BOTNET PERICOL SUBESTIMAT

Inga IAVORSCHI

Universitatea Tehnică a Moldovei

Abstract: *În acest articol sunt elucidate caracteristicile de bază a botneturilor și influnța lor asupra Internet of things.Prin analiza acestor pericole care sau dezvoltat odată cu evoluția rețelelor de calculatoare, bat un semnal de alarmă asupra necesității de a crea siguranță pentru utilizatorii de device de diferite tipuri.La fel prin exemple existente dovedesc că pericolele create de botnet sunt de diferite nivele,neglijența acestora duce la pierderi financiare și amenințări de securitate de nivel personal și statal.Acest domeniu surprinde giganții de securitate zilnic cu transformări periculoase și frauduloase.*

Cuvinte chee: *Botnet, internet of things, dispozitive electronice, rețea de calculatoare, rețea-sistem.*

Calculatoarele infectate cu software rău intenționat, în rețea, sunt o armă cibernetică puternică și o modalitate foarte bună de a îmbogăți unul care funcționează. Astfel, el atacator poate fi oriunde în lume, în cazul în care există pe Internet..

Botnet se referă la o rețea de calculatoare, tablete, smartphone sau IoT – Internet of Things, infectate cu software de tip bot, software ce permite unor persoane rău intenţionate să preia controlul acestora fără cunoştinţa proprietarilor de drept şi să le utilizeze pentru a lansa atacuri cibernetice asupra unor terţi. Prin intermediul botnet-urilor se desfăşoară în mod curent activităţi ilegale cum sunt atacurile informatice (DDoS) sau trimiterea de mesaje spam.

În general, botnet-urile sunt create prin propagarea pe Internet a unui virus sau a unui troian ce facilitează accesul neautorizat la diverse sisteme informatice.

După obţinerea accesului, pe calculatoarele respective se instalează software-ul de comandă şi control denumit bot. Calculatoarele ce alcătuiesc un botnet sunt denumite zombies sau drone. Persoana ce controlează un botnet se numeşte master.

Un botnet poate controla milioane de calculatoare (şi mai nou IoT) răspândite pe întreg globul. Acestea pot fi utilizate pentru efectuarea de atacuri informatice asupra unor ţinte civile sau guvernamentale.

Bot-neturile sunt modalitatea perfectă de lansare a unor atacuri Distributed Denial of Service – DDoS, angajând simultan impotriva unei ţinte, zeci de mii de calculatoare din toate zonele geografice.[1]

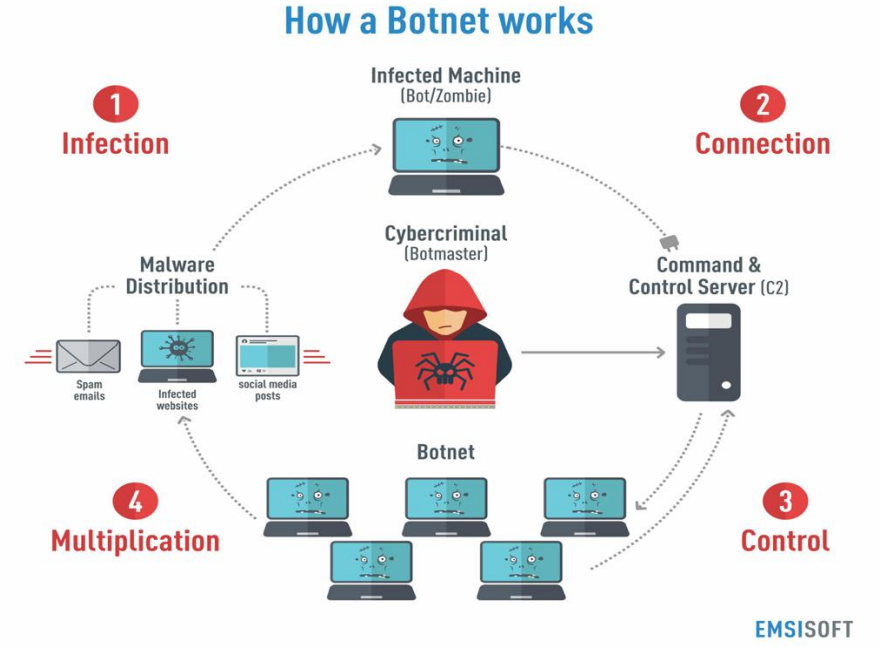

Fig.1 Construcția unui botnet.

Nu este de mirare că cea mai avansată armă din patrimoniul unui hacker este rețeau botnet. În consecință, statele care sponsorizează atacurile cibernetice au fost forțate să folosească aceasta armă. Primul super botnet apărut în media în anul 2011, se numea Stuxnet. Acest malware avea cel mai avansat cod scris,

până atunci, de către o echipă de programatori. Principala țintă a acestui malware au fost instalațiile nucleare iraniene, folosind software-ul Siemens Step. Dauna a fost semnificativă și costul imens pentru guvernul iranian. Codul sursă a fost postat online, toți cercetătorii fiind de acord că acest malware este de departe cel mai avansat. Este interesant că sunt multe versiuni și că acest malware a fost dezvoltat de-a lungul anilor, sugerând că a fost un process continuu.Industria malware este în continuare o afacere mare pentru hackerii profesioniști care vor să facă bani. O dată cu răspândirea telefoanelor mobile și a tabletelor sunt și mai multe ținte, iar competiția este o provocare pentru mulți infractori cibernetici care sunt dispuși să infecteze cât mai multe dispozitive posibile.[2]

Un nou tip de botnet crește în popularitate, botnetul Android. Unul din cele mai mari în acest moment este MisoSMS, originar din China. Nu este sofisticat comparativ cu un Windows botnet dar poate provoca mult rău. De exemplu, acest botnet poate fura toate emailurile și SMS-urile după care să le transmită către un server din China.În aceeași categorie a botneturilor mobile este Oldboot, dezvoltat de hackeri chinezi, care a infectat mai mult de un million de dispozitive în China. După cum se vede, majoritatea dezvoltărilor de botnets are loc în Asia și Europa de Est, în special datorită protecției de care beneficiază infractorii cibernetici în aceste țări. Exemplele asemănătaore pot continua.

Termenul „Internet of Things" este folosit pentru a desemna orice obiect care poate fi interconectat și identificat în mod unic prin utilizarea unor tehnologii diferite, cum ar fi: NFC, digital watermarking (filigran digital) și cod QR.Internet of Things este o paradigmă care schimbă abordarea tehnologiei, extinzând suprafaţa de atac. Dispozitivele IoT sunt deja peste tot și din acest motiv industria IT trebuie să țină cont de problemele de securitate și confidenţialitate. Un studiu recent efectuat de către firma de securitate Veracode a scos în evidenţă faptul că dispozitivele IoT casnice expun utilizatorii la o gamă variată de ameninţări, incluzând furtul de date și sabotaje, iar proliferarea dispozitivelor IoT va avea o influenţă majoră asupra comportamentului uman.

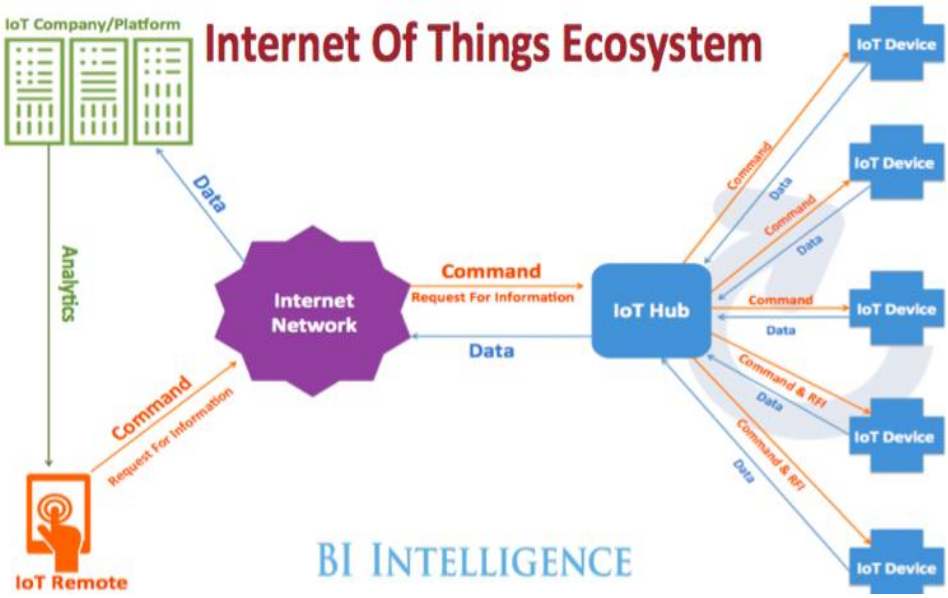

Fig. 2 Internetul dispozitivelor.

Dispozitivele IoT vor influenţa deplasările indivizilor în zonele urbane pe baza parametrilor atmosferici sau pe baza gradului de congestie de trafic din anumite zone specifice.Din păcate, în majoritatea cazurilor dispozitivelor IoT au o protecţie de securitate deficitară încă din faza de design. Infractorii cibernetici, hackerii susţinuţi de state, hack-tiviștii și teroriștii cibernetici pot exploata defectele din arhitectura IoT și pot produce daune extinse în orice industrie. Specialiștii estimează că numărul atacurilor cibernetice împotriva obiectelor inteligente va crește rapid .
Pentru a proteja dispozitivele IoT este important să identificăm principalii actori ai ameninţărilor și motivaţiile lor. Să începem cu analiza categoriilor atacurilor care ameninţă arhitecturile IoT. Din păcate există o mulţime de „băieţi răi" care ameninţă implementarea paradigmei, incluzând infractori cibernetici, entităţi guvernamentale și hackeri motivaţi politic.[3]

Toţi aceşti actori sunt interesaţi în primul rând de cantităţile uriaşe de date pe care le administrează dispozitivele IoT, dar nu putem subestima riscurile unor atacuri cibernetice pentru sabotaje.Erorile de design în privinţa principiilor fundamentale a securizării IoT pot expune utilizatorii la sabotaje, atacuri ale hackerilor (de ex. atacuri man-in-the-middle (MITM), preluarea controlului asupra reţelei), furt de date şi deturnarea funcţionalităţii produselor.Infractorii cibernetici pot fi interesaţi să fure informaţii sensibile administrate de platformele IoT sau pot fi interesaţi să compromită obiectele inteligente şi să le utilizeze în activităţi ilegale, cum ar fi derularea unor atacuri asupra unor terţe entităţi sau mineritul Bitcoin.

Firmele de securitate au depistat deja grupuri de infractori cibernetici care utilizează botneţi alcătuiţi din milioane de dispozitive IoT infectate .

În mod uzual, „băieţii răi" infectează sau compromit obiecte inteligente configurate necorespunzător, cum ar fi routere, dispozitive SOHO, SmartTV-uri şi alte dispozitive IoT.

În mod similar agenţiile de Intelligence sunt interesate să exploateze dispozitivele inteligente pentru a derula campanii de spionaj la scară largă, care utilizează routere, console de jocuri şi smartphone-uri pentru a spiona persoanele vizate. Teroriştii cibernetici şi hack-tiviştii pot fi de asemenea interesaţi să compromită dispozitivele IoT pentru a fura informaţii sensibile sau pentru a provoca daune extinse.

Care sunt principalele ameninţări cibernetice pentru dispozitivele IoT?

Anul trecut specialiştii de la Symantec au publicat un studiu interesant despre principalele ameninţări cibernetice pentru IoT, grupându-le în următoarele categorii:

- **Denial of service** – atacurile DDoS pot viza toate punctele unui scenariu de lucru determinând probleme serioase în reţeaua dispozitivelor inteligente şi paralizând serviciul pe care acestea îl furnizează. Ţineţi cont că elementele aparţinând unei reţele IoT sunt ţinta atacurilor care interferează cu modul de operare şi de comunicare între dispozitive.
- **Botneți și atacuri malware** – Probabil că acesta este scenariul cel mai comun şi mai periculos, dispozitivele IoT sunt compromise de atacatori care abuzează de resursele lor. În mod uzual atacatorii utilizează cod specializat care să compromită software-ul care rulează pe dispozitivele IoT. Codul maliţios poate fi utilizat pentru a infecta calculatoarele utilizate pentru controlul reţelei de dispozitive inteligente sau să compromită software-ul care rulează pe acestea. În cel de-al doilea scenariu atacatorii pot exploata prezenţa unor defecte în firmware-ul care rulează pe aceste dispozitive şi să ruleze codul lor arbitrar care să deturneze componentele IoT spre o funcţionare neplanificată. În noiembrie 2013, experţii Symantec au descoperit un nou vierme Linux, Linux.Darlloz, proiectat în mod special să atace dispozitive IoT Intel x86 care rulează Linux. Atacatorii au compromis dispozitivele IoT pentru a construi un botnet care a fost utilizat pentru activităţi ilegale, incluzând trimiterea de Spam, generarea de mesaje SMS costisitoare sau derularea unor atacuri DDoS. O altă posibilitate pentru atacatori este exploatarea dispozitivelor configurate necorespunzător, de exemplu dacă ştii setările de fabrică ale unui router este posibil să ai acces la consola sa de administrare şi să modifici parametrii care îi controlează comportamentul.
- **Breșe de date** – breşele de date reprezintă un alt risc serios în privinţa adoptării dispozitivelor IoT. Organizaţiile trebuie să conştientizeze potenţialul consecinţelor neplanificate ale situaţiilor de utilizare a IoT. Atacatorii pot spiona comunicaţiile dintre dispozitivele IoT şi să colec teze informaţii despre serviciile pe care acestea le implementează. Datele accesate prin intermediul dispozitivelor IoT pot fi utilizate în scopuri de spionaj cibernetic sau de către o agenţie de Intelligence sau de către o companie privată în scopuri comerciale. Breşele de date reprezintă o ameninţare serioasă pentru organizaţiile sau persoanele care utilizează dispozitive inteligente.
- **Breșe accidentale** – Managementul datelor într-o arhitecutură care include dispozitive IoT este un aspect critic. Informaţiile sensibile pot fi expuse nu numai într-un atac cibernetic, ci pot fi expuse sau pierdute şi în mod accidental. Symantec dă ca exemplu transmiterea coordonatelor autoturismului unui CEO, dar realitatea este că din mediul de business se pot scurge informaţii mult mai sensibile.
- **Perimetre slăbite** – lipsa măsurilor de siguranţă încă din faza de design poate cauza o slăbire a perimetrelor. Prin exploatarea unui defect în SmartTV-ul nostru atacatorul poate avea acces la reţeaua domestică şi să dezactiveze orice sistem antifurt implementat pentru securitatea fizică.

Firmele de securitate au observat o escaladare a atacurilor cibernetice împotriva dispozitivelor IoT, la scară globală. Cel mai întâlnit scenariu este utilizarea de botneţi alcătuiţi din mii de dispozitive din domeniul

IoT, cunoscute și sub denumirea de thingboţi, care sunt utilizaţi pentru a trimite mesaje de spam sau pentru coordonarea unor atacuri DDoS. Rezumând un thingbot poate fi utilizat pentru:a trimite spam.[4]

- a coordona un atac împotriva unei infrastructuri critice.
- a furniza un malware.
- a funcţiona ca punct de intrare în reţeaua unei companii.

Principalele firme de securitate confirmă o creștere a numărului de atacuri împotriva unor obiecte inteligente, incluzând routere, SmartTV-uri, dispozitive

NAS (network-attached storage), console de jocuri şi diferite tipuri de set-top box-uri.

La finele anului 2018 KASPERSKY a publicat un raport efectuat pentru prima jumatate a anului 2018, în care se specifică că au fost identificat 150 de familii malware şi 60000 botnet cu diferite modificări în întreaga lume.

La fel și Norton a anunțat despre un nou botnet Mirai cu mult mai agresiv decît predecesoarii acestuia.

Concluzie

IoT este o paradigmă care ne va influenţa vieţile în anii care vor urma. din acest motiv este esenţial ca problemele de securitate și de confidenţialitate să fie tratate în mod corespunzător.

Experţii în securitate solicită producătorilor și vânzătorilor să ia în considerare ameninţările cibernetice și nivelul de expunere al oricărui dispozitiv IoT. IoT oferă oportunităţi de business fiecărei industrii, dar poate deveni un coşmar în cazul în care componentele de securitate sunt subestimate.

Bibliografie

1. https://despretot.info/botnet-definitie-botnet-ce-inseamna/
2. http://kjn.scrieunblog.com/articles/ce-este-un-botnet.html
3. https://www.quickmobile.ro/articole/ce-este-internet-of-things
4. https://www.quickmobile.ro/articole/ce-este-internet-of-things
5. https://www.kaspersky.com/about/press-releases/2018_botnet-activity-in-h1-2018-multifunctional-bots-becoming-more-widespread
6. https://www.trendmicro.com/vinfo/us/security/news/botnets
7. https://www.recordedfuture.com/mirai-botnet-iot/
8. https://blog.checkpoint.com/2018/12/11/november-2018s-most-wanted-malware-the-rise-of-the-thanksgiving-day-botnet/
9. https://blog.easysol.net/banking-trojan-trends-2018/
10. https://blog.radware.com/security/2018/02/darksky-botnet/