Inspiratron.org - Natural language processing, machine learning and cybersecurity

Kratka istorija malware-a | ?etvrti deo: rootkit

by Nikola Miloševi? - Wednesday, December 19, 2012

https://inspiratron.org/blog/2012/12/19/kratka-istorija-malware-a-cetvrti-deo-rootkit/

U predhonim ?lancima smo se pozabavili prvo DOS virusima, nakon toga smo prešli na prve Windows virusi i prve makro viruse, nakon ?ega smo prešli opis mail crva, da bi na kraju došli do crva kojim nije potrebna korisni?ka interakcija. Ovaj ?lanak ?e biti predposlednji deo u seriji o malware-u i u njemu ?emo se pozabaviti rootkitovima, kao i jednom malware-u uz pomo? kog su ucenjivane žrtve.

Za po?etak treba definisati novu vrstu malware-a koji je dobio ime rootkit. Samo ime govori da se radi o ne?em što korenom. Zapravo rootkit je vrsta malware-a koji se integriše u operativni sistem i postane deo kernela ili korisni?kog sloja operativnog sistema. Dakle deo korena korisni?kog iskustva pri koriš?enju ra?unara. S obzirom da rootkit može postati deo kernela ili deo korisni?kog sloja operativnog sistema postoje dve vrste root kitova. Jedan je kernel level rootkits - oni postaju deo kernela, ?esto se instaliraju poput modula operativnog sistema ili drivera i gotovo ih je nemogu?e detektovati i ukloniti. Rootkiti su poznati po tome što uglavno sadrže funkcijonalnost skrivanja file-ova i procesa. Ukoliko sam kernel operativnog sistema se modifikuje na na?in da vra?a neta?ne podatke o fileovima na hard disku ili pokrenutim procesima, ne?e mo?i ni jedan anti virusni software da otkrije da se na ra?unaru nalazi neki malware, jer i on prikuplja podatke od operativnog sistema. Druga vrsta rootkitova su user level rootkits, koji se umetnu u neke sistemske funckije ili biblioteke. Na ovaj na?in odre?ene komande operativnog sistema, koje koriste te biblioteke ili funkcije ne vra?aju dobar rezultat. Na primer rootkit korisni?kog sloja može da zameni ls ili ps komandu u linuxu, pa tako da ne izlistava odre?ene fajlove ili procese.

Prvi rootkit koji se pojavio nije bio napisan od strane standardnih pisa?a virusa, ve? od strane jednog muzi?kog giganta. Prvi rootkit je napravio Sony i poprili?no ocrnio njime svoju reputaciju.

Sony BMG - Je nastao 2005 godine i napravljen je od strane jedne od najve?ih izdava?kih kompanija. Naime Sony je imao ideju da zaštiti prava svojih izdanja, tako što ?e uz pomo? rootkita da detektuje i zabrani kopiranje. Sony BMG rootkit je bio sastavni deo 52 albuma, me?u kojima i album Ricki Martina i Kelly Minogue. Kada bi se muzi?ki disk ubacio u obi?an CD player, liniju ili diskmen ne bi se desilo ništa. Me?utim, ukoliko bi se disk ubacio u ra?unar instalirao bi se rootkit koji bi sebe i sakrio, kao i sve fajlove koji sadrže sys i kontrolisao na koji na?in korisnik može da pristupi muzici sa diska. Funkcionalnost da sakriva sve fajlove koji po?inju sa sys su iskoristili drugi pisa?i malware-a, sakrivaju?i svoje fajlove uz pomo? imenovanja. Direktor digitalne prodaje u Sony BMG, Thomas Hesse, je izjavio jednom prilikom da ve?ina ljudi ni ne zna šta je rootkit, pa ne vidi razlog za brigu. Ova izjava je izazvala oštre reakcije, s obzirom da se ista predpostavka može postaviti za mnoge stvar, koje treba da nas se ti?u. Epilog skandala je bila tužba koja je završila tako što je Sony ponudio korisnicima povra?aj novca i besplatno skidanje muzike sa interneta. Tako?e pojavio se i komentar da ukoliko slušate Riki Mertina ili Keli Minjon, zaslužujete da budete zaraženi.

Storm Worm - Sedam godina nakon LoveLetter mail virusa pojavio se jedan mail virus koji još snažnije i uspešnije iskoristio socijalni inženjering. Naime, vodio se Makijevelijevom logikom da je bolje biti onaj koga se plaše, nego onaj koga vole. S obzorom da je ovaj virus nešto što je ve? vi?eno nekoliko puta mnogo godina pre, nije se moglo predpostaviti da ?e imati toliko veliki efekat. Moglo se predpostaviti da ?e ljudi ve? biti spremni na ovakvu pretnju, ali o?igledno nisu. Naime virus je slao mail sa naslovom “230 dead as storm batters Europe.” Kada bi prilog bio otvoren bio bi zapravo otvoren trojanac, koji instalira backdoor (program uz pomo? kog napada? može da kontroliše ra?unar), rootkit, koji bi ga sakrio i ra?unar bi se pridružio botnet mreži. Botneti su armije zombi ra?inara, koji mogu biti upotrebljeni za razne svrhe, poput slanja spam poruka, distribuirani denail of service i sli?no. Ovaj virus je zarazio oko 10 miliona ra?unara.

Mebroot (2008)- Ovaj malware je doneo jednu novinu, mogao je da zarazi ra?unar koji je u browseru otvorio zaraženu internet stranicu. Koristio je exploit u browseru i jedan od prvih sajtova koji su širili Mebroot je bio sajt Monike Beluci. Kada bi se ra?unar zarazio, na njega bi se instalirao rootkit koji bi sakrivao mebroot od rootkit detektora, koji su brzo postali deo mnogih internet security paketa. Mebroot je sakupljao podatke o tome šta je korisnik kucao i zapravo ga u nekoj meri špijunirao. Ove podatke je slao napada?u. Jedan je od retkih malware-a koji su dobro debagovani i gotovo nikad nije se rušio. Bio je toliko napredan da ukoliko bi se kojim slu?ajem srušio operativni sistem, Mebroot bi skupio diagnosti?ke podatke o padu sistema, kao i trace podatke i poslao ih autoru ovog malware-a, kako bi u narednoj verziji bio bolji. Remote quality assurance za malware!

Conficker(2008) - Conficker je zarazio jako brzo desetine miliona ra?unara širom sveta. Koristio je ranjivosti Windows-a, kao i krekovanje slabih lozinki pomo?u nekoliko naprednih tehnika. Kada bi ra?unar bio zaražen, instalirala bi se zadnja vrata (backdoor), tako da bi dodatni malware mogao biti instaliran. Ra?unaru bi zabranio da poseti sajtove ve?ine proizvo?a?a antivirusnih alata. Tako?e kreirao bi veliku botnet mrežu, me?utim ova botnet nije nikad iskoriš?ena ni za kakav napad, iako je bila jako kompleksna. Zbog ove ?injenice Mikko Hypponen, glavni istraživa? u F-Secure-u je izjavio da je ovaj malware do danas velika misterija.

Jedan od interesantnih malware-a koje bih pomenuo je ransomware, koji je služio za ucenjivanje korisnika da plate napada?u 120 dolara. Ovaj malware bi enkriptova Office i media fajlove na napadnutom ra?unaru, što bi dovelo do toga da korisnici ne mogu da pristupe svojim datotekama, dok ne plate napada?u, koji bi im dao klju? uz pomo? kog mogu da dekriptuju svoje fajlove.

Na ra?unare je uspevao da u?e ili pomo?u ranjivosti na browseru i zaraženih web sajtova, ali i pomo?u zaraženih PDF fajlova, koji bi sadržali skriptu koja skida i instalira ovaj malware. Kada bi se napad završio, malware bi izmenio desktop korisnika da izgleda na slede?i na?in:

“HOW TO DECRYPT” txt-fajl na desktopu je sadržao slede?u poruku:

```
Attention!!!

All your personal files (photo, documents, texts, databases, certificates, kwm-files, video)
have been encrypted by a very strong cypher RSA-1024. The original files are deleted. You can
check this by yourself - just look for files in all folders.

There is no possibility to decrypt these files without a special decrypt program! Nobody can
help you - even don't try to find another method or tell anybody. Also after n days all
encrypted files will be completely deleted and you will have no chance to get it back.

We can help to solve this task for 120$ via wire transfer (bank transfer SWIFT/IBAN). And
remember: any harmful or bad words to our side will be a reason for ingoring your message and
nothing will be done.

For details you have to send your request on this e-mail (attach to message a full serial key
shown below in this 'how to..' file on desktop): [email address]
```

Poruka bi sadržala i email adresu napada?a, kao i specifi?ni identifikacioni token koji bi trebao da se pošalje napada?u, kako bi on mogao da generiše klju?. Interesantno je da je napada? zaista slao pošteno klju?eve onima koji bi platili 120 dolara. Zbog toga mail koji je bio naveden

u poruci nije blacklistovan, što ve?inom ?ine antivirusne kompanije, kada nai?i na neku mail adresu u kodu malware-a.

Fajlovi koji bi bili kriptovani su: .jpg, .jpeg, .psd, .cdr, .dwg, .max, .mov, .m2v, .3gp, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .rar, .zip, .mdb, .mp3, .cer, .p12, .pfx, .kwm, .pwm, .txt, .pdf, .avi, .flv, .lnk, .bmp, .1cd, .md, .mdf, .dbf, .mdb, .odt, .vob, .ifo, .mpeg, .mpg, .doc, .docx, .xls, and .xlsx.

U narednom postu ?emo se pozabaviti malware-om koji je doneo novu dimenziju u ovu oblast. Odnosno malware-om koji je uspevao da sabotira proces oboga?ivanja uranijuma, kao i dalji razvoj malware-a, koji su preuzele obaveštajne i vojne službe nekih država. Naravno radi se Stuxnetu, DoQu i Flame-u.

- Kratka istorija malware-a | Peti deo: Neka rat po?ne
- Kratka istorija malware-a | Tre?i deo: crvi (worms)
- Kratka istorija malware-a | Drugi deo: Windows era
- Kratka istorija malware-a | Prvi deo: Po?eci