CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Zero day ranjivosti

NCERT-PUBDOC-2010-01-289

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Važna stavka računalne sigurnosti je održavanje sustava ažurnim što se tiče sigurnosnih zakrpa i nadogradnji. Nakon što proizvođači doznaju da postoji ranjivost u njihovom programskom paketu, oni objavljuju sigurnosnu preporuku i po potrebi zakrpu ili obnovljenu inačicu u kojoj je sigurnosni problem uklonjen. Sveti gral napadača je otkrivanje *zero day* ranjivosti, odnosno ranjivosti koje nisu još poznate proizvođačima i za koje ne postoji programska zakrpa. Napadač može iskoristiti takvu ranjivost za stvaranje programskog koda koji ju zloupotrebljava. Informacije o novootkrivenoj ranjivosti i načinima iskorištavanja su profitabilne. Trgovina podacima o *zero day* ranjivostima postoji otkad postoje i sigurnosni propusti u programima. Crno tržište *zero day* ranjivostima razvilo se zbog njihove ilegalne upotrebe. Prije nekoliko godina razvio se trend kupnje i prodaje informacija o spomenutim ranjivostima kao legalni izvor prihoda jer informacije kupuju, na primjer, vladine organizacije ili tvrtke koje se bave računalnom sigurnosti, a prodaju ih stručnjaci za sigurnost. Međutim, *zero day* tržište većim je dijelom ilegalno i pojedinci koji otkriju ranjivosti mogu ostvariti puno veći profit prodajom na crnom tržištu ili iskoritiiti otkrivenu ranjivost u zlonamjerne svrhe.

U dokumentu će biti objašnjen pojam te tržište *zero day* ranjivosti. Također, bit će riječi o etičkim aspektima tržišta informacijama o spomenutim ranjivostima te programima koji ih zloupotrebljavaju. Zatim su opisane poznate *zero day* ranjivosti u posljednjih nekoliko godina uz diskusiju o sigurnosti programa otvorenog koda i onih zatvorenog koda. Osim toga predložene su i moguće metode zaštite.

2. *Zero day* ranjivosti

Zero day ranjivost je sigurnosni propust u računalnoj aplikaciji koji je otkriven i poznat je napadačima prije nego što za njega zna proizvođač i javnost. Za takvu ranjivost proizvođač još nije objavio zakrpe koje uklanjaju problem. Izraz „*zero day*" ili „nulti dan" nastao je kao vremenska oznaka ranjivosti. *Zero day* napad se obično javlja prije prvog ili nultog dana svjesnosti proizvođača o ranjivosti, što znači da proizvođač još nije imao priliku popraviti sigurnosni propust kojeg napadač koristi za pokretanje napada.

Obično postoje dvije skupine stručnjaka koji istražuju i otkrivaju nove sigurnosne propuste:

- oni koji žele popraviti ranjivi program i
- oni koji žele zlonamjerno iskoristiti ranjivost.

Tvrtke kojima je funkcija da učine programske pakete sigurnima imaju dovoljno velik budžet i odlične veze s tvrtkama koje se bave razvojem računalnih programa te često mogu otkriti ranjivosti prije zlonamjernih korisnika. Međutim, u utrci za otkrivanjem ranjivosti novih programa često pobjeđuju zlonamjerni korisnici, obično programeri koji ili sami iskoriste ranjivost ili ju objave tako da ju netko drugi može zlouporabiti. Sve se to odvija bez znanja proizvođača koji zbog toga ne mogu ništa učiniti kako bi spriječili napad. Vrijeme u kojem je ranjivost aktualna, odnosno proizvođač nije svijestan da ona postoji u novo izdanom programu obično traje od nekoliko dana do nekoliko tjedana.

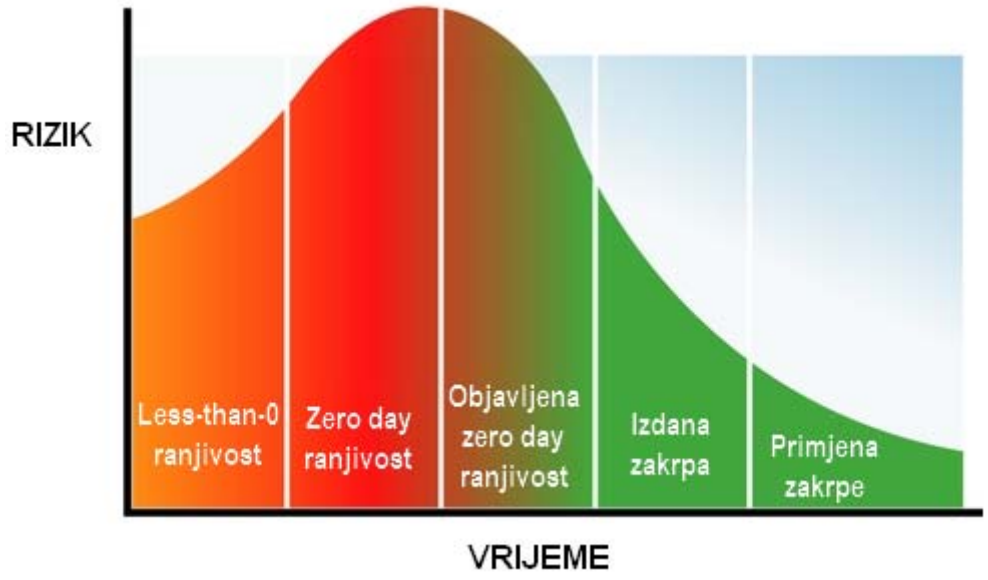
Zero day ranjivosti su opasne jer je korisnicima osobnih računala vrlo teško zaštititi se od njihove zlouporabe, obzirom da još uvijek ne postoji zakrpa ili nova inačica koja uklanja ranjivost.

Nakon što prođe određeno vrijeme od objave *zero day* ranjivosti tvrtka u čijem je programskom paketu otkrivena ranjivost može izdati zakrpe koje ju uklanjaju. Čak i u slučaju kada propust otkriju zlonamjerni korisnici, potrebno je neko vrijeme prije nego što ranjivost bude iskorištena za pokretanje napada jer oni obično prvo pokušaju prodati podatke o ranjivosti ili sami napisati zloćudni programski kod koji iskorištava ranjivost. Pisanje takvog programskog koda nije uvijek jednostavno. U tom vremenu tvrtka ima priliku ukloniti ranjivost prije nego ju netko zlouporabi. Međutim, iskustvo pokazuje da ranjivost najčešće otkriju zlonamjerni korisnici. U tom slučaju može se dogoditi da su i ranjivost i vektori napada objavljeni na isti dan, što znači da je programski paket u kojem je otkriven propust izuzetno podložan napadu protiv kojeg još uvijek ne postoji zaštita.

U hakerskim krugovima se napadači koji izvedu uspješan napad iskorištavanjem *zero day* ranjivosti smatraju elitom jer je vrlo teško otkriti takvu ranjivost i izvesti napad. Otkrivanje *zero day* ranjivosti, kao i pisanje programa za njihovu zlouporabu, zahtjeva opsežno poznavanje programskih jezika, struktura programa u kojem se traži ranjivost, mreža računala, operacijskih sustava te iskustvo, snalažljivost, trud i inovativnost.

2.1. Faze otkrivanja i uklanjanja zero day ranjivosti

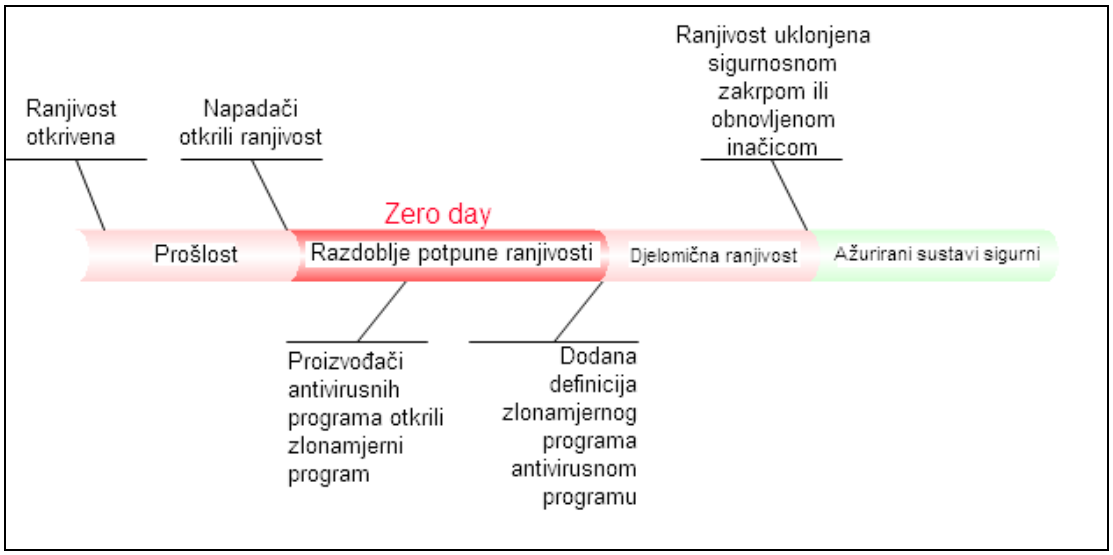
Otkrivanje i uklanjanje *zero day* ranjivosti odvija se u nekoliko faza u kojima opasnost od iskorištavanja ranjivosti raste i pada s vremenom, kao što je moguće vidjeti na sljedećoj slici.



Slika 1. Rizik u odnosu na vrijeme od otkrivanja ranjivosti do primjene zakrpe

Vremensko razdoblje u kojem postoji sigurnosna prijetnja koja još uvijek nije objavljena i/ili priznata naziva se *„less-than-zero"* ranjivost. *Zero day* ranjivost predstavlja velik rizik za korisnike, dok *less-than-zero* ranjivost ne predstavlja toliko velik rizik. Većina *zero day* ranivosti otkriva se raznim testovima ranjivosti i ranjivost je poznata prije nego što je poznat način njezine zlouporabe. *Less-than-zero* ranjivost se otkrije tek nakon što su uočeni dokazi o zlonamjernom programskom kodu.Životni ciklus ranjivosti:

- **Postojanje ranjivosti**: u 99 % slučajeva ranjivost je jednostavna pogreška u programu ili previd koji možda već postoji i u prijašnjim inačicama programa. Problem, prema tome, možda postoji već dulje vrijeme, ali nitko ga nije otkrio u prijašnjim inačicama te je bezazlen.
- **Ranjivost otkrivaju zlonamjerni korisnici:** jednom kada je ranjivost otkrivena počinje utrka između napadača i proizvođača. Napadači će pokušati spriječiti proizvođača da dozna o kakvoj se ranjivosti radi što je dulje moguće kako bi odgodili izdavanje zakrpa koje bi uklonile sigurnosni problem. Neki nazivaju ovu fazu i *vrijeme potpune ranjivosti*. Postoji sigurnosni propust u programu, uz to postoje i metode zlouporabe propusta, a istovremeno ne postoji metoda zaštite od napada i nema zakrpe koja uklanja problem.
- **Otkriveni zlonamjerni programi koji iskorištavaju ranjivost**: u nekom trenutku informacija o postojanju ranjivosti postaje javno dostupna te se objavljuju sigurnosne preporuke u kojima se pojašnjavaju sigurnosni propusti i preporučaju metode zaštite.
- **Detekcija zlonamjernog programa dodana u sigurnosne programe za detekciju**: otkrivanjem novih zloćudnih programa, proizvođači programskih paketa dodaju podatke za njihovo otkrivanje u svoje baze podataka. Zbog toga je vrlo važno da su baze antivirusnih programa na računalima korisnika ažurne.
- Ova faza se može još nazvati i **razdoblje djelomične ranjivosti**. Antivirusni programi, kao i programi za otkrivanje zlonamjernog programskog koda mogu otkriti programe koji iskorištavaju ranjivost. Međutim to je samo djelomična zaštita, ranjivost još uvijek postoji u programu i još uvijek nije objavljena zakrpa. Napadači će napisati nove zlonamjerne programe koji će koristiti istu ranjivost i ostati korak ispred ažurnosti baza podataka.
- **Ranjivost je uklonjena objavom zakrpe ili obnovljene inačice**: proizvođač će objaviti zakrpu koja uklanja sigurnosni problem. Sustavi koji su ažurirani tako da primjenjuju zakrpu sada su zaštićeni od napada koji iskorištavaju spomenuti problem. Zbog toga je bitno održavati operacijski sustav ažurnim, kao i baze virusa i zlonamjernih programa.



Slika 2. Životni ciklus ranjivosti

3. Tržište *zero day* ranjivosti

Crno tržište programima koji zloupotrebljavaju sigurnosne propuste u računalnim programima i operacijskim sustavima prisutno je već duže vrijeme. U početcima crnog tržišta zloćudnim programima napadači su trgovali programima uglavnom zbog prestiža u hakerskim krugovima. Znanstvenici koji su se bavili računalnom sigurnošću i koji su otkrili ranjivost u većini slučajeva su pokazali odgovornost i sigurnosne propuste prijavili proizvođaču. Dovoljno je bilo da dobiju zahvalnost i priznanje proizvođača kada je ranjivost bila objavljena u sigurnosnoj preporuci. U posljednjih nekoliko godina tržište *zero day* ranjivostima, pogotovo onima za koje još uvijek ne postoji zakrpa, postalo je aktualno jer se trgovina više ne obavlja samo u hakerskim krugovima, već se može i legalno prodati tvrtkama koje se bave računalnom sigurnosti.

Crno tržište *zero day* ranjivosti i koncept prodaje i kupnje takvih ranjivosti kao u običnom dućanu postepeno se razvijao tokom nekoliko proteklih godina. Još 2005. godine, ponuda za prodaju *zero day* ranjivosti u programskom paketu Microsoft Office Excel postavljena je na Ebay, potičući sve koji se bave otkrivanjem takvih ranjivosti da traže naknadu za svoje istraživanje. Nedugo zatim počelo se stvarati tržište *zero day* ranjivostima na kojemu je svatko pokušavao postići što bolju zaradu uveličavanjem svojih otkrića. U prosincu 2005. godine prvi javno objavljen slučaj trgovine *zero day* ranjivostima na crnom tržištu bila je WMF (eng. Windows Metafile) ranjivost [27] koja je prodana za 4000 američkih dolara.

Nakon toga su autori tada popularnog programskog paketa za iskorištavanje ranjivosti WebAttacker DIY web exploitation kit počeli provoditi istraživanje potencijala tržišta *zero day* ranjivostima. U anketi su pitali posjetitelje svojih web stranica koliko su spremni platiti za podatke o *zero day* ranjivosti. Rezultati su ukazali da od 155 glasova, 40% potencijalnih kupaca je bilo voljno platiti između 100 i 300 američkih dolara za ranjivost uz to da bi 14.19% njih napisali vlastiti programski kod za pokretanje napada i 17% potencijalnih kupaca koji bi htjeli nabaviti takav kod besplatno.

Nije bilo potrebno dugo da se model crnog tržišta materijalizira u obliku web portala naziva International Exploits Shop, jednog od prvih koji je nudio programski paket za zlouporabu sigurnosnih propusta. Programski paket je sadržavao nekoliko *zero day* ranjivosti. Iako je dućan brzo nestao (propao), koncept prodaje *zero day* ranjivosti na crnom tržištu je opstao.

Postoji nekoliko tvrtki za koje je opće poznato da plaćaju istraživače za pronalazak *zero day* ranjivosti . Na primjer, program Zero Day Initiative [1], kojeg vodi TippingPoint, podružnica tvrtke 3Com ima 532 registriranih sigurnosnih istraživača. 2006. godine kupili su 82 ranjivosti od sigurnosnih istraživača i javno otkrili njih 57. Isto tako, tvrtka iDefense [2] ima velik broj sudionika i objavila je mnogo sigurnosnih preporuka. Dok spomenute tvrtke otvoreno plaćaju istraživače za njihova otkrića, njihov primarni posao nije kupnja i prodaja ranjivosti te oni imaju najmanji poticaj nuditi velike iznose za pojedinu ranjivost. Neke tvrtke, kao što su Argeniss [4],GLEG [5] i IMMUNITY [6] prodaju alate i pakete koje sadrže *zero day* ranjivosti ,dok druge, kao što je tvrtka Netragard SNOsoft [7], posreduju u poslovima između istraživača i vladinih agencija. Isto tako, ilegalno tržište za takve ekskluzivne alate postalo je ekonomski isplativo kada su kriminalci postali zainteresirani za iskorištavanje *zero day* ranjivosti za nezakonite radnje.

Stručnjak u računalnoj sigurnosti poznaje mnogo načina za otkrivanje ranjivosti u popularnim aplikacijama i operacijskim sustavima. Istraživač može prijaviti ranjivost proizvođaču ili jednostavno javno objaviti ranjivost

bez obavještavanja proizvođača zbog toga da poboljša svoju reputaciju ili obogati svoj životopis. Osim toga, ukoliko to želi, pojedinac koji je otkrio ranjivost, može prodati informacije i na crnom tržištu, odnosno prodati ih ilegalno. Na kraju, moguće je pokušati legalno prodati otkrivenu ranjivost vladinoj agenciji, proizvođačima komercijalnih alata za zaštitu računala, tvrtkama koje se bave penetracijskim ispitivanjem programa i sl.

3.1. Prepreke u prodaji zero day ranjivosti

Zbog prirode informacija o sigurnosnim propustima pa tako i *zero day* ranjivostima te programima za njihovu zlouporabu, postoji mnogo prepreka s kojima se konvencionalni poslovi i usluge ne suočavaju. Podaci o ranjivosti su vremenski osjetljiva roba te njihova vrijednost može skočiti s ekstremno visoke na nulu u jednom trenutku. To se događa zbog toga što je informacija vrijedna sve dok nije opće poznata. Čim je ranjivost objavljena, izdaje se zakrpa i podaci o ranjivosti postaju bezvrijedni. Osim toga, postoje i drugi faktori koji mogu utjecati na smanjenje cijene informacija, kao što je uvođenje nove tehnologije. Na primjer, binarna datoteka pisana u programskom jeziku C++ može se prevesti sa zastavicom /GS, što znači da će se tokom prevođenja obavljati sigurnosna provjera međuspremnika. Na taj se način može spriječiti ranjivost prepisivanja međuspremnika koju napadač može iskoristiti za pokretanje zloćudnog programskog koda. Također, korisnik na računalu može imati postavljen operacijski sustav Linux s opcijom SELinux (eng. Security-Enhanced Linux), koja pruža mehanizan kontrole pristupa i postavljanje sigurnosne politike. Kod primjene zakrpa za ranjivi program, može se dogoditi da primjenjena zakrpa promijeni neke datoteke vezane uz neku drugu ranjivost te na taj način neposredno zakrpa i taj sigurnosni propust. Sve spomenuto je izvan kontrole osobe koja je otkrila ranjivost. Nikada nije poznato kada će proizvođač ili netko drugi otkriti istu ranjivost i objaviti informacije o njoj. Prema tome, onaj tko je otkrio i želi prodati ranjivost treba to učiniti vrlo brzo ukoliko ne želi izgubiti tisuće dolara čekajući pravi trenutak za prodaju. Kada se žele prodati informacije o *zero day* ranjivosti, potrebno je brzo pronaći kupca, dogovoriti cijenu i obaviti prodaju. Na trenutnom tržištu to je vrlo teško izvedivo zbog toga što nema fiksnih cijena nijavno dostupnih podataka o cijenama ranjivosti za pojedine aplikacije na različitim platformama. Vrijednost ranjivosti ovisi o mnogo faktora koje je teško izmjeriti. Neki od faktora su:

- raširenost upotrebe aplikacije koja sadrži ranjivost,
- dolazi li aplikacija zajedno s operacijskim sustavom,
- pokreće li se aplikacija zajedno s operacijskim sustavom,
- je li potrebna autentikacija za zlouporabu aplikacije,
- koliko dobro pretpostavljene postavke vatrozida (eng. *firewall*) ograničavaju pristup aplikacijama,
- koje su inačice operacijskog sustava i/ili aplikacija ranjive,
- nalazi li se ranjivost na klijentu ili poslužitelju,
- je li potrebna interakcija s korisnikom za zlouporabu,
- koliko je teško pronaći ranjivost,
- koliko je ljudi upoznato s ranjivosti,
- je li moguće upotrijebiti isti zlonamjerni program na različite inačice ranjivosti.

Različita istraživanja tržišta otkrivaju neke primjere i naznake vrijednosti različitih ranjivosti i/ili programa za njihovu zlouporabu. No, to nije dovoljno za određivanje pravedne cijene između kupca i prodavača. Sljedeća tablica prikazuje procijenjene vrijednosti različitih ranjivosti i zlonamjernog koda za njihovo iskorištavanje.

Ranjivost/Zlonamjerni program	Cijena (u američkim dolarima)	Izvor podataka
Neki zloćudni programi	200 000 – 250 000 Preko 100 000	Vladin predstavnik Predstavnik istraživačke skupine SNOsoft
Ranjivost operacijskog sustava Vista	50 000	Raimund Genes, Trend Micro [8]
Zloćudni programski paket (sa svime potrebnim za uspješnu zlouporabu ranjivosti)	20 000 – 30 000	David Maynor, SecureWorks [9]
ZDI (eng. Zero Day Initiative), iDefense kupnja	2 000 – 10 000	David Maynor, SecureWorks [9]
WMF ranjivosti	4 000	Alexander Gostev, Kaspersky [10]
Microsoft Excel	Oko 1 200	Ebay aukcija [11][12]
Mozilla	500	Mozilla bug bounty program [13]
Program za ubacivanje zlonamjernog koda na udaljeno računalo	120	ZDNet [14]
Program za ubacivanje datoteka na zahtjev	100	ZDNet [14]
SQL injection	70	ZDNet [14]
XSS ranjivost	10 - 40	ZDNet[14]

Tablica 1. Primjer cijena ranjivosti

Uz velik raspon cijena, ako istraživač otkrije sigurnosni problem u programu Internet Explorer, postavlja se pitanje koju bi cijenu trebao postaviti. Cijene u tablici upućuju da je poštena cijena između 5000 i 250000 američkih dolara. To je još uvijek velik raspon i nema ispravnog načina određivanja cijene prikladne vrijednosti takve ranjivosti.

3.2. Pronalazak kupaca i prodavača

Kada pojedinac otkrije ranjivost i želi je prodati, on se ne može obratiti nekom središtu za pronalazak kupaca, već je prisiljen zvati svoje kontakte i upotrijebiti veze koje ima ili pokušati prodati nekim tvrtkama koje bi mogle biti zainteresirane. Spomenuti pristup nije praktičan i prati ga mnogo poteškoća. Ponekad je teško točno opisati ranjivost bez potrebe da se ranjivost učini lako uočljivom. Osim toga, spomenuti proces traženja kupca zahtjeva mnogo vremena. Svako kašnjenje u prodaji može učiniti podatke bezvrijednima. Nije uobičajeno da tvrtke javno objavljuju da kupuju informacije o ranjivostima, izuzev tvrtki iDefense, Tippingpoint i Netragard. Uz to proizvođači obično ne kupuju informacije o ranjivostima u njihovim programskim paketima. Ukoliko bi proizvođači nudili nagradu za pronalazak ranjivosti, možda bi poboljšali sigurnost svojih proizvoda, kao što je to učinila tvrtka Netscape 1995. godine nudivši 1000 američkih dolara nagrade onime tko otkrije sigurnosni propust u njihovim proizvodima.

3.3. Dokazivanje vrijednosti informacija

Jedan od najtežih problema s kojima se prodavači *zero day* ranjivosti susreću je dokazivanje da informacije koje želi prodati nisu izmišljene i lažne. Jedini način da se dokaže ispravnost podataka je njihovo otkrivanje u nekom obliku. Očito otkrivanje informacija nije poželjno jer prodavač može ostati bez dogovorene naknade za intelektualno vlasništvo.

Kako bi prodavač dokazao da je otkriće upravo njegovo, on može stvoriti kriptografski sažetak [15] podataka o ranjivosti i objaviti ga na neko javno mjesto. Kriptografski sažeci se obično koriste u digitalnim potpisima. Na taj način moguće je utvrditi vlasništvo. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije neovlašteno izmijenjen. Postupak digitalnog potpisivanja dokumenta sastoji se od izračunavanja sažetka poruke (izvornog teksta) i kriptiranja sažetka poruke. Kriptirani sažetak čini svojevrstan potpis, tj. digitalni potpis. Detaljan oblik ovog digitalnog potpisa ovisi o

sadržaju poruke te je za svaku poruku drugačiji. Također postoje komercijalne usluge koje bilježe podatke o sažecima kako bi se mogao provjeriti datum kada je podatak javno objavljen [3]. Spomenute radnje štite prodavača od kupca koji želi preuzeti zasluge za otkriće ranjivosti bez plaćanja naknade. Međutim, upotrebom kriptografskog sažetka, prodavač samo može dokazati da je imao saznanje o ranjivosti prije kupca. Još uvijek kupac može prevariti prodavača npr. lažiranjem datuma stvaranja sažetka i preuzimanjem identiteta prodavača.

Još jedan problem za prodavača je kako dokazati da upravo on posjeduje informacije o određenoj ranjivosti. Vrlo je teško dokazati potencijalnom kupcu da prodavač ima saznanje o određenoj ranjivosti bez odavanja tih informacija. Sljedeći postupak je moguće rješenje spomenutog problema:

- Kupac i prodavač dogovore sastanak na fizičkoj lokaciji.
- Kupac donese fizički medij, kao što je CD, DVD i sl. sa snimljenim operacijskim sustavom i potrebnim aplikacijama.
- Prodavač donese demonstraciju zlonamjernog programa koji iskorištava ranjivost i potrebno sklopovlje za demonstraciju.
- Pod nadzorom prodavača kupac instalira i nadogradi operacijski sustav i sve potrebne aplikacije upotrebom svojeg medija.
- Prodavač demonstrira zlouporabu ranjivosti.
- Prodavač zadrži računalo nakon demonstracije.

Iako metoda rješava problem dokazivanja da prodavač posjeduje korisne informacije bez njihovog odavanja, ona sadrži i mnogo nedostataka. Neki od njih su:

- metoda oduzima mnogo vremena,
- skupa je,
- kupac i prodavač trebaju stupiti u fizički kontakt,
- prodavač može prevariti kupca.

Ukoliko prodavač i kupac nisu u mogućnosti stupiti u fizički kontakt, prodavač se može odlučiti na „uzajamno uništenje“. U slučaju kada prodavač vjeruje da je kupac preuzeo podatke o ranjivosti bez plaćanja, on ih može javno objaviti. Takva objava učinit će ukradene podatke o ranjivosti bezvrijednima. Očito ovakav scenarij ne pogoduje ni prodavaču ni kupcu. Sama prijetnja objavom trebala bi biti dostatna da kupac plati informacije.

Kako bi se riješio problem prodaje i kupnje na crnom tržištu *zero day* ranjivostima objavljeni su mnogi znanstveni radovi. U jednom od njih predlaže se pet različitih tipova tržišta za prodaju podataka o ranjivostima [16]:

- nagrade za otkrivenu ranjivost (eng. *bug challenges*),
- aukcije ranjivosti,
- trgovina putem posrednika,
- trgovina izvedenim informacijama o ranjivosti (eng. *exploit derivatives*) i
- *cyber*-osiguranje.

Od navedenih tipova trgovine, prva dva mogu koristiti pojedinci koji se bave istraživanjem računalne sigurnosti, ali takvu trgovinu trebaju započeti prodavači. Raspisivanje nagrade za otkrivanje ranjivosti jedan je od najstarijih oblika tržišta ranjivostima. Dakle, proizvođač unaprijed nudi nagradu ukoliko netko pronađe ranjivost u njegovom programu. Najpoznatiji primjer takvog tipa tržišta je nagrada koju je ponudio Donald E. Knuth za otkrivanje sigurnosnog propusta u programu TeX za pisanje znanstvenih dokumenata. Nagrada je u početku iznosila 1.28 američkih dolara, a rasla je eksponencijalno s godinama upotrebe programa.

Trgovina podacima o ranjivostima putem posrednika uključuje neovisne organizacije poput iDefense i Tipping Point koje nude novčanu naknadu za izvještaje o novim ranjivostima. One dalje obavještavaju i prodaju dobivene informacije sigurnosnim tvrtkama i proizvođačima. U tu skupinu može se uvrstiti i CERT, iako se radi o neprofitabilnoj organizaciji.

Trgovina izvedenim podacima o ranjivostima prevodi mehanizam opcija iz financija u primjenu u računalnoj sigurnosti. Opcije su vrijednosni papiri izvedeni iz prometa vrijednosnih papira koji daju pravo kupnje ili prodaje vezane imovine po izvršnoj cijeni kroz određeno vrijeme ili na određeni dan. Umjesto trgovine informacijama o ranjivostima, tržišni se mehanizam izgrađuje oko ugovora koji isplaćuju predodređenu sumu u slučaju sigurnosnog događaja (npr. otkriće ranjivosti, zlouporaba ranjivosti, pojava zloćudnog programa i slično).

Cyber-osiguranje funkcionira na isti način kao i zdravstveno osiguranje za osobe. To je jedan od najstarijih tipova tržišta. Korisnici zahtjevaju osiguranje od financijskog gubitka podataka koji se može dogoditi za vrijeme napada na njihovo računalo. Osiguravajuće tvrtke prodaju takvo osiguranje nakon pregleda i ispitivanja programa i računala koje osiguravaju. Premija se određuje na temelju pojedinačne procjene rizika korisničkog računala ovisno o tome koji su programi postavljeni te kakvi sigurnosni mehanizmi postoje.

Trgovina preko posrednika i *cyber*-osiguranje ne nude neposredni poticaj prodavaču *zero day* ranjivosti za ostvarenje profita. Teško je steći prednost i unovčiti informacije o ranjivosti na spomenuta dva tržišta. Trgovina izvedenim informacijama o ranjivosti pruža način da prodavač ostvari profit upotrebom podataka o *zero day* ranjivostima. Takav tip tržišta uključuje mehanizam koji se izgrađuje na ugovorima koji isplaćuju određenu svotu u slučaju sigurnosnog događaja. Različite stranke slobodno trguju ugovorima na temelju toga smatraju li da će se takav događaj dogoditi ili ne. Pojedinac ima koristi od takvog sustava jer mu dozvoljava kupnju velikog broja ugovora koji se isplaćuju ukoliko je otkrivena ranjivost. U tom slučaju prodavač može objaviti ranjivost i imati profit od informacija o ranjivosti.

3.4. Primjer uspješne prodaje

U nastavku je dan primjer uspješne prodaje provedene u ljeto 2005. godine. Ranjivost koja je otkrivena vezana je uz pozadinski proces uobičajen na operacijskim sustavima Linux. Prodavač je imao veze u NSA (eng. National Security Agency) agenciji i vladi te u tvrtki Transversal Technologies koje je mogao kontaktirati u vezi prodaje. Iako je imao nekoliko osobnih veza i kontakata, smatrao je da će imati veće šanse na vrijeme pronaći kupca ako kontaktira tvrtku Transversal Technologies, koja je imala mnogo više kontakata i veza u vladi i drugim agencijama. Za 10% provizije tvrtka se složila da pokuša naći kupca te je ponudila informacije o ranjivosti mnogim drugim agencijama. Prodavač je dobio ponudu od 10 000 američkih dolara od jedne organizacije i tražio 80 000 dolara od jedne druge organizacije koja je također bila voljna kupiti podatke. Druga organizacija se složila s ponuđenom svotom vrlo brzo, što je značilo da prodavač vjerojatno nije tražio dovoljno novaca. Nakon toga prodavač je predao svoje intelektualno vlasništvo tvrtki da utvrde može li se ranjivost iskoristiti za napad na Linux platformu. Nakon dva tjedna, prodavaču još uvijek nisu platili te se odlučio staviti kriptografski sažetak u lažnu poruku elektroničke pošte koju je poslao na mailing listu Full-Disclosure za potpunu objavu svih informacija o ranjivosti [17]. Nekoliko dana kasnije ponovno je stupio u pregovore s organizacijom i dogovoren je iznos od 50 000 dolara bez obzira na učinkovitost napada. Nakon tjedan dana prodavač je dobio ček od spomenute organizacije. Sljedeća tablica prikazuje vremensku liniju prodaje.

Datum	Radnja
Ljeto 2005	Ranjivost otkrivena
Studeni 2005	Predano na predpublikaciju u NSA
Srpanj 2006	Odobreno za puštanje u predpublikacijsku ocjenu
Srpanj 2006	Ponuđeno vladinim agencijama preko tvrtke Transversal Technologies
Kolovoz 2006	Verbalni dogovor oko svote od 80 000 dolara
Kolovoz 2006	Informacije o ranjivosti predane na ocjenu (u ovom trenutku kupac je u prednosti)
Kolovoz 2006	Kriptografski sažetak ranjivosti objavljen
Kolovoz 2006	Dogovorena manja svota za ranjivost
Rujan 2006	Kupac je platio prodavaču

Tablica 2. Vremenska linija uspješne prodaje

3.5. Primjer neuspješne prodaje

Primjer neuspješne prodaje ranjivosti otkrivene u siječnju 2007. godine u programskim paketima Microsoft Powerpoint, inačica XP i 2003 dan je u nastavku. Prodavač je kao i u prvom primjeru kontaktirao svoje veze, ali nije znao kako da procjeni vrijednost spomenute ranjivosti. Prodavač je probao procijeniti vrijednost na temelju jedne druge ranjivosti u programu Excel koja je procijenjena na oko 1200 dolara te na temelju sličnih ponuda tvrtki iDefense i Tipping Point (između 1000 i 3000 dolara). Pogađao je da bi informacije o ranjivosti mogle biti vrijedne oko 50 000 dolara vladi ili 20 000 dolara nekoj drugoj tvrtki. U međuvremenu, dok je pokušavao saznati vrijednost informacija o ranjivosti, Microsoft je izdao zakrpu koja uklanja sigurnosni problem. Vremenska linija radnji dana je u tablici 3.

Datum	Radnja
Siječanj 2007	Ranjivost otkrivena
Siječanj 2007	Ponuđeno vladinim agencijama preko tvrtke Transversal Technologies
Siječanj 2007	Microsoft je otkrio ranjivost
Veljača 2007	Informacije su ponuđene tvrtkama koje se bave računalnom sigurnosti
Veljača 2007	Microsoft je izdao zakrpu KB929064 koja uklanja ranjivost

Tablica 3. Vremenska linija neuspješne prodaje

4. Etički aspekt prodaje i objave ranjivosti

Tržište *zero day* ranjivostima je kontroverzna tema koja se tiče svih proizvođača programskih paketa. Nije tajna da proizvođači potiču istraživače na odgovorno prijavljivanje otkrivenih sigurnosnih propusta izravno njima. Ukoliko se sigurnosni propust prijavi izravno proizvođaču, moguće je ukloniti ga i izdati zakrpu prije nego što se vijest o ranjivosti proširi u javnost. Nije iznenađujuće da mnogo istraživača preferira druge načine objave otkrivene ranjivosti, kao što je prodaja na crnom tržištu ili traženje priznanja za otkrivanje ranjivosti. Nekoliko tvrtki, kao što su iDefense i TippingPoint nude kompenzaciju za informacije o ranjivostima. Njihov je interes upotrijebiti kupljene podatke za zaštitu baze korisnika te upozoravanje proizvođača programskog paketa u kojem je ranjivost otkrivena. Uvijek postoje i oni koji odabiru prodati podatke o otkrivenim ranjivostima na crnom tržištu.

Uz mnogo načina na koje se mogu objaviti i iskoristiti podaci o ranjivostima u programskim paketima, tržište *zero day* ranjivosti svakodnevno raste. Vijesti o novoj *zero day* ranjivosti u *cyber* svijetu znače mogućnost velikog profita za one koji ih otkriju. Gledano s etičkog aspekta, ispravno i odgovorno je otkrivenu ranjivost prijaviti proizvođaču, ali, ipak, isplativije je prodati takvu informaciju na tržištu *zero day* ranjivosti. Ta moralna dvojba javlja se kod svakog pojedinca koji otkrije takvu ranjivost.

4.1. Potpuno razotkrivanje i objava podataka

Potpuno razotkrivanje podataka o ranjivosti (eng. *full disclosure*) u području računalne sigurnosti znači javno otkrivanje svih detalja sigurnosnog problema. Spomenuta filozofija upravljanja sigurnošću suprotna je ideji sigurnosti skrivanjem podataka (eng. *security through obscurity*). Koncept potpunog razotkrivanja podataka je kontroverzan, ali nije nov (postoji još od 19. stoljeća).

Potpuno razotkrivanje uključuje objavu svih detalja otkrivene sigurnosne ranjivosti javnosti, što znači i metode otkrivanja i zlouporabe ranjivosti. Ideja iza spomenutog koncepta je da objavljivanje svih podataka o ranjivosti ima kao posljedicu brzo uklanjanje ranjivosti i objavu zakrpa koje proizvođač, na ovaj način, izradi puno prije nego da informacije nisu bile objavljene. Sigurnost programskog paketa u kojem je otkrivena ranjivost je poboljšana, jer je vremenski period u kojem napadač može izvesti napad upotrebom sigurnosnog propusta smanjen.

Potpuno razotkrivanje podataka ostvaruje se putem tzv. *mailing* listi (adresa elektroničke pošte koja se koristi za slanje poruka grupi ljudi) kao što je Full-Disclosure i sličnim sredstvima. Spomenutu *mailing* listu pojedinci koji su otkrili *zero day* ranjivost mogu koristiti za potpuno otkrivanje podataka o ranjivosti sigurnosnoj zajednici. *Mailing* lista Full-Disclosure je ključni dio infrastrukture sigurnosne zajednice jer je jedina sigurnosna lista koju ne uređuju i kojom ne upravljaju komercijalne organizacije. Njome upravlja John Cartwright koji je zajedno sa Len Roseom 2002. godine pokrenuo listu kao alternativu cenzuriranim listama.

Neki vjeruju da je, ukoliko već ne postoje javno objavljene sigurnosne ranjivosti za neki programski paket, potrebno pričekati s potpunim razotkrivanjem podataka o ranjivosti i spomenute podatke prvo prijaviti proizvođaču programskog paketa te tvrtkama koje se bave računalnom sigurnosti. Ideja se katkad naziva „odgovorno razotkrivanje“. Ako je proizvođač obaviješten o postojanju ranjivosti u njegovom programskom paketu i ne ukloni ju u razumnom vremenskom razdoblju, potrebno je obaviti potpuno razotkrivanje javnosti. Postoje različita mišljenja o tome koliko dugo je razumno vrijeme, obično se smatra da je to razdoblje od 14 do 30 dana (iako je katkad mnogo kraće).

Prednost potpune objave svih podataka o ranjivosti je da će proizvođači doći brže do potrebnih podataka te ukloniti problem i objaviti potrebne zakrpe.

5. Poznate ranjivosti i napadi

Vrlo je vjerojatno da svaki složeni računalni program sadrži programske pogreške i previde koje zlonamjerni korisnici mogu iskoristiti za pokretanje napada. Neki programski paketi su poznati po tome da imaju mnogo *zero day* ranjivosti. Obično se najviše *zero day* ranjivosti otkriva u popularnim i raširenim programskim paketima i operacijskim sustavima, kao što su operacijski sustav Windows, program Microsoft Office ili različiti web preglednici. U siječnju 2007. godine, u programskom paketu Microsoft Word otkrivene su četiri *zero day* ranjivosti, od kojih su dvije bile barem mjesec dana javno poznate. Dvije su ranjivosti utjecale na tada najnoviju inačicu programskog paketa. Za zlouporabu jedne od njih nije uopće bilo potrebno pokrenuti Word. Podijeljena su mišljenja oko sigurnosti programa otvorenog koda i programa zaštićenih autorskim pravima.

5.1. Jesu li programi otvorenog koda sigurniji?

Oko pitanja jesu li programi otvorenog koda sigurniji od onih zaštićenih autorskim pravima vodi se velika rasprava. Programski paketi otvorenog koda su, na primjer, web preglednici Firefox i Konqueror, a zatvorenog koda su Internet Explorer i Opera. Pitanje postoji već dugo i sigurnosni stručnjaci kažu da ne postoji jedinstven odgovor.

Jedno je mišljenje da su web preglednici otvorenog koda sigurniji od napada. Dva su glavna razloga tome:

- otvoreni kod je dostupan svima, što znači da će se ranjivosti brže otkriti, ali i brže ukloniti,
- web preglednici otvorenog koda imaju manji broj korisnika pa napadači imaju manje poticaja iskorištavati njihove ranjivosti kako bi ostvarili zaradu.

Drugo mišljenje je da su programski paketi zatvorenog koda bolje zaštićeni jer njihov kod nije svima dostupan i ta činjenica ne potiče korisnike da mijenjaju programski kod.

Ranjivosti svih web preglednika su obično vrlo slične. Napadači koji zloupotrebljavaju ranjivosti srodnih programa obično iskorištavaju iste slabosti programa Internet Explorer, Opera i preglednika otvorenog koda.

U ljeti 2007. godine otkrivene su dvije *zero day* ranjivosti vezane uz Internet Explorer. Spomenute su ranjivosti ugrozile ne samo Internet Explorer, već i preglednik Firefox ukoliko su oba programa bila istovremeno instalirana na računalu. Dvije su pogreške bile vezane uz konflikt s programom Internet Explorer. Napadači su mogli iskoristiti pogreške za pokretanje proizvoljnog programskog koda. Kako bi napad bio uspješan, korisnik je trebao posjetiti zlonamjernu web stranicu koja je u svojoj adresi sadržavala posebno oblikovanu URI (eng. *Uniform Resource Identifier*) oznaku. Oznaka je trebala sadržavati znak postotka i trebala je završavati nastavkom .bat ili .cmd. Napadači obično koriste ranjivosti kako bi preglednike natjerali na pogrešno razumijevanje zahtijevane akcije.

Svi su web preglednici ranjivi na napade ovisno o stanju računala na kojem se pokreću i interakciji s ostalim programima instaliranim na tom računalu. Međutim, stručnjaci tvrde da su web preglednici otvorenog koda sigurniji, ako zbog ničeg drugog, onda zbog toga što je moguće brže ukloniti sigurnosne propuste te zbog malog broja korisnika.

Jedan od najjačih argumenata u korist programa otvorenog programskog koda jest činjenca da mnogo ljudi ima pristup njihovom kodu što u konačnici rezultira kodom koji sadrži malo ili uopće nema ranjivosti..

5.2. Windows 7 zero day ranjivost

U studenom 2009. godine tvrtka Microsoft potvrdila je postojanje prve otkrivene *zero day* ranjivosti u operacijskom sustavu Windows 7 RC (eng. *Release Client*). U sigurnosnoj preporuci tvrtka Microsoft priznaje da postoji sigurnosni propust u SMB (eng. Server Message Block) komponenti. SMB je mrežni protokol u aplikacijskom sloju koji se koristi za raspodjelu mrežnih resursa na operacijskom sustavu Windows. *Zero day* ranjivost otkrio je kanadski stručnjak Laurent Gaffie. Objavio je sigurnosni problem i napadački programski kod kao dokaz koncepta na *mailing* listi Full-Disclosure i svom blogu. Gaffie tvrdi da ranjivost može uzrokovati ulazak računala u beskonačnu petlju te time uskratiti pristup uslugama. Također, napomenuo je da se ranjivost može iskoristiti putem Internet Explorera te napadaču omogućuje zaobilaženje zaštite vatrozidom. Za razliku od ozbiljnijih sigurnosnih propusta, propust u SMB komponenti napadači ne mogu iskoristiti za preuzimanje kontrole nad računalom korisnika. Kako bi se zaštitili od napada korisnicima je Microsoft savjetovao blokiranje TCP (eng. Transmission Control Protocol) priključaka 139 i 445. Ranjivost je uklonjena u finalnoj inačici operacijskog sustava Windows 7.

Slika 3. Windows 7 logo

6. Metode zaštite

Zero day ranjivosti su specifična vrsta sigurnosnih propusta pa je običnom korisniku osobnog računala vrlo teško zaštititi se od napada. Prema tome, zdrav razum i dobre navike upotrebe računala su osnova sprečavanja zlouporabe *zero day* ranjivosti. Ažurne baze antivirusnih definicija i drugih programa koji otkrivaju zlonamjerni programski kod neće pružiti zaštitu od napada koji iskorištava *zero day* ranjivost. Preporuča se ispravno postavljanje vatrozida koji kao takav može spriječiti pokretanje zlonamjernog programskog koda. Također, dobro je izbjegavati programske pakete za koje je poznato da nisu sigurni te da se u njima često javljaju sigurnosni propusti. Kada proizvođač objavi sigurnosnu zakrpu potrebno ju je što prije primijeniti kako bi korisnik zaštitio svoje računalo.

Napadači se često služe socijalnim inženjeringom kako bi iskoristili *zero day* ranjivost i naveli korisnika da im pomogne u izvođenju napada bez znanja da to čine. Primjerice, ukoliko napadač navede korisnika na radnju koja će ugroziti njegovo računalo, kao što je posjeta zlonamjerne web stranice, korisnik bez znanja može preuzeti zlćudni programski kod koji iskorištava *zero day* ranjivost.

U listopadu 2009. godine, istraživači sa MIT-a (eng. Massachusetts Institute of Technology) razvili su programski paket koji sam stvara zakrpe za programe u kojima otkrije ranjivost. Program se zove ClearView i osmišljen je tako da prati uobičajeno ponašanje programa na računalu i prema tome postavlja pravila po kojima će utvrditi je li potrebno stvoriti zakrpu. Program traži određene tipove programerskih pogrešaka koje napadači najčešće iskorištavaju za pokretanje napada. ClearView prati ponašanje određenog programa na razini strojnog koda i stvara popis pravila koja opisuju njegovo uobičajeno (normalno) ponašanje. Kada iz nekog razloga praćeni program prestane poštovati naučena pravila, ClearView smatra da je otkrio ranjivost. Tada pronalazi pravilo koje je ugroženo i stvara potencijalni skup zakrpi koje tjeraju ugroženi program da slijedi pravila koja je ClearView naučio. ClearView tada ispituje svaku zakrpu i primjenjuje onu koja je najuspješnija. ClearView može biti vrlo uspješan ukoliko je pokrenut na više računala s istim programima jer se zakrpa može primijeniti na svim računalima. ClearView zaobilazi izvorni kod i primjenjuje zakrpu na binarnoj razini, odnosno na razini strojnog koda. Program je ispitivan na skupini računala na kojima je bio pokrenut web preglednik Firefox. Na tim računalima pokrenut je napad upotrebom ranjivosti u tom pregledniku. U ispitivanju je korišteno deset metoda napada i ClearView je bio uspješan u sprečavanju svih deset. U prosjeku je bilo potrebno pet minuta prije nego što je primjenjena uspješna zakrpa od početka prvog napada.

Slika 4. Za zaštitu je dobro slijediti dobre navike računalne sigurnosti

6.1. Sigurnost skrivanjem podataka

Sigurnost skrivanjem podataka (eng. *security by obscurity*) je koncept čiji je cilj koristiti tajnost (dizajna, korištenja i sl.) kako bi se postigla određena razina zaštite od napada. Sustav koji se oslanja na spomenuti način zaštite također može sadržavati sigurnosne propuste, ali proizvođači programskih paketa vjeruju da ranjivosti nisu poznate i da je malo vjerojatno da će ih bilo tko otkriti. Napadačev je prvi korak sakupljanje informacija, što može biti teško ukoliko se proizvođač služi skrivanjem podataka o sigurnosnim mehanizmima koje koristi.

Oslanjanje isključivo na sigurnost skrivanjem podataka nije dobro ako je to jedina metoda zaštite. Međutim ukoliko je dio mjera sigurnosti koje primjenjuje proizvođač, tada može biti razumna taktika kao dio strategije zaštite od napada. Metoda može pružiti dovoljno vremena proizvođaču da ukloni ranjivost prije nego ju napadači otkriju. Cilj je smanjiti rizik zlouporabe ranjivosti dok se ona ne ukloni.

Sigurnost skrivanjem podataka može se koristiti i za stvaranje rizika koji će pomoći u detekciji potencijalnih napadača. Kao primjer se može uzeti računalna mreža za koju se smatra da sadrži ranjivost za koju proizvođač zna. Ukoliko napadač ne poznaje dizajn programa, on mora razmotriti hoće li iskoristiti ranjivost ili ne. Ako je sustav postavljen tako da, primjerice, reagira na pokušaje iskorištavanja ranjivosti zaključavanjem sustava, obavještavanjem administratora ili isključivanjem napadača iz mreže, administrator će prepoznati da je sustav napadnut.

Bit principa sigurnosti skrivanjem podataka je povećavanje rizika za napadača i dobivanje na vremenu. Napadač treba odlučiti isplati li mu se napadati sustav koji ne poznaje i možda upasti u zamku ili odustati od napada.

6.2. ZERT

ZERT (eng. Zero Day Emergency Response Team) je skupina inženjera s opsežnim iskustvom u reverznom inženjeringu, razvoju programskih paketa i sklopovlja. ZERT ima veze u industriji te u skupinama za odgovor na sigurnosne incidente (CERT). Skupina surađuje s nekoliko sigurnosnih organizacija i povezana je s antivirusnim zajednicama, ali nije povezana izravno s proizvođačima programskih paketa.

Članovi skupine ZERT rade tako da objavljuju zakrpu bez znanja proizvođača kada doznaju za *zero day* ranjivost za koju smatraju da ju napadači mogu zlonamjerno iskoristiti. Cilj skupine ZERT nije pronalaženje ranjivosti u programskim paketima već uklanjanje opasnih sigurnosnih propusta koje zlonamjerni korisnici mogu iskoristiti za ugrožavanje računalnih sustava.

Uvijek je dobro čekati da proizvođač izda zakrpu i primijeniti je što je prije moguće, međutim postoje slučajevi kada skupina, kao što je ZERT može prije proizvođača stvoriti zakrpu. U nedostatku zakrpa proizvođača, preporuča se primjena zakrpa koje je izdao ZERT.

6.2.1. Odgovor na incident

Nakon što je otkrivena *zero day* ranjivost, skupina se podijeli na sljedeći način kako bi stvorila zakrpu koja uklanja ranjivost:

- Stvara se zakrpa koja uklanja otkrivenu sigurnosnu ranjivost, kao i druge ranjivosti otkrivene u postupku stvaranja zakrpe.
- Testira se zakrpa kako bi se provjerila njezina pouzdanost i stabilnost sustava na koji se primjenjuje.
- Testira se zakrpa u svrhu provjere da ne smanjuje funkcionalnost sustava na koji se primjenjuje.
- Stvara se dokumentacija koja uključuje:
    - objašnjenje da zakrpu nije stvorio proizvođač nego nezavisna skupina,
    - bilješke o smanjenoj funkcionalnosti programa nakon primjene zakrpe, ukoliko postoji,
    - opis okružja u kojima je zakrpa provjerena i
    - upute za instalaciju i uklanjanje zakrpe.
- Objavljuje se izvorni programski kod zakrpe.
- Ažurira se zakrpa ukoliko se daljnjim ispitivanjem otkrije da uzrokuje nestabilnost ili ona sama sadrži ranjivost.
- Preporuča se primjena zakrpa proizvođača kada ih on objavi.

6.2.2. Programi

ZERT je izdao programsku podršku za stvaranje zakrpa i uklanjanje *zero day* ranjivosti - ZProtector. Program je namijenjen operacijskim sustavima Windows, inačica od 95 do 2003. Program nije potrebno ukloniti nakon što zakrpa proizvođača postane dostupna.

7. *Zero day* ranjivosti u budućnosti

Nemoguće je stvoriti složeni programski paket koji ne sadrži određeni broj ranjivosti. *Zero day* ranjivosti još će dugo biti aktualne (može se čak reći da će uvijek biti prisutne) i informacije o njima prodavat će se na tržištu *zero day* ranjivostima dok god postoje ljudi i organizacije zainteresirani za kupnju takvih podataka. Proizvođači čine sve da smanje broj ranjivosti u programima koje postavljaju na tržište te poboljšaju njihovu sigurnost. *Zero day* napadi mijenjat će se u skladu sa zaštitama koje će proizvođači postavljati. To je, u biti, utrka između proizvođača i napadača. U konačnici korisnik je taj koji treba biti na oprezu i slijediti preporučene korake zaštite.

Iz perspektive ljudi koji otkrivaju *zero day* ranjivosti, prodaja informacija o ranjivostima je riskantan posao. Zbog tajne prirode tržišta teško je pronaći kupce, odrediti cijenu podataka, dokazati vrijednost ranjivosti te razmijeniti ih za novčanu naknadu. Uz to, ranjivost može biti uklonjena prije prodaje podataka o njoj što je čini bezvrijednom. Postoje neka rješenja koja olakšavaju prodaju, ali ostvarenje boljih načina trgovine *zero day* ranjivostima tek treba otkriti i primijeniti u budućnosti.

8. Zaključak

Zero day ranjivosti opasne su sve dok proizvođač ili organizacija poput ZERT skupine ne izda sigurnosnu zakrpu koja uklanja problem. Nakon otkrića *zero day* ranjivosti napadači imaju mali vremenski okvir da iskoriste sigurnosni propust za pokretanje napada na osjetljive računalne sustave. Pojedinci koji su otkrili *zero day* ranjivost u nekom programskom paketu imaju izbor:

- potpuno razotkriti sve detalje ranjivosti isključivo proizvođaču,
- potpuno razotkriti sve detalje vezane uz ranjivost javnosti,
- prodati ranjivost na tržištu nekoj od vladinih agencija ili sigurnosnih tvrtki,
- prodati ranjivost na crnom tržištu ili
- zlouporabiti ju za svoje potrebe.

U posljednjem slučaju očito je da će osjetljivi podaci o *zero day* ranjivosti doći u ruke zlonamjernih napadača. Pred pojedincem koji je otkrio ranjivost postavlja se etičko pitanje - kako postupiti? U prva dva slučaja pojedinac neće ostvariti profit, ali će vjerojatno dobiti priznanje za otkrivanje sigurnosnog propusta.

Nakon što proizvođači doznaju da postoji ranjivost u njihovom programskom paketu, oni objavljuju sigurnosnu preporuku i po potrebi zakrpu ili obnovljenu inačicu u kojoj je sigurnosni problem uklonjen.

Ne postoji metoda koja će u potpunosti spriječiti pojavu *zero day* ranjivosti, ali je moguće umanjiti rizik napada. Postoje dvije filozofije koje se mogu koristiti:

- pisanje aplikacija otvorenog programskog koda i
- upotreba sigurnosti skrivanjem podataka o dizajnu aplikacija.

Oba pristupa imaju svoje prednosti i nedostatke. Aplikacije otvorenog koda omogućuju velikom broju ljudi uočavanje sigurnosnog problema, ali i njegovo brzo uklanjanje, dok aplikacije skrivenog dizajna ne pružaju dovoljno podataka napadačima za izvođenje uspješnog napada te ih tako odvraćaju od pokušaja. Njihove prednosti su ujedno i nedostaci. Kod aplikacija otvorenog koda, napadači mogu lakše otkriti sigurnosni propust i zloupotrijebiti ga. Ukoliko netko uspije otkriti dizajn aplikacije čiji je kod skriven, taj pojedinac ima sve informacije potrebne za otkrivanje ranjivosti i njihovo iskorištavanje. To znači da je, ako programeri nisu pazili na sigurnost koda jer su vjerovali da je program zaštićen nedostatkom podataka o njegovom dizajnu, program vrlo ranjiv i pun sigurnosnih propusta. Unatoč spomenutim mjerama obrane proizvođača, korisnici trebaju na svojoj strani primijeniti osnovne mjere zaštite. Korisnicima se svakako preporuča primjena sigurnosnih naputaka objavljenih u sigurnosnim preporukama nakon objave istih. Osim toga, ispravno postavljen vatrozid može spriječiti neke napade u kojima napadač pokreće zlonamjerni programski kod. Također moguće je koristiti sustave za sprečavanje i detekciju upada u računalo (eng. *Intrusion Detection/ Prevention System*) za zaštitu od zloćudnog mrežnog prometa.

Zero day ranjivosti će postojati dok god ne postoji mogućnost stvaranja aplikacija bez sigurnosnih propusta. Pojedinci koji otkriju *zero day* ranjivosti pokušat će unovčiti svoje otkriće i/ili će razotkriti javnosti sve detalje o otkrivenom propustu. Kako još uvijek ne postoje metode sprečavanja *zero day* ranjivosti korisnici trebaju biti na oprezu i slijediti dobre navike zaštite svojih računala kao što su redovita primijena dostupnih zakrpi osjetljivih programa, pažljivo postavljen vatrozid, edukacija i dr.

9. Reference

[1] Zero Day Initiative | 3Com | TippingPoint, a division of 3Com, http://www.zerodayinitiative.com/
[2] Vulnerability Contributor Program // iDefense Labs, http://labs.idefense.com/vcp/
[3] Surety Integrity Advantage, http://surety.com/solutions/integrityadvantage.htm
[4] Argeniss - Information Security, http://www.argeniss.com/products.html
[5] GLEG, http://www.gleg.net/products.html
[6] IMMUNITY: Knowing You're Secure , http://www.immunityinc.com/products-canvas.shtml
[7] SNOsoft Research Team, http://snosoft.blogspot.com/
[8] Hackers Selling Vista Zero-Day Exploit, eWeek, 15.12.2006, http://www.eweek.com/article2/0,1895,2073611,00.asp
[9] Bucks for Bugs, Dark Reading - Risky Business, http://www.darkreading.com/document.asp?doc_id=99518
[10] Researcher: WMF Exploit Sold Underground for $4,000, eWeek, 02.02. 2006, http://www.eweek.com/article2/0,1895,1918198,00.asp
[11] eBay Pulls Bidding for MS Excel Vulnerability, eWeek, 09.12. 2005,http://www.eweek.com/article2/0,1759,1899697,00.asp?kc=EWRSS03129TX1K0000614
[12] Researchers: Flaw auctions would improve security, SecurityFocus, 15.12. 2005, http://www.securityfocus.com/news/11364/1
[13] Mozilla Security Bug Bounty Program, mhttp://www.mozilla.org/security/bug-bounty.html
[14] Black market for zero day vulnerabilities still thriving, studeni 2008, http://blogs.zdnet.com/security/?p=2108
[15] Algoritmi za izračunavanje sažetka, CERT, rujan 2006, http://www.cert.hr/documents.php?id=257
[16] Vulnerability Markets: What is the Economic Value of a Zero-Day Exploit?, Bohme, 22 C3. 2005. Berlin, Germany, http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf
[17] Full-disclosure: Security researcher, 25.08.2006, http://archives.neohapsis.com/archives/fulldisclosure/2006-08/0653.html
[18] Zero day attack, Wikipedia, siječanj 2010, http://en.wikipedia.org/wiki/Zero_day_attack
[19] What is zero day exploit, studeni 2007, http://what-is-what.com/what_is/zero_day_exploit.html
[20] Zero day exploits, http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm
[21] Charles Miller, „The legitimate vulnerability market: the secretive world of 0-day exploit sales", 2007, http://209.85.129.132/search?q=cache:c1gZfSsTfsAJ:securityevaluators.com/files/papers/0daymarket.pdf
[22] Microsoft confirms first Windows 7 zero-day bug, studeni 2009, http://www.computerworld.com/s/article/9140858/Microsoft_confirms_first_Windows_7_zero_day_bug
[23] Zero Day Initiative, http://www.zerodayinitiative.com/
[24] Zeroday Emergency Response Team, http://isotf.org/zert/
[25] Full disclosure, Wikipedia, siječanj 2010, http://en.wikipedia.org/wiki/Full_disclosure
[26] Security through obscurity, Wikipedia, siječanj 2010, http://en.wikipedia.org/wiki/Security_through_obscurity
[27] WMF ranjivost 2005, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560
[28] ClearView program, listopad 2009, http://www.technologyreview.com/computing/23821/