Nähtamatud pahalased

9. november 2005 - 19:02 Autor: Peep Loorits

(Arvutimaailm 9/2005)

Koos Interneti leviku laienemisega on suurenenud oluliselt pahavara levik. Kuid pahavara arendajatel on probleem - pidevalt hingavad kuklasse mitmesuguste tõrjesüsteemide arendajad. Seetõttu toimub intensiivne uute võimaluste ja tehnoloogiate otsimine ja areng. Tõusvaks trendiks on saanud tehnoloogiad, mis võimaldavad pahalasel jääda märkamatuks nii tõrjeprogrammidele kui ka opsüsteemile. Üldiseks nimetuseks kõigile sellisele on saanud rootkit, mille all mõeldakse nii nähtamatuks jäävat pahalast ennast kui ka meetodeid ja valmis koodijuppe, mis annavad mõnele pahaprogrammile peitumisvõime.

Rootkit kui mõiste on tänapäeval veidi laialivalguv, kuid iseenesest ei ole see Unixi maailmast pärit termin uus. Unixites püütakse rootkiti abil salaja midagi toimetada roodu õigustes, katsudes jääda nähtamatuks administraatorile. Nimetus tuleneb kahest mõistest: root ehk administraatori õigused ja kit ehk vahendite kogu rooti õiguste saamiseks või nendes õigustes salaja toimetamiseks.

Unixi rootkitid olid olemas juba ammu enne Windowsi tulekut. Esimese põlve rootkitid püüdsid asendada või muuta mingeid süsteemifaile. Peamiseks märklauaks olid Unixi sisselogimisprogrammid, kus püüti niimoodi kasutajate salasõnu. Vastuseks süsteemi kontrollivahendite tõhustumisele koliti piltlikult öeldes kõvakettalt mällu ehk teisisõnu - rootkit sokutab mällu laetud programmikoodi, püüdes kaaperdada seal mingeid tegevusi. Nö kolmanda põlve rootkitid tungivad juba süsteemi tuuma.

Kahte sorti rootkitte

Praegused rootkitid võib laias laastus jagada kaheks: userlandi rootkitid, mis toimetavad töötavas programmikoodis ja sellega seotud operatsioonisüsteemi osades ning tuuma ehk kerneli rootkitid, mis manipuleerivad juba tuuma objektidega. Teisalt võib rootkitte jagada püsiva koodiga ja mälu baasil toimetavateks. Püsiva koodiga rootkitid on enamasti seotud mingi pahavaraga. Kuna selline pahavara peab startima koos süsteemi laadimisega või mõne kasutaja sisselogimisel, peab ta hoidma oma koodi kuskil püsivas kohas nagu registris või failisüsteemis.

Püütakse kasutada ka selliseid ebaharilikke kohti, nagu näiteks bad sectorid kõvakettal (mis tegelikult ei pruugigi nii pahad olla - lihtsalt Windows arvab nii), videomälu jms. Mälupõhised rootkitid on aga dünaamilised ega oma püsikoodi, seetõttu ei ela nad süsteemi laadimist üle, kuid see polegi probleemiks. Näiteks serverid töötavad pidevalt ja restart on pigem erand. Võimalik on ka selline stsenaarium, et pärast laadimist nakatatakse server uuesti, mille eest on toimiv rootkit juba varakult hoolitsenud.

Kasutajarezhiimis rootkitid on hetkel Windowsis kõige levinumad. Need kasutavad Windowsi API (Aplication Program Interface) võimalusi. Paraku kasutavad rootkitid neid võimalusi kurjasti ära. Lihtsamad kaaperdavad mingeid päringuid, näiteks FindFirstFile/FindNextFile, mida kasutavad failisüsteemi uurivad vahendid (Windows Explorer, käsurida). Sellised utiliidid saavad rootkiti poolt filtreeritud infot failisüsteemi kohta ja me näeme ainult seda, mida rootkit lubab. Windowsis on ka teatud madalama taseme API, mis toimetab vahendajana kasutajarezhiimis kliendi ja kernelirezhiimis töötavate teenuste vahel.

Arenenumad rootkitid oskavad kaaperdada failisüsteemiga, registriga ja ka protsessidega seotud madalama taseme API funktsioone. Nii saavad nad jääda nähtamatuks mitmete skännerite eest. Põhjalikku ülevaadet kasutajarezhiimis rootkittide toimemehhanismidest ja Windowsi poolt pakutavatest võimalustest rootkittide loomiseks võib lugeda SecuriTeami kodulehelt. Kirjutise autor on ühtlasi NtIllusion nimelise rootkiti kirjutaja.

Kernelirezhiimis rootkitid on kõige võimsamad, sest nad oskavad manipuleerida kernelirezhiimis andmestruktuuridega. Nii on võimalik pahavara programmidel jääda varju näiteks Task Manageri ja muude selliste protsesse näitavate programmide eest. Kuna sellised rootkitid võivad kontrollida kogu süsteemi käitumist, on kõige hullem see, et tegelikult ei saa enam midagi usaldada.

Kuidas neist lahti saab?

Hetkel on praktiliseks kasutamiseks olemas kaks rootkittide avastamise/kõrvaldamise programmi: SysInternalsi Rootkit Revealer ja F-Secure'i Black Light. Mõlemad programmid kasutavad sarnaseid avastamismeetodeid, vaadatakse süsteemi kõrgelt tasemelt ja võimalikult madalalt tasemelt ning võrreldakse tulemusi. Kuid paraku oskavad uuemad või modifitseeritud rootkitid neidki programme petta.

Ühe väga huvitava mõttearenduse leiab Joanna Rutkowska kodulehel olevast dokumendist, kus autor näitab, et see meetod, mida kasutavad Rootkit Revealer ja Black Light, ei võimaldagi põhimõtteliselt avastada kõike. Selleks, et suurendada avastamise tõenäosust, peaks juba dubleerima osa operatsioonisüsteemist, mis on aga praktiliselt võimatu. Pealegi, nagu autor näitab, saab ikkagi eeltoodud meetodit kasutavat avastajat lollitada. Parema tulemuse saab, kui ühendada eeltoodud meetod viirustõrjete poolt kasutatavate meetoditega. Sellist lähenemist kasutavad Microsofti uurijad oma projektis Strider GhostBuster.

Üks Hiina uurijate grupp on loonud programmi nimega IceSword, millega saab üksipulgi uurida Windowsi ja avastada jälgi rootkittidest ning neid ilmselt ka kõrvaldada. Kasutan sõna ilmselt sellepärast, et programm on hiinakeelne ja lihtsalt pole võimalik kõiki võimalusi teada saada. Tundub aga, et IceSword on kõvaks pähkliks rootkittide kirjutajatele.

Eelpool mainitud dokumendi autor, sõltumatu uurija Joanna Rutkowska esines hiljuti Malaisias toimunud turvalisuse konverentsil „5th Hack In The Box Security". Ettekandes analüüsis ta olukorda ja pakkus välja teesid, kuidas luua efektiivset rookittide ja üldse pahavara vastu suunatud tarkvara. Presentatsiooni võib allalaadida autori kodulehelt. Samast võib alla laadida ka programmi nimega Sytem Virginity Verifier, mis on loodud neid põhimõtteid arvestades, kuid palju häid mõtteid on programmis veel realiseerimata.

Huvitav on märkida, et mitmed rootkitid on loodud vabavarana. Neid saab vabalt alla laadida, ka lähtekoodid on mitmetel saadaval. Üheks keskseks kohaks on rootkit.com , kus on kirjeldused paljudele rootkittidele ja viited nende arendajate kodulehtedele; on foorumid ja saab ka näidisasju alla tõmmata. Teine selline, aga laiema temaatikaga koht on Phrack. Kuid rootkitte ja sellega seonduvaid utiliite saab edukalt ka müüa. Üheks tuntumaks ja edukamaks projektiks on ilmselt Hakcer Defender, mis üldiselt on avatud koodiga vabavara, kuid sellel on ka võimekam kommertsvariant.

Autori väitel on tema tarkvara müüdud üle 100 000 korra. Hakcer Defender on kasutajarezhiimis toimiv rootkit, mis oskab varjuda enamiku eelpool nimetatud avastamisprogrammide eest. Rootkiti autor pakub ka mitmeid muid pahavarategijatele huvipakkuvaid utiliite, millest tuntuim on Morfine. Morfine, lisatuna pahavara koodi, võimaldab pidevalt muuta pahavara signatuuri. Signatuuri järgi aga tunnevad tõrjujad pahavara ära. Tegelikult käib siin pidev kassi-hiire mäng, kogu aeg toimub nii tõrjeprogrammide kui Morfini täiustamine.

Üheks näiteks rootkiti-laadsete tehnoloogiate kasutamisest on viimase aja CWS (CoolWebSearch) gruppi kuuluvad troojad/nuhkvarad. Need pahalased kaaperdavad Internet Exploreri ja Windowsi töölaua ning on ühed raskemini avastatavad ja kõrvaldatavad nuhkvarad üldse. CWS.Realyellowpage on aga eriti vastik tegelane. Lisaks juba suhteliselt tavapärasele nimevahetuse trikkidele ja ootamatute seoste tekitamisele IE-ga oskab ta ka oma protsesse ja faile varjata nii Task Manageri, Windows Exploreri kui teiste analoogsete programmide eest. Tema kõrvaldamine on suhteliselt problemaatiline, CWS Shreder siinkohal igatahes ei aita.

Proovisin ka praktikas eelpool nimetatud programmide toimimist. Selleks lasin käiku Hacker Defenderi ühe variandi, mis ei ole kõige võimekam. Juhtus see, et kataloog, milles paiknesid programmi failid, muutus nähtamatuks. Seejärel käivitasin nii Rootkit Revealeri kui ka Black Lighti. Mõlemad programmid leidsid pahalase üles, aga sellega asi ka piirdus. Seejärel proovisin käsurealt toimivat utiliiti System Virginity Verifier. See leidis ka kõik üles ja oli võimalik näha päris täpselt, kus ja mis on viltu. Paraku on sellisest infost kasu põhiliselt programmeerijatel ja süsteemi uurijatel.

Kõige parema tulemuse andis programm IceSword. Hoolimata hiinakeelsetest menüüdest on asi enam-vähem arusaadav: näha olid kõik kadunud failid ning rootkiti poolt tekitatud varjatud teenus ja protsess. Kui need sai seisma pandud, muutusid programmi kataloogis olevad failid jälle nähtavaks. Lõpuks uurisin veel seda, kuidas suhtub asjasse viirusetõrje NOD32. Niikaua, kuni varjatud teenus toimis, ei näinud viirusetõrje pahalast, kuid pärast teenuse seismapanekut leidis NOD32 kohe rootkitiga seotu üles.

Seega, nagu näha, on hetkel kõige võimekam IceSword. Mõningase katsetamisega (et taibata, mida konkreetsed menüüd teevad) saab selle programmi abil ilmselt pahalasest ka jagu.

Kokkuvõtteks

tuleb tõdeda, et rootkittide näol on tegu äärmiselt ohtliku pahavaraga. Nagu eeltoodust näha, on paljude rootkittide avastamine problemaatiline, aga päris lahti saamine on juba omaette kunsttükk. Tundub, et antud hetkel on ainuke enamvähem kindel meetod Windowsi uuesti installeerimine koos kõvaketta eelneva formaatimisega.

Lihtsam on rootkittidest ja üldse igasugusest pahavarast hoiduda. Selleks, et vähendada nakatumise tõenäosust, peab arvutis olema toimiv ja täiendatud viiruse- ja nuhkvaratõrje ning abiks on ka korralikult toimiv tulemüür. Tulemüür peaks olema ka mõnes välisseadmes, näiteks ruuteris. Ja muidugi Windows ise peab olema igatpidi uuendatud ja täiendatud.

Lingid samal teemal:

- Phrack
- Ajalugu
- SecuriTeam,kasutajarezhiimis rootkittide ülevaade
- Rootkit Revealer
- Black Light
- Joanna Rutkowska mõtted rootkittide avastamisest
- Microsoft rootkittidest
- IceSword
- Joanna Rutkowska
- Hacker Defender
- Hacker Defenderi kõrvaldamine
- CWS.Realyellowpage

- Lahendused