



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSTDIPLOMSKE STUDIJE

- MASTER STUDIJSKI PROGRAM -
SAVREMENE INFORMACIONE TEHNOLOGIJE

Srdan Jo

**Zaštita računarskih mreža – analiza
antivirusne zaštite**

- Master rad -

Mentor:
Prof dr Mladen Veinović

Student:
Srdan Jo
Br. indeksa:
410464/2013.

Zaštita računarskih mreža – analiza antivirusne zaštite

Sažetak

U ovom radu je opisana zaštita računarskih mreža korišćenjem tehnologija kao što su Firewall, Antivirus programi, IDS i IPS sistemi, kriptografski protokoli, politike i procedure zaštite.

Ključne reči: Firewall, Antivirus programi, IDS, IPS, zaštita mreže, zaštita podataka, hakerski napadi, maliciozni programi.

Abstract

This project describes the various types of network security such as Firewall, Antivirus software, IDS and IPS systems, Cryptographic protocols, politics and procedures.

Key words: Firewall, Antivirus software, IDS, IPS, security and protection of computer networks, data security, hacker attacks, malicious software.

SADRŽAJ

Uvod.....	6
1. Metodologija istraživačkog projekta	8
1.1. Predmet istraživanja	8
1.2. Ciljevi i zadaci istraživanja	8
1.3. Istraživačke hipoteze	9
1.4. Metodi istraživanja i tok istraživačkog procesa	9
2. Bezbednost informacija.....	10
3. Računarske mreže.....	11
3.1. Istorija računarskih mreža	11
3.2. Vrste računarskih mreža.....	11
3.2.1. LAN	11
3.2.2. WLAN	11
3.2.3. WAN.....	12
3.2.4. MAN.....	12
3.2.5. SAN	12
3.2.6. CAN.....	12
3.2.7. PAN	12
3.2.8. DAN.....	13
3.3. OSI model	13
3.3.1. Istorija OSI modela	13
3.3.2. Opis OSI slojeva	13
3.3.3. Sloj 1 – Fizički sloj	14
3.3.4. Sloj 2 – Sloj veze	15
3.3.5. Sloj 3 – Sloj mreže	15
3.3.6. Sloj 4 – Sloj transporta	15
3.3.7. Sloj 5 – Sloj sesije.....	15
3.3.8. Sloj 6 – Sloj prezentacije	15
3.3.9. Sloj 7 – Sloj aplikacije	16
4. Kriptografija	16
4.1. Istorija kriptografije	16
4.2. Osnovni pojmovi kriptografije.....	18
4.3. Klasifikacija šifarnog sistema	19
4.4. Moderni simetrični blokovni šifarski sistemi	19
4.5. Istorijat DES-a.....	20
4.6. Napredni standard šifrovanja.....	20
5. Firewall.....	21
5.1. Zaštita lokalne mreže	22
5.2. Zaštita od štetnog delovanja lokalnih korisnika.....	23
6. IDS.....	23
6.1. Pasivni i reakcioni sistemi	24
6.2. Upoređenje sa firewall.....	24
7. IPS.....	24
7.1. IPS klasifikacije.....	24
7.2. Metode detekcije.....	25
8. Računarski virusi	25
8.1. Vrste računarskih virusa.....	26
8.1.1. Boot sektor virusi.....	26
8.1.2. Fajl virusi	27

8.1.3. Makro virusi	27
8.1.4. Internet virusi	27
9. Worm (crv) i trojanski konj.....	28
9.1. Worm - crv.....	28
9.2. Trojanski konj	28
10. Hronološki raspored nastanka računarskih virusa i crva	29
10.1. 1970.-1979. godina	29
10.1.1. 1971. godina	29
10.1.2. 1974. godina	29
10.1.3. 1975. godina	29
10.2. 1980.-1989. godina	30
10.2.1. 1982. godina	30
10.2.2. 1983. godina	30
10.2.3. 1984. godina	30
10.2.4. 1986. godina	30
10.2.5. 1988. godina	30
10.2.6. 1989. godina	31
10.3. 1990.-1999. godina	31
10.3.1. 1990. godina	31
10.3.2. 1992. godina	31
10.3.3. 1993. godina	31
10.3.4. 1994. godina	31
10.3.5. 1995. godina	31
10.3.6. 1996. godina	32
10.3.7. 1998. godina	32
10.3.8. 1999. godina	32
10.4. 2000.-2009. godina	32
10.4.1. 2000. godina	32
10.4.2. 2001. godina	32
10.4.3. 2002. godina	33
10.4.4. 2003. godina	33
10.4.5. 2004. godina	33
10.4.6. 2005. godina	34
10.4.7. 2006. godina	34
10.4.8. 2007. godina	35
10.4.9. 2008. godina	35
10.4.10. 2009. godina	35
10.5. 2010. godina i posle.....	36
10.5.1. 2010. godina	36
10.5.2. 2011. godina	36
10.5.3. 2012. godina	36
10.5.4. 2013. godina	37
11. Antivirus programi	37
11.1.1. Vrste antivirus programa.....	37
11.2. Antivirus metode rada.....	38
11.2.1. Skeneri	38
11.2.2. CRC skeneri	38
11.2.3. Blokeri događaja	38
11.2.4. Imunizatori	38
11.2.5. Checksum provera	39

11.2.6.	Monitoring.....	39
12.	ESET NOD32 antivirus.....	39
12.1.	Istorijat	39
12.1.1.	NOD32	39
12.1.2.	E-Mail bezbednost za Microsoft Exchange Servere.....	40
12.1.3.	Bezbednost za mobilne telefone	40
12.1.4.	Remote Administrator (udaljeni administrator).....	40
12.1.5.	ESET Smart Security	40
12.1.6.	ESET SysInspector.....	40
12.1.7.	Ostali programi u ponudi ESET-a.....	40
12.2.	Primena ESET NOD32 antivirusa.....	40
12.2.1.	Proxy podešavanja za ažuriranje definicija antivirus programa	43
Zaključak		45
Literatura		46

Uvod

Računarska mreža ili mreža za prenos podataka je telekomunikaciona mreža koja omogućava računarima da razmenjuju podatke. U računarskim mrežama, umreženi računari međusobno prosleđuju podatke preko data konekcija, odnosno veza. Veze (konekcije) između čvorova su ustanovljeni upotrebom ili kablovskih medija ili bežičnih medija. Najpoznatiji računarska mreža je Internet.

Mrežni računarski uređaji koji prenose, rutiraju i ukidaju podatke nazivaju se mrežni čvorovi. Čvorovi mogu da sadrže hostove kao što su serveri i personalni računari, kao i mrežni hardver. Za dva uređaja se kaže da su umreženi kada međusobno mogu da razmenjuju podatke.

Računarske mreže podržavaju aplikacije kao što su pristup World Wide Web (svetskoj internet mreži), mrežno deljenje aplikacija i servera za skladištenje podataka, štampača i fax uređaja, upotreba email i aplikacija za trenutne poruke. Računarske mreže se razlikuju po fizičkim medijima koji se koriste za prenos njihovih signala, protkola za komunikaciju za organizaciju saobraćaja u mrežama i organizacionim namerama.

Kako je sve veća upotreba računara i računarskih mreža, dolazi do sve više hakerskih napada i zloupotrebe podataka krajnjeg korisnika. Kako bi se ti napadi potpuno sprečili ili redukovali potrebno je uvođenje raznih sistema zaštite računarskih mreža kao što su Firewall, Antivirus programi, IDS i IPS sistemi, kritpografski protokoli, politike i procedure. Ove tehnologije onemogućavaju hakeru da dođe do podataka koji se prenose preko mreže, kao i podataka koji se nalaze na samim umreženim računarima jer čim računar pristupi nekoj računarskoj mreži on automatski postaje ugrožen od napada i potrebno je primeniti adekvatnu zaštitu.

Maliciozni programi kao što su računarski virusi, crvi i trojanski konji su predstavljali, ali i dalje predstavljaju ogromnu pretnju za preduzeća, firme i ustanove koje poseduju velike računarske mreže, ali i za običnog korisnika računara.

Oni su u stanju da nanesu ogromnu finansijsku štetu i da kompromituju privatne podatke korisnika računara, tako što npr. beleže unose sa tastature korisnika i šalju ih hakeru koji je napravio maliciozni program, ali postoje i mnogi od njih koji nisu toliko opasni, ali mogu da ometaju korisnika prilikom rada na računaru tako što zagušuju performanse računara i samim tim čine rad gotovo nemogućim. Postoje i oni koji su manje opasni koji ispisuju razne poruke humorističkog tipa ili obaveštavaju korisnika da je zaradio veliku količinu novca, iako to nije istina.

U svakom slučaju te pretnje ne treba ignorisati, već je neophodno instalirati programe koji su specijalizovani za njihovo pronalaženje i uklanjanje. Ti programi nazivaju se antivirus programi. Oni mogu da spreče virus da inficira računar, ali su i u stanju da ih uklone nakon što je računar inficiran. Iz razloga što se stalno pojavljuju nove pretnje, firme koje proizvode programe za antivirus zaštitu moraju stalno da ažuriraju svoje baze podataka (definicije) koje sadrže podatke o novonastalim virusima, crvima i trojanskim konjima, koje korisnik može konstantno da preuzima, odnosno ažurira postojeću bazu podataka kako bi računari i računarske mreže bile što bolje zaštićene.

U ovom radu biće opisane metode rada antivirus programa, način na koji oni detektuju, odnosno pronalaze pretnje, i kako ih uklanjaju. Kao praktičan primer biće odabran ESET NOD32 Antivirus.

1. Metodologija istraživačkog projekta

Master rad ima za cilj da definiše pojmove koji se koriste kada se govori o računarskih mrežama kroz konstituciju, protokole i sisteme za bezbednost vezane za ovu vrstu mreža.

Projektni zadatak se pored organizacionih bavi i tehnološkim aspektima zaštite računarskih mreža. Prikazana su brojna rešenja koja su trenutno aktuelna i u funkciji, ali i rešenja koja tek treba da se implementiraju i usavrše.

Projektni zadatak je izrađen korišćenjem teoretskih i praktičnih znanja iz domena računarskih mreža, a posebno je dat naglasak na primenu zaštite na računarske mreže.

1.1. Predmet istraživanja

Predmet istraživanja su računarske mreže, odnosno organizacioni aspekti zaštite u njima. Može se reći da je bezbednost računarskih mreža direktno povezana sa samim IT administratorom koji je zadužen za održavanje te mreže. Ključna pitanja na koja su traženi odgovori tokom istraživanja su:

- Kako funkcionišu računarske mreže
- Koje vrste zaštita računarskih mreža postoje i kako se one uvode
- Koje su koristi od zaštite računarskih mreža
- Razumevanje i objašnjenje onoga što treba tražiti od kompanije koja prodaje rešenje iz ove oblasti
- Skretanje pažnje korisnicima na bezbednosne aspekte računarskih mreža
- Ukazivanje na aktuelne trendove u ovoj oblasti kao i na razvoj zaštite i bezbednosti računarskih mreža u budućnosti

1.2. Ciljevi i zadaci istraživanja

Ovaj rad je namenjen profesionalcima u oblasti računarskih mreža, kao i IT administratorima koji treba da urade studiju izvodljivosti uvođenja zaštite u računarske mreže. Potrebno je da ovi profili IT administratora imaju dobru osnovu u poznavanju mrežnih tehnologija ali nije nužno da detaljno ulaze u funkcionisanje protokola kao i način rada pojedinih medija koji se koriste u računarskim mrežama. Biće navedeni neki od konkretnih problema do kojih se došlo prilikom istraživanja, a sa kojima će se to je sasvim sigurno susresti bilo koji IT administrator koji planira da uvede neku ili sve navede zaštite računarskih mreža u svoju firmu ili organizaciju.

Treba uzeti u obzir da većina IT administratora olako shvata bezbednost računara i računarskih mreža sve dok ne dođe do propusta u bezbednosti i samim tim do krađe ili gubitka podataka, zbog napada hakera ili malicioznog programa koji je dospao u računar preko mreže. Zato je cilj ovog istraživanja da se utvrde razni načini kako da se zaštititi računarska mreža kako ne bi došlo do gore navedenog slučaja.

1.3. Istraživačke hipoteze

Opšta hipoteza

U početku je težište istraživanja bilo na pojedinačnim metodama zaštite računarskih mreža. Tokom istraživanja pokazalo se da kompanije sve više imaju potrebe za uvođenjem većeg broja računara kao i njihovog umrežavanja i komunikacijom sa računarima van mreže. Samim tim te kompanije podležu sve većem riziku od raznih oblika hakerskih napada i više nije dovoljno upotrebiti samo jedan sistem zaštite, već spojiti što veći broj tehnologija kako bi se obezbedila što veća sigurnost podataka i informacija tih kompanija i njihovih zaposlenih.

Radna hipoteza

U ovom radu će biti opisane razne metode i tehnologije zaštite računara i računarskih mreža. Najbitnije među njima su Firewall, Antivirus programi, IDS i IPS sistemi, kriptografski protokoli, politike i procedure zaštite.

1.4. Metodi istraživanja i tok istraživačkog procesa

Metodologija istraživanja je u osnovi analiza internat sadržaja i korišćenje literature koje se bave oblastima zaštite računarskih mreža. Informacije su takođe tražene i od kompanija koje imaju predstavništva u našoj zemlji, kao što je Cisco.

Najviše informacija je pronađeno preko literatura nađenih putem interneta preko raznih web prezentacija koji nude knjige u elektronskom obliku. Takođe su upotrebljene i informacije dostupne na internetu i sve zajedno svedeno u jednu celinu.

2. Bezbednost informacija

Sigurnost informacija jeste praksa odbrane informacije od neovlašćenog pristupa, korišćenja, otkrivanja, prekida, modifikacije, inspekcije, snimanja ili uništenja. To je opšti naziv koji se može koristiti bez obzira na oblik koji podaci mogu uzeti (elektronski , fizički , itd.).

Dva glavna aspekta bezbednosti, odnosno sigurnosti, informacija i podataka su:

IT bezbednost:

Ponekad se naziva bezbednost računara, informacione tehnologije. Najčešće se odnosi na neki oblik tehnologije (najčešće neki oblik računarskog sistema ili mreže). Vredi napomenuti da termin računar ne mora da se odnosi na kućni računar (desktop računar). Računar je svaki uređaj sa procesorom i memorijom (neki čak i kalkulator). IT administratori zaduženi za bezbednost se gotovo uvek mogu naći u bilo kojem većem preduzeću, odnosno kompaniji, zbog prirode i vrednosti podataka u većim preduzećima. Oni su odgovorni za čuvanje svih tehnologija u kompaniji od zlonamernih sajber napada koji se često dešavaju sa namerom da probiju u kritične privatne informacije ili steknu kontrolu unutrašnjih sistema.

Garancija za bezbednost informacija:

Suština je da se podaci, odnosno informacije, obezbede kada dođe do kritičnih situacija. Ova pitanja uključuju ali se ne ograničavaju na: prirodne katastrofe, računar / server kvara, krađe, fizičkog oštećenja ili bilo koji drugi primer gde podaci imaju potencijal da budu izgubljeni. Budući da se većina informacija čuva na računarima u našem modernom dobu, za bezbednost informacija su zaduženi IT administratori. Jedan od najčešćih metoda pružanja sigurnosti podataka je da se ima off-sajt bekap podataka u slučaju da se dogodi neka od navedenih kritičnih situacija. Vlade, vojske, korporacije, finansijske institucije, bolnice i privatne firme nagomilaju mnogo poverljivih informacija o svojim zaposlenima, kupcima, proizvodima, istraživanjima i finansijskim izveštajima. Većina ovih informacija se sada prikupljaju, obrađuju i čuvaju na računarima i elektronskim putem prenose preko mreže na druge računare. Ukoliko poverljive informacije o poslovnim kupcima, ili finansijama, ili nove linije proizvoda padnu u ruke konkurenta, ili "black hat" hakera, kompanija bi zajedno sa svojim klijentima mogla pretrpeti nepopravljivi opsežni finansijski gubitak, a da ne pominjemo štetu na račun ugleda kompanije. Zaštita poverljivih informacija je poslovni zahtev i u mnogim slučajevima takođe etički i pravni zahtev. Za pojedinca, bezbednost informacija ima značajan uticaj na privatnost, što se znatno razlikuje u različitim kulturama. Oblast bezbednosti informacija je porasla i značajno evoluirala u poslednjih nekoliko godina. Ona nudi mnoge oblasti za specijalizacije uključujući obezbeđivanje mreža i savezničke infrastrukture, obezbeđivanje aplikacija i baza podataka, bezbednosti testiranja, revizije informacionih sistema, kontinuitet poslovanja i planiranje digitalne forenzike, itd.

3. Računarske mreže

Računarska mreža je pojam koji se odnosi na računare i druge uređaje koji su međusobno povezani radi međusobne komunikacije i razmene podataka. U računarskoj mreži osim računara mogu biti i razvodnici, svičevi i ruteri. Veza između dva ili više računara koji dele svoje podatke može da se nazove računarska mreža.

3.1. Istorija računarskih mreža

Džordž Stibic i Semjuel Vilijams su napravili Complex Number Computer, računar koji je imao 400 telefonskih releja i bio je povezan sa tri teleprinterima, koji su prethodnici današnjih terminala. Prvo prenošenje naredjenja između računara bilo je 1940. godine kada je Stibic upotrebio tele mašinu za kucanje, pomoću koje je poslao instrukcije sa njegovog modela K sa Univerziteta Dartmot u Novom Hempširu na Complex Number Calculator u Njujorku, a rezultate je dobio nazad istim putem.

3.2. Vrste računarskih mreža

Jedan od načina da se kategorizuju različite vrste računarskih mrežnih dizajna je po svom obimu ili skali. Uobičajeni primeri tipova mreža po područjima koje obuhvataju:

LAN - Local Area Network

WLAN - Wireless Local Area Network

WAN - Wide Area Network

MAN - Metropolitan Area Network

SAN - Storage Area Network

CAN - Campus Area Network

PAN - Personal Area Network

DAN - Desk Area Network

3.2.1. LAN

Lokalna mreža (LAN) je računarska mreža koja povezuje računare u ograničenom prostoru, kao što su kuće, škole, kompjuterske laboratorije, odnosno poslovni objekti, upotrebom mrežnih medija. Glavna karakteristika koja definiše LAN, za razliku od širokog prostora koji obuhvata mreža WAN, uključuje njenu manju geografsku oblast, i neupotrebu iznajmljenih telekomunikacionih linija. ARCNET, Token Ring i drugi standardi tehnologije su korišćeni u prošlosti, ali Ethernet i Wi-Fi su dve najčešće tehnologije koje se trenutno koriste za izgradnju LAN mreže.

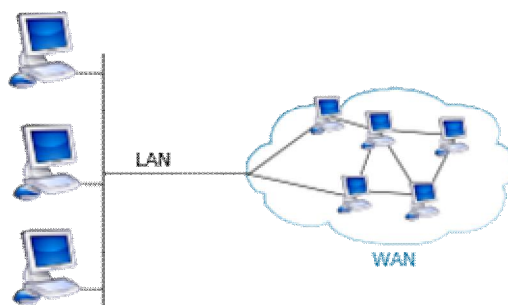
3.2.2. WLAN

Bežična lokalna mreža (WLAN) povezuje dva ili više uređaja upotrebom metoda bežične distribucije (obično spread-spectrum ili OFDM radio), i obično daje konekciju preko pristupne tačke (access point) širem internetu. Ovo daje mogućnost korisnicima da se kreću u užem krugu koji WLAN obuhvata, i da i dalje budu povezani na mrežu.

Bežične lokalne mreže su postale popularne zbog lakoće postavljanja, i zbog komercijalnih svrha (jer se pruža besplatan internet na mestima kao što su restorani, kafići itd.).

3.2.3. WAN

Regionalna mreža (WAN - wide area network) je mreža koja obuhvata široko područje (npr. bilo koju telekomunikacionu mrežu koja povezuje gradove, regione ili celu državu) upotrebom privatnih ili javnih mrežnih prenosa. Kompanije i državne ustanove upotrebljavaju WAN da bi povezali svoje zaposlene, klijente, kupce i dobavljače iz različitih geografskih oblasti. U osnovi ovaj vid telekomunikacije dopušta da se poslovi obavljaju regularno na dnevnoj bazi neovisno od same lokacije. Internet se takođe može smatrati kao WAN, i koriste ga kompanije, državne ustanove i pojedinci za gotovo svaku svrhu koja može da se zamisli.



Slika 1 – Prikaz odnosa LAN i WAN mreže

3.2.4. MAN

Gradska mreža (MAN – metropolitan area network) je računarska mreža u kojoj su dva ili više računara ili uređaja za komunikaciju koji su geografski odvojeni, ali se nalaze u istom gradu i povezani su preko mreže, za njih se kaže da su povezani preko MAN mreže. MAN mreže su ograničene u zavisnosti od veličine grada u kojem se nalaze.

3.2.5. SAN

Mreža za skladištenje podataka (SAN – storage area network) je posvećena mreža koja omogućava pristup konsolidovanom skladištenju podataka na blok nivou. SAN mreže se uglavnom koriste da pouspeše uređaje za skladištenje, kao što su nizovi diskova, biblioteke traka i optički džuboksi, dostupni serverima na način da uređaj izgleda kao da je lokalno povezani uređaj na operativni sistem. SAN obično ima svoju mrežu sačinjenu od uređaja za skladištenje podataka koji u suštini nisu dostupni kroz lokalnu mrežu drugim uređajima. Cena i kompleksnost SAN mreža je opala početkom 2000. godine na nivoe dostupne za velika, srednja i mala preduzeća.

3.2.6. CAN

Kampus mreže (CAN – campus area network) je mreža sačinjena od više povezanih lokalnih mreža unutar ograničenog geografskog područja. Mrežna oprema (svičevi, ruteri) i mediji za prenos (optičke žice, Cat5 kablovi itd.) su gotovo skroz u vlasništvu kampus stanara ili vlasnika (preduzeća, univerziteta, vlade itd.).

3.2.7. PAN

Personalna računarska mreža (PAN – personal area network) je računarska mreža koja se koristi za prenos podataka između uređaja kao što su računari, telefoni i personalna digitalna

pomagala. PAN može da se koristi za komunikaciju između samih personalnih uređaja (interpersonalna komunikacija), ili za povezivanje mreže većeg nivoa na internet.

3.2.8. DAN

Desk računarska mreža (DAN – desk area network) je multimedijalna radna stanica bazirana oko ATM interkonektora. Sva komunikacija između periferija i čak između procesora i glavne memorije se postiže slanjem ATM ćelija kroz žice u sviču. Prototip verzija je bazirana na Fairisle svič vlaknu i napravljena je i upotrebljava se za dalja istraživanja arhitekture ove mreže.

3.3. OSI model

Open System Interconnection (OSI) model (ISO/IEC 7498-1) je konceptualni model koji karakteriše i standardizuje interne funkcije komunikacionog sistema tako što ga particionira na abstraktne slojeve. Ovaj model je projekat od strane Open System Interconnection po ISO standardizaciji.

Model grupiše slične komunikacione funkcije u jedan od sedam logičkih slojeva. Sloj (layer) služi sloju koji se nalazi iznad njega, a njega služi sloj koji se nalazi ispod njega. Npr. Sloj koji pruža serveru error-free komunikaciju preko mreže, prosleđuje neophodne putanje na aplikacije iznad njega, a poziva sledeći niži sloj da šalje i prima pakete koji prave sadržaj putanje. Dve instance na jednom sloju su povezane pomoću horizontalne konekcije na tom sloju.

3.3.1. Istorija OSI modela

Rad na arhitekturi za layer (sloj) model mreže je pokrenut od strane Internacionalne Organizacije za Standardizaciju (ISO) i počeli su da razvijaju OSI frejmwork arhitekture. OSI je imao dve glavne komponente: abstraktni model mreže, nazvan Basic Reference Model ili seven-layer model (model od 7 slojeva), i set specifičnih protokola.

Koncept modela od sedam slojeva je proistekao iz rada Čarlsa Bekhmana, Honeywell Informacione Usluge. Više aspekata OSI dizajna je proisteklo iz iskustva sa ARPANET, NPLNET, EIN, CYCLADES mreža i sa radom u IFIP WG6.1. Novi dizajn i njegovi razni dodaci su dokumentovani u ISO 7498. U ovom modelu, mrežni sistem se deli na slojeve. Unutar svakog sloja, jedan ili više entiteta implementiraju njegovu funkcionalnost. Svaki entitet je komunicirao direktno samo sa slojem ispod njega i pružao je putanje za upotrebu na slojeve iznad njega.

Protokoli su omogućili entitet na jednom hostu da može da komunicira sa odgovarajućim entitetom, na istom sloju ali na drugom hostu. Definicije usluga su abstraktno objasnili funkcionalnost koja je upotrebljena na (N)-layer od strane (N-1)-layer, gde N predstavlja jedan od sedam slojeva protokola koji rade na lokalnom hostu.

Dokumenti o OSI standardima su dostupni od strane ITU-T kao X.200-serija od preporuke. Neke od specifikacija protokola su takođe dostupne kao deo od ITU-T X serije. Ekvivalent ISO i ISO/IEC standardi za OSI model su bili dostupni od strane ISO, ali samo neki od njih su besplatni.

3.3.2. Opis OSI slojeva

Po preporuci X.200, postoje sedam slojeva, numerisani od 1 do 7, tako da je sloj 1 poslednji.

7. sloj – aplikacije (application layer)
6. sloj – prezentacije (presentation layer)
5. sloj – sesije (session layer)
4. sloj – transporta (transport layer)
3. sloj – mreže (network layer)
2. sloj – veze (data link layer)
1. sloj – fizički sloj (physical layer)

OSI Model			
	Jedinica podataka	Sloj	Uloga
Host slojevi	Podaci	7. Aplikacije	Započinje ili prihvata zahtev
		6. Prezentacije	Dodaje informacije koje se koriste za šifrovanje, formatiranje i prikazivanje
		5. Sesije	Dodaje informacije o toku saobraćaja kako bi se odredio trenutak slanja
	Segmenti	4. Transporta	Dodaje informacije koje služe za detektovanje i prevazilaženje grešaka u prenosu
Slojevi medija	Paket/Datagram	3. Mreže	Dodaje informacije koje služe za sekvenciranje i adresiranje paketa
	Bit/Frejms	2. Sloj Veze	Dodaje informacije koje služe za proveru postojanja greške i preprima podatke za fizičko povezivanje
	Bit	1. Fizički	Šalje paket kao niz bitova

Tabela 1 – Prikaz OSI modela i njegovih slojeva

3.3.3. Sloj 1 – Fizički sloj

Fizički sloj (physical layer) ima sledeće važne funkcije:

- Definiše električne i fizičke specifikacije od data konekcije. On definiše odnos između uređaja i medija za fizički prenos (npr. optički kabel). Ovo obuhvata pinove, voltaže, specifikacije kablova, tajming signala, čvorišta, ponavljače, mrežne adaptere itd.

- Definiše protokol za uspostavljanje i ukidanje konekcije između dva direktno povezana mrežna čvora preko medija za komunikaciju.
- Može da definiše protokol za kontrolu protoka.
- Definiše protokol za odredbu konekcije između dva direktno povezana čvora, i modulaciju ili konverziju između digitalnih podataka u korisničkoj opremi i korespondenciju signala emitovanih preko fizičkog kanala za komunikaciju. Ovaj kanal može da obuhvata fizičke kablove ili bežičnu radio vezu.

3.3.4. Sloj 2 – Sloj veze

Sloj veze pruža pouzdanu vezu između dva direktno povezana mrežna čvora, tako što detektuje i po mogućnosti koriguje greške koju mogu da se jave u fizičkom sloju.

Point-to-Point Protocol (PPP) je primer sloja veze u TCP/IP.

3.3.5. Sloj 3 – Sloj mreže

Sloj mreže pruža funkcionalnu i proceduralnu svrhu za prenos sekvenci podataka različitih dužina (nazvani datagrami) od jednog čvora na drugi koji su povezani na istu mrežu. Mreža je medijum na koji mnogi čvorovi mogu da budu povezani, na kojoj svaki čvor ima adresu koja dopušta čvorovima povezanim na njega da prenose poruke na druge čvorove tako što propušta sadržaj poruke na adresu od ciljanog čvora i dopušta mreži da pronade način da dostavi poruku na ciljani čvor. U dodatku na rutiranje poruka, mreža može da implementira dostavu poruka tako što deli poruku na više fragmenata, dostavljajući svaki fragment preko sporedne rute i na kraju spaja fragmente.

3.3.6. Sloj 4 – Sloj transporta

Sloj transporta pruža pouzdano slanje data paketa između čvorova (sa adresama) koji su locirani na mreži, pružajući pouzdan način prenosa podataka na više slojeve.

Primer protokola sloja transporta je standardni Internet protokol TCP, obično izgrađen preko IP protokola.

Sloj transporta kontroliše pouzdanost datog linka kroz kontrolu protoka, segmentacije/desegmentacije, i kontrole grešaka. Transportni sloj može da vodi evidenciju o segmentima i da ponovo pošalje one koji nisu uspeali da prođu. Takođe pruža informaciju o uspešnom prenosu podataka i šalje sledeće podatke ukoliko nije došlo do greške. Transportni sloj pravi pakete od poruka koje je dobio od sloja aplikacije. Paketiziranje je proces deljenja duge poruke u više manjih poruka.

3.3.7. Sloj 5 – Sloj sesije

Sloj sesije kontroliše dijaloge (veze) između računara. On uspostavlja, uređuje i ukida veze između lokalne i udaljene aplikacije. Pruža full-duplex, polu-duplex, ili simplex operaciju, uspostavlja kontrolne tačke, prekid, ukidanje i procedure restartovanja.

3.3.8. Sloj 6 – Sloj prezentacije

Sloj prezentacije uspostavlja kontekst između entiteta sloja aplikacije, u kom slučaju entiteti sloja aplikacije mogu da koriste različite sintakse i šeme ako usluga prezentacije ima mapiranje između njih. Ako je mapiranje dostupno, podaci od usluge prezentacije bivaju pretvoreni u jedinice podataka protokola sesije, i nakon toga prosleđeni u TCP/IP stek.

3.3.9. Sloj 7 – Sloj aplikacije

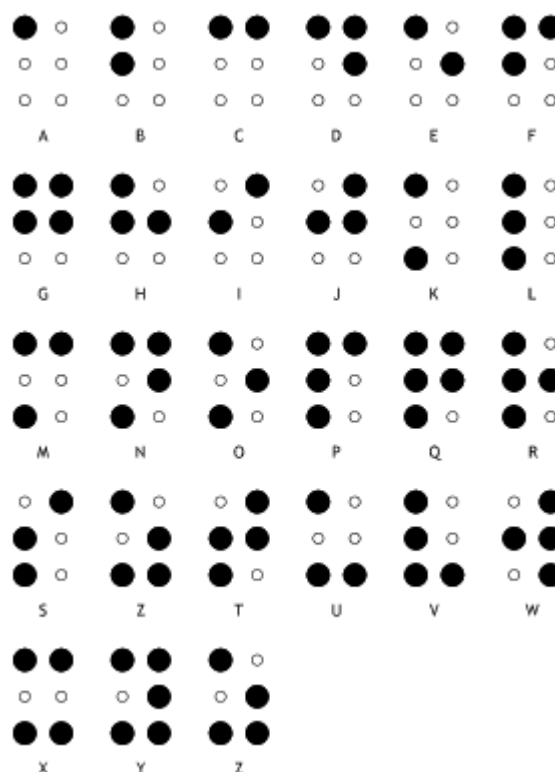
Sloj aplikacije je OSI sloj koji je najbliži krajnjem korisniku, što znači da i OSI i sloj aplikacije i njihov korisnik imaju interakciju direktno preko softverske aplikacije. Ovaj sloj ima interakciju sa softverskom aplikacijom koja implementuje komponentu za komunikaciju. Funkcije sloja aplikacije obično sadrže komunikacione partnere, određivanje slobodnih resursa, i sinhronizaciju komunikacije. U toku identifikovanja partnera za komunikaciju, sloj aplikacije određuje identitet i dostupnost komunikacionih partnera za aplikaciju koja ima podatke koje treba proslediti. Kada se određuje raspoloživost resursa, sloj aplikacije mora da odredi da li postoji dovoljna mrežna mogućnost ili da li zahtevana komunikacija uopšte postoji. U sinhronizaciji komunikacije, sve komunikacije između aplikacija zahtevaju kooperaciju koju uređuje sloj aplikacije.

4. Kriptografija

4.1. Istorija kriptografije

Kroz istoriju čovečanstva postojala je potreba za sigurnom razmenom informacija, odnosno podataka. Problematikom sigurne komunikacije bavili su se već Egipćani i Indijci pre više od 3000 godina i od tada do dan danas se nije promenila osnovna ideja koja je preneti neku poruku sa jednog mesta na drugo što je bezbednije moguće, tj. napraviti algoritam koji bi omogućio skrivanje originalne poruke tako da bude potpuno nerazumljiva osobama koje bi neovlašteno došle u njen posed. Prve upotrebljene metode nisu bili složeni matematički algoritmi nego se počelo sa upotrebom alternativnih jezika koji su bili poznati samo malom broju ljudi. Tek nakon razvoja pisma je počeo razvoj složenijih metoda sigurne komunikacije, što je omogućilo da se bilo koja informacija prikaže određenim brojem znakova koji bi (nakon upotrebe određenog ključa) formirali originalnu početnu poruku. Vremenom se javila i ideja prikaza slova drugim simbolima. Primeri koji se danas koriste su Moresov kod, Braille-ovo pismo i ASCII kod.

Nikad nije tačno utvrđen početak kriptografije, ali se smatra da je počela pre više od 2000 godina pne. jer je iz tog vremena potiču prvi pronađeni tragovi šifrovanja. Tačnije oko 1900. godine pne. u Egiptu je nastao natpis koji se danas smatra prvim dokumentovanim primerom pisane kriptografije. U 6. veku pne. u zapisu dela Biblije, Knjige o Jeremiji, korišćena je jednostavna šifra koja izvrće abecedu naopako. Šifra je poznata pod imenom ATBASH, a bila je jedna od hebrejskih šifri koje su u to vreme upotrebljene. U 6. deceniji pne. Julije Cezar je u državnim komunikacijama koristio jednostavnu zamenu koja je kasnije njemu u čast dobila naziv „caesar“ šifrovanje. Ideja je bila u pomicanju svih slova za tri mesta napred. Takva šifra danas se smatra slabijom čak i od ATBASH šifre, ali je u to vreme bila dobra jer je mali broj ljudi znao čitati. U srednjem veku kriptografija je često upotrebljavana u službi Crkve, a jedan od primera je nomenclator koji je kombinacija malog koda i supstitucijske abecede koje je na zahtev pape Clementa VII stvorio Gabrieli di Lavinde. Ova šifra ostala je u upotrebi sledećih 450 godina, iako su u međuvremenu stvorene i sigurnije šifre. Razlog za to je najverovatnije bio u njenoj jednostavnosti. 1518. godine Johannes Trithemius je napisao prvu pisanu knjigu o kriptografiji. Oko 1790. godine Thomas Jefferson je uz pomoć matematičara dr. Roberta Pattersona izumeo šifarnik sa točkom. On je kasnije ponovo napravljen u nekoliko različitih oblika i korišćen je u II. Svetskom Ratu od strane američke ratne mornarice. 1861. godine u kancelariji za patente u SAD prijavljen je prvi izum vezan za kriptografiju. Do 1980. godine prijavljeno je 1769 takvih izuma. U 20. veku je bilo veoma burno - 2 svetska rata i mnogo raznih sukoba u kojima je kriptografija odigrala značajnu ulogu.



Slika 2 – Braille-ov alfabet

William Frederick Friedman (poznat kao otac američke kriptanalize) prvi je uveo pojam „kriptoanaliza“. Kriptografiju su rado koristili i kriminalci, a jedan vrlo interesantan primer je doba prohibicije u SAD. Da bi mogli švercovati alkohol koristili su vrlo komplikovane sisteme šifriranja koji su u to vreme bili veoma napredni. 1923. godine Arthur Scheribus proizvodi svoj najslavniji proizvod – široko poznatu Enigmu. Ona je prvobitno trebala biti komercijalni proizvod, ali nije uspela pa su je preuzeli nemački nacisti. Oni su je poboljšali pa je postala glavni uređaj za šifrovanje u nacističkoj Nemačkoj. Prvi je njenu šifru slomio jedan poljski matematičar na osnovi ukradenog primerka šifrovanog teksta i dnevnih ključeva za tri meseca unapred. Kasnije su uspešno razbijene i druge Enigmine šifre prvenstveno pod vođstvom Alana Turinga. 30-ih godina 20. veka nastaje američki protivnik Enigme, nazvan SIGABA. Važno je spomenuti da je SIGABA bila tehnički naprednija od Enigme.

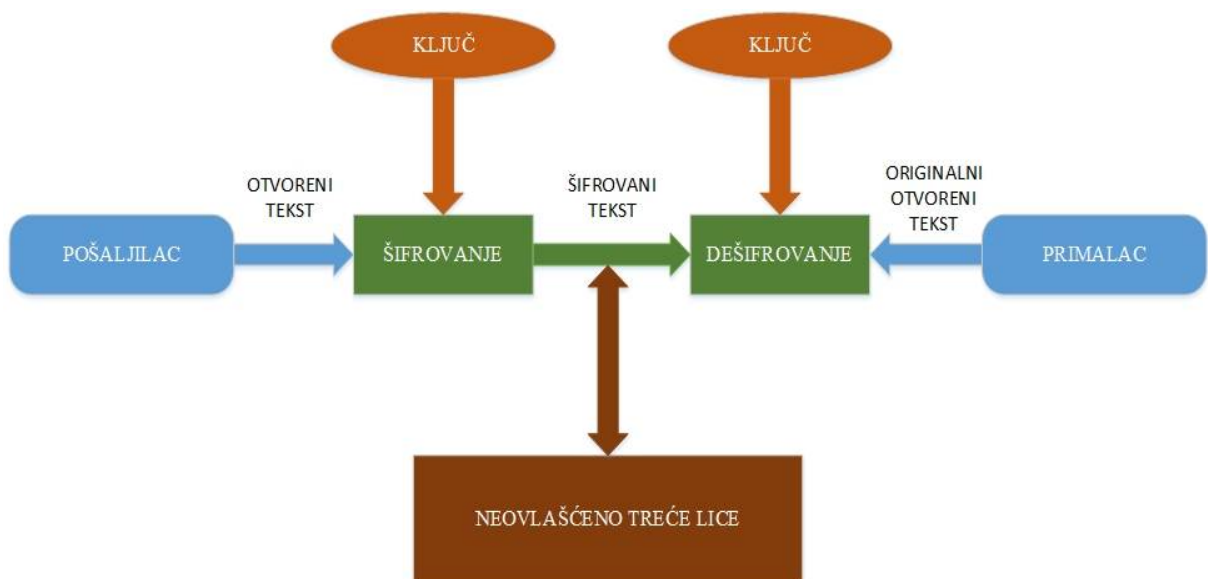
Nakon II. svetskog rata razvoj računara daje novi zamah kriptografiji. Tako 1970. godine IBM razvija šifru pod nazivom Lucifer, koja kasnije, 1976. godine inspiriše stvaranje DES (Data Encryption Standard) šifre. Široko je prihvaćena u svetu zbog svoje dokazane otpornosti na napade. 1976. godine se takođe pojavila ideja javnih ključeva. Godinu kasnije grupa početnika u kriptografiji Rivest, Shamir i Adleman stvorili su algoritam koji su po prvim slovima svojih prezimena nazvali RSA algoritam. To je bila praktična šifra sa javnim ključevima koja se mogla koristiti i za šifrovanje poruka i za digitalni potpis, a bazirala se na težini faktorizovanja velikih brojeva. 1984.-1985. u softveru za čitanje novosti na USENET-u upotrebljena je rot13 šifra (rotiranje slova za 13, slično "caesar" šifri) da bi se sprečio pristup dece za njih neprikladnim sadržajima. Ovo je prvi poznati primer uspešnog korišćenja šifre sa javnim ključem. 1990. je u Švajcarskoj objavljen "Predlog za novi Standard za šifrovanje blokova podataka" tj. predlog za International Data Encryption Algorithm (IDEA), koji bi trebao zameniti DES. IDEA koristi 128-bitni ključ i koristi operacije koje je lako

implementirati na računarima. 1991. Phil Zimmermann objavljuje prvu verziju svog PGP-a (Pretty Good Privacy) programa za zaštitu e-mailova i podataka uopšteno. Zbog toga što je bio freeware, komercijalni proizvodi iste vrste su redom propali, a PGP je postao svetski standard. U početku koristio je RSA algoritam koji se dugo vremena smatrao dosta sigurnim. Računari su sve brži i brži, a razvoj svega vezanog uz njih sve je teže pratiti. Budućnost kriptografije je danas povezana sa budućnošću računara.

4.2. Osnovni pojmovi kriptografije

Kriptografija je naučna disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namenjene može pročitati. Sama reč kriptografija je grčkog porekla i mogla bi se bukvalno prevesti kao tajni zapis.

Osnovni zadatak kriptografije je omogućiti za dve osobe (pošiljalac i primalac) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računarska mreža, itd.) na način da treća osoba (neovlašćeni posmatrač), koja može nadzirati komunikacioni kanal, ne može razumeti njihove poruke. Poruku koju pošiljalac želi poslati primaocu nazvaćemo otvoreni tekst (plaintext). To može biti tekst na njihovom maternjem jeziku, numerički podaci ili bilo šta drugo. Pošiljalac transformiše otvoreni tekst koristeći unapred dogovoreni ključ. Taj postupak se naziva šifrovanje, a dobijeni rezultat šifrat (ciphertext) ili kriptogram. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacionog kanala. Neovlašćeni posmatrač prisluškujući može saznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac koji zna ključ kojim je šifrovana poruka može dešifrovati šifrat i odrediti otvoreni tekst.



Slika 3 – Proces kriptografije

Za razliku od dešifrovanja, kriptanaliza ili dešifrovanje je naučna disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptologija je ipak naučna grana koja obuhvata kriptografiju i kriptanalizu.

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifrovanje i dešifrovanje. Uopšteno, radi se o dve funkcije, jednoj za šifrovanje, a drugoj za dešifrovanje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifara, i obrnuto. Funkcije se biraju iz određene

familije funkcija u zavisnosti od ključa. Skup svih mogućih vrednosti ključeva nazivamo prostor ključeva. Šifarski sistem se sastoji od kriptografskog algoritma, kao i svih mogućih otvorenih tekstova, šifara i ključeva.

4.3. Klasifikacija šifarnog sistema

Šifarne sisteme obično klasifikujemo sa obzirom na sledeća tri kriterijuma:

1. Tip operacija koje se koriste pri šifrovanju

Imamo podelu na supstitucijske šifre u kojima se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamenjuje sa nekim drugim elementom, transpozicijske šifre u kojima se elementi otvorenog teksta permutuju (premeštaju). Npr. ako reč TAJNA šifrujemo u XIWOI, napravili smo supstituciju, a ako je šifrujemo u JANAT, napravili smo transpoziciju. Postoje takođe i šifarski sistemi koji kombinuju ove dve metode.

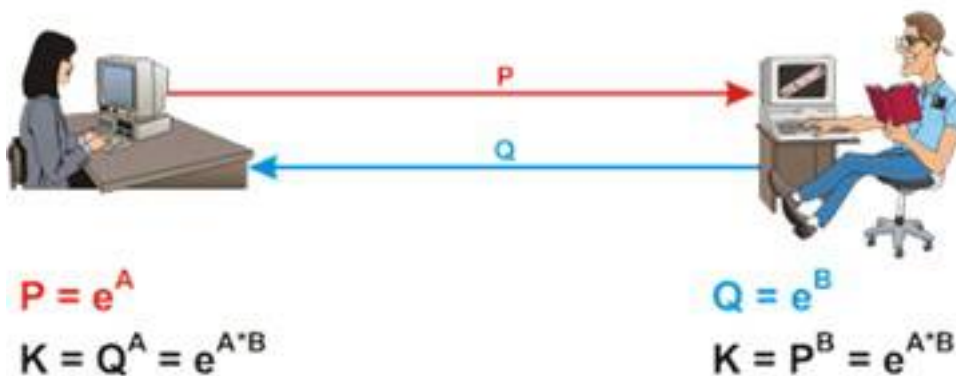
2. Način na koji se obrađuje otvoreni tekst

Ovde razlikujemo blokovne šifre, kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan isti ključ K , šifre koje protiču (stream cipher) kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom niz ključeva (keystream) koji se paralelno generiše.

3. Tajnost i javnost ključeva

Ovde je osnovna podela na simetrične šifarske sisteme i šifarske sisteme sa javnim ključem. Kod simetričnih ili konvencionalnih šifarskih sistema, ključ za dešifrovanje se može izračunati poznavajući ključ za šifrovanje i obrnuto. Ustvari, najčešće su ovi ključevi identični. Sigurnost ovih šifarskih sistema leži u tajnosti ključa. Zato se oni zovu i šifarski sistemi sa tajnim ključem. Kod šifarskih sistema sa javnim ključem ili asimetričnih šifarskih sistema, ključ za dešifrovanje se ne može (barem ne u nekom razumnom vremenu) izračunati iz ključa za šifrovanje. Ovde je ključ za šifrovanje javni ključ. Naime, bilo ko može šifrovati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifrovanje (privatni ili tajni ključ) može dešifrovati tu poruku. Ideju javnog ključa prvi su javno izneli Whitfield Diffie i Martin Hellman 1976. godine, kada su dali predlog rešenja problema razmenjivanja ključeva za simetrične šifarske sisteme putem nesigurnih komunikacijskih kanala.

4.4. Moderni simetrični blokovni šifarski sistemi



Slika 4 – Šifarski sistem, tajni i javni ključ

4.5. Istorijat DES-a

Krajem 60-tih i početkom 70-tih godina 20. veka, razvojem finansijskih transakcija, kriptografija postaje zanimljiva sve većem broju potencijalnih korisnika. Do tada je glavna primena kriptografije bila u vojne i diplomatske svrhe, pa je bilo normalno da svaka država (ili čak svaka zainteresovana državna organizacija) koristi svoju šifru za koju je verovala da je najbolja. Ipak, tada se pojavila potreba za šifrom koju će moći koristiti korisnici širom sveta, i u koju će svi oni moći imati poverenje - dakle, pojavila se potreba uvođenja standarda u kriptografiji.

Godine 1972. američki National Bureau of Standards (NBS) inicirao je program za zaštitu računarskih i komunikacionih podataka. Jedan je od ciljeva bio razvijanje jednog standardnog šifarskog sistema. Godine 1973. NSB je raspisao javni konkurs za takav šifarski sistem. Taj šifarski sistem je trebao zadovoljiti sledeće uslove:

- visoki nivo sigurnosti
- potpuna specifikacija i lako razumevanje algoritma
- sigurnost leži u ključu, a ne u tajnosti algoritma
- dostupnost svim korisnicima
- prilagodljivost upotrebi u različitim primenama
- ekonomičnost implementacije u elektroničkim uređajima
- efikasnost
- mogućnost provere
- mogućnost izvoza (zbog američkih zakona)

Na tom konkursu ni jedan predlog nije zadovoljavao sve ove zahteve. Međutim, na ponovljeni konkurs iduće godine pristigao je predlog algoritma koji je razvio IBM-ov tim kriptografa. Algoritam je zasnovan na tzv. Feistelovoj šifri. Gotovo svi simetrični blokovni algoritmi koji su danas u upotrebi koriste ideju koju je uveo Horst Feistel 1973. godine. Jedna od glavnih ideja je alternovana upotreba supstitucija i transpozicija kroz više iteracija (rundi). Predloženi algoritam je nakon nekih transformacija, u kojima je učestvovala i National Security Agency (NSA), prihvaćen kao standard 1976. godine i dobio je ime Data Encryption Standard (DES).

4.6. Napredni standard šifrovanja

Godine 1997. National Institute of Standards and Technology (NIST) objavio je konkurs za šifarski sistem koji bi trebao kao opšte prihvaćeni standard zameniti DES. Pobjednik konkursa dobio je ime Advanced Encryption Standard (AES). NIST je postavio sledeće zahteve na šifarski sistem:

- mora biti simetričan
- mora biti blokovan
- treba raditi sa 128-bitnim blokovima i ključevima sa tri dužine: 128, 192 i 256 bitova.

Nekoliko je razloga zbog kojih NIST nije odabrao 3DES kao AES:

- 3DES koristi 48 rundi da bi postigao sigurnost za koju je verovatno dovoljno 32 runde.
- Softverske implementacije 3DES-a su prespore za neke primene, posebno za digitalne video podatke.
- 64-bitni blokovi nisu najefikasniji u nekim primenama.

Svakako je veliki značaj 3DES-a što je pružio zadovoljavajuće privremeno rešenje za DES, do izbora novog standarda. Konkurs je zaključen 15.06.1998. Od 21 pristigle prijave, 15 ih je

zadovoljilo NIST-ove kriterijume. U avgustu 1999. NIST je objavio 5 finalista: MARS, RC6, RIJNDAEL, SERPENT i TWOFISH. Nekoliko reči o ovih 5 finalista.

MARS (IBM), RC6 (RSA Security Inc.) i TWOFISH (Counterpane Systems) spadaju u Feistelove šifre. Podsetimo se da je Feistelova šifra blokovna šifra u kojoj u i-toj rundi koriste formule $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ (dakle, isto kao kod DES-a).

MARS spada u nebalansirane Feistelove šifre jer se blokovi ne dele na 2, već na 4 dela. MARS ima 32 runde, RC6 ima 20 rundi, dok TWOFISH ima 16 rundi. Specifičnost šifarskog sistema RC6 (koji je dosta sličan RC5) su korišćenje funkcije $f(x) = x(2x+1)$, koja daje difuziju, pa je rotacija zavisna o podacima, koje daju otpornost na diferencijalnu i linearnu kriptanalizu. Specifičnost TWOFISH-a je da se S-kutije dinamički menjaju u zavisnosti od ključa, što komplikuje diferencijalnu i linearnu kriptanalizu.

SERPENT su konstruirali kriptografi iz Engleske, Izraela i Danske. Spada u supstitucijsko-permutacijske šifre. Ima 32 runde i, što je za njega specifično, u svakoj rundi paralelno koristi 32 identične S-kutije.

RIJNDAEL su razvili belgijski kriptografi. Razlikuje se od ostalih finalista po tome što se u konstrukciji S-kutija koriste operacije u konačnom polju $GF(2^8)$.

Konačno, 02.08.2000. objavljeno je da je pobednik konkursa za AES RIJNDAEL (rejn dol). RIJNDAEL su razvili belgijski kriptografi Joan Daemen i Vincent Rijmen sa Katoličkog univerziteta Leuven, po kojima je i dobio ime.

5. Firewall

Firewall je sigurnosni element smešten između neke lokalne mreže i javne mreže (Interneta), a koji je napravljen kako bi zaštitio poverljive, korporativne i korisničke podatke od neautoriziranih korisnika, (blokiranjem i zabranom prometa po pravilima koje definiše usvojena sigurnosna politika). Nije neophodno da svi korisnici u LAN-u imaju jednaka prava pristupa Internet mreži. Postavljanjem Firewall uređaja između dva ili više mrežnih segmenata mogu se kontrolisati i prava pristupa pojedinih korisnika pojedinim delovima mreže. U takvom slučaju Firewall je napravljen da dopušta pristup korisnim zahtevima, a blokira sve ostale. Firewall ujedno predstavlja idealno rešenje za kreiranje Virtualne Privatne mreže jer stvarajući virtualni tunel kroz koji putuju kriptovani podaci (omogućuje sigurnu razmenu osetljivih podataka između dislociranih korisnika). Firewall je servis (koji se tipično sastoji od firewall uređaja i Policy-a (pravilnika o zaštiti), koji omogućuje korisniku filtriranje određenih tipova mrežnog saobraćaja sa ciljem da poveća sigurnost i pruži određeni nivo zaštite od provale.

Osnovna namena Firewall-a je da spreči neautorizovani pristup sa jedne mreže na drugu. U suštini, ovo znači zaštitu unutrašnje mreže od Internet-a. Ako sistem raspolaže Firewall-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije - već doneta. Ove odluke su u direktnoj vezi sa politikom sigurnosti informacionog sistema. Pri planiranju ponude informacionih servisa, politika sigurnosti određuje opcije konfiguracije servisa. Osnova rada Firewall-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smera. Za Firewall je tipičan i kompromis između sigurnosti i lake upotrebe. Stav da "sve što nije dozvoljeno je zabranjeno" zahteva da se svaki novi servis individualno omogućava.

Firewall je odgovoran za više važnih stvari unutar informacionog sistema:

- Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogućiti rad u tom smislu.
- Firewall treba da beleži sumnjive događaje.

- Firewall treba da upozori administratora na pokušaje prodora i kompromitovanja politike sigurnosti.
- U nekim slučajevima Firewall može da obezbedi statistiku korišćenja.

Firewall može biti softverski ili hardverski. Softverski firewall omogućava zaštitu jednog računara, osim u slučaju kada je isti računar predodređen za zaštitu čitave mreže. Hardverski firewall omogućava zaštitu čitave mreže ili određenog broja računara. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja definišu kakav mrežni saobraćaj je dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.

5.1. Zaštita lokalne mreže

Firewalli koji nemaju čvrste i stroge politike prema dolaznim paketima podložni su različitim vrstama napada. Ukoliko firewall ne podržava kreiranje virtualnih privatnih mreža, a organizacija želi omogućiti pristup sa određenih IP adresa lokalnoj mreži, moguće je konfigurisati firewall da propušta pakete sa tačno određenim izvornim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primer napadač se može domoći paketa pa saznati logičku adresu sa kojom je dozvoljeno spajanje na lokalnu mrežu. Nakon toga napadač može kreirati pakete kojim kao izvornu stavlja logičku adresu računara kojem je dozvoljeno spajanje i tako pomoću posebno prilagođenih paketa naneti štetu lokalnoj mreži.

Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade. Većina današnjih proizvođača firewalla ponosno ističe na koje napade su njihovi firewall-ovi otporni, ali nove vrste napada se svakodnevno razvijaju i sve su komplikovaniji i kompleksniji. Ipak svaki firewall bi trebao biti otporan na poznate napade kao što su sledeći navedeni.

- **Address Spoofing** napad omogućava da paket bude prosleđen sa spoljnog okruženja na neki od internih računara ukoliko napadač kao izvornu adresu uzme neku od adresa unutar lokalne mreže. U tom slučaju firewall je možda konfigurisan da omogućava prolazak paketa i time ciljni računar može primiti posebno prilagođeni paket. Da bi se ovakva vrsta napada sprečila potrebno je onemogućiti prosleđivanje paketa koji kao izvornu adresu imaju neku od lokalnih adresa, a kao ulazno okruženje ono okruženje koje je spojeno na Internet.

- **Smurf napad** spada u grupu napada koje imaju za cilj onemogućavanje rada pojedinih servera i računara, tzv. DoS napad (Denial of Service). Napadač šalje ICMP echo request paket na broadcast adresu cele lokalne mreže. Time su adresirani svi računari unutar lokalne mreže. Kao odredište navodi se ciljani računar koji se želi onesposobiti velikim brojem odgovora. Za odbranu od ovakve vrste napada dovoljno je u konfiguracijskoj datoteci firewalla onemogućiti broadcast paket.

- **Syn-Flood** napad zasniva se na napadačevom slanju velikog broja početnih konekcijskih TCP paketa koji imaju postavljenu SYN zastavicu, i ignorisanjem TCP odgovora sa postavljenim SYN i ACK zastavicama. Time su resursi ciljanog računara zaokupljeni odgovaranjem na pakete. Da bi se spriječio ovakav oblik napada potrebno je ograničiti na firewallu broj dolazećih TCP paketa.

- **Port-Scanner** napad zasniva se na otkrivanju otvorenih TCP i UDP portova slanjem SYN ili FIN paketa na ciljane portove i čekanjem na RST odgovor. Potrebno je ograničiti broj takvih ispitivanja.

- **Ping-of-Death** napad može uzrokovati rušenje operativnog sistema, ukoliko se na računar usmeri veliki broj ICMP echo zahteva. Najbolje rešenje je onemogućavanje echo-request paketa, a alternativo rešenje je ograničenje broja ICMP echo zahteva.

5.2. Zaštita od štetnog delovanja lokalnih korisnika

Prilikom konfigurisanja firewalla najveća se pažnja posvećuje obradi dolaznih paketa. Danas sve više komercijalnih firewalla omogućava bolju kontrolu rada zaposlenih u kompaniji. Oni su konfigurisani na način da ne dozvoljavaju lokalnim korisnicima pristup određenim materijalima. To mogu biti porno web stranice, web stranice koje propagiraju mržnju, web stranice za skidanje raznih video i audio zapisa itd. Uzevši u obzir činjenicu da takve stranice sve češće nastaju, potrebno je osvežavati podatke unutar firewalla, tj. imati pretplatu kod distributera takvih informacija.

Organizacijama je danas veoma bitno da ograniče svojim zaposlenima preveliku slobodu na Internetu kako zaposleni ne bi naneli štetu ugledu organizacije posećivanjem određenih web stranica, ali i neobavljanjem posla za koji su zaduženi. Pri uvođenju restrikcija potrebno je paziti da se ne pretera sa ograničenjima, što bi moglo imati kontraefekat kod zaposlenih. Zaposleni bi u takvoj situaciji bili u nemogućnosti da pristupe materijalima koji im pomažu pri radu, ili bi takav tretman kod njih uzrokovao tzv. pasivni otpor prema radu.

Prilikom konfiguracije firewalla moguće je primeniti različita pravila ograničenja spajanja lokalnih korisnika na Internet. Prvi koncept bio bi da se prema svim korisnicima lokalne mreže jednako odnosi, tj. da su svi u istom položaju. Isto tako moguće je lokalne računare svrstati u klase zavisno od njihovih IP adresa. Na taj način moguće je samo jednom sektoru unutar organizacije omogućiti nesmetani pristup Internetu, a ostalim ograničen ili nikakav. Firewall može biti konfigurisan na način da propušta sve pakete osim paketa koji su usmereni prema računarima sa određenim IP adresama na Internetu. Na tim se računarima nalaze materijali koji nisu potrebni zaposlenima (porno materijali, audio zapisi, itd.). Moguće je primeniti i drugačiji princip filtriranja paketa. Propuštaju se paketi koji su namenjeni samo računarima koji imaju tačno definisane IP adrese, a svi ostali paketi koji dolaze sa lokalne mreže ne prosljeđuju se. Takav koncept mogu primeniti organizacije koje svojim zaposlenima dozvoljavaju pristup samo prema računarima na kojima se nalaze podaci bitni za rad zaposlenih.

6. IDS

Sistem za detekciju upada (IDS – intrusion detection system) je uređaj ili softverska aplikacija koja posmatra mrežu ili systemske aktivnosti tražeći maliciozne aktivnosti ili kršenja polisa i procedura, i pravi izveštaj na administratorskoj stanici (računaru). Neki sistemi mogu da pokušaju da spreče upad, ali to nije ni zahtevano niti neophodno od sistema koji je namenjen za posmatranje. Sistemi za detekciju i prevenciju upada (IDPS – intrusion detection and prevention systems) su primarno fokusirani na identifikaciju mogućih incidenata, loguju podatke o incidentu, i daju izveštaj o pokušajima upada. Organizacije koriste IDPS-ove za druge svrhe, kao što je identifikacija problema sa polisama bezbednosti, dokumentovanje postojećih pretnji i sprečavanje pojedinaca od kršenja polisa bezbednosti. IDPS-ovi su postali neophodni dodatak u bezbednosnoj infrastrukturi mreže gotovo svake organizacije.

IDPS-ovi obično snimaju podatke vezane za posmatrane događaje, obaveštavaju IT administratore vezano za važne događaje i prave izveštaje. Mnogi IDPS sistemi mogu da reaguju na detektovane pretnje tako što ih sprečavaju u uspevanju delovanja. Oni koriste nekoliko tehnika odgovora, koji uključuju da sam IDPS spreči napad, tako što menja okruženje bezbednosti (npr. rekonfigurisanje firewall podešavanja) ili menja sadržaj samog napada.

6.1. Pasivni i reakcioni sistemi

U pasivnom sistemu, IDS senzor detektuje potencijalni sigurnosni propust, čuva informaciju i daje upozorenje na konzolu i/ili vlasniku. Na reakcionom sistemu, takođe poznatom kao IPS (intrusion prevention system), IPS automatski reaguje na sumnjivu aktivnost tako što resetuje konekciju ili reprogramira firewall da blokira mrežni saobraćaj od malicioznog izvora.

6.2. Upoređenje sa firewall

Iako su oba vezana za mrežnu bezbednost, IDS se razlikuje od firewall-a u tome što firewall traži unapred napade kako bi ih sprečio. Firewall limitira pristup između mreža da bi se sprečio upad i ne daje signal (alarm) unutar mreže. IDS vrši evaluaciju upada kada se dogodi i daje signal. IDS takođe pazi na napade koji potiču iz samog unutrašnjeg sistema. Ovo se tradicionalno postiže tako što se posmatra mrežna komunikacija, identifikuju heuristike i šabloni (signatures) od čestih oblika napada na računare, i preuzima se akcija da se obavesti administrator. Sistem koji ukida konekcije naziva se IPS (intrusion prevention system) i on je drugi oblik aplikacionog sloja firewall-a.

7. IPS

Sistemi za prevenciju upada (IPS – Intrusion prevention systems), takođe poznati kao sistemi za detekciju i prevenciju upada (IDPS), su sistemi koji posmatraju mrežu i/ili systemske aktivnosti radi pronalaženja malicioznih aktivnosti. Glavna uloga sistema za prevenciju upada je da identifikuje maliciozne aktivnosti, zabeleži podatke o toj aktivnosti, pokuša da je blokira/zaustavi, i da je prijavi.

Sistemi za prevenciju upada se smatraju kao dodaci od sistema za detekciju upada zato što oba posmatraju mrežni saobraćaj i/ili systemske aktivnosti u potrazi za malicioznim aktivnostima. Glavna razlika između njih je to što sistemi za prevenciju upada se postavljaju direktno na liniju (in-line) i oni su u stanju da aktivno vrše prevenciju i/ili blokiranje upada koji se detektuju. IPS može da preduzme razne akcije kao što je slanje alarma za uzbunu, ukidanje malicioznih paketa, resetovanje konekcije i/ili blokiranje mrežnog saobraćaja sa IP adrese napadača. IPS takođe može da koriguje CRC greške, razfragmentira pakete protoka, spreči TCP probleme kod sekvenciranja, i da obriše neželjene opcije kod transporta i mrežnih slojeva.

7.1. IPS klasifikacije

Sistemi za prevenciju upada (IPS) mogu da se klasifikuju na četiri različita tipa:

1. Sistemi za prevenciju upada bazirani na mreži (NIPS – network-based intrusion prevention systems): posmatraju celu mrežu i traže sumljivi saobraćaj u mreži tako što analiziraju aktivnosti protokola.
2. Bežični sistemi za prevenciju upada (WIPS – wireless intrusion prevention systems): posmatraju bežičnu mrežu i traže sumljivi saobraćaj u bežičnoj mreži tako što analiziraju protokole bežičnih mreža.
3. Analiza ponašanja na mreži (NBA – network behavior analysis): posmatra mrežni saobraćaj da bi identifikovao pretnje koje generišu neobični protok u mreži, kao što je

distribuisano sprečavanje servisa (DDos) tip napada, neki oblici kršenja policy violations (kršenje pravila).

4. Host-zasnovani sistemi za prevenciju upada (HIPS – host-based intrusion prevention system): instalirani softverski paket koji posmatra pojedinačni host za sumljivim aktivnostima tako što analizira događaje koji se dešavaju unutar tog host-a.

7.2. Metode detekcije

Većina sistema za prevenciju upada koriste jedan od tri metoda detekcije (IDS metode): metod baziran na potpisu (signature-based), baziran na anomalijama (anomaly-based), baziran na analizi stanja protokola (stateful protocol analysis).

1. Detekcija bazirana na potpisu: IDS baziran na potpisu posmatra pakete na mreži i upoređuje sa ranije konfigurisanim i ranije definisanim šablonima napada poznatijim kao potpisi.
2. Detekcija bazirana na anomalijama: IDS baziran na anomalijama utvrđuje normalnu aktivnost na mreži kao što je tip protoka koji se obično koristi, koji protokoli se koriste, koji portovi i uređaji se obično povezuju jedan na drugi, i zatim upozoravaju administratora ili korisnika kada se detektuje saobraćaj u mreži koji nije normalan.
3. Detekcija bazirana na analizi stanja protokola: Ova metoda prepoznaje devijacije u stanjima protokola tako što upoređuje posmatrane eventove (događaje) sa ranije definisanim profilima generalno prihvaćenih definicija benignih aktivnosti.

8. Računarski virusi

Računarski virusi su vrsta malicioznih programa koji se razmnožavaju kada se pokrenu tako što ubacuju kopije samog sebe (sa mogućnostima modifikacije) u druge računarske programe, data fajlove, ili boot sektor na tvrdom disku. Kada dođe do uspešnog razmnožavanja, za obuhvaćene delove se kaže da su inficirani. Računarski virusi često obavljaju neku vrstu štetnog delovanja na inficiranim domaćinima, kao što je krađa prostora na tvrdom disku ili zauzimanje resursa procesora, pristupanje privatnim informacijama, korumpiranje podataka, prikazivanje na ekranu političkih ili humorističkih poruka, spamovanje korisnikovih kontakata, ili logovanje njihovih unosa sa tastature. Ali ipak nisu svi virusi destruktivnog karaktera, ili ne pokušavaju da sakriju sami sebe, tako da karakteristika koja definiše viruse je to da su oni računarski programi koji se sami instaliraju i razmnožavaju bez saglasnosti korisnika.

Programeri koji pišu viruse koriste socijalni inženjering i eksploatišu široko znanje o bezbednostnim propustima kako bi dobili pristup resursima na računarima domaćina. Velika većina računarskih virusa su pravljeni za operativne sisteme Microsoft Windows, angažujući niz mehanizama da bi se inficirali novi domaćini, i često koriste kompleksne strategije da izbegnu detekciju, kako bi izbegli antivirus programe. Motivi za pravljenje virusa mogu da budu želja za zaradom, želja da se pošalje neka poruka, lična razonoda, da se demonstrira da postoji bezbednosni propust u računarskom programu, za sabotazu i uskraćivanje usluga (denial of service), ili jednostavno iz same želje za istraživanjem.

Računarski virusi trenutno su uzrok ekonomske štete u vrednostima od više milijardi dolara svake godine, zato što izazivaju pad sistema, troše resurse računara, oštećuju podatke, povećavaju trošak održavanja, itd. Kao odgovor su razvijeni besplatni open-source antivirus alati, i multi milijarderska industrija komercijalnih antivirus programa je procvetala prodavajući antivirus zaštitu Windows korisnicima. Na žalost trenutno ne postoji ni jedan

antivirus program koji je u mogućnosti da pohvata sve računarske viruse (pogotovo one nove). Istraživači iz oblasti bezbednosti računara aktivno tragaju za načinima kako da omoguće antivirus programima da efikasnije pronalaze novonastale viruse, pre nego što se oni rasprostrane.



Slika 5 – Blaster Virus koji je ostavio poruku Bil Gejtsu, generalnom direktoru Microsoft kompanije

8.1. Vrste računarskih virusa

Nakon godina evolucije i razvijanja alata za zaštitu od virusa, i sve više stečenog znanja o njima od strane kompanija koje ih proizvode, virusi su podeljeni u sledeće osnovne kategorije:

- boot sektor virusi
- fajl virusi (file infectors)
- makro virusi
- Internet virusi

8.1.1. Boot sektor virusi

Boot sektor je deo diska koji sadrži kod za učitavanje operativnog sistema. Virus obriše sadržaj tog sektora i umesto programa za podizanje sistema snimi sebe. Ako se podigne sistem sa zaraženog diska, virus se aktivira i učitava se u RAM memoriju, odakle će zaraziti svaku disketu koja se od tog trenutka bude koristila (osim diskete koja je zaštićena od snimanja).

Boot sektor virusi inficiraju boot sektor flopi ili hard diska, a u mogućnosti su inficirati i Master Boot Record (MBR) korisničkog hard diska. Najčešće menjaju originalni sadržaj MBR-a sadržajem virusnog koda da bi se virus učitao u memoriju prilikom paljenja računara. Uklanjanje boot sektor virusa vrši se isključivo boot-ovanjem računara preko "čiste" systemske diskete ili CD-a koji sadrži alat za uklanjanje virusa.

8.1.2. Fajl virusi

Poznati i kao programski virusi, generalno se prenose preko fajlova koji su ili izvršni ili sadrže izvršne komponente fajlova i grupisani su prema klasama programa koje inficiraju. Mogu biti izuzetno infektivni i mnogo ih je teže otkriti nego viruse koji napadaju boot sektor zbog širokog obima potencijalnih meta. Mogu se podeliti na parazitne, pridružene, povezujuće i prepisujuće.

Svaki fajl virus može sadržati različite tehnike za poboljšanje brzine širenja ili za izbjegavanje otkrivanja.

Parazitni virusi

Čine većinu od svih fajl virusa i šire se tako što modifikuju kod izvršnog programa. Oni se kače na izvršni fajl i menjaju njegov sadržaj tako da se aktiviraju čim operativni sistem pokuša da izvrši inficirani program.

Pridruženi virusi

Koriste sistemske osobine DOS-a vezane za sekvencu učitavanja i izvršavanja programa. Oni ne modifikuju inficirani program i obično prolaze kontrolu originalnog EXE – fajla ali kada se jednom detektuju laki su za čišćenje.

Povezujući virusi

Inficiraju program tako što menjaju informaciju u strukturi direktorijuma i modifikuju pokazivače fajlova, tako da se svaki inficirani program startuje sa iste lokacije koja sadrži kod virusa.

Prepisujući virusi

Prepišu deo inficiranog fajla tako da on više nije operativan. To ih čini prilično primetnim, tako da se retko dešava da se daleko prošire.

8.1.3. Makro virusi

Macro virusi su mali programi napisani u nekom internom programskom jeziku (skript – language ili macro – language) nekog aplikativnog programa kao što je to WORD, EXCEL, itd. Ovi virusi su tipično pisani da se razmnožavaju unutar dokumenata kreiranih tom aplikacijom. Mogu se proširiti i na druge računare ukoliko se na oba računara koristi napadnuta aplikacija i vrši se razmena inficiranih dokumenata. Makro virusi mogu se izvršavati na svakoj platformi na kojoj postoji ovakav program (i pripadajući interni jezik). Oni nisu ograničeni na pojedinačne računare ili samo određeni operativni sistem.

8.1.4. Internet virusi

E-mail virus se kreće u sklopu e-mail poruka i najčešće se razmnožava automatski putem adresa koje se nalaze u adresaru (Address Book). Najpoznatiji virus ovog tipa bio je virus Mellisa iz marta 1999. godine. Širio se uz pomoć MS Word dokumenata poslatih putem e-maila. Nastao je tako što je neko na Internet news grupu presnimio Word dokument. Ko je god kopirao i otvorio dokument, povukao je i virus. Virus je inficirao Noral.dat datoteku i prilikom slanja uzimao je prvih 50 adresa i slao im je inficirani dokument. Nakon virusa Melissa, virus I love you se pojavio u maju 2000. godine i sadržao je mali deo koda i zakačku za e-mail. Virus se izvršavao dvostrukim klikom na zakačku. Ceo koncept bio je baziran na ljudskoj radoznalosti, neopreznosti i želji da se pregleda "ljubavna poruka".

9. Worm (crv) i trojanski konj

9.1. Worm - crv

Worm je mali računarski program koji koristi računarsku mrežu i sigurnosne propuste da se razmnoži sa računara na računar. Najčešći način širenja crva je putem e-maila. Kao uslov za razmnožavanje neophodna je računarska mreža (obično Internet). Koristeći se njom, program pretražuje mrežu i pronalazi računare sa specifičnim sigurnosnim propustima. Dalje se crv sam kopira na drugi računar, sve dok ne bude otkriven i uklonjen. Postoje dvije vrste crva: crv na domaćinskom, odnosno host računaru (HOST WORM) i mrežni crv (NETWORK WORM).

HOST WORM se celokupan nalazi i izvršava na host računaru, a vezu s mrežom koristi samo za svoje razmnožavanje na druge računare. Ovaj tip crva nakon što pokrene svoju kopiju na novom inficiranom računaru samostalno uništava svoju prvobitnu kopiju. Na taj način u određenom trenutku negde na mreži uvek se nalazi samo jedna kopija tog crva. Ovaj tip crva naziva se još i "zec" (RABBIT) upravo zato što stalno beži naokolo mrežom.

NETWORK WORM sastoji se od više delova, segmenata, od kojih se svaki pokreće na različitom računaru u mreži i najčešće svaki segment obavlja različitu funkciju koristeći mrežu samo za određene svrhe komunikacije. Mrežni crv koji ima jedan glavni segment koji koordinira radom ostalih segmenata na mreži naziva se još i "hobotnicom" (OCTOPUS). 19. jula 2001. godine pojavio se worm Code Red koji se za nepunih devet sati namnožio 250.000 puta. Napao je Windows platformu, i to NT i 2000 servere na kojima su se "vrteli" Internet Information Server-i. Karakteristika crva je da pored standardne replikacije, nanose dodatnu štetu. Code Red se namnožio prvih 20 dana u mesecu, menjao sadržaj web sajtova na inficiranim serverima stranicom pod nazivom Hacked by Chinese. Code Red je usporavao Internet saobraćaj kada bi se razmnožavao. Svaka kopija proverava da li WINDOWS NT ili WINDOWS 2000 server ima instalisanu sigurnosnu zakrpu i ukoliko ustanovi da nema, kopira se na njega. Ta nova kopija radi isto što i original, sve dok ne bude otkrivena i uklonjena.

9.2. Trojanski konj

Trojanci su svoje ime dobili prema čuvenom epu o opsadi Troje, koju su grci bezuspešno napadali 10 godina i na kraju se povukli ostavljajući pred njenim ulazom ogromnog konja kao znak priznavanja poraza. Trojanski ratnici su oduševljeno konja uvukli unutar grada i posvetili su se proslavljanju svoje velike pobjede. Međutim, kada su svi zaspali pijani, na konju su se otvorila dobro skrivena vrata i iz njega je izašao odred grčkih ratnika koji su otvorili vrata tvrđave, puštajući unutra ostale grke, koji su iscenirali povlačenje i čekali na pravi trenutak. Nakon toga Troju su veoma lako zauzeli. Potpuno je pogrešno trojance zvati virusima, zato što su oni kompletne aplikacije i ne šire se kao virusi. Trojanski konji se mogu ukloniti brisanjem njihovog fajla iz određenog direktorijuma, za razliku od virusa koji su obično zakačeni za druge datoteke i ubacuju se u memoriju. Većina njih nije sama po sebi destruktivna ali zato omogućuje bilo kome na Internetu da upravlja zaraženim računarom ili mu šalje njegove lozinke itd., tako da to kolika će šteta biti naneta zavisi samo od onoga ko se domogao podataka.

Računarski trojanski konj pod maskom stiže putem e-maila, news grupe ili popularnih chat programa do lakovernih i nedovoljno informisanih korisnika mreže, navodeći ih da ga pokrenu i instaliraju na računar. Za razliku od virusa, trojanci su kompleksne klijent-server aplikacije za pristup udaljenom računaru u mreži. Server se nalazi na računaru žrtve i to je

sam trojanac, dok je klijent program pomoću koga se njime upravlja. Klijent se nalazi na računaru osobe koja namerava da dođe do bitnih informacija sa računara žrtve. Zadatak trojanca je da pronalazi datoteke koje sadrže šifre potrebne za instaliranje na računar, server ili konektovanje na Internet i distribuira ih udaljenom hakeru. Osoba koja kontroliše trojanca na računaru žrtve u mogućnosti je potpuno preuzeti kontrolu nad njim. U tom trenutku jedino rešenje je fizičko gašenje računara ili nasilni prekid Internet konekcije. Trojanci su u mogućnosti dobro sakriti kod i iskoristiti mnoštvo sigurnosnih propusta u e-mail klijentima. Većina trojanaca instalira se u Start Up grupu Windows-a. Pregledanje tog foldera može pouspešiti zaštitu računara. Najefikasniji način zaštite od trojanaca je instaliranje firewall sistema ili jednostavno ne otvaranje poruka od nepoznatih osoba.

Najpoznatiji trojanac je svakako Back Orifice, koga je samo za mesec dana preuzelo i koristilo skoro 100.000 ljudi na Internetu. On izgleda kao obična klijent-server aplikacija za rad na udaljenom računaru sa izuzetkom što se server, tj. sam trojanac, instalira bez pitanja, kao virus, kada startujete zaraženu aplikaciju i omogućava svakome ko dođe do IP adrese da preuzme kontrolu nad računarom. Pored BO-a poznati su još NetBus, Millenium itd.

10. Hronološki raspored nastanka računarskih virusa i crva

10.1. 1970.-1979. godina

10.1.1. 1971. godina

Creeper sistem, eksperimentalni program koji se sam razmnožava, je napisao Bob Thomas na BBN Technologies. Creeper je napadao DEC PDP-10 računare koji su koristili TENEX operativni sistem. Creeper je dobio pristup preko ARPANET-a i kopirao je sam sebe na udaljeni sistem gde je prikazana poruka „I'm the creeper, catch me if you can!“ (ja sam puzavac, uhvati me ako možeš!).

10.1.2. 1974. godina

Rabbit (ili Wabbit) virus je napisan. Rabbit virus pravi više kopija samog sebe na pojedinačnom računaru (I nazvan je Rabbit – Zec zbog brzine razmnožavanja) sve dok ne zaguši sistem, umanjujući performanse računara, dok na kraju ne dođe do krajnje granice i sruši sistem.

10.1.3. 1975. godina

April: ANIMAL (životinja) je napisan od strane John Walker-a za UNIVAC 1108. ANIMAL je postavio niz pitanja za korisnika u nameri da pogodi o kojoj životinji korisnik razmišlja, dok sličan program PERVADE pravi kopije sam sebe i ANIMAL-a u svaki direktorijum na koji korisnik ima pristup. On se širi preko multi-korisničkih UNIVAC-ova kada korisnik sa preklapajućim privilegijama pokrene igricu, a na druge računare kada se dele trake. Program je pažljivo napisan da bi se izbegla šteta na postojeće fajlove i direktorijume, i da se ne kopira ukoliko privilegije ne postoje ili ako bi mogla da usledi nekakva šteta. Njegovo širenje je na taj način zaustavljeno zakrpom za operativni sistem koja je promenila format od tabela statusa fajlova koji je PERVADE koristio za bezbedno kopiranje. Iako nije maliciozan, „Prežimajuća životinja“ predstavlja prvi trojanski konj.

10.2. 1980.-1989. godina

10.2.1. 1982. godina

Program nazvan Elk Cloner, napisan za Apple II sisteme, je napravljen od strane Richard-a Skrenta. Apple II je viđen kao naročito ranjivi operativni sistem zato što je lociran na floppy disketi. Elk Cloner-ov dizajn u kombinaciji sa javnim ignorisanjem o tome šta malware predstavlja i kako se odbraniti od toga, dovelo je do toga da je Elk Cloner postao odgovoran za prvi široko rasprostranjeni računarski virus u istoriji.

10.2.2. 1983. godina

Novembar: Terminologiju virus je smislio Frederick Cohen u opisivanju samorazmnožavajućih računarskih programa. 1984. godine Cohen koristi frazu računarski virus (po sugestiji njegovog učitelja Leonard Adleman-a) da definiše operacije kao što su programi vezani za infekciju računara. On definiše virus kao program koji može da inficira druge programe tako što ih modifikuje da sadrže moguću kopiju samog sebe. Cohen demonstrira program koja je sličan virusu na VAX11/750 sistemu u Lenigh University. Program je bio u mogućnosti da instalira sam sebe na, ili inficira, druge objekte u sistemu.

Veoma stari trojanski konj napravljen za IBM računare nazvan ARF-ARF je preuzet sa web sajta BBS-a i tvrdilo se da sortira direktorijume DOS disketa. Ovo je bila veoma poželjna mogućnost zato što DOS nije izlistavao sve fajlove po alfabetskom redu u 1983. godini. Umesto toga, program je brisao sve fajlove na disketi, ispraznio zapise na ekranu i dao prikaz ARF-ARF. ARF je bila referenca za čestu poruku "Abort, Retry Fail" koja se mogla videti kada računar nije bio u mogućnosti da se podigne.

10.2.3. 1984. godina

Avgust: Ken Thompson objavljuje svoj seminarski rad, Reflections on Trusting Trust, u kojem opisuje kako je modifikovao C kompajler tako da kada se koristi da kompajlira specifičnu verziju Unix operativnog sistema, on ubacuje backdoor na login komandu, i kada se koristi da kompajlira samog sebe, koristio je backdoor kod za ubacivanje čak iako ni backdoor ni backdoor kod za ubacivanje nisu prisutni u izvornom kodu.

10.2.4. 1986. godina

Januar: The Brain boot sektor virus je napravljen. Brain je smatran prvim IBM računarski kompitabilnim virusom i program odgovoran za prvu IBM epidemiju računarskih virusa. Ovaj virus je takođe poznat kao Lahore, Pakistani, Pakistani Brain, i Pakistani flu, jer je napravljen u mestu Lahore, Pakistan od strane devetnaestogodišnjeg Pakistanskog programera Basit Farooq Alvi i njegovog brata Amjad Farooq Alvi.

Decembar: Ralf Burger je prezentovao Virdem model programa na mitingu nelegalnih Chaos Computer Club u Nemačkoj. Virdem model predstavlja prve programe koji su mogli da se umnožavaju sami putem dodatka njihovog koda u izvršne DOS fajlove u COM formatu.

10.2.5. 1988. godina

Mart: Ping-Pong virus (takođe poznat kao Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A ili VeraCruz) je MS-DOS boot sektor virus, koji je napravljen na Univerzitetu u Turinu, u Italiji.

Jun: CyberAIDS i Festering Hate Apple ProDOS virusi se šire putem nelegalnih piratskih BBS sistema i počinju da inficiraju mainstream mreže. Festering Hate je bio poslednje ponavljanje od CyberAIDS serija virusa gledajući unazad od 1985. do 1986. godine. Za razliku od nekoliko Apple virusa koji su došli prethodno i koji su u suštini samo bili uznemiravajući za korisnika, ali nisu pravili nikakvu štetu, Festering Hate serija virusa je bila veoma destruktivne prirode, šireći se na sve systemske fajlove koje je mogao da pronađe na host računaru (hard disk, flopi disk i systemska memorija) i nakon toga uništava sve nakon što više ne može da pronađe inficirane fajlove.

Novembar: Morris worm (crv), napravljen od strane Robert Tappan Morris-a, inficira DEC VAX i Sun mašine koje pokreće BSD UNIX, koji su povezani na internet, i samim tim postaje prvi crv koji se brzo širi i jedan od prvih dobro poznatih programa koji eksploatiše buffer overrun slabosti.

10.2.6. 1989. godina

Oktobar: Ghostball, prvi multipartitni virus, je napravljen od strane Fridrik Skulason-a. On napada izvršne .COM fajlove i boot sektor na MS-DOS sistemima. On hvata određene podatke koji su uneseni ili sačuvani od strane korisnika, specifične fajlove ili generalno podatke, utiče na performanse računara, mrežu na koju je računar povezan ili na druge udaljene sajtove, smanjuje nivo bezbednosti računara, ali se ne širi sam automatski.

10.3. 1990.-1999. godina

10.3.1. 1990. godina

Mark Washburn radi na analizi virusa Vienna i Cascade i sa Ralf Burger-om izrađuje prvu familiju polimorfnih virusa: Chameleon familiju. Chameleon serija virusa je debitovala sa izlaskom izdanja 1260.

10.3.2. 1992. godina

Mart: Smatralo se za Michelangelo virus da će napraviti digitalnu apokalipsu 6. marta, zbog više miliona računara za koje se smatralo da će im podaci biti očišćeni po masovnoj histriji koja se stvara zbog virusa. Kasnije procene štete su pokazale da je šteta minimalna. John McAfee je rekao za medije da će 5 miliona računara biti inficirano. Kasnije je rekao da je bio pod pritiskom novinara da smisli broj i ispravio se da će raspon biti između 5 hiljada i 5 miliona inficiranih računara.

10.3.3. 1993. godina

Leonardo ili Leonardo & Kelly i Freddy Krueger virusi se šire brzo zbog popularnosti BBS i shareware distribucija.

10.3.4. 1994. godina

April: Javlja se OneHalf koji je polimorfni računarski virus zasnovan na DOS-u.

10.3.5. 1995. godina

Prvi Macro virus, nazvan Concept, je napravljen. Napadao je Microsoft Word dokumente.

10.3.6. 1996. godina

Ply-DOS 16 bit zasnovani komplikovani polimorfni virus se pojavio sa ugrađenim permutacijskom mašinom.

10.3.7. 1998. godina

Jun: Javlja se prva verzija CIH virusa. Bio je to prvi poznati virus koji je mogao da obriše sadržaj BIOS-ovog fleš ROM-a.

10.3.8. 1999. godina

Januar: Happy99 crv se pojavio. On sam sebe nevidljivo kači na email-ove, prikazuje vatromet da sakrije promene koje se prave, a zatim poželi korisniku srećnu novu godinu. Modifikuje sistemske fajlove vezane za Outlook Express i Internet Explorer na Windows 95 i Windows 98.

Mart: Melissa crv je napravljen, koji cilja Microsoft Word i Outlook bazirane sisteme, a zatim pravi veliko mrežno opterećenje.

Jun: ExploreZip crv, koji uništava Microsoft Office dokumente, je prvi put detektovan.

Decembar: Kak crv je crv koji cilja Javascript računare i koji širi sam sebe tako što iskorištava grešku u Outlook Express-u.

10.4. 2000.-2009. godina

10.4.1. 2000. godina

Maj: ILOVEYOU crv, takođe poznat kao ljubavno pismo, ili VBS, ili Love Bug worm, je računarski crv navodno napravljen od strane studenta informatičkih nauka sa Filipina. Napisan u VBScript, inficirao je milione Windows računara širom sveta samo nekoliko sati nakon što je pušten. Smatra se da je to jedan od najdestruktivnijih crvova ikada.

Jun: Pikachu virus se smatra da je prvi računarski virus čija su ciljana grupa deca. On sadrži karaktera Pikaču iz Pokemon serija, a nalazi se u formi email-a sa naslovom „Pikachu Pokemon“ sa porukom: „Pikachu is your friend.“. Zakačka na email-u ima sliku sa zamišljenim Pikačuom sa porukom koja glasi: „Među milionima ljudi na svetu ja sam pronašao tebe. Nemoj zaboraviti da stalno pamtiš ovaj dan MOJ PRIJATELJU“. Zajedno sa slikom nalazi se program, napisan u Visual Basic 6, nazvan pikachupokemon.exe koji modifikuje AUTOEXEC.BAT fajl i dodaje komandu za uklanjanje sadržaja direktorijuma C:\Windows i C:\Windows\System nakon što se računar restartuje. Operativni sistemi koje je ovaj virus obuhvatao su Windows 95, Windows 98 i Windows Me.

10.4.2. 2001. godina

Februar: Anna Kournikova virus napada email servere tako što šalje email kontakte u Microsoft Outlook adresaru. Njegov kreator, Holanđanin Jan de Wit, je dobio kaznu od 150 sati rada za zajednicu.

Maj: Sadmin crv se širi tako što eksploatiše rupe u Sun Solaris-u i Microsoft IIS.

Jul: Sicram crv je pušten u upotrebu, šireći se kroz Microsoft sisteme putem email-a i nezaštićenih deljenja preko mreže.

Code Red crv napada Index Server ISAPI Extension u Microsoft-im Internet Information Services.

Avгуст: Potpuno prepravljeni Code Red crv, Code Red II, počinje da se agresivno širi na Microsoft sisteme, uglavnom u Kini.

Septembar: Nimda crv je pronađen i on se širi na više načina uključujući slabosti u Microsoft Windows i backdoor-ima ostavljenim od strane Code Red II i Sadmin Worm.

Oktobar: Klez crv je pronađen. On eksploatiše ranjivosti u Microsoft Internet Explorer-u, Microsoft Outlook i Outlook Express-u.

10.4.3. 2002. godina

Februar: Napisan je Simile virus koji je metamorfičan računarski virus.

Beast je Windows-baziran backdoor trojanski konj, više poznatiji kao RAT (alat za udaljeno upravljanje). On je sposoban da napadne gotovu svaku verziju Windows-a. Napisan je u Delphi programskom jeziku i pušten na internet od strane autora Tataye, njegova najnovija verzija je puštena 3. oktobra 2004. godine.

Mart: Mylife je računarski crv koji širi sam sebe tako što šalje maliciozne email-ove svim kontakima u Microsoft Outlook.

Avгуст: Optix Pro je podesiv alat za upravljanje na daljinu ili trojanski konj, sličan SubSeven-u ili BO2K.

10.4.4. 2003. godina

Januar: SQL Slammer crv, poznat i kao Sapphire crv, Helkern itd., napada putem ranjivosti na Microsoft SQL Server-ima i MSDE, postaje jedan od crva koji se najbrže širi u istoriji virusa, zaustavljen je 15 minuta nakon što je pušten.

April: Graybird je trojanski konj takođe poznat kao Backdoor.Graybird.

Jun: ProRat je Turski backdoor trojanski konj napisan za Microsoft Windows, više poznatiji kao RAT (alat za udaljeno upravljanje).

Avгуст: Blaster crv, poznat i kao Lovesan crv, brzo se širi tako što iskorištava slabosti u sistemskim servisima prisutnim na Windows računarima.

Welchia (Nachi) crv je pronađen. Crv pokušava da ukloni Blaster crva i da patch-uje Windows.

Sobig crv (tehnički Sobig.F worm) se brzo širi kroz Microsoft sisteme putem email-a i mrežnih deljenja.

Septembar: Nastaje Swen računarski crv napisan u C++ programskom jeziku.

Oktobar: Sober crv je prvi put pronađen na Microsoft sistemima i zadržava svoju prisutnost sve do 2005. godine sa mnogo novih varijanti. Istovremeni napadi na slabe tačke na mreži od strane Blaster i Sobig crva izaziva masovnu štetu.

Novembar: Agobot je računarski crv koji može da se širi tako što iskorištava slabosti u Microsoft Windows-u. Neke od slabosti su MS03-026 i MS05-039.

Bolgimo je računarski crv koji se širi tako što iskorištava buffer overflow slabosti na Microsoft Windows-ovom DCOM RPC interfejsu.

10.4.5. 2004. godina

Januar: Bagle je crv koji se širi putem masovnog mailing-a i napada sve verzije Microsoft Windows-a. Postojale su dve varijante Bagle crva, Bagle.A i Bagle.B.

L10n crv (obično se izgovara kao lion – lav) je bio Linux crv koji se širio tako što je iskorištavao buffer overflow na BIND DNS serveru. Bio je baziran na starijem crvu poznatim

kao Ramen crv koji je napisan da napada sisteme koje pokreće verzija 6.2 i 7.0 Red Hat Linux distribucija.

MyDoom crv nastaje i trenutno drži svetski rekord kao masovni mailing crv koji se najbrže širi.

Februar: Netsky crv je pronađen. Crv se širi putem email-a i tako što kopira sam sebe na foldere na lokalnom hard disku kao i na mapiranim mrežnim folderima ako su dostupni. Mnogo varijanti od Netsky crva su se pojavili.

Mart: Witty crv je crv koji obara rekorde po mnogim kriterijumima. On je iskorištavao rupe u nekoliko Internet Security Systems (IIS – sistemi za internet bezbednost) proizvodima. Bilo je to najbrže obelodanjivanje jednog crva, bio je to prvi internet crv koji nosi sa sobom destruktivni kod i širio se brzo upotrebom prethodno napravljenih lista ground-zero hostova.

Maj: Sasser crv se širi tako što iskorištava bezbednosni propust u Microsoft Windows LSASS servisu i izaziva probleme u mreži, dok uklanja MyDoom i Bagle varijante, čak i prekida obavljanje poslova.

Jun: Caribe ili Cabir je računarski crv koji je napravljen da napade mobilne telefone koji koriste Symbian operativni sistem. To je prvi računarski crv koji je mogao da inficira mobilne telefone. Širio se putem bluetooth-a.

Avgust: Nuclear RAT (skraćenica od nuklearni alat za udaljenu administraciju) je backdoor trojanski konj koji inficira Windows NT sisteme (Windows 2000, Windows XP, Windows 2003).

Vundo, ili Vundo Trojan (takođe poznat kao Virtumonde ili Virtumondo i ponekad nazvan MS Juan) je trojanski konj poznat po tome što izbacuje popup-ove i reklame za anti-spyware programe, i povremene degradacije u performansama računara ili denial of service (odbijanje usluge) sa nekim web sajtovima uključujući Google i Facebook.

Oktobar: Bitfrost, takođe poznat kao Bitfroze, je backdoor trojanski konj koji može da inficira Windows 95 preko Viste. Bitfrost koristi tipični server, server builder, i klijent backdoor programsku konfiguraciju da dozvoli daljinski napad.

Decembar: Santy, prvi poznati webworm (web crv) je pušten. On je iskorištavao bezbednosne propuste u phpBB i koristio je Google da pronađe nove mete. Inficirao je oko 40000 web prezentacija pre nego što je Google uspeo da isfiltrira rezultate pretrage koje je koristio crv, i tako ga sprečio da se širi.

10.4.6. 2005. godina

Avgust: Zotob

Pred kraj 2005. godine: Zlob Trojan je trojanski konj koji se maskira kao neophodni video codec u formi Microsoft Windows ActiveX komponente. Prvi put je detektovan pred kraj 2005. godine.

Bandbook ili Bandbook Rat (Bandbook alat za udaljenu administraciju) je backdoor trojanski konj koji inficira Windows operative sisteme. On korisiti kreator servera, klijenta i server da preuzme kontrolu nad udaljenim računarom. Koristi proces hijacking/kernel pečovanje da zaobiđe firewall i dozvoljava da serverska komponenta ukrade procese i pribavi privilegije za pristup internetu.

10.4.7. 2006. godina

Januar: Nyxem crv je pronađen. On se širio preko masovnog mailing-a. Njegov sadržaj, koji se aktivira trećeg dana svakog meseca, počevši trećeg februara, pokušava da ukloni bezbednosne softvere i softvere za mrežno deljenje fajlova, i da uništi fajlove određenog tipa, najčešće Microsoft Office fajlove.

Februar: Pronađen je prvi malware za Mac OS X, trojanski konj koji nije mnogo opasan poznat kao OSX/Leap-A ili OSX-Oompa-A.

Mart: Brontok varijanta N je pronađena krajem marta. Brontok je bio masovni e-mail crv i on potiče iz Indonezije.

Septembar: Stration ili Warezov crv je prvi put pronađen.

10.4.8. 2007. godina

Januar: Storm Worm je identifikovan kao crv koji se brzo širi i predstavlja veliku pretnju spamovanjem za Microsoft sisteme. On započinje da sakuplja inficirane računare na Storm botnet. Do 30. juna inficirao je 1.7 miliona računara i kompromitovao je bezbednost između 1 i 10 miliona računara do septembra. Smatra se da potiče iz Rusije i on je maskirao sebe kao dodatak za email u obliku novosti koje sadrže snimak o prividnim novostima koje traže od korisnika da preuzme dodatak za koji se misli da je u pitanju snimak.

Jul: Zeus je trojanski konj koji napada Microsoft Windows sa ciljem da pokupi bankarske informacije tako što prikuplja, odnosno loguje, unose sa tastature.

10.4.9. 2008. godina

Februar: Mocmex je trojanski konj koji je pronađen u digitalnom foto frejmu. To je bio prvi ozbiljni računarski virus koji se nalazio na digitalnom foto frejmu. Virus se smatra da potiče od jedne grupe hakera iz Kine.

Mart: Torpig. Takođe poznat kao Sinowal i Mebroot, je trojanski konj koji napada windows tako što gasi antivirus programe. On dozvoljava drugima da pristupe računaru, modifikuje podatke, krađe poverljive informacije (kao što su korisničke šifre i ostali osjetljivi podaci) i instalira još više malware-a na inficirani računar.

Maj: Rustock.C, poznati spambot tip malware-a sa naprednim rootkit sposobnostima, je detektovan na Microsoft sistemima i analiziran, ali se smatra da je bio nepronaden još od oktobra 2007. godine.

Jul: Bohmini.A je alat za udaljenu kontrolu nad računarom ili trojanski konj koji iskorištava bezbednosne propuste u Adobe Flash 9.0.115 sa Internet Explorer-om 7.0 i Firefox-om 2.0 na Windows XP SP2 operativnom sistemu.

Koobface računarski crv cilja korisnike na Facebook i MySpace. Nove varijante se konstantno pojavljuju.

Novembar: Računarski crv Conficker je inficirao između 9 i 15 miliona Microsoft server sistema koji pokreću sve od Windows 2000 pa do Windows 7 Beta. Francuska Mornarica, Englesko Ministarstvo Odbrane, Sheffield bolnička mreža, Nemački Bundeswehr i Norveška Policija su bili napadnuti. Microsoft je objavio da nagrada od 250,000 dolara pripada onome ko da informaciju koja će dovesti do hapšenja hakera koji su napravili tog crva. Pet glavnih varijanti Conficker crva su nazvani Conficker A, B, C, D i E. Oni su pronađeni 21. novembra 2008. godine, 29. decembra 2008. godine, 20. februara 2009. godine, 4. marta 2009. godine i 7. aprila 2009. godine. Na 16. decembar Microsoft je objavio KB958644 patch za serverske servise preko kojih se širio Conficker.

10.4.10.2009. godina

Jul: 2009 u julu su se pojavili cyber napadi i W32.Dozer napda Sjedinjene Američke Države i Južnu Koreju.

Symematec otkriva Daprosy crva. Smatra se da ovaj trojanski crv ima nameru da ukrade šifre od online igrica u internet igraonicama. Mogao je da presretne sve unose sa tastature i pošalje ih autoru virusa što predstavlja veliku pretnju za B2B sisteme.

10.5. 2010. godina i posle

10.5.1. 2010. godina

Januar: Botnet nazvan Waledac je slao spam email-ove. U februaru 2010., međunarodna grupa istraživača bezbednosti i Microsoft su srušili Waledac.

Februar: Microsoft objavljuje da je Alueron trojanski konj napravio BSoD problem na nekim Windows računarima preko batch fajla Patch Tuesday koji služi za ažuriranje.

Jun: Stuxnet, Windows trojanski konj, je pronađen. To je prvi crv koji napada SCADA sisteme. Postoje spekulacije da je napravljen da napada Iranske nuklearne elektrane. Koristi validan sertifikat od Realtek-a.

Septembar: here you have ili VBMania je jednostavan trojanski konj koji stiže u sanduče preko email-a sa naslovom "here you have". Telo poruke ispisuje: „This is The Document I told you about, you can find it Here“ ili „This is The Free Download Sex Movies, you can find it Here“.

Kenzero virus se širi online preko P2P (peer to peer) sajtova i uzima istoriju pretraživanja od računara.

10.5.2. 2011. godina

SpyEye i Zeus spojeni kod se vidi. Nove varijante napadaju podatke od mobilnog bankarstva. Anti-Spyware 2011 je trojanski konj koji napada Windows 9x, 2000, XP, Vistu i Windows 7, predstavljajući se kao anti-spyware program. On zapravo gasi bezbednosne procese antivirusa programa i takođe blokira pristup internetu što sprečava njihovo ažuriranje.

Leto 2011: Morto crv pokušava da se proširi na više računara preko Microsoft Windows Remote Desktop Protocol (RDP). Morto se širi tako što tera inficirani sistem da skenira Windows servere i dopusti RDP login. Kada Morto pronađe RDP-pristupačan sistem, on pokušava da se uloguje na domen ili lokalni sistemski nalog nazvan Administrator upotrebom više šifara koje se često koriste. Detaljni pregled kako ovaj crv funkcioniše kao i listu šifara koje koristi kada pokušava da se uloguje, obavila je Imperva.

Jul: ZeroAccount rootkit (takođe poznat kao Sirefef ili max++) je pronađen.

Septembar: Duqu je crv koji se smatra da je povezan sa Stuxnet crvom. Laboratorija Kriptografije i Bezbednosti Sistema (CrySyS Lab) u Budimpeštanskom Univerzitetu za Tehnologije i Ekonomiju u Mađarskoj je pronašla ovu pretnju, analizirali su malware, i napisali izveštaj od 60 strana i nazvali pretnju Duqu. Duqu dobija svoje ime zbog prefiksa „~DQ“ koje daje fajlovima koje sam napravi.

10.5.3. 2012. godina

Maj: Flame takođe poznat kao Flamer, sKyWIper i Skywiper je modularni računarski malware pronađen u 2012. godini i on napada računare koji koriste Microsoft Windows. Program je upotrebljen za ciljanu cyber špijunažu u zemljama Bliskog Istoka. Njegovo otkriće je objavljeno 28. maja od strane MAHER Centra Iranskog Nacionalnog Tima za Urgentne Računarske Odgovore (CERT), Kaspersky Lab i CrySyS Lab od Budimpeštanskog Univerziteta Tehnologije i Ekonomije. CrySyS je objavio u svom izveštaju: „sKyWIper je

definitivno najnapredniji malware koji smo sreli tokom našeg rada, čak se smatra i da je najkompleksniji malware ikada pronađen”.

Avugust: Shamoon je računarski virus dizajniran da cilja računare koji koriste Microsoft Windows u energetsom sektoru. Symantec, Kaspersky Lab i Seculert su objavili njegovo otkriće avgusta 16. 2012. godine.

Septembar: NGRBot je crv koji koristi IRC mrežu za prenos fajlova i tako šalje i prima komande između zombi mrežnih mašina i napadačevog IRC servera, i posmatra i kontroliše mrežnu povezanost i presreta je. On koristi korisnički-mod rootkit tehnike da sakrije i ukrade podatke od žrtve. Ova porodica botova je takođe napravljena da inficira HTML stranice sa ifrejmovima, izazivajući redirekcije, blokira žrtve da dobiju najnovije definicije za svoje bezbednosne/antivirus programe, i ubija te servise. Bot je napravljen da se poveže preko predefinisano IRC kanala i komunicira sa udaljenim botnetom.

10.5.4. 2013. godina

April: CryptoLocker trojanski konj je pronađen. CryptoLocker šifruje fajlove na korisnikovom hard disku, zatim traži od korisnika otkupninu koju treba da plati hakeru koji ga je napravio, kako bi dobio ključ za dešifrovanje i tako ovo postaje prvi na svetu pravi ransomware (virus koji traži otkupninu).

11. Antivirus programi

Predstavljaju prvi nivo zaštite od virusa i trojanaca. To su softverski paketi sposobni da detektuju, izdvoje i (ili) eliminišu viruse. Svi antivirusni programi sastoje se iz više celina. Jedan njegov deo "Monitor" je rezidentan u memoriji i osigurava neprestanu zaštitu od virusa, dok drugi deo "Scan" omogućava skeniranje celog sistema.

Antivirusi su danas neophodan deo softvera koji svaki klijent treba imati instaliran na svom računaru, a pogotovo kada se radi o ozbiljnim računarskim mrežama. Ovi programi uključuju različite načine nadgledanja i zaštite računara od malicioznog koda. Najčešće se radi o zaštiti u realnom vremenu i skeniranju na zahtev korisnika, dok moderne verzije ovih programa nude razne druge vidove zaštite od virusa koji se šire putem Interneta.

Postoji dosta kompanija koje razvijaju i nude ove programe, a najpoznatiji među njima su: Symantec, Eset, Panda, Kaspersky itd. One nude dopunu i ažuriranje antivirusnih definicija svakodnevno. Dosadašnja praksa bazirala se na petnaestodnevnom osvežavanju. Broj danas poznatih virusa je oko 65.000, s tim da se opasnim smatra nekoliko stotina. Kvalitetna zaštita svodi se na opreznost, upotrebu dobrih antivirusnih programa, redovno osvežavanje virusnih definicija.

11.1.1. Vrste antivirus programa

Najpoznatiji i najčešće korišćeni antivirusni programi su:

- Eset NOD32 antivirus
- Norton antivirus
- McAfee antivirus
- Bitdefender antivirus
- Kaspersky antivirus

11.2. Antivirus metode rada

11.2.1. Skeneri

Princip rada antivirus skenera bazira se na proveravanju datoteka, sektora i sistemske memorije u potrazi za poznatim i nepoznatim malicioznim kodom. Potraga za poznatim virusima naziva se maskiranje (masking). Virus "maska" je specifični deo koda sadržan u virusu. Ako neka datoteka ne sadrži masku (taj deo koda) ili je veličina maske nedovoljna, koriste se druge metode za pronalaženje virusa.

Heurističko skeniranje je analiza dela instrukcija u kodu datoteka koje se proveravaju, za koje postoji mogućnost da je maliciozni kod. Na ovaj način pronalaze se još uvek neotkriveni virusi.

Skeneri se dele u dve kategorije: opšti (general) i specijalni (special). Generalni skeneri su dizajnirani da pronađu i onemoguće sve vrste virusa za određeni tip operativnog sistema dok specijalni pronalaze ograničen broj virusa ili određene tipove virusa, recimo makro viruse. Skeneri se još dele na rezidentne i nerezidentne (proveravaju sistem samo ako se to traži od njih). Rezidentni pružaju sistemu bolju zaštitu, jer reaguju odmah po pojavi virusa, dok nerezidentni detektuju virus tek kad bude pokrenut.

11.2.2. CRC skeneri

CRC skeneri deluju tako što računaju sa CRC sumama za disk, datoteku ili sistem sektora. CRC sume sadrže bazu podataka sa podacima kao što su veličina datoteka, datum i sl. Oni upoređuju informaciju sa bazom i kontrolišu vrednosti. Ako su podaci u bazi različiti od onih koje je skener pronašao, ukazuje na mogućnost postojanja virusa na računaru.

CRC skeneri koriste moćne anti-stealth algoritme u borbi protiv virusa i često se zna desiti da virusi mogu biti detektovani samo ovom metodom. Problem kod ove vrste skenera je što ne mogu registrovati postojanje virusa u trenutku inficiranja sistema, jer još uvijek nisu napravljene potrebne izmene u sis datotekama. CRC skeneri ne mogu detektovati postojanje virusa u pristiglim datotekama, kao što su e-mail, diskete, vraćene backup datoteke, raspakovane arhive i sl., jer njihova baza nema podatke o njima.

11.2.3. Blokeri događaja

Antivirus blokeri događaja (behaviour blockers) su memorijski rezidentni programi koji "osluškiju" reakciju virusa i obaveštavaju o tome korisnika. Takve informacije mogu se dogoditi za vreme pokretanja izvršnih datoteka, zapisivanje u Boot sektor diskova itd. Dobra osobina blokera je što zaustavljaju izvršavanje virusa u trenutku infekcije, a loša je što vrlo često greše.

11.2.4. Imunizatori

Dele se u dva tipa: one koji upozoravaju na infekciju i one koje blokiraju pokušaj virusa da uđe u sistem.

Prvi tip se i sam ponaša kao virus, tako što se dodaje na kraj datoteke i pri svakom njenom pokretanju proverava izmene. To uradi samo jednom.

Drugi tip ove metode štiti sistem na način da menja datoteke i praktično uverava virus da su te datoteke zaražene. Za zaštitu od rezidentnih virusa koristi se mali TRS (rezidentni) program koji je ubačen u memoriju računara. On takođe nastoji uveriti virus (ako pokuša pristupiti

memoriji), da je memorija već zaražena. Ova metoda nije potpuno pouzdana, jer je nemoguće zaštititi sve datoteke od svih mogućih virusa.

11.2.5. Checksum provera

Provera checksum-a se bazira na mogućnosti da se na zaštićenom sadržaju proveri svaka promena. Checksum radi po principu da zaleđi sistem u prethodno utvrđenom neinficiranom stanju. Nakon zaleđivanja se proverava da li je u sistemu došlo do nekih promena u određenim vremenskim intervalima. Trenutno je jedina poznata metoda koja uklanja sve vrste virusa neovisno od toga da li su oni ranije otkriveni.

Mana kod upotrebe checksum je u tome što se njima otkriva infekcija tek nakon što je nastala, ali se redovnom primenom ove metode može otkriti virus pre nego što dođe do neke velike štete.

11.2.6. Monitoring

Programi za monitoring rade kao TSR (Terminate and Stay) koji pretražuje odvijanje sistemskih funkcija preko interrupt-a. Uvek kada sistem dobije naređenje za učitavanje neke datoteke koja je izvršnog tipa, može i da se izvrši i provera. Neki programi za monitoring ne traže specifične viruse već pokušavaju ukloniti sumnjive aktivnosti kao što su pisanje po boot sektoru ili nekim izvršnim programima, pokretanje formatiranja diska, pokušaji programa da postane rezidentan u memoriji itd. Glavna prednost monitora je u tome što mogu u realnom vremenu da otkriju virus.

Monitoring ima mnogo nedostataka. Glavni nedostatak je to što nije moguće učinkovito primeniti TSR program koji bi u sebi zadržavao podatke za detekciju, odnosno prepoznavanje svih poznatih virusa. Monitori kada otkrivaju sumnjive aktivnosti često dovode do velikog broja lažnih uzbuna, jer često označavaju i regularne aktivnosti kao što su formatiranje diska ili instaliranje raznih programa kao potencijalne pretnje.

12. ESET NOD32 antivirus

ESET NOD32 Antivirus, poznat kao NOD32, je antivirus programski paket napravljen od strane Slovačke kompanije ESET. ESET NOD32 Antivirus se prodaje u dva izdanja, Home Edition (Kućno izdanje) i Business Edition (Poslovno izdanje). Poslovno izdanje poseduje ESET Remote Administration (udaljena administracija) što omogućuje njegovo postavljanje i upravljanje, mirror-ovanje ažuriranih baza podataka sa potencijalnim pretnjama i mogućnost postavljanja na Microsoft Windows Server operativne sisteme.

12.1. Istorijat

12.1.1. NOD32

Prva verzija NOD32 (nazvana NOD-ICE), je napravljena 1987. godine od strane Miroslava Trnka i Peter Pasko-a kada su počeli da dominiraju računraski virusi.

U početku je program postao popularan među IT radnicima u zemljama Istočne Evrope, jer je ESET nastao u Slovačkoj, dok kasnije nije postao jedan od najpopularnijih antivirus rešenja na svetskom tržištu. Kompanija ESET je 3. novembra 2013. Dostigla 9000 ažuriranih definicija virusa.

Akronim NOD ima značenje Nemocnica na Okraji Disku (Bolnica na kraju diska).

12.1.2. E-Mail bezbednost za Microsoft Exchange Servere

10. marta 2010. godine ESET je objavio ESET Mail Security za Microsoft Exchange Servere, koji sadrži i anti-malware i antispam module. Podržava Microsoft Exchange 5.5, 2000, 2003, 2007 i 2010.

12.1.3. Bezbednost za mobilne telefone

ESET Mobile Security je zamena za ESET Mobile Antivirus, koji je pružao anti-malware i antispam funkcionalnosti. ESET Mobile Security sadrži sve karakteristike od starijeg proizvoda i još mu je dodato anti-theft (protiv krađe) funkcionalnosti kao što su SIM zaključavanje i udaljeno čišćenje kao bezbednosni dodatak i firewall. Verzije za Windows telefone i Symbian OS su postale dostupne na tržištu od Septembra 2010., za kućne korisnike kao i za preduzeća.

12.1.4. Remote Administrator (udaljeni administrator)

ESET Remote Administrator je konzola za centralno upravljanje koja je napravljena da dozvoljava mrežnim administratorima da upravljaju sa ESET programima preko korporativne mreže.

12.1.5. ESET Smart Security

05.11.2007. ESET je objavio komplet za internet zaštitu, ESET Smart Security verzija 3.0, kako bi bio konkurencija sa ostalim kompletima za internet zaštitu, kao što su McAfee, Symantec, AVG i Kaspersky. ESET Smart Security sadrži anti-spam i firewall kao i tradicionalne anti-malware karakteristike koje poseduje ESET NOD32 Antivirus.

12.1.6. ESET SysInspector

ESET SysInspector je alat za dijagnostiku koji omogućava duboku analizu više aspekata operativnog sistema, uključujući procese koji su pokrenuti, sadržaj registry-a, programi koji se pokreću prilikom pokretanja operativnog sistema i mrežnih veza. Anti-Stealth Technology se koristi da se otkriju skriveni objekti (rootkitovi) u Master Boot zapisu, boot sektoru, unosima u registry-u, drajverima, servisima i procesima. SysInspector Log-ovi su standardni XML fajlovi i mogu da se pošalju IT ekspertima za dalju analizu. Dva log-a mogu da budu upoređena da se pronađe set predmeta koji nisu zajednički za oba log-a. Log fajl može da bude sačuvan kao servis skripta za uklanjanje malicioznih objekata iz računara.

12.1.7. Ostali programi u ponudi ESET-a

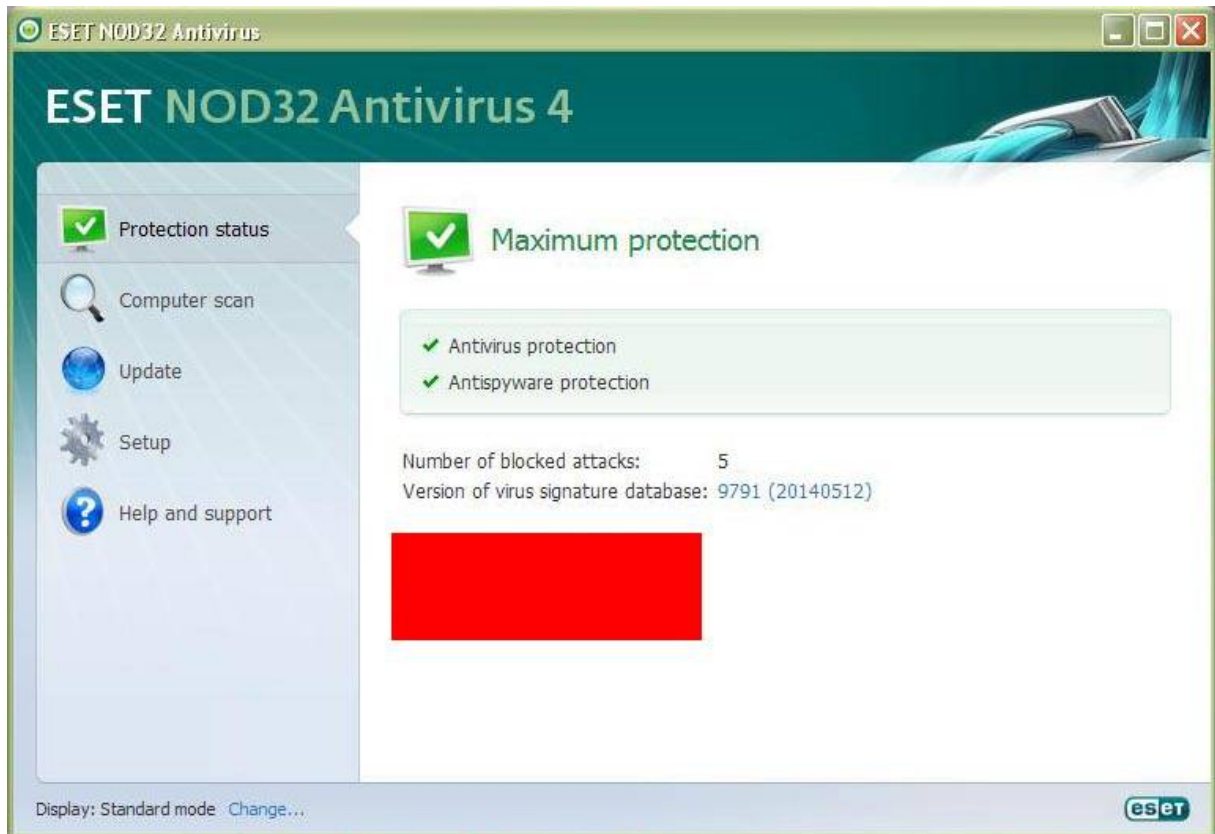
ESET je objavio besplatne alate za uklanjanje malware-a kada se oni prošire po sistemu, kao što je Mebroot.

12.2. Primena ESET NOD32 antivirusa

ESET NOD32 zbog svoje efikasnosti i veoma male potrošnje resursa računara, odnosno računarske memorije i procesora, spada u jedan od najboljih izbora za antivirus zaštitu u velikim računarskim sistemima.

U ovom radu će biti prikazana primena NOD32 antivirusa u Opštoj Bolnici Subotica, jer ima preko 500 računara. Takođe će biti prikazana količina pronađenih virusa, crva, trojanaca i blokiranih napada.

U bolnici se kod računara slabijih performansi koristi NOD32 Antivirus 4, iz razloga što troši manje resursa nego novija verzija NOD32 Antivirus 5, koja se koristi kod jačih računara.



Slika 6 – Korisnički interfejs ESET NOD32 Antivirus verzija 4

U ovom slučaju najčešći virus, odnosno crv koji NOD32 blokira je WIN32/Conficker.AA kao što se može videti na slikama 7, 8, 9.



Slika 7 – Primer crva koji je blokiran tako što je veza ukinuta

Log - ESET NOD32 Antivirus

Detected threats

Time	Source	Object	Name	Threat	Action	User	Information
13.5.2014 10:11:43	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
13.5.2014 10:11:39	HTT...	file	http://192.168.28.66:5354/grenvk	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
13.5.2014 9:19:49	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
13.5.2014 9:19:47	HTT...	file	http://192.168.28.225:3293/owob	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
13.5.2014 9:16:19	Real...	file	C:\Documents and Settings\Netwo...	a variant of Win32/Conficker.Gen ...	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
13.5.2014 9:16:16	HTT...	file	http://192.168.28.3:2441/wyxyxyv	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
13.5.2014 8:50:27	HTT...	file	http://192.168.28.22:1751/cnuabtv	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
13.5.2014 8:36:15	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
13.5.2014 8:36:11	HTT...	file	http://192.168.28.169:2447/yqaz	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 8:37:23	HTT...	file	http://192.168.29.125:9734/mmwl...	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 8:32:28	HTT...	file	http://192.168.28.157:1751/uhleku	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 7:51:57	HTT...	file	http://192.168.28.66:5354/ogofc	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 7:40:08	HTT...	file	http://192.168.29.33:2441/goderp	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 7:36:39	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
12.5.2014 7:36:36	HTT...	file	http://192.168.29.37:2540/bmlvl	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
12.5.2014 7:28:44	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
12.5.2014 7:28:41	HTT...	file	http://192.168.29.92:8618/bwovo	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
9.5.2014 8:14:57	HTT...	file	http://192.168.29.81:7690/adpdp	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
9.5.2014 7:38:29	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
9.5.2014 7:38:25	HTT...	file	http://192.168.28.143:8981/ulvzz	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
30.4.2014 7:51:27	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
30.4.2014 7:51:24	HTT...	file	http://192.168.29.55:6479/xopa	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
28.4.2014 7:41:54	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
28.4.2014 7:41:51	HTT...	file	http://192.168.28.52:2441/okbx	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
25.4.2014 7:55:53	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
25.4.2014 7:55:50	HTT...	file	http://192.168.28.110:2540/vavdc	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
25.4.2014 7:47:37	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
25.4.2014 7:47:34	HTT...	file	http://192.168.28.79:5354/gogof	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
24.4.2014 7:59:21	HTT...	file	http://192.168.29.29:7690/vxisfivo	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
24.4.2014 7:55:07	HTT...	file	http://192.168.28.110:2540/hyds...	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
24.4.2014 7:44:14	Real...	file	C:\Documents and Settings\Netwo...	a variant of Win32/Conficker.Gen ...	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
24.4.2014 7:44:11	HTT...	file	http://192.168.28.79:5354/phorg...	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
24.4.2014 7:43:54	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
24.4.2014 7:43:50	HTT...	file	http://192.168.28.213:3293/kcnj	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
23.4.2014 10:06:38	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
23.4.2014 10:06:34	HTT...	file	http://192.168.28.79:5354/brmedhe	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
23.4.2014 7:48:32	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
23.4.2014 7:48:29	HTT...	file	http://192.168.28.21:2441/dowgmw	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was
23.4.2014 7:38:52	Real...	file	C:\Documents and Settings\Netwo...	Win32/Conficker.AA worm	cleaned by deleting - quarantined	NT AUTHORITY...	Event occur
23.4.2014 7:38:48	HTT...	file	http://192.168.28.79:5354/brmedhe	Win32/Conficker.AA worm	connection terminated	NT AUTHORITY...	Threat was

Filter... Copy

Slika 8 – Primeri računarski virusa, crva i trojanaca koji su pronađeni prilikom skeniranja jednog od računara

ESET NOD32 Antivirus 4

User interface Setup Tools Help

Protection status
Computer scan
Update
Setup
Tools
Log files
Quarantine
Scheduler
SysInspector
Help and support

Log files

Log: Detected threats

Time	S...	O...	Name	Threat	Action	User
13.5.2014 10:...	R...	file	C:\Documents and S...	Win32/Conficker.AA worm	cleaned...	NT AUT...
13.5.2014 10:...	H...	file	http://192.168.28.6...	Win32/Conficker.AA worm	connect...	NT AUT...
13.5.2014 9:1...	R...	file	C:\Documents and S...	Win32/Conficker.AA worm	cleaned...	NT AUT...
13.5.2014 9:1...	H...	file	http://192.168.28.2...	Win32/Conficker.AA worm	connect...	NT AUT...
13.5.2014 9:1...	R...	file	C:\Documents and S...	a variant of Win32/Conficker.Gen worm	cleaned...	NT AUT...
13.5.2014 9:1...	H...	file	http://192.168.28.3...	Win32/Conficker.AA worm	connect...	NT AUT...
13.5.2014 8:5...	H...	file	http://192.168.28.2...	Win32/Conficker.AA worm	connect...	NT AUT...
13.5.2014 8:3...	R...	file	C:\Documents and S...	Win32/Conficker.AA worm	cleaned...	NT AUT...
13.5.2014 8:3...	H...	file	http://192.168.28.1...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 8:3...	H...	file	http://192.168.29.1...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 8:3...	H...	file	http://192.168.28.1...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 7:5...	H...	file	http://192.168.28.6...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 7:4...	H...	file	http://192.168.29.3...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 7:3...	R...	file	C:\Documents and S...	Win32/Conficker.AA worm	cleaned...	NT AUT...
12.5.2014 7:3...	H...	file	http://192.168.29.3...	Win32/Conficker.AA worm	connect...	NT AUT...
12.5.2014 7:2...	R...	file	C:\Documents and S...	Win32/Conficker.AA worm	cleaned...	NT AUT...
12.5.2014 7:2...	H...	file	http://192.168.29.9...	Win32/Conficker.AA worm	connect...	NT AUT...

Filter... Copy

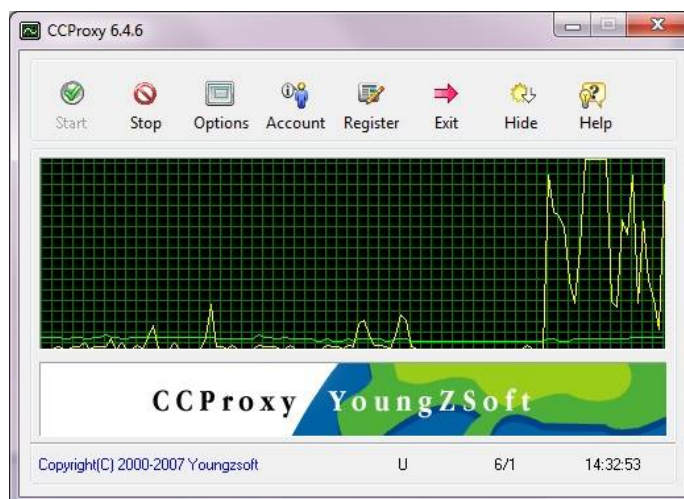
Open in a new window

Display: Advanced mode Change...

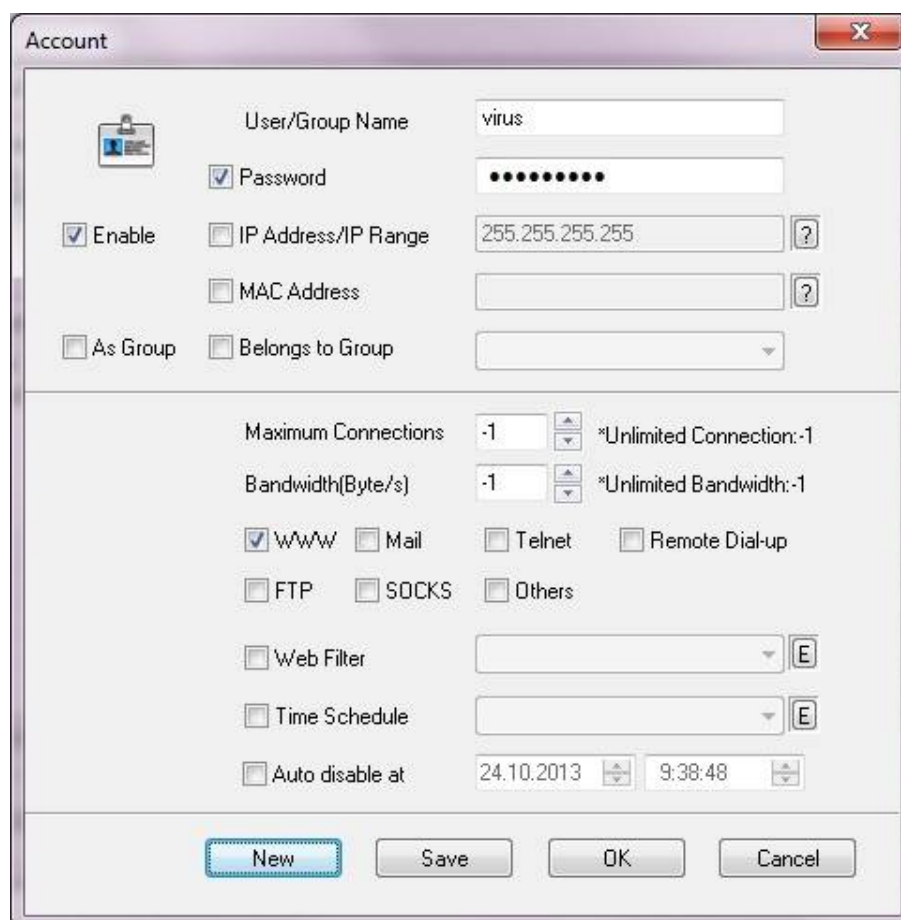
Slika 9 – Log fajlovi koji prikazuju pretnje koje su primećene prilikom skeniranja, kao i šta je antivirus program učinio sa njima nakon njihovog otkrivanja

12.2.1. Proxy podešavanja za ažuriranje definicija antivirus programa

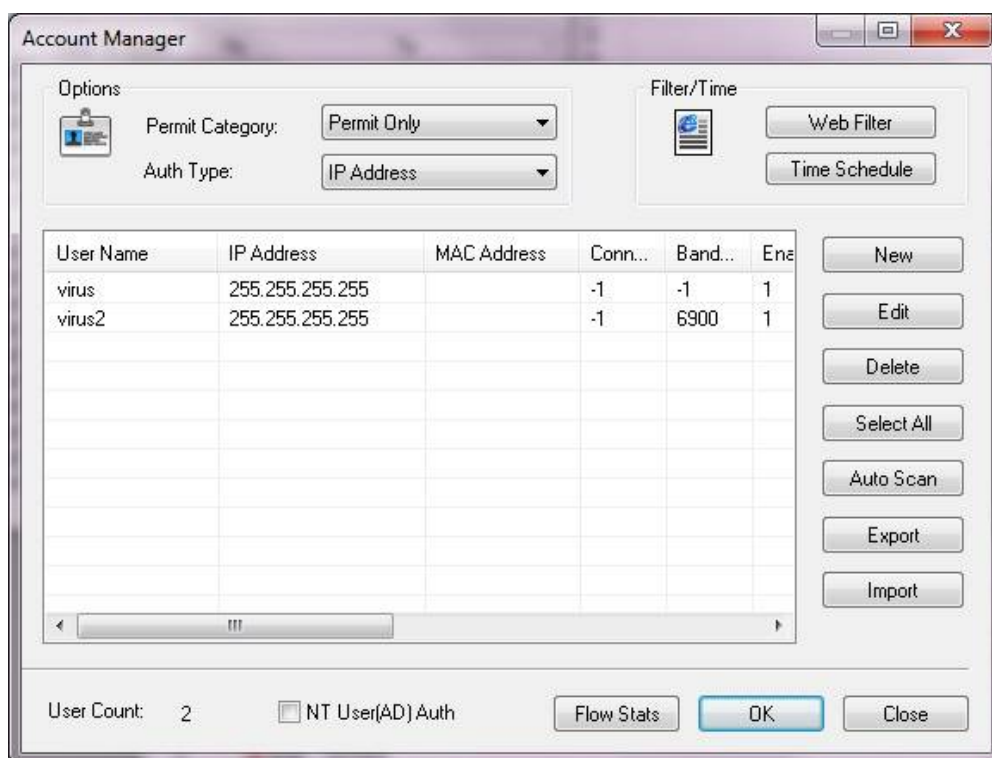
Kao i kod mnogih antivirus programa kod ESET NOD32 ima opcija da se ažuriranje definicija baza podataka najnovijih virusa vrši preko proxy-ja odnosno preko mreže. Potrebno je podesiti proxy server sa programom kao što je CCProxy. Ovaj metod je posebno koristan u velikim mrežnim sistemima gde ima mnogo računara koji nemaju pristup internetu, a poželjno je da imaju najnovije definicije baze podataka virusa.



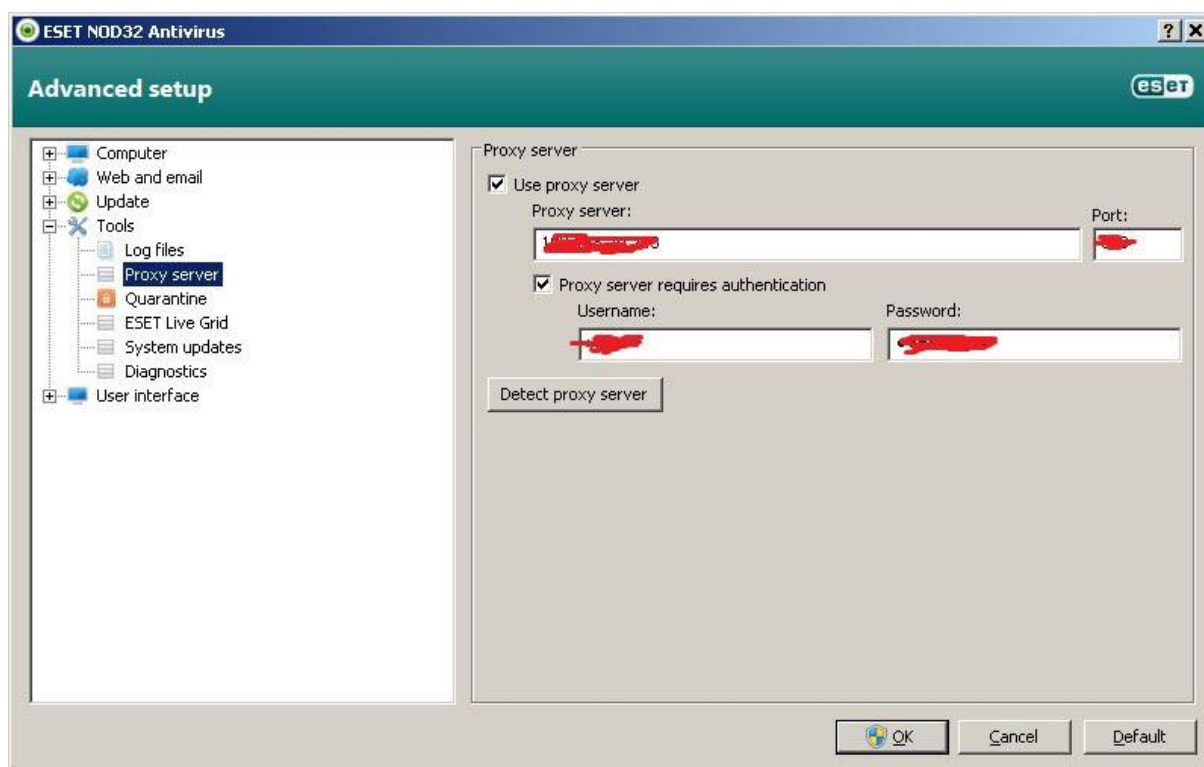
Slika 10 – Prikaz korisničkog interfejsa programa CCProxy



Slika 11 – Prikaz podešavanja pristupa internetu preko proxy-ja sa CCProxy



Slika 12 – Prikaz podešavanja pristupa internetu preko proxy-ja sa CCProxy



Slika 13 – Prikaz proxy podešavanja u ESET NOD32 za pristup internetu preko servera radi ažuriranja definicija baze podataka virusa

Zaključak

U ovom radu je razmatrana zaštita računarskih mreža. Na početku rada prikazana je metodologija po kojoj je istraživanje obavljeno što je pored ostalog podrazumevalo predmet istraživanja, ciljeve i zadatke istraživanja, istraživačke hipoteze, metode istraživanja i tok istraživačkog procesa.

U poglavlju o bezbednosti informacija pored osnovnih pojmova i istorijata bezbednost informacija analizirani su osnovni principi bezbednosti informacija.

U poglavlju o računarskim mrežama opisane su osnovne vrste računarskih mreža, istorijat računarskih mreža, a takođe je prikazan i OSI model. Što se tiče OSI modela posebno je opisan svaki od sedam slojeva kroz koje paketi prolaze, ali što je još važnije prikazano je kako on funkcioniše u realnom okruženju.

U poglavlju o računarskim virusima opisani su računarski virusi, kako oni funkcionišu, koje vrste postoje i kako oni deluju kada inficiraju računar.

U poglavlju o malicioznim programima opisani su maliciozni programi, crvi (worm) i trojanski konji (trojan horse).

U poglavlju o hronološkom nastanku računarskih virusa opisan je hronološki nastanak virusa, crva i trojanskih konja kao i njihovo delovanje na računare i mreže koje inficiraju.

U poglavlju o zaštiti protiv računarskih virusa opisano je kako se zaštititi od računarskih virusa, trojanskih konja i crva. Tu se spominje zaštita pomoću specijalizovanih programa koji su namenjeni za ovu vrstu pretnji, a to su antivirus programi. Opisano je kako oni funkcionišu, koje sve opcije i metode rada imaju.

U poslednjem poglavlju za praktičan primer uzet je ESET NOD32 Antivirus čija je funkcionalnost prikazana na različitim primerima.

Glavni deo rada usmeren je na tipove zaštite računarskih mreža. Tu se spominje kriptografija, njena istorija i važna uloga u zaštiti računarskih i mrežnih sistema. Spominju se najvažniji i u javnosti najpoznatiji tipovi zaštite računarskih mreža kao što su Firewall, IDS i IPS sistemi, kao i antivirus zaštita. Ovi tipovi zaštite i njihova primena su detaljno opisani u poglavljima u kojima se pominju, a akcenat je na antivirusnim zaštitama.

Iz razloga što su informacioni sistemi u stalnom razvoju, dolazi do novih pretnji od strane hakera i kako bi se zaštitila računarska mreža neke organizacije, preduzeća ili ustanove potrebno je primeniti bar neke (ako ne i sve) sisteme zaštite navedene u ovom radu.

Literatura

- [1] Cryptography and Network Security, William Stallings, peto izdanje.
- [2] End-to-End Network Security, Omar Santos, <http://ciscopress.com>
- [3] Network Security: History, Importance, and Future, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya
- [4] William Stallings, "Cryptography and Network Security", Prentice Hall, 2005.
- [5] Mark Stamp. Information security: principles and practice. John Wiley & Sons, Inc, 2006.
- [6] Milan Milosavljević i Gojko Grubor, "Osnovi bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, 2006.
- [7] Mladen Veinović i Saša Adamović, "Kriptologija 1", Univerzitet Singidunum, 2013.
- [8] John E. Canavan, "Fundamentals of Network Security", 2001.
- [9] Michael Sikorski i Andrew Honig, "Practical Malware Analysis", 2012.
- [10] Michael Davis, Sean Bodmer, Aron LeMasters, "Hacking Exposed", 2009.
- [11] James F. Kurose i Keith W. Ross, "Computer Networking: A Top-Down Approach, 6/E", 2012.
- [12] Wikipedia, Information Security, <http://en.wikipedia.org/wiki/>
- [13] Wikipedia, Cryptography, <http://en.wikipedia.org/wiki>
- [14] Wikipedia, Computer Network, <http://en.wikipedia.org/wiki>
- [15] Wikipedia, OSI model, <http://en.wikipedia.org/wiki>
- [16] Wikipedia, Intrusion detection system, <http://en.wikipedia.org/wiki>
- [17] Wikipedia, Intrusion prevention system, <http://en.wikipedia.org/wiki>
- [18] Wikipedia, Firewall, <http://en.wikipedia.org/wiki>
- [19] Wikipedia, Antivirus, <http://sh.wikipedia.org/wiki>
- [20] Wikipedia, Antivirus software, <http://en.wikipedia.org/wiki>
- [21] Wikipedia, Malware, <http://en.wikipedia.org/wiki>
- [22] Wikipedia, Computer virus, <http://en.wikipedia.org/wiki>
- [23] Wikipedia, Computer worm, <http://en.wikipedia.org/wiki>
- [24] Wikipedia, Trojan horse, <http://en.wikipedia.org/wiki>
- [25] Wikipedia, Timeline of computer viruses and worms <http://en.wikipedia.org/wiki>
- [26] Wikipedia, ESET NOD32, <http://en.wikipedia.org/wiki>