MAGAZIN POSVEĆEN VAŠEM SAJBER ZDRAVLJU

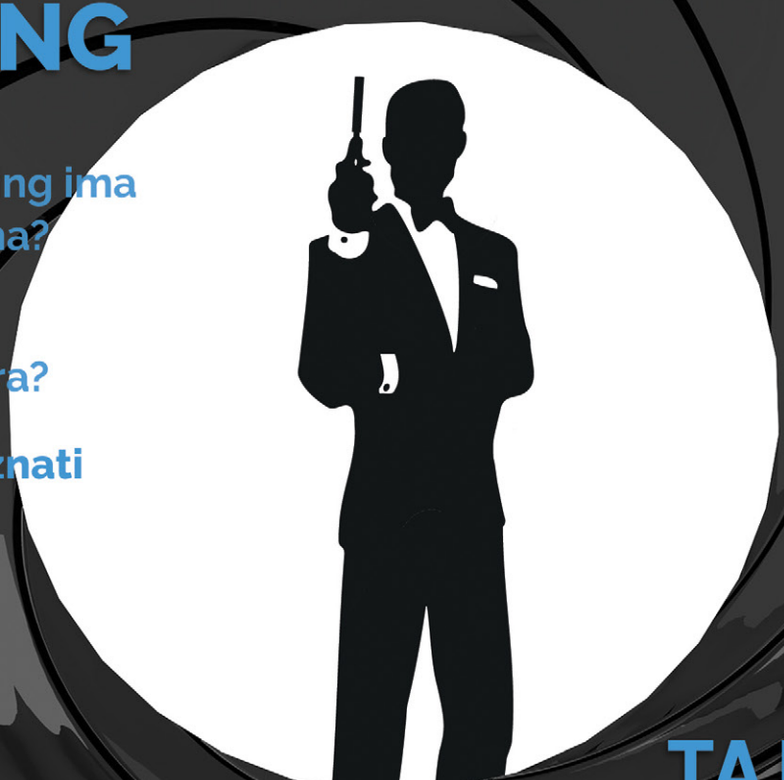
NOV 2016

IT KLINIKA

Tema broja

PHISHING

- Zašto phishing ima toliko uspeha?
- Šta je biznis email prevara?
- Kako prepoznati phishing?



INSAJDERSKA PRETNJA

KAKO SE BORITI SA AUTOIMUNIM BOLESTIMA IT SISTEMA

U SUSRET

SECURITY EVENT

TAJNI AGENTI

U SLUŽBI VAŠEG IT SISTEMA

RAZOTKRIVAMO

10 Mitova o bezbednosti na internetu


PREVENCIJA JE NAJBOLJA
ZA VAŠ SISTEM
Ako želite da vam
šaljemo BESPLATAN
časopis pretplatite se na:
www.it-klinika.rs

UVODNA REČ

Dragi čitaoci,

Hvala vam što ste nam pisali i što ste se interesovali kada će izaći novi broj IT klinike. U prethodnom periodu nam je prioritet bio blog IT klinika – www.it-klinika.rs, pa ste zbog toga na novi broj magazina čekali malo duže. Trudili smo se da uvažimo vaše želje i sugestije, pa se nadamo da će vam se ovo drugo izdanje još više dopasti.

Ako pratite naš blog, a nadamo se da pratite, videli ste da se trudimo da pišemo o aktuelnim pretnjama i popularnim IT security temama, ali i da objasnimo ključne pojmove vezane za IT bezbednost. U ovaj broj magazina uvrstili smo i nekoliko najpopularnijih tekstova sa našeg bloga.

Period od prethodnog broja IT klinike do danas možemo opisati kao izuzetno turbulentan kada je u pitanju IT bezbednost. Proleće i leto bili su u znaku phishinga i biznis imejl prevara, a od jeseni kreću opasne DDoS kampanje do sada neviđenih razmera, koje i dalje traju. Zahvaljujući nedavnom DDoS napadu na DNS i padu velikog broj najposećenijih sajtova, Internet bezbednost je postala globalna tema. Ransomware je i dalje aktuelan, ali smo manje-više naučili kako da ga izbegnemo ili barem da saniramo posledice. Sajber kriminalci su dakle veoma aktivni, ali ni proizvođači bezbednosnih softvera ne spavaju. Na tržištu su se pojavili novi proizvodi i nove poboljšane verzije proizvoda, za koje kažu da su sledeća generacija rešenja za endpoint zaštitu. O svemu tome moći ćete da čitate u ovom broju IT klinike. *ANJA KIŠ*

Izdavač
Net++ technology
Bulevar vojvode Mišića 39a,
11040 Beograd
Telefon: 011/3699-967
Mail: office@netpp.rs
Web: www.netpp.rs

Glavna i odgovorna urednica
Anja Kiš

Saradnici
Biljana Vučinić, Vladimir Vučinić, Dimitrije Veličanin, Siniša Stojanović, Filip Blagojević.

Urednik izdanja
Voja Gašić, PC Press

Dizajn i DTP
Vojislav Simić, PC Press

Za izdavača
PC Press d.o.o.
Osmana Đikića 4, 11108 Beograd 12
Telefon: 011/2080-220
Mail: pc@pcpress.rs
Web www.pcpress.rs

Direktorka
Vesna Čarknajev

Direktor PC Press izdanja
Dejan Ristanović

Štampa
La Mantini, Beograd

SADRŽAJ

U SUSRET DOGAĐAJU

TAJNI AGENTI

U SLUŽBI VAŠEG IT SISTEMA

IT bezbednost je ozbiljna tema i treba joj tako i pristupiti – sa **ozbiljnošću** tajnih službi!

Za tajne službe i tajne agente bezbednost države je prioritet broj 1. Za naše sajber agente je **bezbednost vašeg IT sistema najvažnija misija.**

Pridružite nam se **24. novembra u Crowne Plazi** i upoznajte tajnu službu, sajber špijune i hakere!

Naše IT bezbednosne agencije pripremile su za vas sledeće pokazne vežbe:

Security Agency

NET++ TECHNOLOGY

Agents:
Vladimir Vučinić,
Dimitrije Veličanin
i Siniša Stojanović

Mission Code Name:
Golden Eye

Da li možete da vizualizujete kako izgleda sajber napad? Ako ne možete mi ćemo vam „otvoriti oči“. Pokazaćemo vam kako da identifikujete, locirate i zaštitite se od sajber pretnji.

Na našoj sesiji videćete:

- Live preview IoT napada
- Kako izgledaju napadi na nezaštićenu mrežu/sistem
- Kako izgleda honeypot i kako se primenjuje u savremenoj zaštiti

Security Agency

SYMANTEC

Agents:
Davor Perat
i Davor Kodrnja

Mission code name:
Daredevil

Sajber pretnje postaju sve prefinjenije, a napadi na organizacije svih veličina su svakodnevna pojava. Nepoznate pretnje mogu biti pogubne po organizacije koje se oslanjaju na tradicionalni AV. Symantec je uveo novo oružje u arsenal SEP-a mašinsko učenje koje služi za borbu protiv novih, nepoznatih pretnji.

Pridružite nam se i otkrijte:

- Kako se mašinsko učenje koristi u borbi protiv nepoznatih pretnji
- Zašto je mašinsko učenje koje je integrisano u SEP jedinstveno
- Kako se uklapa sa višeslojnom zaštitom

Security Agency

PALO ALTO NETWORKS

Agents:
Patrick Reischl
i Andreas Persson

Mission code name:
Click–Read–Encrypt

Tradicionalni antivirus više nije rešenje za prevenciju napada na endpoint – više je problem. Hakerima nikad nije bilo lakše. Palo Alto Networks Traps zamenio je tradicionalni antivirus tehnologijom Multi-Metodske prevencije.

Pridružite nam se na ovoj sesiji i saznaćete:

- Zašto tradicionalni antivirus više ne nudi značajan nivo zaštite
- Kako funkcioniše Ransomware
- Kako Traps zamenjuje tradicionalni Antivirus

Security Agency

BALABIT

Agents:
Gabor Illes
i Tamas Farkas

Mission Code Name:
Insider

Najveći izazov za IT bezbednost danas je ljudski faktor. U tipičnoj kompaniji postoje privilegovani korisnici koji imaju pristup osetljivim podacima i neretko zloupotrebljavaju ovu privilegiju i čine štetu. Za ovakve korisnike polise ili kontrola pristupa nisu pravo rešenje.

Pratite našu sesiji i otkrićete:

- Kako da kontrolišete privilegovane naloge u vašem IT okruženju
- Kako da nadgledate i kontrolišete aktivnosti privilegovanih korisnika u realnom vremenu
- Kako SCB može da vam pomogne u istragama incidenata povezanih sa IT sistemima

Ako niste u mogućnosti da dođete u Crowne Plazu 24. novembra, moći ćete da pogledate sva predavanja na YouTube kanalu IT klinike

ZAŠTO JE VELIKI DDOS NAPAD NA DNS UMALO SRUŠIO INTERNET?

21. oktobra 2016. dogodio se DDoS napad ogromnih razmera na servere kompanije Dyn, najvećeg DNS hosta. Još uvek nisu poznati svi detalji napada (ko i kako), ali je napad pokazao koliko lako i brzo može nestati, žargonski rečeno, „pola interneta“ kada na tu ideju dođu odlučni hakeri. Čak i najveći globalni sajtovi poput Twitter, Spotify, Reddit, Etsy, Wired i PayPal mogu u delić sekunde otići offline.

Napad je sproveden sa desetina miliona IP adresa, a veliki broj kompromitovanih uređaja koji su korišćeni u napadu spadaju u grupu IoT (DVR, štampači, pametni kućni uređaji itd.).

KAKO DNS FUNKCIONIŠE?

DNS (Domain Name Servers) je praktično „telefonski imenik“ za internet i on izvršava zahteve za konkretne veb stranice. Dakle, DNS se stara da se nađete na pravoj stranici kada ukucate željenu adresu tj. URL u vaš browser.

Računari koji su deo mreže (interneta) komuniciraju tako što svako ima svoj broj koji je poznat kao IP adresa. DNS prevodi zahteve kao što je URL u IP adrese. Kada u browser ukucate neku adresu, npr. http://www.it-klinika.rs - browser tada traži gde se taj veb sajt nalazi tako što pinguje seriju servera. Kao deo ovog sistema obavlja se veliki broj precizno definisanih operacija, a sve se dešava u delić sekunde. Sistem besprekorno funkcioniše svaki put, kad god otvorite novu stranicu i/ili novi tab – sve dok se ne desi napad poput ovog!

Dakle, hakeri napadaju DNS provajdere kako bi srušili sajtove koji koriste usluge tih provajdera. To se ovih dana desilo Twitteru, Redditu, PayPalu i ostalima.

KAKO JE DOŠLO DO PUCANJA SISTEMA?

DDoS napad je napad u kome se veliki broj kompromitovanih računara koristi kako bi se preopteretio određeni sajt, server ili sistem sa ciljem da se isti privremeno ili trajno onesposobi.

U ovom napadu meta su bili serveri kompanije Dyn koja hostuje DNS za mnoge velike sajtove poput Basecamp, CNN, Etsy, Github, Grubhub, HBO Now, Imgur, Paypal, Playstation Network, Reddit, Squarespace i Twitter. Kada su serveri kompanije Dyn srušeni, browseri više nisu znali gde treba da idu po potrebne informacije kako bi učitali traženu veb stranicu.

KAKO SE ZAŠTITITI?

Odgovor na ovo pitanje nije jednostavan. U kontekstu napada na DNS infrastrukturu, mišljenje većine eksperata je da je najbolji način za zaštitu sajta diversifikacija – da bude hostovan na više različitih mesta. To se zove DNS redundancy i verovatno je razlog što su neki sajtovi bezbolno preživeli napad.

Najveći broj DDoS napada traju između 6 i 24 sata. Od obima napada zavisi i da li ćete moći sami da se odbranite ili ćete morati da potražite profesionalnu pomoć.

DDoS napade malog obima moći ćete i sami da ublažite tako što ćete zaštiti server pomoću mod_evasive, mod_security i drugih funkcija koje nudi operativni sistem ili pomoću Web Application Firewalla).

U slučaju obimnijih DDoS napada, a to znači već od 5Mbps, morali biste da se obratite profesionalnim servisima za zaštitu od DDoS. Najveći broj provajdera ovih usluga nudi probni period od 7 dana, recimo Imperva Incapsula, ili CoudFlare koji osnovne usluge zaštite nudi besplatno.

Na kraju, ako ne želite da vaši uređaji budu deo botneta za DDoS napade, proverite da li je neki od vaših pametnih uređaja kompromitovan (ili ima predispoziciju da to postane), pomoću Internet of Things (IoT) skenera (http://iotscanner.bullguard.com/). Ukoliko jeste, odmah promenite login i password.

ŠTA JE DDOS NAPAD?

DDoS (DDoS – Distributed Denial-of-Service) su napadi sa više hiljada računara kojima je cilj da dovedu do preopterećenja veb servera, mreže ili nekog drugog dela infrastrukture i tako onemoguće pristup njihovim korisnicima. Na primer DDoS napad na link onemogućava pristup internetu, dok DDoS napad na veb server dovodi do „obaranja“ veb sajta.

Moderni DDoS napadi generišu ogromne količine saobraćaja pomoću botova (botnet). Botovi predstavljaju mrežu računara koji su zaraženi malicioznim softverom zbog čega haker ima kontrolu nad njima sa udaljene lokacije. Zaraženi računari rade sasvim normalno najveći deo vremena, osim kada im se zada komanda da spamuju metu.

IOT & DDOS

Pošto broj **IoT uređaja** dinamično raste, povećava se i broj mesta (ulaznih tačaka) preko kojih napadači mogu ući u vaš sistem. Zbog niskog nivoa bezbednosti i enkripcijskih mehanizama, IoT uređaji su laka meta i sajber-kriminalci ih sve više koriste za DDoS napade.

"OVH", hosting provajder iz Francuske, nedavno je bio žrtva DDoS napada jačine preko **1 terabit po sekundi**. Napad je izveden uz pomoć više od 152.000 IoT uređaja, a među njima su i kompromitovane CCTV kamere i lični video rekorderi.

Još prošle godine stručnjaci su upozoravali na problem da proizvođači IoT uređaja i kućnih rutera koriste nepromenjene SSH kriptografske ključeve što milione uređaja poput kućnih rutera, modema i IP kamera ostavlja podložnim za hakovanje. Najgore od svega je što se za te nebezbedne IoT uređaje više ne prave bezbednosna ažuriranja.

IOT UREĐAJI SVE ČEŠĆA META NAPADAČA

Šta možemo očekivati od DDoS napada u budućnosti?

- The Internet of Things (IoT) će verovatno biti sve češća meta.
- Nadzorne kamere (CCTV) su mnogo puta bile hakovane i korišćene kao botovi, očekuje se nastavak tog trenda.
- Ruteri su takođe uobičajena meta, sada i u budućnosti.

Većina IoT malvera cilja uređaje koji nisu povezani sa računarom. Mnogi imaju pristup internetu, ali zbog svog operativnog sistema i tehničkih ograničenja često nemaju napredne bezbednosne opcije. Uređaji su često dizajnirani tako da kada se jednom aktiviraju (podese se osnovna podešavanja), više im se ne posvećuje pažnja. Za mnoge ne postoji ažuriranje firmwarea ili vlasnici zaboravljaju da to urade, a uređaji se zamenjuju tek kad postanu tehnički zastareli. Kada se sve ovo ima u vidu, jasno je da bilo kakva infekcija ili kompromitovanje uređaja može vrlo lako proći neopaženo. Zbog toga su IoT toliko privlačni za DDoS napade.

NAJČEŠĆI IOT MALVERI

Kako napadači ubacuju malver u IoT uređaj? Najčešći metod je traženje nasumičnih IP adresa sa otvorenim Telnet ili SSH portovima nakon čega slede brute-force pokušaji logovanja pomoću uobičajenih kredencijala. Zbog različitih platformi na kojima IoT uređaji rade, IoT malver ponekad funkcioniše tako što nasumično downloaduje bot exe fajlove za više platformi i pokreće ih jedan po jedan dok ne nađe odgovarajući. Malver takođe može imati modul koji vrši proveru platforme i onda downloaduje samo odgovarajući bot binary.

Kada se bot binary izvrši, uspostavlja se veza sa C&C serverom i čeka se komanda.

MALVER ZA VIŠE PLATFORMI

Napadači na jednostavan način kreiraju malver za veći broj platformi. Najčešće mete su x86, ARM, MIPS i MIPSEL platforme, a ta lista se stalno povećava tako da sada postoje varijante malvera za PowerPC, SuperH i SPARC platforme. Tako lista potencijalno ranjivih uređaja stalno raste – ugroženo je sve više web servera, rutera, modema, NAS uređaja, CCTV sistema, ICS sistema i drugih IoT uređaja.

NAJČEŠĆE KORIŠĆENA KORISNIČKA IMENA I LOZINKE

Napadi na Symantecov honeypot su otkrili koji se kredencijali najčešće koriste za logovanje u IoT uređaje. Na prvom mestu je kombinacija 'root' i 'admin', a ostale se mogu videti u tabeli ispod.

TOP USER NAMES	TOP PASSWORDS
root	admin
admin	root
DUP root	123456
ubnt	12345
access	ubnt
DUP admin	password
test	1234
oracle	test
postgres	qwerty
pi	raspberry

Jedna interesantna karakteristika mnogih IoT malvera je mogućnost prekidanja drugih procesa, naročito onih koji su pokrenuti od strane drugih poznatih varijanti malvera. Nekada je to korišćeno kako bi se eliminisao konkurentski malver. Danas postoji i sofisticiraniji pristup (promena iptable pravila), a pored eliminacije konkurencije, cilj je sprečiti bilo kakav pokušaj eksternog pristupanja uređaju i ponekad sprečavanje pristupa legitimnim administratorima.

ŠTA JE PHISHING?

Phishing je napad velikog obima gde haker pravi lažnu imejl poruku koja treba da izgleda kao da je poslata od legitimne kompanije (najčešće banke) sa namerom da prevari primaoca da preuzme malver ili da ostavi poverljive podatke na lažnoj web stranici (lažnu web stranicu kreira napadač tako da liči na neku drugu, legitimnu web stranicu, a podaci koji se na njoj ostave su dostupni napadaču). Obično se tehnikom phishing napada cilja veliki broj primaoca u nadi da će se makar jedan mali broj njih „upecati", što za napadače znači da je napad uspešan.

ŠTA JE SPEAR PHISHING?

To je vrsta phishing napada koji je dobro osmišljen i usmeren na jednog pojedinca ili konkretnu organizaciju. Reč „spear" se koristi kao analogija sa tehnikom lova kopljem. Kod Spear phishinga napadač se najčešće pretvara da je neki pojedinac iz organizacije ili da je zaposlen u određenom sektoru. Na primer, može vam stići lažna poruka od IT sektora da treba da ponovo unesete kredencijale na određenom sajtu ili poruka od HR sektora koja sadrži „novi paket beneficija" u atačmentu.

ZAŠTO JE PHISHING VELIKA PRETNJA?

Phishing je velika opasnost zato što ga je nekad teško uočiti. Prema nekim studijama, čak 94% zaposlenih ne umeju da razlikuju legitimnu od phishing imejl poruke, a oko 11% njih preuzme sadržaj u atačmentu (koji obično sadrži malver). U nekim slučajevima, phishing je lako uočljiv. U nekim drugim, nije. Na primer, word dokument u atačmentu koji kada se otvori izvršava macro komandu je vrsta phishinga koju je nemoguće uočiti, a posledice mogu biti ozbiljne.

Prema jednoj studiji, 96% rukovodilaca širom sveta nije bilo u stanju da razlikuje pravu od phishing poruke u 100% slučajeva. Iz toga se može izvući zaključak da su čak i oni koji vode računa o bezbednosti ugroženi. Naravno, što su manje upućeni u problematiku, veći je rizik.

KREIRATI LAŽNI IMEJL NALOG VEOMA JE JEDNOSTAVNO

Možete kreirati lažni imejl nalog koristeći SMTP alat koji se može preuzeti sa interneta. Takođe, možete kreirati domene i korisnike sa servera ili direktno preko svog Outlook naloga. Npr., napravite sledeće naloge (kao u primeru ispod): bill.gates@microsoft.com i barrack.obama@whitehouse.gov. Možete odmah početi da šaljete poruke sa ovih adresa iz Outlooka.

Istina je da u sajber prostoru svako može da oponaša svakoga bez mnogo muke. Iako je ta istina zastrašujuća, postoje različita rešenja, uključujući digitalne sertifikate.

ŠTA JE DIGITALNI SERTIFIKAT?

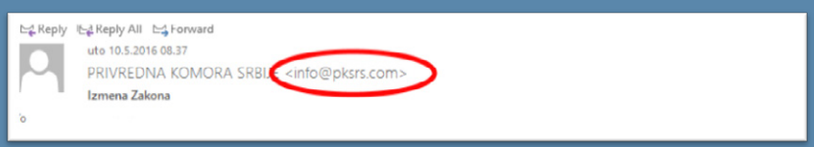
Digitalni sertifikat je nešto poput virtuelnog pasoša. On kaže korisniku da ste vi onaj za koga se predstavljate. Digitalne sertifikate izdaju nadležna tela, tzv. Certificate Authorities (CAs). Da bi neko dobio digitalni sertifikat, mora da prođe proces provere (eng. vetting). Postoji više nivoa provere. Najniži nivo provere je kada se proverava da li je određena osoba vlasnik imejl naloga. Drugi nivo proverava identitet osobe. Na višim nivoima provere potvrđuju se informacije o kompaniji i fizičkoj lokaciji.

Digitalni sertifikat pruža mogućnost digitalnog potpisa i kriptovanja imejla.

Digitalni potpis u imejlu daje primaocu informaciju da je poruka poslata iz legitimnog izvora. Na sledećoj slici možete jasno videti verifikovani identitet pošiljaoca.

Pored toga što pruža dokaz o identitetu pošiljaoca, digitalni potpis obezbeđuje i sledeće:

PRVI (OZBILJAN) PHISHING NA SRPSKOM

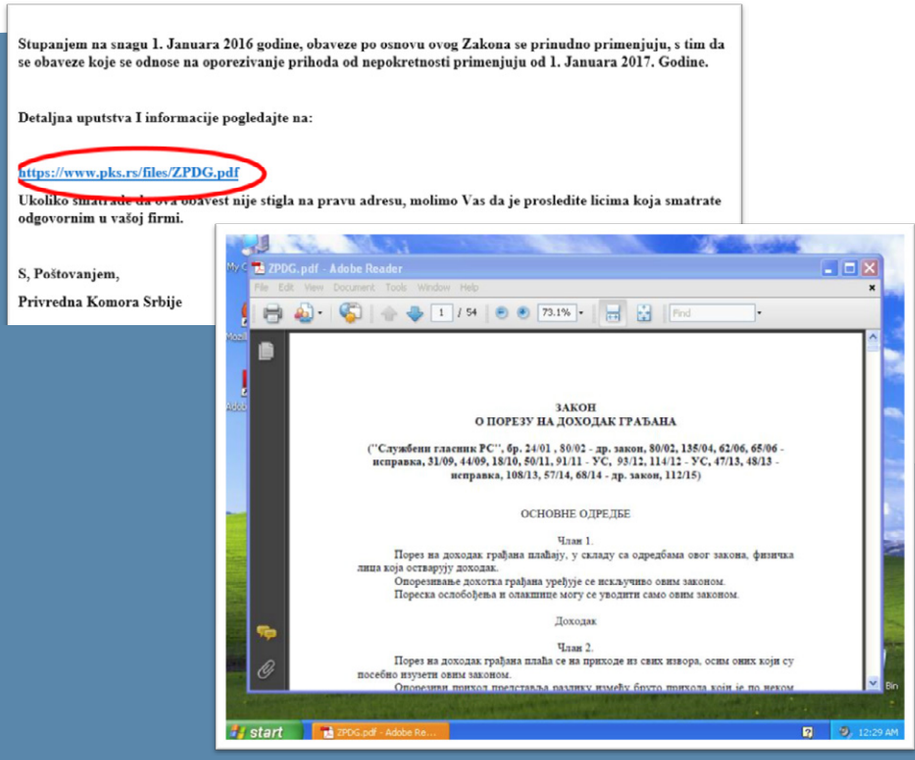


10 maja ove godine otkrili smo phishing kampanju direktno usmerenu na Srbiju. Pošiljalac emaila je navodno bila PRIVREDNA KOMORA SRBIJE. Poruka je bila napisana na srpskom, bez gramatičkih i slovnih grešaka, sa naslovom „Izmena zakona". Naizgled poruka kakvu i inače primamo od Privredne komore.

Ono što je izazvalo sumnju bio je domen sa kog poruka poslata – **pksrs.com,** adresa info@pksrs.com. Pošto smo znali da Privredna

- Neporecivost – kako je u potpisu imejl poruke lični sertifikat pošiljaoca, on ne može kasnije tvrditi da to nije njegov potpis.
- Integritet poruke – kada primalac otvori poruku, imejl klijent provera da li se sadržaj poruke potpuno poklapa sa sadržajem koji je postojao u trenutku kada je stavljen digitalni potpis. I najmanje odstupanje od originala znači da poruka nije prošla proveru.

Kako da prepoznate phishing email?



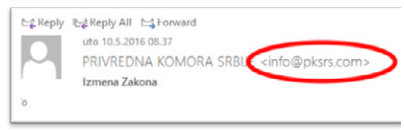
Svakoga dana bezbroj phishing imejl poruka se pošalje širom sveta. Neke od njih je lako prepoznati, neke malo teže. Kako razlikovati phishing od legitimne pošte? Nažalost, ne postoji univerzalno primenjiva tehnika za svaku situaciju, ali postoji nekoliko stvari na koje bi trebalo obratiti pažnju.

1) URL SE NE POKLAPA

Prva stvar koju treba da proverite ako vam je imejl poruka sumnjiva je URL. Često je na prvi pogled URL u phishing poruci legitiman. Ako kursorom miša pređete preko URL-a, možete videti pravu hiperlinkovanu adresu (npr. u Outlook-u). Ukoliko je hiperlinkovana adresa drugačija od one koja se prikazuje, verovatno je u pitanju maliciozna poruka.

2) URL SADRŽI IME DOMENA KOJE VAS DOVODI U ZABLUDU

Prevaranti računaju na to da ljudi često nisu upoznati kako funkcioniše sistem kreiranja imena domena. Poslednji deo imena domena je najvažniji. Na primer, phishing email (navodno) od Privredne komore Srbije, koji su mnogi od nas primili početkom maja ove godine, poslat je sa domena **pksrs.com**. Privredna komora Srbije koristi domen **pks.rs**. Pokušaj manipulacije je očigledan.



Primer manipulacije url-om u phishing poruci

Ovaj trik je mnogo puta korišćen, naročito kada prevaranti žele da uvere žrtvu da je poruka poslata od strane velikih kompanija poput Microsoft ili Apple. Na primer, naprave domen microsoft.malicioznidomen.com i sa njega šalju poruke.

komora koristi domen **pks.rs,** proverili smo na koga je registrovan pksrs.com. Ispostavilo se da je registrovan na izvesnu ENOM INC iz Paname. Dakle, ni reči o Privrednoj komori Srbije, jasno je da se radi o phishingu.

ŠTA SE KRILO U PORUCI?

U tekstu poruke govorilo se o izmenama Zakona o porezu na dohodak građana, sa linkom za preuzimanje navodno .pdf fajla sa detaljnim uputstvima i informacijama.

Link u poruci je zapravo bio .exe fajl koji u sebi sadrži Remote Admin alat!

Kada se pokrene, virus/trojanac otvara PDF dokument sa Zakonom o porezu na dohodak građana, tako da i dalje ne primećujete ništa sumnjivo:

Međutim sa preuzimanjem pdf-a istovremeno se instalira i remote admin alat i dodaje u startup Windows-a koji pokušava da komunicira sa sledećim domenima/IP adresama:

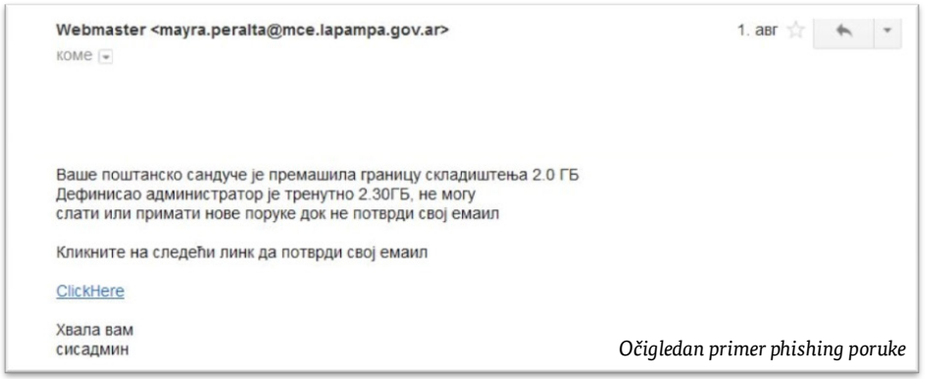
- rutils.com 104.236.34.44
- server.rutils.com 70.38.38.43

Virus takođe preuzima i Windows ProductID, verovatno da bi proverio da li se izvršava u sendbox-u.

rutils.com je servis za Remote Admin Utility, koji omogućava da se računaru pristupi spolja . Mada se sama aplikacija za Remote Admin može upotrebiti i kao alat za administraciju u ovom slučaju se koristi za neovlašćeni pristup računaru bez znanja korisnika.

PRVI SMO OTKRILI PRETNJU

Čim smo otkrili pretnju, objavili smo vest na našem blogu IT klinika, podelili vest na društvenim mrežama i poslali upozorenje svim pretplatnicima našeg email biltena.



Očigledan primer phishing poruke

3) PORUKA SADRŽI GRAMATIČKE I PRAVOPISNE GREŠKE

Kada velike kompanije šalju poruke, po pravilu pre slanja provere pravopis i gramatiku, kao i pravni aspekt. Ukoliko ste dobili poruku sa puno grešaka, gotovo je sigurno da poruku nije poslala neka velika kompanija.

4) OD VAS SE ZAHTEVAJU LIČNI PODACI

Bez obzira na to koliko zvanično izgleda imejl poruka, ukoliko se od vas traže lični podaci, treba da se upali lampica. Banka zna vaš broj računa, tako da vam sigurno niko iz banke neće tražiti da mu pošaljete isti. Takođe, bilo koja respektabilna kompanija vam nikada neće tražiti lozinku, broj kreditne kartice ili odgovor na sigurnosno pitanje.

5) OSVOJILI STE NAGRADU, A NISTE UČESTVOVALI U IGRI

Ako primite imejl poruku od nepoznatog pošiljaoca koja sadrži obećanje o velikoj nagradi, svoti novca i slično, verovatno je u pitanju prevara.

Česte su phishing poruke koje vas obaveštavaju da ste osvojili novac na lutriji ili poklon u nagradnoj igri. Ako niste kupili srećku i ako niste učestvovali u nagradnoj igri, pogađate, u pitanju je phishing.

6) TRAŽE VAM NOVAC ZA POKRIĆE TROŠKOVA

Jedan od znakova da je u pitanju phishing je ako se od vas traži novac. Možda vam to neće tražiti u prvoj poruci, ali, pre ili kasnije, prevarant će zahtevati izvesnu sumu novca za pokriće troškova, poreza, nadoknadu, članarinu ili nešto slično. Tad će vam biti definitivno jasno da je u pitanju prevara.

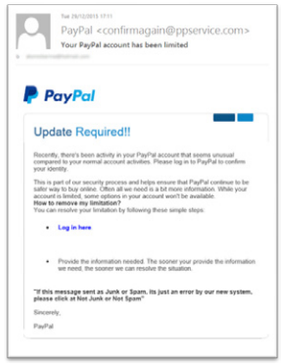
7) NEREALNE PRETNJE

Ovo nije česta taktika prevaranata koji se bave phishingom. Oni najčešće pokušavaju da od vas izvuku novac ili osetljive podatke obećavajući vam brzu zaradu. Međutim, ponekad koriste i taktiku nerealnih pretnji. Evo jednog primera. Stigne vam poruka od banke ili PayPal-a, deluje legitimno, ali vas obaveštava da vam je račun kompromitovan i da morate da im pošaljete broj računa!? i druge lične podatke ili će vam u suprotnom račun biti ugašen, a sredstva zamrznuta. Naravno da vam banka, kao što je i ranije rečeno, nikada neće tražiti broj računa i naravno da vam neće ugasiti račun i zamrznuti sredstva samo zato što niste odgovorili na imejl poruku.

8) PORUKA NAIZGLED POSLATA OD STRANE NEKE DRŽAVNE INSTITUCIJE

Ovakav pokušaj phishinga imali smo nedavno kod nas kada je poruku navodno poslala Privredna komora Srbije. U poruci je bio maliciozni link na kome se navodno nalaze izmene zakona koje su „od izuzetne važnosti“ za kompanije.

Takođe, prevaranti u sklopu tehnike zastrašivanja šalju poruke pretvarajući se da su policija, poreska uprava i sl. sa namerom da izvuku osetljive podatke ili novac. Budite sigurni da tako ne funkcionišu državne institucije ni u svetu, a ni kod nas, tj. ukoliko žele da stupe u kontakt sa vama bilo kojim povodom, prvi korak sigurno neće biti preko imejl poruke.



Nerealna pretnja

9) PORUKE NEPOZNATIH POŠILJALACA SA ATTACHMENTOM

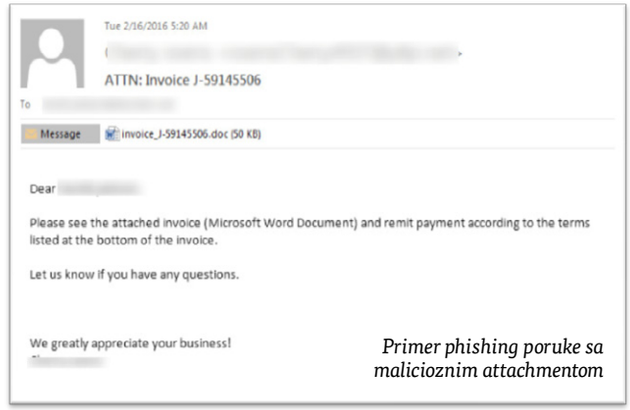
Phishing poruke su obično imale za cilj da žrtva klikne na link u telu emaila, međutim u poslenjih godinu dana učestale su phishing poruke koje ne sadrže link, već attachment – obično Word, Excel ili PDF koji je maliciozan. Često su naslovljene sa INVOICE, ACCOUNT STATEMENT i slično. Kada otvorite dokument u pokrećete skriptu koja preuzima virus, trojanac ili ransomware.

10) NEŠTO VAM JE SUMNJIVO

Ako vam bila šta u imejl poruci deluje sumnjivo, mudar potez je da ne radite ono što se od vas u poruci traži. Posebno budite oprezni sa porukama od **poznatih pošiljalaca koji traže nešto neuobičajeno od vas**. Recimo stigao vam je email od direktora ili saradnika koji traži da izvršite transfer na neki novi račun. Obavezno proverite telefonom da li vam je stvarno ta osoba poslala taj email i ne izvršavajte ono što se od vas traži sve dok ne dobijete usmenu potvrdu.

Još nešto na šta treba da obratite pažnju su detalji u zaglavlju:

- Da li ste dali svoju imejl adresu kompaniji pošiljaocu? Da li imate otvoren nalog kod njih? Da li je identitet pošiljaoca u skladu sa temom imejl poruke? Poruka od banke ili određene institucije se ne šalje sa neke nasumične imejl adrese. Ukoliko vam je **pošiljalac nepoznat**, u 99% slučajeva u pitanju je phishing.
- Ukoliko piše da ste poruku primili sa **sopstvene imejl adrese**, u pitanju je phishing.
- Da li je **poruka poslata** konkretnom primaocu (vama) ili **velikom broju ljudi**? Uobičajeno, neko sa kim ste u poslovnom odnosu će poslati poruku adresiranu jedino na vas. Ukoliko se u poruci zahtevaju neke poverljive informacije, a adresirana je na više primaoca, definiivno je u pitanju phishing.



Primer phishing poruke sa malicioznim attachmentom

ZAŠTO PHISHING IMA TOLIKO USPEHA?

EKSPERIMENT POKAZAO DA 50% LJUDI NASEDNE NA KLIK-MAMAC!

Istraživači dva univerziteta u Nemačkoj, sproveli su phishing eksperiment na studentima i došli su do saznanja da čak polovina korisnika klikne na linkove u porukama od nepoznatih pošiljalaca, uprkos poznavanju rizika o phishingu i malverima.

U ovom eksperimentu phishing imejl i Facebook poruke sa lažnih email adresa i naloga, poslate su na adrese 1700 studenta. U poruci se primaoci podstiču da kliknu na link koji ih navodno vodi na stranu na kojoj su njihove slike sa zabave (na kojoj nisu ni bili). Kada bi neko kliknuo na link, otvorila bi se stranica na kojoj piše „Zabranjen pristup". Na taj način su istraživači evidentirali stopu poseta, tj. klikove.

Eksperiment se sastojao od dve odvojene studije. U prvoj studiji, istraživači su u poruci primaoce oslovili imenom, dok su u drugoj izostavili ime, ali su detaljnije opisali lažnu zabavu.

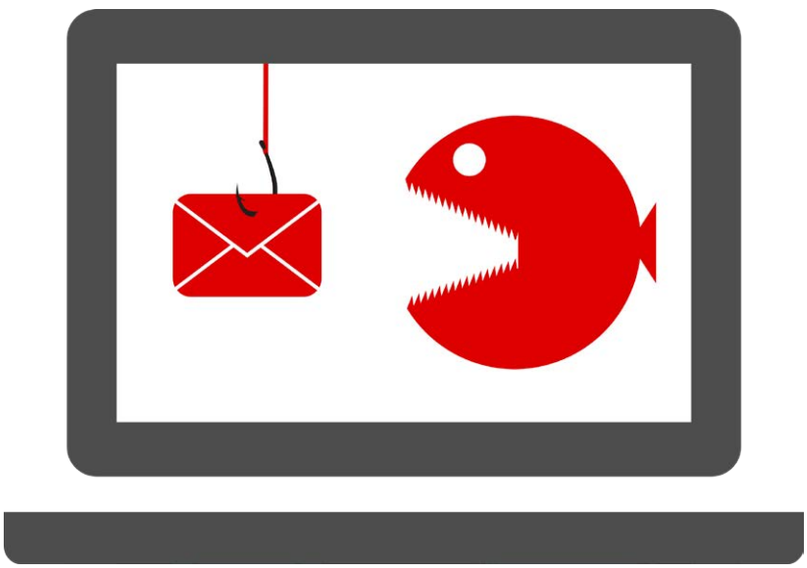
U prvoj studiji, 56% studenata kojima je poslata imejl poruka i 38% studenata kojima je poslata poruka na Facebook su kliknuli na link. U drugoj studiji, na link je kliknulo 20%, odnosno 42% studenata.

Ono što iznenađuje više od rezultata eksperimenta su odgovori učesnika nakon eksperimenta. Naime, nakon eksperimenta, studenti su upitani da objasne zašto jesu, odnosno nisu kliknuli na link. Većina onih koji su kliknuli su naveli da su bili svesni rizika, ali da su svejedno kliknuli.

Samo 20% studenata iz prve i 16% studenata iz druge studije priznalo je da je kliknulo na link, iako objektivna merila pokazuju da su te cifre 45% i 25%. Pretpostavljamo da se neki od njih i ne sećaju da su kliknuli na link, što znači da ne bi bili ni svesni da su žrtve prevare da se radilo o pravom zlonamernom phishingu.

Na pitanje zašto su kliknuli, većina studenata je odgovorila da su bili radoznali da vide slike. Ostali su odgovorili da su nedavno bili na zabavi koja se uklapa u opis iz lažne poruke.

Odgovori studenata ilustruju zašto je tehnika socijalnog inženjeringa toliko uspešna. Ključ nije u tome da se traže ranjivosti u bezbednosti sistema, ključ je u tome da se iskoristi ljudska priroda. U ovom slučaju, u pitanju su radoznalost i uobičajene navike/aktivnosti (studenti često posećuju zabave).



ZAŠTITA

Ljudi će i dalje „padati" na klik-mamac i druge slične prevare, naročito ako se prevara pažljivo osmisli i izvede.

Zbog toga je neophodno uložiti napore da se poveća svest o napadima ove vrste, što je naročito važno za kompanije i njihove zaposlene. Edukacija korisnika, odnosno zaposlenih, je prva mera zaštite od phishing prevara.

Međutim, kako je i eksperiment pokazao, edukacija i svesnost postojanja rizika, ne umanjuju radoznalost!

Zbog ljudskog faktora, ali i zbog toga što su phishing napadi sve sofisticiraniji, kompanijama i drugim organizacijama su potrebna i bezbednosna softverska rešenja koja mogu da prepoznaju napredne pretnje i pruže zaštitu od phishinga, ciljanih napada i drugih opasnosti koje se kriju u imejlovima.

DRAMATIČAN PORAST
BIZNIS IMEJL PREVARA

FBI je u aprilu 2016. upozorio javnost o dramatičnom porastu tzv. Biznis email prevare (Business Email Compromise – BEC) ili kako ih još zovu „direktorskih imejl prevara“ (eng. **CEO Fraud**). U pitanju je takva vrsta imejl prevare gde zaposleni misli da je dobio imejl od poslovnog saradnika ili rukovodioca iz svoje firme, u kome se traži da se izvrši određena finansijska transakcija, a novac, u stvari, završi na računu napadača.

Napadači se koriste različitim tehnikama:

- email spoofing, koja koristi nedostatke imejl protokola koji nemaju mehanizam za autentifikaciju,
- slanje imejla sa sličnog domena gde se računa na to da primalac neće primetiti razliku,
- ubacivanje malvera kojim se prati komunikacija
- hakovanja imejl naloga nekog rukovodioca i slanja poruka sa legitimne adrese.

Za razliku od uobičajenih phishing prevara, imejl poruke koje se šalju u „direktorskoj prevari“ retko alarmiraju antispam zaštitu zato što se ne šalju masovno na razne adrese, nego ciljano na jednu.

Ove prevare su pažljivo planirane. Pre napada, napadač upoznaje odnose, aktivnosti, interesovanja, planove putovanja i kupovina u organizaciji. Napadač najpre skida sa sajta kompanije dostupne informacije: imejl adrese zaposlenih i sve ostalo što mu može pomoći kako bi pismo koje sastavi bilo što uverljivije.

U slučajevima kada je napadač hakovao imejl nalog zaposlenog ili rukovodioca, on u imejl porukama traži određene pojmove koji mu mogu pomoći da otkrije da li kompanija redovno vrši finansijske transakcije; traži poruke koje sadrže reči poput „faktura“, „depozit“, „predsednik“.

Kada se pomoću spajvera prati komunikacija firme, poruke, recimo poruka od dobavljača sa instrukcijama za plaćanje, se presreću, tako da prava poruka ne dolazi do firme kupca, već modifikovana poruka sa novom instrukcijom za plaćanje, u kojoj je navedena nova banka. Uz to obično ide i objašnjenje da su iz nekog razloga prešli na novu banku. Kupci uplate novac, a da pri tom nisu kontaktirali dobavljače telefonom da provere da li je zaista došlo do promena

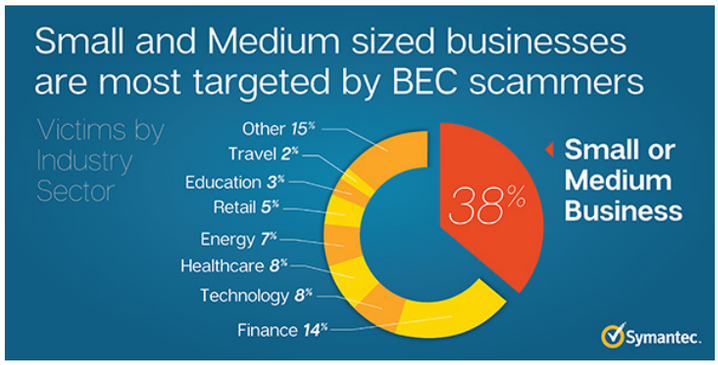
Na prvu loptu, ovakva vrsta prevara deluje nesofisticirano u odnosu na prevare koje uključuju kompleksne maliciozne softvere, poput Dyre ili ZeuS-a. Ali, u praksi se pokazalo da je „direktorska imejl prevara“ sve raznovrsnija i veštija u zaobilaženju osnovnih bezbednosnih strategija koje koriste banke i njeni klijenti. U uobičajenim phishing prevarama, napadač pravi interakciju direktno sa bankom potencijalne žrtve, dok u ovoj prevari napadač praktično navede žrtvu da ona sama to učini umesto njega.

KO SU ŽRTVE?

Više od 400 kompanija dnevno postaju žrtve BEC odnosno direktorske prevare.

Mala i srednja preduzeća čine gotovo 40% od svih meta napada. Što se tiče sektora privrede, najviše je na udaru finansijski sektor (14%).

FBI procenjuje da su kompanije prosečno u ovim napadima gubile između $25.000 i $75.000, Međutim, bilo je i slučajeva kada je jedna organizacija prevarena za milione dolara. Npr, „Mattel“, kompanija koja proizvodi igračke (Barbie), je u ovoj prevari izgubila $3 milona, firma „Ubiquiti“ čak $46.7 miliona, „The Scoular Co.“ $17.2 miliona. Jedna austrijska firma iz aero industrije je nedavno otpustila pred-



Prema Symantec-ovom istraživanju, najčešća meta su mala i srednja preduzeća

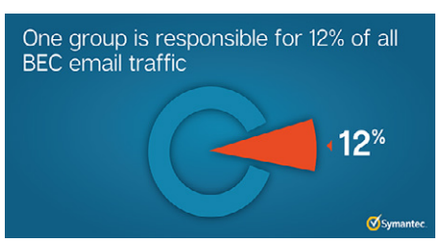
Za sad su gubici kompanija veći od $3 milijarde

sednika i finansijskog direktora kompanije zbog gubitka od skoro $50 miliona usled BEC prevare.

Kada se saberu gubici svih 22.000 žrtava u protekle 3 godine, sajber kriminalci su zaradili više od 3 milijarde dolara!

DVE FIRME IZ SRBIJE OŠTEĆENE ZA 800.000 EVRA

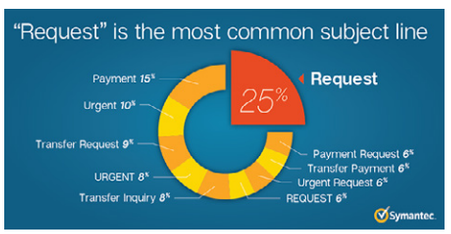
Blic je nedavno pisao o učestalosti BEC prevara u Srbiji. Prema informacijama Odeljenja za borbu protiv visokotehnološkog kriminala MUP, u poslednjih godinu dana ukupna šteta od ove prevare iznosi više od milion evra, a samo dve domaće firme oštećene su za 800.000 evra.



Više kriminalnih grupa bavi se BEC prevarama, ali jedna je dominantna

Jedna grupa napadača je odgovorna za 12% BEC prevara. U protekla 2 meseca, ova grupa je hakovala najmanje 68 imejl naloga, ciljala preko 2.700 organizacija i vršila korespondenciju sa žrtvama sa 147 imejl naloga. Najveći deo aktivnosti ove grupe dolazi iz Nigerije, a jedan deo iz SAD-a i UK-a.

Nije iznenađenje da se najveći broj BEC mejlova šalju radnim danima. Prevaranti znaju da zaposleni u kompanijama uglavnom tada očekuju mejlove. Što je još važnije, najveći deo finansijskih transakcija se odobrava samo radnim danima. Prevaranti su najaktivniji u periodu tipičnog radnog vremena – počnu da šalju mejlove u 7 ujutru po GMT, prave pauzu od 11-14, a onda nastavljaju do 18h. Prevaranti ne žele da previše



Najčešći naslov u mejlu je „Zahtev" (eng. „Request")

komplikuju stvari i zato u naslov mejla uglavnom stave samo jednu reč. Uvek je u pitanju najmanje jedna od sledećih reči: zahtev, plaćanje, hitno, transfer, upit (eng. request, payment, urgent, transfer, enquiry). Jednostavan naslov ima manje šansi da izazove sumnju, a i teže se filtrira.

KAKO SE ZAŠTITI OD „DIREKTORSKE" PREVARE?

Prvo i najvažnije – edukacija korisnika. Naučite ih da:

- Budu sumnjičavi ukoliko dobiju bilo koji zahtev koji deluje neobično ili koji nije u skladu sa uobičajenom procedurom.
- Proveravaju adresu pošiljaoca.

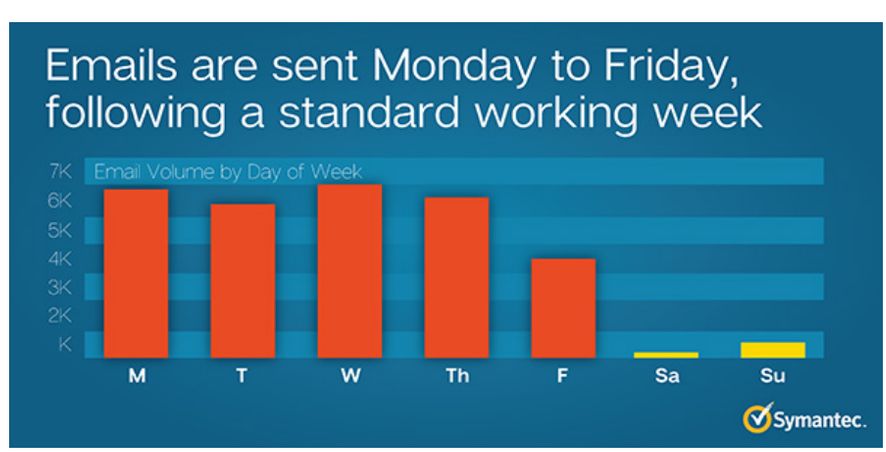
Drugo, koristite dvofaktorsku autentifikaciju za započinjanje procesa transfera novca i uspostavite dodatni kanal komunikacije za transakcije visokih iznosa, npr. verifikacija telefonskim pozivom.

Takođe, se savetuje da kompanije ne objavljuju informacije o aktivnostima zaposlenih na svojim sajtovima i društvenim mrežama, jer napadačima neke od tih informacija mogu biti od izuzetne važnosti.

Ukoliko sumnjate da ste postali žrtva BEC prevare, što je pre moguće obavestite finansijsku instituciju preko koje obavljate transfer novca i prijavite slučaj policiji.

NAJBOLJI SAVETI IZ PRAKSE KOJI SE TIČU ODBRANE OD BEC NAPADA

- Pošaljite uzorke BEC napada kako bi se podigao opšti nivo zaštite. Deljenje informacija pomaže da se brzo detektuju i zaustave ovi napadi.
- Budite sumnjičavi svaki put kada dobijete poštu sa zahtevima koji deluju neuobičajeno ili koji nisu u skladu sa standardnom procedurom.
- Ne odgovarajte na mejlove koji vam deluju sumnjivo. Pogledajte u kompanijskom spisku adresa koja je prava adresa pošiljaoca i pitajte ga da li je poslao poruku.
- Koristite dvofaktorsku autentifikaciju kod iniciranja prenosa novca.



Mejlovi se šalju u skladu sa standardnom radnom nedeljom – od ponedeljka do petka

KAKO DA OJAČATE SVOJE OKRUŽENJE ZA BORBU PROTIV RANSOMWARE-A?

Ransomware postoji od 1989. godine i AIDS trojanca. U prvih nekoliko godina postojanja, ransomware je bio retka pojava. U poslednjih nekoliko godina, međutim, došlo je do prave epidemije ransomwarea. U pitanju je malver koji zaključava ili kriptuje vaše fajlove i gde napadači traže novac kako bi vam vratili fajlove. Napadači imaju veliki finansijski motiv da kontinuirano kreiraju nove vrste i varijante ransomwarea kojima će zaraziti što veći broj žrtava, bilo u masovnim, bilo u ciljanim napadima.

Razumno je pretpostaviti da će ransomware još dugo postojati kao jedan značajan pravac sajber-napada. Zato budite spremni za odbranu od ove pošasti! Što više posla oko zaštite obavite danas, bićete spremniji sutra. Svaka od sledećih preporuka će vam pomoći da smanjite rizik uspešne ransomware infekcije.

ŠTA MOŽETE DA URADITE PO PITANJU IT INFRASTRUCTURE?

1. **NEMOJTE SVIM KRAJNJIM KORISNICIMA** dozvoliti admin privilegije. Uvek poštujte **princip minimalnih privilegija.**
2. **PAŽLJIVO KONTROLIŠITE KO IMA PRAVA PISANJA (WRITE-ACCESS PERMISSIONS)** na fajlovima sa udaljene lokacije. **Koristite Access Control liste** kako biste precizirali koje akcije korisnici mogu da obavljaju sa fajlovima. Ako korisnički nalog ima **samo „Read Only“** dozvole, onda napadači ne mogu preko tog naloga da izvedu ransomware napad.
3. **KORISTITE FSRM ZA BLOKIRATE PROMENE KOJE RANSOMWARE PRAVI NA VAŠIM FAJL SERVERIMA.** Većina fajl servera se kompromituje preko laptopa ili radne stanice koji imaju mapirani disk na udaljenoj lokaciji. FSRM neće spasiti taj računar, ali će sprečiti infekciju zajedničkog diska i pozvati na uzbunu.
4. **VRŠITE REDOVAN BACKUP!** Backup je spas u slučaju ransomwarea, jer možete da vratite svoje fajlove.
5. **DRŽITE BACKUP-OVANE FAJLOVE NA SIGURNOM.** Fajlovi se moraju čuvati tamo gde ne mogu biti pogođeni ransomwareom, crvom, hakerskim napadom bilo koje vrste i uopšteno tamo gde su zaštićeni od svih rizika. Možete alternativno backup napraviti na DVD-jevima ili nekom drugom mediju za čuvanje podataka koji je zaštićen od pisanja (write-protected).
6. **OZBILJNO SHVATITE EMAIL BEZBEDNOST.** Nemojte samo kupiti proizvod i ostaviti podrazumevana podešavanja pod pretpostavkom da ste bezbedni. Konfigurišite Rapid Release definicije, ojačajte njegove polise, implementirajte Disarm i blokirajte atačmente koji su uvek malveri. Ovo je izuzetno efikasna zaštita kada se uradi kako treba.
7. **REDOVNO PRIMENJUJTE ZAKRPE (PATCH)** kako bi se zaštitili od **Drive-by downloadsa**.
8. **KONFIGURIŠITE OKRUŽENJE** tako **da ne pokreće nepotpisane Macroe**. Ako baš morate da dozvolite macro, dozvolite samo potpisane.
9. **ZAKLJUČAJTE RDP.** Ako dođe do kompromitovanja korisničkog imena i lozinke, napadač može sa udaljene lokacije da izvrši bilo koju akciju, npr. može da isključi zaštitu sistema i da ubaci ransomware.
10. **IZBEGAVAJTE MAPIRANJE MREŽNIH DISKOVA.** Poneki ransomware može da sabotira čak i nemapirane diskove. Preporuka je da ih u svakom slučaju sakrijete.

NAJVAŽNIJE: ŠTA ZAPOSLENI MOGU DA URADE?

1. **ČITAJTE LOGOVE.** Ne ignorišite upozorenja. Recimo, u slučaju da dobijete izveštaj da je sistem inficiran i da se IPS bori sa cryptolockerom, izolujte taj računar i prijavite malver Security Response timu.
2. **TESTIRAJTE SPOSOBNOST OPORAVKA U SLUČAJU KATASTROFIČNOG DOGAĐAJA.** Proverite koliko brzo možete da povučete fajlove iz backupa.
3. **TESTIRAJTE KORISNIKE.** Proverite da li znaju šta da rade u slučaju da dobiju sumnjivu email poruku.
4. **EDUKUJTE KORISNIKE.**
   - **Nipošto nemojte omogućiti Macro za pregled atačmenta u dolaznoj pošti!** Ne klikćite na „Enable hidden contents“, nemojte davati lozinku kako biste videli skrivenu poruku u dokumentu, nemojte nasedati na obećanja iz poruke.
   - **Podesite Windows da prikazuje poznate vrste fajlova** („show known file types“). Kažite korisnicima da ne otvaraju nijedan fajl koji ima više od jedne ekstenzije.
   - **Atačmente čuvajte u folderu iz koga nije dozvoljeno pokretanje .exe fajlova** (to možete uraditi preko ADC polisa) i ako deluju legitimno, otvorite ih u tom folderu.

BEST PRACTICE
KONTROLNA LISTA ZA SAJBER BEZBEDNOST

Organizacije koje poznaju svoje pretnje i koje su svesne svojih jakih strana i slabosti, imaju više šansi za uspeh u ratu za sajber bezbednost koji neprekidno traje. Ne čekajte da vaša organizacija bude napadnuta pa da tek onda podižete nivo sajber bezbednosti. Krenite u napad na napadače! Dajemo vam kontrolnu listu sa 7 stavki koje vam pomažu da podignete sajber bezbednost.

JEDAN Neka svi uređaji koji imaju pristup kompanijskim mrežama budu adekvatno zaštićeni. Koristite aktivni nadzor i upravljanje konfiguracijom kako bi inventar uređaja povezanih na mrežu organizacije bio ažuran. Ovo uključuje servere, radne stanice, laptop računare i uređaje sa udaljenih lokacija.

DVA Primenite polisu o prenosnim uređajima. Ograničite pristup neovlašćenim uređajima poput eksternih prenosnih memorija i drugih prenosnih uređaja tamo gde je to moguće. Ovi uređaji mogu preneti malver i ugroziti poverljivost podataka, bilo namerno bilo nenamerno. Ukoliko omogućite pristup ovim uređajima, automatski skenirajte da li sadrže viruse čim ih povežete na mrežu. Takođe, koristite neki od proizvoda za prevenciju gubitka podataka (eng. Data loss prevention – DLP) kako bi pratili i onemogućili kopiranje poverljivih podataka na nekriptovani eksterni uređaj.

TRI Budite posvećeni redovnom ažuriranju i patchovanju. Ažurirajte redovno, preuzimajte bezbednosne zakrpe i ne koristite neažurne i nebezbedne pregledače, aplikacije i plug-inove u pregledaču. Ovo važi za sve operativne sisteme, ne samo na računarima, već i na mobilnim uređajima, ICS i IoT uređajima. Neka antivirus i rešenja za sprečavanje upada u sistem uvek budu ažurna, a za to koristite automatska ažuriranja proizvođača. Većina proizvođača softvera marljivo radi na pravljenju zakrpa za primećene ranjivosti. Automatske zakrpe treba dozvoliti svuda gde je to moguće.

ČETIRI Uspostavite efikasnu polisu lozinki. Neka lozinke budu jake i sa barem 8-10 karaktera koji su kombinacija slova i brojeva. Upozorite korisnike da ne treba da koriste iste lozinke na više sajtova. Deljenje lozinki sa drugima mora biti zabranjeno. Korisnici moraju da menjaju lozinke redovno, najmanje jednom u 3 meseca.

PET Neka backup podaci budu dostupni. Redovno pravite backup kritičnih sistema i endpoint-a. U slučaju bezbednosnih problema, pristupanje backup-u treba da bude jednostavno kako bi se minimiziralo vreme do povratka u redovne tokove.

ŠEST Ograničite atačmente u imejlu. Konfigurišite servere tako da blokiraju ili uklanjaju imejlove koji sadrže atačmente sa ekstenzijama koje se često koriste za širenje virusa poput .VBS, .BAT, .EXE, .PIF i .SCR. Takođe, trebalo bi preispitati polise koje organizacija koristi kada su u pitanju .PDF fajlovi u atačmentu. Imejl serveri bi trebalo da budu zaštićeni adekvatnim softverima i imejlovi se moraju temeljno skenirati.

SEDAM Napravite proceduru za reagovanje u slučaju infekcija i incidenata:

- Neka vam kontakt informacije firme za bezbednost sistema čije usluge koristite budu pri ruci. Odredite koga ćete zvati i koje ćete korake preduzeti ukoliko dođe do infekcije jednog ili više sistema.
- Koristite pouzdana rešenja za backup i restore podataka kako bi mogli da vratite izgubljene ili kompromitovane podatke u slučaju uspešnog napada ili velikog gubitka podataka.
- Iskoristite web gateway, firewall i bezbednosna rešenja za endpoint kako bi identifikovali zaražene sisteme.
- Izolujte zaražene računare kako bi sprečili dalje širenje infekcije u organizaciji i restore podataka vršite sa pouzdanih servera.
- Ako su mrežni servisi pogođeni malicioznim kodom ili nekom drugom pretnjom, onemogućite ili blokirajte pristup tim servisima dok se ne pojavi zakrpa.

Pored primene uputstava sa ove liste, ono što bi uvek trebalo da radite je sledeće - **testirajte, testirajte, testirajte**! Da li se vaša bezbednosna rešenja redovno ažuriraju? Da li znate kako će vaš tim da reaguje u slučaju napada? Važno je da stalno testirate ne samo vašu bezbednosnu tehnologiju, nego i timove koji njome upravljaju kako bi uvek bili korak ispred pretnji.

„Ukoliko poznaješ svog neprijatelja i ukoliko poznaješ samoga sebe – ne treba da se plašiš rezultata stotine bitaka. Ukoliko poznaješ sebe, ali ne i svog neprijatelja, u svakoj pobedi pretrpećeš i gubitke. Ukoliko ne poznaješ ni neprijatelja ni sebe, izgubićeš svaku bitku.“ – SUN CU

RAZOTKRIVAMO

10 MITOVA O BEZBEDNOSTI NA INTERNETU

Šta znamo o online bezbednosti? Na internetu se mogu naći različite informacije, priče i mitovi koje nekad i nesvesno uzimamo kao istinite. Zbog obilja informacija na internetu nije uvek lako odvojiti istinite. Verovanje da smo bezbedni, a da to nismo, može skupo da nas košta. Izdvojili smo 10 mitova o bezbednosti u koje se najčešće veruje.

MIT BR. 1

NEĆE MENE, META SU SAMO VAŽNI I BOGATI POJEDINCI.

U korenu ovog mita je uvreženo mišljenje da je internet veliko mesto i da vi nikome niste bitni. Čak i da dođe do napada, smatrate da nemate previše vrednih podataka koje vam mogu ukrasti. Pre ili kasnije zbog takvog stava može doći do uspešnog sajber napada. Nije u pitanju to koliko jeste ili niste bitni, jer u sajber napadu nema ničeg ličnog. Sajber-kriminalci koriste automatizovane alate za eksploataciju ranjivosti vašeg sistema i uzeće vam sve što mogu. Mogu da vam ukradu lične podatke i mogu da koriste vaš računar kao sredstvo za napade na druge korisnike (DDoS), što samo po sebi ima određenu vrednost. I to malo informacija koje o vama dobiju mogu biti od velikog značaja, naročito ako ih kombinuju sa informacijama do kojih su došli iz drugih izvora. Na taj način stvaraju kompletniju sliku o vama i povećava se verovatnoća da postanete žrtva krađe identiteta. Zašto rizikovati kada postoji puno mehanizama i alata za zaštitu?

Morate prestati da razmišljate da vas niko neće napasti i da ste bezbedni. Sve dok imate digitalni identitet, vi ste vredna meta.

MIT BR. 2

AKO IMAM ANTI-VIRUS, BEZBEDAN SAM

Kada korisnici kupe i instaliraju AV ili drugu aplikaciju za zaštitu sistema očekuju da su rešili sve brige koje se tiču bezbednosti. Istina je da svako bezbednosno rešenje ima ranjivosti, zbog toga ne smete ceo sistem prepustiti samo jednom rešenju.

Ne možete da očekujete da vas jedno rešenje zaštititi od malvera, krađe podataka, napada i svih poznatih i nepoznatih pretnji. Dobar sistem odbrane mora da ima više slojeva, kao što tvrđava ima više zaštitnih zidova.

Antivirus je efikasan u zaštiti od poznatih pretnji i njihovih novih varijanti, ali dok se pretnja ne otkrije i dok ne primimo definicije za nju praktično smo nezaštićeni.

MIT BR. 3

NIJE MI POTREBNA ZAŠTITA, NE POSEĆUJEM SUMNJIVE SAJTOVE.

Možda i vi spadate među one koji smatraju da im ne treba zaštita od malvera i da su dovoljno pametni da ne nasednu na trikove sajber-prevaranata. Mnogi veruju da je zdrav razum dovoljna zaštita od malvera, phishinga, krađe identiteta itd. I zaista, to može biti tačno kada je reč o prilozima iz spam email poruka i dosadnim iskačućim prozorima. Međutim, to nije jedina opasnost koja vreba.

Postoje brojni drugi malver napadi i ranjivosti koje nisu vidljive. Sajber-napadači su u stanju da uđu u bezbedne sajtove i ubace malver u reklamu, preko reklame u vaš sistem. Možete posetiti bezbedan i

potpuno legitiman sajt i svejedno pokupiti malver i bez da ste kliknuli na bilo šta. Drugim rečima, možete proći podjednako loše kao da ste posetili rizičan, ilegalni sajt.

Nekoliko svetski poznatih sajtova, kao što su New York Times, BBC, MSN i AOL, bili su ove godine žrtve malvertajzing kampanje, odnosno korišćeni su kao sredstvo širenja malicioznih oglasa.

Maliciozni softver i načini njihovog širenja se konstantno razvijaju. Samo zato što ih niste primetili ne znači da nisu prisutni.

MIT BR. 4

KREIRAO SAM JAKU I SLOŽENU LOZINKU I ZATO SAM BEZBEDAN.

Ne računajte na to. Da, preporuka je da se kreira jaka lozinka. Ona treba da sadrži više od 15 karaktera, mala i velika slova, brojeve i simbole. Pritom, lozinka treba da bude skup nasumičnih znakova kako bi potencijalnim napadačima još više otežali posao. Ali, imajte na umu da sve to nije dovoljno da biste bili bezbedni. To je samo jedan od nekoliko nivoa bezbednosti koji moraju postojati kako biste bili bezbedni.

Sledeća bezbednosna mera je da proverite da li je lozinka jedinstvena. Nemojte koristiti istu lozinku dva ili više puta zato što će na taj način napadač otkrivanjem jedne moći da pristupi i drugim nalozima u kojima ste koristili istu lozinku. Gde god je moguće, koristite dvofaktorsku autentifikaciju za dodatnu zaštitu.

Dugačke, složene i jedinstvene lozinke imaju jednu veliku manu – teško ih je zapamtiti. Svi mi imamo na desetine različitih naloga tako da ovaj problem postaje još izraženiji, a posebno ako se poštuje preporuka da se s vremena na vreme lozinke promene. Nemojte zapisivati lozinke, ni na računaru, ni na papiru, jer to samo povećava rizik. Umesto toga, problem može da se reši tako što ćete lozinke bezbedno čuvati i kriptovati pomoću softvera za čuvanje lozinki (kao što je na primer LastPass ili KeePass).

MIT BR. 5

BEZBEDNOSNI SOFTVER JE SKUP.

Svako ko je bio žrtva nekog virusa ili ransomware-a, ili neke sajber prevare (kao što je BEC prevara), zna koliko je u stvari skupo nemati zaštitu ili backup.

Više od 400 kompanija dnevno postaju žrtve BEC, odnosno direktorske prevare. „Blic“ je nedavno pisao o učestalosti BEC prevara u Srbiji. Prema informacijama Odeljenja za borbu protiv visokotehnološkog kriminala MUP, u poslednjih godinu dana ukupna šteta od ove prevare iznosi više od milion evra, a samo dve domaće firme oštećene su za 800.000 evra.

Cena otkupnine u slučaju da ste se zarazili ransomware-om može da ide i do 16.000 dolara (suma koju je platio Univerzitet Kalgarija u junu ove godine)! S obzirom na to da napad može da se izvrši iz bilo kog dela sveta, napadači retko budu uhvaćeni i izvedeni pred lice pravde, dakle šanse da vratite novac su nikakve.

Kad sve ovo imate u vidu shvatite da je skuplje biti nezaštićen. Tako da, zašto rizikovati?

MIT BR. 6

OTVARAM SAMO EMAIL PORUKE OD POZNANIKA TAKO DA SAM BEZBEDAN.

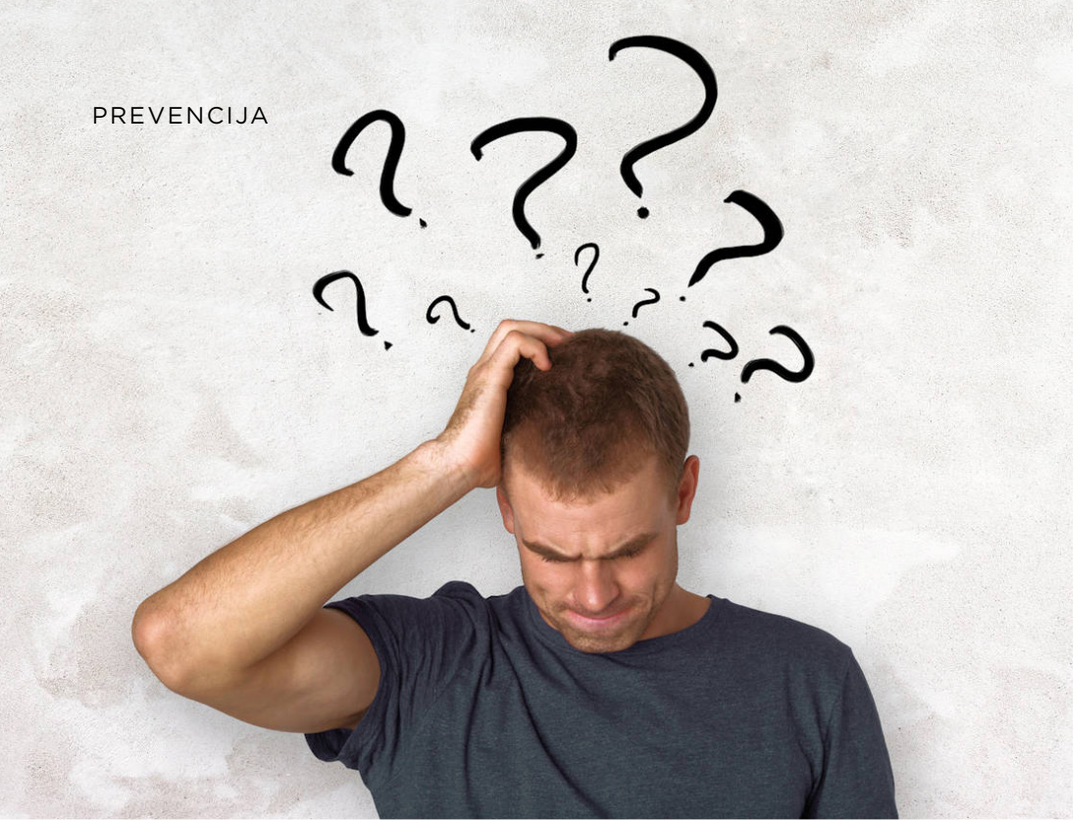
Ovo je sasvim validan argument sve dok ne shvatite da ste prevareni i da ste otvorili poštu od nekoga ko se pretvarao da je vaš poznanik. Nije teško napraviti lažni nalog i staviti bilo koje ime kao ime pošiljaoca. Ako nemate dovoljno iskustva u otkrivanju sumnjive pošte, dovoljan je jedan klik kako biste pokupili malver. Ako kliknete na poslati link ili prilog možete preuzeti neki od opasnih malvera.

Maliciozne email poruke mogu delovati kao da ih je poslao kolega ili neke finansijska institucija, najčešće banka. Mogu izgledati dovoljno uverljivo da vas prevare da pošaljete osetljive informacije.

MIT BR. 7

PREUZIMAM SAMO SADRŽAJE IZ POUZDANIH IZVORA I ZATO SAM BEZBEDAN.

Ovaj mit je teško razbiti. Mnogi misle da su bezbedni zato što posećuju bezbedne lokacije i odatle preuzimaju sadržaj: „Čim se nešto nalazi na internetu, sigurno je bezbe-



dno, jer bi ga u suprotnom skinuli administratori". Stvarnost je poprilično drugačija.

Kao što smo rekli, sajber-napadači mogu da ubace maliciozan sadržaj i na legitimne sajtove koje smatramo bezbednim. Što je najstrašnije, vlasnici sajta često ne znaju da im je sajt kompromitovan, već to saznaju tek kad posetioci počnu da im se žale da su pokupili malver na njihovom sajtu.

Zato ne računajte na administratore sajta, oni su obično zatrpani poslom i ne mogu da isprate sve aktivnosti.

Regularni korisnici sajtova, odnosno posetioci, trebalo bi da imaju rešenje koje proaktivno sprečava napade. To je dodatni nivo zaštite koji nude neka endpoint security rešenja, koja su više od klasičnog anti-virusa. Ono što vlasnici sajta mogu da urade kako bi povećali bezbednost sajta i svojih korisnika, je da redovno ažuriraju web servere i da obezbede dnevno anti-malver skeniranje sajta, koje nude čak i neki SSL sertifikati.

MIT BR. 8

DRUŠTVENE MREŽE KOJE POSEĆUJEM SU BEZBEDNO MESTO, A PRIJATELJIMA VERUJEM.

Da li ste sigurni u ovo? Kada društvena mreža postane popularna, možete se opkladiti da će se tu naći i sajber-prevaranti.

Društvene mreže su raj za prevarante. Oni mogu da nanjuše potencijalne žrtve. Prevaranti stalno smišljaju nove trikove kojima će vas prevariti i podmeću maliciozni sadržaj koji žrtva, ne sluteći da je reč o prevari, preuzima, a tu su i standardni iskačući prozori.

Druga opasnost koja se sreće na društvenim mrežama su lažni profili. Oni služe za prikupljanje informacija o ljudima. Iako vam te informacije mogu delovati bezazleno, one itekako pomažu prevarantima u krađi identiteta. Zato budite oprezni koga dodajete na listu prijatelja.

MIT BR. 9

U RAČUNARU I EMAIL NALOGU NEMAM OSETLJIVE PODATKE. ZAŠTO BIH ONDA BRINUO?

Naravno da imate, samo toga niste svesni. Ili ih ne posmatrate kao vredne. Da li vaš browser čuva sve vaše lozinke za online naloge, uključujući bankovne račune i email naloge? Da li vaš email nalog sadrži privatne konverzacije i slike, poslovne kontakte, fakture, poreske obrasce? Da li ste sve to povezali sa drugim nalozima, na primer sa nekom društvenom mrežom ili cloud servisom?

Možda sve ovo vama ne izgleda bitno, ali sajber-kriminalci skupljaju i sortiraju te informacije i kasnije ih mogu iskoristiti za krađu identiteta ili ih mogu prodati na crnom tržištu. Sve i da zaista nemate nikakvih vrednih podataka, prevaranti mogu iskoristiti vaš uređaj u maliciozne svrhe.

MIT BR. 10

AKO POKUPIM MALVER, SIGURNO ĆU TO PRIMETITI.

Ovo je ranije bilo tačno. Kada su računari počinjali da rade značajno sporije i kada su se pojavljivali dosadni iskačući prozori u prošlosti, to je bio siguran znak da je došlo do infekcije. Danas sajber-kriminalci koriste poboljšane metode. Metode su efektnije i napadači znaju kako da maskiraju napade.

U većini slučajeva žrtve nisu svesne da se njihov računar koristi za spam kampanje i koordinirane DDoS napade.

Malveri se dizajniraju tako da AV ne može da ih detektuje niti da im uđe u trag. Na taj način napadači dolaze do osetljivih informacija. Mogu proći meseci dok ne primetite nešto sumnjivo.

Zato treba da koristite softver koji nudi višeslojnu zaštitu i služi, kako za odbranu od klasičnih pretnji, tako i za zaštitu od sofisticiranih, ciljanih napada, zero-day i drugih pretnji koje zaobilaze tradicionalne zaštitne mere.

I naravno, ne zaboravite da redovno vršite backup fajlova.

ZAKLJUČAK

Mitovi o bezbednosti na internetu žive zato što ljudi traže laka rešenja i jednostavne odgovore na svoje strahove. Mitove treba odbaciti i pažnju usmeriti na stvarne bezbednosne rizike. Edukacija počinje odbacivanjem lažnih informacija koje smo prihvatali kao istinite.

A HACKER'S VIEW OF ANTIVIRUS

Protect Yourself From Antivirus

Traditional antivirus is not the solution to breach prevention on the endpoint — it's the problem. If you're still using antivirus, you're leaving your organization vulnerable to cyberattacks.

It's time to replace your traditional antivirus with next-generation endpoint security. **Learn more at go.paloaltonetworks.com/traps**

paloalto NETWORKS®

NOVA GENERACIJA ZA ZAŠTITU ZDRAVLJA

PALO ALTO NETWORKS TRAPS

NAPREDNA ENDPOINT ZAŠTITA

Novi proizvod Traps kompanije Palo Alto zamenjuje tradicionalni antivirus višestrukim metodama prevencije – jedinstvenom kombinacijom ciljano kreiranih metoda za prevenciju malvera i eksploatacije koji štite korisnike i endpointe od poznatih i nepoznatih pretnji. Traps sprečava upad u sistem za razliku od tehnika koje samo detektuju upad i vrše reagovanje na incidente nakon kompromitovanja kritičnih digitalnih resursa.

Većina organizacija koristi mešavinu različitih bezbednosnih rešenja kako bi zaštitila endpoint sisteme, uključujući i jedan ili više tradicionalnih AV rešenja. Probojem besplatnih i jeftinih napadačkih alata, sajber-kriminalci su u stanju da kreiraju nove i jedinstvene napade koji zaobilaze AV zasnovane na potpisu. Postojeća endpoint bezbednosna rešenja i AV ne mogu da zaštite korisnike i sisteme od prikrivenih, nepoznatih i zero-day napada.

Traps sa svojom jedinstvenom kombinacijom najefektnijih, ciljano kreiranih metoda za prevenciju malvera i eksploatacije štiti od poznatih i nepoznatih pretnji pre nego što one kompromituju endpoint.

TRAPS VIŠESTRUKI METOD PREVENCIJE MALVERA

Traps sprečava izvršenje malicioznih aktivnosti jedinstvenim pristupom višestrukih metoda prevencije koji maksimiziraju pokrivenost u borbi protiv malvera dok istovremeno smanjuju prostor za napad i povećavaju preciznost detekcije malvera. Pristup kombinuje nekoliko metoda prevencije kako bi momentalno sprečio da poznati i nepoznati malveri inficiraju sistem.

1. **STATIČKA ANALIZA PREKO MAŠINSKOG UČENJA** Ovaj metod donosi momentalnu „presudu“ svim nepoznatim izvršnim (.exe) fajlovima pre nego što dozvoli njihovo (ne)pokretanje. Traps ispituje na stotine karakteristika datog fajla u deliću sekunde, bez oslanjanja na potpise, skeniranje i analizu ponašanja.
2. **WILDFIRE INSPEKCIJA I ANALIZA** Ovaj metod se oslanja na Palo Altov cloud servis za analizu malvera kako bi brzo detektovao nepoznate malvere i automatski reprogramirao Traps da spreči poznate malvere. WildFire eliminiše nepoznate pretnje tako što ih transformiše u poznate za 300 sekundi.
3. **OGRANIČENJA ZA EXE. FAJLOVE KOJI DOLAZE IZ POUZDANIH (TRUSTED) IZVORA** Ovaj metod dozvoljava organizacijama da identifikuju .exe fajlove koji spadaju u grupu „dobrih nepoznatih“ zato što su ih objavili i digitalno potpisali pouzdani autori – ali pod uslovom da ih i Palo Alto Networks prepoznaje kao pouzdane autore softvera.
4. **OGRANIČENJA .EXE FAJLOVA NA BAZI POLISA** Organizacije mogu da definišu polise kako bi sprečile određene scenarije izvršenja i tako smanjile površinu za napad u svom okruženju. Na primer, Traps može sprečiti izvršenje fajlova iz Outlookovog „temp“ direktorijuma ili može sprečiti izvršenje datog tipa fajla direktno sa USB-a.
5. **POLISE ZA ADMINISTRATORE** Ovaj metod dozvoljava organizacijama da definišu polise zasnovane na hashu ili .exe fajlovima kako bi kontrolisale šta sme, a šta ne sme da se pokrene u nekom okruženju. Ova suptilna tehnika belih (ili crnih) lista kontroliše izvršenje bilo kog fajla zasnovano na uslovima koje je definisao korisnik i

TRAPS NAPREDNA ENDPOINT ZAŠTITA RADI SLEDEĆE

Sprečava upade u sistem preventivnim blokiranjem poznatih i nepoznatih malvera, eksploatacija i zero-day pretnji.

Štiti i omogućava korisnicima obavljanje uobičajenih dnevnih aktivnosti na mreži bez bojazni od poznatih i nepoznatih sajber-pretnji.

Automatizuje prevenciju tako što se autonomno reprogramira koristeći informacije o pretnjama koje se nalaze u WildFire servisu.

REŠENJA
KRAJNJIH TAČAKA IT SISTEMA

važi za sve sisteme koji koriste Microsoft Active Directory. Svaki .exe fajl za koji se sumnja da je maliciozan i čije je pokretanje u endpointu onemogućeno se stavlja u karantin u zaštićeno skladište kome samo administratori sistema mogu da pristupe. Traps administratori mogu da pregledaju fajlove iz karantina, da ih obrišu ili vrate na originalnu lokaciju u endpointu, ukoliko je potrebno.

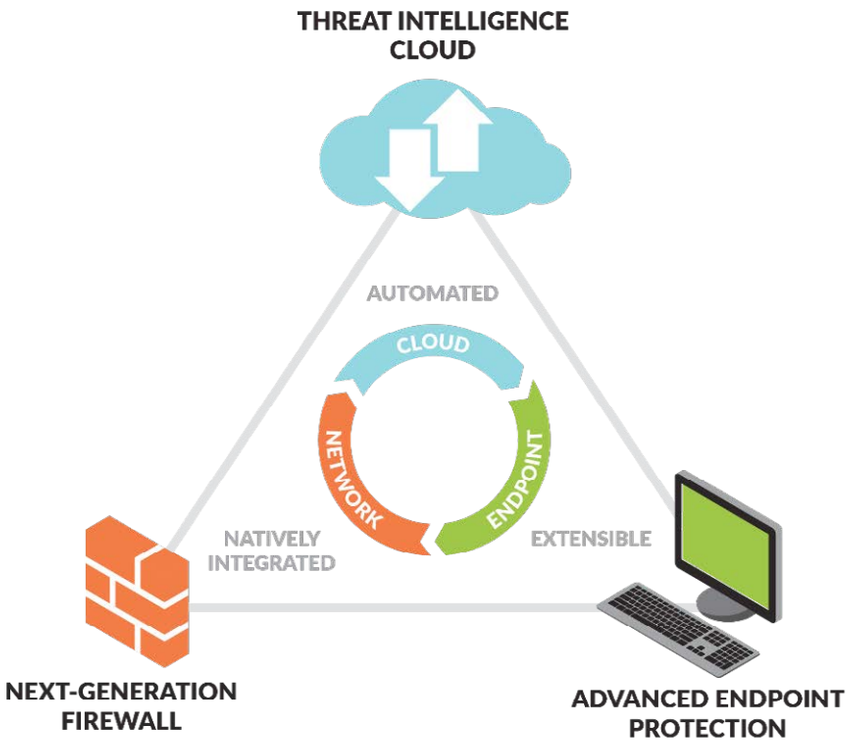
TRAPS VIŠESTRUKI METOD ZA PREVENCIJU EKSPLOATACIJE

Traps koristi potpuno novi i jedinstveni pristup za sprečavanje eksploatacija. Umesto da se fokusira na milione pojedinačnih napada, ili na njihove softverske ranjivosti, **Traps se fokusira na suštinske eksploatacione tehnike** koje se koriste u svim napadima koji se baziraju na eksploataciji. Svaka eksploatacija koristi seriju eksploatacionih tehnika kako bi uspešno kompromitovala aplikaciju. **Traps čini ove tehnike neefikasnim tako što momentalno blokira svaki pokušaj njihovog korišćenja.** Organizacije koje imaju Traps mogu da koriste sve aplikacije bez bojazni od trenutnog izlaganja opasnosti, uključujući i aplikacije koje su interno razvijene i one za koje se više ne prave ažuriranja. Traps implementira pristup višestrukog metoda prevencije eksploatacija, kombinujući nekoliko slojeva zaštite kako bi blokirali eksploatacione tehnike:

1) PREVENCIJA KOMPROMITOVANJA MEMORIJE Traps sprečava da tehnike za eksploataciju kompromituju mehanizme za upravljanje memorijom u operativnim sistemima u aplikacijama koje otvaraju fajlove koji sadrže eskploataciju.

2) PREVENCIJA LOGIČKIH PUKOTINA Traps prepoznaje i blokira eksploatacione tehnike koje manipulišu normalnim procesima i izvršnim mehanizmima u aplikacijama operativnih sistema.

3) PREVENCIJA UBACIVANJA MALICIOZNOG KODA U većini slučajeva, cilj



eksploatacije je izvršenje komandi napadača koje su ubačene u eksploatacioni fajl. Ovaj metod prevencije prepoznaje eksploatacione tehnike pomoću kojih se izvršava maliciozni kod i blokira ih pre nego što uspešno izvrše komandu.

BEZBEDNOSNA PLATFORMA SLEDEĆE GENERACIJE

Troškovi IT infrastrukture potrebne za napad se konstantno smanjuju tako da su danas napadači u stanju da izvrše napade većeg obima i stepena sofistikacije mnogo lakše nego ikada pre. Neusklađeni slojevi bezbednosti i point rešenja koja se oslanjaju na zastarele tehnologije ili ljudski faktor više nisu dovoljna. Samo platforma koja konsoliduje, automatizuje i prirodno integriše veći broj tehnologija za prevenciju može garantovati prevenciju naprednih, ciljanih i skrivenih napada.

Prirodna integracija Trapsa u Palo Altovu bezbednosnu platformu sledeće generacije omogućava organizacijama da kontinuirano dele informacije o pretnjama koje su prikupljene od hiljada kompanija, kako u mrežama, tako i u endpointima kako bi se koordinisali prevencija i reakcija. Automatsko reprogramiranje i pretvaranje informacija o pretnjama u prevenciju onemogućava napadače da iskoriste nepoznate i napredne malvere kako bi inficirali sistem. Napadač u najboljem slučaju po njega može koristiti jedan malver najviše jedanput u celom svetu i ima na raspolaganju samo par sekundi da izvede napad pre nego što WildFire taj malver učini potpuno jalovim.

SISTEMSKI ZAHTEVI I PODRŠKA ZA PLATFORMU

Traps štiti sisteme koji nisu izvršili zakrpu i podržan je za svaku platformu koja radi na Windows OS: desktope, servere, industrijske kontrolne sisteme, komponente virtuelne desktop infrastrukture (VDI), virtuelne mašine (VM) i ugrađene sisteme.

SYMANTEC
ENDPOINT PROTECTION 14

Symantec Endpoint Protection 14 promeniće vaš pogled na Endpoint bezbednost.

U 2016. godini gotovo svakoga dana možemo pročitati neku vest o bezbednosnim pretnjama: ransomware napadi na bolnice i banke, geopolitički napadi, finansijski motivisani napadi na internacionalni bankarski sistem za transfer novca (SWIFT) i napadi na ključne infrastrukturne objekte poput napada koji je srušio ukrajinsku električnu mrežu.

Poslovanje, državni aparat i čovekov privatni život postaju sve više i više deo digitalne sfere što dovodi do velikog broja napada iz različitih izvora. Mnogi napadi, direktno ili indirektno, počinju sa malverom koji targetira endpointe.

Tempo nastanka i nivo prefinjenosti novih pretnji može da obeshrabri. Symantec je u 2015. zabeležio više od 430 miliona novih malvera, što je više od milion novih varijanti malvera svakoga dana! U 2016. se nažalost očekuje još veći broj malver varijanti, jer se očekuje dalji porast zero-day i ransomware napada koji su finansijski motivisani. Ovi napadi se dizajniraju tako da mogu da kompromituju targetirano okruženje na mnogo različitih načina što čini endpointe još ranjivijim i povećava potrebu da se endpointi zaštite.

Upravo ovo radi Symantec sa svojim novim partnerima iz Blue Coat. Više nema potrebe da se mučite da integrišete na desetine različitih bezbednosnih rešenja različitih vendora koji nisu kompatibilni. Symantec i Blue Coat rade zajedno na izgradnji integrisane sajber-bezbednosne platforme budućnosti koja omogućava da se obave sve aktivnosti oko prevencije, detekcije i reakcije u endpointima, gateways, sistemu razmene poruka i cloudu.

Symantec Endpoint Protection 14 (SEP14) predstavlja značajnu inovaciju za endpoint bezbednost. Symantecov softver za zaštitu endpointa je vodeći na tržištu što dokazuje liderska pozicija u Gartner Magic Quadrantu već 14 godina za redom i na desetine dobijenih nagrada. Najnovija verzija SEP14 donosi **višeslojnu zaštitu endpointa u jednom agentu**, uključujući inovacije u oblasti naprednog mašinskog učenja i prevencije zero-day eksploatacije, kao i proverenu tehnologiju za reputaciju fajlova, analizu ponašanja, firewall i zaštitu od upada u sistem. Sve ovo je podržano najvećom civilnom mrežom informacija o pretnjama.

Da objasnimo korak po korak.

VIŠESLOJNA ENDPOINT ZAŠTITA

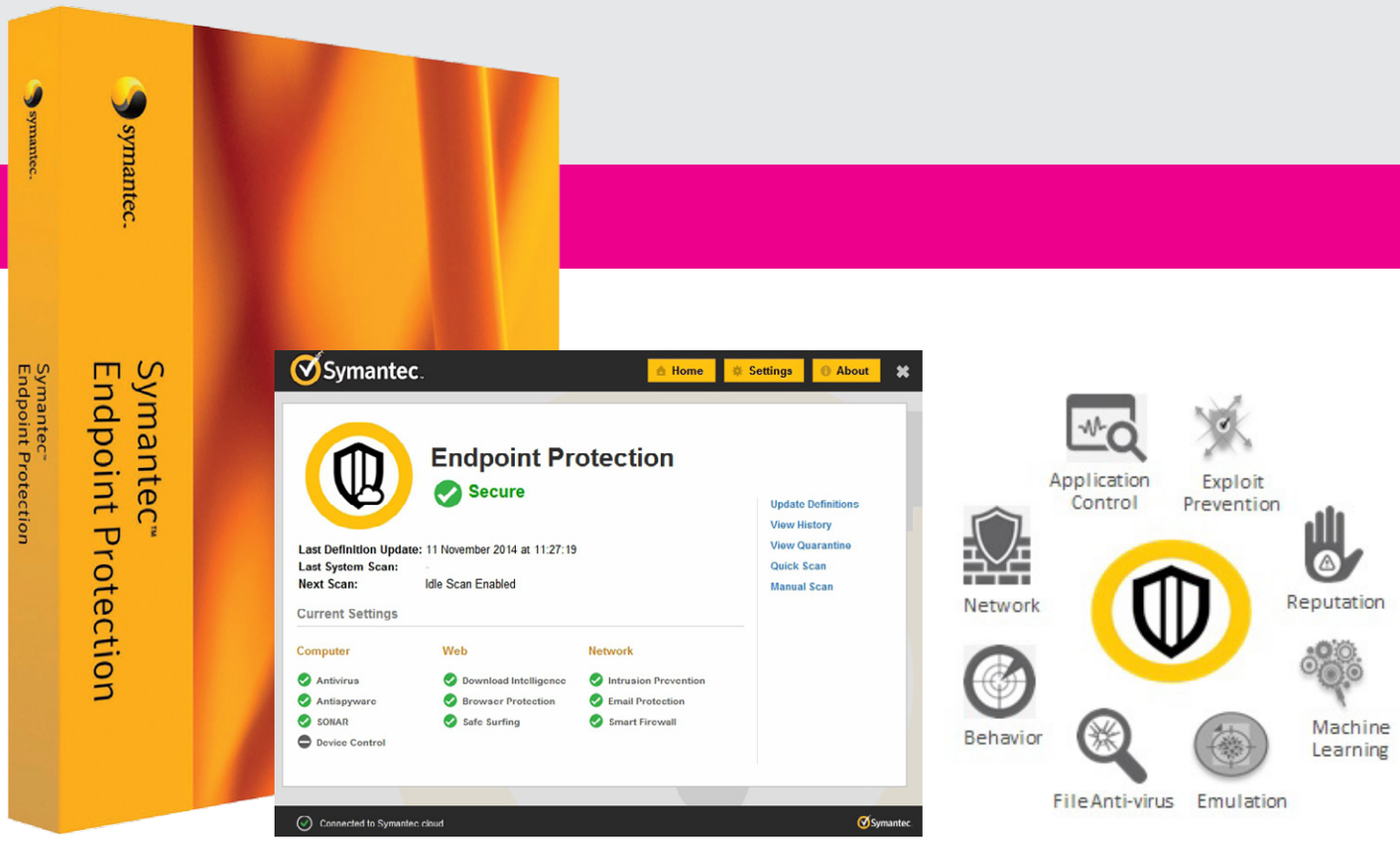
Zaštita endpointa zahteva brzu analizu pretnji u realnom vremenu – evaluaciju fajlova na osnovu njihovih atributa (statička), na osnovu ponašaja (dinamička) i njihovog globalnog konteksta (reputacija). Zaštitni slojevi su kombinacija dokazanih i novih tehnologija koje neprimetno rade na endpointu, a to uključuje analizu fajlova, reputacije i ponašanja zajedno sa firewallom, prevencijom upada i prevencijom pokušaja eksploatacije.

Jedini pravi odgovor na povećan obim pretnji je inovacija i integracija još većeg broja odbrambenih mehanizama kroz različite kontrolne tačke.

ZAŠTITA, DETEKCIJA I REAKCIJA U JEDNOM AGENTU

SEP14 objedinjuje endpoint zaštitu, detekciju i odgovor na pretnje u jednom agentu. SEP14 donosi moćnu zaštitu u laganom


Symantec™
079_00jackp9093_operation
01-K.graph
concept
node based object
INITIATING THE CODE:
WRITE
newly diagnosed
SMS Education
Research Updates
Conference Information
Contacting Material
Membership Area



pakovanju, uz vodeću efikasnost na tržištu od 99,9% i nisku stopu lažno pozitivnih, a zahteva čak 70% manje prostora na disku u odnosu na prethodnu generaciju proizvoda kroz unapređenja u korišćenju clouda. Uz sve ovo, SEP14 značajno smanjuje ukupne troškove za korisnika i pojednostavljuje upravljanje endpointima.

VEŠTAČKA INTELIGENCIJU I MAŠINSKO UČENJE

SEP14 koristi naprednu tehnologiju mašinskog učenja i u endpointu i u cloudu, a uz to koristi i dodatne mehanizme veštačke inteligencije u cloudu. Zašto je ovo važno? Mašinsko učenje nam omogućava detekciju nepoznatih pretnji ili familija pretnji koje evoluiraju u ranoj fazi infekcije kako bi se pretnje sprečile pre nego što dobiju šansu da se izvrše. Naši sistemi kontinuirano uče kako da razlikuju dobre od loših fajlova koristeći postojeću bazu informacija i obučene mašine. Tu ima jedna začkoljica: Mašine su pametne onoliko koliko su kvalitetni podaci koje koriste za učenje. Ova činjenica leži u korenu razloga zašto Symantec ima novi pristup za endpoint bezbednost – zato što postoji veštačka inteligencija u cloudu koja izvlači podatke iz Symantecove globalne informacione mreže, najveće civilne kolekcije informacija o globalnim pretnjama na svetu.

SC Magazine: „SEP14 je najsveobuhvatniji alat svoje vrste koji smo ikada videli i koji ima superiornu instalaciju i dokumentaciju“.

ULOGA BIG DATA

Symantec prikuplja informacije o pretnjama sa preko 175 miliona endpointa i 57 miliona senzora napada u različitim organizacijama, industrijama i geografskim područjima. Uz to, na raspolaganju je i više od 3,7 biliona nizova podataka koji su relevantni za sajber-bezbednost. Ova velika kolekcija informacija o različitim pretnjama se koristi kako bi mašine naučile kako da se ponašaju u prvim redovima globalne bitke koja se menja svakoga dana, iz minuta u minut. Pored globalne informacione mreže (Global Intelligence Network), SEP14 deli informacije i sa Blue Coatovim Secure Web Gatewayom. S obzirom na to da endpoint bezbednost uči od mrežne bezbednosti i obrnuto, pretnje se mogu identifikovati i blokirati na bilo kojoj od ovih kontrolnih tačaka.

Inovacija i integracija su ključne za endpoint bezbednost. Neprijatelji rade neprestano širom sveta razvijajući načine za krađu informacija, sabotažu poslovanja, iznuđivanje novca i zlonamerno mešanje u uobičajeni tok svakodnevnog života. Takođe, i reputacija je ključna, zato su u Symantecu ponosni na svoju globalnu zajednicu koju čine hiljade i hiljade organizacija i milioni ljudi koji su bezbednost svojih najvrednijih digitalnih resursa poverili Symantecu.

Symantec™

INSAJDERSKE PRETNJE
AUTOIMUNE BOLESTI IT SISTEMA

Insajder je svako ko ima pristup vrednim (osetljivim) podacima organizacije. To može biti zaposleni, poslovni partner, vendor ili neko ko je ranije imao pristup, a u organizaciji su zaboravili da mu ga ukinu (na primer, bivši zaposleni).

U izveštaju IBM-a, *2016 Cyber Security Intelligence Index,* navodi se da je čak 60% svih sajber napada povezano sa insajderima. Od tih 60%, 3/4 su napadi „zlonamernih" insajdera, dok je 1/4 napada posledica nenamerne greške insajdera. Najviše insajderskih napada beleži se u organizacijama iz sektora zdravstenih usluga, proizvodnje i finansijskih usluga.

Istraživanje instituta Ponemon pokazalo je da privilegovani korisnici, kao što su administratori baze podataka, mrežni inženjer, stručnjaci za IT bezbednost i osobe zadužene za cloud, često zloupotrebljavaju svoja odobrenja i izlažu riziku osetljive informacije organizacije. 58% stručnjaka i menadžera za IT bezbednost veruje da organizacije daju veća ovlašćenja zaposlenima nego što im je za obavljanje posla potrebno. Jedan od problema je što organizacije često ne mogu da utvrde da li neka aktivnost insajdera jeste ili nije pretnja. Insajderske incidente je najteže otkriti i često je za to potrebno da prođu meseci ili godine. Zabeleženo je 10.489 incidenata povezanih sa insajderima i privilegovanim korisnicima, a u 172 slučaja zabeleženo je kompromitovanje podataka (u proseku, 1 slučaj na svaka 2 dana).

OSNOVNE VRSTE INSAJDERSKIH RIZIKA SU SLEDEĆE:

- **Ljudska greška.** Ove greške mogu skupo koštati. U pitanju su, na primer, mejlovi poslati na pogrešnu adresu ili poverljivi podaci poslati preko nebezbedne mreže (ka ili od kuće). Najveći rizik nose IT administratori zato što imaju potpuni pristup IT infrastrukturi organizacije i stoga samo mala greška može značiti katastrofu.
- **Namerno „curenje" informacija**. Zaposleni sa lošim namerama predstavljaju realan i veliki rizik. Neki kradu informacije koje prodaju konkurenciji, a neki samo žele da naprave štetu kako bi se „osvetili" organizaciji.
- **Vuk u jagnjećoj koži**. Sajber-kriminalci su eksperti za krađu identiteta. Do krađe identiteta dolazi tako što napadači kompromituju računar zaposlenog malverom ili phishing napadom, a drugi način je krađa kredencijala, posebno sa društvenih mreža. U mnogim slučajevima, napadači uspevaju da dobiju i viši nivo privilegija od zaposlenog čiji su nalog hakovali i tako dolaze do još vrednijih podataka.

KAKO SE ZAŠTITITI?

Kako se organizacije najčešće štite od insajderskih pretnji? Najpre tako što proveravaju kandidate pre nego što ih zaposle, zatim preko orijentacije, zabranom pristupa određenim delovima sistema, obaveštenjima o polisama korišćenja itd. Sve to često nije dovoljno da se spreče zloupotrebe.

Insajderske pretnje i napadi su jako skupi za organizaciju:

- Zbog toga što ih je teško otkriti.
- Zbog toga što je za otkrivanje potrebno dosta vremena.
- Zbog toga što je potrebno vreme i novac da se saniraju posledice.

Najopasniji aspekt insajderskih pretnji je činjenica da se radi o sistemima i poje-

dincima koji su od poverenja tako da se potencijalno opasne aktivnosti mogu provući ispod radara bezbednosnih alata za detekciju i menadžerske kontrole. Insajderi mogu obrisati dokaze o svojim malicioznim aktivnostima i tako otežati eventualnu forenzičku istragu. Neke kompanije su zato uspostavile okruženje „nultog poverenja". Međutim, to nije dobro rešenje, jer negativno utiče na produktivnost, inovativnost i generalno frustrira korisnike. Srećom, analitika i napredak u oblasti veštačke inteligencije omogućavaju jednostavnija i elegantnija rešenja za detekciju potencijalnih insajderskih pretnji. Pritom je neophodno da menadžeri znaju šta da traže i kako da na najbolji način iskoriste bezbednosna rešenja i znanje o problematici kojim raspolažu.

Potrebno je imati u vidu sledeće:

1) ŠTA BI TREBALO ZAŠTITITI?

- Fokusirajte se na najvrednije resurse. Potrebno je zaštititi informacije i usluge. Informacije postoje u formi dokumenata (fizičkih ili virtuelnih), zatim kao izvorni kôd, u mejlovima, kod ljudi (da, ljudi su ti koji često poseduju ključne informacije koje nisu sadržane u dokumentima) itd. Vrsta usluga zavisi od vrste delatnosti u kojoj poslujete.
- Napravite listu informacija i usluga prema nivou kritičnosti odnosno važnosti za vaše poslovanje. Postavite jednostavno pitanje: Ako se nešto dogodi sa određenom informacijom/uslugom, da li se poslovanje može nesmetano nastaviti? Ako je odgovor DA, onda taj resurs nije kritičan. Primenite najjaču zaštitu na najvrednije, odn. kritične podatke i za njih primenite najfrekventniji monitoring.

2) OD KOGA BI SE TREBALO ZAŠTITITI?

Insajder koji je učestvovao u incidentu nije uvek šef (osoba sa specijalnim ovlašćenjima) ili ekspert (inženjer). U trećini slučajeva u pitanju su krajnji korisnici koji su imali uvid u osetljive podatke jer im je to potrebno za obavljanje posla. Samo mali procenat su zaposleni na rukovodećim mestima, a isti taj procenat čine zaposleni sa većim ovlašćenjima poput sistem administratora i developera. Poenta priče je da bi trebalo manje brinuti o formalnoj poziciji, a više o nivou ovlašćenja koji zaposleni imaju i mogućnostima njihovog nadzora. Preporučuje se jedan zdrav nivo sumnje prema svim zaposlenima.

3) PRIMENITE DUBINSKU ANALITIKU.

Ljudi vole da se drže svojih navika – dolaze na posao u isto vreme i obavljaju poznate zadatke. Isto važi i kad je u pitanju način na koji koriste tehnologiju. Dubinska analitika i veštačka inteligencija mogu otkriti devijacije u ponašanju svakog zaposlenog što značajno olakšava pronalaženje dokaza o kompromitovanosti sistema.

4) UPOZNAJTE KLJUČNE INSAJDERE.

Razumevanje korisnika koji potencijalno mogu napraviti veliku štetu je od krucijalne važnosti. Trebalo bi proceniti koliki bezbednosni rizik svako od njih nosi. Sa posebnom pažnjom treba nadzirati IT administratore, top menadžment, ključne vendore i ostale zaposlene koji imaju pristup najvrednijim resursima kompanije.

5) NE ZABORAVITE OSNOVE BEZBEDNOSTI.

U oblasti bezbednosti novi alati su veoma poželjni. Međutim, bitno je poštovati stare, dobro poznate bezbednosne preporuke – redovno ažuriranje softvera kako hakeri ne bi iskoristili ranjivost, primenu visokih standarda autentifikacije korisnika kako bi se otežala krađa kredencijala, prikupljanje svih podataka i forenzike sa svih uređaja koji dolaze u interakciju sa vašom mrežom kako bi prvi saznali da li ste hakovani. Bez obzira na tehnologiju, ključ edukacije insajdera su programi obaveštenosti. Organizujte treninge, testirajte ih i zadajte im iznenadne vežbe.

BALABIT SCB

BALABIT

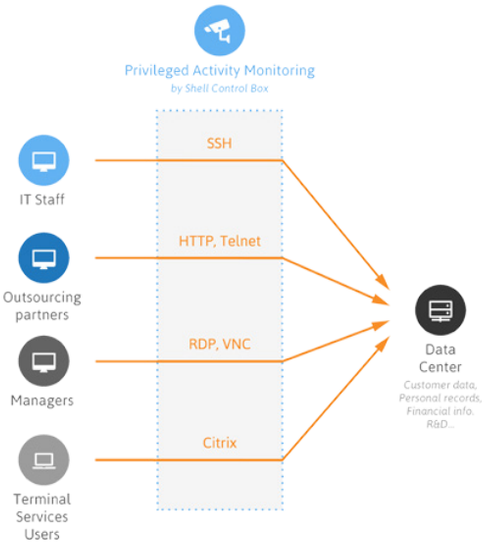
Kontrola pristupa može doneti više štete nego koristi. Zbog nefleksibilnosti, ona obično ne može da spreči gubitke ali zato sprečava ljude da efikasno obave svoj posao. Napredan monitoring može da bude efektivan alat protiv IT bezbednosnih rizika povezanih sa ljudskim faktorom, bez obzira da li je izvor eksterni ili interni. Ljudski rizik može se drastično umanjiti otkrivanjem i blokiranjem sumnjivog ponašanja korisnika. Obaveštavanje u realnom vremenu i monitoring su neizbežni za privilegovane naloge, koji imaju pravo da pristupaju, modifikuju ili brišu osetljive informacije, jer su njihovi podaci (credentials) primarna meta hakerima. Viši nivo detekcije je bolja prevencija nego pasivna kontrola i više je „business-friendly".

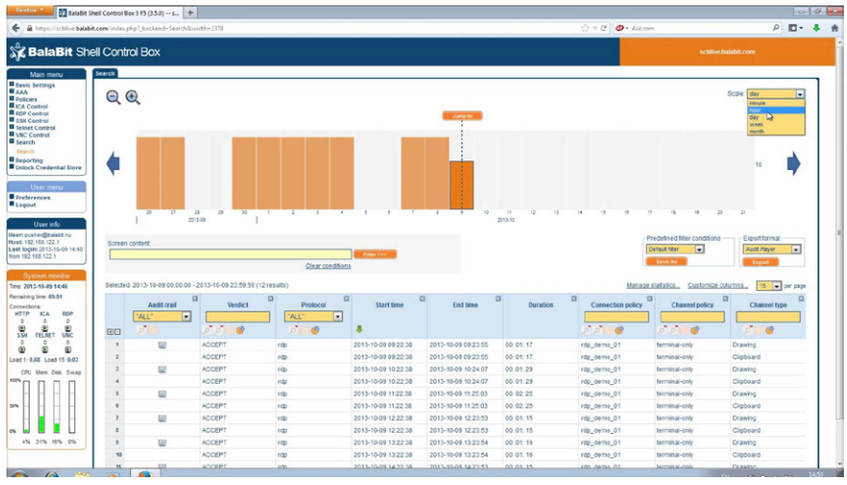
ŠTA JE REŠENJE ZA DETEKCIJU I PREVENCIJU LJUDSKIH GREŠAKA?

BalaBitov Shell Control Box, uređaj za monitoring rešava upravo ovaj složen problem. BalaBitov Shell Control Box (SCB) 4 LTS je uređaj za monitoring aktivnosti na nivou celog preduzeća koji kontroliše privilegovane pristupe udaljenim IT sistemima, snima aktivnosti kao pretražive revizijske tragove koje možete gledati kao film, i na taj način sprečava maliciozne akcije.

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE





SCB pomaže pri forenzičkim istragama IT sistema. Snimljeni revizijski tragovi mogu biti ponovo pušteni kao film kako bi se pregledali događaji tačno onako kako su se desili. Sadržaj revizijskih tragova se indeksira i na taj način omogućava se ad-hoc pretraživanje događaja i automatsko izveštavanje. Na primer, u slučaju manipulacije bazom podataka, okolnosti događaja se lako mogu videti u revizijskim tragovima, tako da se i uzrok incidenta može odmah otkriti. Dakle, SCB će vam pomoći ne samo da otkrijete uzrok problema, nego i osobu odgovornu za problem.

"KLJUČ U RUKE" UREĐAJ SA BRZIM RASPOREĐIVANJEM

Značajna prednost ovog uređaja je to što nije potrebno praviti nikakve izmene na postojećem IT okruženju. SCB može da se instalira i počne sa radom za 2 do 4 dana, i osoblje ne mora da menja radne procese.

VISOK KVALITET, REVIZIJA I FORENZIKA

SCB olakšava forenzičke istrage zahvaljujući mogućnosti pretraživanja bilo koje vrste komandi i sadržaja ekrana. Revizijski tragovi mogu imati vremensku oznaku, mogu biti kriptovani i potpisani.

UPOZORAVANJE U REALNOM VREMENU O MALICIOZNIM AKTIVNOSTIMA

Omogućava korisniku da blokira veze koje narušavaju konfigurisana pravila, kao i da šalje upozorenja u takvim situacijama.

KOJE SU POSLOVNE I TEHNIČKE PREDNOSTI ZA PREDUZEĆA KOJA PLANIRAJU DA INVESTIRAJU U OVAJ PROIZVOD?

SCB izoluje osetljive sisteme od nepoznatih uljeza ili neautorizovanih korisnika. Ono nadgleda sve udaljene pristupe kritičnim elementima IT sistema. Jaka autentifikacija i pristup kontrolnoj tački u IT okruženju koje **povećava bezbednost i smanjuje troškove administracije**.

SCB beleži ko je šta uradio u IT sistemima. Svesni toga, zaposleni će obavljati svoj posao odgovornije, što će dovesti do **smanjenja ljudskih grešaka**. Kada imate zapis koji je lak za tumačenje i koji se ne može menjati, lako je otkriti osobu odgovornu za grešku.

Zahvaljujući SCB **sve aktivnosti korisnika je moguće pratiti i snimati** ih u revizijske tragove koji se mogu lako pretraživati. Revizijski tragovi najvišeg kvaliteta omogućavaju pristup svim neophodnim informacijama putem ad-hoc analize ili izveštaja o aktivnosti.

Kada se desi nešto loše, analiziranje hiljada tekstualnih logova može da bude noćna mora i može zahtevati angažovanje skupih eksperata. SCB može lako da rekonstruiše incidente, što **skraćuje istragu i pomaže da se izbegnu nepredviđeni troškovi**.

KOLIKI SU UKUPNI TROŠKOVI OVOG PROIZVODA?

SCB se prodaje kao uređaj i kao virtuelni imidž. Implementacija i obuka ne traju duže od 2 do 4 dana. U roku od 2 sata posle implementacije SCB je spreman za korišćenje. SCB ima jednostavan web interfejs, firmware upgrade i mogućnost downgradea. Jedan uređaj može da rukuje sa više stotina paralelnih konekcija i sa sto hiljada uređaja. BalaBit IT Security nudi 24/7 podršku kao opciju. SCB radi u pozadini kao crna kutija, bez potrebe za dodatnim angažovanjem oko njega.

ZAŠTO JE OVAJ PROIZVOD DOBRA INVESTICIJA I NA KOJI NAČIN SE ULOŽENA SREDSTVA VRAĆAJU KUPCU?

SCB omogućava nesmetan i kontinuiran rad poslovnih operacija kompanije. Rezultat njegovog rada je viši nivo IT bezbednosti i manji rizik od neispunjavanja zahteva i usklađenosti sa propisima. SCB nudi bolju kontrolu zaposlenih i partnera tako što pruža dokaze za pristup privilegovanih korisnika. SCB takođe povećava odgovornost kod zaposlenih i pruža neoborive dokaze u pravnim postupcima.

SCB obezbeđuje brz povraćaj investicija kroz brže i kvalitetnije revizije, manje troškove traženja i otklanjanja grešaka i forenzike, centralizovanu autentifikaciju i kontrolu pristupa i nudi kompletno rešenje za monitoring privilegovanih korisnika.

KAKO DA **UKLONITE MALWARE** SA WINDOWS RAČUNARA U 6 KORAKA?

Da li vam računar radi sporije nego inače? Da li vam se pojavljuje puno pop-up prozora? Da li ste primetili neke druge, neuobičajene pojave na računaru? Ako jeste, vaš PC je verovatno pokupio virus, spyware ili neki drugi malver, uprkos tome što imate instaliran antivirus program. Sada ćemo vam u nekoliko koraka pokazati kako da izvršite proveru sistema.

KORAK 1
PRIPREMITE SE (PO MOGUĆSTVU NA SIGURNOM RAČUNARU, KOJI NIJE ZARAŽEN)

Preuzmite alate koji vam mogu pomoći da detektujete viruse/pretnje na računaru. Na raspolaganju je niz besplatnih alata koji omogućavaju i online (dok ste na Internetu) i offline skeniranje računara.

Naš savet je da probate sa dva odlična alata:

- **SymDiag (Symantec)** - koji možete da preuzmete ovde: http://www.symantec.com/docs/TECH170752
- **Malwarebytes** - koji možete da preuzmete ovde: https://www.malwarebytes.com/mwb-download/thankyou/

Pored ovih alata tu su još i Kaspersky Virus Removal Tool, Microsoft Malicious Software Removal Tool, BitDifender Free Edition i drugi.

Snimite alate koje ste preuzeli na USB i bacite se na zaraženi računar.

KORAK 2
POKRENITE SISTEM U SAFE MODE-U

Najpre **diskonektujte računar sa interneta** i nemojte se povezivati dok ne budete spremni da očistite računar. To može pomoći da se zaustavi širenje malvera i/ili kompromitovanje vaših fajlova. Ako sumnjate na malver, pokrenite računar iz **Safe Mode-a**. U ovom modu dostupni su samo neophodni programi i servisi. Ako je malver programiran da se automatski pokrene pri pokretanju Windowsa, Safe Mode to može sprečiti. Ovo je važno zbog toga što se odatle fajlovi mogu lakše uklanjati jer nisu pokrenuti ili aktivni.

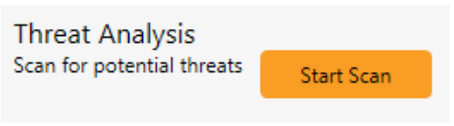
Nažalost, Microsoft je zakomplikovao proces ulaska u Safe Mode u Windows 10 u odnosu na Windows 7 i 8. Da uđete u Safe Mode kod **Windows 10** operativnog sistema, kliknite na Start i odaberite dugme Power, ali nemojte kliknuti ni na šta. Onda držite Shift i kliknite na Reboot. Kada se pojavi meni celog ekrana, izaberite **Troubleshooting** -->> **Advanced Options** -->> **Startup Settings**. U sledećem prozoru kliknite dugme Restart i čekajte da se pojavi sledeći ekran. Pojaviće se meni sa Startup opcijama – odaberite broj 4, tj. Safe Mode. Da napomenemo, ako želite da koristite neki od online skenera morate izabrati opciju broj 5, a to je Safe Mode sa internetom.

Kada je u pitanju **Windows 7 (ili 8)**, u Safe Mode se ulazi mnogo jednostavnije – dovoljno je pre nego što se učita operativni sistem (dakle, odmah pošto ste uključili računar) da pritisnete **F8** (nekada pomaže uzastopno pritiskanje F8) dok se ne pojavi Safe Mode meni.

Moguće je da će vaš računar raditi primetno brže u Safe Mode-u. To verovatno znači da je sistem zaražen malverom, mada može značiti i da vam se puno regularnih programa pokreće zajedno sa Windowsom.

KORAK 3
IZBRIŠITE PRIVREMENE FAJLOVE (ENG. TEMPORARY FILES)

Za brisanje možete koristiti ugrađeni **Disk Cleanup** utility u Windows 10. U Safe Mode-u pokrenite skeniranje virusa. Pre toga, izbrišite privremene fajlove. To može ubrzati skeniranje, osloboditi prostor na disku, pa čak i ukloniti neke malvere. Disk Cleanup utility ćete naći ako u pretragu ukucate „Disk Cleanup“ ili će vam se pojaviti ako kliknete na dugme Start.

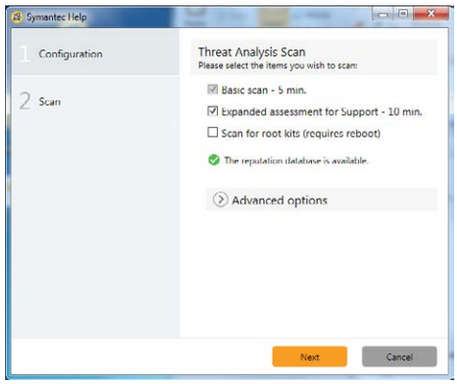


KORAK 4, OPCIJA A
SKENIRAJTE SISTEM SA SYMDIAG ALATOM

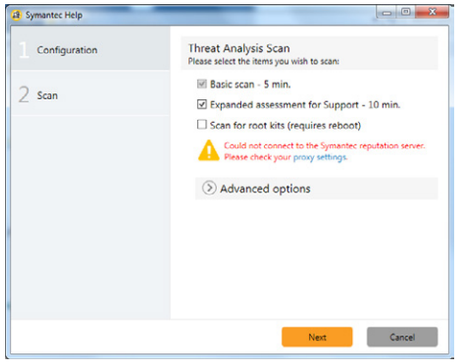
Dva puta kliknite na preuzeti fajl, **SymDiag**, da ga pokrenete i prihvatite EULA...

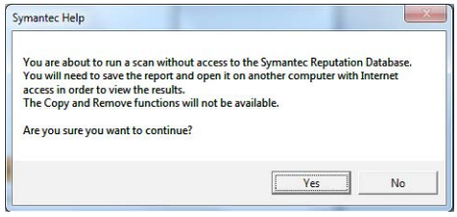
Zatim kliknite na dugme **'Start Scan'** pored 'Threat Analysis' u delu **'Scans'** na naslovnoj strani:

Pojaviće se dijalog **'Threat Analysis'** gde je dovoljno da kliknete **'Next'** kako bi skeniranje računara počelo (možete da odaberete i opciju **'Scan for root kits'**):



Ako računar nije povezan na Internet, možete da nastavite sa skeniranjem, ali je potrebno da rezultate skeniranja snimite kako bi kasnije mogli da ih analizirate na računaru koji ima pristup Internetu, tačnije **Symantec Reputation** bazi:

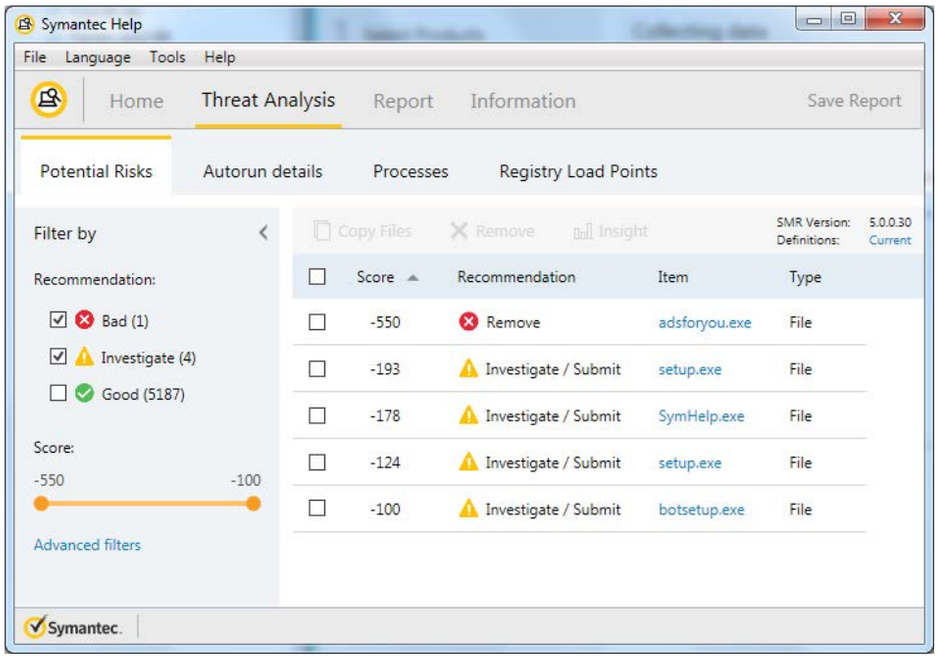




Ako imate pristup Internetu kada se završi skeniranje prikazaće se opcije koje će vam pružiti dodatnu analizu. Ove opcije uključuju:

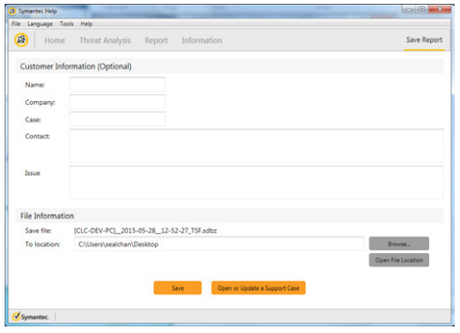
- Kopiranje jednog ili više fajlova u zip kako bi mogli da ih pošaljete Symantec-u na analizu (možete da upotrebite i **Virus Total** servis, www.virustotal.com);
- Uklanjanje fajlova;
- Filtriranje prikaza fajlova;
- Pregled podataka koji su prikupljeni tokom analize.

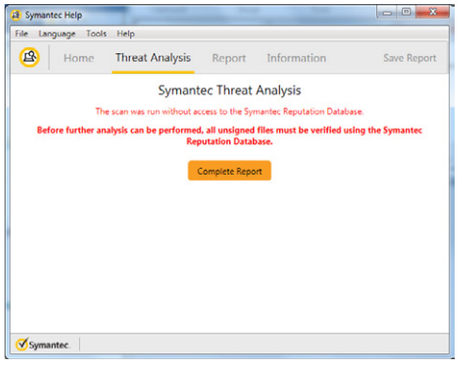
Ako ste pokrenuli analizu bez pristupa Internetu, potrebno je da snimite rezultate analize, kako bi dovršili posao na računaru sa pristupom Internetu, tj. Symantec Reputation bazi. Izaberite **'Save'** listić da dođete do strane za snimanje rezultata analize gde možete da izaberete direktorijum gde će fajl biti snimljen (USB koji ste pripremili u prvom koraku, na primer). Fajl je sa nastavkom **.sdbz** i može se otvoriti sa SymDiag alatom.



Da završite skeniranje koje ste pokrenuli na računaru bez pristupa Internetu, pokrenite isti alat, SymDiag na računaru koji ima pristup Internetu i Symantec Reputation bazi i u meniju izaberite **File >> Open Report** i otvorite fajl koji ste snimili sa .sdbz ekstenzijom. Izaberite **'Threat Analysis'** listić i zatim kliknite na **'Complete Report'** dugme.

Proverite fajlove koji imaju negativan rezultat analize (označeni crvenom bojom) u izveštaju – velika je verovatnoća da su upravo ti fajlovi virus ili delovi virusa. Obavezno pošaljite ove uzorke na analizu (bilo Symantec-u, bilo preko Virus Total servisa) i proverite da li se zaista radi o virusu i ako je potrebno ukolonite ih. SymDiag sadrži u sebi i **Power Eraser** koji efikasno uklanja pronađene viruse.





KORAK 4, OPCIJA B
SKENIRAJTE SISTEM SA MALWAREBYTES

Pokrenite Malwarebytes koji ste preuzeli u prvom koraku sa USB-a. Kada ste instalirali program, pokrenite podrazumevanu opciju **"Threat Scan"** (prvo će se izvršiti provera ažuriranja). Ova opcija je uglavnom dovoljna da pronađe sve infekcije. Kada se završi skeniranje, dobićete rezultate. Ako vam izađe obaveštenje da nema malvera, ali vi i dalje sumnjate, pokrenite **"custom scan"** i probajte neki od drugih, gore pomenutih skenera. Ako Malwarebytes pokaže da ima infekcija, uklonite ih pomoću opcije **"remove"** i restartujte računar ako se to traži. Ako se problem nastavi, pokrenite **"full scan"** (i u Malwarebytes i u drugim skenerima). Ako mislite da je malver uklonjen, pokrenite „full scan" u vašem AV programu u realnom vremenu da bi potvrdili rezultate.

Može se desiti da nakon pokretanja Malwarebytes nestane, a to verovatno znači da je u pitanju neka duboka infekcija i onda je bolje i mnogo jednostavnije da prvo izvršite backup fajlova, a zatim i da reinstalirate Windows ili da prepustite računar nekome ko ima više iskustva i znanja.

KORAK 5

„POPRAVITE“ I INTERNET PREGLEDAČ

Postoje malveri koji menjaju vašu početnu stranicu u pregledaču (browser-u) kako bi nanovo inficirali vaš računar, prikazivali reklame, sprečavali vas da surfujete i nervirali vas. Pre nego što pokrenete pregledač, proveriti početnu stranicu i podešavanja konekcije.

KORAK 6

AKO JE MALVER UPORAN, URADITE BACKUP I REINSTALIRAJTE WINDOWS

Ako niste uspeli da uklonite malver ili ako Windows ne radi kako treba, morate da reinstalirate Windows ili da računar odnesete na servis, tj. da ga prepustite nekome ko ima više iskustva i znanja. Pre toga, kopirajte fajlove na eksterni disk ili USB. Ako koristite neki imejl klijent (npr. Outlook), eksportujte podešavanja i poruke kako bi ih sačuvali. Takođe, uradite backup drajvera pomoću aplikacija poput Double Driver ukoliko ne želite da ih ponovo preuzimate. Nakon što ste izvršili backup svega neophodnog, možete reinstalirati Windows.

KAKO DA VAŠ RAČUNAR OSTANE ČIST I BEZ MALVERA?

Uvek koristite najnoviju ažuriranu verziju AV programa u realnom vremenu. Možete dodatno koristiti besplatni **OpenDNS servis** (https://www.opendns.com/home-internet-security/) koji blokira opasne sajtove. Ako posećujete sumnjive sajtove, možete se zaštititi tako što ćete pokrenuti internet pregledač u sandbox mode-u (to sprečava da malver nanese štetu sistemu). Proverite vaše onlajn naloge (bankovne naloge, imejl i društvene mreže) i fokusirajte se na sumnjive aktivnosti. Ako ih primetite, promenite lozinke zato što sajber-kriminalci mogu doći do njih pomoću određenih malvera.

Ako koristite automatski backup fajlova, skenirajte i njih kako bi bili sigurni da slučajno nije sačuvan neki zaraženi fajl. Neka vam sve aplikacije, uključujući i Windows, uvek budu ažurirane. Najbolje je da bude podešena opcija automatskog ažuriranja sistema i aplikacija, gde god je moguće.

KAKO DA OTKRIJETE PROBLEME NA MREŽI POMOĆU WIRESHARKA?

Wireshark je besplatan alat za analizu mreže za Windows, Mac i Linux. Koristi se za ispitivanje podataka koji prolaze kroz mrežu, bilo da se radi o Ethernetu, LAN-u, wirelessu.

Kako Wireshark funkcioniše? Svi podaci koji prolaze kroz mrežu su u obliku paketa. Paketi se sastoje od različitih vrsta podataka, od browsing istorije do logova, a Wireshark hvata sve pakete koji se šalju ili primaju kroz mrežu i dekodira ih, što nam omogućava da ih analiziramo.

Fleksibilnost i dubina inspekcije je ono što ovaj alat čini nezamenljivim za ispitivanje sumnjivih programa koji prolaze kroz mrežu, za analizu protoka saobraćaja i za troubleshoot mrežnih uređaja za bezbednost.

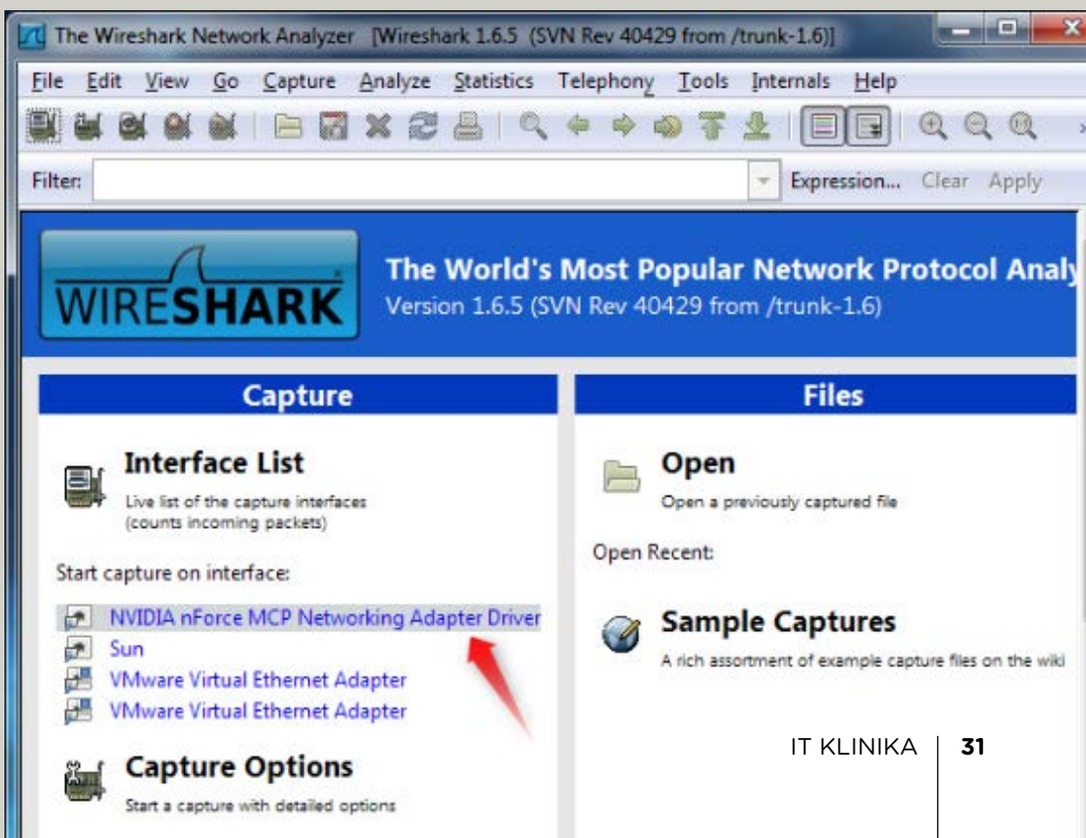
Zašto je važno pratiti mrežni saobraćaj? Prvo, u slučaju napada na mrežu, gledanjem detalja paketa dolazimo do izuzetno važnih informacija koje mogu da pomognu u kreiranju kontra mera. Na primer, ako dođe do DoS (denial od service) napada, Wireshark može da se koristi za otkrivanje izvora napada. Na osnovu dobijenih podataka možemo da kreiramo firewall pravilo kojim blokiramo neželjeni saobraćaj.

Drugo, Wireshark možemo da koristimo za troubleshoot uređaja za bezbednost, recimo za troubleshoot firewall pravila. Ako je sistem na kojem vam je Wireshark povezan sa firewallom, lako možemo da vidimo koji paketi uspešno zaobilaze uređaj i da utvrdimo da li je firewall uzrok problema.

Međutim, Wireshark koriste i dobri i loši momci. U rukama administratora mreže, Wireshark je vredan troubleshoot alat, ali u rukama sajber kriminalaca, postaje alat za prisluškivanje i krađu informacija. Zato treba biti oprezan pri korišćenih javnih otvorenih mreža.

KAKO SE WIRESHARK KORISTI?

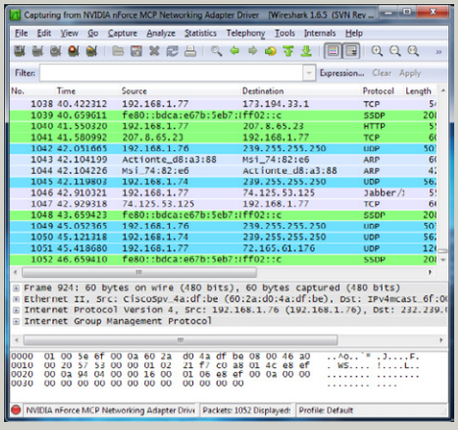
Wireshark se jednostavno instalira. Za Windows ili Mac OS X, Wireshark možete da preuzmete na zvaničnom web sajtu wireshark.org. Ako koristite Linux ili neki



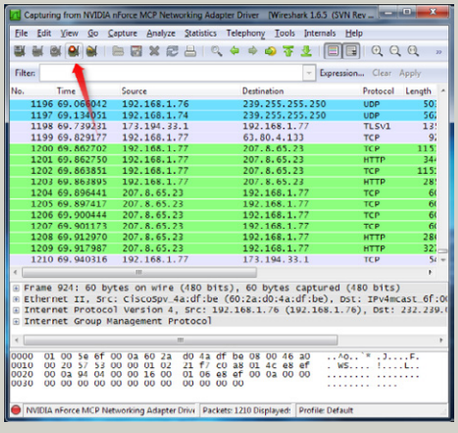
drugi Unix sistem, trebalo bi da nađete Wireshark u standardnom sistemskom paketu na svojoj platformi. Takođe, na zvaničnom sajtu možete da nađete i Source code za instalaciju na druge operativne sisteme.

Kada preuzmete i instalirate Wireshark, pokrenite ga. Da biste počeli sa snimanjem saobraćaja, u meniju Capture kliknite na ime interfejsa u Interface Listi na kom želite da pratite saobraćaj. Ako recimo hoćete da pratite saobraćaj u wireless mreži, izaberite wireless interface.

Kad kliknete na ime interfejsa videćete da paketi počinju da se pojavljuju.



Kad budete želeli da prekinete snimanje saobraćaja i analizirate neki paket, kliknite na stop dugme u gornjem levom uglu.

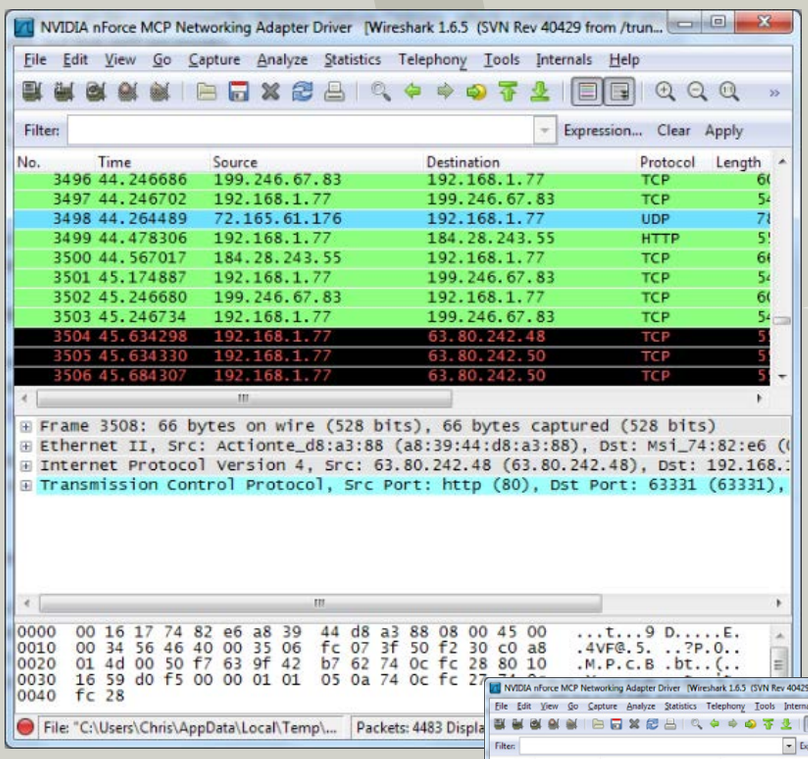


KAKO INTERPRETIRATI REZULTATE?

Svaki red u Wireshark prozoru označava jedan paket. Možete da vidite vreme kad je paket poslat, IP adresu izvora i destinacije, protokol koji je korišćen i neke informacije o paketu.

ŠTA ZNAČE BOJE?

Primetićete odmah da su redovi, odnosno paketi različitih boja – zeleni, plavi i crni. Wireshark koristi boje da bi vam pomogao



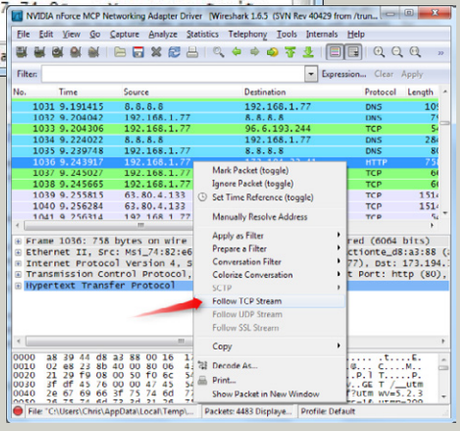
da već na prvi pogled identifikujete tip saobraćaja. Prema podrazumevanim podešavanjima, zelena je boja za TCP saobraćaj, tamno plava za DNS saobraćaj, svetlo plava za UDP, a crna označava TCP pakete koji imaju neke probleme. Šemu boja možete i sami da birate i prilagođavate.

FILTRIRANJE PAKETA

Ako želite da ispitate nešto konkretno, možete da primenite filter kako bi vam se prikazali samo paketi koji ispunjavaju taj parametar. Na primer, želite da vidite samo DNS pakete, ukucajte „dns“ u filter box na vrhu prozora i kliknete na Apply ili stisnite Enter. Prikazaće vam se samo DNS paketi.

Takođe, u meniju Analyze možete da kreirate i novi filter, izaberite Display Filters i kreirajte novi filter.

Još interesantnih informacija možete da dobijete kada kliknete desnim klikom na neki od paketa i izaberete select Follow

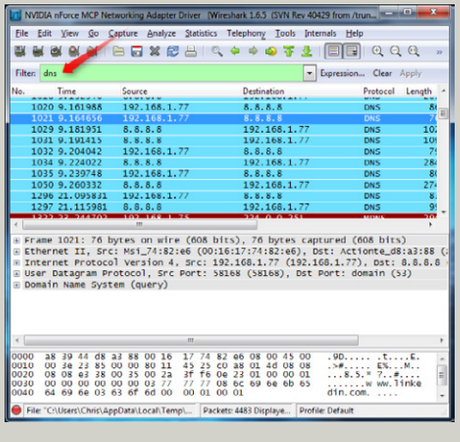


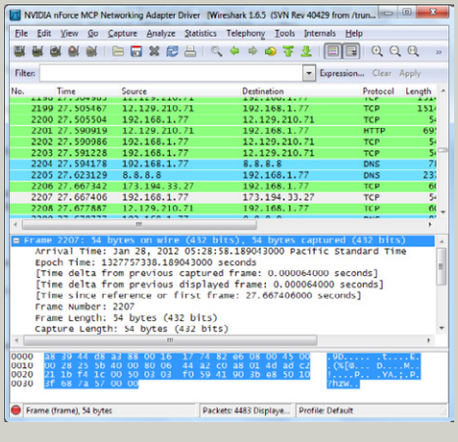
TCP Stream. Ova opcija omogućava vam da vidite celokupnu konverzaciju klijenta i servera.

ISPITIVANJE PAKETA

Ako kliknete na paket možete da vidite detaljnije informacije o paketu. Ove informacije prikazaće vam se u donjem prozoru.

Ovo su osnove korišćenja Wiresharka snimanje i analiziranje mrežnog saobraćaja. Preporučujemo da i sami krenete da istražujete sve mogućnosti ovog alata.





CHECKLISTA ZA BEZBEDNOST VAŠEG SAJTA

KADA POSTAVITE SAJT NA INTERNET, ON POSTAJE IZLOŽEN POTENCIJALNIM HAKERSKIM NAPADIMA i aplikacijama koje skeniranju portove, analiziraju saobraćaj i skupljaju podatke. Ako imate sreće, možda će vaš sajt zabeležiti i određenu količinu legitimnog saobraćaja, ali ne ako vam pre toga neko sruši ili hakuje sajt. Mnogi od nas znaju da pri surfovanju internetom treba obratiti pažnju na to da li određeni sajt ima ikonu katanca (SSL sertifikat koji garantuje da je sajt bezbedan), ali to je samo delić onoga što možete da uradite za bezbednost vašeg sajta. I što se tiče samog SSL-a, postoje bolji i lošiji, oni koji pružaju veći i manji obim i kvalitet zaštite. Cookiesi čuvaju osetljive informacije sa sajta i bitno je da budu zaštićeni na pravi način. Takođe, ako konfigurišete puno korisnih opcija u podešavanjima sajta to će pomoći u zaštiti od napada i sprečiti kompromitovanje podataka vaših klijenata. Pripremili smo uputstvo od 12 koraka koje će pojačati otpornost i podići nivo zaštite vašeg sajta.

1 POKRIJTE SSL-OM SVE STRANICE SAJTA

Pretpostavljate da katanac u browser address baru znači da vam je sajt bezbedan. Međutim, to u stvari samo znači da trenutno postoji SSL konekcija na toj stranici. Za potpuno korišćenje svih mogućnosti koje nudi SSL, on treba da bude primenjen na ceo sajt, a ne samo na pojedinim stranicama. Ukoliko ceo sajt nije pokriven SSL-om, i najmanja sitnica može kompromitovati ceo sajt.

2 VERIFIKUJTE SSL SERTIFIKAT

Kada vam ističe SSL sertifikat? Da li ga najveći browseri po difoltu označavaju kao bezbednog (trusted)? Ako znate odgovore na ova pitanja, vaš trud oko implementacije SSL-a nije bio uzaludan i neće se dogoditi da vam slučajno istekne sertifikat ili da nekom vašem klijentu izađe obaveštenje da je sajt nebezbedan. Najbolje je da imate neki mehanizam koji će vas obavestiti kad se približi kraj roka važenja sertifikata. Sertifikate većine glavnih provajdera sertifikata browseri automatski označavaju kao bezbedne, ali svakako pre kupovine proverite da li vaš provajder i dalje prati sve bezbednosne promene koje proizvođači browsera unose. U suprotnom, može vam se desiti situacija da imate sertifikat sa slabim Diffie-Hellmann ključem, a te sajtove Firefox i Chrome blokiraju. Velike promene poput ove zahtevaju da administratori sajtova reizdaju sve sporne sertifikate ili da ažuriraju konfiguraciju servera.

3 KORISTITE ENKRIPCIJU SHA256

Kada govorimo o velikim promenama, sertifikati koji koriste standard SHA1 više se ne smatraju bezbednim. Umesto njega, sada se koristi standard SHA256 koji je drastično unapredio enkripciju. Ako i na vašem sajtu postoji sertifikat sa SHA256, onda je to u skladu sa modernim zahtevima. Ako imate samo SHA1, onda treba da se reizda novi ili zameni sa 2048-bitnim SHA256 sertifikatom zato što će podrška za SHA1 biti uklonjena u većini browsera od 2017. godine. Standardi enkripcije će se menjati i u budućnosti kako se budu otkrivale slabosti u postojećim standardima i kako se budu razvijali novi, bezbedniji enkripcijski metodi.

4 ONEMOGUĆITE NEBEZBEDNE CIPHER SUITES

Čak i ako imate najbolje enkripcijske opcije na raspolaganju, to ne znači da nemate podešene i neke lošije opcije zajedno sa njima. Difoltne konfiguracije na većini web servera i dalje dozvoljavaju SSL cipher suites koji se smatraju nebezbednim, poput RC4. Oni se moraju onemogućiti na web serveru (Apache, IIS) kako maliciozni hakeri ne bi mogli da eksploatišu tu slabost. Ovo nije ključno samo za bezbednost, već i za upotrebljivost vašeg sajta s obzirom na to da neki browseri automatski blokiraju sajtove koji dozvoljavaju nebezbedne cipher suites.

5 ZAMASKIRAJTE INFORMACIJE U ZAGLAVLJU (HEADERU)

Ako javno objavite tip i verziju vašeg web servera to će samo pomoći hakerima koji vrebaju priliku da ga kompromituju. Kada potencijalni napadači znaju koja je platforma i verzija servera u pitanju, onda mogu da se fokusiraju na njihove poznate ranjivosti. Ovo važi za X-Powered-By headers, header za informacije o serveru i ASP .NET headers. Najbolje je da te heade-

re zamaskirate i da posetiocima ne pružate nikakve identifikacione informacije. Ovo nije podrazumevano podešavanje tako da mnogi serveri, verovatno nenamerno, pružaju informacije o headerima.

6 OMOGUĆITE HTTP STRICT TRANSPORT SECURITY

HTTP Strict Transport Security (Linux, Windows) se stara o tome da browseri komuniciraju sa sajtom samo preko SSL-a. Zahtevi koji nemaju SSL (http://) se automatski menjaju u SSL zahteve (https://). Ako se ova opcija ne omogući, može doći do man-in-the-middle napada u kome napadač može preusmeriti korisnika na lažni sajt.

7 KORISTITE HTTPONLY KOLAČIĆE

Zaštitom kolačića se starate o tome da informacije koje vaš sajt čuva o posetiocima ostanu privatne i da ih hakeri ne mogu eksploatisati. Koristite restriktivni pristup kolačićima 'HttpOnly cookies'. Ovo pruža dodatnu zaštitu modernim browserima koji podržavaju HttpOnly.

8 KORISTITE OBEZBEĐENE KOLAČIĆE

Obezbeđeni kolačići mogu se prenositi samo kroz SSL konekciju. To sprečava da neko „namiriše" kolačiće sa potencijalno osetljivim informacijama dok putuju između servera i klijenta. Ukoliko se ne koriste obezbeđeni kolačići, treća strana može da presretne kolačić poslat klijentu i da oponaša klijenta kod web servera. Da bi se koristili obezbeđeni kolačići, morate prvo imati postavljen SSL na celom sajtu kako kolačići ne bi bili izloženi nekriptovanim konekcijama.

9 OBEZBEDITE WEB SERVER PROCESE

Web server proces ili sam servis ne treba da se pokreće kao root ili Local System. Na Linux sistemima, većina web servera radi kao dodeljeni korisnik sa ograničenim privilegijama, ali treba da proverite koji je to korisnik i koja odobrenja ima. Na Microsoftovim sistemima, najverovatnije je Local System podrazumevano podešen tako da to morate promeniti pre nego što napravite nalog za dodeljeni servis, lokalni, osim ukoliko web server ne zahteva pristup resursima domena. Taj korisnik ne treba da bude administrator (ili još gore, admin domena), i treba da ima pristup samo onim fajlovima koji su mu neophodni. Ako ovo uradite sprečićete da kompromitovani web server dalje kompromituje druge resurse. To funkcioniše na taj način što se izoluje i ograniči nalog koji web server koristi.

10 KORISTITE VALIDACIJU UNOSA U FORMAMA

Ako imate forme koje prihvataju unose korisnika, mehanizam za unošenje podataka mora da bude validiran kako bi se samo odgovarajući podaci unosili i čuvali u bazi podataka. Ovo je prvi korak u zaštiti od SQL injections i sličnih napadačkih tehnika koje unose loše podatke i onda eksploatišu sajt. Ovaj korak mora da se preduzme u izgradnji sajta kako bi postao deo standardnih procedura (ukoliko već to nije).

11 ZAŠTITA OD SQL INJECTION

Drugi i najvažniji korak u zaštiti od ovih napada je da iskoristite dobro implementirane i sačuvane procedure umesto da otvarate upite koji će izvršavati funkcije baze podataka. Uvođenjem ograničenja da vaša web aplikacija pokreće samo sačuvane procedure će u najvećem broju slučajeva sprečiti pokušaje ubacivanja SQL koda u forme. Sačuvane procedure prihvataju samo određene vrste unosa i odbijaju sve što ne odgovara zadatim kriterijumima. Postoji i opcija da sačuvane procedure mogu da pokreću specifični korisnici u okviru baze podataka kako bi se napravila još veća ograničenja. Najbolje je ovo konfigurisati u toku izgradnje sajta.

12 ZAŠTITA OD DDOS NAPADA

O DDoS napadima detaljno smo pisali. Ne postoji stoprocentno siguran način da se ovi napadi spreče zato što napadači koriste legitimne komunikacione puteve, ali postoji način da se napadi ukrote ukoliko se dogode. Ukoliko koristite usluge cloud mitigation provajdera, gotovo sigurno ćete bezbolno prebroditi napad. Ova rešenja koriste postojanje razvijene i velike mreže clouda kako bi rasporedila teret DDoS napada, a pružaju i mehanizme za identifikovanje i blokiranje malicioznog saobraćaja. Možete postaviti i in-house sistem za ublažavanje posledica napada koji funkcioniše po sličnom principu, ali tu ste ograničeni resursima vašeg hardverskog rešenja.

ZAKLJUČAK

Ovo nisu jedini koraci koje možete da preduzmete kako bi se zaštitili od pretnji, ali oni štite najčešće ranjivosti. Možda još važniji doprinos ovih stavki je što njihova implementacija može voditi ka stvaranju svesti o tome koliko je bezbednost organizacije bitna. Konačno, redovnim testiranjem konfiguracija, kompanije mogu da prate promene i da otkriju bezbednosne probleme pre nego što ih hakeri eksploatišu.

Vaši kupci veruju vama.

Kome vi verujete?

Hakeri, špijuni i kradljivci pokušaće na sve načine da se domognu podataka sa vašeg sajta i da ga obore. Zato su Symantec Website Security rešenja naoružana moćnim funkcijama koje štite sajt bolje nego samo običan SSL. Pored SSL enkripcije koja je vodeća u industriji, sa Symantec Website Security rešenjima dobijate i anti-Malware skeniranje sajta, vidljiv Seal-in-Search, ocenu ranjivosti i nesavladivu proširenu validaciju. Symantecu možete poveriti bezbednost vašeg sajta i vaših kupaca.
Uspostavite kontrolu nad svojim sajtom pre nego što to neko drugi učini.

Norton™ SECURED
powered by Symantec

thawte™ it's a trust thing™

GeoTrust®

https://www.ssl.co.rs

Net++ TECHNOLOGY

Bulevar vojvode Mišića 39a, Beograd • Tel. 011/36 999 67, 40-53-516 • office@netpp.rs | www.netpp.rs

Net++ TECHNOLOGY

tel. (011) **36-999-67, 4053-516**
www.netpp.rs; **office@netpp.rs**