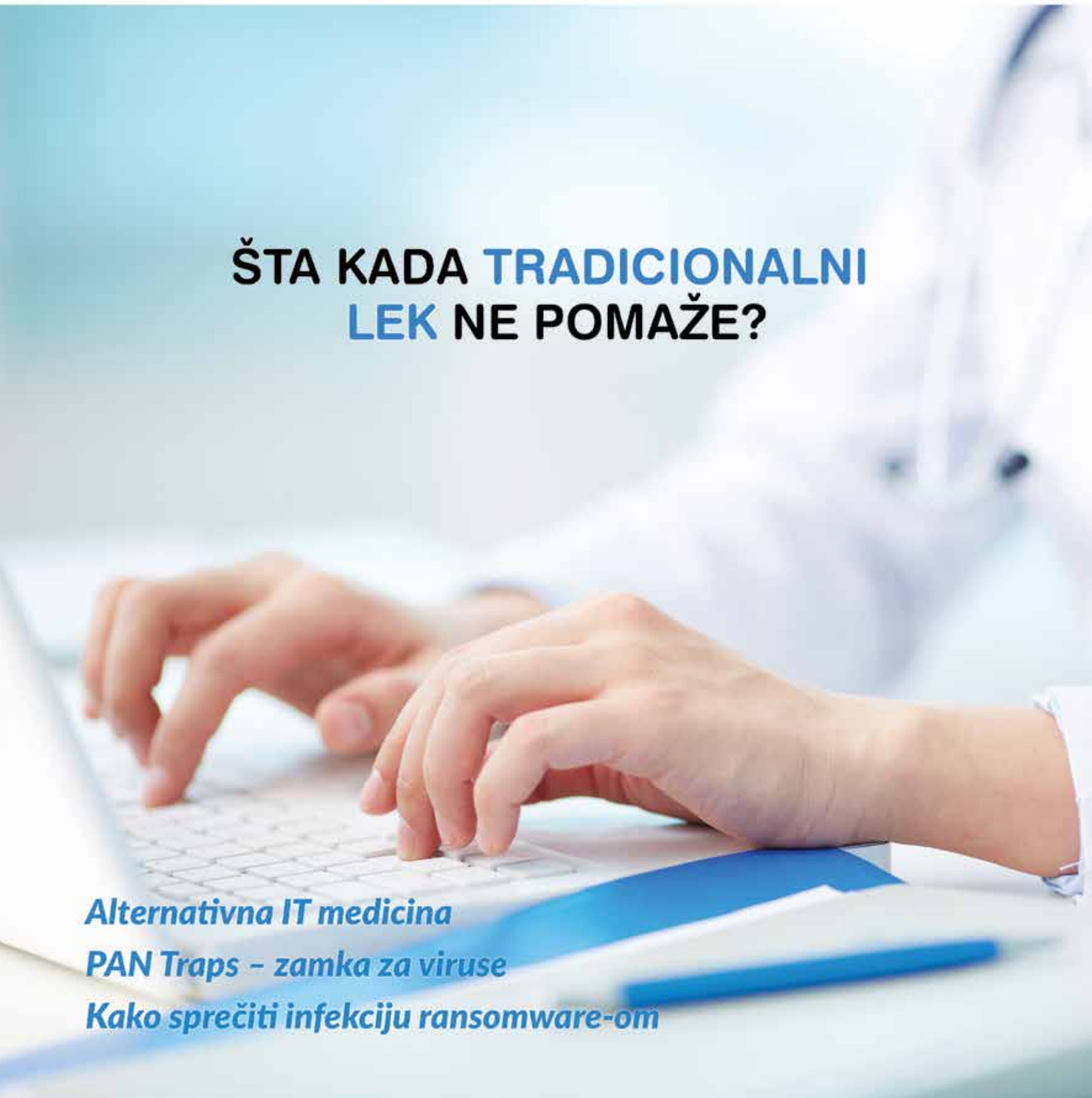
KLINIKA

Magazin posvećen vašem sajber zdravlju

maj 2016.

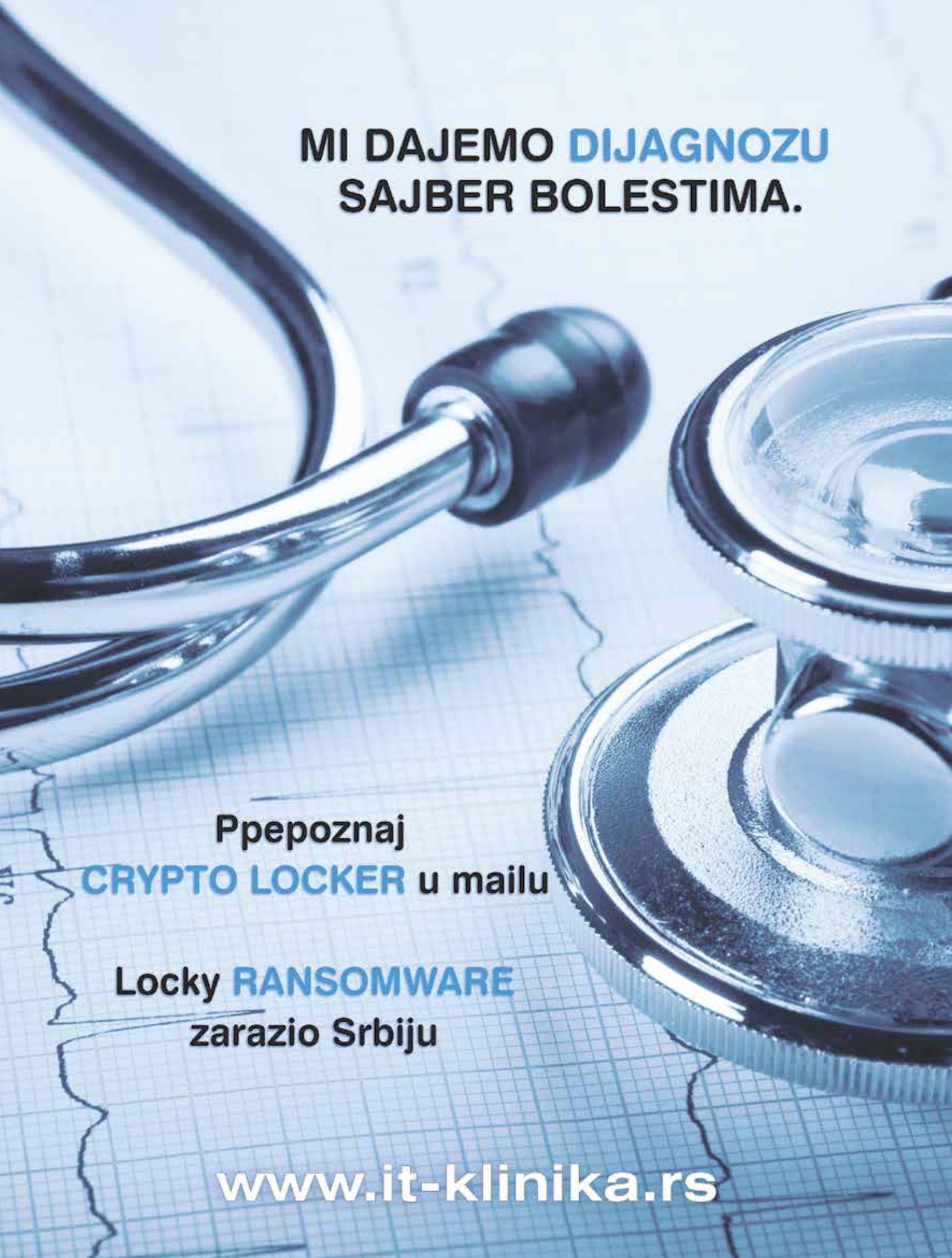


ŠTA KADA TRADICIONALNI LEK NE POMAŽE?

Alternativna IT medicina

PAN Traps – zamka za viruse

Kako sprečiti infekciju ransomware-om


MI DAJEMO DIJAGNOZU
SAJBER BOLESTIMA.
Ppepoznaj
CRYPTO LOCKER u mailu
Locky RANSOMWARE
zarazio Srbiju
www.it-klinika.rs

UVODNA REČ

Dragi čitaoci,

Pred vama se nalazi prvi broj časopisa „IT klinika“, namenjen IT menadžerima, IT security specijalistima i svima koji brinu za zdravlje IT sistema. Kroz ovaj časopis želimo da na zanimljiv način prikažemo aktuelne teme iz oblasti IT bezbednosti i predstavimo proizvode, ali i besplatne načine koji mogu da vam pomognu da unapredite vašu IT bezbednost. Izabrali smo naziv „IT klinika“ jer je IT bezbednost ključna za zdravlje IT sistema, a time i čitavog preduzeća s obzirom na moderan način poslovanja.

Naša zamisao je da „IT klinika“ ne bude reklamna publikacija, već da ponudimo interesantno i korisno štivo koje ćete voleti da čitate. „IT klinika“ je nekomercijalan časopis i neće se prodavati na kioscima. Želimo da nam i vi pomognete u uređivanju narednih izdanja tako što ćete nam predlagati teme, upućivati nam kritike ili pohvale i pisati o problemima sa kojima se vaš IT sistem susreće. Osim u štampanom obliku, naše tekstove ćete moći da čitate i na Web-u, na www.it-klinika.rs.

Ovaj broj posvetili smo crypto ransomware-u, novoj popularnoj metodi kojom se služe sajber kriminalci, a koja je postala prava noćna mora velikog broja IT administratora i stručnjaka za IT bezbednost. Crypto ransomware je ucenjivački malver koji kriptuje podatke svojih žrtava i traži otkupninu za njih, uz pretnju da će podaci biti izbrisani ukoliko žrtva ne reaguje na vreme. Na žalost, kako se radi o sajber kriminalcima, ni plaćanje otkupnine nije siguran način da žrtva vrati svoje fajlove. Budući da za crypto ransomware nema efikasnog leka, želeli smo da skrenemo pažnju na načine prevencije širenja ove zaraze. *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

Urednik izdanja
Bojan Stanojević, 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

AKTUELNOSTI
4 Upomoć, rasturi nas crypto Locker!
5 Zaraza iz oglasa
6 Tvorci SpyEye virusa osuđeni na 24 godine zatvora
8 Symantec ISTR 2016 - kako je izgledala 2015

PREVENCIJA
12 Kako sprečiti infekciju ransomware-om
13 Deset koraka za bolju IT bezbednost
14 Zaštitite računar od malvera na bazi Macro-a u dva koraka
15 Pet mitova o zaštiti od pretnji

LEČENJE
16 Šta je firewall nove generacije?
17 Kad tradicionalni lek ne pomaže – Antivirus je mrtav, šta dalje?
18 PAN Traps – zamka za viruse
20 Alternativna IT medicina – SaaS (security as a service)
22 BYOD - nove ranjive tačke bezbednosti sistema i podataka

PRIČE IZ ORDINACIJE
24 Istinita sajber horor priča
26 Analiza tipičnog JavaScript virusa

WEB SITE ZDRAVLJE
27 Šest stvari opasnih po zdravlje vašeg Web sajta
29 Šta je SSL i kako doprinosi zdravlju Web sajta?

UPOMOĆ, RASTURI NAS CRYPTO LOCKER!

Poslednjih nekoliko meseci *crypto locker*, *ransomware*, je hit tema u Srbiji i regionu. Prvobitna verzija pojavila se u martu 2015.g. i uglavnom se širila kroz igrice, pa su gejmeri bili i prve žrtve. Zaražene su uglavnom bile igrice koje su se preuzimale torentom. *Crypto Locker* šifruje fajlove, obriše originalne dokumente i traži otkup – plaćanje (odatle i izraz *ransomware*) za ključ kojim se mogu dešifrovati dokumenti/fajlovi. Zbog ograničenog načina infekcije, nije bilo mnogo žrtvi, ali je *cyber* podzemlje nastavilo sa razvojem *crypto locker*-a i danas svi vidimo rezultat...

Neko se dosetio da je najefikasniji način inficiranja kroz *e-mail* i to kroz najobičnije *Word* i *Excel* dokumente (uz pomoć *JavaScript*-a). Masovno se šalju e-mailovi koji liče na račune, zaduženja, vraćena plaćanja i sl. u kojima se nalazi *Word* ili *Excel* (po negde i sam *JavaScript*) u koje su vešto ubačeni makroi/skriptovi koji se izvršavaju i preuzimaju *crypto locker*, koji započinje svoj destruktivni posao – uništenje vrednih dokumenata, slika, mrežnih foldera...

Zbog veštog načina skrivanja, ove nove makro/*javascript* viruse je vrlo teško detektovati klasičnim tehnikama, tako da se dešava da prolaze kroz osnovne sisteme e-mail zaštite, a onda je samo pitanje kada će neko od korisnika kliknuti na *invoice*, *account statement* ili sličan dokument. Takođe, sam *ransomware* se menja, a veliki broj varijanti je moguće kupiti i na „crnom" tržištu *cyber* kriminalaca.

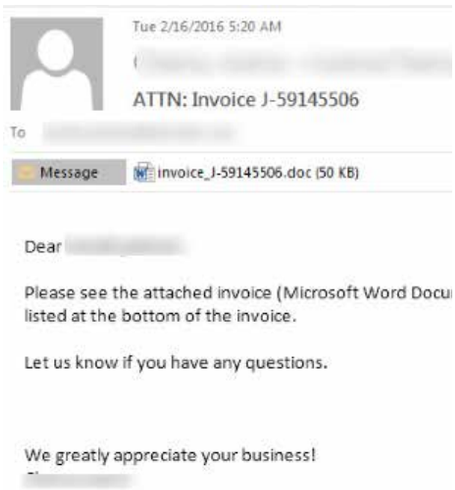
LOCKY RANSOMWARE ZARAZIO SRBIJU

Jedna od varijanti *ransomware*-a, poznata pod imenom *Locky*, otkrivena je sredinom februara i brzo se širila kroz spam e-mail ili preko kompromitovanih sajtova. Srbija se našla među deset najugroženijih zemalja, sa 840 infekcija u samo jednom satu!

KAKO IZGLEDA LOCKY?

Locky kriptuje fajlove na računarima žrtava i traži otkupninu, obično od 0,5 do 1 bitcoin (oko 240 do 420 US dolara). Iako postoji više varijanti, najveći broj spam e-mail-ova sadrži naslov sličan ovom:

```
ATTN: Invoice J-[NASUMIČNI
BROJEVI]
```



E-mail obično u prilogu ima *Word* dokument sa malicioznim makroom. Ako je omogućen makro, računar će se zaraziti *Locky ransomware*-om.

Fajlove je moguće vratiti samo iz bekapa, pod uslovom da vam i on nije kriptovan.

ZARAZA IZ OGLASA

Velika *malvertising* kampanja pogodila je nekoliko svetski poznatih sajtova, uključujući i *Forbes.com*, *Huffington Post* i *The Daily Mail*. *Malvertising* je pojava koja nastaje kada *cyber* kriminalci naprave oglas koji izgleda kao pravi, ali koji u stvari širi malver tako što je mali deo koda duboko u skriptu sakriven. Kada osoba klikne na njega, njen kompjuter se povezuje na kriminalne servere umesto na server oglašivača i tako se preuzima malver, a da žrtva toga nije ni svesna. Ova kampanja obavlja se preko platforme za oglašavanje koja učitava eksterne skripte pre nego što preusmeri saobraćaj na *Angler Exploit Kit*. Odatle je moguće raširiti *TeslaCrypt*, *Cryptowall* i ostale „negativce".

Malvertising je metod napada koji beleži rastuću popularnost zbog toga što ga je relativno jednostavno izvesti. Skorašnje istraživanje *RiskIQ*-a otkriva da se *malvertising* povećao za 300% u 2015. u odnosu na 2014. godinu. Najčešći mamac koji se koristi u malvertisingu je lažno ažuriranje *Flash*-a.

Prošlog meseca, nekoliko svetski poznatih sajtova, uključujući i *New York Times*, BBC, MSN i AOL postali su žrtve širenja malcioznih oglasa, a gotovo je izvesno da su napadi izvedeni koordinisano.

Očigledno je da *cyber* kriminalci ciljaju sajtove sa velikim saobraćajem kako bi došli do velikog broja klikova, a posetioci su skloniji da veruju oglasima koji stoje na renomiranim sajtovima.

Zahvaljujući *Web* kolačićima, autori malvera mogu da skroje maliciozni kod koji precizno cilja određenu grupu ljudi, prema geografskom području, kompaniji, interesovanju ili skorašnjoj aktivnosti na internetu.

Kompanije koje se bave oglašavanjem često ne proveravaju svoje oglašivače, što olakšava posao kriminalcima da se maskiraju u legitimne firme i pošalju maliciozne oglase koji će se pojaviti na sajtovima koje ciljaju.

ŠTA SE DEŠAVA KAD KLIKNETE NA OGLAS?

Kada kliknete na maliciozni oglas (koji izgleda kao legitiman oglas), on vas preusmerava na ciljnu stranu (*landing page*) na kojoj se nalazi *Angler Exploit Kit*.

On sadrži više hakerskih alata i *zero day exploit*-a koji omogućavaju hakerima da otkriju ranjivosti vašeg sistema i da kroz njih instaliraju trojance i *ransomware*. Ako dođe do instalacije, *ransomware* kriptuje vaše podatke i ostavlja otkupnu poruku u kojoj zahteva isplatu u bitcoinima za otključavanje fajlova.

BANKE BEZ FIREWALL-A: EVO KAKO SU HAKERI USPELI DA UKRADU $80 MILIONA

Forenzički istražitelji iz Bangladeša koji su istraživali pljačku banke u vrednosti od 80 miliona dolara otkrili su da su hakeri upali u mrežu zbog toga što je banka koristila polovne mrežne svičeve bez *firewall*-a, koji koštaju $10. Kada je prošlog meseca prijavljeno da je nepoznata hakerska grupa korišćenjem malvera pokušala da ukrade milijardu dolara sa bankovnog računa bangladeških federalnih rezervi, i pri tom, uspela da ukrade više od 80 miliona, istražitelji nisu želeli da otkriju kako su hakeri premostili sigurnosna rešenja u mreži banke. Istina je da nikakva sigurnosna rešenja za zaštitu od sve sofisticiranijih napada nisu bila primenjena.

Nedostatak sigurnosnih rešenja bitno je olakšao hakerima upad u sistem i krađu 81 miliona dolara, a samo je obična greška u kucanju koju su hakeri napravili sprečila transfer od još 850 miliona! Računari u mreži koji su bili povezani preko polovnih rutera bili su prikačeni na SWIFT (globalnu mrežu za transfer novca), što to je omogućilo hakerima pristup kredencijalima koji su potrebni za transfer velikih iznosa direktno na svoje račune. Forenzički istražitelji rekli su da bi hakovanje bilo teže izvodljivo da je postojao *firewall*. *Firewall* služi kao odbrana od hakera i malvera. Istražitelj je dodao i to da im je korišćenje jeftinih rutera otežalo (i za sada onemogućilo) pronalaženje hakera koji stoje iza najveće pljačke banke, kao i otkrivanje njihovih taktika. Istražitelji su okrivili i banku i sistem SWIFT rekavši da su morali da se konsultuju oko zaštite pre nego što se pljačka dogodila. Hakeri su upali u mrežu banke i pokušali da ukradu milijardu dolara sa računa banke *Federal Reserve* u Njujorku početkom februara i tom prilikom su prebacili velike sume novca na lažne račune u Filipinama i Šri Lanki. Bangladeška policija je identifikovala 20 stranaca koji su bili povezani s pljačkom, ali se ispostavilo da su ti ljudi samo primili određene sume tog novca i da nisu hakeri koji su ukrali novac.

Istražitelji se još uvek pitaju kako da identifikuju hakere kad nemaju dovoljno tragova, a ovaj incident je dobra opomena finansijskim institucijama širom sveta da podignu nivo sigurnosti svojih sistema.

Nadamo se da naše banke imaju bolji sistem zaštite od bangladeških…

TVORCI SPYEYE VIRUSA OSUĐENI NA 24 GODINE ZATVORA

Dva internacionalna hakera, *Aleksandar Andrejevič Panin* i *Hamza Bendelađ*, zajedno su osuđeni na 24 godine i 6 meseci zatvora zbog toga što su razvili i distribuirali bankarskog trojanca *SpyEye*, moćnog *botnet*-a koji je sličan zloglasnom malveru *Zevs*. Obojica su optuženi za krađu stotina miliona dolara iz banaka širom sveta. *SpyEye*, koji se smatra naslednikom zloglasnog bankarskog malvera *Zevs*, noćna je mora finansijskih institucija još od 2009. godine.

Kada malver prodre u sistem, povezuje se sa komandnim serverima koje kontrolišu napadači i krade podatke lične i finansijske prirode, kao što su podaci za e-banking i podaci sa kreditne kartice. To rade koristeći *keylogger*-e i *Web injection.*

27-godišnji ruski programer *Panin*, poznat pod alijasima *Gribodemon* i *Harderman*, osuđen je na devet godina i šest meseci zatvora zbog toga što je napravio *SpyEye*, naslednika *Zevs*-a. On je 2010. navodno primio izvorni kod i prava na prodaju *Zevs*-a od *Jevgenija Bogačeva* (alijas *Slavik*) i implementirao je brojne njegove komponente u *SpyEye*. *Bogačev* je još uvek na slobodi i trenutno je najtraženiji haker na spisku FBI-a.

Paninov saradnik *Bendelađ* je 27-godišnji alžirski haker poznat pod alijasima *Bx1* i *Happy Hacker*. On je hakovao 217 banaka i donirao više od 280 miliona dolara palestinskim humanitarnim organizacijama. Osuđen je na petnaest godina zatvora zbog reklamiranja malvera *SpyEye* po raznim forumima na internetu. Gotovo 150 klijenata je od njega kupilo verzije malvera *SpyEye* po ceni od 1000 do 8500 dolara, a jedan klijent sa alijasom *Soldier* je objavio da je uz pomoć ovog malvera zaradio više od 3,2 miliona dolara za samo šest meseci.

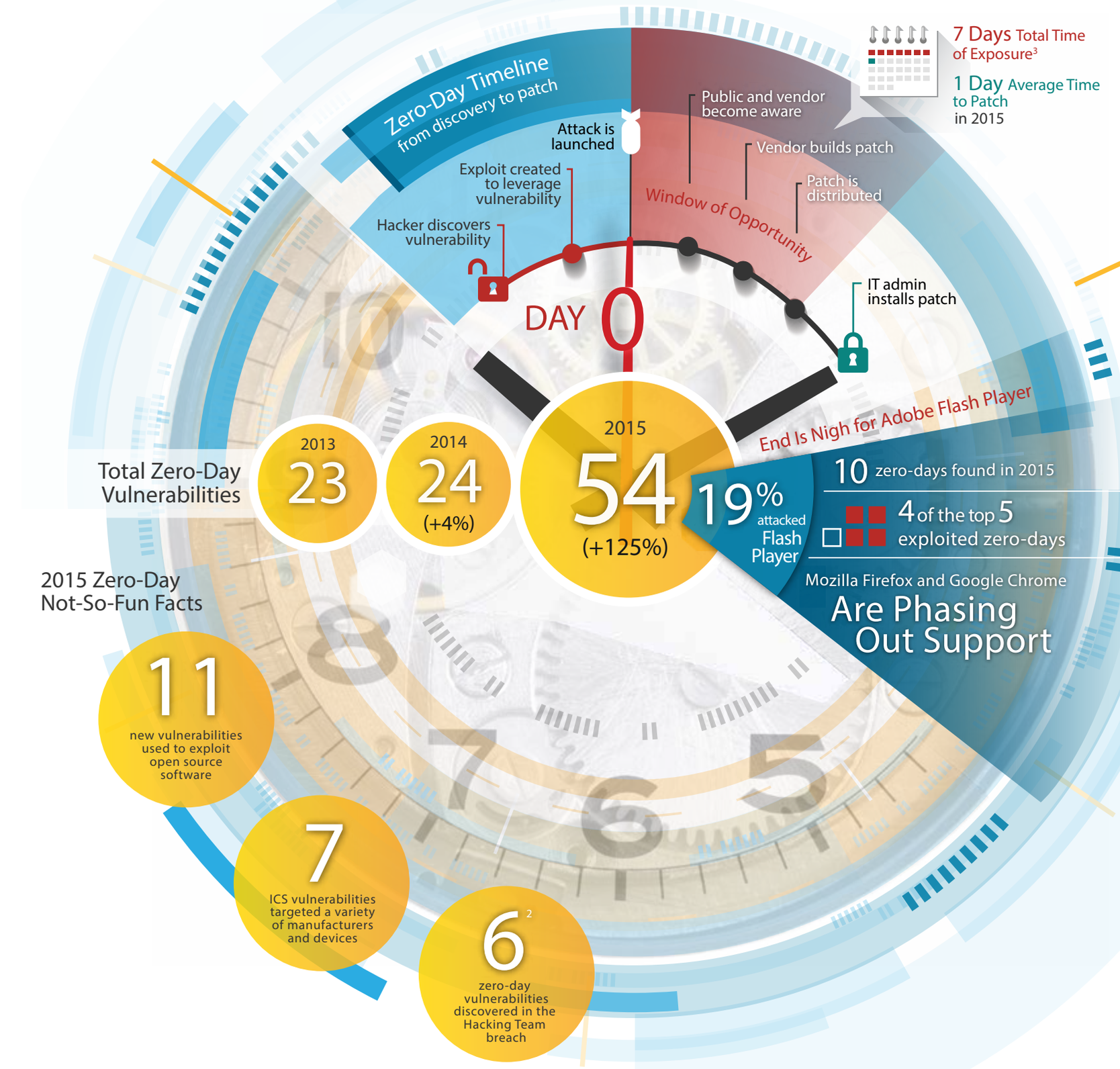
Iz Ministarstva pravde opisali su *SpyEye* kao „najuspešniji od svih bankarskih malvera/trojanaca“ koji je uspeo da zarazi više od 50 miliona računara širom sveta od 2010. do 2012. i izazove više od milijarde dolara gubitaka pojedincima i finansijskim institucijama širom sveta.

Bendelađ je uhapšen u Tajlandu januara 2013. i izručen SAD-u iste godine, dok je *Panin* priveden jula 2013. na međunarodnom aerodromu u Atlanti.

A New Zero-Day Vulnerability Discovered Every Week in 2015[1]

Advanced attack groups continue to profit from previously undiscovered flaws in browsers and website plugins.

In 2015, 54 zero-day vulnerabilities were discovered.



[1] on average, based on 54 vulnerabilities

[2] symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache

[3] Total time of exposure for the top five zero-day vulnerabilities

Symantec™

SYMANTEC ISTR 2016
2015. U KRATKIM CRTAMA

Svake godine *Symantec* objavljuje *Internet Security Threat Report*, izveštaj koji sumira informacije vezane za bezbednost, kao što su trendovi napada, aktivnosti malicioznog koda, fišing, spam i slično. Ove informacije *Symantec* prikuplja zahvaljujući svojoj obaveštajnoj mreži – *Global Intelligence Network*, koju čini više od 63 miliona senzora koji registruju hiljade napada u sekundi. *Symantec* je otkrio više od 430 miliona novih jedinstvenih malvera u 2015, 36% više nego prethodne godine.

Iz ovog sveobuhvatnog izveštaja, koji možete preuzeti na adresi *https://www.symantec.com/security-center/threat-report*, može se izdvojiti šest ključnih trendova.

SVAKE NEDELJE OTKRIVENA JE PO JEDNA ZERO-DAY RANJIVOST

Organizovane grupe sajber napadača nastavljaju da profitiraju od neotkrivenih propusta u browser-ima i plug-in-ovima

Tokom 2015, broj otkrivenih *zero-day* ranjivosti uvećao se više od dva puta, tačnije porastao za 125 procenata u odnosu na prethodnu godinu. Drugim rečima, svake nedelje otkrivena je u proseku jedna *zero-day* ranjivost. Iako u 2014. nije došlo do većeg rasta u broju ovih ranjivosti, u 2015. ipak nije došlo do stagnacije kako se očekivalo, već do prave eksplozije.

Ranjivosti mogu da se pojave kod bilo koje vrste softvera, ali je najčešća meta softver koji je u najširoj upotrebi. Najveći broj ranjivosti se otkriva za *Internet Explorer* i *Adobe Flash*, koje svakodnevno koristi veliki broj ljudi. Čak četiri od pet najviše eksploatisanih ranjivosti bile su za *Adobe Flash*. Hakeri stalno traže ranjivosti popularnih programa i čim ih otkriju, brzo ih iskoriste kako bi inficirali što veći broj računara pre nego što proizvođač ažurira softver, odnosno pre nego što se pojavi bezbednosna zakrpa za tu ranjivost. Obično uspeju da zaraze stotine računara pre nego što se objavi zakrpa. Naravno, i nakon objave zakrpe moći će da zaraze one računare koji nisu ažurirani na vreme.

VIŠE OD POLA MILIJARDE LIČNIH PODATAKA JE UKRADENO ILI IZGUBLJENO U 2015.

Veliki broj kompanija ne prijavljuje curenje podataka

Pri kraju 2015. bili smo svedoci najvećeg curenja podataka koje javno prijavljeno. Neverovatnih 191 milion poverljivih dokumenata je iscurelo. Ovo je bio najveći prijavljeni incident, ali ne i jedini – prijavljeno je devet velikih incidenata sa više od deset miliona dokumenata.

Ukupan broj ugroženih ličnih dokumenata, a time i identiteta, popeo se na 429 miliona. Međutim, taj broj je samo vrh ledenog brega, jer je veći broj onih

kompanija koje nisu želele da prijave ovakve incidente ili tačan broj dokumenata koji su iscureli. *Symantec* procenjuje da je realna cifra izgubljenih dokumenata više od pola milijarde.

VELIKE BEZBEDNOSNE RANJIVOSTI U TRI TREĆINE POPULARNIH SAJTOVA SVE NAS IZLAŽU RIZIKU

Web administratori i dalje imaju teškoće sa bezbednosnim ažuriranjima

Over Half a Billion Personal Information Records Stolen or Lost in 2015

and more companies than ever not reporting the full extent of their data breaches

36% of breaches included medical records

The largest number of breaches took place within the Health Services sub-sector, which actually comprised 39 percent of all breaches in the year. This comes as no surprise, given the strict rules within the healthcare industry regarding reporting of data breaches.

39%

120 Incidents

4 Million Identities Exposed

2015 Stats

Total Reported Identities Exposed

numbers in millions

2015	429	+23%
2014	348	-37%
2013	552	

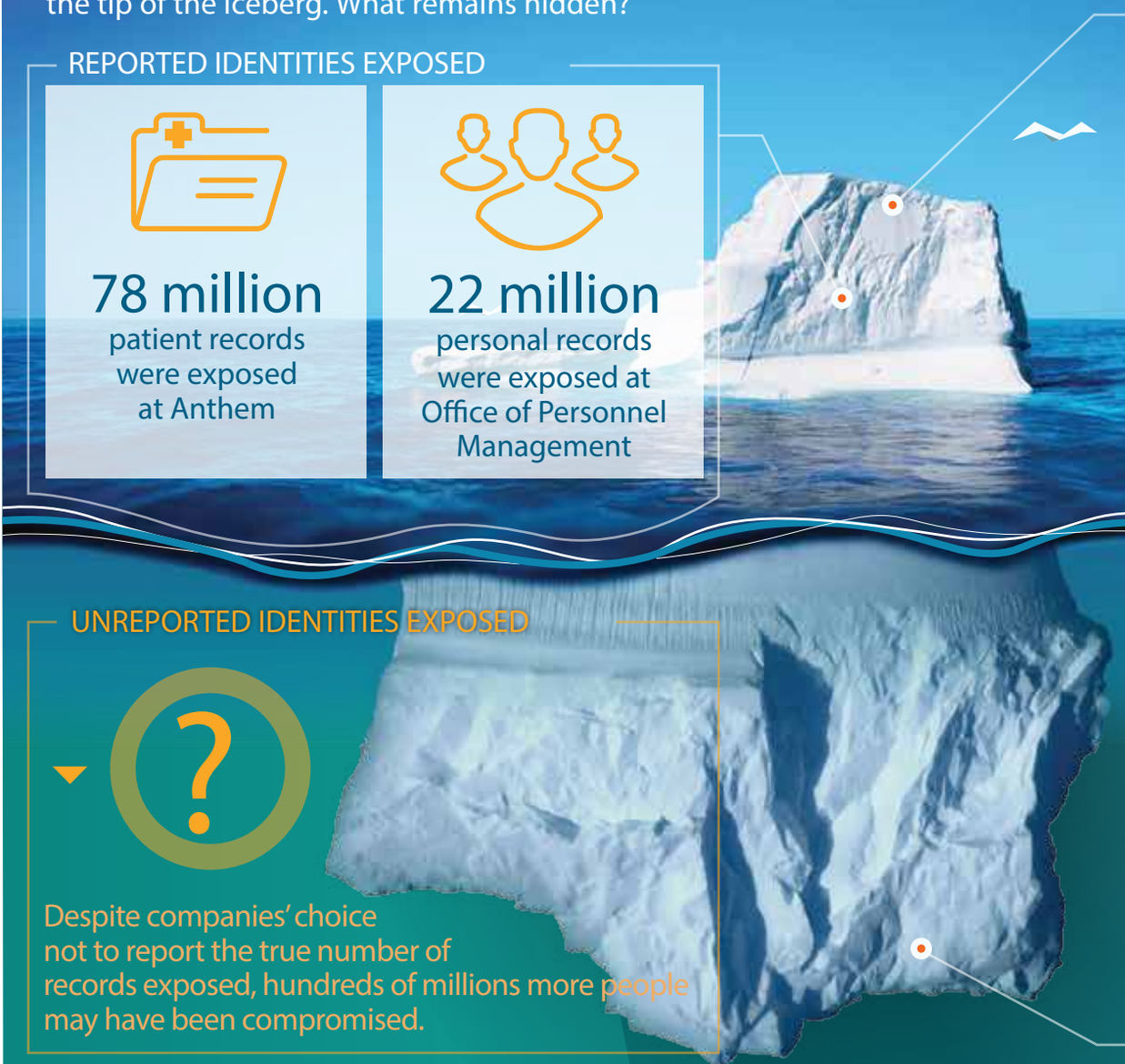
These numbers are likely higher, as many companies are choosing not to reveal the full extent of their data breaches.

Most of an iceberg is submerged underwater, hiding a great ice mass. The number of reported identities exposed in data breaches are just the tip of the iceberg. What remains hidden?

REPORTED IDENTITIES EXPOSED

78 million patient records were exposed at Anthem

22 million personal records were exposed at Office of Personnel Management



UNREPORTED IDENTITIES EXPOSED

Despite companies' choice not to report the true number of records exposed, hundreds of millions more people may have been compromised.

2014: **61** Incidents that did not report identities exposed in 2015

2015: **113** +85%

Given the facts, it is possible that **500** Million* identities were exposed

*estimated

Symantec

Zabeleženo je više od milion Web napada svakog dana u toku 2015. Mnogi ljudi veruju da će biti bezbedni od *cyber* kriminala ako se drže samo legitimnih, proverenih sajtova. Međutim, mnogo ljudi je u zabludi. *Cyber* kriminalci iskorišćavaju ranjivosti legitimnih Web sajtova da preko njih inficiraju posetioce, jer administratori ne uspevaju da zaštite sajtove. Više od 75% legitimnih sajtova ima nesanirane ranjivosti. 15% legitimnih sajtova ima kritične ranjivosti, što znači da ne zahtevaju od napadača mnogo truda da iskoriste sajt za svoje maliciozne namene. Web administratori moraju da se pozabave pitanjem bezbednosti ozbiljnije i da se agresivnije suprotstave napadačima

SPEAR-PHISHING KAMPANJE KOJE CILJAJU ZAPOSLENE PORASLE SU ZA 55 PROCENATA U 2015.

Cyber napadači ne odustaju nakon jednog napada

Tokom 2015, vladine ili finansijske organizacije koje su jednom napadnute, bile su napadnute bar još tri puta. Velike kompanije koje su se našle na meti napadača, u proseku su bile uspešno napadnute svaka po 3,6 puta.

U poslednjih pet godina, možemo da primetimo rast broja napada na preduzeća sa manje od 250 zaposlenih, odnosno 43% napada bilo je usmereno na male firme, što potvrđuje da su firme svih veličina ugrožene. Ne radi se dakle samo o velikim, uspešnim firmama, već i o lokalnim radnjama sa par računara.

Primer: Lokalna firma od 35 zaposlenih bila je žrtva cyber napada konkurencije. Konkurent je dve godine imao pristup njihovoj mreži i krao podatke o kupcima i cenama, čime je sticao prednost na tržištu.

Sve firme su potencijalne žrtve ciljanih napada. Broj *spear-phishing* napada, odnosno *phishing* kampanja koje su krojene za jednu ili nekoliko osoba zaposlenih u preduzeću (zbog čega su uverljivije i teže se otkrivaju), povećao se za 55% u 2015.

RANSOMWARE SE UVEĆAO ZA 35 PROCENATA

Cyber kriminalci koriste enkripciju kao oružje protiv kompanija i pojedinaca

Ransomware nastavlja da evoluira. Prošle godine smo mogli da vidimo kako *Crypto-ransomware* koji zaključava fajlove izbacuje iz igre benigniju verziju koja samo zaključava ekran računara. Broj *Crypto ransomwarea* je porastao za 35 procenata u 2015. Ovaj vid napada je izuzetno profitabilan za kriminalce, zbog čega se očekuje da će i dalje beležiti rast i da će novi oblici moći da zaraze sve uređaje koji se nalaze na istoj mreži. *Ransomware* u 2015. nije pogađao samo personalne računare, nego i pametne telefone, pa čak i *Mac* i *Linux* sisteme.

SYMANTEC JE BLOKIRAO 100 MILIONA PREVARA SA LAŽNOM TEHNIČKOM PODRŠKOM

Cyber prevaranti navode vas da ih pozovete i predate im novac

Dok *ransomware* nastavlja da raste, on nije jedina pretnja sa kojom se susrećemo. Kako ljudi sve više poslova obavljaju *online*, napadači nalaze načine da namame žrtve. Prevare sa lažnom tehničkom podrškom prvi put su otkrivene 2010, ali su od tad evoluirale od *cold calling* telefonskih poziva nepoznatih ljudi, do toga da navedu žrtve da pozovu njih misleći da zovu tehničku podršku.

Napadači koriste lažna *pop-up* upozorenja koja žrtvi govore da je došlo do ozbiljne greške i da treba da pozovu neki broj telefona (obično počine sa 800), gde lažni predstavnik tehničke podrške pokušava da proda žrtvi neku vrstu usluga, koje su uzgred nepotrebne i bezvredne. Tokom 2015. *Symantec* je blokirao sto miliona ovakvih napada.

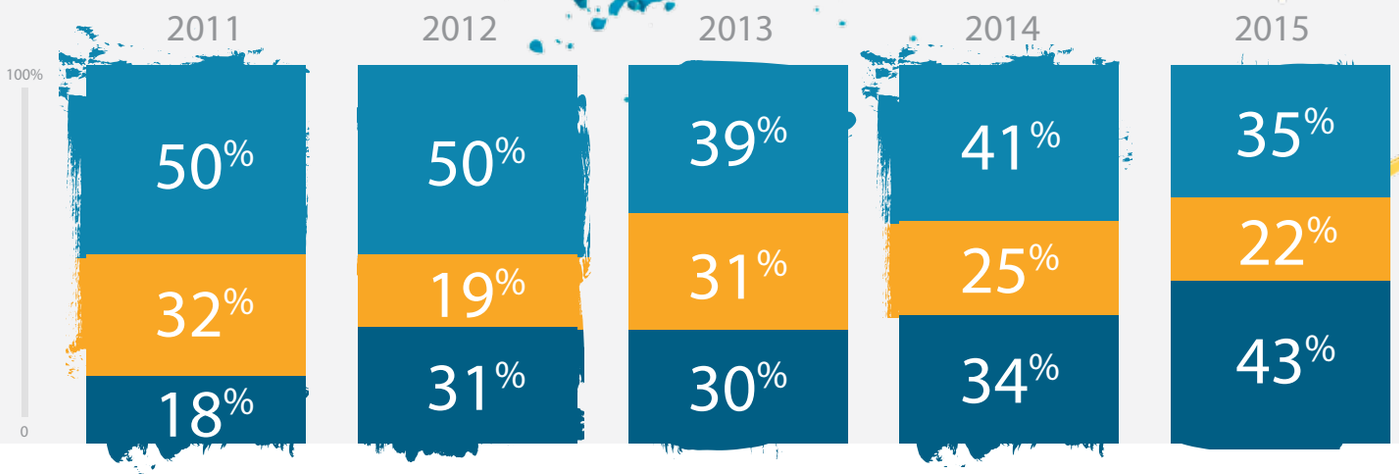
Attackers Target Both Large and Small Businesses

Like thrown paint on a blank canvas, attacks against businesses, both large and small, appear indiscriminate. If there is profit to be made, attackers strike at will.

The last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.

Number of Employees
- Large Enterprises 2,500+
- Medium-Size Businesses 251 to 2,500
- Small Businesses (SMBs) 1 to 250

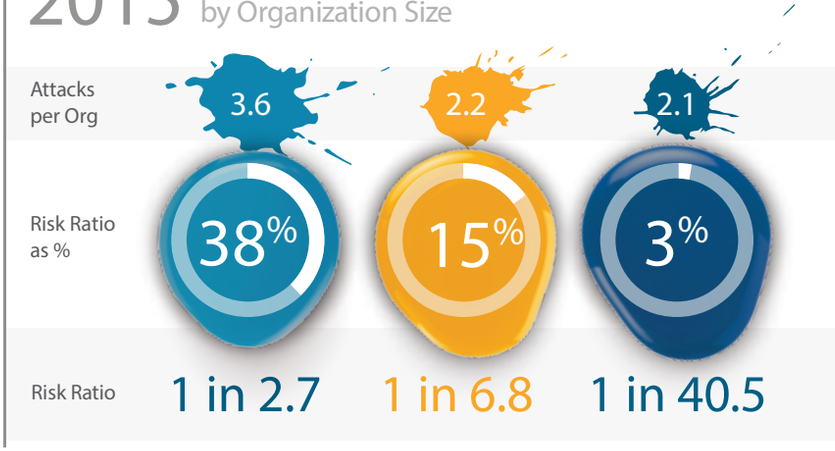
Spear-Phishing Attacks by Size of Targeted Organization



Cyber attackers are playing the long game against large companies, but all businesses of all sizes are vulnerable to targeted attacks. In fact, the number of spear-phishing campaigns targeting employees increased 55% in 2015.

2013	2014	2015
779	841	1,305
+91%	+8%	+55%

2015 Risk Ratio of Spear-Phishing Attacks by Organization Size



Symantec

KAKO SPREČITI INFEKCIJU RANSOMWARE-OM

Ključno pitanje poslednjih nekoliko meseci je kako sprečiti infekciju *ransomware*-om i šta činiti kada je već kasno – kada je računar zaražen?

PRVI KORAK jeste da ne otvarate priloge e-mail poruka od nepoznatih ljudi. Naročito je važno da ni drugi ljudi iz vašeg okruženja to ne čine, zato ih upozorite pre nego što bude kasno.

DRUGI KORAK – napravite bekap podataka. Ako nemate, pobrinite se za bekap podataka i sa radnih stanica (servere već bekapujete, redovno, zar ne?)!

TREĆI KORAK je da poboljšate zaštitu e-mail saobraćaja ili ako je već nemate – uvedete je!

ČETVRTI KORAK je višeslojna antivirusna zaštita na računarima! Možda klasične definicije virusa ne mogu da „uhvate" sve varijante *crypto ransomwarea*, ali neka druga komponenta zaštite hoće.

Održavajte sistem zaštite i pratite šta se dešava. Pripremite plan šta treba učiniti i ko će to raditi u slučaju incidenta. Testirajte plan.

Ko želi da ode korak dalje – ili je već otišao – tu su *firewall* sistemi sledeće generacije, NGFW, koji uglavnom „hvataju" ovakve pretnje. Takođe, tu su i *Advanced Threat Protection* rešenja i izvršavanje potencijalnog malvera *sandboxu*-u, koja su jednako uspešna u otkrivanju ovakvih pretnji.

Od pomoći je i sprečavanje izvršavanja *JavaScript*-ova, mada se time dosta gubi na izgledu i funkcionalnosti dobrog dela današnjih *Web* prezentacija. *Word* i *Excel* makroe takođe možete da blokirate.

Na kraju, šta ako je neki računar već zaražen? Odmah ga „skinite" sa mreže. Isključite ga. Potražite bekap podataka – to je zapravo jedini pravi spas. Ako nemate bekap, možete da probate alate za dešifrovanje koji se mogu naći na Internetu – ali ne očekujte čuda. Ako imate uključeno čuvanje kopija verzija fajlova u *Windows*-u, možda ima nade da vratite prethodne verzije fajlova. Takođe, ako nije mnogo fajlova šifrovatno, možete da pokušate sa *undelete* alatima, za vraćanje obrisanih fajlova – ponovo, sa malom verovatnoćom uspeha.

Važno je napomenuti: nemojte plaćati otkup – ucenu! Time samo pomažete njihov dalji razvoj i mogućnost da se ponovo nađete u sličnoj neprilici.

Porast broja novih malvera povećao je vidljivost i značaj IT bezbednosti. Na žalost, većina preduzeća stavlja akcenat na antivirusnu zaštitu i tu se zaustavlja, što nije ni iz daleka dovoljno za poboljšanje IT bezbednosti. Evo osnovnih deset koraka koje svako preduzeće treba da preduzme kako bi poboljšalo bezbednost svojih sistema i podataka:

0 OBUČITE ZAPOSLENE O OSNOVAMA IT BEZBEDNOSTI: Možda najvažniji korak, a čini mi se da mu se obraća najmanje pažnje, jeste obuka zaposlenih, korisnika o bezbednosti IT sistema, socijalnom inženjeringu, *phishing*-u, načinima inficiranja malverom, prepoznavanju lažnih sajtova i e-mail poruka, pravilnom otvaranju priloga e-mail poruka, maskiranju ekstenzija fajlova i dr. Obuka korisnika je od ključne važnosti za bezbednost IT sistema – pri čemu obuku može da organizuje i drugo preduzeće – vaš partner od poverenja, koji može testovima i da izmeri i proceni stepen svesti o IT bezbednosti u preduzeću, kao i korake za poboljšanje.

1 OBEZBEDITE ŠTO BOLJE ANTIMALVER REŠENJE: Uvedite antivirus koji nudi više slojeva zaštite (pored klasične, zasnovane na definicijama virusa), heuristiku i reputaciju, centralizovano upravljanje i izveštavanje, lako ažuriranje definicija virusa i dobar mehanizam za oporavak od malvera. Primer: *Symantec Endpoint Protection.*

2 PATCH MANAGEMENT – UPRAVLJANJE AŽURIRANJEM APLIKACIJA I OPERATIVNIH SISTEMA: Deo preduzeća ažurira operativne sisteme radnih stanica i servera, ali mnogi ne ažuriraju aplikacije, što je neophodno za zaustavljanje malvera. Posebnu pa-

DESET KORAKA ZA BOLJU IT BEZBEDNOST

žnju treba obratiti na Javu, PDF čitače, *Flash*, *Web browser*-e i *Microsoft Office* aplikacije. Potrebno je skratiti vreme ažuriranja na najkraće moguće. *Shavlik* nudi odlična rešenja za ažuriranje/*patch* aplikacija i OS-a. (Napomena: izbacite *Windows XP* i *Windows 2003*, što pre.)

3 OGRANIČITE PRIVILEGIJE ADMINISTRATORIMA I ZA OPERATIVNE SISTEME I ZA APLIKACIJE: Administratori treba da koriste nalog sa ograničenim pravima za svakodnevni rad sa *office* aplikacijama, za Web surfovanje i e-mail. Privilegovani nalozi treba da se koriste samo po potrebi i sa najmanjim mogućim pravima. Isključite (*disable*) lokalne administratore ako je to moguće, kako bi sprečili da neki kompromitovani nalog lokalnog administratora napravi problem i na mreži, tj. drugim računarima koji najčešće imaju istu šifru.

4 OGRANIČITE KORIŠĆENJE KORISNIČKIH APLIKACIJA/APPLICATION WHITELISTING: *Java* aplikacije iz *Web browser*-a, *Microsoft Office* makroi, skripte i sl. treba da budu pod kontrolom – po mogućstvu, onemogućene. Poželjno je uvesti i spiskove dozvoljenih aplikacija – *application whitelisting* (zahteva dosta truda i rada, ali se naknadno isplati). Bolja *endpoint protection* rešenja, kao što je *Symantec Endpoint Protection*, nude alate koji pomažu u ovom poslu.

5 URADITE SEGMENTACIJU LOKALNE MREŽE I UVEDITE FIREWALL SLEDEĆE GENERACIJE: Podelite mrežu na različite zone sigurnosti i segmente kako bi lakše zaštitili kritične resurse i servere/aplikacije. Zamenite klasičan *firewall firewall*-om sledeće generacije. Obratite pažnju na IPv6 koji je negde automatski konfigurisan i „prođe“ ispod radara ili se ne nalazi pravilima za zabranu pristupa. *Palo Alto Networks* NGFW (*Next Generation Firewall*) nudi odlična rešenja na ovom polju, posebno VM-ove za podelu i zaštitu zona u virtualizovanoj infrastrukturi, pored klasičnih *firewall* uređaja za zaštitu Internet saobraćaja.

6 ZAŠTITITE E-MAIL I WEB SAOBRAĆAJ: Uvedite e-mail filtriranje, antispam i antivirus, kao i osnovno filtriranje sadržaja. Rešenje treba da omogućava upravljate pravilima šta i kako može da se šalje i prima emailom. Takođe, uvedite *Web* filtriranje i korišćenje URL lista/kategorija za ograničavanje pristupa *Web* lokacijama. *Web whitelisting* se pokazao izuzetno efikasnim (ali zahteva više truda i rada). *Symantec Messaging Gateway*, *Barracuda Email Security* i *Barracuda Web Filter* su dobra rešenja u ovoj oblasti. Ovo važi i za korisnike cloud e-mail servera, kako *Office 365*, tako i rešenja koja nude lokalni ISP-ovi za e-mail.

7 DINAMIČKA ANALIZA POTENCIJALNIH MALVERA IZVRŠAVANJEM U SANDBOX-U: za veća preduzeća i ona koja imaju potrebe i mogućnosti, treba uvesti dinamičku analizu aplikacija, e-mail poruka i mrežnog saobraćaja izvršavanjem u tzv. *sandbox*-u koji će „detonirati“ (pokrenuti) potencijalni malver, analizirati dejstvo i kreirati korake za sprečavanje širenja i izvršavanja. *Symantec ATP* (*Advanced Threat Protection*) ili *Palo Alto Networks WildFire* nude dobra rešenja u ovom domenu.

8 UVEDITE SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) ILI BAREM LOG MANAGEMNET: Prikupljanje, centralizovanje i analiza logova omogućava da se nakon incidenta utvrdi šta se zapravo desilo, odakle je sve počelo i kojeg je obima incident. SIEM takođe može da kreira pravovremena upozorenja koja su obično prvi signal da nešto nije uobičajeno ili u redu. *ManageEngine EventLog Analyzer* predstavlja povoljno i dobro SIEM rešenje.

9 KRIPTUJTE – ŠIFRIRAJTE POVERLJIVE PODATKE/SISTEME: Laptopovi, folderi sa poverljivim podacima, *SharePoint* portali, USB diskovi koji se koriste za prenos poverljivih podatkaa treba da koriste šifriranje/kriptovanje. *Symantec Encryption* rešenja pružaju odličnu zaštitu u ovom domenu.

10 UVEDITE VIŠEFAKTORNU AUTENTIFIKACIJU: Za korisnike koji rukuju poverljivim, osetljivim podacima, uvedite višefaktornu autentifikaciju: tokeni, *smart* karice, usb ključevi, biometrija. Posebno važna kod udaljenog pristupa ili pri pristupanju poverljivim podacima.

Spisak koraka ka boljoj IT bezbednosti se ovim ne završava, ali verujemo da ovih deset koraka (zapravo jedanaest) predstavlja suštinu u naporu za bolju bezbednost.

ZAŠTITITE RAČUNAR OD MALVERA NA BAZI MAKROA U DVA KORAKA

Da li svakodnevno koristite MS Word dokumenta? Ako je odgovor pozitivan, sledeće pitanje je da li ste svesni da otvaranje najobičnijeg dokumenta može ugroziti vaš sistem? Stvar je u tome što virus ne pogađa vas direktno, ali na ovaj način vi ste mu dozvolili napad tako što ste dopustili smrtonosnom „Macro-u" uvid u sadržaj poverljivih dokumenata poput bankarskih faktura.

NA KOJI NAČIN MAKROI SLABE VAŠ SISTEM?

Koncept makroa datira još iz 1990-ih. Sigurno vam je poznata ova poruka – *"Upozorenje: Ovaj dokument sadrži makroe."*

Makro je serija komandi i akcija koja pomaže da se određeni zadaci automatizuju. Programi *Microsoft Office*-a podržavaju makroe napisane u *Visual Basic for Applications* (VBA), ali oni se mogu koristiti i za zlonamerne aktivnosti kao što je instaliranje malvera.

Hakeri mudro koriste ove tehnike slanjem malicioznih makroa preko *.doc* fajlova ili radnih tabela, tako što u zaglavlje e-pošte koje šalju korporativnim mrežama stavljaju tekst koji privlači pažnju primaoca. Kada primalac otvori zlonamerni *Word* dokument, *.doc* fajl se preuzima u njegov sistem. Međutim, opasnost nastupa kada korisnik otvori fajl i kada se pojavi prozor u kojem piše „Omogućiti uređivanje" (eng. *Enable Editing*) kako bi videli sadržaj.

Kada korisnik klikne na „Omogućiti uređivanje", zlonamerni dokument počinje sa zloglasnim aktivnostima u sistemu, npr. zakači se za druge *.doc* fajlove kako bi povećao jačinu napada koja rezultira u slabljenju vašeg sistema. Ove aktivnosti zavise od *payload* programa definisanih u makrou.

KAKO DA SE ZAŠTITITE OD VIRUSA KOJI U SVOJOJ OSNOVI KORISTE MAKRO?

1: Konfigurišite sigurnu lokaciju

Onemogućavanje makroa nije izvodljiva opcija, naročito u kancelarijskom okruženju gde su makroi osmišljeni da pojednostave i automatizuju složene zadatke.

Ako vaša organizacija koristi makroe, možete premestiti dokumente koja koriste makroe u kompanijin DMZ (demilitarizovana zona), koja se još naziva i „sigurna lokacija". Da konfigurišete sigurnu lokaciju, može da koristite sledeći način:

```
User Configuration/Administrative
Templates/Microsoft Office XXX
20XX/Application Settings/
Security/Trust Center/Trusted
Locations
```

Kada je konfigurišete, makroi koji ne pripadaju sigurnoj lokaciji neće biti pokrenuti ni na koji način, a to ojačava sigurnost vašeg sistema.

2: Blokirajte makroe u Office dokumentima koji su primljeni preko Interneta

Misrosoft je nedavno otkrio novi metod zaštite dodajući novu funkciju taktičke sigurnosti kako bi se ograničili napadi preko makro-komandi u *MS Office 2016*. Ta zaštita u krajnjoj liniji sprečava da sistem bude nasilno preuzet. Nova funkcija predstavlja skup podešavanja koja dopuštaju administratorima u preduzećima da onemoguće pokretanje makroa u *Office* dokumentima koji su primljeni preko Interneta.

Novo podešavanje ima naziv *Block macros from running in Office files from the Internet* i može se obaviti preko *Group policy management editor-a* na sledeći način:

```
User configuration >>
Administrative templates >>
Microsoft Word 2016 >> Word
Options >> Security >> Trust
Center
```

Može se izvršiti konfiguracija za svaki pojedinačni *Office* program. Omogućavanjem ove opcije, makroi koji dolaze sa Interneta su blokirani, čak iako imate opciju „omoguću sve Makro-e" (eng. *Enable all macros*) u podešavanjima makroa. Dalje, umesto opcije *Enable Editing,* primićete obaveštenje da su makroi blokirani zato što dolaze iz nepouzdanog izvora. Jedini način da se pokrene takav *Office* dokument jeste da se sačuva u sigurnoj lokaciji i da se tako dozvoli pokretanje makroa.

PET MITOVA O ZAŠTITI OD PRETNJI

Najveći broj kompanija i državnih organizacija sazna da su im podaci ukradeni tek kad ih o tome obavesti neka treća strana, a tada je najčešće prekasno. Problem delom nastaje i zbog toga što menadžeri veruju u neke često pominjane teze o bezbednosti, iako te teze ne prolaze proveru realnog sveta.

Kako broj sofisticiranih ciljanih napada raste, sve je veći i broj organizacija koje su izložene riziku. Na žalost, mnoge od njih ni ne znaju da su meta napada, pored ostalog i zato što čak i informatički profesionalci veruju u neke mitove koji, pokazuje se, čine njihove sisteme manje bezbednim. Rezimirajmo te mitove, ukazujući na realnost…

MIT #1 **Najveći broj bezbednosnih incidenata se otkrije u roku od 30 dana i otkloni se brzo.**

ISTINA Više od 65% upada, odnosno probijanja sistema bezbednosti ostane neotkirveno duže od 30 dana. Zapravo, prosečnoj organizaciji je potrebno devet meseci da otkrije upad u svoje okruženje. Čak i kad se upad otkrije, potrebno je više od četiri meseca za potpunu sanaciju i čišćenje okruženja.

MIT #2 **Samo sofisticirani napadi treba da nas brinu, jer će naš antivirusni softver da se postara za ostale pretnje.**

ISTINA Istina je da su napadi najvišeg profila često jedinstveni i ciljaju specifične tačke. Ali isto tako postoji i tržište za već gotove viruse i malvere, za koje napadač ne mora da ima posebna tehnička znanja. Krajem 2013. drugi najveći američki lanac prodavnica *Target*, pretrpeo je veliki gubitak zbog upada, kada su iscureli lični i finansijski podaci više od 110 miliona kupaca. Napadač nije bio hakerski genije, već je koristio malver koji košta manje od 2.500 dolara na crnom tržištu.

MIT #3 **Bezbednosne zakrpe operativnog sistema dovoljne su da nas zaštite od *zero-day* (sasvim novih) pretnji.**

ISTINA Dostupnost *zero-day* i drugih *exploit*-a za najčešće korišćene operativne sisteme, i ranjivosti kao što su *HeartBleed* i *Shellshock* koji su „gađali" SSL komponente u širokoj upotrebi, pokazuju da ne funkcionišu sve mere zaštite onako kako pretpostavljamo.

MIT #4 ***Air-gapped* mreže su bezbedne od napada.**

ISTINA Čak su se i izolovani uređaji i mreže pokazali kao nebezbedni, to su nam pokazali *Stuxnet* i *Duku* napadi. Zbog velikog broja vektora napada, sistema, protivnika i ciljeva, postalo je nemoguće blokirati svaku pretnju pre nego što stigne do mreže. Ne treba zaboraviti ni to da sistem može da bude ugrožen i iznutra, da neki zaposleni ili spoljni saradnik, namerno ili slučajno, može da kompromituje mašinu čak i u okviru izolovane mreže.

MIT #5 **Upadi su neizbežni. Samo moramo da se fokusiramo na zaštitu mašina i mreže.**

ISTINA Nije tačno. Organizacije moraju da nastave da blokiraju pretnje na svim kontrolnim tačkama u realnom vremenu; to je ključna funkcija koja postoji u modernim rešenjima, kao što su *endpoint protection* proizvodi, *e-mail security* sistemi, *secure Web gateway*-i i *firewall*-ovi nove generacije.

ŠTA JE FIREWALL NOVE GENERACIJE?

Nir Zuk, osnivač kompanije *Palo Alto Networks*, tvorac je *firewall* uređaja nove generacije.

On je otpočeo karijeru i rad na *firewall* zaštiti u izraelskoj armiji, kada je otišao na odsluženje vojnog roka i ušao u elitnu elektronsku obaveštajnu jedinicu *Unit 8200*. *Gil Shwed*, koga je tada upoznao, ubrzo po izlasku iz vojske je osnovao *Check Point* (1993). Tokom rada u izraelskoj vojsci, *Zuk* je osmislio tehnologiju *Statefull Inspection*, koja će kasnije postati i ostati deo gotovo svakog ozbiljnog *firewall* rešenja, pa ga je *Shwed* već 1994. „regrutovao" u redove *Check Point*a, gde je učestvovao u pravljenju njihovog vodećeg proizvoda *Firewall-1*. Nažalost, *Check Point* nije imao razumevanja za rešenja koja je predlagao *Nir Zuk* i on je 1999. napustio tu firmu i osnovao *OneSecure*, koji 2002. prodaje *Netscreen*u. *Juniper Networks* je kupio *Netscreen 2004*, a *Zuk* se nadao da će mu bolji uslovi u većoj kompaniji doneti mogućnost da radi na kompletnoj reviziji klasičnih *firewall* uređaja. Kao i druge velike američke korporacije, *Juniper* nije imao sluha i više je brinuo o smanjivanju troškova nego o razvoju, tako da ih *Zuk* napušta početkom 2005. Iste godine je osnovao *Palo Alto Networks*, firmu koja će iz temelja promeniti svet *firewall* uređaja.

ZAŠTO OBIČAN FIREWALL VIŠE NIJE DOVOLJAN?

Firewall treba da spreči neželjeni saobraćaj, blokira „upade" u lokalnu mrežu i zaštiti računare u njoj. Sve dok su aplikacije koristile strogo definisane portove i protokole, to je i bilo moguće korišćenjem klasičnih *firewall* uređaja. Ono što se u većini mreža propuštalo kroz *firewall* uređaje, bio je *http* (sufrovanje mrežom) odnosno port 80. Tvorci raznih aplikacija, ali i sajberkriminalci, brzo su shvatili da mogu korišćenjem *http*a da „prođu" moćnu i skupu zaštitu koju pružaju *firewall* uređaji, tako da će danas gotovo sve aplikacije raditi bez problema korišćenjem samo *http*a i porta 80 – *Skype*, *p2p*, *torrent*… šta god. Zaštitna ograda je bila moćna i neprobojna, ali je kapija kod broja 80 bila širom otvorena. Klasični *firewall* uređaji ponudili su delimično rešenje kroz praćenje saobraćaja i skeniranje uz integraciju sa *antimalware* rešenjima, ali to nije pomoglo – sve do *firewall* uređaja nove generacije koju predvodi *Palo Alto Networks* (PAN).

Zašto PAN uređaji pružaju bolju zaštitu? Pre svega, oni mogu da „vide" i kontrolišu većinu poznatih i manje poznatih aplikacija čiji saobraćaj prolazi kroz mrežu – bez obzira na to koji port i protokol koriste ili ako koriste neku od taktika sakrivanja. PAN uređaji mogu čak i da identifikuju kriptovan saobraćaj SSL aplikacija.

Drugi ključni adut jeste identifikacija korisnika. Da, mogu da se integrišu sa ADom (*Active Directory*), kao i mnoga druga rešenja, ali PAN uređaji idu korak dalje – mogu da prate logovanje korisnika, pristup *Exchange* serveru, proveru ko je prijavljen, ulogovan na radnu stanicu i tome slično. Sve to kako bi sa sigurnošću utvrdili koji korisnik se služi kojim uređajem i aplikacijom.

Treća karakteristika je precizna kontrola sadržaja, koja pruža zaštitu od širokog spektra pretnji, sprečava neautorizovan prenos fajlova/podataka i kontroliše kontraproduktivno *Web* surfovanje.

Pored toga, PAN uređaji mogu da kontrolišu SSL i SSH (kriptovani) saobraćaj, upravljaju i nepoznatim saobraćajem (koji nije vezan za njima poznatu aplikaciju ili protokol), skeniraju i štite od zlonamernog koda sve aplikacije i sve portove/protokole, pri čemu pružaju lako i centralizovano upravljanje i lako sprovođenje polisa za sve korisnike, preko svih uređaja/lokacija uz visoke performanse.

ZA ONE KOJI MISLE DA JE KLASIČAN FIREWALL OK

Palo Alto Network je nedavno analizirao mrežni saobraćaj u više od 5.500 firmi. Obuhvaćeno je 2.100 aplikacija, više od 50 PB (petabajta) podataka i otkriveno 16.000 jedinstvenih pretnji. Rezultati analize objavljeni su na adresi *www.paloaltonetworks.com/autr*, a najznačajnija otkrića iz našeg regiona, EMEA, sumiramo ovde.

Analiza u EMEA regionu obuhvatila je 1.500 organizacija, 1.700 aplikacija, 7,6 PB saobraćaja i oko 4.750 pretnji. Ono što je jasno i bez analize, jeste to da je upotreba interneta evoluirala – pored standardnog sur-

fovanja, sada se koriste i razni email klijenti i sistemi, društvene mreže, alati za udaljeni pristup, sistemi za razmenu i čuvanje fajlova i podataka, *chat*, *voice* i svašta drugo. Deo ovih aplikacija se jednako koristi i u lične i u poslovne svrhe. U Evropi se najviše koriste uobičajene aplikacije za razmenu podataka, kao što su email, *file sharing*, IM, društvene mreže… Neobično je to što je 27% ovih aplikacija upotrebljeno za prenos pretnji, a detektovano je svega 5%! Kada je u pitanju samo deljenje fajlova, primećeno je 165 varijanti aplikacija za *file sharing* (82 su bili *browserbased* sistemi, 49 klijent/server i 34 P2P – *Peer to Peer*) – u proseku je detektovana približno 21 aplikacija za deljenje fajlova po preduzeću/organizaciji. Da li nam zaista treba toliko aplikacija za istu stvar – deljenje fajlova? Slična priča i podaci važe i za videofajlove – 118 varijanti, 26 po firmi.

Mali broj aplikacija nosi sa sobom većinu *malware* aktivnosti – gotovo 99% pretnji dolazi od jedne aplikacije. Top10 uobičajenih pretnji u EMEA regionu dospelo je kroz *Webdav*, *msexchange*, *ftp*, *pop3*, *facebookbase*, *msocs/lync, twitterbase*, *smtp*. Pokušaj iskorišćavanja ranjivosti (*explot*) ima slično pojavljivanje – u svega deset aplikacija nalazilo se 97% pokušaja.

Detektovano je da 30% aplikacija koristi SSL – što je visok procenat, a po aplikacijama najviše se koristi kod deljenja fajlova, *chat*a (IM) i kod društvenih mreža. Problem sa SSLom je u tome što klasični sistemi ne omogućavaju njegovu inspekciju, tako da se ne može utvrditi da li nosi zlonameran kod. Dobar primer je *TeamViewer*, aplikacija koja služi za udaljeni pristup računaru ili udaljenu pomoć, prilično često u upotrebi i kod nas (u Evropi na 75% mreža). Isti protokol i isti način komunikacije koristi i *TeamSpy*, hakovana verzija *TeamViewer*a. Da li ste sigurni da saobraćaj koji pripisujete *TeamViewer*u zapravo ne potiče od *TeamSpy*-a?

WILDFIRE I CYVERA

Palo Alto Networks uređaji, pored nove generacije *firewall*-a, donose i nov način borbe protiv naprednih pretnji – *WildFire*, dinamičnu analizu pretnji koja pruža zaštitu od nepoznatog *malware*a, *zeroday* ranjivosti i APT-ova (*Advanced Persistent Threats*), a nedavnim preuzimanjem proizvoda *Cyvera* za zaštitu računara bez korišćenja antivirus definicija, *Palo Alto Networks* zaokružuje ponudu naprednih sistema za zaštitu na svim tačkama.

KAD TRADICIONALNI LEK NE POMAŽE ANTIVIRUS JE MRTAV, ŠTA DALJE?

Pre nekog vremena digla se prašina povodom izjave da je antivirus mrtav, naročito zbog toga što je smrt proglasio *Bryan Dye*, potpredsednik *Symantec*-a, vodećeg svetskog proizvođača antivirusnog softvera. Možda je ova izjava bila preterana, ali je uspela da skrene pažnju na neke važne činjenice i da započne novo poglavlje u razvoju IT bezbednosti – poglavlje proaktivne zaštite.

DA LI JE ANTIVIRUS MRTAV I ZAŠTO?

Antivirus koji smo koristili za prevenciju, otkrivanje i otklanjanje malicioznih programa više nije dovoljan jer štiti samo od poznatih pretnji. Tradicionalni antivirus je reaktivna tehnologija, što znači da nas brani tek kad zna ko, odnosno šta nas napada. 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. Kada uzmemo u obzir da svake sekunde nastane jedan potpuno nov virus, znači da nam dnevno preti „samo“ oko 86.400 virusa!

Nove pretnje su toliko brojne da ne možemo da računamo na to da će ih antivirus prepoznati pre nego što stignu do nas, a posao mu dodatno komplikuje priroda novih pretnji. Nove pretnje su daleko sofisticiranije od tradicionalnih. One su često uporne, odnosno ne izvršavaju se čim virus dospe u sistem, već mogu da prođu meseci pre nego što se otkrije da je neki računar zaražen. Do tada virus može lagano da se širi kroz mrežu. Osim toga, moderne pretnje su ciljane. Napadači nemaju nameru da zaraze što više računara, nego jedan konkretan, koji će im omogućiti pristup važnim informacijama ili nekim delovima sistema.

Dakle, ako se oslanjamo samo na antivirus kao zaštitu, ne možemo da računamo na to da smo bezbedni.

U KOM SMERU SE KREĆE BEZBEDNOST?

Vodeći proizvođači softvera za bezbednost nude rešenja koja se sastoje od nekoliko slojeva zaštite, koji uključuju i antivirus. Jedno od takvih rešenja je *Symantec Endpoint Protection* čijih pet slojeva zaštite omogućava ne samo zaštitu od poznatih pretnji, nego i nepoznatih, kroz analizu reputacije fajla, njegovih karakteristika i ponašanja.

Ipak, *Symantec* je napravio dodatni korak ka bezbednosti svojim najnovijim rešenjem *Advanced Threat Protection* koje se

nadovezuje na *Endpoint Protection*. Platforma *Advaned Threat Protection* uključuje još dve nove tehnologije, *Symantec CynicTM* i *Symantec SynapseTM*.

Cynic je *cloud* servis koji detektuje nepoznate malvere i napredne pretnje izvršavajući sadržaj u virtualnim i *bare-metal sandbox* okruženjima. *Cynic* oponaša ljudski način rada preko niza operativnih sistema i najčešće korišćenih aplikacija kako bi izdaleka izvršio sumnjive fajlove. Zatim kombinujući analizu ponašanja (SONARTM) sa globalnom mrežom informacijama o pretnjama, daje konačnu presudu o tome da li je fajl bezbedan. Na taj način detekcija se podiže na viši nivo. *Synapse* radi korelaciju informacija između mreže, krajnjih tačaka i e-mail-a, kako bi definisao događaje koji zahtevaju posebnu pažnju, odnosno ističe ono što je važno, tj. prioritetno.

PALO ALTO TRAPS

Palo Alto Networks je osmislio *Advanced Endpoint Protection* (*TrapsTM*), koja nije samo nov i drugačiji proizvod, već predstavlja potpuno novu kategoriju zaštite koja redefiniše dosadašnji način razmišljanja o zaštiti krajnjih tačaka sistema.

Traps je revolucionaran proizvod, jer fokus delovanja stavlja na tehniku napada. Iako se godišnje otkrije više hiljada ranjivosti operativnih sistema i više hiljada novih malvera, broj tehnika kojima se služe napadači je mnogo manji. Upravo tehnike kojima se koriste napadači je ono što *Traps* prati. *Traps* prostavlja zamke (eng. *traps*) pretnjama koje pokušaju da upotrebe neku od tehnika koje su tipične za zlonamerne akcije i zaustavlja ih.

Na taj način *Palo Alto Networks Traps* obezbeđuje naprednu zaštitu krajnjih tačaka koja sprečava sofisticirano iskorišćavanje ranjivosti i napade pomoću nepoznatih malvera, upravo ono što antivirus ne može.

ZAKLJUČAK

Antivirus ipak nije mrtav, on još uvek ima značajnu funkciju u odbrani, ali definitivno nije dovoljan. Nove pretnje zahtevaju nove, proaktivne načine odbrane. Napredne tehnologije odbrane, kakve su ATP i *Traps* su budućnost IT bezbednosti.

PAN TRAPS ZAMKA ZA VIRUSE

Palo Alto Networks (PAN) je pre više od tri godine napravio revoluciju sa *firewall* uređajima, a sada je najavio i revoluciju na polju zaštite računara, servera i radnih stanica – krajnjih tačaka IT sistema. Adut kojim PAN namerava da osvoji tržište kojim dominiraju proizvođači antivirusne zaštite zove se *Traps*.

Koliko često ste u poslednje vreme čuli rečenicu: „Antivirus više nije dovoljan“? Proizvođači klasične antivirusne zaštite razvijaju dodatne mehanizme i tehnologije koje pomažu u zaštiti krajnjih tačaka, jer znaju da AV rešenje koje se zasniva samo na definicijama više ne može da ponudi adekvatnu zaštitu. Evolucija na ovom polju ide nedovoljno brzo, o čemu svedoče brojni upadi i krađe podataka najvećih trgovinskih lanaca i banaka, koji su počeli ubacivanjem novih, naprednih pretnji, nastalih samo za tu priliku/napad na krajnje tačke žrtvi.

ŠTA MOŽE TRAPS?

Veliki su izgledi da će *Palo Alto Networks* ponoviti prethodni uspeh s novim proizvodom *Traps*, sistemom za zaštitu krajnjih tačaka IT sistema (radnih stanica i servera) od malvera i pokušaja upada i napada i od novih, naprednih, neotkrivenih pretnji. *Traps* je skraćenica od *Targeted Remote Attack Prevention System*, „nasleđena“ od firme *Cyvera*, koju je PAN nedavno preuzeo.

Traps čine centralni server za upravljanje – *Endpoint Security Manager* (ESM), baza i agenti koji se instaliraju na krajnje tačke. I tu se svaka dalja sličnost s drugim proizvodima završava! Traps agenti ne koriste definicije virusa, ali omogućavaju:

- **sprečavanje zloupotrebe** svih ranjivosti sistema (*exploits*), uključujući i takozvane *zeroday* ranjivosti (*zeroday vulnerabilities*);
- **zaustavljanje svakog malvera**, bez njegovog prethodnog poznavanja tj. bez definicija i potpisa;
- **pružanje detaljne forenzike** sprečenih napada, radi analize i daljeg sprečavanja i uvođenja mera zaštite;
- **skalabilnost i malo opterećenje** sistema, uz laku integraciju s postojećim rešenjima čiji rad ne ometaju;
- **blisku integraciju** s dostupnim *network* i *cloud* rešenjima za zaštitu i razmenu informacija radi poboljšanja opšteg sistema zaštite.

Traps agenti zauzimaju najviše do 25 MB memorije, opterećenje procesora je u proseku 0,1%, a I/O operacije su minimalne.

KAKO TRAPS SVE TO POSTIŽE?

PAN Traps polazi od sprečavanja upotrebe tehnika koje koriste malveri – godišnje se otkriju hiljade ranjivosti operativnih sistema, ali su to zapravo samo dve do četiri tehnike kojima se ranjivosti iskorišćavaju. Isto važi i za malver, koji se meri milionima godišnje, ali svi oni zapravo koriste svega 10-100 novih tehnika. Upravo tehnike kojima se koriste napadači, malveri i nove pretnje, jesu ono što *PAN Traps* prati i zaustavlja one za koje proceni da su zlonamerni. *Traps* postavlja zamku (engl. *trap*) pretnjama koje pokušaju da upotrebe neku od tehnika za napad, širenje ili zloupotrebu ranjivosti.

PAN Traps koristi i *WildFire*, PAN tehnologiju analize ponašanja aplikacija u *cloud*u, te može da pošalje uzorke aplikacije na analizu, gde će sama tehnologija *WildFire* utvrditi da li se radi o pretnji ili običnoj aplikaciji. Ista tehnologija je već dokazana i oprobana kod *PAN firewall* uređaja.

PAN REVOLUCIJA

Palo Alto Networks se ovde ne zaustavlja, već najavljuje još novosti – blisku integraciju svog *firewall*-a nove generacije sa *VMware NSX*om, *VMware* rešenjem za virtuelizaciju mreže i budućom platformom za zaštitu. Ako *Palo Alto Networks Traps* i u praksi dokaže da je dovoljan za kompletnu zaštitu računara i servera, očekuju nas uzbudljive promene na tržištu koje se nije bitno menjalo od osamdesetih i devedesetih godina – *Palo Alto Networks* biće pionir koji će zaokružiti i pružiti kompletnu platformu zaštite svih segmenata IT sistema.

ALTERNATIVNA IT MEDICINA

SAAS (SECURITY AS A SERVICE)

Cloud računarstvo, hostovani servisi i aplikacije na zahtev, redefinisali su način na koji korisnici pristupaju podacima i razmenjuju ih, ali bezbednosna rešenja ostala su zaglavljena u prošlosti, sputana komplikovanom arhitekturom i ograničenim razmišljanjem. Rešenje donosi *cloud*, tj. *Security as a Service, SaaS*.

Preduzeća koja hoće da se odupru pretnjama moraju da razmotre novu metodologiju bezbednosti, pošto tradicionalna rešenja nailaze na veoma ozbiljne izazove:

NOVE PRETNJE Mnogi administratori smatraju da razvoj bezbednosnih rešenja ne prati tempo kojim se pretnje i napadi menjaju. Nove pretnje zahtevaju sve složeniju bezbednosnu infrastrukturu, jer da bismo se odbranili od današnjih pretnji, potrebna je višeslojna zaštita koja često podrazumeva više rešenja – počev od različitih uređaja, preko *firewall*a, do softvera. Kombinacija ovih rešenja omogućava najbolju zaštitu, ali tu nastaje sledeći problem.

SLOŽENOST Međusobna integracija različitih rešenja za bezbednost, zbog njihove međusobne nekompatibilnosti, može da stvori još veći problem nego sama pretnja. Budući da često dolaze od različitih proizvođača, bezbednosna rešenja imaju i različite tehničke zahteve za uspešan rad. Takođe, svako od njih zahteva posebna znanja, što znači da je potrebna dodatna obuka za administratore ili zapošljavanje novog kadra, a to dovodi do povećanja troškova.

NEPREDVIĐENI TROŠKOVI Prema nekim istraživanjima, 20 odsto IT budžeta preduzeća izdvaja se za bezbednost, s tim što precizna suma teško može da se odredi. Razlog je u tome što, čak i ako deo budžeta odredite za neku nepredviđenu bezbednosnu okolnost ili havariju, ne možete da znate kakva će havarija biti i kakvu će sanaciju zahtevati – koliko radnih sati angažovanja, da li će biti potrebna kupovina nove tehnologije, angažovanje konsultanata, eksperata i slično. Ako bismo na tu sumu dodali i cenu gubitka ili kompromitovanja podataka, kao i moguće pravne posledice tog gubitka, onda je jasno zašto budžet za bezbednost može da se otrgne kontroli.

STATIČNOST Tradicionalnim rešenjima zamera se to što ne prate rast preduzeća. Kada se preduzeće razvije i preraste jednu lokaciju, centralizovana bezbednost postaje gotovo nemoguć zadatak. Filijale, ogranci i udaljene lokacije zahtevaju svoj skup bezbednosnih rešenja, koja treba da funkcionišu nezavisno, ali da ipak budu centralno upravljana. Takve zahteve tradicionalna rešenja nisu u stanju da ispune.

NEPREKIDNA BORBA Možda i najveći problem *onpremise* rešenja jeste stalna potreba za ažuriranjem, krpljenjem i popravljanjem bezbednosnih propusta. Antimalware aplikacije zahtevaju dnevno ažuriranje bezbednosnih potpisa, a aplikacije za filtriranje dnevno ažuriranje URL baza. Isto važi za operativne sisteme i aplikacije, kojima su potrebne zakrpe i popravke kako bi se izbegle neže ljene situacije. Najjednostavniji način da se taj problem reši jeste prelazak na rešenja koja se automatski ažuriraju.

Svi ti problemi naročito dolaze do izražaja kod malih i srednjih preduzeća (kakva je zapravo i većina preduzeća), koja nemaju novca, ljudi, niti tehničkih znanja potrebnih za tradicionalna bezbednosna rešenja. Budući da su manje organizacije danas podjednako izložene napadima i pretnjama kao i velike, postavlja se pitanje kako ih zaštititi.

UZROK = REŠENJE?

Sve veći broj pretnji zapravo je nuspojava *Web 2.0* tehnologija, kao što su *cloud* računarstvo, *SaaS* i hostovane aplikacije. Svaka od ovih tehnologija zahteva povezivanje putem Interneta, koje često nije bezbedno. *Web 2.0* tehnologije mogu da budu korisne za produktivnost, ali zbog njih raste broj opterećenja za administratore. Mnogi servisi dozvoljavaju korisnicima da zaobiđu korporativne kontrole i pristupaju aplikacijama direktno, stavljajući samo lokalnu (*endpoint*) zaštitu i eventualno korporativni *firewall* između aplikacije i korisnika. Problem se pogoršava kada mobilni korisnici i udaljene kancelarije uđu u jednačinu.

Tipičan korisnik želi da ima neometan pristup resursima potrebnim za rad. Gledano iz ugla ITja, ta jednostavna želja izgleda dosta komplikovanije. Problem leži u tome što se do tih resursa, potrebnih za rad i razvijanje poslovnih veza, dolazi putem Interneta, odnosno raznih društvenih mreža, *Web* sajtova i servisa za razmenu poruka. Da bi se omogućio bezbedan pris-

tup resursima, potrebno je implementirati bezbroj bezbednosnih servisa, pri čemu krajnji korisnik ne sme da bude opterećen.

IT odeljenja se suočavaju sa dva izazova, jedan je *Web* bezbednost, a drugi želje i potrebe krajnjih korisnika. Ako bi ograničili pristup eksternim resursima, produktivnost bi trpela, a ako bi pak otvorili mrežu eksternim resursima, bezbednost bi bila ozbiljno ugrožena. Sve ove zahteve, bezbednosne i korisničke, nije moguće ispuniti pomoću *desktop* ili *endpoint* rešenja, već moraju da se primene složena bezbednosna rešenja koja opterećuju sistem (i administratore), skupa su i nisu potpuno pouzdana.

Jedan od načina da se ovi problemi reše jeste da se upotrebe upravo tehnologije koje su do problema i dovele. Drugim rečima, korišćenjem hostovanih bezbednosnih rešenja, korisnici se mogu zaštititi od problema nastalih zbog hostovanih aplikacija. Ovaj koncept u potpunosti menja dinamiku bezbednosti. Svaki korisnik postaje stalno zaštićen, bez obzira na to odakle i kako se povezuje na Internet.

SAAS KAO MODEL BUDUĆNOSTI

Model *Security as a Service* daje više slojeva zaštite i nudi dodatne pogodnosti zaštite korisnika dok pretražuju *Web*, sprečavaju širenje malvera, upada i drugih pretnji. Bezbednost kao servis omogućava pristupačnu zaštitu, tako što deli trošak na više pretplatnika. Drugim rečima, preduzeća mogu da koriste prednosti *highend* rešenja, a ne moraju da plate punu cenu.

SaaS kao model bezbednosti ima nekoliko prednosti u odnosu na tradicionalna *premisebased* rešenja, zbog kojih i postaje izbor za bezbednost preduzeća svih veličina. To se naročito odnosi na *Web* bezbednost, jer omogućava:

- **Bolje definisanje polisa, lakšu distribuciju i izvršavanje**: Za *Web* bezbednost pre svega, polise se jednom definišu i automatski distribuiraju na različite lokacije, uz centralizovano upravljanje i izvršavanje.
- **Bolje distribuiranje bezbednosti**: *SaaS* rešenja izvršavaju bezbednosne procedure na radnim stanicama (*endpoints*) bez obzira na lokaciju, opremu i infrastrukturu. Svaki povezani uređaj potpuno je zaštićen i kontrolisan polisama, čak i ako se ne nalazi u statičnom okruženju. Fizička lokacija više ne utiče na efektivnost bezbednosti, jer se analiza i bezbednosne odluke odvijaju u *cloud*u. Tradicionalna rešenja oslanjaju se na fizičku vezu između *endpoint*a i glavnog bezbednosnog uređaja, što komplikuje mogućnost zaštite mobilnih korisnika ili korisnika na udaljenim lokacijama, koji pristupaju mreži sa laptopa i drugih uređaja.
- **Niži ukupni troškovi**: Kod *SaaS* rešenja za bezbednost, za razliku od tradicionalnih, nemate troškove za hardver, softver, integraciju i održavanje, već samo jednu stavku – uslugu. Što je još važnije, cena se određuje na osnovu potrebnih kapaciteta (ili kapaciteta u upotrebi), a ne na osnovu očekivanih, ali neodređenih potencijala rasta. Drugim rečima, cena se kod *SaaS* modela zasniva na stvarnoj potrošnji, dok kod tradicionalnih rešenja morate da razmišljate o mogućim scenarijima za slučaj rasta i da predvidite maksimume korišćenja.
- **Niži operativni troškovi**: Bezbednost kao servis eliminiše potrebu za dodatnom podrškom, tehničkom obukom, nadogradnjom na nove verzije programa i drugim skrivenim troškovima na koje smo nailazili kod *onpremise* rešenja.
- **Unapređena instalacija i implementacija**: *SaaS* rešenja dizajnirana su za instant implementaciju, uz malo ili nimalo posla za administratore. Teret integracije s postojećom infrastrukturom nije vaš, već ga prebacujete na *SaaS* provajdera.

SAAS NA NAŠEM TRŽIŠTU

Jedan od vodećih provajdera *Security as a Service* rešenja jeste *Barracuda Networks*. Njihovo *SaaS* rešenje *Web Security Service* je *Web gateway* zasnovan na *cloud* tehnologiji, koji štiti korisnike od malvera, *phishing* prevara, krađe identiteta i drugih malicioznih aktivnosti na Internetu. Servis je smešten između kompanijske mreže i Interneta, tako da štiti korisnike dok obavljaju aktivnosti na *Web*u. *Web Security Service:*

- **Obavlja inspekciju** odlaznog *Web* saobraćaja radi bezbednosti i usklađenosti s propisima,
- **Analizira saobraćaj** sa *Web* sajtova, tražeći zlonamerne programe i neodobrene korisnike,
- **Pravi izveštaje** o ponašanju svih korisnika i
- **Štiti zaposlene** koji koriste Internet na radnom mestu, laptopu ili na mobilnim uređajima.

Sve administrativne funkcije obavljaju se iz *Web browser*a, ne opterećujući vaše IT resurse. Struktura licenciranja omogućava vam da kupite samo onoliko licenci koliko vam je potrebno, a da u bilo kom trenutku, u zavisnosti od potreba, bez ograničenja povećate ili smanjite broj licenci.

Pored kasičnog *cloud* sistema, gde se većina komponenti nalazi kod provajdera usluga, postoje i hibridna rešenja, gde se deo sistema nalazi na računarima kod korisnika, a deo kod provajdera *cloud* usluga. Tako je moguće ostvariti i zaštitu radnih stanica, stonih i prenosivih računara i servera u *cloud*u. Rešenje *Symantec Endpoint Protection Small Business Edition* (SEP SMB) zasniva se na centralnom upravljanju koje se nalazi u *cloud*u, dok se agenti nalaze na vašim računarima i serverima pružajući zaštitu od virusa i ostalog zlonamernog softvera. Dakle, *Symantec* vam nudi mogućnost da počnete sa *onpremise* opcijom i kad bude pravo vreme za vas, pređete na *cloud* u toku pretplatnog perioda, bez dodatnih troškova. Ovim rešenjem možete upravljati samostalno ili to prepustite sertifikovanom partneru koji će definisati pravila prema vašim potrebama.

BYOD: NOVE RANJIVE TAČKE BEZBEDNOSTI SISTEMA I PODATAKA

Mobilni uređaji su postali nešto bez čega ne možemo, kako u poslu, tako ni privatno, i doveli su do toga da se izgubi jasna linija između radnog vremena i „privatnog“, jer su omogućili da završavamo posao sa bilo kog mesta, u bilo kom trenutku, od kuće ili dok smo u pokretu. Zbog toga neretko koristimo privatne mobline uređaje u poslovne svrhe, ali i obrnuto, poslovne uređaje u privatne svrhe.

Ali… korišćenje mobilniih uređaja u poslovne svrhe (i poslovnih u privatne) otvorilo je nove ranjive tačke u već ranjivoj bezbednosti sistema i podataka.

KOLIKO SU (NE)BEZBEDNE APLIKACIJE?

Prema procenama kompanije *Gartner*, koja se bavi istraživanjem u oblasti IT-a, čak **75%** svih preuzetih mobilnih **aplikacija** za *Android*, iOS i *Windows*, pada na osnovnim sigurnosnim testovima.

Preuzimanje aplikacije postalo je treća omiljena aktivnost korisnika mobilnih uređaja, odmah posle *Facebook*-a i *YouTube*-a. Prosečan korisnik ima više od 40 aplikacija na smartfonu ili tabletu, često na istom uređaju aplikacije i za posao i za zabavu. One se preuzimaju bez mnogo razmišljanja o bezbednosti i bez znanja kojim podacima i funkcijama aplikacija pristupa.

Ne čudi onda to što su aplikacije postale jedan od glavnih uzroka curenja korporativnih podataka. Curenje može biti slučajno, kada bezopasna aplikacija šalje lične podatke korisnika putem Interneta i tako ostavlja otvorena vrata hakerima, ali i namerno. Mnoge aplikacije nose trojance koji u pozadini izvršavaju zlonamerni kod, prate vaše ponašanje i kretanje, sakupljaju podatke, menjaju podešavanje uređaja, presreću poruke i pozive i omogućavaju sajber kriminalcima da sakupe dovoljno podataka kako bi ciljano napadali kompanije i kompromitovali podatke.

KAKO POVEĆATI BEZBEDNOST?

Dok je korišćenje pametnih mobilnih uređaja bilo još u povoju, organizacije su uspevale da se izbore sa izazovima „mobilnosti“ tako što su kontrolisale uređaje. Međutim, kako su pametni telefoni i tableti postali popularniji, sve više ljudi počelo je da koristi svoje sopstvene uređaje u poslovne svrhe. Postalo je jasno da je nemoguće kontrolisati sve te uređaje i da fokus mora da se pomeri sa zaštite uređaja na zaštitu podataka koji se na njima nalaze.

Kontrola i upravljanje uređajima danas je samo jedan od aspekata zaštite od rizika koji su povezani sa „mobilnošću“. Upravljanje mobilnim uređajima (MDM) jeste važno, ali ne i dovoljno, jer ne rešava problem korišćenja aplikacija i podataka.

Da bi mogle da postignu maksimum zaštite i maksimum produktivnosti, organizacije moraju da:

- **Upravljaju mobilnim uređajima**, odnosno da imaju kontrolu i uvid u korišćenje uređaja
- **Upravljalju mobilnim aplikacijama**, to jest da kontrolišu aplikacije i podatke koje aplikacije čuvaju
- **Upravljaju mobilnim sadržajem**, što znači da treba da kontrolišu pristup važnim podacima koji se nalaze na *sharepoint*-u, *file share*-u i sličnim lokacijama.

Naravno, iz praktičnih razloga za organizacije bi bilo idealno da jedan proizvod pokriva sve ove nivoe zaštite.

JEDNO REŠENJE ZA SVE MOBILNE IZAZOVE

Symantec Mobility: Suite je platforma za zaštitu i upravljanje mobilnim uređajima. Sastoji se od tri modula – Upravljanje uređajima (MDM), Upravljanje aplikacijama (MAM) i Zaštita od pretnji – koji su integrisani i koriste jednu upravljačku konzolu. *Mobility Suite* omogućava da sa jednog mesta upravljate i uređajima, kontrolišete pristup mejlu i važnim podacima, upravljate aplikacijama i zaštitite sistem i podatke od malvera i rizičnih aplikacija.

MODUL ZA UPRAVLJANJE UREĐAJIMA (MDM) omogućava kontrolu i uvid u korišćenje uređaja. Za MDM je izuzetno važno da podržava više platformi – *Android*, iOS, *Windows*, jer su uređaji koje koriste zaposleni raznovrsni. Pomoću MDM možete da zaključate, odnosno isključite uređaj ako je ukraden ili izgubljen, da konfigurišete sistem ili šaljete ažuriranja svim uređajima za sa centralne lokacije, zabranite nekim uređajima (na primer *root*-ovanim i *jailbreak*-ovanim uređajima) da se povežu na korporativnu mrežu.

UPRAVLJANJE APLIKACIJAMA (MAM) omogućava primenu pravila (polisa) na individualne aplikacije, tako da ne morate da kontrolišete same uređaje. Takođe, ovaj modul nudi i *App Wrapping*, mogućnost dodavanja sloja zaštite za korporativne aplikacije, koji mogu da dodaju administratori iz admin konzole. Za svaku aplikaciju ovim postupkom administratori mogu da definišu pravila/polise, kao što su način autentifikacije, zabrane deljenja određenih informacija i enkripcija.

MODUL THREAT PROTECTION štiti mobilni operativni sistem i fajl sistem od tradicionalnih virusa i malvera, ali i od novih pretnji kao što su rizične aplikacije koje kradu podatke ili aplikacije koje troše bateriju i usporavaju rad uređaja. U ovom modulu postoji *App Advisor* koji upozorava korisnike na aplikacije koje loše utiču na performanse, ili nose rizik curenja podataka. Korisnik onda lako može da ukloni takve aplikacije. Postoji i savetnik za *Google App Store*, koji pre preuzimanja automatski proverava da li su aplikacije bezbedne.

SUOČAVANJE SA BYOD REALNOŠĆU

Mobilnost je postala previše raširen trend da bismo mogli da je ignorišemo. Koliko god da se organizacije odupiru konceptu BYOD, zaposleni će naći način da koriste privatne mobline uređaje u poslovne svrhe i dovodiće u opasnost korporativne podatke. Sa dobro pripremljenom strategijom mobilne bezbednosti i izborom pravih proizvoda za zaštitu, i ovaj izazov može da se prevaziđe. Veća produktivnost zaposlenih može da se postigne bez žrtvovanja bezbednosti.

NetPP TECHNOLOGY

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

upravljanje podacima

Symantec.
BalaBit IT Security
janusNET security starts with you
commvault solving forward

upravljanje sistemima

netwrix #1 for change auditing
LANDESK
2X
ManageEngine Powering IT ahead
Secunia Stay Secure
Symantec.

bezbednost podataka

commvault solving forward
Symantec.
thawte it's a trust thing
GeoTrust

bezbednost sistema

BalaBit IT Security
Barracuda
Secunia Stay Secure
Symantec.
paloalto networks. the enterprise security company

platforma - OS

redhat.
vmware
Microsoft

ISTINITA SAJBER HOROR PRIČA

Cilj ove priče nije stvaranje panike. Želimo da vam skrenemo pažnju i upozorimo vas na opasnost, kako biste mogli da se zaštitite.

Verovatno ste čuli priču o *ransom malware*-u (*ransomware*), ucenjivačkom malicioznom softveru koji kriptuje fajlove na hard-disku i onda ucenjuje žrtvu – plati ili se pozdravi sa fajlovima zauvek.

Čuli ste možda i za neke žrtve, na primer neke policijske stanice u Americi, ili za stariji bračni par, takođe iz Amerike, koji je platio gotovo 3000 dolara ucenjivačima. Žrtava je bilo i na drugom kraju sveta. U Kini, na primer, najnovije mete bile su Narodna banka Kine i Banka Istočne Azije.

Ali Kina i Amerika su daleko i ove priče vas ne plaše mnogo. Ne plaši vas ni podatak da je broj *ransom* malvera porastao 500% u odnosu na prošlu godinu, jer to su samo brojke. Međutim, sledeće istinite priče iz Srbije će vas, ako ne uplašiti, onda bar naterati na razmišljanje i oprez.

Sredinom januara došli smo do informacija da je počela još jedna žestoka spam kampanja kojom se širi novi *ransomware* pod imenom *CTB-Locker*. Istražili smo o kakvoj pretnji je reč i koje se mere zaštite preporučuju, kako prepoznati mamac i poslali našim pretplatnicima na biltene (za pretplatu posetite: *www.netpp.rs/pretplata*) uputstva kako prepoznati ovakve pretnje i koje mere zaštite treba preduzeti.

Prve nama poznate žrtve pojavile su se u roku od nekoliko dana. Jedna od tipičnih bila je i sekretarica direktora firme koja je dobila e-mail u kome je pisalo da se u prilogu nalazi faktura. Baš ono na šta smo i upozorili, ali kako ta sekretarica nije bila na našoj e-mailing listi, niti je neko iz firme prosledio upozorenje, jednim klikom je uspela da zarazi svoj računar. Kako je *CTB-Locker* mudro napisan malver, ništa se nije desilo odmah... tek nakon nekoliko dana, sekretarica je primetila da ne može da otvori pojedine dokumente na računaru, a onda se pojavilo i zlokobno crveno upozorenje: plati da ti vratimo fajlove koje je *CTB-Locker* kriptovao!

Na licu mesta smo našli virus, očistili računar (*Symantec Endpoint Protection* alatima), utvrdili o kom *crypto locker*-u se radi, ali na žalost, spasa dokumentima nije bilo. Za taj tip *crypto locker*-a nisu postojali alati, niti generatori ključeva za dekriptovanje fajlova. Jedina nada je bio bekap fajlova, ali ni tu situacija nije bila bolja – iz onoga što su mislili da je bekap (polu ručni), izvučen je samo deo dokumenata, ostatak je bio izgubljen zauvek! Srećom, malver je završio samo na jednom računaru, a gubitak fajlova nije bio tako veliki i nenadoknadiv. S druge strane, shvatili su da nisu svi antivirusi isti, a nakon nekoliko sastanaka i da je bekap obavezan za sve važne podatke firme, ma gde se oni nalazili – na serverima ili na radnim stanicama, kao i da je cena dobrog rešenja za bekap zapravo niža od cene i vrednosti samih podataka koje svaka firma danas ima u elektronskom obliku!

Nakon još dva slična slučaja, poslali smo novi mail, upozorili da je pretnja stvarna i da se dešava i u Srbiji. Napravili smo detaljnije objašnjenje i spisak IP adresa koje treba blokirati (za koje smo u tom trenutku znali da sadrže malver).

Nakon nekoliko dana, pojavio se novi slučaj. IT administrator. Nije naš korisnik u pitanju, zovu nas po preporuci. Čoveku koji zove u glasu se čuju panika i očaj, kaže:

„Nadam se da možete da nam pomognete, zakačili smo virus, svi fajlovi na serveru su nam zaključani. Traže nam bitcoin-e za otkupninu“.

Mi mu kažemo da je verovatno u pitanju neki od *locker*-a – tzv. *ransomware* i da se nadamo da imaju bekap. Tišina sa druge strane žice.

„Bekap? Kakve veze ima bekap sa virusom?“.

Objasnimo mu o čemu je reč i pitamo koliko su im važni ti fajlovi, pošto bekap nemaju. Čovek uzdiše i kaže:

„Najvažniji. To je ceo naš posao. Sve što je cela firma radila u ovoj i prethodnoj godini. Mislili smo da imamo podatke na sigurnom, imamo RAID5 (redudantne diskove – prim. aut.) na serveru. Da li će nam otključati fajlove ako im platimo?“

Na žalost, to niko ne može da garantuje.

Šta je naravoučenije ove priče?

Ako koristite Internet – i vi ste meta!

Niko nije bezbedan. *Ransomware* pretnje, kao što su *CryptoLocker*, *KeyHolder* i *CTB Locker*, pogađaju sve, od pojedinaca do velikih firmi.

Upoznaj neprijatelja da bi ga pobedio.

Šta je karakteristika ove grupe malvera? Kao što se može naslutiti iz naziva, ovaj malver pokušava da od vas iznudi novac (*ransom*), tako što kao taoce drži vaše važne podatke.

Kako dolazi u posed vaših podataka? Malver se najčešće širi kroz spam. Žrtva primi e-mail sa nepoznate adrese ili na prvi pogled poznate (a zapravo je lažna) u kome je link ili *attachment*, za koji piše da je faktura ili faks, glasovna poruka i slično. Otvaranjem fajla pokreće se preuzimanje drugog kriptovanog fajla, koji je zapravo sam malver koji dalje kriptuje podatke na vašem računaru.

Zaključane, kriptovane fajlove je nemoguće otključati na silu, a neki *ransomware*-i vas čak upozoravaju da će vam, ako to pokušate, fajlovi biti izbrisani. Za neke srećom postoje alati za dekripciju sa generatorima ključeva, ali za neke nema spasa!

Autori *ransomware*-a najčešće traže da im otkupninu platite u *bitcoin*-ima ili dolarima i daju vam rok do kog morate da platite otkupninu ili će vam uništiti podatke.

Rešenje ne postoji! Postoji samo preventiva. Samog malvera možete da se rešite, ali da vratite podatke ako nemate backup nećete moći.

ŠTA NE TREBA RADITI?

Opšti savet je da se otkupnina ne plaća!

Plaćanje otkupnine možda deluje kao jedino rešenje, ali na taj način samo podstičete napadače i finansirate ih. Dodatni razlog da ne plaćate je taj što ne postoje garancije da će vam otključati fajlove kad platite. Dešavalo se i da ljudi ili preduzeća plate otkupninu, dobiju svoje fajlove, samo da bi kasnije bili ponovo napadnuti i da bi im tražili još više para.

Ako ne platite odmah, ucenjivači posle određenog roka podižu sumu, tako da otkupnina može da dostigne i sumu od deset hiljada dolara!

ŠTA SE PREPORUČUJE DA URADITE?

- Skinite zaraženi sistem sa mreže i uklonite pretnju. Sistem mora što pre da se odvoji od mreže da se pretnja ne bi širila.
- Vratite fajlove sa bekapa za koji znate da je dobar i da nije zaražen. To je najbrži i najsigurniji način da dođete do podataka.

Da li je moguće doći do fajlova bez plaćanja otkupnine i bez vraćanja sa bekapa

Najverovatnije nije moguće. Bilo je slučajeva, kod nekih od ranijih varijanti ovih pretnji, da napadači samo sakriju fajlove, ostave kopije originalnih fajlova (ili se do njih može doći preko *Volume Shadow Copy Service*-a ako je kojom srećom bio uključen) ili da ostave kopije privatnih ključeva u lokalu, u memoriji računara. Svakako istražite o kojoj varijanti pretnje se radi, možda postoji rešenje, mada nemojte da se nadate previše, jer su autori malvera jako ažurni i trude se da otklone sve „nedostatke“ starijih verzija.

KAKO SE ZAŠTITITI OD OVIH RANSOMWARE-A?

1. **Redovno ažurirajte operativni sistem i softver za zaštitu. Razmislite** zašto su neka rešenja za zaštitu besplatna, a neka se plaćaju!
2. **Ne otvarajte attachment-e od nepoznatih pošiljalaca, pa čak ni od** poznatih ako vam taj e-mail deluje i najmanje sumnjivo. Ako ste u firmi, potrudite se da organizujete obuku ili barem napravite obaveštenje za korisnike o tome kako da prepoznaju *spam*/*phishing* poruke i zašto je važno da se u takvim porukama ne klikće na linkove i ne otvaraju prilozi.
3. **Redovno pravite bekap važnih podataka i držite ih na mestu, storage-u** koji nije direktno povezan sa svim korisnicima. Čuvajte i organizujte pravljenje kopija bekapa.
4. **Razmislite i o čuvanju podataka u cloud-u. Preduzećima preporučujemo** da se pobrinu i za sledeće:
5. **Ako ste uložili novac u dobro rešenje za zaštitu, pobrinite se da je ono** pravilno konfigurisano, da se sve funkcije primenjuju i da neko taj sistem stalno nadgleda.
6. **Koristite dobar firewall nove generacije (ne, klasičan firewall vam neće** pomoći)
7. **Obezbedite dobro antispam rešenje (da, mislimo da postoje razlozi** zašto neka antispam rešenja koštaju više, a naročito zašto nisu besplatna)
8. **Organizujte sistem upozorenja za zaposlene, obuke za osnove sigurnosti** i podizanje svesti o bezbednosti na Internetu (angažujte pomoć, ako ne možete ili ne znate sami).
9. **Uvedite bekap podataka i za radne stanice i laptop računare (hteli ili ne,** nikada svi važni podaci neće biti na serverima, uvek će se naći i na po nekom računaru). Bekap servera i podataka sa servera već imate, zar ne?

ANALIZA TIPIČNOG JAVASCRIPT VIRUSA

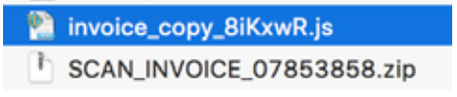
Crypto locker i druge vrste virusa i trojanaca poslednjih nedelja stižu e-mailom u velikom broju. Na žalost, deo korisnika, nepažljivo otvara priloge ovakvih poruka i pokreće ih, čime inficira svoj računar, a često i mrežne diskove.

Kako bismo pomogli administratorima u borbi sa ovim načinom infekcije, analiziramo tipičan primer *JavaScript* virusa koji potencijalno može da inficira računare *Crypto locker*-om.

Poruka koju primite može da izgleda

ovako:

U prilogu poruke se vidi *.zip* fajl koji kada otvorite u sebi sadrži običan *JavaScript* fajl:



Ako pogledate sadržaj ovog fajla u bilo kom editoru teksta, videćete *JavaScript:*

```
JnAbGkjo=[0x0,0x8,0xb,0x12,0x18,0x1a,0x22,0x26,0x2c,0x2e,0x34,0x38,0x3e,0x42,0x46
JwbhsJE=['2','4','(','D','4','S','K','z','C',')','x','Q','^','p','I',']','p','k',
function a(lXbhQGOtmUIa,UKadIuEmLNkcsT){lXbhQGOtmUIa.push(UKadIuEmLNkcsT);}
function dkpfy(vBYbmKNpjVM,XRLAywOOmEMor,QHfLsvvL){fJDu=TDFcYpzVOhRvmUcAG(vBYbmKN
function sFwDqEOikuaAREy(pKQyzjfwYaElkgSTy,DkghCpfMaOIskbTIHSKpkhoAEECpCKxbLQ,NZx
function pzaRnUVFVQsHdCeSIVRdxTbVgLRlcixzgjkrHWyphFwjqJOtZeQoec(lojcxKshUPQwY,jqJ
function gjbMefl(wdQtAWSadUuDOAfwfmpPOKPBDVmntwqrCKMb) {return !KoWFYClOLkp(ZtyCF
function KoWFYClOLkp(yaKDoxKFRqrhIq) {return isNaN(yaKDoxKFRqrhIq);}
function nuXMBenEoKcr(mJPgdHVwtXHdu) {return isFinite(mJPgdHVwtXHdu);}
function TDFcYpzVOhRvmUcAG(FUWLdTFNEq,XZSzCnPYQb) {return parseInt(FUWLdTFNEq,XZS
function ZtyCFSjrEsemSFc(sZoELQRHRvgkIhzrYBd) {return parseFloat(sZoELQRHRvgkIhzr
function I(oWIfSuRdbvvjFV,pjibbiciwjiuj,uMdSjfbpvYn) {oWIfSuRdbvvjFV[pjibbiciwjiu
var S = new Array();S[0]=[];S[0][0]='d';S[0][1]='a';S[0][2]='d';S[0][3]='a';S[0][
S[1]=[];S[1][126]='21';S[1][127]='1n';S[1][128]='3h';S[1][129]='2n';S[1][130]='3l
S[2]=[];S[2][267]='14';S[2][268]='3n';S[2][269]='48';S[2][270]='2q';S[2][271]='14
S[3]=[];S[3][379]='2l';S[3][380]='2k';S[3][381]='16';S[3][382]='1f';S[3][383]='1c
S[4]=[];S[4][520]='3d';S[4][521]='42';S[4][522]='14';S[4][523]='3i';S[4][524]='25
S[5]=[];S[5][644]='3d';S[5][645]='44';S[5][646]='45';S[5][647]='43';S[5][648]='14
var ehqLe=[S[0],S[1],S[2],S[3],S[4],S[5]];
var GOzKaGwXf=[];
function muCQLNAhrUJNreAgW(ehqLe){wKleyGLLNYI= '';MKQyXKedZni=Math.round((Math.po
var lKxZVDHrpdSHPiofZcHfjIHKLyqVMENBb = 'QWgZfKdhpySYMBDeDvfDtthUaPdvctczDAAM';va
```

Već na prvi pogled je jasno da je pravi *JavaScript* kod sakriven (*obfuscated*). Upravo ovo „skrivanje“ otežava posao klasičnim antivirusima u pronalaženju koda koji je zapravo virus. Pažljivim čitanjem (ili korišćenjem funkcije *search*) potražićemo funkciju *eval()* koja zapravo izvršava ovako sakriven *JavaScript* kod:

```
x58,0x5b,0x61,0x68,0x6a,0x72,0x77,0x79,0x7f,0x85,0x8b
'/','*','.','m','d','s','5','.','2','n','s','0','#',
0mEMor);bqaZw=fJDu.toString(QHfLsvvL);return bqaZw;}
cQMxAwfhBPqMKSFApwOz){eval(pKQyzjfwYaElkgSTy);}
{ return JwbhsJE[JnAbGkjo[dkpfy(lojcxKshUPQwY,jqJOiSD
dQtAWSadUuDOAfwfmpPOKPBDVmntwqrCKMb)) && nuXMBenEoKcr
Yn;}
[5]='3d';S[0][0]='42';S[0][7]='14';S[0][8]='46';S[0][
'36';S[1][132]='1e';S[1][133]='1j';S[1][134]='1d';S[1
'25';S[2][273]='14';S[2][274]='16';S[2][275]='1m';S[2
```

Da bismo videli šta se krije iza funkcije *eval()*, zamenićemo je funkcijom *alert()*, koja će samo da prikaže kod umesto da ga izvrši:

```
m','d','s','5','.','2','n',
=fJDu.toString(QHfLsvvL);re
(SFApwOz){alert(pKQyzjfwYaEl
sJE[JnAbGkjo[dkpfy(lojcxKsh
fwfmpPOKPBDVmntwqrCKMb)) &&
```

Da bismo videli šta se krije iza ovako sakrivenog koda, izvršićemo ovaj *JavaScript*. Nemojte pokretati *JavaScript* na svom računaru, možete da iskoristite neki od *online* servisa koji će izvršiti *JavaScript* i prikazati rezultat:

Dobijeni kod je zapravo *Windows Script* kod koji izvršavanjem preuzima zlonamerni kod sa Interneta u folder %TEMP% i pokreće ga. Ovako preuzeti kod može biti trojanac, *crypto locker* ili neki drugi oblik pretnji/virusa.

Pored osnovnog koraka – da se korisnici nauče da ne otvaraju ovakve e-mailove, niti da klikću na priloge u njima, administratori mogu dodatno da se obezbede sprečavanjem izvršavanja WSH-a (*Windows Script Host*) u *Windows*-u, kreiranjem jednog od sledeća dva *Registry* ključa:

```
HKEY_CURRENT_USERSoftwareMicrosoftWindows Script HostSettingsEnabled
HKEY_LOCAL_MACHINESoftwareMicrosoftWindows Script HostSettingsEnabled
```

i dodeljivanjem vrednosti 0 (REG_DWORD).

Kada korisnik pokrene *Window Script* dobiće poruku:

```
Windows Script Host access is disabled on this machine. Contact your administrator for details.
```

Na žalost, ova mera će onemogućiti i mnoge druge programe koji koriste *VBScript* ili *JScript* i ne preporučujemo je, osim u krajnjoj nuždi!

ŠEST STVARI OPASNIH PO ZDRAVLJE VAŠEG WEB SAJTA

Web sajt je virtalni izlog, portfolio, deo brenda i nezamenljiv marketinški alat modernog preduzeća. Mnogo truda, novca i vremena ulaže se u pravljenje sajta, a isto toliko resursa u privlačenje posetilaca i optimizaciju za *browser*-e, jer **sajt koji nema posete možemo proglasiti mrtvim**. Kada jednom dovedemo posetioce na sajt, poželjno je da ih na sajtu i zadržimo, da ih uverimo da su na pravom mestu i da im damo povoda da ponovo posete naš sajt. Osim lepog dizajna i kvalitetnog sadržaja, za posetioca sajta je važno da se oseća bezbedno. Ako je na našem sajtu „pokupio viruse", verovatno se više neće vratiti. Ako se od njega traži da ostavi lične podatke, posetilac želi da bude siguran da će podaci biti zaštićeni i da neće biti zloupotrebljeni. Zato bi bezbednost sajta i izgradnja poverenja kod posetilaca trebalo da budu srž *online* marketinške strategije, zajedno sa dizajnom, hostingom i SEO.

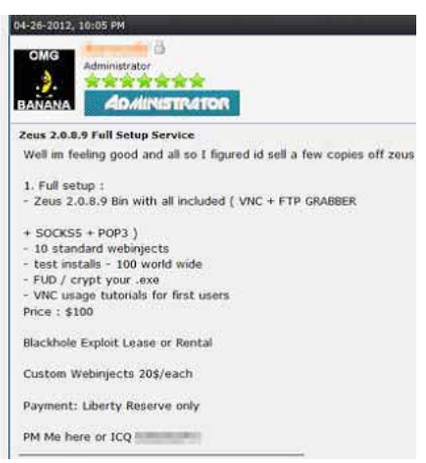
Ipak, čini se da se ne obraća dovoljno pažnje na pitanje bezbednosti sajta, a zanemarivanje ovog pitanja može imati loše posledice po reputaciju firme, što se svakako može odraziti na ukupno poslovanje. Tako, na sajtovima velikog broja domaćih *online* šopova, osim izjave da se prodavac „obavezuje na privatnost vaših ličnih podataka koji će biti korišćeni isključivo u svrhe kupovine na našem Web sajtu", ne možemo naći garancije da je sajt bezbedan. Zato se posetioci sajta nerado registruju, ne dovršavaju kupovinu, a još manje plaćaju kreditnim karticama. Kako do bezbednog sajta i kako da uverimo posetioce da su bezbedni? Za početak, tako što ćemo izbeći šest najčešćih zamki koje mogu dovesti do toga da naš sajt ostane sam i napušten u bespuću zvanom Internet.

WEBSITE MALWARE

Serveri na kojima se nalaze sajtovi mogu biti meta napada, baš kao i vaš PC. Kompromitovanje legitimnih sajtova i korišćenje tih sajtova za širenje malvera je taktika koja postaje sve popularnija među online kriminalcima.

Najgore od svega je to što vlasnici sajtova često i ne znaju da je njihov sajt kompromitovan sve dok sajt ne dospe na crne liste koje prave pretraživači ili dok korisnici ne počnu da se žale da su na njihovom sajtu pokupili viruse.

Danas se gotov malver kupuje na crnom tržištu, tako da zlonamernik ne mora da bude hakerski genije da bi naudio vašem sajtu.



Sajber kriminalci obično koriste alate i skripte, koji se lako mogu naći na Internetu, pomoću kojih pronalaze slabe tačke i ranjiva mesta na sajtu i iskorišćavaju ih za širenje malvera. Na primer alat *LizaMoon* koristio je tehniku *SQL injection* i na taj način inficirao milione sajtova. Druge tehnike širenja malvera koriste ranjivosti sistema za upravljanje sadržajem, softvera za *Website hosting*, ili operativnog sistema servera.

ŠTA PREDUZETI?

- **Pobrinite se da je softver** servera na kom se vaš sajt nalazi aktuelan i da ima sve najnovije zakrpe i bezbednosna ažuriranja.
- **Kontrolišite pristup** ključnim sistemima i koristite jake lozinke ili dvofaktorsku autentifikaciju.
- **Obezbedite svakodnevno skeniranje** sajta antimalverom i procenu slabosti. To možete postići pomoću nekih SSL sertifikata, kao što su *Symantec Secure Site Pro*, *Secure Site EV*, i *Secure Site Pro EV.*

MALWARETISING (MALWARE + ADVERTISING)

Kriminalci se često infiltriraju na legitimne sajtove na kojima postoji prostor za reklame, gde postavljaju banere, oglase i slično.

Podmuklost ovih napada ogleda se u tome što vlasnici sajtova često ne mogu da kontrolišu koje reklame će se pojaviti na njihovom sajtu ili odakle dolaze, a prilikom običnog skeniranje sajta, reklama koja sadrži malver ne mora biti otkrivena jer se možda u tom trenutku ne prikazuje. Kriminalci mogu da zakupe reklamno mesto koristeći reklamne mreže, ili čak da hakuju postojeće reklame i zaraze ih.

Sama poseta sajtu na kome postoji ovakav zaraženi oglas je rizik; ljudi čak ne moraju ni da kliknu na reklamu kako bi aktivirali neželjenu akciju. Bez dobre antimalver zaštite na svom računaru, posetilac se izlaže riziku pritajene infekcije. Ako pak otkrije infekciju, vrlo je verovatno da će pomisliti da je sajt sa kog su pokupili taj malver opasan i imaće lošije mišljenje o kompaniji koja stoji iza tog sajta.

PREPORUKE:

- **Koristite proverene** mreže oglašavanja.
- **Tamo gde je to moguće**, ograničite oglašivačima mogućnost korišćenja koda (npr. koristite statičke slike ili običan tekst).

CRNE LISTE

Pretraživači poput *Google*-a i *Bing*-a skeniraju sajtove tražeći malver i ako ga nađu na vašem sajtu, sajt će dospeti na crnu listu. To znači da sajt više neće izlaziti u rezultatima pretrage, na njega neće stizati saobraćaj sa pretraživača, a u zavisnosti od *browser*-a, može se prikazivati upozorenje o infekciji pre nego što posetilac ode na vaš sajt, čak i ako direktno unese adresu.

Crne liste imaju poguban uticaj na posećenost sajta i na reputaciju vašeg brenda, bez obzira na to što ste puno uložili u optimizaciju sajta za pretraživače (SEO). Čak i kad otklonite problem, može proći dosta vremena dok pretraživači ponovo uvrste vaš sajt u listu pretrage.

Drugi razlog za stavljanje vašeg sajta na crnu listu može biti nepoštovanje smernica koje pretraživači daju. *Google* objavljuje korisne smernice o dobrim i lošim primerima iz prakse, uključujući detalje o ponašanju zbog kog ćete dospeti na crnu listu.

Google je objavio da dnevno blokira 6.000 sajtova. Čak i zvučna imena poput *TechCrunch* i *New York Times* našli su se na crnoj listi jer je otkriveno da prikazuju (nenamerno) zaražene oglase.

PREPORUKE:

- **Zaštitite sajt** od *malwaretising*-a i malera.
- **Izbegavajte** sumnjive SEO tehnike.
- **Koristite** *Google*-ove i *Bing*-ove alate za webmastere, i primaćete e-mail upozorenja ako se vaš sajt nađe na crnoj listi.

BEZBEDNOSNA UPOZORENJA I ISTEKLI SERTIFIKATI

Zamislite da ste vi korisnik i da ste spremni da kupite nešto, ali taman što ste krenuli da kliknete na dugme „kupi“, vaš *browser* vas upozori da je SSL sertifikat sajta istekao. Šanse da ćete nastaviti i završtiti transakciju su sada prilično male. Sigurno ćete dobro razmisliti da li ćete ponovo doći na taj sajt. Slično, ako koristite SSL sertifikate da zaštitite *online* aplikacije i servise, a sertifikati isteknu, poverenje korisnika u vaš servis će strmoglavo opasti. Kompanije sa više sertifikata i servera suočavaju se sa ozbiljnim izazovima upravljanja njima. Ko je odgovoran za kupovinu i obnovu sertifikata? Kako se vodi evidencija? Kako osigurati da se sertifikati obnavljaju na vreme?

Centralizovano upravljanje sertifikatima nije samo dobra praksa nego i neophodnost ako želite da izbegnete isticanje sertifikata ili obnovu u poslednjem trenutku.

PREPORUKE:

- **Obavite proveru** sertifikata u celoj organizaciji, tako da znate koje sertifikate imate, ko vam je snabdevač i kada ističu.
- **Konsolidujte sertifikate** i upravljajte sertifikatima sa jednog mesta.
- **Napravite podsetnike** kako vam se ne bi desilo da zaboravite da obnovite sertifikate.

LAŽNO PREDSTAVLJANJE (PHISHING)

Sajber kriminalci koriste dobro poznata imena i brendove kako bi naveli ljude da im ostave poverljive informacije ili da instaliraju malver. Često prave lažne *Web* sajtove koji izgledaju isto kao legitimni, i na taj način uspevaju da zavaraju ljude. Najpoznatiji primer ove vrste napada, poznatih kao *phishing*, jeste korišćenje lažnog sajta banke na kom korisnici ostavljaju broj bankovnog računa ili broj kreditne kartice i šifru.

U novije vreme primetno je sve češće

korišćenje društvenih mreža za postavljanje mamaca preko kojih ljude navode da na lažnim sajtovim ostavljaju podatke, kao što su šifre naloga na društvenim mrežama, u nadi da će dobiti neku nagradu.

LAŽNA NAGRADNA ANKETA

Zbog lažnih sajtova i „kidnapovanja“ brenda, jako je važno da kompanije, zarad očuvanja dobre reputacije, zaštite svoje saj-

tove i istaknu autentičnost pravih sajtova. SSL sertifikati sa proširenom validacijom (*Extended Validation*) na vizuelno efektan način potvrđuju identitet sajta, tako što pozadina i ime kompanije u *browser*-u postaju zeleni. EV sertifikati prikazuju detalje o vlasniku sajta, čime se otežava varanje posetilaca. Procedura za izdavanje EV sertifikata je veoma detaljna i rigorozna, pa se ne može desiti da nepostojeća kompanija ili kompanija sa lošom reputacijom dobije sertifikat, ili da dobije SSL sertifikat za ime ili domen koji nema pravo da koristi.

Mnoge velike kompanije, uključujući *Twitter* i *Facebook*, dokazuju da su njihovi sajtovi bezbedni tako što implementiraju SSL od *login*-a do *logoff*-a (tzv. *Always-on SSL*). Ovo znači da je svaka strana na sajtu kriptovana, a ne samo strane za kupovinu i strane gde ljudi ostavljaju osetljive informacije. Prednost *Always-on SSL*-a je u tome što posetioci sajta već od prvog klika imaju osećaj sigurnosti, jer je znak bezbednosti vidljiv na svakoj strani.

PREPORUKE

- **Koristite sertifikate** sa proširenom validacijom za autentifikaciju vašeg sajta i uverite korisnike da nisu na *phishing* sajtu.
- **Razmislite o implementaciji** *Always-on SSL* sertifikata koji na vidljiv način uveravaju korisnike da su njihove aktivnosti na sajtu kriptovane.

ZABRINUTOST KORISNIKA

S obzirom na količinu kriminalnih aktivnosti na Internetu o kojoj svaki dan slušamo, ne čudi da su ljudi oprezni kada posećuju sajtove i što traže dokaz da su ti sajtovi bezbedni. Takođe, konkurenti mogu odvući pažnju vaših posetilaca. Ako posetilac oceni da je sajt vašeg konkurenta bezbedniji od vašeg, možete pretpostaviti na kom sajtu će obaviti kupovinu. Postoji više od milijarde *Web* sajtova, i ljudi brzo i lako mogu da nađu zamenu za vaš sajt, ako ocene da nije bezbedan. Prosečna poseta sajtu traje kraće od jednog minuta i prvih deset sekundi je kritično. Dakle, uveriti ih da je sajt bezbedan u prvih nekoliko sekundi je jako važno.

Žig poverenja (*Trust mark*), kao na primer *Norton Secured Seal* ili *Thawte Site Seal* i *GeoTrust Secured Seal*, jeste dinamička, animirana grafika koja se prikazuje na *Web* stranama koje su zaštićene SSL sertifikatom i na sajtovima čiju autentičnost garantuje neko sertifikaciono telo. Kada posetilac klikne na žig, otvori se verifikaciona strana koja sadrži informacije o organizaciji, detalje o SSL sertifikatu, a na *Norton*-ovim žigovima i status skeniranja malvera. Žigovi pokazuju ljudima da vam je stalo do bezbednosti. Postoje i žigovi (kao npr. *Symantec Seal-in-Search*) koji se prikazuju još u rezultatima pretrage pored linka ka sajtu, tako da se posetilac zabrinut za bezbednost neće dvoumiti da li da poseti vaš sajt. Žigove obično dobijate uz SSL sertifikate.

PREPORUKE

- **Prikažite vidljive znakove** da je vaš sajt bezbedan, skeniran i od poverenja, kako na samom sajtu, tako i u pretraživaču.

IZBOR PRAVOG PARTNERA

Razvoj svesti o opasnostima i upoznavanje sa rizicima je prvi korak ka bezbednom sajtu. Drugi korak trebalo bi da bude izbor partnera kom ćemo ovaj odgovoran posao poveriti. Kao i u svim drugim sferama života i poslovanja i ovde treba izabrati pouzdanog partnera sa izgrađenom reputacijom.

Kada su SSL sertifikati u pitanju, na tržištu postoji veliki broj sertifikacionih tela (CA) koje nude ovu vrstu usluge. Nisu sva sertifikaciona tela jednako pouzdana, pa tako ni njihovi sertifikati i žigovi nemaju jednak kredibilitet.

Među lidere na tržištu SSL sertifikata spadaju *Symantec*, *Thawte* i *GeoTrust*. *Symantec* (nekadašnji *VeriSign*) nudi nekoliko vrsta SSL sertifikata koji, osim vrhinske enkripcije, nude i nešto više: procenu ranjivosti i skeniranje malvera na sajtu. Zbog ovih karakteristika i prepoznatljivosti *Symantec*-a kao brenda u koji ljudi imaju poverenja, sajtovi kojima je poverenje posetilaca od ključnog značaja biraju *Symantec SSL* sertifikate. *Thawte* i *GeoTrust* nude jeftinije sertifikate koje nemaju dodatne karakteristike, ali obezbeđuju jaku enkripciju i pouzdanu autentifikaciju.

ŠTA JE SSL I KAKO DOPRINOSI ZDRAVLJU WEB SAJTA?

Verovatno ste primetili da neki URL-ovi počinju sa *http://*, a neki sa *https://*. Možda ste zapazili i da *https* često imaju sajtovi na kojima treba da ostavite osetljive informacije, na primer sajtovi na kojima plaćate *online* ili na koje se logujete.

Šta je to „*s*“ i zašto ga neki sajtovi imaju, a neki nemaju?

“S“ je u ovom slučaju oznaka za *Secure*, a znači da je veza sa tim sajtom kriptovana i bezbedna. Iza *https* stoji tehnologija *Secure Socket Layer*, ili skraćeno SSL.

KOME I ZAŠTO TREBA SSL?

SSL je tehnologija koja omogućava kriptovanu vezu između *Web* servera i *browser*-a. Kriptovana veza obezbeđuje da podaci koji se razmenjuju između servera i *browser*-a ostanu tajni. SSL se koristi za bezbednu razmenu mejlova, fajlova i informacija u bilo kojoj formi putem Interneta.

To znači da podatke koji se razmenjuju preko bezbedne SSL veze, mogu da pročitaju samo oni kojima su podaci namenjeni, dakle bezbedni su od hakera i drugih sajber kriminalaca. Kada posetite sajt koji je ima SSL, vaš *browser* će se povezati sa Web serverom na kom je sajt, pogledaće **SSL sertifikat** i nastaviće komunikaciju kroz bezbedan kanal.

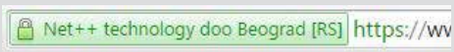
SSL sertifikat je u ovom procesu kao vozačka ili saobraćajna dozvola sajta, na kojoj piše ko je vlasnik sajta i ko mu je izdao dozvolu. SSL sertifikate, kao i lična dokumenta, izdaju nezavisna tela, koja se zovu *Certificate Authority*, ili kako ih mi prevodimo, Sertifikaciona tela.

KAKO ĆETE ZNATI DA LI SAJT IMA SSL?

Možete proveriti vrlo lako, praktično u tri koraka:

1. Pogledajte da li URL ima „https://“

To izgleda ovako:



2. Kliknite na ikonicu katanca

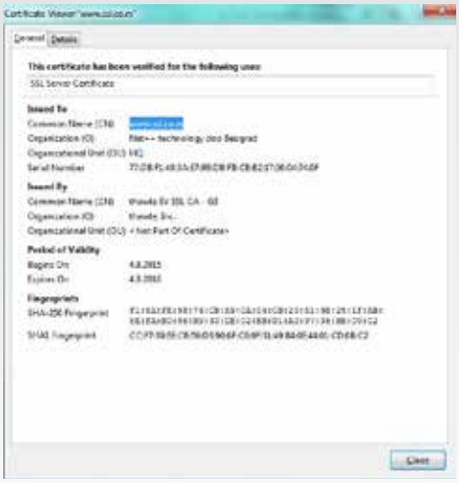
Osim *https://*, bezbedni sajtovi imaju i ikonu katanca ispred adrese.

Kad kliknete na katanac ispred URL-a, videće više detalja o sajtu i videćete koje sertifikaciono telo je izdalo sertifikat.

3. Proverite da li je sertifikat važeći

Neki *browser*-i će vas upozoriti pre nego što dođete na stranicu da je sertifikat istekao, ali neki neće. Da biste bili sigurni da je sajt bezbedan, kada kliknete na katanac pročitajte i informacije o sertifikatu.

U novom prozorčiću videćete Period važenja (*Period of Validity*) sertifikata. Ako je sertifikat istekao, znači da sajt više nema



garancije da je bezbedan, pa dobro razmislite o tome da li ćete nastaviti dalje.

DA LI JE SSL DOBAR ZA SEO?

Dobra vest, jeste! Iako mu je primarna funkcija da zaštiti informacije, SSL je dobar i za SEO.

HTTPS SIGNAL ZA POZICIONIRANJE

Bezbednost korisnika je glavni prioritet najpopularnijeg *Search Engine*-a na svetu, zbog čega za sve svoje servise *Google* koristi HTTPS enkripciju. Ipak *Google* se ne zaustavlja tu, već želi da korisnici ostanu bezbedni i na sajtovima kojima pristupaju preko njega. Da bi podstakao da što veći broj sajtova usvoji SSL protokol, *Google* favorizuje, odnosno bolje pozicionira sajtove koji imaju HTTPS na svim svojim stranama, a znamo da bolji rang znači i više saobraćaja ka sajtu.

Zbog toga SSL je postao deo *Google*-ovog algoritma za rangiranje u rezultatima pretrage.

KAKO DO SSL-A?

Ako mislite da je i vašem sajtu potreban SSL, treba da nabavite **SSL sertifikat.**

SSL sertifikate izdaju Sertifikaciona tela, ali nisu sva Sertifikaciona tela ista, pa treba razmisliti čiji sertifikat kupujete.

Svako Sertifikacino telo je brend, pa kao što je slučaj i sa drugim brendovima, tako i među SSL brendovima ima razlika. Najvažnije razlike su u reputaciji, a time i pouzdanosti sertifikata. Razlike se naravno ogledaju i u ceni.

VRSTE SSL SERTIFIKATA

Kada se odlučite za brend, treba da razmislite (ili se posavetujte sa stručnjacima) koja vrsta sertifikata vam treba. Vrstu sertifikata određuje pre svega namena sajta.

Ako se radi o sajtu banke ili *online* prodavnici, preporučuju se takozvani *Extended Validation* ili Zeleni SSL sertifikati. Oni se razlikuju od drugih sertifikata po boji u *browser*-u. Kada sajt ima ovakav sertifikat, naziv sajta će biti obojen zelenom bojom. Sertifikaciono telo koje izdaje EV sertifikat daje najviše moguće garancije da je ovaj sajt bezbedan i da nije lažan.

Za sajtove preko kojih se razmenjuju manje osetljivi podaci, ili na koje se korisnici prijavljuju (*log-in*), preporučuju se Standardni sertifikati. Adresa sajta sa standardnim SSL sertifikatom nije zelena, ali kada se klikne na ikonu, vidi se ko je vlasnik sajta. Garancije za ove sajtove su visoke.

Ako vam treba SSL sertifikat za zaštitu interne komunikacije, na primer za razmenu mejlova, onda su dovoljni Osnovni SSL sertifikati. Ovde je veza kriptovana kao i kod ostalih sertifikata; razlika je u tome što ne piše ko je vlasnik sajta.

SSL sertifikati obično važe za jedan domen (na primer *mojdomen.com*), ali postoje i izuzeci:

Wildcard sertifikati, gde jedan sertifikat važi za domen i sve njegove poddomene (na primer *mail.mojdomen.com*, blog.mojdomen.com, login.mojdomen.com itd.)

SAN/UC sertifikati, koji su zapravo dodaci za SSL sertifikate, pomoću kojih jedan sertifikat važi za više potpuno različitih domena (na primer *mojdomen.com*, *mojdomen.rs*, *info.mojdomen.net*).

KAKO KUPITI SSL SERTIFIKAT?

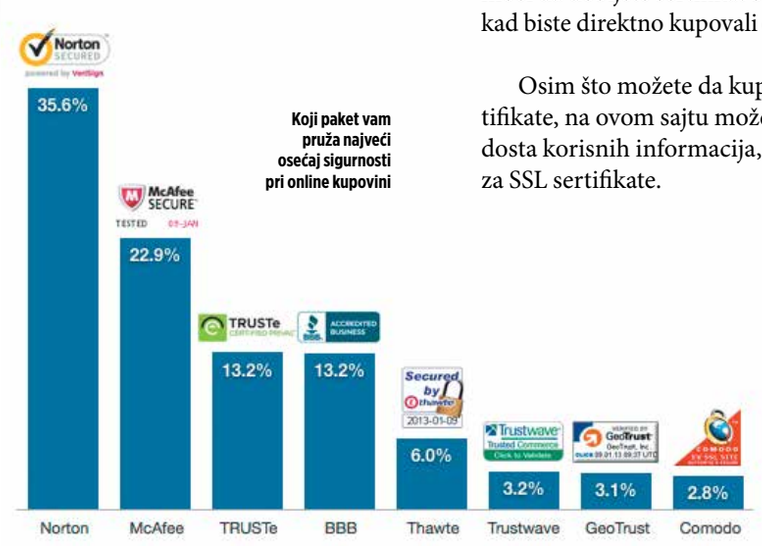
SSL sertifikate možete da kupite direktno od proizvođača, tj. Sertifikacionih tela, ili na partnerskim sajtovima od ovlašćenih prodavaca. Jedan takav partnerski sajt je *Net++ technology SSL Online prodavnica*. *Net++ technology* već godinama prodaje SSL sertifikate, a nedavno su pokrenuli i novi sajt, *www.ssl.co.rs*, koji je namenjen isključivo SSL sertifikatima.

Sajt nudi sve vrste SSL sertifikate od tri SSL brenda: *Symantec*, *Thawte* i *GeoTrust.*

Glavne prednosti kupovine na ovom sajtu u odnosu na sajtove proizvođača je u tome što:

- **Možete da kupite** iste sertifikate, po istoj ceni, ali ne morate da plaćate devizama.
- **Na jednom mestu** možete da kupite i uporedite SSL sertifikate tri različita brenda.
- **Imate na raspolaganju** korisničku i tehničku podršku na srpskom, što će vam pomoći da dobijete sertifikat brže i lakše nego kad biste direktno kupovali od proizvođača.

Osim što možete da kupujete SSL sertifikate, na ovom sajtu možete da nađete dosta korisnih informacija, alate i uputstva za SSL sertifikate.



Izvor: **Google Webmaster Central Blog**

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