HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

WormRadar projekt

CCERT-PUBDOC-2004-04-69

CARNet CERT u suradnji s LS&S

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

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

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Razni crvi i drugi maliciozni programi koji se šire Internetom već nekoliko godina su veliki problem, a na to su posebno osjetljivi Windows sustavi. Prvi crvi koji su poharali Internet i izazvali mnoge probleme bili su CodeRed tijekom ljeta i Nimda u rujnu 2001. godine. Oba crva su iskorištavala nedostatak unutar IIS-a, Microsoftovog Web poslužitelja. Bez obzira što su zakrpe postojale već prije toga, čak i danas se na Internetu može detektirati postojanje tih crva. Nakon toga, početkom 2002., pojavio se pojavio SQL Slammer, koji je iskorištavao nedostatak unutar SQL Server poslužitelja, da bi sredinom prošle godine velik broj računalnih mreža ostao paraliziran nakon pojave Blaster, odnosno Nachi crva koji su se širili iskorištavanjem nedostatka unutar Microsoftove implementacije RPC servisa.

Zajedničko svim tim crvima bilo je to da su iskorištavali sigurnosne nedostatke u Microsoft proizvodima, koji su bili već ranije identificirani i za koje su postojale odgovarajuće zakrpe.

Osim tih crva, postoje i postojali su mnogi crvi, virusi i trojanski programi koji se šire preko elektroničke pošte ili na druge načine.

Najbolja i najefikasnija metoda zaštite od svih tih prijetnji jest implementacija preventivnih kontrola, odnosno pravovremena instalacija sigurnosnih zakrpi i ispravna konfiguracija poslužitelja i servisa. Unatoč tome, iz raznih razloga to se vrlo često propušta napraviti.

Bez obzira na preventivne metode, uvijek je poželjno implementirati metode detekcije koje omogućavaju detekciju neovlaštenih aktivnosti. Prije svega to su razni IDS i *Honeypot* sustavi, koji prate rad mreže ili pojedinih sustava te detektiraju i prijavljuju (potencijalno) neovlaštene aktivnosti.

WormRadar je projekt distribuiranog Windows *honeypot* sustava. Sam sustav je još u razvojnoj fazi, te kao takav ima određenih propusta i nedostataka, no sama ideja projekta je potencijalno vrlo zanimljiva.

Esencijalno, radi se o sustavu koji funkcionira na volonterskoj bazi, a rezultati, koje kontinuirano prikupljaju pokrenuti agenti, prikupljaju se na jedinstvenom mjestu i obrađuju, te se na temelju toga, u stvarnom vremenu, generira statistika detektiranih, potencijalno neovlaštenih, aktivnosti.

Osim toga, svaki agent može funkcionirati kao jedinstveni sustav, odnosno koristiti se za generiranje lokalnih administrativnih upozorenja na temelju detektiranih aktivnosti.

2. Instalacija i pokretanje

Instalacija WormRadar aplikacije je vrlo jednostavna. S referentne lokacije (http://wormradar.com) dovoljno je skinuti izvršnu datoteku `WormRadar.exe` i snimiti je u za to predviđeni direktorij. Korištenje posebnog direktorija poželjno je pošto aplikacija prilikom prvog pokretanja u tom direktoriju generira `WormRadar.ini` konfiguracijsku datoteku u kojoj su pohranjene informacije o konfiguraciji aplikacije i koju aplikacija provjerava prilikom pokretanja.

Ukoliko se mijenja konfiguracija, odnosno postavke aplikacije, nužan je restart aplikacije da bi te promjene postale aktivne.

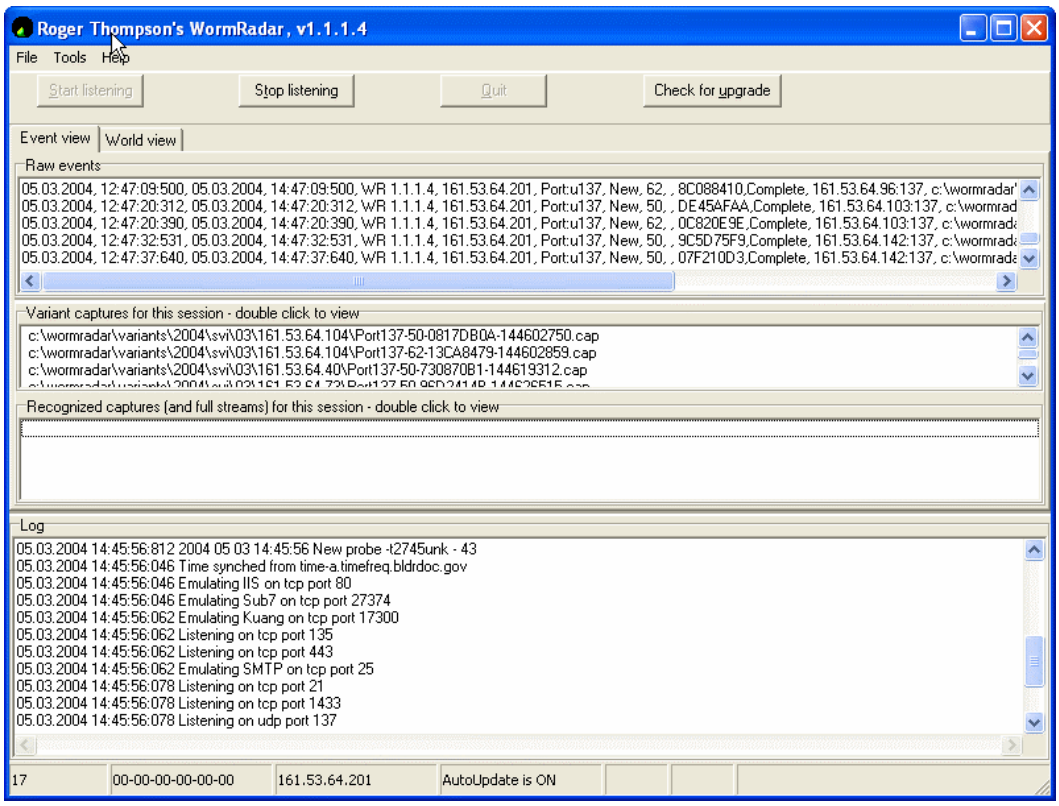
Osim tih datoteka, u uobičajenom načinu rada aplikacija generira log datoteke koje je također poželjno držati u odgovarajućim poddirektorijima.

3. Sučelje

Sučelje aplikacije (Slika 1) podijeljeno je na traku s izbornicima i radno područje te je vrlo jednostavno i pruža uvid u trenutnu aktivnost.

Traka s alatima sastoji se od izbornika *File*, *Tools* i *Help*.

Izbornik File služi za skeniranje ili pregled arhiviranih log datoteka (opcije *Scan old captures*, *View a file*). Kroz izbornik Help može se doći do osnovnih uputa za rad s aplikacijom, povijesti promjena i osnovnih informacija o inačici aplikacije.



Slika 1: *Sučelje WormRadar aplikacije*

Iz *Tools* izbornika moguće je odabrati naredbu *Properties* za podešavanje postavki aplikacije, a u idućim inačicama aplikacije biti će omogućene još neke naredbe koje su u ispitanim inačicama bile neaktivne.

Radno područje aplikacije u gornjem dijelu ima četiri gumba koji redom služe za pokretanje osluškivanja (*Start listening*), zaustavljanje (*Stop listening*), izlazak iz aplikacije (*Quit*) i provjeru raspoloživosti nove inačice (*Check for upgrade*).

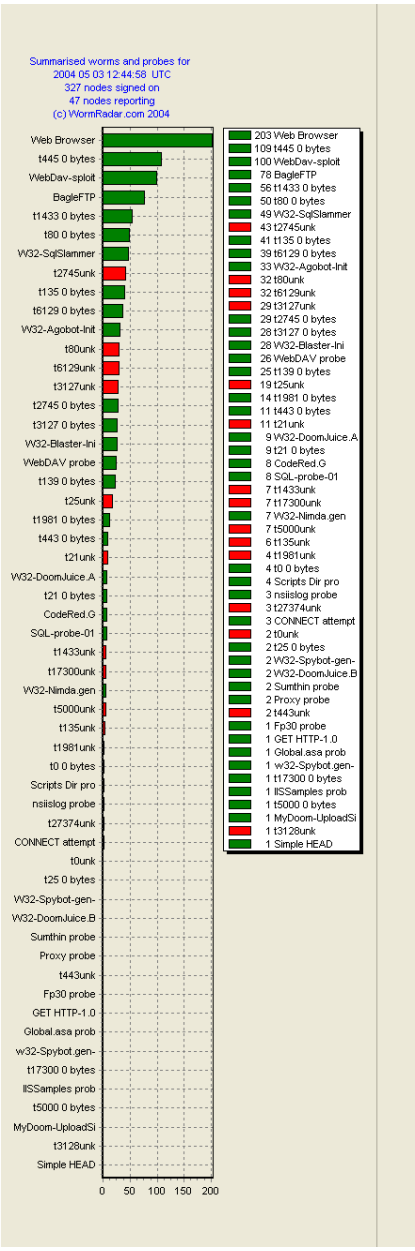
Najveći dio radnog područja zauzimaju *Event View* i *World View* kartice kroz koje je moguće u stvarnom vremenu nadgledati rad.

Kartica *Event View* podijeljena je u četiri dijela kroz koje je moguće u stvarnom vremenu nadzirati:

- sve događaje (*Raw events*),
- prepoznate uzorke (*Recognized captures*),
- varijante (*Variant captures*) i
- poruke o stanju same aplikacije (*Log*).

Kartica *WorldView* ne odnosi se na rad aplikacije same po sebi, već služi za statistički pregled koji se generira automatski na temelju podataka koje na središnju lokaciju šalju svi aktivni WormRadar agenti. Pregled se u aplikaciji automatski osvježava svakih 15 minuta, dok se isti graf na Webu osvježava svakih 30 minuta. Redci u grafu označavaju potencijalne napade ili skenove, odnosno promet detektiran na pojedinim portovima koji se nadziru (Slika 2).

Zelenom bojom označene su aktivnosti koje paket prepoznaje, dok su crvenom bojom označene nove aktivnosti (koje mogu biti i legitimne). Iz *Worldview* kartice također je moguće pregledavanje informacija koje bilježi aplikacija (*Log*), te podešavanje opcija za slanje upozorenja (*WorldView notifications* naredba).



Slika 2: *Graf s prikazom raspodjele detektiranih aktivnosti*

4. Podešavanje postavki

Podešavanje radnih postavki WormRadar sustava vrši se kroz naredbu *Properties* izbornika *Tools*. Postavke se podešavaju kroz sljedeće kartice:

- *Notification options*,
- *Configure emulations*,
- *General TCP ports*,
- *General UDP ports*,
- *Miscellaneous options*,
- *WorldView*.

4.1. Upozorenja

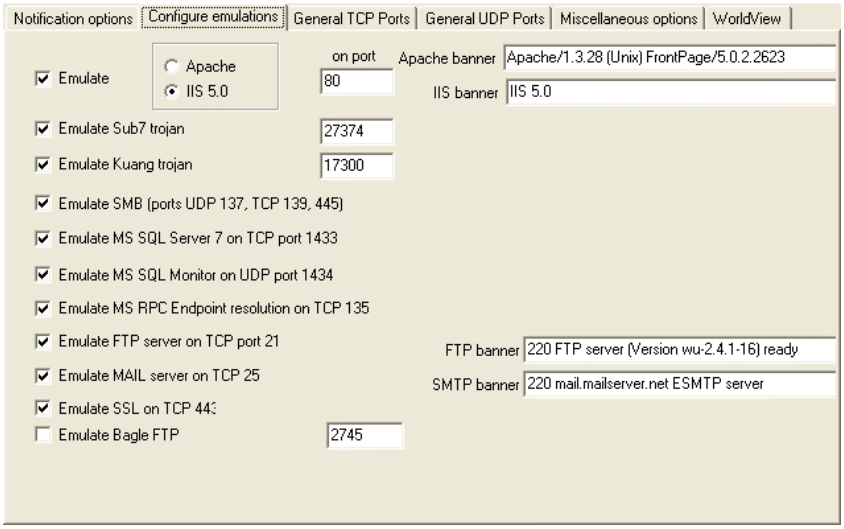
Kartica *Notification options* služi za podešavanje slanja administrativnih upozorenja prilikom detekcije incidenata/napada. Upozorenja se mogu podesiti na nekoliko razina. Kao prvo; alat u svojstvu udaljenog agenta podatke o detektiranim aktivnostima može slati na središnju lokaciju. Za to se koristi slanjem poruka elektroničke pošte (predefinirana adresa je wormtrap@bellsouth.net), te slanjem UDP paketa (predefinirana IP adresa: 68.157.174.28, UDP port 23515). Slanje ovih upozorenja moguće je isključiti, no ono je uvjet za mogućnost besplatnog korištenja paketa.
Slanje obavijesti o detektiranim aktivnostima služi za središnju analizu i statističku obradu, te generiranje globalnog dijagrama koji se automatski osvježava svakih 30 minuta.
Osim središnjeg obavješćivanja sustav je također moguće podesiti za slanje dodatnih upozorenja korištenjem sustava elektroničke pošte, što se može iskoristiti za udaljeno praćenje rada paketa. Granularnost ovog sustava je takva da omogućava slanje poruka u slučaju detekcije bilo kakvih aktivnosti koje sustav bilježi (opcija *CC event notifications to*) ili detekcije novih varijanti (opcije *Send variant captures to* i *Also page this address on variant detection*) napada.
Konačno, moguće je podesiti lokalno generiranje zvučnih upozorenja na samom sustavu (opcije *Beep on known capture*, *Beep on variant capture*, *Play .wav on variant capture*).
Valja napomenuti da paket nema vlastiti SMTP sustav, već koristi postojeću mrežnu infrastrukturu, te je za uspješno slanje upozorenja korištenjem poruka elektroničke pošte potrebno definirati SMTP poslužitelj te, opcionalno, korisničko ime i zaporku, ukoliko je lokalni SMTP poslužitelj konfiguriran tako da prihvaća *relaying* samo autenticiranim klijentima.

4.2. Emulacija servisa

WormRadar predefinirano može emulirati sljedeće servise (inačica 1.1.1.4):

- Web poslužitelj (Apache ili IIS 5.0) na proizvoljnom portu (predefinirano port 80),
- Sub7 trojanski program na proizvoljnom portu (predefinirano TCP port 27374),
- Kuang trojanski program na proizvoljnom portu (predefinirano TCP port 17300),
- Windows SMB protokol (UDP port 137 i TCP portovi 139, 445),
- MS SQL Server 7 (TCP port 1433),
- MS SQL Server monitor (UDP port 1434),
- MS RPC servis (TCP port 135),
- FTP poslužitelj (TCP port 21),
- poslužitelj elektroničke pošte (SMTP) (TCP port 25),
- SSL poslužitelj (TCP port 443),
- Bagle (crv) FTP poslužitelj (predefinirano TCP port 2745).

Slika 3 prikazuje karticu kroz koju se WormRadar konfigurira za emulaciju pojedinih servisa.



Slika 3: *Konfiguriranje predefiniranih emulacija*

Napomena: Prilikom testiranja aplikacije uočeno je da u prvoj inačici (1.1.0.249), emulacija IIS 5.0 poslužitelja nije funkcionirala ispravno. Odnosno, ukoliko se emulirao Web poslužitelj, aplikacija je bez obzira na odabir tipa (Apache ili IIS 5.0) emulirala Apache. U trenutnoj inačici (1.1.1.4) taj je nedostatak ispravljen.
Emuliranje svih gore navedenih servisa moguće je selektivno uključivati i isključivati. Ovdje valja uzeti u obzir da paket ne može raditi kao *proxy*, odnosno prosljeđivati zahtjeve eventualnim legitimnim servisima na tim portovima. To znači da niti jedan servis koji se emulira ne može istovremeno koegzistirati na sustavu.
Za većinu emulacija to ne predstavlja problem, obzirom da postojanje legitimnih servisa koji koriste te portove na *honeypot* sustavu nije opravdano. Međutim, emulacija nekih servisa koji se predefinirano pokreću i predstavljaju temelj za mrežnu komunikaciju NT/2000/XP sustava (MS RPC i SMB servisi) zahtijeva eksplicitno onemogućavanje tih servisa na razini operacijskog sustava.

4.2.1. Zaustavljanje servisa koji rade na portovima koje WormRadar osluškuje

Kako je spomenuto, na NT baziranim sustavima (2000, XP), neki servisi predefinirano koriste portove na kojima WormRadar osluškuje, te je za potpunu funkcionalnost WormRadar-a potrebno te servise onemogućiti.
Za emulaciju SMB protokola (TCP portovi 139 i 445, te UDP port 137) potrebno je:

1. onemogućiti NetBIOS korištenjem TCP/IP protokola (*TCP/IP properties*, *Advanced*, *WINS*, *Disable NetBIOS over TCP/IP*), čime se zaustavlja osluškivanje na UDP portovima 137 i 138, te na TCP portu 139,
2. onemogućiti SMB protokol preko TCP/IP protokola (u *registry* ključu `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`, postaviti string vrijednost `TransportBindName` na nul string), čime se zaustavlja se osluškivanje na TCP portu 445 (ovim korakom automatski se zaustavlja osluškivanje na portovima navedenim u koraku 1).

Za emulaciju MS RPC servisa (TCP port 135) potrebno je:
1. pokrenuti `dcomcnfg` alat, te za DCOM isključiti podršku za TCP/IP (*My Computer*, *Properties*, *Default Protocols*, *Connection-orientied TCP/IP – remove)*, te onemogućiti sam DCOM (*My Computer*, *Properites*, *Default Properties*, isključiti *Enable Distributed COM on this computer*)
2. onemogućiti servise koji koriste RPC :
   - *Distributed Transaction Coordinator (MSDTC)*,
   - *Messenger* i
   - *Task Scheduler*,

   zaustavljanjem navedenih servisa, te postavljanjem načina pokretanja na *Disabled*.

4.3. Definiranje proizvoljnih emulacija

Osim predefiniranih servisa, moguće je definirati i proizvoljne TCP i UDP portove na kojima će WormRadar osluškivati. Kroz karticu *General TCP ports* moguće je definirati do 16 dodatnih TCP portova, dok je kroz karticu *General UDP ports* moguće definirati maksimalno 10 dodatnih UDP portova.

4.4. Ostale opcije

Uz sve ranije spomenute opcije vezane uz obavješćivanje i emulaciju, moguće je podesiti i neke dodatne opcije:

- vremensku sinkronizaciju,
- automatsku nadgradnju preko Interneta,
- bilježenje aktivnosti u log datoteke i
- automatsko pokretanje WormRadar aplikacije.

Vremenska sinkronizacija provodi se korištenjem NTP (TCP/UDP port 37) protokola prema NTP poslužiteljimu `time-c.timefreq.bldrdoc.gov` (IP adresa: `132.163.4.103`), a za automatsku nadgradnju, koja se provodi korištenjem standardnog HTTP protokola (TCP port 80), WormRadar kontaktira poslužitelj `webhost.ih.earthlink.net` (IP adresa `207.217.96.29`).

Bilježenje aktivnosti u log datoteke moguće je provoditi na tri razine: bilježenje poznatih napada, bilježenje varijanti, te bilježenje aktivnosti same aplikacije.

5. Postavke vatrozida

Ukoliko se WormRadar nalazi iza vatrozida, na vatrozidu je potrebno propustiti određeni dolazni i odlazni TCP/UDP promet. Tablica 1 daje detaljne informacije o konfiguraciji vatrozida.

Svrha	Protokol	Port	Smjer	IP adresa
Slanje upozorenja na centralni poslužitelj	UDP	23515	odlazni	68.157.174.28
Predefinirane emulacije	TCP	21	dolazni	–
	TCP	25	dolazni	–
	TCP	80	dolazni	–
	TCP	135	dolazni	–
	TCP	139	dolazni	–
	TCP	443	dolazni	–
	TCP	445	dolazni	–
	TCP	1433	dolazni	–
	TCP	1434	dolazni	–
	TCP	2745	dolazni	–
	TCP	17300	dolazni	–
	TCP	27374	dolazni	–
	UDP	137	dolazni	–
Dodatne emulacije	TCP/UDP	ovisi	dolazni	–
Automatsko osvježavanje	TCP	80	odlazni	207.217.96.29
Vremenska sinkronizacija	TCP/UDP	37	odlazni	132.163.4.103

Tablica 1: *TCP/UDP promet koji je potrebno propustiti za ispravno funkcioniranje WormRadar paketa*

6. Zaključak

WormRadar projekt predstavlja zanimljiv pokušaj da se formira distribuirani sustav za praćenje napada na Windows sustave s agentima koji kontinuiranim osluškivanjem te slanjem relevantnih podataka na središnju lokaciju omogućavaju praćenje učestalosti napada, te njihovu statističku obradu.
Osim toga svaki WormRadar agent može služiti kao neka vrsta lokalnog *honeypot* ili IDS sustava. Pravilnom konfiguracijom aplikacije administrator može pratiti pojavu određenih vrsta napada na mreži koju administrira; bez obzira dolaze li ti napadi izvana ili iznutra, te na taj način u ranoj fazi otkriti neke vrste napada na svoju mrežu.
Obzirom da je ovaj projekt tek u početnoj fazi, aplikacija ima manje nedostatke, koje bi u sljedećim inačicama svakako valjalo ispraviti.
Isto tako, dodavanje novih potpisa napada koji se prepoznaju provodi se ručno, što bi moglo biti unaprijeđeno dodavanjem neke vrste inteligencije unutar središnje lokacije koja bi na temelju dobivenih podataka mogla automatski prepoznavati nove uzorke.
Ukoliko se ispune ti zahtjevi, moguće je očekivati da bi WormRadar projekt mogao zaživjeti kao skalabilni sustav za detekciju i analizu napada na Windows platforme.