează problemele de securitate de WordPress***;***
6. ***Schimbați cheile de securitate***. Cheile de securitate sunt folosite în calitate de generatoare de cookies de autentificare. În cazul în care site-ul este spart, este recomand ca aceste chei de securitate să fie înlocuite.
7. ***Întotdeauna actualizați temele și plugin-urile WordPress***. Actualizările WordPress de obicei sunt emise în scopul soluționării potențialei probleme de securitate.
8. ***Preveniți navigarea în directoriu***. Navigarea în directoriu permite oricui să vadă toate fișierele din directoriul site-ului. Adaugă următorul cod în fișierul *.htaccess*:

```
Options -indexes
# Asigurați-vă că ați adăugat un rând liber.
```

Citiți mai mult pe:
http://dl.packetstormsecurity.net/papers/general/8in1wordpress.pdf