UBT-CERT Internship

Java e tretë deri tek java e gjashtë

Hulumtimi & Analiza e softuer-ve të dëmshëm (Malware Analysis)

Maj 2017

Përgatitur nga studentët e SHKI/UBT: Kujtim Morina student I vitit të I

Rrustem Shehu studentit i vitit të III

Edi Bushati student I vitit të II

Ndihmës: Atdhe Buja UBT-CERT manager

Demonstruesit e Malwares: Agon Hysenaj

Rexhep Bërlajolli

Përmbajtja

Hyrje

Ky dokument është përgatitur me qëllim që të vetëdijsoj të gjithë ata qe jane te angazhuar ne fushen e TIK-ut dhe I dedikohet komunitetit te TIK-ut.

Përmirëson nivelin e sigurise te sistemeve kompjuterike te nje kompanie ose organizate, ndihmon perdoruesit e ketyre sistemeve per shfrytezim sa me te sigurt te tyre.

Koncepti etik (defense cyber security)

Ky dokument pasqyron aspektin etik apo mbrojtës, duke identifikuar malware-t më të rrezikshëm dhe zakonshëm që kanë ndodhur në botë.

Çka është "Malware Analysis"

Eshtë një process i studimit të përcaktimit të funksionimit, origjinës dhe impakteve potenciale të një shembulli të malware – softuer të dëmshëm siq janë virusët, worm, Trojan, backdoor etj.

Analiza e parë "I"

Dëmi nga softuerët e dëmshëm (ang. Malwares) mund të jetë shumë i madhë në kosto, humbje të imazhit dhe i ndryshëm në lloje, metoda dhe teknika. Virusët e kompjuterëve, worm's dhe Trojan virusët mund të shkaktojnë dëme të ndryshme në kompjuterë, rrjetë, pajijsje mobile dhe në të dhëna.

URL https://usa.kaspersky.com/resource-center/threats/malware-damage

Analiza e dytë "II"

Internet Attack Was Strongest of Its Kind by Far

URL- http://www.newser.com/story/233175/internet-attack-was-strongest-of-its-kind-by-far.html

Me ane te nje sulmi nga hakeret amatorë me shperndarjen e një shërbimi që u dërgua përdorueseve te internetit në një teleferik ishte më i fuqishmi i këtij lloji deri tani, thonë studiuesit e sigurisë së kibernetikës. Twitter, Netflix, Reddit u rrezuan, pasi botneti Mirai mori përsipër pajisjet e mbrojtura ne menyre jo eftektive "Internet of things" si DVR-të dhe Webcams,pronarët e të cilëve nuk kishin ndryshuar fjalëkalimet e paracaktuara të pajisjeve dhe bombarduan kompaninë e hostit të domainit Dyn. Kështu që përdoruesit e rregullt nuk mund të kishin kyqje.Kompaina Dyn thotë se kishte nje impakt te madh me "100,000 pika të dëmshme" që çuan një sulm dy herë më të fuqishëm se çdo sulm tjetër DDoS.

Hulumtuesit nga firma e sigurisë në internet, Flashpoint, dyshojnë se sulmi ishte i lidhur me komunitetin në Hackforums.net, ku kodi burimor Mirai ishte botuar më pare dhe kishte për qëllim të synonte një kompani video lojë, ndoshta PlayStation Network, raporton Computer World . Nëse hakeret amator kanë bërë aq shumë dëme, "imagjinoni se çfarë mund të bëjë një aktor i rezervuar i shtetit me pajisjet e pasigurta të internetit", thotë një përfaqësues i sigurisë së kibernetikës në Këshillin për Marrëdhëniet me Jashtë. "Ne kemi një problem serioz me pasigurinë kibernetike të pajisjeve IoT dhe nuk ka strategji konkrete për ta luftuar atë."

Rekomandim

"Ekspertët rekomandojnë që përdoruesit të rivendosin një pajisje IoT në cilësimet e fabrikës për të fshirë çdo malware ekzistues, dhe pastaj të krijojnë një fjalëkalim të ri menjëherë''

Analiza e tretë "III"

Benefits of Malware Analysis

Analiza e malware është një pjesë e rëndësishme e parandalimit dhe zbulimit të sulmeve kibernetike në të ardhmen. Duke përdorur mjete të analizës malware, ekspertët e sigurisë kibernetike mund të analizojnë

ciklin jetësor të sulmeve dhe të mbledhin detaje të rëndësishme ligjore për të rritur inteligjencen e tyre te kërcënimit.

Analizat e Malware (AX series) ofrojnë një mjedis të sigurt për të testuar, përsëritur, karakterizuar dhe dokumentuar aktivitetet e avancuara me qëllim të keq. Analiza Malware tregon ciklin e jetës së sulmeve kibernetike, nga shfrytëzimi fillestar dhe programi i ekzekutimit të malware në destinacionet e thirrjes.

"Malware i avancuar është pjesë e kërcënimeve kibernetike të avancuara dhe të vazhdueshme që veprojnë në mënyrë të koordinuar për të depërtuar në mbrojtjen e një organizate dhe për të krijuar një terren afatgjatë në rrjet".

Njohuri per sulmet kibernetike per te ulur rrezikun e biznesit.

• Informoni strategjitë e ardhshme të parandalimit duke ofruar një depërtim më të thellë në mjetet dhe taktikat e sulmuesit

• Ndaloni përhapjen e sulmeve duke përdorur profilet e sulmeve lokale të gjeneruara automatikisht, të shpërndara menjëherë në të gjithë ekosistemin FireEye

Analiza e automatizuar per te permisuar efikasitetin

- Ngarko file prej simple interface
- Identifikoni malware te cilat nuk jane pare me pare
    - Integrohuni me produkte antivirus për një inspektim më të thellë të malware

Single-test environment for Windows and MacOS

- Hostimi i makinave virtuale Microsoft Windows dhe Mac OS X në një hypervisor të përshtatur
- Eliminon koston dhe lartësinë e krijimit dhe mirëmbajtjes së konfigurimeve të shumta të testimit
- Automate setup, restaurimin e makinave virtuale për të përputhur përdorimin aktual të OS

URL https://www.fireeye.com/products/malware-analysis.html

Analiza e katërt "IV"

Shamoon

https://blog.vectranetworks.com/blog/an-analysis-of-the-shamoon-2-malware-attack

Shamoon njihet edhe me emrin Disttrack, eshte nje virus kompjuterik i zbuluar nga SECULERT(Kompani per siguri kibernetike me baze ne Izrael) ne vitin 2012. Ky virus eshte perdore per spiunazh ne sektorin energjetik. Ky viruse ndryshe nga viruset e tjera ka pasur permbajtje per spiunazh. Shamoon mundet te shperndaht nga nje paisje kompjuterike ne te gjithe kompjuteret e tjere ne rrjete. Ne momentin qe sistemi infektohet, virusi fillon te perpilpoje lista nga lokacionet specifike the te i uploadoje ato ne databaze specifike dhe i fshinte te gjitha ato nga kompjuteri. Dhe ne fund ky virus e rishkruante master book record te kompjuterit qe mos te kete mundesi te ndezet ai kompjuter. Ky virus jo vetem qe ka sulmuar sektorin energjetik, por gjithashtu edhe ate te naftes. Nje grup i quajtur "Cutting Sword of Justice" ka marre pergjegjesine e sulmit te 35 mije workstations te kompanis se naftes

ARAMCO (Arabian American Oil Company) kompani arabe-amerikane ne qytetin Dhahran te Arabis Saudite. Shamoon i ka shkatuar probleme te medha kesaj kompanie, ARMACO ka shpenzuar po thuaj nje jave qe te i resetoje te gjitha sherbimet. Ky malware kishte nje konfigurim parazgjedhore qe shkaktonte fshirjen e diskut ne kohe 8.45 te pasdites ku pjesa me e madhe e punonjeseve nuk ishin aty, per arsye qe mundesite per te dalluar infektimin dhe parandalimin e tij te ishin me te vogla.

Shamoon perdore disa komponente per te infektuar kompjutera. Komponenti kryesore eshte nje Dropper (komponente qe leshon komponente te tjera) i cili krijonte nje sherbim me emrin NtsSRV qe te mbante qendrueshmeri ne kompjuterin e infektuar. Ky virus shperndahet lehte ne rrjetin LAN duke e kompjuar vetveten e vet ne kompjutera te tjere. Dhe vendoske komponentet tjera ne kompjutere, Dropper-i ishte ne dy versione 32-bit dhe 64-bit. Varesishte prej arkitektures kompjuterike 32-bit apo 64-bit dropper-i leshonte versionin perkates. Komponenta e dyte eshte WIPER(i ndryshem nga malware wiper), i cili leshonte nje komponente te trete i njohur si Eldos Driver. Kjo lejonte akcesin ne hard disk direkt nga user-mode pa nevojen e Windows APIs. Ky wiper perdorte drajverin Eldos qe te mbishkruante harddisqet me foto te nje djaloshit Sirian.

Analiza e pestë “V”

Stuxnet
https://en.wikipedia.org/wiki/Stuxnet
Sulm mbi centralin berthamore ne Iran, ku qelllimi i tij ishte te e ngadalsonte prodhimin e Uraniumit nga Iran qe sipas Kombeve te bashkuara paraqiste shqetesim dhe kercenim per lufte.
Ende mbetet mister se kush e krijoi Malwaren apo Virusin Stuxnet.

Stuxnet nje dobesi kompjuterike, ka befasuar cdo haker dhe cdo inxhinier te programimit dhe rrjetave. Emrin Stuxnet ia kane vendosur nga dy terma kyq ne kod .stub dhe mrxnet.sys . Fillimisht eshte identifikuar ne vitin 2010, por zhvillimi i saje thuhet te kete filluar qe nga viti 2005. Ka bere dem ne programin nuklear te Iranit. Edhe pse askush nuk ka marre ende pergjegjesine per kete sulm, por nje gje eshte e sigurte ne kete sulm kibenertik jane te perfshira kombet, thuhet se ne te jane te perfshira Shtetet e Bashkuara te Amerikes dhe Izraeli. Dhe eshte hera e pare qe perdoret nje virus si arme.

Sipas dokumentarit “Zero Days” drejtuar nga Alex Gibney Shtetet e Bashkuara te Amerikes dhe Izraeli jane jo te dyshimtit per sulem, por fajtore edhe pse nuk e marrin pergjegjesine. Ne dokumentare paraqitet nje punonjeseve e National Security of America NSA e cila pranon qe Stuxnet eshte krijuar nga NSA dhe Izraeli, ku qellimi i tyre ishte qe te i shkaktonin ngadalesim ne pasurim me uranim ne centralin berthamor te Iranit. Ne dokumentare pershkruhet edhe se si eshte arritur qe te dergojne nje dobesi te tille ne sistemet kompjuterike te Iranit. Sulmuesit fillimisht kane sulmuar ministrite e Iranit, sepse ata kane hulumtuar dhe kane pare qe punonjes te ministrise se mbrojtjes leviznin shpesh ne centralin berthamor, keshtu ata fillimisht kane hakuar kompjuteret e punonjeseve te ministrive te cilet pastaje kane derguar virusin brenda centralit berthamor.

Irani pasurimin me uranium e bente permes nje procesi me centrifuga. Ato centrifuga rrotulloheshin rreth boshtit te tyre. Inxhinieret e Stuxnet kane koduar virusin qe te i pershpejtonte centrifugat qe te rrotulloheshin rreth boshtit te tyre. Keshtu qe ato u demtonin dhe dilnin nga funksioni. Iranit ky sulem i ka shkaktuare deme te medha si ne nderrimin e centrifugave ashtu edhe ne punetore, shume inxhiniere jane shkarkuar nga puna duke menduar qe faji eshte tek punetoret.

Stuxnet nuk ka infektuar vetem sistemet kompjuterike te Iranit, por edhe te Indise, indonezise Britanis se Madhe, SHBA-ve dhe shtete te tjera, mirpo sipas Kaspersky Lab shteti i Iranit ishte i prekur shume, prej te gjithe kompjuterve te infektuar 60% ishin te Iranit duke u ndjekur nga Indonezia me rreth 20%.

Prej ketije sulmi dhe shume sulmeve te tjera kibernetike si Shamoon, Duqu etj te gjitha shtetet kane filluar te krijojne planprogame dhe strategji te ndryshme per te u mbrojtur nga sulme te ndryshme kibernetike. Keto sulme na kane deshmuar se nuk ka siguri te plote ne sistemet kompjuterike, gjithmone eshte diku nje leshim. Nje sulm i tille ne energji, uje, sisteme te sigurise, telekomunikacion ose aviacion do te i shkaktonte probleme te medha si dhe deme me pasoja te medha. Dhe duke pa zhvillimet e fundit ne fushen e kibernetikes shihet qarte se do te krijohet nje lloj tjeter i luftes, pra lufta kibernetike.

Rekomandim per Shamoon dhe Stuxnet

Te gjithe kompanite e sistemeve operative dhe prodhuesit e kompjutereve rekomandojne qe te behen gjithmone perditesimet e antivirusit, dhe ne raste kur hasni ne ndonje gje te dyshimet te kerkoni ndihme nga CERT-i i shtetit ose organizata dhe kompani te tjera dhe njekohesisht te lajmerohen dhe ata per nje sulem te tille. Neqoftese punoni ne sektore te sigurise informative keshillohet qe nese perdorni laptopin e punes ne shtepi per te kryer ndonje detyre shtepie te keni kujdes se cka shkarkoni ne ate laptop, se cka fusni ne laptop. Ka shume gjasa qe ju te perdoreni si nje bartes i ndonje virusi qe do te i shkaktonte kolaps shtetit.