

Rootkiti na Windowsima



Crne prognoze kažu da će 2006. godina biti obilježena pošašku rootkit-a. Epidemija zlo?udnog koda ubrzava već godinama, a s rootkitima se podiže na novu razinu. Ova tehnologija prijeti da će izmjeniti naše stavove o sigurnosti, a procjenu o zaraženosti nekog računala zlo?udnim kodom učini komplikiranijom.

Pojam rootkit označava tehniku prikrivanja. Zlo?udni kod se načini nevidljivim OS-u, uključujući antivirusni software i sistemske alate. Najgore je što prisutnost nekog rootkita može ostati nezapažena godinama.

Ova je tehnologija začeta početkom devedesetih na Unixu. Krajem devedesetih seli se na Windows sustave, kad su neki programeri počeli objavljivati setove alata koji dozvoljavaju modificiranje i proširivanje funkcionalnosti.

Neki rootkiti su tako dobro pakirani da je autoru zlo?udnog koda dovoljno samo editirati konfiguracijsku datoteku i poslati ga zajedno sa svojim malwareom. Centralno mjesto na internetu koje obraća ovu temu je <http://www.rootkit.com> - ovdje se mogu naći objavljeni rootkiti Vanquish, FU, Afx Rootkit 2005, NT Rootkit i Hacker Defender.

Medijska pozornost koju rootkiti dobijaju s prelaskom na Windows osvještava krajnje korisnike, ali i malware zajednicu koja bi ih mogla poticati u inkovitije koristiti protiv sve manjih tradicionalnih antivirusnih i antispaware rješenja. Da li će virusni, spyware i adware kod uskoro biti nemoguće obrisati osim formatiranjem diska i reinstalacijom OS-a?

Osnove rootkita

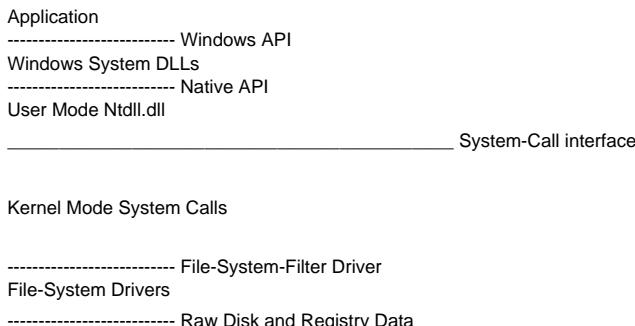
Na svojim počecima rootkiti su koristili jednostavne metode zamjene sistemskih alata verzijama koje skrivaju zlo?udne datoteke i procese. Tako bi, naprimjer, Unixov alat *ps* "zaboravio" izlistati aktivne zlo?udne procese o kojima informaciju dobiva iz kernela, a naredba *ls* previdjela bi datoteke. Razvojem sustava i antivirusnih rješenja, ova je jednostavna tehnika zamjene napuštena. Rad na modificiranju Windows Task Managera ili tasklist naredbe zahtjeva mnogo vremena i truda, a proizvod pada u vodu onog momenta kad korisnik pokrene antivirusni skener ili neki drugi alat za listanje procesa.

Sljedeći korak bio je napad na neki API koji koristi određena aplikacija za dobavu informacija, a ne na samu aplikaciju. Presretanjem API-ja kojim aplikacija dobiva popis aktivnih procesa, rootkit s popisa uklanja svoje ime i ime malwarea i oni postaju nevidljivi u Task Manageru ili alatu za listanje procesa. Ova tehnika rabi se i danas, a popis objekata koji se na ovaj način skrivaju je dugačak - datoteke, direktoriji, ključevi i vrijednosti u registry bazi, Windows servisi, pogonski programi, TCP/IP portovi, korisnički računi i procesi.

Primjerice, popularni Hacker Defender se sastoji od konfiguracijske i izvršne datoteke, hxdef100.ini i hxdef100.exe. Nakon pokretanja hxdef100.exe će sakriti sve datoteke, direktorije, pogonske programe, servise, procese i TCP/IP portove koji su navedeni u konfiguracijskoj datoteci. Osnovna konfiguracija će sakriti svaki od ovih objekata koji u imenu sadrži hxdef.

API nivoi

Windowsi sadrže nekoliko API nivoa:



S obzirom na sofisticiranost izrade, različiti rootkiti napadaju različite nivoje. Viši nivoi su bolje dokumentirani i kao takvi se lakše preseguju, ali niži nude bolju razinu nevidljivosti. Nadalje, ako rootkit presegne na Windows API nivou, sve aplikacije koje vuku podatke iz Native API nivoa neće prikazivati podatke u skladu s promjenom koju unosi rootkit. Nativne API funkcije imaju samo jednu funkciju, a to je pozivanje sistemskih servisa u Kernel Modu. Na nivou Kernela se izvršavaju bazični NT procesi - direktno pristupanje hardwareu preko funkcija koje manipuliraju resursima računala - memorijom, uređajima i procesima.

Rootkiti namijenjeni radu u user modu mogu sakriti svaki proces koji se pokreće pod istim korisničkim računom kao i zlouđni program, a najefektniji su ako taj korisnički račun ima Debug Programs privilegije odn., pripada grupi Debugger Users. Grupa Administrators prema osnovnim postavkama ima ove privilegije. U ovom slučaju, rootkit ima kontrolu nad svim procesima sustava, pa i onima pod Local System računom. Namotniji su rootkiti pisani za Kernel Mod, no korisnički račun pod kojim se pokreće zlouđni program mora imati privilegije za instalaciju drivera, odnosno pripadati grupi Administrators. Za izradu Kernel rootkita potrebno je već znanje i iskustvo.

Podjela rootkita nadalje slijedi klasifikaciju s obzirom na to da li zlouđni program preživljava reboot ili ne. Dijeli se na trajne (Persistent), koji se pokreću automatski prilikom podizanja sustava ili logiranja, te memoriske (Memory-Based), koji ne preživljavaju reboot jer nemaju postojani kod. Trajni se moraju pohraniti kod na disku, odnosno u registry bazi i datotečnom sustavu, kako bi se mogli pokrenuti bez upitivanja korisnika.

Unutrašnjost user mode rootkita

Najviši API nivo je Windows API user moda, dokumentiran u Platform Software Development Kitu (SDK).

Da bi Windows Explorer izlistao datoteke unutar nekog direktorija, pozvat će Windows API koji će pokrenuti funkcije FindFirstFile i FindNextFile implementirane unutar datoteke kernel32.dll (\windows\system32\). Korištenje naredbe "dir" unutar komandne linije pokrenuti će isti postupak, osim što će poziv doći od strane cmd.exe. Proces kojeg sačinjava izvršna datoteka u sebe učitava API kod iz dll datoteke.

API se importira u proces staticki ili dinamički. Staticko importiranje podrazumijeva stvaranje posebne tablice (import table) koja referencira na zahtijevani DLL i API, a koju OS loader provjerava prilikom pokretanja procesa - OS loader će itavu DLL u memoriski adresni prostor namijenjen procesu i ujedno mu omoguće vezu s referenciranim funkcijama. Kod dinamičkog importiranja proces poziva Windows funkciju LoadLibrary koja će itavu DLL, te funkciju GetProcAddress koja od OS-a dobiva informaciju o memoriskoj adresi funkcije eksportirane iz DLL datoteke. Program Dependency Walker (www.dependencywalker.com [1]) omogućuje pogled na staticke importiranja i eksportiranja, a profiliranje izvršne datoteke omogućuje pogled na dinamička importiranja.

Jedna od metoda koju koriste rootkiti je skeniranje import tablice odredenog procesa i zamjena reference funkcije iz sistemske DLL datoteke vlastitom, ili informacijom o memoriskoj adresi funkcije koju je rootkit prethodno direktno upisao u adresni prostor procesa. Na ovaj način proces je upisan, a postupak se naziva DLL import hooking. Poziv funkcije FindNextFile preusmjeren je tako na vlastiti kod - rootkit poziva originalnu funkciju iz kernel32.dll datoteke, ali prilikom njenog izvršavanja preuzima kontrolu nad outputom na način da prilikom listanja direktorija i datoteka izbací one koje namjerava sakriti odn., svoje vlastite datoteke. Prilikom

dinam?kog importiranja, rootkit mora upecati GetProcAddress da bi dobio adresu memorijskog prostora funkcije i aplikaciji koja ju je pozvala vratiti svoju vlastitu funkciju - ovu metodu koristi rootkit Vanquish.

Rootkit još mora sakriti i vlastiti proces - ve?ina nativnih Windows APIja koji obavljaju zadatke vezane uz datoteke, memoriju i procese, koriste funkcije nižih APIja koji predstavljaju su?ejje prema APIma user moda. Niži APIji smješteni su i eksportiraju se iz datoteke ntdll.dll (\windows\system32\). Da bi prikazao aktivne procese, Task Manager koristi API NtQuerySystemInformation koji je implementiran unutar datoteke tdll.dll, a rootkit mora presresti ovu funkciju i modificirati njen output.

Windows API, prethodno spomenut, koji lista direktorije i datoteke, poziva funkciju datoteke Ntdll.dll koja se zove NtQueryDirectoryFile i manipulacijom njenih izlaznih podataka utje?e na podatke koje ?e naknadno vratiti funkcije FindFirstFile i FindNextFile. Rootkitovi ?e?e pecaju funkcije API-ja viših nivoa jer je to jednostavnije, a i mnogi sistemski utility koriste upravo ove više funkcije.

Postoji još jedna rootkit tehnika. Popularni Hacker Defender patchira Windows API funkcije - upisuje svoj kod u ciljani proces tako da izmjeni prvi nekoliko bajtova originalne funkcije tog procesa i preusmjeri kontrolu na rootkit funkciju. Nakon uspostavljenе kontrole nad procesom, rootkit poziva svoju verziju funkcije i manipulira rezultatima koje ?e vratiti pozivnoj aplikaciji.

Unutrašnjost Kernel Mode rootkita

Ovaj tip rootkita, koji se naziva i NT rootkit, sofisticiraniji je jer presre?e API-je iz kernel moda i peca sistemske pozive. Funkcije sadržane u datoteci ntdll.dll sistemski su pozivi funkcijama iz kernel moda. Identifikacija sistemskih API-ja vrši se preko dodijeljenih brojeva, tako da nativna API funkcija inicira sistemski poziv slanjem broja funkcije kernel moda. Ovi se brojevi nalaze u tablici koja referencira na odre?ene funkcije sistemskih poziva. Na isti na?in kao što funkcionira pecanje DLL importiranih podataka, rootkit manipuliranjem brojevima mijenja poziv na željenu funkciju. Metoda Hacker Defendera tako?er je primjenjiva i u kernel modu, iako patchiranje ne koristi niti jedan od objavljenih rootkitova.

Još jedna popularna tehnologija je direktna manipulacija objektima. Ovom metodom napad se vrši na samu strukturu podataka karnela, umjesto na API-je koji vra?aju informacije o strukturi podataka. Naprimjer, da bi sakrio sebe, rootkit ga "brise" sa kernelovog popisa aktivnih procesa. Funkcija NtQuerySystemInformation ne?e prijaviti proces jer ovisi o podacima sa ovog popisa, iako ?e kernel i dalje obra?ivati threadove unutar tog procesa. Rootkit FU se skriva koriste?i direktnu manipulaciju kernel objektima.

Posljednja metoda kojom se koriste kernel rootkiti je skrivanje podataka unutar file system filter drivera. Ovaj informacijski nivo stoji na vrhu file system drivera, od kojih je jedan, naprimjer, NTFS, a ispod API-ja sistemskih poziva, te kao takav ima uvid u cijelokupnu aktivnost datote?nog sustava. Naprimjer, svi "on-access" virus skeneri koriste presre?u operacije otvaranja datoteka; na ovaj na?in skeniraju datoteke prije nego ova operacija zapo?ne.

NT rootkitovi koriste file system filter driver da bi presreli upite o direktorijima i iz njegovog outputa uklonili reference na zlo?udni kod. Na ovaj na?in, svaka aplikacija u user modu ili neki drugi driver u kernel modu, a koji zahtjevaju listanje direktorija, mogu biti mjesto u kojem se skriva NT rootkit.

čet, 2006-05-11 12:03 - Uredništvo**Vijesti:** [Windows](#) [2]

Kategorije: [Sigurnost](#) [3]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/6>

Links

- [1] <http://www.dependencywalker.com/>
- [2] <https://sysportal.carnet.hr/taxonomy/term/12>
- [3] <https://sysportal.carnet.hr/taxonomy/term/30>