Sigurnost računalnih sustava

Zlođudni kod

doc. dr. sc. Ante Đerek
izv. prof. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Što je zlćudni kod?

- **Zlćudna funkcionalnost** (engl. malicious logic) je sklopovlje, firmware ili programska podrška koja je namjerno uključena ili ubačena u sustav radi štetnih ciljeva.
  - Obratiti pozornost da se ne radi samo o kodu
  - Ubacivanje zlćudnog koda u firmware čvrstog diska
    - https://www.malwaretech.com/2015/04/hard-disk-firmware-hacking-part-1.html
    - http://spritesmods.com/?art=hddhack
- Mi ćemo se pozabaviti **zlćudnim kodom**
  - Malware – MALicious softWARE

Neke osnovne činjenice

- Zloćudni kod je značajan mehanizam djelovanja raznih napadača
  - Krađom vjerodajnica moguće je napraviti značajnu štetu, ali su ipak ograničene mogućnosti u odnosu na zloćudni kod
- Izuzetno dinamično područje
- Terminologija nesređena

Klasifikacija zloćudnog koda (1)

- Način širenja
  - Na koji način dolaze do računala žrtve
    - Privitak u porukama elektroničke pošte
    - Web
    - Prijenosni mediji (primjeri zaraženih CD-ova, USB-ova)
- Način pokretanja
  - Na koji način započinje njihovo izvršavanje
    - Samostalno – bez intervencije čovjeka
    - Uz intervenciju čovjeka

Klasifikacija zloćudnog koda (2)

- Monolitni ili modularni
- Platforma
  - Kako/gdje se izvršava zloćudni kod
    - Direktno kao aplikacija na operacijskom sustavu
    - Unutar neke aplikacije (MS Office, Adobe Acrobat Reader, Web preglednik)
      - Modifikacija koda aplikacije
      - Izvršavanje unutar aplikacije
- Perzistencija
  - Perzistentni i neperzistentni (engl. fileless)

Klasifikacija zlćudnog koda (3)

- Način prikrivanja od korisnika
  - Dio su nekakve aplikacije
    - Trojanski konji
  - Prikrivanje na razini operacijskog sustava
    - rootkits
- Zlćudna funkcionalnost
  - Backdoor, RAT, cryptominer, dropper, downloader, ucjenjivački kod, bot

Često spominjani zloćudni kod (1)

- Virusi
  - Temeljna karakteristika je da se šire tako što se ubacuju u izvršne kodove legitimnih programa te se pokreću njihovim pokretanjem
- Crvi
  - Temeljna karakteristika je da se mogu samostalno širiti putem mreže (ranjivi servisi, dijeljeni diskovi)
- Downloader
  - Zloćudni kod koji skida i instalira neki drugi zloćudni kod
- Dropper
  - Zloćudni kod koji sadrži drugi zloćudni kod te ga postavlja na kompromitirano računalo

Česti spominjan zloćudni kod (2)

- Logička bomba (engl. logic bomb)
  - Zloćudni kod koji obavlja nekakvu zloćudnu aktivnost kada se ispune određeni uvijeti
    - Nešto oblika `if (conditions_met) then do_bad_stuff()`
- Špijunski zloćudni kod (engl. spyware)
  - Zloćudni kod koji na neki način izvlači podatke korisnika računala
    - Lozinke, pohranjene lozinke u Web preglednicima, podatke iz raznih aplikacija
- Alat za udaljen pristup (engl. remote access tool)
  - Nije nužno zloćudni kod, primjerice *downloader* može instalirati TeamViewer

Često spominjan zloćudni kod (3)

- Trojanci (engl. Trojan horse)
  - Temeljna karakteristika je da se pretvaraju kako obavljaju neku korisnu funkciju dok u biti sadrže maliciozni teret
  - Korisnu funkciju mogu doista i obavljati, ali je onda bolje govoriti o “backdooranoj” programskoj podršci
- Ucjenjivački zloćudni kod (engl. Ransomware)
  - Kod koji na nekakav način pokušava ucijeniti vlasnika kompromitiranog računala
  - Najčešći oblik je šifriranje sadržaja diska (samo podataka) te se potom vlasnik ucjenjuje s određenim iznosom kako bi mogao vratiti svoje podatke

Forma zlćudnog koda (1)

- Zlćudni kod može biti gdje god se nalazi programski kod
- Zlćudni kod može biti i u podacima
  - Podaci se u računalu ne izvršavaju, ali…
  - Uz pomoć raznih trikova može se navesti procesor da počne tretirati te podatke kao instrukcije koje potom izvršava
    - shellcode

Forma zloćudnog koda (2)

- Izvršne datoteke operacijskog sustava
  - Na Windowsima to su PE datoteke (EXE, DLL)
  - Na Linuxu i ostalim Unixoidima ELF
- Skripte operacijskog sustava
  - PowerShell
- MS Office dokumenti
  - MS Office dokumenti mogu sadržavati makroe pisane u Visual Basicu
  - Nekada su se ti makroi automatski izvršavali prilikom otvaranja dokumenata, sada MS Office traži korisnika da potvrdi njihovo pokretanje

Forma zloćudnog koda (3)

- PDF dokumenti
  - PDF dokumenti mogu sadržavati izvršne dijelove pisane u programskom jeziku JavaScript
  - Drugi način je da se iskorištava ranjivost u PDF čitaču (najčešće Adobe Acrobat)
- Mobilne aplikacije
  - Uglavnom trojanci jer mobilni uređaji imaju dosta dobro riješenu sigurnost
- Web
  - JavaScript kodovi

C&C poslužitelj

- Jako često se zloćudni kod po uspješnoj instalaciji javlja nekom računalu na Internetu (engl. phone home)
  - Ako napadač izvlači podatke od žrtve (eksfiltracija) tada se oni pohranjuju na tom poslužitelju
  - Radi se o kompromitiranom ili zakupljenom poslužitelju
  - Putem tog poslužitelj napadač upravlja zloćudnim kodom
- Korištenjem C&C poslužitelja napadač se štiti od otkrivanja
  - Može se otkriti C&C poslužitelj, ali je teško otkriti tko stoji iza tog poslužitelja
  - Prepreke u otkrivanju napadača su pravne i tehničke prirode

Neki načini zaštite od zloćudnog koda

- **Odgovorno ponašanje**
- Anti-virusna (AV) programska podrška
  - AV se baziraju na dva mehanizma detekcije malicioznog koda
    - Potpisi
    - Praćenje ponašanja
  - Nadogradnje potpisa je nužna za ispravnu zaštitu
  - Mnoštvo AV-ova na tržištu, ali nisu svi jednaki!
  - Nedostatak AV-a je što zloćudni kod aktivno pokušava zaobići detekciju
- Dinamička analiza elektroničke pošte i Web prometa
- Blokiranje C&C poslužitelja

Indikatori kompromitacije

- Indikatori kompromitacije (engl. indicators of compromise, IOC) su podaci koji omogućavaju detekciju zlćudnog koda
- Radi se o raznim tehničkim karakteristikama
  - Kriptografski sažetak datoteke, datoteke koje zlćudni kod kreira na disku, podaci u Windows bazi (registry), IP adrese s kojima zlćudni kod komunicira, domene koje zlćudni kod pokušava razriješiti, …
- Vrlo brz način utvrđivanja je li nešto zaraženo
- Napadačima je jednostavno promijeniti IOC-e

Analiza potencijalno zlćudnog koda

- Zašto analiza?
  - Utvrđivanje radi li se doista o zlćudnom kodu
    - Primjerice, kada netko primi sumnjiv privitak u elektroničkoj pošti
  - Analizom je moguće otkriti namjere napadača
    - Je li ciljani napad, ili nije; što žele dohvatiti, …
  - Postavljena nova aplikacija na Google Play (ili Appleov ekvivalent)
    - Otkrivanje funkcionalnosti
    - Na taj način se može utvrditi djelovanje, šteta, mogućnosti zaštite
- Reverzno inženjerstvo
  - Metode, tehnike i procesi uz pomoć kojih se pokušava saznati što i kako nešto radi

Reverzno inženjerstvo (1)

- Metode
  - Pokretanje koda u zaštićenoj okolini (engl. sandbox) i praćenje rezultata
    - Kod se pokrene u zaštićenoj okolini – DETONIRA
    - Maliciozni kod ima ugrađene provjere izvšrava li se u zaštićenoj okolini
    - Primjer otvorenog rješenja Cuckoo Sandbox
  - Analiza koda u debugeru
    - Vrlo mukotrpno, potencijalno i opasno ako malware ode „predaleko” u izvršavanju
  - Statička analiza (Radare2, Ghidra, IDA, …)
    - Dekompajleri
- Zloćudni kod pisan je u raznim jezicima i alatima
  - Ne postoji univerzalni skup alata za sve potrebe reverzanja
  - strojni kod Intel/ARM/PowerPC/JVM/Pascal

Reverzno inženjerstvo (2)

- Napadači koriste razne tehnike otežavanja reverzanja
  - Višestruke virtualizacije, obfuskacija, pakiranje, trapovi, značajne količine koda koje ničemu ne služe…
- NIKAKO NE POKRETATI SUMNJIV KOD NA SVOM RAČUNALU
- Imajte na umu da zloćudni kod može “pobjeći” iz ograničene okoline

VirusTotal

- Usluga za detekciju zloćudnog koda
  - Može analizirati datoteke ili Web stranice
  - Integrira niz AV proizvoda koje koristi za detekciju
    - Moguće pratiti kvalitetu AV-ova
- Kada primite nekakvu sumnjivu datoteku postavite ju na VirusTotal
  - Budite pažljivi da ne postavljate tajne podatke jer svemu što se pošalje VirusTotal usluzi postaje efektivno javno

Usluge za dinamičku analizu

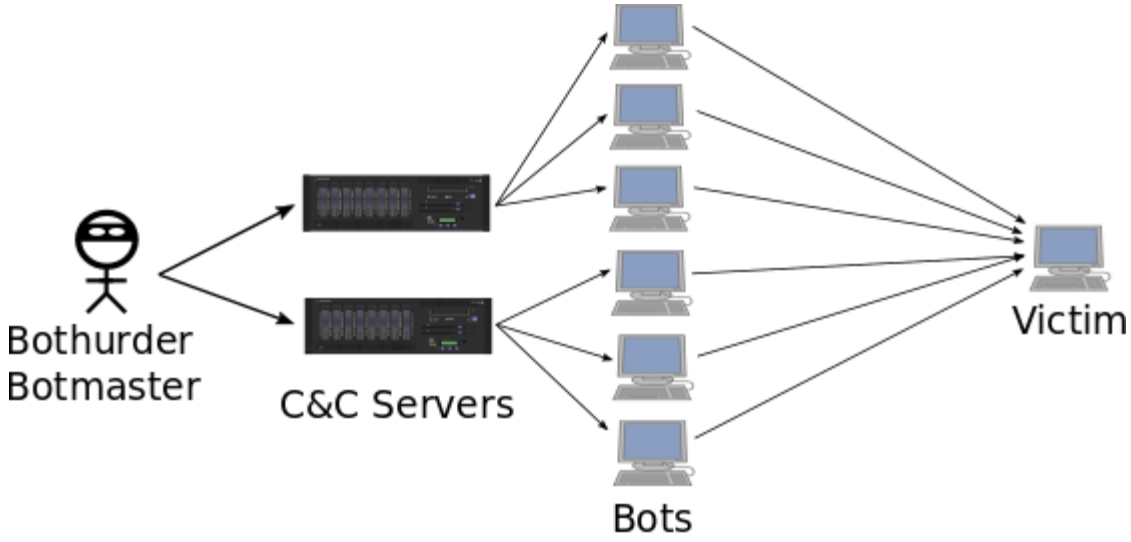
- Izvršavaju predani kod u zaštićenoj okolini (engl. sandbox)
  - Problem je što zloćudni kod može imati ugrađenu detekciju sandboxa i zbog toga ne pokazuje svoje zloćudno ponašanje
- Specifični su za pojedinu platformu
  - Android, Windows, Linux, …
- Primjer jedne takve usluge https://any.run/

Botnet

- Skup zaraženih računala kojima upravlja **botmaster**
  - Svako računalo izvršava maliciozni kod koji čini računalo dijelom botneta
    - Vlasnici nisu svjesni da im je računalo zaraženo
  - Broj zaraženih računala u botnetu može biti reda veličine 100,000 računala
- Botnet nije statička tvorevina
  - Vlasnici sa zaraženih računala uklanjaju zloćudni kod i računala prestaju biti dijelom botneta
  - Botmaster cijelo vrijeme pokušava zaraziti nova računala
    - Slanje poruka elektroničke pošte sa malicioznim privicima, korištenje crva

Arhitektura botneta

- Sastoji se od napadača, C&C poslužitelja, botova, žrtve i komunikacijskih puteva
- Komunikacija između zaraženih računala i handlera odvija se putem IRC-a, HTTP-a ili nekog P2P protokola
  - Postoje primjeri i korištenja Twitera!



Neke upotrebe botneta

- Preplavljivanje žrtava
  - Primjer 100.000 računala, svako neka generira 100kbps (skoro neprimjetno!)
- Širenje neželjene pošte (SPAM)
  - Korištenje žrtvinog korisničkog računa za slanje pošte - otežava detekciju
- Eksfiltracija podataka
  - Skuplja sve lokalno dostupne podatke i šalje napadaču
  - Podaci mogu biti ciljani (lozinke, Web browser kolačići, …) ili svi
- Napad na pojedine korisnike zaraženih računala
  - Primjer, MITB prilikom korištenja Interent bankarstva

Primjeri velikih botneta

- Mariposa
  - Otkriven 2008. godine, onemogućen 2009., 12 milijuna jedinstvenih IP adresa

    On 18 July 2010, Matjaž Škorjanc (alias: Iserdo), the creator of the "Butterfly bot" malware, was arrested in Maribor by Slovenian police for the first time,[16] but released due to lack of evidence. He was arrested again in October 2011. In December 2013 Škorjanc was convicted in Slovenia of "creating a malicious computer program for hacking information systems, assisting in wrongdoings and money laundering." He was sentenced to 4 years and 10 months imprisonment and fined €3,000 ($4,100). The court also ordered the seizure of Škorjanc's property acquired with the proceeds of crime. After he appealed the verdict his fine was in February 2015 raised for additional 25,000 EUR.
    [https://en.wikipedia.org/wiki/Mariposa_botnet]
- Emotet
  - Detektiran 2014. godine, uklonjen početkom 2021. koordiniranom akcijom policija iz više država, oko 120000 jedinstvenih IP adresa

Izrada zloćudnog koda (1)

- Izrada zloćudnog koda je u osnovi razvoj programske podrške
  - Jedino što ova programska podrška ima zloćudnu temeljnu funkciju
- Dva su temeljna pristupa u razvoju zloćudnog koda
  - Razvoj od početka za vlastitu upotrebu
    - Mogu priuštiti samo APT-ovi
  - Kitovi za izradu zloćudni kod
    - Češće korišteno u kriminalnom miljeu

Izrada zloćudnog koda (2)

- Zaštite od detekcije
  - Cilj je spriječiti detekciju antivirusne programske podrške
    - Ne nužno sve, samo one koja se očekuje kod žrtve
  - Obavlja se transformacijom koda kako bi se uklonile karakteristike koje AV-ovi prepoznaju
  - Postoje usluge koje nude kriminalci, a koje obavljaju tu funkcionalnost i testiraju na AV-ovima
- Zaštite od reverzanja
  - Spriječiti otkrivanje funkcionalnosti koda
    - Značajna količina informacija za branitelja
  - Reverzanje može trajati mjesecima, a u dosta slučajeva se ne otkrije sve

Špijunska programska podrška

- U svijetu postoje tvrtke koje prodaju špijunsku programsku podršku, primjerice
  - NCO Team – Tvrtka bazirana u Izraelu
  - Nedavno su se našli u središtu afere sa WhatsApp platformom
- Hacking Team – Tvrtka bazirana u Italiji
- Vrlo tajanstvene tvrtke
  - Njihovi korisnici su policije i tajne službe
  - Cijena je isključivo na upit
  - Radi se o tvrtkama upitne legalnosti i etičnosti
  - One same tvrde da ne posluju s opresivnim režimima i kriminalnim miljeom, ali...

Hvala!

slido

Jeste li pročitali Krebsov post vezan uz NetWire?

ⓘ Start presenting to display the poll results on this slide.

slido

Kako bi ste okarakterizirali osumnjičenika iz Zaprešića?

ⓘ Start presenting to display the poll results on this slide.

slido

Koje sve zlоćudne aktivnosti ima NetWire?

ⓘ Start presenting to display the poll results on this slide.