ZIUR FUNDAZIOARENTZAKO ZIBER-IRUZURRERAKO (CYBER DECEPTION) IRTENBIDE AURRERATU BATEN ZERBITZU KUDEATUARI BURUZKO BALDINTZA TEKNIKOEN AGIRIA (2020018 ESPED.)

I.- ZERBITZUAREN XEDEA ETA IRISMENA

Ziur Fundazioari ziber-iruzurrari ("deception") buruzko zerbitzu kudeatu baterako hiru kanpaina aurrera eramateko behar duen laguntza teknikoa ematea da kontratuaren xedea, Baldintza Teknikoen Agiri honetan zehazturiko baldintzetan. Zerbitzuak aukera eman beharko du kanpainaren barruan dauden Gipuzkoako industria-sektoreko enpresen azpiegitura teknologikoei egindako ziber-erasoak detektatzeko eta datuak lortzeko, honako helburu hauekin:

- Gipuzkoako enpresek dituzten arrisku eta erasoen ikuspegi global bat izatea
- Gipuzkoako enpresa industrialei zuzendutako erasoen joerak ezagutzea
- Sare industrialen erasotzaileen profilak ikertzea
- Erasotzaileen "modus operandi"-a ezagutzea eta aurretiaz eta modu eraginkorrean jardutea talde horiek egiten dituzten erasoen aurrean

II.- ZERBITZUAREN DESKRIBAPENA

Kontratuak xede duen jarduera aurrera emateko, honako baldintza hauek bete beharko ditu esleipendunak:

a) Engainu-aktiboak sarean −barnekoa nahiz kanpokoa− modu automatizatuan eta dinamikoki denbora errealean egokitzeko moduan diseinatu, monitorizatu eta mantentzeko gaitasuna duen tresna bat izatea. Esleipendunak proiektuan parte hartzeko aukeratutako enpresa industrialetan zabaldu behar du tresna hori.

   Lizitatzaileak jarri beharko ditu aplikatiboa amaierako enpresan zabaltzeko behar diren hardware eta software lizentzia guztiak.

b) Ziur Fundazioak izendatutako pertsonak tresnaren erabileran trebatzea.

c) Barne- eta kanpo-erabilerako kasuen katalogo bat eskura jartzea −horietatik, 3 kanpainetan aplikatuko direnak aukeratuko ditu Ziur Fundazioak, kasuan kasuko beharren, aukeren edo premien arabera− eta erabilera-kasu horiek diseinatu eta martxan jartzea.

d) Zerbitzuan jasotzen diren 3 kanpainak aurrera eramatea −4 hilabeteko iraupenekoa bakoitza− ZIUR Fundazioak aukeratutako enpresetan. ZIUR Fundazioak identifikatu eta aukeratuko ditu enpresak, eta kanpaina bakoitzeko 5 enpresek hartu beharko dute gutxienez, hargatik eragotzi gabe esleipendunak partaide kopuru handiagoa proposatzeko duen aukera.

   Horretarako, martxan jartzeko lanak zehaztean, kanpaina bakoitzean zerbitzua abian jartzeko eta kanpaina bakoitzean jasotako enpresa bakoitzerako behar den guztia jaso beharko da.

ZIUR Fundazioa harremanetan jarriko da zerbitzuaren prestazioa egingo den enpresekin. Ziur Fundazioaren eta enpresa partaide bakoitzaren arteko harreman hori juridikoa izango da kasu guztietan. Horretarako, dagozkion lankidetza-hitzarmenak formalizatuko dira Fundazioaren eta enpresa partaideen artean. Hitzarmen horien bidez, enpresako baliabideetarako sarbidea ahalbidetuko da, kontratuaren xedea bete ahal izateko.

e) Kanpaina bakoitzean eta enpresa bakoitzarekin honako jarduera hauek egitea:

1.- Detekzioa

- Mehatxu konplexuen eragileak detektatu (asmo txarreko barneko pertsonak, jadanik erakunde baten barruan dauden APTak edo etorkizuneko eraso bideratuetarako errekonozimenduak egiten dituzten kanpo-eragileak).
- Sistemaren mailako ekintza oso sotil eta sakonak detektatu.
- Ezkutuko detekzio-lanak egin, erasotzailea konturatu ez dadin.
- Erasotzailearen mugimenduei buruzko datuak atera, hura konturatu gabe, eta, aldi berean, engainu-zerbitzariaren erabateko kontrola mantendu.

2.- Ikerketa

- Erasoen azterketa eta monitorizaziorako gaitasun aurreratuak eskaini.
- Erasotzaileen TTPen goi-mailako ikerketa eta identifikazio automatikoa egin, MITRE ATT&CK matrize integratuan oinarrituz.
- Eskura dauden defentsa aktiboei buruzko informazioa eman, MITRE SHIELD matrize integratuaren bidez.
- Mehatxuzko ekitaldien eta mehatxuei buruzko azterketa adimentsuen iragazki indartsu bat eskaini, IoC eta TTP ezagunen aurkako jarduera amarrutsuak identifikatu eta etiketatzeko. Detektatutako jarduera bisualki bistaratu beharko da MITRE ATT&CK esparruan.

f) Mehatxuen aurreko portaerari buruzko datu-basea aldizka eguneratu, zerbitzuan erabilitako tresnaren bitartez.

g) Ziur Fundazioari, gutxienez, honako jakinarazpen-dokumentu hauek eman, enpresa bakoitzean egindako kanpainari buruz:
   1. Tresnak izandako zabalkundeari eta erabilera-kasuei buruzko txostena.
   2. Enpresa bakoitzak jasaten duen eraso motaren monitorizazioaren egoerari buruzko hileko txostena.
   3. Detektatutako aurkikuntzei buruzko amaierako txostena.

Horrez gainera, kanpaina bakoitzaren amaieran, emaitza-txosten bat entregatu beharko da, lau hilean behin. Txosten horretan, egindako jarduerak eta ateratako ondorioak zehaztu beharko dira.

h) Kanpaina guztiak amaitzean, Gipuzkoan egiten diren eraso motei buruzko azken ebaluazio txostena entregatu.

III.- METODOLOGIA

ZIUR Fundazioak lanak ikuskatzeko eta kontrolatzeko bete beharreko funtzioak eraman beharko ditu aurrera enpresa esleipendunak, eta, horretarako, zorrotz bete beharko ditu jasotako ohar eta gomendio guztiak.

Lanen bilakaeraren eta segimenduaren berri izateko, Ziur Fundazioak aukera izango du −zerbitzuaren beharren arabera− zerbitzua aurrera eramateko beharrezko jotako behar adina dokumentu aurkez ditzan eta beharrezko jotako lan- edo informazio-bileretara joan dadin eskatzeko enpresa eleipendunari (presentzialki eta/edo telematikoki egin ahal izango du esleipendunak).

Edonola ere, segimendua egiteko modua (bilerak, aktak, txostenak…) aldatu ahal izango du ZIUR Fundazioak, baldin eta beharrezkoa dela iruditzen bazaio.

Kontratu honen barruan egindako dokumentuak eta aurrera eramandako ekintzak Ziur Fundazioaren nortasun korporatiboaren eskuliburuaren arabera eraman beharko dira aurrera.

Kontratuaren betearazpen materiala fase hauen arabera egin beharko da:

1. fasea - Aurretiazko lanak eta tresnaren zabalkundea.

2. fasea - 1. kanpainaren garapena, gauzatzea eta ebaluazioa.

3. fasea - 2. kanpainaren garapena, gauzatzea eta ebaluazioa.

2. fasea - 3. Kanpainaren garapena, gauzatzea eta amaierako ebaluazioa.

1. fasea aurrera eramateko, zerbitzuaren lehenengo hilabetean, kanpaina bakoitzean lortu nahi diren helburuak eta parte hartuko duten enpresen zerrenda zehaztuko dizkio Ziur Fundazioko zuzendariak proiektuaren arduradunari, eta, halaber, kanpaina bakoitzean aurrera eramango diren erabilera-kasuak azalduko dizkio. Halaber, zerbitzua aurrera eramateko egingo diren jardueren kronograma onartu beharko du, enpresak egindako proposamenaren eta Ziur Fundazioak tresnaren erabileran trebatzeko hautatuko pertsonei zuzendutako prestakuntza-planaren edukiaren arabera.

Kanpaina bakoitza hasi aurretik, aldeek xehe-mehe zehaztu beharko dituzte aurrera eramango dituzten ekintzak.

Kanpaina bakoitzaren amaieran, zerbitzuaren atzerabegirako azterketa egin beharko da. Azterketa horretan, Ziur Fundazioak aurrez zehazturiko helburuen betetze-maila eta lan-metodologiaren egokitasuna ebaluatu beharko dira, eta azken kanpaina amaitzean, zerbitzuaren eta lortutako emaitzen balorazio globala ere egin beharko da.

V.- TRESNAREN EZAUGARRI TEKNIKOAK

Baldintza-agiri honetan eskatutako zerbitzua emateko erabiliko den ziber-engainurako tresnak gaitasuna izan beharko du interakzio- edo eraso-arauak ("engagement rules") ezartzeko, zeintzuen bidez, kanpaina bakoitzean zehazturiko enpresek, aurrez esleipendunak adierazi ondoren, eraso-zuhaitzaren kontrola eraman ahal izango baitute, erasotzailearen erabakietan aurrez zehazturiko moduan eta denbora errealean eragin ahal izateko, interakzioa luzatu eta TTP datu gehiago jasotzeko, azterketa-datuak jaso eta hurrengo pausoak aurreikusi ahal izateko ziurtasun-maila adierazgarriarekin eta emandako erantzunari egoki erantzun ahal izateko.

Horrez gainera, honako baldintza hauek bete beharko ditu, gutxienez:

1. Baztertu egiten dira "appliance" eredu fisiko batean oinarritutako irtenbideak. Engainu Aplikatiboak gai izan behar du bezeroaren eta zerbitzu-hornitzailearen ingurunetik jarduteko, eta ingurune fisikoetan, birtualetan nahiz "cloud"-ean instalatzeko. Irtenbideak ez luke izan behar intrusiboa, eta ez luke eskatu behar ekoizpen-sarean aritzen diren eragileen edo bestelako software-gailuen instalaziorik.

2. Irismena eta sakontasuna:
   Engainu Aplikatiboak mekanismo sinple bat izan beharko du erasotzaileen artean amu ("breadcrumbs") erakargarri eta sinesgarriak banatzeko "endpoint" eta zerbitzarietan, eta, modu horretan, engainu-estaldura zabala eskaintzeko barneko nahiz kanpoko sarean. Eta, aldi berean, interakzio altuko "honypots"-ak (engainu-zerbitzariak) automatikoki sortzeko gaitasuna izan beharko du, hau da, barneko sare batean, DMZ batean edo hodeian kokatuta dauden sistema eragile osoak (ez emulazioak), zehatzak eta sinesgarriak.

3. Instrumentazio osoa:
   Interakzio altuko "honypots"-ek guztiz definituak eta paketatuak egon behar dute, Kernel mailan dagoen eta zerbitzariko jarduera guztia detektatzen duen eragile guztiz ezkutu bat erabiliz. Detektatutako jarduera engainu-azpiegituraren bidez transmitituko da Engainu Aplikatibora edo irtenbidearen gunera, trafiko zifratua erabiliz, eta han prozesatu eta biltegiratuko da. Komunikazio-kanalak enkriptatuta egongo dira, eta ataka komunak erabiliko dira monitorizatutako trafikoa engainu-sarean disimulatzeko. Horrez gainera, TCP atakak ausaz esleitu ahal izango dira, engainu-"hosts"-ek erasotzaileen aurrean portaera berdina ez agertzeko.

4. Mehatxu-adimena testuinguruan jartzea:
   Engainu Aplikatiboak automatikoki aztertuko ditu "honeypots"-etan jasotako datuak, eta iturri gehigarrietako datuekin (adibidez MITRE ATT&CK) aberastu behar diren gertaerak sortzeko erabiliko ditu, horien interpretazioa errazago egiteko eta testuinguruan jartzeko. Halaber, gertaerak aztertuko dira IP helbideetan, "script" edukietan, artxibo-izenetan, komandoetan, argumentuetan eta abarretan bildutako objektuak identifikatzeko. Horien bidez, xehetasun handiz azter daiteke erasotzailearen jarduera, eta testuinguruan jarritako mehatxu-adimen

gidatua eta prozesagarria sor daiteke, enpresako sistementzat % 100 garrantzitsua izango dena. Erasotzailearen jarduerari buruzko datu guztietara sartzeko aukera izan beharko da tresnaren kontsolatik −web sarbidea izan beharko du− eta APi RESTful esportagarritik, mehatxu-trukerako protokolo komunak erabiliz (adibidez, STIX2 edo OpenIOC).

5. Kudeaketa zentralizatua:
   Engainu Aplikatiboaren kudeaketa zerbitzuaren esleipendunaren web-interfaze baten bitartez egin beharko da. Web-kontsolaren bidez, engainu-ingurunearen diseinua, inplementazioa eta kudeaketa egin ahal izango da; engainu-kanpainak sortzetik hasi –“breadcrumb”-ak sortzea eta banatzea barne–, eta maiztasun handiko zerbitzuekin interakzio altuko “honeypots”-ak inplementatzeraino. Web-kontsolak, halaber, zenbait tresna eskaintzen ditu gertaerei buruzko datuak bilatu, erasoen kronogramak bistaratu eta gorabeherei buruzko txostenak egiteko.

6. Integrazio osoa eta eskalan:
   Engainu Aplikatiboaren funtzio guztiek irisgarriak izan behar dute API interfaze baten bidez. Horrez gainera, tresnak integrazio natiboa eskaini behar du honako irtenbide komertzial hauekin, zibersegurtasun arloko hornikuntza, jakinarazpen, aberaste eta irtenbideen alorrean (horien artean, SIEM eta SOAR):
   - Google Suite
   - IPAbuseDB
   - Yara
   - Signal
   - VirusTotal
   - Microsoft Office 365
   - SNMP
   - Twitter
   - Microsoft Azure
   - POP3/IMAP
   - Cuckoo Sandbox
   - Amazon Web Services (AWS)
   - MaxMind
   - ElasticSearch ELK
   - IP2Location
   - Docker
   - SMTP
   - Devo
   - Palo Alto Demisto
   - VMware vSphere
   - Syslog
   - MISP
   - Tor nodes
   - Slack

- Splunk
- Alien Vault USM
- IBM Qradar
- Pagerduty
- Microsoft Teams
- Pastebin
- RequestTracker (RT)
- Twilio
- Telegram

V.- ERABILERA-KASUEN ADIBIDEAK

Adibide gisa, Ziur Fundazioak honako erabilera-kasu hauek proposatzen ditu zerbitzu kudeatuarentzat:

V.1..- VPN babesa

Erakundearen VPN azpiegituraren aurkako erasoak desbideratzea da kanpo-kanpaina honen helburu nagusia, erasoaren egileen arreta engainua moteltzeko gune edo “honynet” batera bideratu edo erakartzeko informazioa jasotzen duten “breadcrumb”-ak ezarriz. Engainua moteltzeko gune edo “honeynet” horretan, saio-hasierako VPN atari bat eta engainu-host batean inplementatutako web-zerbitzari bat egongo da, Engainu Aplikatiboari informazioa emango diona. Ogi-mami edo “breadcrumb” horiek Interneteko zerbitzu publikoetan ezarri ahal izango dira (adibidez, AWS S3 Bucket, Dropbox, Pastebin, shodan, GitHub, LinkedIn, Twitter, etab.), eta ziber-engainuko VPN zerbitzuaren konfigurazio-xehetasunak eduki ahal izango dituzte, hainbat formatutan (posta elektronikoa, Word dokumentua, SSL ziurtagiria), erakundearen izena jasotzen dutenak, web-saioaren hasiera-atariko DNS erregistroa adierazten dutenak, web-gune engainagarria adierazten duten txioak −TI departamentuko pertsonenak diruditenak−, etab.

Erasotzailea engainu-ingurune batean sartzen denean, alerta konfirmatu bat bidaliko da, eta, mehatxuen analisiaren bidez, adimen prozesagarria bidaliko zaio erakundeari TTP edo IoC modura, baita IPak eta erabilitako kredentzialak ere, zeinak segurtasun-irtenbideei bidali ahal izango baitzaizkie (adibidez, MISP, SIEM, SOAR, etab.).

V..2.- Kanpoko IoT gailuak

IoT gailu baten bidez, erakundearen aurkako mehatxu gidatuak identifikatzea da kanpainaren helburu orokorra, Interneten “breadcrumb”-ak ezarriz. Instrumentazio handiko “Deception Hosts” inguruneetan erabilitako metodologia behatuz, ekoizpen-zerbitzuaren ahuleziak aurkitu ahal izango dira, kontrainteligentzia akzionagarria eskura jartzeko.

Horretarako (1. fasea), ziber-eragileak IoT gailu bateko ezaugarri zaurgarri bat identifikatzen du bezeroaren IoT gailu batean. Puntu horretan, ziber-eragileak “honeypots”-ak aurkituko ditu, Engainu Aplikatiboari informazioa bidaliko diotenak. Hala, kontsolaren bidez, egoera aztertu ahal izango da, ingurune korporatibotik.

Horretarako, RISC, Linux ARM 7 32 bits eta MIPS LE 32 bit kontrolagailuen instrumentazioaren euskarri-lanak egingo ditu Engainu Aplikatiboak.

V..3- Errekonozimendu-jardueraren identifikazioa

Bezeroaren erakundearen aurkako errekonozimendu aktibo gidatuak identifikatzea da kanpainaren helburu nagusia, Interneten “breadcrumb”-ak ezarriz. Horretarako, egindako saiakeren eta erasoen metodologia behatzen da, eta kanpaina guztiz kanpokoa denez, korporazioaren barneko sarea babesten da.

Horretarako (1. fasea), ziber-eragileak Internet publikoaren bidez egiten du errekonozimendua, Pastebin edo Shodan bidez. Ustez nahi duen web-gunearen helbidea lortu ondoren, “login” ataria duen “honeypot” batera iritsiko da ziber-eragilea, eta, ingurune horretan, Fileshare bidezko fitxategi bat aurkituko du, okerreko aztarna bat emango diona. Atari horrek Engainu Aplikatiboari pasatzen dio informazioa (2. fasea).

Puntu horretan, ziber-eragileak “honeypots”-ak aurkituko ditu, Engainu Aplikatiboari informazioa bidaliko diotenak. Hala, kontsolaren bidez, egoera aztertu ahal izango da, ingurune korporatibotik.

V..4.- Informazioaren kanpoko filtrazioen identifikazioa

Informazioaren kanpoko filtrazioetan oinarrituta bezeroaren erakundearen aurka egindako mehatxuak identifikatzea da kanpainaren helburu orokorra, Interneten “breadcrumb”-ak ezarriz. Horretarako, egindako saiakeren eta erasoen metodologia behatzen da, eta, kanpaina guztiz kanpokoa denez, korporazioaren barneko sarea babesten da.

Horretarako (1. fasea), ziber-eragileak Internet publikoaren bidez egiten du errekonozimendua, AWS S3 Bucket edo Dropbox bezalako biltegiratze-zerbitzuen bitartez. Ustez nahi duen web-gunearen helbidea lortu ondoren, “login” ataria duen “honeypot” batera iritsiko da ziber-eragilea, eta, ingurune horretan, Fileshare bidezko fitxategi bat aurkituko du, okerreko aztarna bat emango diona (2. fasea). Atari horrek Engainu Aplikatiboari pasatzen dio informazioa.

Puntu horretan, ziber-eragileak “honeypots”-ak aurkituko ditu −instrumentazio handikoak CounterCraft eragilearen bidez (3. Fasea) −, Engainu Aplikatiboari informazioa bidaliko diotenak. Hala, kontsolaren bidez, egoera aztertu ahal izango da, ingurune korporatibotik.

V.2.5.- Deep Web

Bezeroaren erakundearen aurkako errekonozimendu aktibo gidatuak identifikatzea da kanpainaren helburu nagusia, DeepWeb-en “breadcrumb”-ak ezarriz.

Horretarako (1. fasea), ziber-eragileak Internet publikoaren bidez egiten du errekonozimendua, Pastebin edo Shodan bidez. Ustez nahi duen web-gunearen helbidea lortu ondoren, “login” ataria duen “honeypot” batera iritsiko da ziber-eragilea, eta, ingurune horretan, Fileshare bidezko fitxategi bat aurkituko du, okerreko aztarna bat emango diona (2. fasea). Atari horrek Engainu Aplikatiboari pasatzen dio informazioa.

Puntu horretan, ziber-eragileak instrumentazio handiko “honeypots”-ak aurkituko ditu (3. Fasea), Engainu Aplikatiboari informazioa bidaliko diotenak. Hala, kontsolaren bidez, egoera aztertu ahal izango da, ingurune korporatibotik.

72724351F KOLDOBIKA PECIÑA (R: G75203067)

Digitalki sinatuta norengandik: 72724351F KOLDOBIKA PECIÑA (R: G75203067)
Data: 2020.11.09 13:23:39 +01'00'