HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni problemi Microsoft Outlook 2000 programskog paketa

CCERT-PUBDOC-2003-03-09

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

Microsoft Outlook Express i Outlook 2000 predstavljaju jedne od najčešće korištenih klijentskih programa za slanje i čitanje elektroničke pošte. Microsoft Outlook je, zahvaljujući brojnim funkcijama, našao primjenu i u korporacijskim okruženjima. Lošu reputaciju, što se tiče sigurnosti, ovi su programski paketi dobili prilikom rasprostranjivanja Love Letter crva. Osnovni problem koji je omogućio široko rasprostiranje ovog crva bili su sigurnosni problemi u Outlooku. Ovi sigurnosni problemi došli su do izražaja kada je Microsoft uključio jednostavno sučelje za upravljanje porukama u Outlook 98/2000, koje je omogućilo iskorištavanje već postojećih sigurnosnih problema. Naravno, ne može se kriviti samo Microsoft za rasprostranjivanje crva, već i vrlo nizak stupanj sigurnosti koji je implementiran u pojedinim korporacijskim mrežama.

Osnovno pravilo zaštite od raznih virusa i crva je da se ne pokreću neprovjereni programi, a pogotovo ne privitci koji su došli s porukama elektroničke pošte od nepoznatih pošiljatelja. Ovo pravilo ne može se uzeti za konačno budući da crvi vrlo često dolaze u privitcima od poznatih pošiljatelja, što smanjuje mogućnost korištenja heuristike na osnovu navedenog pravila. Ovi problemi nastaju kada se razni makro virusi i drugi maliciozni programi repliciraju koristeći adresar na inficiranom računalu te se na taj način šalju poznatim primateljima.

Uznemiravajuća je činjenica ta da potrebno iskustvo za pisanje crva kao što je *Love Letter* ili *Melissa* nije veliko. Osnovno iskustvo s Visual Basic for Application programskim jezikom dovoljno je za kreiranje većine današnjih crva koji se rasprostiru putem elektroničke pošte.

Ovaj dokument objašnjava neke informacije o konstrukciji takvih programa da bi se bolje dobio pregled sigurnosnih problema u Outlook programskom paketu.

2. Najčešći sigurnosni propusti

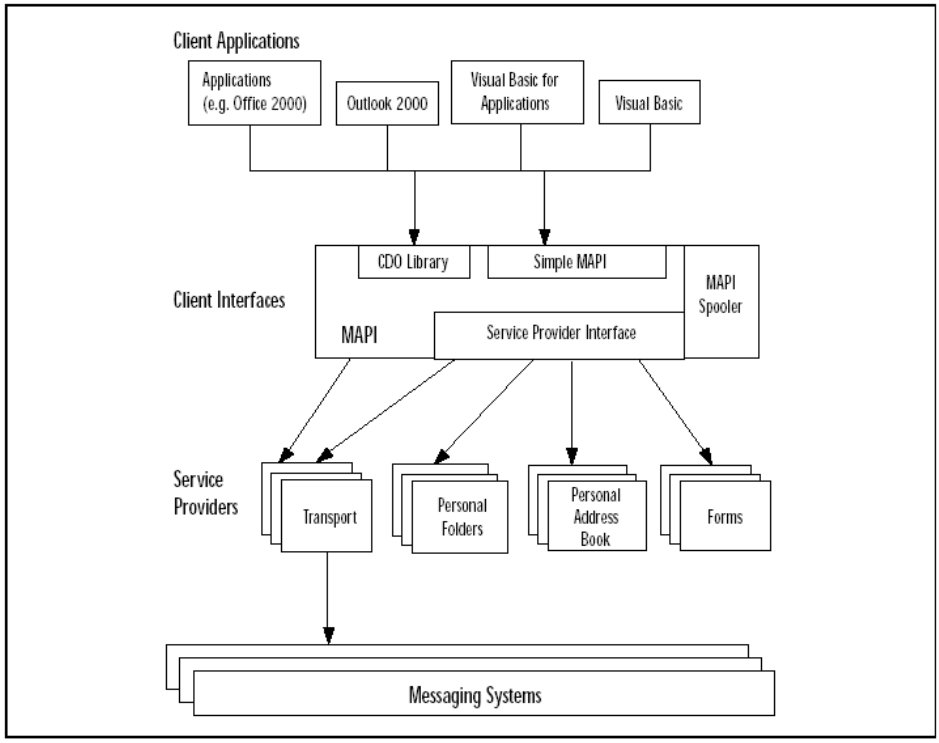
Microsoft je u Outlook 2000 dodao dvije glavne funkcionalnosti koje su omogućile pristup informacijama kreiranim u drugim Office 2000 aplikacijama. Glavna namjena ovih funkcionalnosti bila je integriranje svih aplikacija iz Office 2000 paketa, što u konačnici omogućava korisnicima jednostavno pisanje automatiziranih programa. Spomenute funkcionalnosti su:

- Pojednostavljeni pristup na *Messaging Application Program Interface* (MAPI) sučelje putem *Collaborative Data Objects* (CDO) biblioteke. CDO omogućava jednostavno korištenje MAPI-ja i drugih resursa, kao što je osobni adresar korisnika (engl. *Personal Address Book* – PAB) te različitih poštanskih sandučića. Gotovo svi makroi i programi koji se upotrebljavaju unutar Outlooka koriste CDO za pristup poštanskim sandučićima i adresarima – npr. kada se upotrebljava makro za slanje poruke elektroničke pošte na grupu kontakata iz adresara.
- Upotreba Visual Basic for Applications (VBA) u Outlooku 2000 putem CDO biblioteke. Ovaj postupak nije bio moguć u prijašnjoj inačici Outlooka.

Kao što se može vidjeti, MAPI predstavlja vrlo kompleksan sustav koji je jako pojednostavljen prema aplikacijama i korisniku. Microsoft je napravio MAPI kako bi se omogućilo drugim aplikacijama (npr. Internet Exploreru) slanje elektroničke pošte. S druge strane, budući da je MAPI integriran, krajnji korisnik uopće ne mora znati o njegovom postojanju. Dakle, MAPI se sastoji od različitih biblioteka koje aplikacijama omogućavaju vrlo jednostavno slanje elektroničke pošte, na osnovu čega tu aktivnost i mogu provoditi različite aplikacije čija je funkcija u potpunosti drukčija, kao što je npr. obrada teksta ili glazbenih zapisa. Osim toga, kompletan postupak može se i automatizirati – nakon što korisnik pokrene određenu funkciju ili pritisne tipke koje odgovaraju postavljenom uvjetu, aplikacija može putem MAPI sučelja poslati elektroničku poštu. Navedene funkcije vrlo su upotrebljive za krajnjeg korisnika. Međutim, problem predstavlja činjenica da je upotreba tih funkcija vrlo jednostavna i za malicioznog korisnika koji može nadasve jednostavno napraviti aplikaciju koja će poslati elektroničku poštu drugom korisniku. Tako su *Melissa* i *Love Letter* koristili upravo ove jednostavne pozive MAPI sučelja.

Važna činjenica vezana za MAPI je da aplikacija može pristupati različitim sustavima za upravljanje porukama ukoliko oni upotrebljavaju isto MAPI sučelje. Osim toga, upotreba CDO biblioteke ovaj postupak još više pojednostavljuje. Zbog toga je vrlo važno zapamtiti da svaki program pokrenut iz Outlooka zapravo ima iste privilegije kao i sam Outlook.

Ograničenja pristupa prilikom upotrebe na Windows NT ili 2000 operacijskim sustavima u ovom su slučaju postavljena samo na korisnički račun na Exchange ili drugom poslužitelju. Informacijama koje su pohranjene lokalno, a čiji je vlasnik upravo korisnički račun, može se pristupati bez ikakvih ograničenja, budući da korisnik ima sva prava nad navedenim podacima. Maliciozni korisnici u ovakve svrhe obično pišu različite programe i skripte u Visual Basic-u, Visual Basic for Applications ili JavaScript-u. Ovdje je potrebno napomenuti da se navedeni programi ne mogu pokrenuti izvan Outlooka, osim ako je na računalu instaliran *Windows Scripting Host*.
Na slijedećoj slici prikazan je okvir karakterističan za današnji Office programski paket. Okvir se sastoji od tri glavna dijela. Prvi dio opisuje programske pakete i jezike koje će korisnik vidjeti (kao što su npr. Outlook, Excel i Visual Basic). Drugi dio predstavlja sučelja koja djeluju kao posrednici između klijentskih aplikacija i dijelova koji omogućavaju različite funkcije. Sučelja, poput MAPI ili CDO biblioteke predaju informacije između dva krajnja nivoa. Na kraju, dijelovi koji omogućavaju različite funkcije predstavljaju neovisne elemente kojima mogu pristupiti različiti klijenti. Tako je moguće npr. imati centralizirani osobni adresar kojem mogu pristupati različite aplikacije. MAPI i drugi posrednici imaju pristup lokacijama osobnih direktorija korisnika, kao što je npr. My Documents direktorij na Windows operacijskim sustavima. Ova posrednička sučelja i biblioteke mogu prenositi informacije iz tih direktorija ili osobnog adresara sustavima za upravljanje porukama kao što je npr. SMTP (engl. *Simple Mail Transfer Protocol*) ili POP-3 (engl. *Post Office Protocol 3*) servisi na lokalnom računalu. Ovaj okvir od tri dijela je, kao što se može vidjeti, vrlo moćan. No, kao i bilo koji moćan alat, tako je i ovaj okvir potencijalno opasan. Maliciozni korisnik može iskoristiti navedene mogućnosti za pisanje aplikacija koje mogu uništiti ili kompromitirati podatke korisnika.
Na slici je prikazano funkcioniranje Outlook-a s navedenom MAPI shemom. Office 2000 programski paket (u kojem je i Outlook) sadrži sučelje za upravljanje porukama (MAPI) kao integralni dio, zajedno za programskim sučeljem (Visual Basic). Kako su Outlook i druge aplikacije iz Office 2000 programskog paketa vezane na CDO biblioteku i MAPI sučelje, krajnji korisnik može vrlo jednostavno stvarati i slati poruke elektroničke pošte. Microsoftova strategija prilikom ovog postavljanja paketa zasnovana je na činjenici da korisnici radije rade s informacijama nego s aplikacijama. Ovakva veza omogućava korisniku pristup istim, centraliziranim, informacijama korištenjem različitih aplikacija, umjesto da uvijek mora koristiti jednu te istu aplikaciju. Dakle, kada se jednom pristupa aplikaciji zapravo se pristupa klijentskom sučelju i servisima na lokalnom računalu (primjer takvog servisa je centralizirani osobni adresar).



Slika 1: MAPI arhitektura

2.1. Adresar

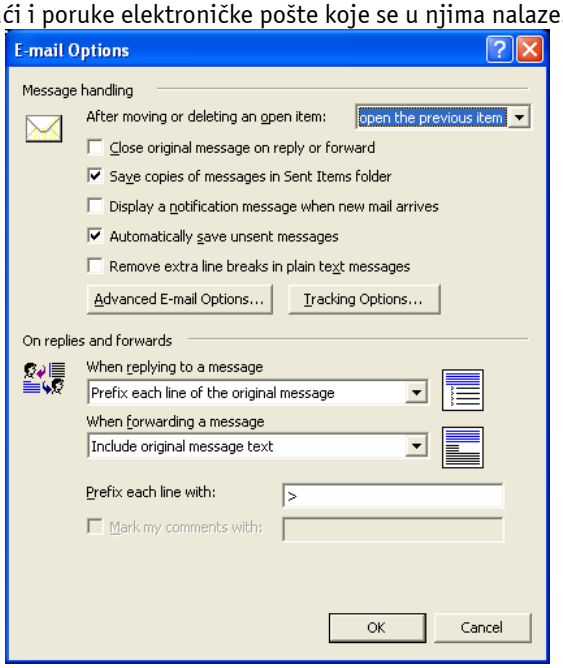
Adresar se sastoji od jednog ili više pod-adresara (koji se još nazivaju i spremnici). Adresarom upravlja *Address Book Provider*. Putem MAPI ili CDO poziva informacija se prenosi između adresara i klijenta. Postoji čitav niz spremnika koji se mogu vidjeti upotrebom *Address Book* izbornika.
Prilikom češće upotrebe adresara korisnici obično u njega spremaju sve više i više informacija. Budući da su svi spremnici unutar adresara uvijek dostupni, te sadrže veliki broj osobnih informacija, adresar predstavlja izvrstan resurs za upotrebu u napadu malicioznog programa. E-mail crv tako može doći do svih zapisa unutar adresara upotrebom samo nekoliko CDO poziva iz Visual Basica. Ovi se zapisi obično upotrebljavaju za širenje crva. Osim toga, maliciozni program može i kopirati kompletan sadržaj adresara te ga poslati na bilo koju adresu elektroničke pošte.

2.2. Poštanski sandučići

Outlook pruža korisniku pristup na različite datoteke koje sadrže poštanske sandučiće (engl. *Personal Folders*, .pst datoteke), kao i na poštanski sandučić koji se nalazi na Exchange poslužitelju. Svi poštanski sandučići koji se upotrebljavaju unutar Outlooka imaju četiri standardna pod-direktorija:

- *Inbox* – u ovom direktoriju nalaze se primljene poruke elektroničke pošte;
- *Outbox* – u ovom direktoriju nalaze se poruke elektroničke pošte koje još nisu poslane na odredište;
- *Sent Items* – u ovom direktoriju nalaze se sve poruke elektroničke pošte koje su bile uspješno poslane na lokalni SMTP poslužitelj. Ova opcija u Outlooku nije obavezna i moguće ju je isključiti opcijom Save copies of messages in Sent Items folder u Options/Preferences/E-mail Options izborniku, kao što je to prikazano na slici;
- *Deleted Items* – u ovom direktoriju nalaze se obrisane poruke elektroničke pošte. Ponovnim brisanjem poruka iz ovog direktorija one se nepovratno gube.

Budući da je lokalni korisnik ujedno i vlasnik ovih pod-direktorija, on nad njima i svim porukama koje se nalaze u tim direktorijima ima sva prava, osim prava za brisanje standardnih pod-direktorija koji moraju biti prisutni u poštanskom sandučiću. Međutim, zabrinjavajuća je mogućnost brisanja svih pod-direktorija, uključujući i poruke elektroničke pošte koje se u njima nalaze.



Slika 2: Opcija za isključivanje pohranjivanja poslanih poruka elektroničke pošte

Kako je na gornjoj slici prikazano, pohranjivanje poslanih poruka elektroničke pošte u *Sent Items* direktorij moguće je isključiti, no potrebno je napomenuti da istu aktivnost može provesti i maliciozni Visual Basic program, bez znanja korisnika.
Prilikom pokretanja malicioznog programa isti može poslati bilo kakvu poruku elektroničke pošte u korisnikovo ime ili čak obrisati sadržaj svih poštanskih sandučića, uključujući i onaj na Exchange

poslužitelju. Navedeni programi u Visual Basicu upotrebljavaju CDO biblioteku za ostvarivanje svojih malicioznih aktivnosti.

2.3. Visual Basic datoteke

Visual Basic datoteke već su spomenute u ovom dokumentu. Prilikom klasične upotrebe Visual Basica potrebno je programski kod prevesti u izvršnu datoteku koju je tek tada moguće pokrenuti. Međutim, postoje dvije iznimke:

- Visual Basic for Applications (VBA);
- Visual Basic Script (VBScript).

VBA omogućava izradu programa koji mogu biti jednostavni poput različitih makroa za upotrebu u Office 2000 aplikacijama, dok se VBScript obično upotrebljava na HTML stranicama. Budući da poruke elektroničke pošte mogu biti napisane u HTML-u, VBScript programe moguće je dodati tako da će prilikom čitanja poruke isti biti izvedeni.

Da bi Visual Basic programi bili pokrenuti bez prevođenja, na lokalnom računalu mora biti instaliran VB interpreter. Outlook i druge Office aplikacije često instaliraju takav interpreter u svrhu olakšavanja funkcije pisanja i izrade makroa. Ukoliko je na lokalnom računalu instaliran *Windows Scripting Host* (WSH), VBScript programi moći će biti pokrenuti samo izvan Office 2000 aplikacija.

WSH predstavlja interpreter koji omogućava izvođenje VBScript programa bilo gdje na sustavu. Ukoliko je WSH prisutan na računalu, potrebno je ustanoviti da li se isti upotrebljava od strane korisnika, a ukoliko to nije slučaj preporučuje se deinstalacija interpretera, budući da se s tim postupkom onemogućuje eventualno pokretanje malicioznog VBScript programa.

3. Specifični napadi

Od službenog izdavanja Outlook 2000 aplikacija, pronađen je određen broj sigurnosnih nedostataka prisutnih u implementaciji. Ti sigurnosni problemi postali su glavno sredstvo uspješnosti raznih malicioznih programa. Budući da je Outlook dio Office 2000 programskog paketa, sigurnosni problemi pronađeni u kompletnom programskom paketu vrlo se često mogu iskoristiti i u samom Outlooku, što je naročito prisutno kod postavljanja osnovnih (engl. *default*) parametara rada programa i interakcije s ostalima aplikacijama u Office 2000 programskom paketu.

3.1. Sigurnost privitaka

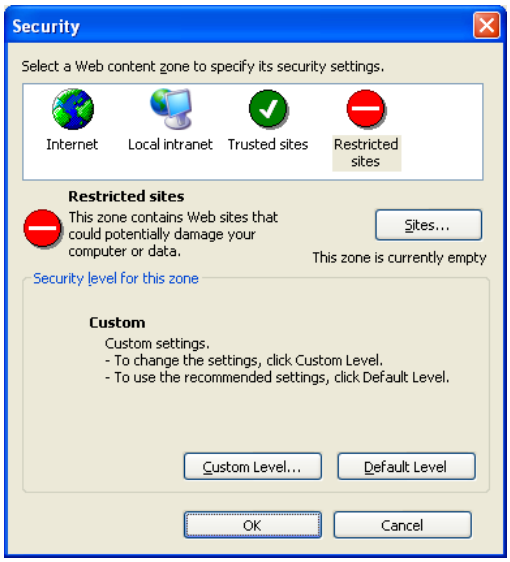
Datoteke koje su poslane kao privitci s porukama elektroničke pošte ne mogu se otvoriti na siguran način. Prilikom dvostrukog klika na datoteku u privitku, Windows operacijski sustav će pokrenuti izvršne datoteke dok će VBScript datoteke biti interpretirane i također izvedene. Prilikom ovog sigurnosnog problema korisnici trebaju obratiti naročitu pažnju na ispravnost privitka koji se pokreće. Vrlo je uobičajeno da razni virusi i drugi maliciozni programi pokušavaju prikriti svoju primjenu (tj. činjenicu da se radi o izvršnim datotekama) upisivanjem višestrukih ekstenzija. Ovdje je potrebno napomenuti da Windows operacijski sustav uvijek uzima u obzir samo zadnju ekstenziju. Za primjer možemo uzeti *Love Letter* virus koji je pokušavao sakriti svoju izvršnu datoteku postavljanjem imena poput *LOVE-LETTER-FOR-YOU.TXT.vbs*, što je manje iskusne i nepažljive korisnike natjeralo da povjeruju da se radi o tekstualnoj datoteci, dok je u biti riječ o VBScript programu. Neovlašteni korisnici iskorištavaju ovakve ranjivosti, koje su izraženije kod neiskusnih korisnika.

Neki tipovi privitaka mogu iskoristiti i sigurnosne probleme u samom operacijskom sustavu ili u drugim aplikacijama na računalu. Ukoliko u privitku dolazi datoteka s CIL ekstenzijom, koja zapravo predstavlja *Clip Art Information Library*, ista će omogućiti instalaciju za upotrebu s *Clip Gallery*, koristeći artgalry.exe. Kako je u datoteci artgalry.exe pronađen sigurnosni problem prepisivanja podataka na stogu, maliciozna CIL datoteka može ovaj problem iskoristiti za pokretanje proizvoljnih programa na računalu, što znači da u privitku ne mora biti konkretna izvršna datoteka, da bi neovlašteni korisnik izveo željeni program na udaljenom računalu.

3.2. Sigurnost osnovnih postavki

Kao i većina drugih Microsoftovih programskih paketa, osnovne postavke Outlook aplikacije postavljaju nesigurno okružje rada za korisnika. Budući da je većina korisnika zapravo nižeg stupnja

znanja, obično ostavljaju takvo nesigurno okružje rada, koje kasnije maliciozni korisnici vješto iskorištavaju u svoje svrhe.
Ovi sigurnosni problemi uglavnom su zasnovani na mogućnosti Outlook-a da interpretira HTML poruke elektroničke pošte. Ove poruke elektroničke pošte mogu u sebi sadržavati razne JavaScript, VBScript i ActiveX kontrole te Java applete, čiji stupanj izvođenja ovisi o sigurnosnim postavkama unutar Outlook-a.



Slika 3: Sigurnosne zone

Vrlo je važno razumjeti sigurnosne zone unutar Outlook-a te ih postaviti tako da se onemogući bilo kakvo izvođenje malicioznih programa i skripti, kao što je prikazano na gornjoj slici. Ovdje je potrebno napomenuti da su postavke sigurnosnih zona dijeljene između Internet Explorera i Outlooka, te ukoliko korisnici promijene postavke unutar Internet Explorera iste će se propagirati na Outlook. Problem koji ovdje nastaje je da korisnici vrlo često smanjuju sigurnosni nivo u Internet Exploreru da bi omogućili izvođenje svih elemenata Web stranica, što s druge strane umanjuje i sigurnost unutar Outlook-a te omogućava potencijalno izvođenje malicioznih programa.

4. Zaključak

U ovom dokumentu navedeni su osnovni sigurnosni problemi Microsoft Outlook 2000 programskog paketa. Kao i kod drugih programskih paketa, osnovnu mjeru zaštite korisnika predstavlja redovno održavanje sigurnosnog nivoa instaliranih programskih paketa i operacijskog sustava (redovito primjenjivanje sigurnosnih zakrpi).
Osim toga, korisnici se trebaju upoznati s svim opcijama vezanim za sigurnost Outlooka, kao i postavkama sigurnosnih zona koje predstavljaju glavna ograničenja postavljena pred izvođenje raznih komponenti HTML poruka elektroničke pošte.