Dvoslojna proaktivna zaštita računarske mreže od malicioznog softvera

Ivan Đokić, Irfan Fetahović, Aleksandra Pavlović, *Državni univerzitet u Novom Pazaru*

Sadržaj — **Prisustvo malicioznog softvera u računarskoj mreži Državnog univerziteta u Novom Pazaru zahtevalo je preduzimanje hitnih mera. Snimljeni su profili korisnika, saobraćaj u mreži, najprisutniji maliciozni softver i načini njegove propagacije. Na bazi stanja u mreži primenjena je dvoslojna proaktivna zaštita, kojom se upravlja centralizovano, sa jednog mesta u mreži.**

Ključne reči **— maliciozni softver, proaktivna zaštita, računarska mreža,**

I. Uvod

U cilju smanjenja efekata prisustva malicioznog softvera i povećanja raspoloživosti, pouzdanosti i integriteta računarske mreže Državnog Univerziteta u Novom Pazaru (DUNP), autori su definisali i primenili koncept dvoslojne proaktivne zaštite računarske mreže. Sistem je proaktivan zbog uvođenja upravljačke petlje koja se sastoji od tri povezane stalne aktivnosti: (1) nadgledanja stanja u mreži, (2) analize pretnji, i (3) preduzimanja mera za otklanjanje pretnji. Slojevi zaštite su: (I) globalna zaštita na nivou računarske mreže univerziteta, i (II) parcijalna zaštita na nivou svakog računara u mreži. Parcijalna zaštita je prilagođena profilu korisnika računarske mreže (administracija, profesor, asistent, student), jer svaki korisnik sa svojim specifičnim profilom različito utiče na infekciju računara i propagaciju zlonamernog softvera kroz mrežu. Zaštitom se upravlja sa jednog mesta u mreži, a ostvarena je organizacionim i tehničkim merama.

II. Stanje u svetu

Tokom nekoliko prvih decenija postojanja računarske mreže su uglavnom koristili istraživači sa univerziteta da bi razmenjivali e-poštu i zaposleni u preduzećima da bi zajednički koristili kancelarijske štampače. Tada niko nije obraćao pažnju na sigurnost. Ali danas, kada milioni ljudi koriste računarske mreže za obavljanje bankarskih transakcija, razmenu poverljivih informacija, upravljanje kompanijama, sigurnost u mreži počinje da predstavlja veliki problem [1]. Jedan od najozbiljnih sigurnosnih problema u računarskim mrežama je maliciozni softver. Pod malicioznim (zlonamernim) softverom podrazumeva se niz instrukcija koji radi na napadnutom računaru, pri čemu napadnuti računar izvršava funkcije koje je definisao napadač. Računar inficiran malicioznim softverom može da ima sledeće simptome: usporen rad, brisanje ili izmenjen sadržaj datoteka, otežan upis podataka, prikupljanje podataka sa napadnutog računara i automatizovano slanje napadaču, slanje malicioznog softvera drugim računarima u mreži radi širenja infekcije, itd. Na taj način se ugrožava raspoloživost, pouzdanost i integritet računara i mreže. Sistemi za detekciju i prevenciju upada u računarske mreže postali su deo arsenala za borbu protiv napada na mrežu. Većina ovih sistema je pasivna jer prikuplja podatke o događajima u mreži i služi za analizu napada. U cilju poboljšanja performansi ovakvih sistema predlažu se kombinacije različitih tehnologija [2]. Razvijene su različite metode za otkrivanje ranjivosti mreža. Neke od tih metoda koriste grafove mreže [3], a neke dinamičku identifikaciju najznačajnijih faktora rizika u mreži [4]. Postojeći reaktivni mehanizmi zaštite mreža dopuštaju da se u slučajevima napada širokih razmera ošteti i deo mreže koji nije direktno napadnut (kolateralna šteta). Zato su razvijeni posebni mehanizmi za smanjenje kolateralne štete, čija se efikasnost kreće u granicama 60-97.8% [5]. Za upravljanje današnjim kompleksnim mrežama, koje rade u neprijateljskom okruženju, predlaže se centralizovana politika – celim domenom se upravlja sa jednog mesta. Za ovakvu politiku su razvijeni sistemi za nadgledanje sigurnosti i eventualnu poluautomatsku promenu politike, bazirani na reaktivnim i proaktivnim tehnologijama [6]. Jedinstvena politika sigurnosti računarske mreže Univerziteta u Lidsu, na primer, projektovana je da zaštiti kompletnu mrežu od spoljašnjih i unutrašnjih pretnji, bilo da su namerne ili slučajne. Obuhvata organizacione, fizičke i tehničke mere [7]. Radi sinergističkog efekta često se predlaže preduzimanje organizacionih, fizičkih i pravnih metoda zaštite, zajedno, tj. u korelaciji sa tehničkim, programskim i kriptografskim metodama [8].

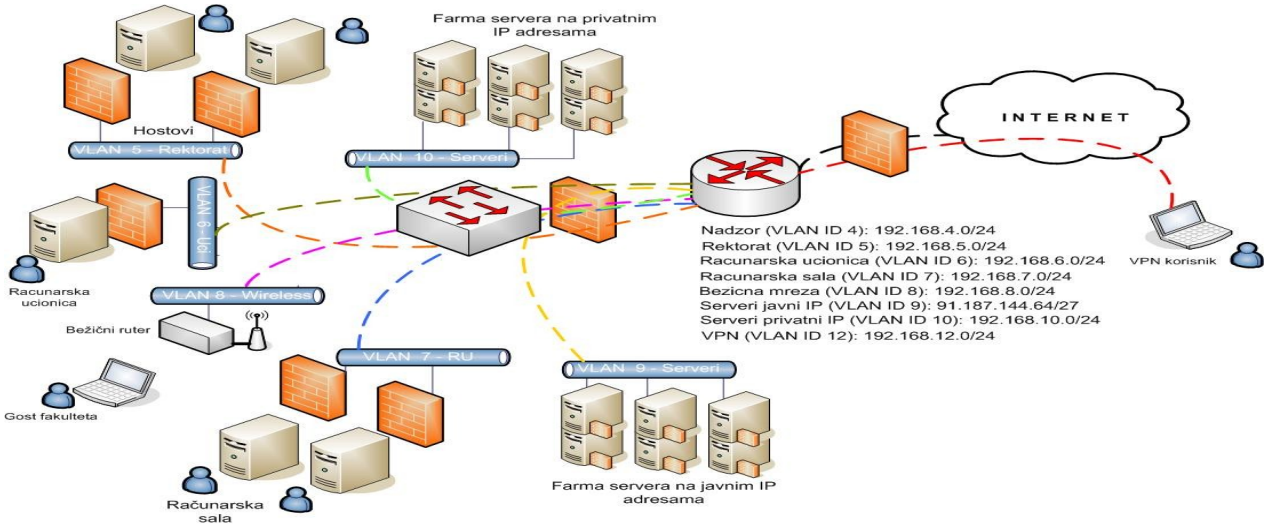
Dosadašnja odbrana od malicioznog softvera uglavnom je bila bazirana na reaktivnim tehnologijama (detekcija upada, filtriranje saobraćaja u mreži, detekcija i blokiranje malicioznog softvera). O upotrebi i dobrim stranama ovih tehnologija postoje snažni argumenti, ali se često izostavlja činjenica da ova rešenja zahtevaju kompetentne operatore – bez dobrog administratora detekcija upada u mrežu je beskorisna. Imajući u vidu stalni višeslojni i eksponencijalni rast pretnji, koje u suštini predstavljaju sofisticirane automatizovane napade na mreže i računare, bila su neophodna i stalna poboljšanja odbrambene strategije i tehnoloških rešenja. Poboljšanje strategije se

Rezultati prikazani u ovom radu su deo istraživanja u okviru projekta TR13018 - "Integralni i optimizirani proces testiranja i održavanja softvera", koje finansira Ministarstvo za nauku u tehnološki razvoj Republike Srbije

Ivan Đokić, Državni univerzitet u Novom Pazaru, ul. Vuka Karadžića bb, 36300 Novi Pazar, Srbija (telefon: 381-62-1279038, e-mail: idjokic@np.ac.rs)

Irfan Fetahović, Državni univerzitet u Novom Pazaru, ul. Vuka Karadžića bb, 36300 Novi Pazar, Srbija (telefon: 381-64-3626634, e-mail: ifetahovic@np.ac.rs)

Aleksandra Pavlović, Državni univerzitet u Novom Pazaru, ul. Vuka Karadžića bb, 36300 Novi Pazar, Srbija (telefon: 381-64-0479783, e-mail: apavlovic@np.ac.rs)



Sl. 1. Topologija računarske mreže Državnog Univerziteta u Novom Pazaru

ogledalo u pristupu da je bolje mrežu učiniti manje ranjivom, nego razvijati tehnologije za detekciju i blokiranje 100% napada. Kada se mreža učini manje ranjivom, napadač, koji radi automatizovano, radije prelazi u napad na drugi cilj nego da i dalje napada mrežu sa manjim stepenom ranjivosti.

III. Računarska mreža Državnog univerziteta u Novom Pazaru

Poboljšanje sigurnosti računarske mreže Državnog Univerziteta u Novom Pazaru proisteklo je iz realne potrebe, jer su infekcije čvorova u mreži postale tako česte da su ugrožavale operativni rad. Najčešći izvor infekcija bili su prenosivi memorijski elementi (USB flash drive), koje studenti koriste za skladištenje predavanja, vežbi i literature. Poboljšanje sigurnosti bilo je fokusirano samo na jednu oblast – eliminisanje najčešće pretnje u mreži, maliciozni softver, dok je zaštita od ostalih vidova pretnji ostala nepromenjena.

Računarska mreža Državnog Univerziteta u Novom Pazaru namenjena je za: (1) podršku nastavnom procesu, (2) podršku istraživanjima i razvoju, (3) podršku menadžmentu u upravljanju univerzitetom, (4) poboljšanje efikasnosti administracije, i (5) poboljšanje protoka informacija. Toplogija računarske mreže, koja odgovara ovim namenama, prikazana je slikom 1. Mreža je bazirana na Ethernet tehnologiji (standard 802.3, CSMA/CD), sa mogućnošću povezivanja 150 računara i brzinom prenosa podataka 1000 Mbps. Segmentacija mreže je izvršena u više virtuelnih lokalnih mreža (VLAN). Komunikacija između računara u okviru istog VLAN-a je slobodna, ali se na mrežnim barijerama vrši filtriranje saobraćaja.

IV. Maliciozni softver u računarskoj mreži

Prisustvo malicioznog softvera u mreži je manifestovano kroz usporen rad računara, nemogućnost aktiviranja pojedinih aplikacija, otežanu komunikaciju i stalna upozorenja instaliranih antivirusnih programa na postojanje pretnji. Raspoloživost računarske mreže je značajno redukovana a kod pojedinih računara u mreži praktično svedena na 0%. S obzirom da je nemoguće zaštititi nešto ako nije potpuno jasno šta se želi zaštititi, u cilju definisanja najbolje strategije za poboljšanje sigurnosti u mreži i izbora najboljih tehnoloških rešenja, izvršeno je u više navrata skeniranje stanja u mreži i analiza dobijenih podataka.

Tabela 1: Maliciozni softver u računarskoj mreži DUNP

MALWARE NAME	Infections
WORM DOWNAD.AD	151
Mal DownadJ	127
TROJ UTOTI.FQ	122
TROJ Gen CZ0359	97
PE SALITY.JER	80
WORM OTORUN.DV	75
WORM DAWNAD	74
Mal Otorun1	41

Statistički podaci o mreži ukazuju na nekoliko karakteristika značajnih za strategiju zaštite mreže, i to:

- U mreži postoje različite vrste malicioznog softvera (virusi, crvi, logičke bombe, i dr.). Tabela 1 prikazuje najprisutniji maliciozni softver u računarskoj mreži DUNP.

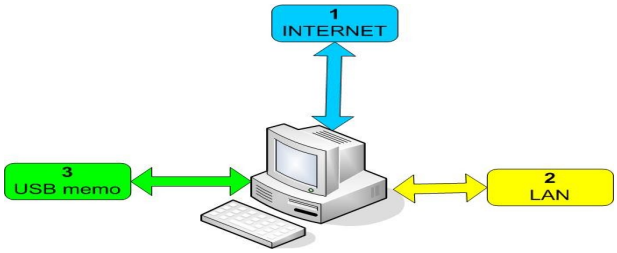
Tabela 2: Računari sa najvećim brojem infekcija

INFECTED COMPUTER NAME	Detections
ADMIN8	180
K2A	130
303ASIST9	91
ADMIN1	64
ADMIN20	53
ADMIN14	42
ADMIN5	37
ADMIN18	36
1RCSALA7	34

- U mreži postoji više grupa korisnika sa različitim profilima upotrebe računarske mreže DUNP (vreme upotrebe, trajanje uključenja računara, najčešće korišćene aplikacije, količina prenetih podataka, način unosa i skladištenja podataka, itd.). Tipične su sledeće grupe korisnika: (1) administratori sistema, (2) profesori, (3) asistenti, (4) studenti, i (5)

menadžment DUNP. Svaka od ovih grupa zbog razlike profila inficira računare različitim malicioznim softverom i ima različit intenzitet unošenja malicioznog softvera. U Tabeli 2 prikazani su računari sa najvećim brojem infekcija malicioznim softverom. Lako je uočiti da među njima ima računara iz svih grupa korisnika, ali da najveći broj infekcija pripada računarima koje koriste administratori mreže. To je posledica prirode aplikacija koje su aktivne na ovim računarima.

- Unošenje malicioznog softvera u računare u mreži DUNP vrši se na tri načina – sa Interneta, od drugog računara u lokalnoj mreži i korišćenjem prenosivih memorijskih elemenata (Sl. 2). Identifikaciju izvora infekcije moguće je izvršiti na bazi statistike platforme za zaštitu mreže DUNP (Trend Micro).



Sl. 2. Načini unošenja malicioznog softvera u računare mreže DUNP

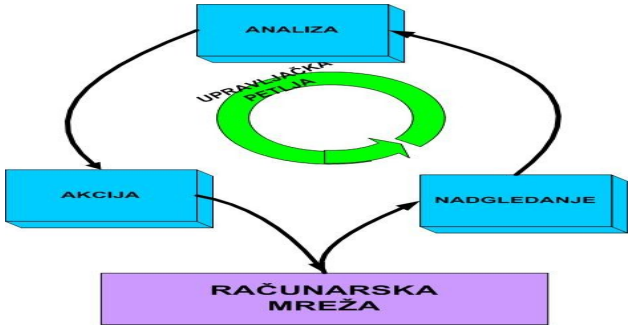
Svaka grupa korisnika zbog različitog profila ima različitu raspodelu u pogledu načina unošenja malicioznog softvera u računar. Tako profesori, asistenti i studenti najčešće inficiraju računar korišćenjem prenosivih memorijskih elemenata, a menadžment DUNP i administratori sistema putem Interneta. Najmanji procenat infekcija je nastao komunikacijom unutar lokalne mreže.

V. Strategija zaštite računarske mreže

Imajući u vidu namenu računarske mreže, topologiju, karakteristike korisnika, najčešće pretnje i načine unošenja malicioznog softvera u računare, pri izboru strategije zaštite mreže postavljeni su sledeći ciljevi: (1) primeniti proaktivne mere zaštite, (2) mere sprovesti u što kraćem roku, (3) ne narušavati kvalitet usluga mreže, (4) minimalno ograničiti pogodnosti i slobodu korisnika, (5) minimizirati troškove uvođenja mera sigurnosti, i (6) ne usložnjavati proceduru održavanja mreže. Na bazi ovih ciljeva izabrana je strategija zaštite računarske mreže DUNP koja:

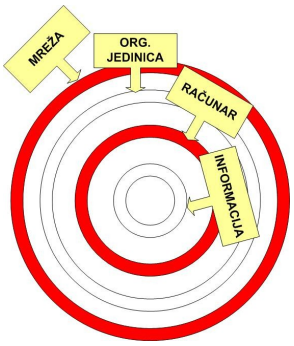
- Ima centralizovano upravljanje,
- Ima stalno aktivnu upravljačku sigurnosnu petlju, prikazanu slikom 3,
- Ima 2 sloja zaštite, prikazana slikom 4.

Stalno aktivna upravljačka sigurnosna petlja je neophodna zbog prirode malicioznog softvera, koji predstavlja „pokretan cilj“ u smislu oblika koji uzima, sofisticiranosti, načina unošenja u mrežu i propagacije, efekata koje izaziva, načina na koji se skriva. Osim malicioznog softvera menjaju se i karakteristike same mreže – njena topologija, aplikacije, profil i mobilnost korisnika, itd.



Sl. 3.Upravljačka sigurnosna petlja računarske mreže DUNP

Sve ove promene zahtevaju da upravljačka sigurnosna petlja bude stalno aktivna i da regularno prati stanje u mreži, analizira stanje i traži optimalna rešenja i izvršava akcije neophodne za sigurnost mreže. O funkcionisanju petlje staraju se administratori mreže.



Sl. 4. Dvoslojna zaštita računarske mreže DUNP

Iako se u teoriji sigurnosti računarskih mreža najčešće govori o 4 sloja zaštite (zaštita kompletne mreže, zaštita dela mreže na nivou organizacione jedinice, zaštita računara i zaštita informacija), u slučaju zaštite računarske mreže DUNP odabran je koncept zaštite u 2 sloja - na nivou mreže i na nivou računara. Zaštita u 2 sloja je odabrana zbog jednostavnosti realizacije i fokusiranosti odbrane mreže od samo jedne vrste pretnji – malicioznog softvera.

VI. Realizacija zaštite računarske mreže

Oba sloja zaštite mreže predstavljaju kombinaciju organizacionih i tehničkih mera, a one čine konzistentnu celinu i zadovoljavaju postavljene ciljeve zaštite mreže.

I – Sloj na nivou mreže: Zaštita na nivou mreže bazirana je na centralizaciji upravljanja mrežom i propisivanja pravila koja sprovode administratori mreže (organizacione mere), kao i upotrebi savremenih platformi za zaštitu mreža (tehničke mere). Mere su: (1) Upravljanje mrežom vrši se centralizovano sa jasnim ovlašćenjima svakog administratora. Na taj način se obezbeđuje jedinstven koncept upravljanja i dosledno sprovođenje mera zaštite i sigurnosti mreže, (2) Zaštita mreže i virtuelnih lokalnih mreža vrši se mrežnim barijerama, na kojima se vrši filtracija saobraćaja tako da ne ugrožava potrebe aplikacija, (3) Nadgledanje saobraćaja u mreži vrši se korišćenjem platforme za nadgledanje „Cacti“ koja prikuplja podatke, smešta

podatke u datoteku i vrši grafičku prezentaciju podataka o saobraćaju u čvorovima mreže, (4) Kontinualno praćenje stanja linkova korišćenjem softverskih alata MRTG i NAGIOS, gde se svaka neregularnost ispituje kroz log-ove na serveru, računaru, ruteru, (5) Limitiranje saobraćaja za pojedine grupe korisnika, (6) Svakodnevno skeniranje kompletne mreže radi utvrđivanja prisustva malicioznog softvera, korišćenjem platforme „TrendMicro“, (7) Čišćenje mreže od detektovanog malicioznog softvera, (8) Uvođenje sistema upravljanja kursevima. Koristi se MOODLE - Modular Object Oriented Learning Enviroment, koji omogućava da resursi za učenje (prezentacije, literatura, beleške, itd.) budu dostupni studentima putem Interneta. Na taj način se gubi potreba za korišćenjem prenosivih memorijskih elemenata u računarskoj mreži DUNP, a time se eliminiše i značajan izvor malicioznog softvera, i (9) Zabrana upotrebe prenosivih memorijskih elemenata.

II – Sloj na nivou računara: Karakteristike zaštite na nivou računara su – (1) Nadgledanje saobraćaja i analiza paketa koja se realizuje pomoću platforme PRTG Network Monitor. Ovo rešenje omogućava administratoru mreže ili korisniku da postavi senzore na računare u mreži i da nadgleda brzinu prenosa podataka, količinu prenetih podataka, najčešće uspostavljene veze, najviše korišćene protokole, idr. Nadgledanje, slanje izveštaja i upozorenja mogu da se automatizuju što poboljšava proaktivnu ulogu ovakvog sistema zaštite, (2) Stalno skeniranje računara antivirusnim programima radi detekcije prisustva malicioznog softvera. Na raspolaganju je veliki broj softverskih rešenja (BitDefender, Kaspersky, Avira, itd.) koja omogućavaju efikasnu detekciju prisustva malicioznog softvera. Ipak, treba imati na umu da ne postoji 100% efikasna detekcija malicioznog softvera, (3) Brisanje ili onemogućavanje detektovanog malicioznog softvera, (4) Zabrana i blokiranje upotrebe prenosivih memorijskih elemenata za neke grupe korisnika i neke čvorove u mreži, (5) Skeniranje prenosivih memorijskih elemenata pre upotrebe, za one korisnike i čvorove gde upotreba nije zabranjena.

Tabela 3: Računari mreže DUNP sa najvećim brojem infekcija nakon uvođenja zaštite

INFECTED COMPUTER NAME	Detections
K2A	8
BiologijaLAB	8
REFERENTI2	6
STSLUZBA2	4
ADMIN5	1
ADMIN7	1
303ASIST8	0
303ASIST9	0

Ovako relizovana zaštita mreže DUNP značajno je smanjila prisustvo malicioznog softvera u mreži i omogućava raspoloživost mreže bolju od 98%. Najveći problem u određivanju stvarne raspoloživosti mreže predstavlja teškoća tačne detekcije neregularnog stanja i utvrđivanje uzroka tog stanja. U Tabeli 3 prikazani su računari sa najvećim brojem infekcija nakon 5 meseci primene predložene dvoslojne proaktivne zaštite. Uočava se drastično smanjenje prisustva malicioznog softvera kod najinficiranijih računara.

VII. Zaključak

Rad računarske mreže Državnog univerziteta u Novom Pazaru ugrožen je prisustvom i stalnim širenjem malicioznog softvera. U cilju poboljšanja raspoloživosti, pouzdanosti i integriteta mreže autori su snimili stanje mreže, definisali ciljeve zaštite, definisali i primenili koncept dvoslojne proaktivne zaštite, koji je omogućavao izvršenje postavljenih ciljeva. Nakon 5 meseci od uvođenja zaštite, na bazi praćenja raspoloživosti i skeniranja mreže radi utvrđivanja prisustva malicioznog softvera, potvrđena je raspoloživost mreže od 98% i značajno smanjenje broja infekcija računara kod svih profila korisnika.

Literatura

[1] A. S. Tanenbaum, *Računarske mreže*, Mikro knjiga, Beograd, 2005. poglavlje 8.

[2] M. V. R. Murthy, P. R. Kumar, E. D. Rao, A. C. Sharma, S. Rajender, S. Rambabu, “Performance of the Network Intrusion System”, International Journal of Computer Scince and Network Security, Vol. 9 No 10, Okt 2009.

[3] S. Noel, S. Jajodia, "Proactive intrusion prevention and response via attack graphs," in *Practical Intrusion Analysis - Prevention and Detection for the Twenty-First Century*, Ryan Trost, ed., Pearson Education, Boston, 2010, str. 119-149

[4] E. Al-Shaer L. Khan, M. S. Ahmed, „A Comprehensive Objective Network Security Metric Framework for Proactive Security Configuration“ ., Dostupan: www.mnlab.cs.depaul.edu

[5] J. Chou, B. Lin, S. Sen, O. Spatscheck, “Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks”, IEEE/ACM Transactions on Networking, Vol. 17 Issue 6, Dec 2009.

[6] T. Dorges, K-P. Kossakowski, “Proactive Security Monitoring in a Policy Managed Network”, Dostupan: www.first.org/conference/2006/papers/dorges-till-papers.pdf

[7] J. K. Darley, „Information Security Policy“, Dostupan: http://campus.leeds.ac.uk/isms

[8] D. Pleskonjić, N. Maček, B. Đorđević, M Carić, *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007

Abstract

Presence of malicious software in computer network at State university of Novi Pazar demanded urgent measures to be taken. Profiles of users, network traffic and most present software threats and ways of their propagation were recorded. Based on this information we have applied two-layer proactive protection which is fully centralized, and administered from one place in network.

TWO-LAYER PROACTIVE PROTECTION OF COMPUTER NETWORK FROM MALICIOUS SOFTWARE

Ivan Đokić, Irfan Fetahović and Aleksandra Pavlović