NAPREDNE TRAJNE GROŽNJE IN USMERJEN KIBERNETSKI NAPAD NA ORGANIZACIJE

Daša Janja Banovec

Namen prispevka

Prispevek predstavi napredne trajne grožnje (APT - advanced persistent threats) in usmerjen napad na organizacije. Namen prispevka je predstaviti obravnavano tematiko ter opozoriti na problematiko in posledice tovrstnih napadov. Tovrstni napadi so namreč izvedeni z namenom protipravnega pridobivanja ali uničenja kritičnih informacij, poslovnih skrivnosti in intelektualne lastnine ciljnih organizacij. Pred APT ni zares varna nobena organizacija, neglede na velikost, lastniško strukturo in tržno panogo.

Metode

Osnova prispevka je analiza literature različnih avtorjev in organizacij, ki se ukvarjajo s problematiko usmerjenih napadov in APT. Obstoječa spoznanja bodo z metodo kompilacije in metodo deskripcije predstavila problematiko in podala predloge za zaznavanje in učinkovitejše zoperstavljanje tej problematiki.

Ugotovitve

Uporaba zlonamerne programske opreme za protipravno pridobivanje kritičnih informacij, intelektualne lastnine ipd., z namenom pridobivanja finančne koristi ali konkurenčne prednosti, ni nov trend. Kljub temu, da so bili usmerjeni napadi, ki vključujejo APT in so usmerjeni proti podjetjem, korporacijam, vladnim in državnim službam ter posameznim industrijam zaznani že pred leti, pa se je v zadnjih letih število tovrstnih napadov močno povečalo. Tovrstni napadi predstavljajo grožnjo v obliki mednarodnega, gospodarskega ali konkurenčnega vohunstva in ogrožajo številne organizacije in nacionalna gospodarstva. Problematika se kaže predvsem v oteženem zaznavanju napadov, ponavljajočem in dolgoročnem izvajanju napadov ter konstantnem izboljševanju in prilagajanju metod, vrst in orodij napadov glede na uspešnost izvedenih predhodnih napadov ter varnostne zaščite ciljne organizacije.

Izvirnost/pomembnost prispevka

Prispevek je pripravljen kot pregledni članek, kjer so na enem mestu zbrane ugotovitve z analiziranega področja, z namenom širitve zavesti o obravnavani problematiki in zagotavljanja učinkovitejšega zoperstavljanja APT in usmerjenim napadom.

Ključne besede: usmerjen napad, napredna trajna grožnja, zlonamerna programska oprema, organizacije

1 UVOD

Že od nekdaj so ljudje iz najrazličnejših razlogov želeli (protipravno) pridobiti lastnino, znanja in informacije, ki jih posedujejo drugi posamezniki, organizacije ali države. Pridobivanje lastnine, informacij in znanja se je z digitalizacijo preneslo iz fizičnega v digitalno oz. spletno okolje. Tako so kibernetski napadi postali neizogibna posledica digitalizacije. In kakor so se spreminjali načini pridobivanja informacij, tako so se spreminjale tudi varnostne rešitve za njihovo preprečevanje in obratno. Bolj učinkovite, kot so postale varnostne rešitve, bolj sofisticirani in napredni so postali kibernetski napadi.

Velika večina tradicionalnih (t.j. ne-ciljno usmerjenih) kibernetskih napadov, storjenih z zlonamerno programsko opremo, ne kaže dokazov o posebni izbiri prejemnika napada. Praviloma je namen tovrstnih napadov želja po ogrozitvi večjega števila sistemov, neglede na identiteto teh sistemov. V teh primerih je napadalec najverjetneje prepričan, da lahko nekateri izmed ogroženih sistemov vsebujejo informacije, ki jih je mogoče prodati oz. ovrednoti z drugimi sredstvi (Thonnard, Bilge, O'Gorman, Kiernanin in Lee, 2012: 66). Medtem ko je prejemnik napada pri ne-ciljnih napadih bolj ali manj naključno izbran, pa je pri ciljno usmerjenem napadu prejemnik napada skrbno izbran, napad pa je ciljno usmerjen in premišljeno izveden (Thonnard et al., 2012). Namen usmerjenih napadov je pridobiti dostop do informacij visoke vrednosti, ki jih poseduje napadeni subjekt, ogroziti te informacije ali pa uporabiti ogroženi sistem za izvajanje napadov na druge sisteme, ki vsebujejo informacije visokih vrednosti. Problematika usmerjenih napadov se še dodatno kaže v izvedbi napadov, saj so tovrstni napadi najpogosteje izvedeni s pomočjo naprednih trajnih groženj, ki omogočajo zaobitje tradicionalnih varnostnih zaščit in manjšajo možnosti (pasivne) zaznave napada.

Uporaba zlonamerne programske opreme, z namenom protipravnega pridobivanja oz. kraje občutljivih, poslovno pomembnih in/ali zaupnih informacij organizacijam (iz organizacij), ni nov trend, saj je prisoten že zadnja desetletja. Kljub temu, da so bili ciljno usmerjeni napadi zaznani že pred leti, pa se je v zadnjem času število tovrstnih napadov močno povečalo. Pri Symantec (2013a) so tako leta 2005 identificirali (prepoznali) in blokirali približno en usmerjen napad na teden, naslednje leto se je število tovrstnih napadov povečalo na napad do dva tedensko, leta 2012 pa se je število usmerjenih napadov povečalo na kar 116 napadov dnevno. Kljub temu, da so se usmerjeni napadi z zlonamerno programsko opremo v zadnjih letih povečali v obsegu in zahtevnosti izvedbe, pa je

zaznavanje in prepoznavanje napadov s strani prejemnikov napadov še vedno zelo težko in zahtevno delo (Symantec, 2013a).

Vidimo lahko, da so usmerjeni napadi in napredne trajne grožnje (kot oblika izvedbe usmerjenega napada) postali realnost sodobnega časa, ki organizacije sili v upravljanje tovrstnih groženj. Ozaveščanje tako predstavlja prvi korak na poti do preprečevanja tovrstnih groženj in trdne organizacijske varnosti.

2 PROBLEMATIKA

Kljub temu, da se računalniška omrežja že več desetletij uporabljajo tudi za namene vohunjenja, obstaja splošno mnenje oz. prepričanje, da so usmerjeni napadi svojevrstna oblika varnostne grožnje. Tovrstni napadi so v javnosti znani od sredine leta 2000, ko so se pojavili incidenti, ki so kazali znake, da so zagrešeni s strani nacionalnih vlad ali na podlagi njihovih naročil[1] (Microsoft, 2012: 7).

Ko govorimo o naprednih trajnih grožnjah in usmerjenih napadih, najpogosteje pomislimo, da so »tarče« tovrstnih napadov predvsem velike, znane organizacije, multinacionalke ter (zasebne in javne) organizacije, ki delujejo v posameznih ekonomsko in gospodarsko bolj zanimivih panogah (npr. obramba, energetika, farmacija ipd). Zagotovo so tovrstne organizacije in panoge nekoliko bolj izpostavljene napadom in grožnjam, vendar pa je potrebno poudariti, da se je v zadnjih letih obseg ciljno usmerjenih napadov močno povečal in vključuje oz. zajema najrazličnejše organizacije, neglede na njihovo velikost in tržno panogo. Symantec (2013b) tako ugotavlja, da so tarče oz. žrtve usmerjenih napadov, v zadnjih letih, postala tudi mala in srednjevelika podjetja in organizacije.

Kljub temu, da lastniki in vodstva malih in srednje velikih podjetij menijo, da sami (zaradi svoje majhnosti) ne morejo postati žrtve ciljnih napadov, pa podatki kažejo, da je kar polovica tovrstnih napadov usmerjenih na organizacije z manj kot 2.500 zaposlenimi. Pravzaprav je kar 31 odstotkov (usmerjenih) napadov usmerjenih na podjetja, ki zaposlujejo manj kot 250 ljudi (Symantec, 2013b). Zapisano bi lahko pojasnili s tem, da lahko mala podjetja izvajalcem napadov predstavljajo »odskočno desko« za olajšan vdor v informacijski sistem večjih organizacij (npr. dobavitelji, partnerji ipd.), s katerimi mala podjetja sodelujejo (Symantec, 2012). Razloge za izvajanje usmerjenih napadov na mala podjetja je moč iskati tudi v slabše zaščiteni (informacijski) infrastrukturi malih podjetij ter odsotnosti ali pomanjkanju nadzorovanja podatkovnega prometa.

Medtem ko je 55 odstotkov elektronske pošte z zlonamerno programsko opremo usmerjenih na visoke in višje vodstvene delavce ter zaposlene na področju raziskav in razvoja, torej na ljudi, ki dnevno operirajo s pomembnimi poslovnimi informacijami, pa je večji del naprednih groženj usmerjenih na

[1] Kot primer lahko navedemo Kitajsko, ki naj bi izvajala usmerjene napade na kritično državno, gospodarsko in vojaško infrastrukturo Združenih držav Amerike.

ljudi, ki nimajo neposrednega dostopa do zaupnih podatkov (Symantec, 2012; Symantec, 2013a). Predvsem so to ljudje s področja prodaje, marketinga, odnosov z javnostmi ter osebni asistenti, torej ljudje, ki jih je lahko preučiti (npr. na spletnih straneh organizacije) in s katerimi je dokaj enostavno stopiti v kontakt. Ti ljudje predstavljajo izvajalcem napada »odskočno desko« za dosego svojih ciljev oz. vstopno točko za izvedbo kibernetskega napada, saj so to ljudje, ki so v okviru svojih delovnih obveznosti redno v stikih z ljudmi, ki jih ne poznajo (Symantec, 2013a). Tako npr. kadrovniki dnevno prejemajo elektronsko pošto, poslano s strani (nepoznanih) posameznikov, ki iščejo zaposlitev. To izvajalcu usmerjenega napada močno olajša delo, saj lahko pod pretvezo iskanja zaposlitve kadrovniku posreduje elektronsko pošto in priponko z lažnim življenjepisom, ki vsebuje zlonamerno programsko opremo, s čimer napadalcu nevede omogoči vdor v informacijsko infrastrukturo ciljne organizacije.

Potrebno je poudariti, da pred usmerjenimi napadi in naprednimi trajnimi grožnjami ni varna nobena gospodarska panoga in da tovrstni napadi vplivajo na vse sektorje gospodarstva (Symantec, 2011). Naj dodamo, da enake tehnike, kot jih uporabljajo kibernetski napadalci za izvajanje industrijskega ali konkurenčnega vohunstva, lahko uporabljajo tudi države za izvajanje političnega vohunstva (Symantec, 2013a). Iz zapisanega izhaja, da morajo usmerjeni napadi in APT-ji organizacijam predstavljati enega izmed osrednjih izzivov pri zagotavljanju poslovne oz. organizacijske varnosti.

2.1 Terminološka opredelitev

V tem delu prispevka bomo predstavili terminološko opredelitev usmerjenih napadov in naprednih trajnih groženj (APT). Opredelitev usmerjenih napadov in APT je namreč pomembna za razumevanje narave tovrstnih groženj in hkrati organizacijam omogoča iskanje in vzpostavitev najprimernejših in najučinkovitejših varnostnih rešitev.

Čeprav usmerjene napade lahko razumemo kot evolucijo konvencionalnega »maleware-a« na višji, bolj prefinjeni stopnji, jih bolj natančno lahko označimo kot evolucijo konvencionalnih tehnik vohunjenja, usmerjenega na ciljne posameznike in organizacije, razvitih do mere, ki je bila še nedolgo nazaj prava redkost (Microsoft, 2012: 7).

Usmerjen napad lahko opredelimo kot dolgoročno kibernetsko vohunstvo usmerjeno proti organizaciji, podjetju oz. korporaciji, vladnim službam ali posamezni industriji. Cilj izvajalcev usmerjenih napadov je pridobiti dolgoročen (stalen) dostop do omrežja prejemnika napada. Tovrsten dostop napadalcu omogoča pridobivanje zaupnih podatkov ciljne organizacije oz. omogoča, da napadalec logično oz. strateško postavi »bombe«, ki lahko poškodujejo celotno mrežo in informacijsko infrastrukturo ciljne organizacije. Stalen oz. dolgoročen dostop namreč napadalcem omogoča, da napadeno infrastrukturo, nad katero ima nadzor, uporabi za napade na druge organizacije. Tak napad ima tudi dodatno mero legitimnosti (npr. prihaja od zaupanja vrednega partnerja). Uporaba

tako okuženih omrežij pri napadih na druge organizacije pomeni tudi težjo izsledljivost napada nazaj do napadalca. Posledice tovrstnega napada so lahko še bolj dramatične v primeru, da je napadena organizacija vključena v upravljanje s kritično infrastrukturo (Trend Micro, 2013a: 5).

Napad lahko obravnavamo kot usmerjen, kadar je namenjen določeni osebi ali organizaciji. Tovrstni napadi so praviloma ustvarjeni tako, da se izognejo tradicionalnim varnostnim zaščitam (Symantec, 2013a). Usmerjeni napadi se izvajajo s pomočjo prilagojene oz. po meri narejene zlonamerne programske opreme in s pomočjo prefinjenega, usmerjenega socialnega inženiringa, z namenom pridobitve nepooblaščenega dostopa do občutljivih informacij. V prefinjeno usmerjenem socialnem inženiringu, ki je nova stopnja v evoluciji socialnega inženiringa, so žrtve vnaprej raziskane in skrbno izbrane (Symantec, 2011: 14). Izvrševalci tovrstnih napadov najpogosteje uporabljajo usmerjene napade za nepooblaščeno pridobivanje poslovno pomembnih podatkov (npr. podatke o strankah, razvoju ipd.), z namenom pridobivanja finančne koristi ali pridobivanja konkurenčne prednosti.

Lahko rečemo, da napredne trajne grožnje predstavljajo vrsto kibernetskega napada, ki uporablja usmerjene napade kot del organiziranega dolgoročnega vohunjenja (običajno) za ciljnimi informacijami ali sistemi visokih vrednosti. Vendar pa je na tem mestu potrebno poudariti, da so napredne trajne grožnje vedno (ciljno) usmerjene, da pa usmerjeni napadi ne predstavljajo vedno napredne trajne grožnje (Symantec, 2011). Da je temu tako, bomo razložili in prikazali s pomočjo terminološke opredelitve naprednih trajnih groženj.

Izraz napredne trajne grožnje (ang. advanced persistent threat – APT) se je razvil za opis edinstvene kategorije usmerjenih napadov, ki so oblikovani posebej za ciljnega posameznika ali organizacijo, z namenom pridobivanja kritičnih informacij. Napredne trajne grožnje (v nadaljevanju APT) so oblikovane tako, da ostanejo v sistemu kar se da dolgo neodkrite ter so zasnovane tako, da se v sistemu premikajo počasi in »tiho« z namenom, da se izognejo zaznavi in odkritju (Symantec, 2013a: 52). Za razliko od tradicionalnih napadov, ki so hitro izvedeni in predstavljajo hitro pridobivanje koristi (predvsem finančnih), pa imajo lahko APT-ji cilj mednarodnega, industrijskega ali konkurenčnega vohunstva in/ali sabotaže (Symantec, 2013a: 52). Cilji APT lahko vključujejo vojaška, politična ali gospodarska zbiranja obveščevalnih podatkov, pridobivanje zaupnih podatkov in/ali poslovnih skrivnosti organizacij, motenje delovanja organizacij ali celo uničevanje podatkov in opreme ciljne organizacije (Symantec, 2013a). Namen večine APT je pridobivanje informacij iz sistema »napadene« organizacije (npr. ključne raziskave, poslovne skrivnosti, intelektualno lastnino, tehnološke in proizvodne podatke ipd).

Ameriški Nacionalni inštitut za standarde in tehnologijo opredeljuje napredne trajne grožnje kot »nasprotnika oz. tekmeca, ki poseduje prefinjeno raven strokovnega znanja in pomembnih virov, ki mu omogočajo ustvarjanje priložnosti in doseganje ciljev z več vrstami napadov (npr. kibernetski napad, fizični napad, prevara). Ti cilji navadno vključujejo vzpostavitev in razširitev dostopa v infrastrukturo informacijske tehnologije ciljnih organizacij, z namenom pridobivanja zaupnih informacij ter oviranja ali ogrožanja ključnih procesov v ciljni organizaciji. APT tako pomeni

večkratno uresničevanje teh ciljev v daljšem časovnem obdobju in neprestano prilagajanje na zaščito ciljnih organizacij, z namenom ohraniti stopnjo interakcije, ki je potrebna za izvršitev zastavljenih ciljev« (National Institute of Standards and Technology, 2011: B-1). Zapisana opredelitev predstavlja dobro izhodišče za razumevanje razlik med tradicionalnimi grožnjami in naprednimi trajnimi grožnjami. Ponavljajoče opravljanje ciljev, prilagajanje in vztrajnost namreč razlikujejo APT od ostalih tradicionalnih groženj in napadov. Naprednost grožnje se tako kaže v uporabljenih metodah, ki omogočajo izogibanje zaznavi in odkritju. Naprednost se kaže tudi v uporabi sredstev za vzpostavitev komunikacije in nadzora nad omrežjem, pri čemer izvrševalci napadov uporabljajo enkripcijo in podatke pošiljajo razpršeno, v majhnih količinah ter prikrito, kar se v omrežju kaže kot navidezno običajen promet. Izvrševalci napada se za zagotavljanje neodkritja eksfiltracije ukradenih informacij izogibajo uporabi enostavnega in z lahkoto zaznanega šifriranja ter uporabljajo običajne kanale in protokole, ki niso videti sumljivi in zagotavljajo, da podatki ostanejo skriti (Symantec, 2013a: 52). Trajnost grožnje se kaže predvsem v odsotnosti iskanja kratkoročnih ciljev, saj se napadalci poslužujejo počasnih in postopnih pristopov, ki praviloma nimajo neposrednih učinkov, s katerimi bi napadeno organizacijo opozorili na nenavadno dogajanje (Symantec, 2013a). Grožnja pa se nanaša na dejstvo, da tovrstni napadi niso posledica neke pomanjkljivosti ali (programske) napake, temveč so posledica usklajenega delovanja posameznika ali skupine, ki je usposobljena, dobro organizirana in motivirana ter se sistematično loti izvedbe napada na ciljno organizacijo.

Značilnost APT je tudi ta, da predstavlja dolgoročen napad, ki ne sledi oportunističnemu pristopu (hitro doseganje ciljev), značilnim za večino napadov izvedenih z zlonamerno programsko opremo. Tako je cilj APT, da ostane kar se da dolgo neodkrit ter da v tem obdobju izvaja in uporablja različne vrste napadov. APT izvajalcu napada omogoča, da v primeru neuspelega napada uporabi drugačen pristop izvedbe napada. Tovrstni napadi napadalcu omogočajo, da lahko okužen sistem uporabi tudi kot »oporišče« za izvedbo naslednjih napadov (Symantec, 2013a: 52). Pri Trend Micro (2012a) opozarjajo, da kljub temu, da se zlonamerna programska oprema običajno uporablja kot orodje napada, predstavljajo APT resnično grožnjo, saj napade izvajajo posamezniki ali skupine, ki na podlagi informacijske zaščite (napadene) organizacije spreminjajo, prilagajajo in izboljšujejo metode izvedb napadov.

2.2 Modus operandi

V tem delu prispevka bomo predstavili metodološko premico, ki prikazuje~~,~~ kako poteka izvajanje APT in usmerjenih napadov. APT potekajo v več fazah: vdor, odkritje, zajetje in eksfiltracija podatkov. Pred dejansko izvedbo napada pa izvajalci napadov pridobivajo informacije o cilju napada, kar bi lahko označili za/kot predhodno fazo.

2.2.1 Predhodna faza – pridobivanje informacij o cilju napada

Navadno napadalec pred izvedbo napada zbira oz. pridobiva podatke in uporabi tehnike socialnega inženiringa, ki mu omogočajo učinkovitejšo izvedbo napada. V tej fazi je cilj izvajalca napada pridobiti strateško pomembne podatke o ciljnem informacijsko-tehnološkem okolju, kot tudi podatke o ciljni organizacijski strukturi. Zbrane informacije lahko obsegajo različne poslovne aplikacije in programsko opremo organizacije, vloge in odnose, ki obstajajo znotraj ciljne organizacije ipd. (Trend Micro, 2012b: 1). Pridobljeni podatki napadalcu npr. omogočajo oblikovanje (relevantne) vsebine e-pošte, ki naj bi bila za prejemnika pomembna in/ali dovolj zanimiva, da bo odprl prejeto priponko ali kliknil na priloženo spletno povezavo.

2.2.2 Faza vdora

Prva faza je faza vdora, v kateri poskuša napadalec vdreti (prodreti) v omrežje organizacije. Za dosego tega cilja lahko napadalci uporabijo različne pristope. Najpogostejšo »vstopno točko« izvajalcev usmerjenih napadov predstavlja najpogostejša oblika pisarniškega komuniciranja, t.j. elektronska pošta. Tako je, zaradi nizke stopnje vloženega truda in pogoste oblike komunikacije preko e-pošte, običajna praksa, da napadalec izbrani žrtvi pošlje e-pošto, ki vsebuje zlonamerno priponko. Takšne priponke so tarčam najpogosteje posredovane v obliki PDF dokumentov, Microsoft Word, Excel ali PowerPoint dokumentov ter izvršljivih datotek (.exe datoteke) (Trend Micro, 2013a; Thonnard et al., 2012; Symantec, 2012). Izvrševalec napada lahko po e-pošti cilju napada namesto priponke posreduje spletno povezavo, ki išče in izkorišča ranljivost spletnih brskalnikov ali dodatkov in vtičnikov za spletne brskalnike (Trend Micro, 2012a). Za vdor lahko napadalec uporabi tudi alternativne pristope; npr. napadalec poišče spletno mesto, ki ga uporablja žrtev in preko tega poizkuša vdreti v informacijski sistem oz. celotno informacijsko infrastrukturo (Thonnard et al., 2012). Izvajalci napadov pa lahko za vstopno točko uporabijo tudi t.i. instant sporočila ali socialna omrežja, s katerimi pritegnejo potencialno tarčo in jo (pod pretvezo) pripravijo, da klikne na priloženo povezavo ali da naloži oz. prenese datoteko, ki vsebuje zlonamerno programsko opremo (Trend Micro, 2012a: 1). Vdor se lahko izvede tudi s pomočjo okužbe z zlonamerno kodo preko fizičnega nosilca, kot so okuženi USB ključi ali drugi podatkovni nosilci (Symantec, 2011).

Za pošiljanje elektronske pošte tarčam, uporabljajo izvrševalci napadov lažne elektronske naslove ali e-naslove organizacij ali oseb, s katerimi je tarča napada v preteklosti že komunicirala, saj tako povečajo možnost za realizacijo napada. Za povečanje možnosti realizacije napada napadalci pogostokrat, glede na ciljno organizacijo ali posameznika, prilagodijo tudi vsebino e-pošte, da je le-ta za prejemnika relevantna (Trend Micro, 2013b). Thonnard in sodelavci (2012) ugotavljajo, da

zlonamerne priponke elektronske pošte najpogosteje vsebujejo nevarnost v obliki »trojanskega konja« oz. »Backdoor Trojan[2]«. Ko žrtev prejme e-pošto in odpre priloženi dokument, postane njen računalnik ogrožen, saj se trojanski konj naloži na žrtvin računalnik, kar napadalcu omogoči oddaljen dostop in nadzor ter upravljanje z okuženim sistemom.

2.2.3 Faza odkrivanja

Ko izvajalc napada dobi dostop do sistema organizacije, začne ocenjevati omrežje, pridobivati načrt oz. strukturo sistema ter na podlagi tega locirati zaupne podatke. Odkritje lahko vključuje nezaščitene podatke in omrežja, varnostne luknje v programski in strojni opremi ter nezaščitene, izpostavljene dostopne podatke (uporabniška imena in gesla ipd.) ter povezave do dodatnih virov ali dostopnih točk (Symantec, 2011; Thonnard et al., 2012). V fazi odkrivanja je torej vloga napadalca, da poišče ranljivosti napadenega sistema in omrežja, da si omogoči dostop do čim večjega števila podatkov ter da v sistemu ostane kar se da dolgo neodkrit, saj si s tem omogoči dolgoročen dostop do podatkov ciljne organizacije.

2.2.4 Faza zajetja

V fazi zajetja dobi napadalec dostop do nezaščitenih sistemov oz. omrežij, kar mu omogoča namestitev zlonamerne programske opreme, ki omogoča (prikrit) dostop do podatkov ali motenje delovanja sistema ciljne organizacije (Symantec, 2011). V tej fazi izvajalci napadov identificirajo informacije ciljne organizacije z uporabo različnih orodij, ki omogočajo spremljanje in zbiranje podatkov še pred izvedbo dejanske eksfiltracije podatkov. Napadalec tako pridobi seznam datotek, ki so shranjene v različnih mapah na različnih mestih, kar mu omogoča, da pregleda dokumente in ugotovi katere so tiste informacije in podatki, ki so zanj pomembni in dragoceni. Hkrati lahko identificira tudi strežnike elektronske pošte, kar napadalcu omogoča prebiranje e-pošte z namenom odkritja pomembnih informacij in podatkov (Trend Micro, 2012a: 2). V fazi zajetja tako napadalec pridobi dostop do podatkov, ki jih nato analizira z namenom, da ugotovi, katere podatke želi v nadaljevanju eksfiltrirati. Ugotovimo lahko, da izvajalci napadov ne eksfiltrirajo vseh podatkov, do katerih si zagotovijo dostop, saj vsi podatki zanje niso pomembni.

2.2.5 Faza eksfiltracije

[2] »Backdoor Trojan« je trojanski konj (zlonamerna koda), ki povezuje delovno postajo in strežnik ter omogoči razvijalcu oddaljen dostop in nadzor nad okuženim računalnikom.

Končni cilj APT napada je prenos informacij ciljne organizacije na lokacijo, ki jo upravlja in nadzira izvajalec napada. V fazi eksfiltracije poišče napadalec mehanizme, ki mu omogočajo krajo podatkov ciljne organizacije. Izvajalec napada lahko ciljne podatke naloži na oddaljen strežnik ali spletno mesto do katerega ima dostop. Bolj prikrite metode pa lahko vključujejo tudi šifriranje in/ali steganografijo[3] podatkov za dodatno prikrivanje eksfiltracije (Symentec, 2014: 28). Eksfiltracijo podatkov lahko izvajalec napada izvede hitro, lahko pa jo izvaja postopoma. Na tem mestu je potrebno poudariti, da APT napadi praviloma niso izvedeni zgolj v enkratnem procesu, pač pa se cikel odkrivanja, zajemanja in eksfiltracije pogosto ponavlja. V tem primeru izvajalec napada išče nove cilje ter širi svoj nadzor nad sistemom in omrežjem organizacije, pri tem pa lahko spreminja svoje načrte ter prilagaja tehnike in orodja, ki mu omogočajo dosego cilja.

3 PREVENCIJA

APT predstavljajo enega izmed osrednjih izzivov pri varovanju omrežij organizacij, saj za zaščito pred njimi ne obstaja programska oprema, ki bi sistematično odpravljala težave s tovrstnimi napadi. Za zaščito pred tovrstnimi napadi je tako ključno, da organizacije vzpostavijo kombinacije različnih orodij za spremljanje, nadzorovanje, evidentiranje in preučevanje podatkovnega prometa, ki poteka skozi omrežje organizacije. Naj poudarimo, da je vzpostavitev tovrstne zaščite zahteven izziv tudi za največje organizacije in korporacije[4] (Cisco, 2011; Symantec, 2011).

Za zoperstavljanje APT morajo organizacije težiti k celovitemu pristopu, ki se osredotoča tako na večplastno zaščito, kot tudi na analiziranje in odzivanje na incidente. Elementi APT obrambne strategije morajo vsebovati razumevanje tega, kaj je potrebno zaščititi, kako so razvrščani oz. klasificirani podatki, kakšna je informacijsko-varnostna »drža« organizacije in kakšne so organizacijske zmožnosti odkrivanja incidentov. Za zoperstavljanje APT morajo organizacije ozaveščati in usposabljati zaposlene, kot tudi pripraviti proaktivni načrt za ukrepanje v primeru zaznave incidenta.

3.1 Opozorilni znaki in metode zaznavanja

[3] Steganografija je znanost, ki omogoča skrivanje podatkov v navidezno nepomembnem prenosnem mediju. Podatki so skriti tako, da ni mogoče ugotoviti, ali nosilni podatki (npr. slikovna datoteka) vsebujejo skrito sporočilo ali druge podatke. Za razliko od kriptografije oz. šifriranja podatkov, katere cilj je narediti podatke neberljive, steganografija poskuša prikriti obstoj podatkov. Naj poudarimo, da sta kriptografija in steganografija sicer sorodni tehniki.

[4] Leta 2010 je bil izveden izredno prefinjen napad na Google, poimenovan Operacija Aurora, kjer so napadalci poskušali pridobiti Googlovo intelektualno lastnino - izvorno kodo.

V tem delu prispevka bomo predstavili znake, ki opozarjajo na APT in metode, ki omogočajo zaznavo opozorilnih znakov. Opozorilne znake lahko razdelimo na zgodnje in pozno zaznane. Zgodnji opozorilni znaki so: sumljiva elektronska pošta, nenavaden promet, nenavadne datoteke (škodljiva koda v lupini), sumljive povezave. Glede na to, da predstavlja e-pošta najpogostejšo vstopno točko izvajalcev APT napadov, lahko s spremljanjem dejavnosti in prometa e-pošte, z namenom zaznavanja sumljivih sporočil in prenosov, pripomoremo k zgodnjemu odkrivanju APT. Nenavaden promet lahko organizacija zazna v primeru, da ima vzpostavljeno izhodišče za normalno/običajno obnašanje/vedenje omrežja (npr. protokole, aplikacije, vedenje uporabnikov ipd.). V tem primeru je za zaznavo APT potrebno spremljati nepričakovane spremembe v uporabi protokola, obsega prometa in vedenja uporabnikov. Škodljiva koda je pogosto skrita v običajnih skupinah datotečnih formatov (PDF, HTML, Gif ipd.). Sposobnost dešifriranja, dekodiranja in odkrivanja škodljive kode v lupini je eden izmed najbolj učinkovitih načinov za odkrivanje APT (McAfee, 2011: 5). Glede na to, da izvajalci APT napadov pogostokrat uporabljajo IP naslove, spletne strani, datoteke in strežnike elektronske pošte, ki že imajo zgodovino zlonamernih aktivnosti, je za zaznavanje APT priporočena uporaba orodij za nadzor ugleda/slovesa povezave z nezanesljivimi viri izven organizacije (McAfee, 2011).
Glede na to, da je večji del APT odkrit šele takrat, ko je varnost organizacije že ogrožena, je potrebno predstaviti tudi t.i. pozne opozorilne znake. Pozni opozorilni znaki so: spremembe v nameščenih aplikacijah oz. programski opremi, poizkusi pridobivanja dostopa do podatkov in prenosi podatkov. Izvajalci napadov po vdoru v omrežje pogostokrat poskušajo izdati ukaze ključnim aplikacijam in na ta način spreminjati njih ali njihovo delovanje. Za odkrivanje in preprečevanje nedovoljenih (poizkusov) sprememb na ključnih aplikacijah se priporoča uporaba tehnike s seznamom dovoljenih aplikacij. Za odkrivanje nepooblaščenih poskusov dostopanja do podatkov in podatkovnih baz je priporočena uporaba orodij za spremljanje aktivnosti podatkov in podatkovnih baz. Za zaznavanje nepooblaščenega prenosa podatkov je potrebno spremljati vrsto, količino in lokacijo prenesenih podatkov. Priporočena je uporaba orodij za preprečevanje izgube podatkov, nadzorovanje (nenavadne) količine prenosa podatkov, netipičnih prenosov in šifriranega prometa podatkov ter uporaba orodij, ki omogočajo spremljanje ugleda IP naslovov lokacije prenosa podatkov (McAfee, 2011). Nenavadni IP naslovi, ki uporabljajo nestandardne protokole ali netipične vstopne ali izstopne točke v/iz organizacijkega omrežja prav tako opozarjajo na APT grožnjo.

3.2 Informacijska infrastruktura

Brez ustrezno konfigurirane infrastrukture so organizacije nemočne pri zoprestavljanju zoper usmerjene napade in APT. Kljub temu, da predstavlja ustrezna konfiguracija informacijske infrastrukture organizaciji zajeten izdatek, se morajo organizacije zavedati, da dejanski in prihodnji

stroški, ki jh povzroči izguba ali iznos zaupnih in pomembnih poslovnih informacij, odtehtajo izdatek, ki ga nosi ustrezno konfiguriranje informacijske infrastrukture (Trend Micro, 2013a: 8).

3.2.1 Segmentacija

Za zagotavljanje večje stopnje varnosti omrežja in posledično varovanja poslovnih podatkov, morajo organizacije svoje omrežje razčleniti na logične segmente, ki preprečujejo dostop do celotnega omrežja. Omrežje se tako lahko razčleni glede na funkcijo (npr. finance, marketing, inženiring, prodaja, podpora, proizvodnja ipd), glede na nivo varnosti (npr. neuvrščeno, zaupno, strogo zaupno ipd.) ter glede na geografsko lokacijo (v primeru podružnic, večih poslovnih stavb ipd.). Vsak segment mora biti zaščiten s požarnim zidom, ki neavtoriziranim sistemom preprečuje neželen dostop. Tako npr. naprave v marketinškem omrežju ne smejo imeti neposrednega dostopa do omrežja inženirjev, naprave iz omrežja inženiringa ne smejo imeti neposrednega dostopa do omrežja financ itd., razen v primeru obstoja tehtnih poslovnih razlogov. Odsotnost omrežnih segmentov namreč omogoča, da lahko vsakdo, ki ima dostop do le-tega, dostopa do vseh podatkov v omrežju. V primeru kibernetskega napada bi omrežje, ki ni razčlenjeno na segmente, izvajalcem napada omogočilo neoviran dostop do celotne informacijske infrastrukture organizacije. Hkrati segmentacija omrežja otežuje oz. preprečuje zaposlenim dostop do podatkov do katerih nimajo avtoriziranega dostopa (Trend Micro, 2013a), kar je prav tako pomembno z vidika varovanja poslovnih skrivnosti in kritičnih informacij organizacije.
Jeun, Lee in Won (2012) menijo, da je za preprečevanje okužb z zlonamerno programsko opremo s spleta ter za preprečevanje uhajanja notranjih informacij priporočeno tudi (fizično) ločevanje notranjega omrežja organizacije od spletnega omrežja.

3.2.2 Dnevniki beleženja (logging)

Ključno metodo za zaznavanje in posledično preprečevanje kibernetskih napadov na organizacije predstavlja beleženje, aktivno spremljanje in analiza dnevnikov aktivnosti omrežnega prometa. Beleženje, aktivno spremljanje in analiza prometa podatkov v omrežju, poleg zaznavanja virov v sistemu, zmanjšujejo možnosti za uspešno izvedbo kibernetskega napada ter v primeru le-tega omogočajo, da strokovnjaki s področja informacijske varnosti ugotovijo, kateri del omrežja je bil ogrožen ter katere podatke je napadalec v omrežju iskal (Jeun et al., 2012; Trend Micro, 2013a). Dnevniki beleženja hkrati omogočajo hitrejši postopek preiskave v primeru kibernetskega napada ter posledično nižajo stroške sanacije.

3.2.3 Uporabniški računi in delovne postaje

Večina uporabnikov želi dostopati do vseh podatkov; želijo imeti možnost, da lahko gredo kamorkoli in od tam dostopajo do vseh podatkov. Ker ima večina teh uporabnikov osebni računalnik tudi doma, svoje delo s kritičnimi podaki opravljajo na domačem računalniku, kar pa ne predstavlja varnega korporativnega okolja (Trend Micro, 2013a: 11; Gartner, 2012). Organizacije bi si zato morale prizadevati, da ima posamezen uporabniški račun v osnovi kar najmanj dostopnih pravic in da se do kritičnih podatkov lahko dostopa samo s sprotnim omogočanjem dostopa. Vse to pomeni precej več dela za oddelke informacijske tehnologije (v nadaljevanju IT), zato morajo organizacije pretehtati med dodatnim delom in stroški, ki jih takšna praksa prinese s sabo in potencialno izgubo kritično pomembnih podatkov (Trend Micro, 2013a: 11).

Uporabniški računi naj bi tako delovali s kar najmanj dostopnimi pravicami, zaščiteni pa naj bi bili z varnimi gesli (Trend Micro, 2013a; Jeun, et al., 2012; Gartner, 2012). Pri Trend Micro (2013a) priporočajo uporabo dvofaktorskega overjanja. Uporabniška gesla naj bi se redno menjavala, hkrati pa naj bi bila preprečena uporaba enakih gesel za dostope do različnih uporabniških računov. IT oddelek bi moral posamezna gesla preverjati z orodji za dešifriranje gesel in vsako uspešno dešifrirano geslo takoj zamenjati. Lokalni administratorski računi bi morali biti ukinjeni, dostopni podatki za ostale uporabniške račune pa se ne bi smeli shranjevati v predpomnilnik. Z administratorskimi pravicami naj bi se na posamezen računalnik v mreži dostopalo oddaljeno (Trend Micro, 2013a: 12).

Po končanem delu naj bi se delovna postaja ugasnila oz. ponovno zagnala, politika gesel naj poskrbi, da se uporabniški račun zaklene po nekaj napačnih vnosih gesla – za reaktivacijo gesla pa poskrbi IT oddelek. Vsaka delovna postaja bi morala biti zaklenjena, z vsemi nameščenimi posodobitvami za programsko opremo in s stalno omogočenim administratorskim popolnim dostopom na daljavo. Implementirana varnostna programska oprema, ki omogoča centralni nadzor, redno pregledovanje posameznega računalnika ter zbiranje, pošiljanje in pregledovanje dnevnikov beleženja močno olajša upravljanje z vsemi tveganji in pristojnim oddelkom omogoča učinovito odzivanje za nastale težave (Trend Micro, 2013a: 12).

3.3 Varovanje podatkov

Eden bistvenih motivov izvajalcev APT napadov je iskanje pomembnih podatkov organizacije z namenom njihove kraje ali poškodovanja. Shranjevanje in upravljanje vseh podatkov v centraliziranem, slabo (informacijsko) zaščitenem mestu izvajalcem kibernetskih napadov omogoča hitrejšo in uspešnejšo izvedbo kraje podatkov. Dalj časa kot bo izvajalec napada iskal podatke v omrežju napadene organizacije, več časa in možnosti bo organizacija imela za zaznavo in odkritje napadalčevih aktivnosti (Trend Micro, 2013a), kar bo organizaciji omogočilo učinkovitejši odziv na grožnjo.

3.3.1 Segmentacija podatkov

Glede na to, da niso vsi podatki ustvarjeni na enak način, da nimajo enakih vrednosti ter, da niso vsi podatki ključnega pomena za uspeh organizacije, mora vsaka poslovna enota organizacije ugotoviti, kateri podatki so tisti, katerih kraja in razkritje bi povzročilo največ škode in ogrozilo obstoj ter konkurenčnost organizacije. Te (kritične) podatke je potrebno obravnavati drugače kot običajne, vsakodnevne podatke in dokumente, ki za organizacijo nimajo pomembne teže in vrednosti. Občutljivi podatki npr. ne smejo biti na voljo za prenos na delovno postajo in morajo biti dostopni samo na datotečnem strežniku, do katerega lahko dostopajo le uporabniki s t.i. priviligiranim dostopom. Prav tako morajo biti občutljivi podatki tudi dodatno zaščiteni s kompleksnim šifriranjem, ki napadalcu v primeru poizkusa kraje onemogoči ali vsaj močno oteži dostop. Prav tako morajo biti, ločeno od sistema organizacije, šifrirani vsi občutljivi podatki, ki se jih pošilja preko elektronske pošte (Trend Micro, 2013a). Pri Trend Micro (2013a) poudarjajo, da je potrebno zaščititi tudi posamezne dele kritičnih informacij, saj s tem izvajalcu napada močno otežimo dostop do vseh ključnih podatkov. Tako bi npr. farmacevtsko podjetje moralo nekatere dele informacij (npr. recepture) razčleniti in razpršiti po svojem informacijskem okolju, s čimer se zagotovi, da s krajo enega dela informacije napadalec ne dobi dostopa do celotne informacije (v našem primeru celotne recepture). Vendar pa je potrebno poudariti, da v primeru, ko ima izvajalec napada možnost pregledati celotno informacijsko okolje organizacije, lahko s časoma pridobi vse dele informacije in jih združi ter tako pridobi celotno informacijo (v našem primeru formulo in proces izdelave).

3.3.2 Infrastruktura za varovanje podatkov

Kot že omenjeno, zahtevajo različne vrste podatkov različne ravni zaščite. Podatki, ki zahtevajo najvišjo raven zaščite se lahko hranijo na ločenem omrežju, ki ni povezano s svetovnim spletom, kar pomeni, da je do teh podatkov možno dostopati le fizično (Jeun et al., 2012; Trend Micro, 2013a). Podatki, ki zahtevajo nekoliko nižjo, a še vedno visoko raven zaščite so lahko shranjeni na varnem strežniku, do katerega se lahko dostopa na podlagi dvofaktorskega overjanja. Varni strežnik ne bi smel sprejemati dostopa z gesli, ki so bila shranjena v predpomnilniku, niti ne bi smel dovoliti, da se shranjene podatke odstrani iz strežnika. Za učinkovito zaščito podatkov shranjenih na varnem strežniku je potrebno predvsem skrbno spremljati dnevnik dostopa do strežnika. Podatki, ki ne potrebujejo visoke ravni zaščite so lahko shranjeni na rednem datotečnem strežniku, vendar pa so lahko na tem strežniku shranjeni le podatki, ki v primeru kraje organizaciji ne povzročijo večje škode (Trend Micro, 2013a).

3.4 Priporočila

Za učinkovito zoperstavljanje APT grožnjam je potrebna t.i. »poglobljena obrambna strategija« (ang. defense-in-depth strategy), sestavljena iz večplastnih zaščitnih ukrepov, ki se medsebojno prekrivajo in podpirajo. Celotna strategija temelji na naslednjih taktičnih korakih, ki morajo biti implementirani v vsako plast: zaznati, preprečiti, odzvati se in eliminirati. Večplastni zaščitni ukrepi so sestavljeni iz požarnega zidu, antivirusne zaščite, sistema za preprečevanje vdorov, požarnega zidu za spletne aplikacije, spletne zaščite in zaščite elektronske pošte, sistema za odkrivanje botnet-ov, kontrole upravljanja (ang. command & control) ipd. (Sophos, 2014). Naj poudarimo, da je omenjene varnostne rešitve potrebno redno posodabljati in nadgrajevati, saj bodo le tako lahko učinkovito sledile svojemu namenu.

Elementi dobre prakse, ki so primerni in uspešni pri preprečevanju APT na vseh plasteh (t.j. omrežje elektronska pošta, splet in končni uporabnik), vsebujejo (Gartner, 2012: 9-10):

- Uporabo najnovejše varnostne zaščite in sprotno posodabljanje le-te.
- Ocenjevanje varnostnih zmožnosti ponudnika varnostne platforme, ki jo organizacija uporablja in zamenjava ponudnika storitev, v kolikor ne zadošča varnostnim potrebam in zahtevam organizacije.
- Uporabo orodij, ki omogočajo spremljanje, prepoznavo ugleda in filtriranje IP, URL in e-mail naslovov. Tovrstnih orodij se je potrebno posluževati tudi pri uporabi oblačnih storitev.
- Uporabo orodij za preprečevanje izgube podatkov.
- Uporabo orodij SIEM (ang. Security Information and Event Management), ki omogočajo nadzor in spremljanje uporabnikov, dostop do podatkov in drugih virov organizacije, ter poročanje o zaznanih tveganjih.

APT in njihove tehnike se hitro spreminjajo in postajajo vse bolj dovršene, kar močno otežuje spremljanje dogajanja na tem področju ter s tem otežuje tudi boj proti tej problematiki. Še nikoli ni bilo redno izobraževanje in usposabljanje odgovornih za informacijsko varnost v organizaciji tako pomembno.

APT pogosto ciljajo končne uporabnike s pomočjo socialnega inženiringa, ki so pogostokrat zelo učinkoviti, saj so ciljani na podlagi informacij, ki jih napadalec zbere na družbenih omrežjih, spletnih straneh ciljne organizacije ali drugače. Še več, obstaja velika verjetnost, da bo napadalec preko prosto dostopnih podatkov poizkušal sestaviti večjo sliko v smislu organizacijske strukture, vlog zaposlenih ipd. Zato je izrednega pomena, da organizacije sprejmejo ustrezne ukrepe za ustrezno obravnavanje in obvladovanje socialnega inženiringa. Ti ukrepi so lahko v obliki predpisov ali določitvenih členov v pogodbah zaposlenih, lahko pa se zaposlene osvešča tudi s tem, da se jim nazorno pokaže, kako lahko napadalci pridejo do zaupnih podatkov (Gartner, 2012).

4 RAZPRAVA

Izvajalce APT napadov zanima širok spekter informacij; vse od vojaških obrambnih načrtov in strategij pa do načrtov za izdelavo igrač. Prav tako so zelo različni tudi motivi za izvajanje APT. Izvajalci tovrstnih napadov so lahko motivirani s finančnim dobičkom, s pridobivanjem konkurenčne prednosti na trgu, s sabotažo ali zgolj z namenom maščevanja. Zaradi zapisanega APT in ciljni napadi ne predstavljajo zgolj poslovnega oz. organizacijskega varnostnega problema, pač pa lahko predstavljajo tudi nacionalni varnostno-gospodarski problem. Uspešno izveden APT napad lahko namreč močno vpliva na finančno uspešnost in ugled organizacije, kot tudi države. Vidimo lahko, da so usmerjeni napadi in APT postali realnost sodobnega časa, ki organizacije silijo v učinkovito upravljanje in zoperstavljanje tovrstnim grožnjam.

Naj poudarimo, da ozaveščanje predstavlja prvi korak na poti do preprečevanja naprednih trajnih groženj in ciljnih napadov ter trdne organizacijske varnosti. Za zmanjševanje možnosti tovrstnih groženj in napadov je poleg ozaveščanja, potrebno tudi usposabljati in izobraževati zaposlene o potencialnem socialnem inženiringu, o vrednosti in shranjevanju zaupnih podatkov in o tem, kako kritične podatke učinkovito zaščititi. Glede na to, da globje kot se izvajalci napadov pomikajo v ciljno omrežje, težje je skrbnikom omrežja odkriti in ublažiti APT, lahko zaključimo, da je zgodnje odkrivanje APT ključno pri preprečevanju kraje ali nepooblaščenega spreminjanja zaupnih podatkov.

V pričujočem prispevku smo podali predloge in ukrepe za zaznavanje in upravljaje APT, vendar je na tem mestu potrebno poudariti, da izvajanje tovrstnih predlogov in ukrepov ne bo prispevalo k povečanju učinkovitosti in poenostavljanju delovnih procesov ter ne bo izboljšalo uporabniške izkušnje, bo pa povečalo stroške za zagotavljanje (informacijske) varnosti organizacije. Tovrstne stroške organizacije ne smejo smatrati kot nepotrebne, pač pa bi jih morale obravnavati kot »strošek poslovanja«, tako kot obravnavajo npr. zavarovanje, ki organizaciji ne predstavlja nobenih koristi (predstavlja le strošek), vse dokler se ne zgodi kaj slabega. Vodilo organizacij pri zagotavljanju poslovne varnosti (v najširšem smislu) naj bo, da koristi (dolgoročno gledano) prevladajo nad stroški in da je neželjene dogodke bolje preprečevati kot odpravljati njihove posledice, saj lahko le-te povzročijo velike finančne izgube in resno ogrozijo eksistenco organizacije. Tako naj organizacije pri zaznavanju in zoperstavljanju APT, kot tudi sicer pri zagotavljanju svoje organizacijske varnosti (v najširšem smislu), vzamejo v obzir star pregovor, ki pravi, da je bolje preprečevati kot zdraviti.

LITERATURA

Cisco. (2011). *Cisco 2Q11 Global Threat Report*. Pridobljeno na http://www.cisco.com/c/dam/en/us/products/collateral/security/cisco_global_threat_report_2q2011.pdf

Gartner. (2012). Best Practices for Mitigating Advanced Persistent Threats. Pridobljeno na http://www.trendmicro.de/media/wp/gartner-best-practices-for-mitigating-apts-whitepaper-en.pdf

GFI. (2009). *Targeted cyber attacks: The dangers faced by your corporate network*. Pridobljeno na http://www.gfi.com/whitepapers/cyber-attacks.pdf

Jeun, I., Lee, Y. in Won, D. (2012). A Practical Study on Advanced Persistent Threats. V T. Kim, A. Stoica, W. Fang, T. Vasilakos, J. Garcia Villalba, K. P. Arnett, M. Khurram Khan in B. Kang (ur.), *Computer Applications for Security, Control and System Engineering, International Conferences on Security technology* (str. 144-153). Berlin: Springer Berlin Heidelberg.

McAfee. (2011). *Combating Advanced Persistent Threats: How to prevent, detect, and remediate APTs*. Pridobljeno na http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf

Microsoft. (2012). *Determined Adversaries and Targeted Attacks: The threat from sophisticated, well-resourced attackers*. Pridobljeno na http://download.microsoft.com/download/9/3/6/93652DC7-7B93-4A88-87AC-933F7D4516EB/Determined%20Adversaries%20and%20Targeted%20Attacks_EN.docx

National Institute of Standerds and Technology. (2011*). Managing Information Security Risk: Organization, Mission, and Information System View*. Pridobljeno na http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Sophos. (2014). *Advanced Persistent Threats: Detection, Protection and Prevention*. Pridobljeno na http://i.crn.com/custom/Sophos_Advanced_Persistent_Threats.pdf

Symantec. (2011). *Advance Persistent Threats: A Symantec Prospective*. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

Symantec. (2012). *Interenet Security Threat Report: 2011 Trends*. Pridobljeno na http://www.dhses.ny.gov/ocs/resources/documents/Symantec-Internet-Threat-Report-Trends-for-2011-APR2012.pdf

Symantec. (2013a). *Internet Security Threat Report - Appendix: 2012 Trends*. Pridobljeno na https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v18_2012_221284438.en-us.pdf

Symantec. (2013b). *Internet Security Threat Report: 2012 Trends*. Pridobljeno na http://www.lsec.be/upload_directories/documents/Symantec/Symantec_InternetSecurityThreatReport2013_istr18_en.pdf

Symantec. (2014). *Internet Security Threat Report: 2013 Trends*. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S. in Lee, M. (2012). Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat. V D. Balzarotti, S. J. Stolfo in M. Cova (ur.), *Research in Attacks, Intrusions, and Defenses, 15th International Symposium* (str. 64-85). Berlin: Springer Berlin Heidelberg.

Trend Micro. (2012a). *Detecting the Enemy Inside the Network: How Touhg Is IT to Deal with APTs?* Pridobljeno na http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apt-primer.pdf

Trend Micro. (2012b). *Targeted Attack Entry Points: Are Your Bussiness Communications Secure?* Pridobljeno na http://www.trendmicro.com/cloud-content/us/pdfs/business/tlp_targeted_attack_entry_points.pdf

Trend Micro. (2013a). *Suggestions to Help Companies with the Fight Against Targeted Attacks*. Pridobljeno na http://www.trendmicro.com.ru/media/wp/suggestions-to-help-companies-with-the-fight-against-targeted-attacks-whitepaper-en.pdf

Trend Micro. (2013b). *Data Exfiltration: How Do Threat Actors Steal Your Data?* Pridobljeno na http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf

Trend Micro. (2013c). *Lateral Movement: How Do Threat Actors Move Deeper Into Your Network?* Pridobljeno na http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf