

ՏԵԽՆԻԿԱԿԱՆ ԱՌԱՋԱԴՐԱՆՔ

Նպատակային Հարձակումներից և «Zero day» -ի սպառնալիքներից պաշտպանական համակարգին ներկայացվող պահանջներ

1. Համակարգի լրակազմին ներկայացվող պահանջներ

Նպատակային Հարձակումներից և «Zero day» -ի սպառնալիքները պաշտպանական համակարգը պետք է ունենա մոդուլային կառուցվածք և կազմված լինի նույն արտադրողի՝ միմյանց հետ ինտեգրված ապարատա-ծրագրային համալիրից (ԱՕՀ): Այն պետք է ներառի հետևյալ ենթահամակարգերը.

- Օգտագործողի INTERNET հասանելիության մակարդակով պաշտպանելու համար՝ WEB կոնտենտի դինամիկ վերլուծության ենթահամակարգ
- Էլեկտրոնային փոստի մակարդակով պաշտպանելու համար էլեկտրոնային հաղորդագրությունների դինամիկ վերլուծության ենթահամակարգ
- Օգտագործողների աշխատանքային կայանների պաշտպանության ենթահամակարգ
- Կենտրոնացված կառավարման ենթահամակարգ

2. WEB կոնտենտի դինամիկ վերլուծության ենթահամակարգին ներկայացվող պահանջները

«Zero day» -ի սպառնալիքները արդյունավետ պաշտպանության համար տվյալ ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- Մուտքային մասում «թափանցիկ» («inline») ռեժիմ՝ սպառնալիքների հայտնաբերման (մոնիթորինգ) և շրջափակման հնարավորությամբ
- Թրաֆիկի կրկնօրինակների վերլուծության (SPAN, TAP) ռեժիմ՝ սպառնալիքների ավտոմատ հայտնաբերման և TCP-reset և UDP Unreachable փաթեթների ավտոմատ ուղարկման հնարավորությամբ
- («inline») ռեժիմում խափանումների նկատմամբ կայունությանը (отказоустойчивость) ներկայացվող պահանջները
 - Ներկառուցված «bypass» մոդուլի առկայություն՝ ապարատային և/կամ ծրագրային խափանումների դեպքում (fail-open) սարքի միջոցով ցանցային անընդհատ հասանելիության ապահովման համար
 - Կառավարման ինտերֆեյսի կարգաբերումներում «bypass»-ի ստիպողական միացման հնարավորություն
 - Ձեռքբերվող համակարգի լրակազմում չընդգրկված (կարող է ձեռք բերվել առանձին) արտաքին ակտիվ մոդուլի (active-fail-open) հետ (արտաքին «bypass») աշխատանքի ապահովման հնարավորություն
- Անկախ՝ օգտագործվող «TCP-port»-երից, առկա թրաֆիկում HTTP արձանագրության (protocol) նույնականացման և վերլուծման ապահովում
- Անկախ՝ օգտագործվող «TCP-port»-երից, առկա թրաֆիկում FTP և TFTP արձանագրությունների (protocol) նույնականացման և վերլուծման ապահովում
- Անկախ՝ օգտագործվող «TCP-port»-երից, առկա թրաֆիկում DNS արձանագրությունների(protocol) նույնականացման և վերլուծման ապահովում

- Լրակազմի մեջ չմտնող (հնարավոր է՝ լրացուցիչ ձեռք բերված) առանձին արտաքին ակտիվ մոդուլից եկող HTTPS և FTPS վերձանված ողջ թրաֆիկի՝ այլ ոչ թե առանձին ֆայլերի, վերլուծության ապահովում
- Պաշտպանության ֆունկցիոնալին ներկայացվող պահանջներ.
 - WEB հասանելիությամբ տարածվող «Zero day»-ի «exploit»-ների և վնասաբեր ծրագրային ապահովման ավտոմատ հայտնաբերում
 - Ցանցի ներսում տարածվող վնասաբեր օրինակների տարածման և տվյալների էքսֆիլտրացիայի ավտոմատ հայտնաբերում
 - Մոնիտորինգի ռեժիմում՝ «վարակված» համակարգիչներից կառավարման արտաքին սերվերներին (CommandandControl, C&C) միանալու փորձերի(ներառյալ նաև՝ HTTP և DNS հարցումները), ավտոմատ հայտնաբերում
 - «inline» ռեժիմում՝ «վարակված» համակարգիչներից կառավարման արտաքին սերվերներին (CommandandControl, C&C) միանալու փորձերի(ներառյալ նաև՝ HTTP և DNS հարցումները) ավտոմատ հայտնաբերում և կասեցում
 - Նախկինում հայտնաբերված սպառնալիքների կողմից կրկնակի վարակման փորձերի ավտոմատ կանխարգելում
 - Կրկնակի վարակման փորձերի և «CommandandControl, C&C»-ի ավտոմատ կանխարգելում՝ նույն ապարատա-ծրագրային համալիրի (ԱՕՀ) վրա հայտնաբերումից ոչ ուշ քան 5 (հինգ) վայրկյանի ընթացքում: Բանկի կորպորատիվ ցանցի APT սպառնալիքներից պաշտպանելու համակարգի մաս հանդիսացող այլ ենթահամակարգերի կողմից նախկինում անհայտ սպառնալիքները՝ հայտնաբերումից ոչ ուշ քան 5 (հինգ) րոպեի ընթացքում: Նախկինում անհայտ սպառնալիքները՝ այլ պատվիրատույի(ոչ Բանկի) համակարգերով հայտնաբերումից հետո ոչ ուշ քան 1 (մեկ) ժամվա ընթացքում
- Համակարգերի միջով անցնող ողջ WEB- կոնտենտի, ներառյալ՝ WEB կայքերը և ֆայլերը, ստատիկ և դինամիկ վերլուծությունը պետք է իրականացվի լոկալ անմիջականորեն ենթահամակարգերի վրա:
 - Արգելվում է ստուգման նպատակով, որևէ կոնտենտի ուղարկումը արտադրողի որևէ սերվերի
 - Արգելվում է կորպորատիվ ցանցում շրջանառվող ցանկացած տվյալների (ներքին փաստաթղթեր, օգտատերերի գրամուցումների տվյալներ, ներքին IP հասցեներ և այլն) ուղարկումը արտադրողի որևէ սերվերի
 - Թույլատրելի է՝ արտադրողի WEB կայքից թարմացումների ավտոմատ ներբեռնումը (IP- հասցեները և արձանագրությունները (protocols) պետք է տրվեն ստատիկ), լոկալ վերլուծության որակի բարձրացման նպատակով
 - Թույլատրելի է՝ պաշտպանվածության ընդհանուր մակարդակի բարձրացման և համակարգի կեղծ գործարկումների մակարդակի իջեցման նպատակով՝ տեղադրված Ապարատա-ծրագրային համալիրի(ԱՕՀ) կողմից լոկալ հայտնաբերված սպառնալիքների մասին արտադրողի սերվերներին ուղարկել չանհատականացված տվյալներ
- Նախկինում հայտնաբերված սպառնալիքների հայտնաբերման նպատակով Օգտագործողի ողջ INTERNET թրաֆիկի ստատիկ վերլուծության ապահովում(կրկնակի

վարկման և C&C բացառում) և դինամիկ վերլուծություն պահանջող նոր, կասկածելի WEB կոնտենտի նույնականացում

- Կասկածելի WEB-էջերի դինամիկ վերլուծություն (վիրտուալ միջավայրում WEB հասանելիության էմուլյացիա) և «zero day» ներդիրներ պարունակող WEB-էջերի նույնականացում՝ ոչ սիգնատուր մեթոդներով
- Սկզբնական HTTP-հարցման մեջ «User-Agent»-ի վերնագրի վերլուծության հիման վրա օգտագործողի աշխատակայանների բնութագրերին առավելապես բնորոշ օպերացիոն համակարգեր և կիրառական ծրագրեր պարունակող մեկ կամ մի քանի վիրտուալ մեքենաների ավտոմատ ընտրություն
- Կասկածելի ֆայլերի դինամիկ վերլուծություն (վիրտուալ միջավայրում կատարման էմուլյացիա), «zero day» և ներդիրներ (այդ թվում նաև rootkit) պարունակող ֆայլերի նույնականացում՝ ոչ սիգնատուր մեթոդներով
- 3GP, ASF, AVI, BAT, CHM, CMD, COM, CSV, DLL, DOC, DOCX, EXE, FLV, GIF, HLP, HTM, HWP, HWT, ICO, JAR, JPG, JS, LNK, MHT, MIDI, MOV, MP3, MP4, MPG, MSI, PDF, PNG, PPS, PPSX, PPT, PPTX, QT, RM, RMI, RTF, SWF, TIFF, VBS, VCF, VCS, WAV, WMA, WSF, XLS, XLSX, XML և այլն ֆորմատներով ֆայլերի դինամիկ (ոչ սիգնատուր մեթոդներով) վերլուծության ապահովում
- ZIP, GZ, RAR, 7Z, CAB, TNEFF և այլն ֆորմատի արխիվային ֆայլերի պարունակության դինամիկ վերլուծություն
- Դինամիկ և ստատիկ վերլուծությունների արդյունքների վրա հիմնված կշռված գնահատման միջոցով նոր «zero day» վնասաբեր ծրագրային ապահովում և ներդիրներ պարունակող ֆայլերի նույնականացում
- «zero day» վնասաբեր ծրագրային ապահովման և ներդիրների օգտագործմամբ բաղադրյալ հարձակումների հայտնաբերում
- Մեկ վիրտուալ մեքենայում օգտագործողի ներբեռնած (այդ թվում նաև՝ տարբեր հոսքերի (սեանսների) և տարբեր արտաքին աղբյուրներից ներբեռնված) ողջ WEB-կոնտենտի (այլ ոչ թե առանձին ֆայլերի) էմուլյացիա
- Ֆայլի կատարման էմուլյացիայի գործընթացում Օպերացիոն համակարգում իրադարձությունների վերահսկումը պետք է իրականացվի հիպերվիզորի (Կենտրոնական պրոցեսորի հրահանգների, համակարգային հարցումների, օպերատիվ հիշողության հասանելիության, ֆայլային համակարգին դիմումների) մակարդակով, այլ ոչ թե՝ վիրտուալ մեքենայի ներսում մոնիտորինգի նպատակով տեղադրված լրացուցիչ ծրագրային գործիքների, քանի որ դրանք կարող են հայտնաբերվել և անջատվել (շրջանցվել) վնասաբեր ծրագրային ապահովման կողմից:
- «sandbox»-ի շրջանցման փորձերի (VM-Evasion, Sandbox-Evasion) ավտոմատ հայտնաբերում և հակազդում, այդ թվում նաև՝ հետաձգված թողարկումները և «քնել»-ու (sleepcall) փորձերը: Ապարատա-ծրագրային համալիրը(UOZ) պետք է ի վիճակի լինի հետևել ու հայտնաբերել օպերացիոն համակարգին և ռեեստրի փոփոխություններին ուղղված հարցումները և ավտոմատ կերպով արագացնել էմուլյացիայի գործընթացը:
- Առանց օգտագործողի մասնակցության կամ INTERNET հասանելիության տրամադրման անհրաժեշտության, վիրտուալ մեքենայի պրոցեսների հետ փոխգործակցության համար՝ օգտագործողի (ստեղնաշարից մուտք, «մկնիկ»-ի շարժումներ և կոճակների

սեղմումներ) և ցանցային միջավայրի (DNS, HTTP, NTP սերվերներ) ակտիվության ավտոմատ էմուլյացիա:

- Կասկածելի ֆայլերի՝ տարբեր վերսիաներով օպերացիոն համակարգեր (ներառյալ՝ Microsoft Windows XP x32 (SP3), Windows 7 x32, x64 (ներառյալ՝ SP1-ը), Windows 10x64) ունեցող վիրտուալ մեքենաների վրա միաժամանակյա թողարկման ավտոմատ էմուլյացիա:
- Վրիտուալ մեքենաների վրա կասկածելի ֆայլերի ավտոմատ թողարկման էմուլյացիա՝ մի քանի (2 և ավելի) տարբերակների կիրառական ծրագրերի կիրառմամբ (այդ թվում՝ InternetExplorer, Java, MicrosoftWord, Excel, PowerPoint, AdobeReader, Flash, WindowsMediaPlayer, QuickTimePlayer, RealPlayer, VLCMediaPlayer, Windows-ի ստանդարտ հավելվածներ):
- Ֆայլերի դինամիկ վերլուծության ընթացքում օգտագործողի աշխատանքային էկրանի (Desktop) պարունակության ավտոմատ տեսագրման հնարավորություն:
- Ենթահամակարգը չպետք է էական ուշացումներ (ոչ ավել քան 100 միլիվայրկյան) մտցնի Օգտագործողների՝ WEB- հասանելիության ընթացքում:
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և առնվազն SSHv2 արձանագրություններով:
- Հայտնաբերված սպառնալիքների վիճակագրության, վերլուծվող թրաֆիկի քանակի և ապարատա-ծրագրային համալիրի (ՄՕՀ) հաշվողական ռեսուրսների ծանրաբեռնվածության մասին տվյալների ներկայացման համար ապարատա-ծրագրային համալիրի (ՄՕՀ) կառավարման ինտերֆեյսը պետք է տրամադրի վիզուալացման միջոցներ (Dashboard):
- Հայտնաբերված սպառնալիքների (էքսպլոիթների, վնասաբեր ծրագրային ապահովման, C&C) և հայտնաբերված պոտենցիալ անցանկալի ծրագրային ապահովման մասին տեղեկատվությունը կառավարման ինտերֆեյսը պետք է տրամադրի տարանջատված ձևով:
- Կառավարման ինտերֆեյսը պետք է տրամադրի հնարավորություն՝ հայտնաբերված սպառնալիքների մասին իրադարձությունների մատյաններում(Log) փնտրման, դասավորման և ֆիլտրման համար, ներառյալ՝ ըստ սպառնալիքի տիպի, SMTP վերնագիրի, աշխատակայանների (IP հասցեներ):
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ բոլոր (ստուգված փոխանցված, կարանտին տեղակայված, մշակման, ուղարկման հերթերում գտնվող) էլեկտրոնային նամակների փնտրման (ըստ SMTP վերնագիրի, արտացոլված կարգավիճակի և նամակի ստուգման արդյունքի), նրանց պարունակության դիտման, ինչպես նաև նամակն ամբողջությամբ արտահանելու հնարավորություն:
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ կարանտին և ստուգման հերթերում տեղակայված էլեկտրոնային նամակների դիտարկման և ադմինիստրատորի հարցումով ազատման հնարավորություն:
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ մանրամասն տեղեկություններ հայտնաբերված սպառնալիքի, ներառյալ՝ MD5/SHA1 ֆայլերի մասին, WEB-հղումները, սկզբնաղբյուրի և վերջնակետի IP-ները, դինամիկ վերլուծության ընթացքում յուրաքանչյուր վիրտուալ մեքենայի օպերացիոն համակարգում և ցանցային

ակտիվության հայտնաբերված բոլոր փոփոխությունները քրոնոլոգիական հերթականությամբ (ներառյալ՝ անհաջող փորձերը) ինչպես նաև՝ պրոցեսների (ներառյալ կողի ներարկումները և DLL-ների օգտագործումը), ֆայլային օպերացիաները, Windows-ի ռեեստրի փոփոխությունները, համակարգային հարցումները՝ օպերացիոն համակարգին դիմումները (API calls), ստեղծված mutex-ները, DNS հարցումները, HTTP, ցանցային միացումների packet capture (PCAP), վիրտուալ մեքենայի աշխատանքային սեղանի տեսագրության ֆայլերին հասանելիության հղումները:

- Կառավարման ինտերֆեյսը պետք է տրամադրի հնարավորություն՝ PDF ձևաչափով արտահանել ստատիկ և դինամիկ վերլուծությունների արդյունքների մանրամասն հաշվետվությունները, գրաֆիկական պատկերներ, հայտնաբերված սպառնալիքների վիճակագրությունը և տրված ժամանակահատվածի համար(օր, շաբաթ, ամիս) ընդհանրացված հաշվետվությունները:
- Կառավարման ինտերֆեյսը պետք է տրամադրի հայտնաբերված վնասաբեր ֆայլերի անվտանգ արտահանման հնարավորություն՝ անհրաժեշտության դեպքում այլ փորձագետների կողմից հետագա վերլուծման համար:
- Իրադարձությունների մասին RSyslog, HTTP, SMTP, SNMP (XML կամ JSON ձևաչափերով) արձանագրություններով ծանուցումների ուղարկման աջակցություն՝ մոնիթորինգի և SIEM համակարգերի հետ ինտեգրման համար:

3. Էլեկտրոնային հաղորդագրությունների դինամիկ վերլուծության ենթահամակարգին ներկայացվող պահանջները

Նպատակային Հարձակումներից և «Zero day» -ի սպառնալիքները արդյունավետ պաշտպանության համար, ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- SMTP և SMTPS (SMTP over SSL) արձանագրություններով աշխատանքի ապահովում:
- Ֆիշինգային հարձակումների և նոր, անհայտ վնասաբեր ծրագրերի օգտագործմամբ աշխատակայանների վարկաբեկման փորձերի ոչ միայն հայտնաբերման, այլև՝ կանխարգելման նպատակով փոստային շյուզի (MTA (MailTransferAgent)) ռեժիմում աշխատանքի ապահովում:
- Ստուգվող մուտքային էլեկտրոնային հաղորդագրությունների ընդունման ժամանակավոր հետաձգման (ստուգման ընթացքում) և հայտնաբերված վնասաբեր հաղորդագրությունների կարանտին ուղարկման ապահովում: Ստուգումն անցած մյուս հաղորդագրությունների էլեկտրոնային կորպորատիվ փոստային սերվերներին ուղարկման ապահովում՝ վերջիններիս համապատասխան ցանցային անունների (DNS –ի MX և A գրառումներ) օգտագործմամբ և մի քանի արտաքին կորպորատիվ փոստային սերվերների միջև ծանրաբեռնվածության ավտոմատ բաշխմամբ:
- Ստուգված մուտքային հաղորդագրությունների վերահասցեագրում տարբեր կորպորատիվ դոմեյններում գտնվող առանձին փոստային սերվերներում:
- Էլեկտրոնային փոստով ստացված հաղորդագրության շրջափակման և շրջափակման պատճառների մասին օգտագործողին և անվտանգության ադմինիստրատորին ավտոմատ հաղորդագրության ուղարկում: Հաղորդագրության տեքստի փոփոխության հնարավորություն:

• Ապարատա-ծրագրային համալիրի (ԱՕՀ) միջով անցնող ողջ կոնտենտի, ներառյալ՝ էլեկտրոնային նամակները, WEB-հղումները և ներդրված ֆայլերը, ստատիկ և դինամիկ վերլուծությունը պետք է իրականացվի լոկալ՝ անմիջականորեն Ապարատա-ծրագրային համալիրի (ԱՕՀ) վրա.

- Արգելվում է՝ ստուգման նպատակով, որևէ կոնտենտի ուղարկումը արտադրողի որևէ սերվերի:
- Արգելվում է՝ կորպորատիվ ցանցում շրջանառվող ցանկացած տվյալների (ներքին փաստաթղթեր, օգտատերերի գրամուցումների տվյալներ, ներքին IP հացեներ և այլն) ուղարկումը արտադրողի որևէ սերվերի:
- Թույլատրելի է՝ արտադրողի WEB-կայքից թարմացումների ավտոմատ ներբեռնումը(IP-հասցեները և արձանագրությունները (protocols) պետք է տրվեն ստատիկ), լոկալ վերլուծության որակի բարձրացման նպատակով:
- Թույլատրելի է՝ պաշտպանվածության ընդհանուր մակարդակի բարձրացման և համակարգի կեղծ գործարկումների մակարդակի իջեցման նպատակով՝ տեղադրված Ապարատա-ծրագրային համալիրի(ԱՕՀ) կողմից լոկալ հայտնաբերված սպառնալիքների մասին արտադրողի սերվերներին ուղարկել չանհատականացված տվյալներ:
- Էլեկտրոնային հաղորդագրությունների պարունակության, նրանցում առկա ներդիրներում (attached file) և WEB հղումներում՝ հայտնի սպառնալիքների առկայության մասով ստատիկ վերլուծության և կասեցման ապահովում:
- 3GP, ASF, AVI, BAT, CHM, CMD, COM, CSV, DLL, DOC, DOCX, EXE, FLV, GIF, HLP, HTM, HWP, HWT, ICO, JAR, JPG, JS, LNK, MHT, MIDI, MOV, MP3, MP4, MPG, MSI, PDF, PNG, PPS, PPSX, PPT, PPTX, QT, RM, RMI, RTF, SWF, TIFF, VBS, VCF, VCS, WAV, WMA, WSF, XLS, XLSX, XML և այլն ֆորմատներով ֆայլերի դինամիկ (ոչ սիգնատուր մեթոդներով) վերլուծության ապահովում:
- ZIP, GZ, RAR, 7Z, CAB, TNEFF և այլն ֆորմատի արխիվային ֆայլերի պարունակության դինամիկ վերլուծություն:
- Գաղտնաբառով պաշտպանված արխիվների պարունակության ստուգման ապահովում՝ հենց հաղորդագրության մեջ գաղտնաբառերի ավտոմատ փնտրելու միջոցով (առանց նախնական կարգաբերման անհրաժեշտության):
- Էլեկտրոնային հաղորդագրության «մարմնում» (body), վերնագրում և կցված փաստաթղթում առկա WEB-հղումների(URL) սինտակսիսի վերլուծման ապահովում, նշված հղումներով INTERNET-ից ֆայլերի ավտոմատ ներբեռնում՝առանձնացված ցանցային թրաֆիկի օգտագործմամբ և ներբեռնված ֆայլի դինամիկ վերլուծություն:
- Ֆայլի կատարման էմուլյացիայի գործընթացում Օպերացիոն համակարգում իրադարձությունների վերահսկումը պետք է իրականացվի հիպերվիզորի(Կենտրոնական պրոցեսորի հրահանգների, համակարգային հարցումների, օպերատիվ հիշողության հասանելիության, ֆայլային համակարգին դիմումների) մակարդակով, այլ ոչ թե՛ վիրտուալ մեքենայի ներսում մոնիտորինգի նպատակով տեղադրված լրացուցիչ ծրագրային գործիքների, քանի որ դրանք կարող են հայտնաբերվել և անջատվել(շրջանցվել) վնասաբեր ծրագրային ապահովման կողմից:

- «sandbox»-ի շրջանցման փորձերի (VM-Evasion, Sandbox-Evasion) ավտոմատ հայտնաբերում և հակազդում, այդ թվում նաև՝ հետաձգված թողարկումները և «քնելու» (sleepcall) փորձերը: Ապարատա-ծրագրային համալիրը (ԱՕՀ) պետք է ի վիճակի լինի հետևել ու հայտնաբերել օպերացիոն համակարգին և ռեեստրի փոփոխություններին ուղղված հարցումները և ավտոմատ կերպով արագացնել էմուլյացիայի գործընթացը:
- Առանց օգտագործողի մասնակցության կամ INTERNET հասանելիության տրամադրման անհրաժեշտության, վիրտուալ մեքենայի պրոցեսների հետ փոխգործակցության համար՝ օգտագործողի(ստեղնաշարից մուտք, «մկնիկ»-ի շարժումներ և կոճակների սեղմումներ) և ցանցային միջավայրի (DNS, HTTP, NTP սերվերներ) ակտիվության ավտոմատ էմուլյացիա:
- Կասկածելի ֆայլերի՝ տարբեր վերսիաներով օպերացիոն համակարգեր(ներառյալ՝ Microsoft Windows XP x32 (SP3), Windows 7 x32, x64 (ներառյալ SP1), Windows 10x64) ունեցող վիրտուալ մեքենաների վրա միաժամանակյա թողարկման ավտոմատ էմուլյացիա:
- Վրիտուալ մեքենաների վրա կասկածելի ֆայլերի ավտոմատ թողարկման էմուլյացիա՝ մի քանի (2 և ավելի) վերսիաների կիրառական ծրագրերի կիրառմամբ (այդ թվում՝ InternetExplorer, Java, MicrosoftWord, Excel, PowerPoint, AdobeReader, Flash, WindowsMediaPlayer, QuickTimePlayer, RealPlayer, VLCMediaPlayer, Windows-ի ստանդարտ հավելվածներ):
- Ապարատա-ծրագրային համալիրի(ԱՕՀ) օգտագործումը չպետք է պահանջի լրացուցիչ լիցենզիաներ՝ «ընդունող» վիրտուալ մեքենաների օպերացիոն համակարգերի և կիրառական ծրագրերի համար:
- Ֆայլերի դինամիկ վերլուծության ընթացքում օգտագործողի աշխատանքային էկրանի (Desktop) պարունակության ավտոմատ տեսագրման հնարավորություն:
- Ստուգվող էլեկտրոնային հաղորդագրությունների մեծությունները պետք է հնարավոր լինի կարգաբերել Բանկի փոստային կորպորատիվ սերվերների նկատմամբ կիրառվող սահմանափակումներին համապատասխան և պետք է լինի ոչ պակաս 30ՄԳբ-ից:
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և առնվազն SSHv2 արձանագրություններով:
- Կառավարման ինտերֆեյսը պետք է տրամադրի հնարավորություն՝ հայտնաբերված սպառնալիքների մասին իրադարձությունների մատյաններում (Log) փնտրման, դասավորման և ֆիլտրման համար, ներառյալ՝ ըստ սպառնալիքի տիպի, SMTP վերնագիրի, աշխատակայանների (IP հասցեներ):
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ բոլոր(ստուգված փոխանցված, կարանտին տեղակայված, մշակման, ուղարկման հերթերում գտնվող) էլեկտրոնային նամակների փնտրման (ըստ SMTP վերնագիրի, արտացոլված կարգավիճակի և նամակի ստուգման արդյունքի), նրանց պարունակության դիտման, ինչպես նամակն ամբողջությամբ արտահանելու հնարավորություն:

- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ կարանտինի և այլ ստուգված էլեկտրոնային նամակների համար նախատեսված պահոցի չափերի կառավարման հնարավորություն:
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ կարանտին և ստուգման հերթերում տեղակայված էլեկտրոնային նամակների դիտարկման և ադմինիստրատորի հարցումով ազատման հնարավորություն:
- Կառավարման ինտերֆեյսը պետք է տրամադրի՝ մանրամասն տեղեկություններ հայտնաբերված սպառնալիքի, ներառյալ՝ MD5/SHA1 ֆայլերի մասին, WEB-հղումները, սկզբնաղբյուրի և վերջնակետի IP-ները, դինամիկ վերլուծության ընթացքում յուրաքանչյուր վիրտուալ մեքենայի օպերացիոն համակարգում և ցանցային ակտիվության հայտնաբերված բոլոր փոփոխությունները քրոնոլոգիական հերթականությամբ (ներառյալ՝ անհաջող փորձերը) ինչպես նաև՝ պրոցեսսների (ներառյալ կոդի ներարկումները և DLL-ների օգտագործումը), ֆայլային օպերացիաները, Windows-ի ռեեստրի փոփոխությունները, համակարգային հարցումները՝ օպերացիոն համակարգին դիմումները (APIcalls), ստեղծված mutex-ները, DNS հարցումները, HTTP, ցանցային միացումների packetcapture (PCAP), վիրտուալ մեքենայի աշխատանքային սեղանի տեսագրության ֆայլերին հասանելիության հղումները:
- Դինամիկ վերլուծության արդյունքների մանրամասն հաշվետվություններում պետք է տեսանելի ձևով առանձնացվեն հայտնաբերված վնասաբեր ակտիվության հայտանիշները՝ հաշվետվության վերլուծության պարզեցման և վարակվածության պոտենցիալ հայտանիշների (IndicatorsofCompromise, IoC) ցանկի կազմման համար:
- Կառավարման ինտերֆեյսը պետք է տրամադրի հնարավորություն՝ PDF ձևաչափով արտահանել ստատիկ և դինամիկ վերլուծությունների արդյունքների մանրամասն հաշվետվությունները, գրաֆիկական պատկերներ, հայտնաբերված սպառնալիքների վիճակագրությունը և տրված ժամանակահատվածի համար (օր, շաբաթ, ամիս) ընդհանրացված հաշվետվությունները:
- Կառավարման ինտերֆեյսը պետք է տրամադրի հայտնաբերված վնասաբեր ֆայլերի անվտանգ արտահանման հնարավորություն՝ անհրաժեշտության դեպքում այլ փորձագետների կողմից հետագա վերլուծման համար:
- Իրադարձությունների մասին RSyslog, HTTP, SMTP, SNMP (XML կամ JSON ձևաչափերով) արձանագրություններով ծանուցումների ուղարկման աջակցություն՝ մոնիթորինգի և SIEM համակարգերի հետ ինտեգրման համար:

4. Կառավարման կենտրոնացված համակարգին ներկայացվող պահանջներ

Նպատակային Հարձակումներից և «Zero day» -ի սպառնալիքները արդյունավետ պաշտպանության համար, ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և առնվազն SSHv2 արձանագրություններով:
- Կենտրոնացված կառավարման WEB-ինտերֆեյսից պետք է տրամադրվի հասանելիություն յուրաքանչյուր տիպի կառավարվող ենթաբաժիններին
- Կառավարվող յուրաքանչյուր տիպի համակարգերի համար, կառավարման ինտերֆեյսը պետք է տեսարտացոլման միջոցներ ապահովի՝ հայտնաբերված

սպառնալիքների վիճակագրության, վերլուծվող կոնտենտի քանակի և հաշվողական ռեսուրսների ծանրաբեռնվածության արտացոլման համար:

- Կառավարման ինտերֆեյսը պետք է ապահովի տարբեր պարամետրերի և ֆիլտրերի կիրառմամբ հաշվետվությունների ստեղծումը՝ ըստ հայտնաբերված սպառնալիքների:
- Syslog, HTTP, HTTPS (XML կամ JSON ձևաչափով) արձանագրություններով Log-երի ուղարկում՝ SIEM-ի հետ ինտեգրացիայի համար:
- Պետք է ապահովվի՝ ԱՕՀ-ի արտադրողի WEB-կայքից թարմացումների (սպառնալիքների նոր նկարագրություններ) ավտոմատ կենտրոնացված կիրառումը:

5. Օգտագործողների աշխատատեղերի պաշտպանության ենթահամակարգին ներկայացվող պահանջներ

Նպատակային Հարձակումներից և «Zero day» -ի սպառնալիքները արդյունավետ պաշտպանության համար, ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և առնվազն SSHv2 արձանագրություններով:
- Ենթահամակարգը պետք է տրամադրի մանրամասն հաշվետվություն՝ աշխատակայանում առկա կասկածելի ակտիվության մասին:
- Աշխատակայանում տեղակայված ազենտը պետք է ապահովի կենտրոնացված կառավարումը և կարգաբերումը, վիճակագրության հավաքագրումը և գրանցամատյաններից տվյալների հավաքագրումը:
- Ենթահամակարգը պետք է թույլատրի համակարգերի բոլոր հոսթերի ֆայլերում, ռեեստրի բանալիներում և համակարգի այլ կոմպոնենտներում իրականացնել IoC-ի առկայության և անվտանգության այլ համակարգերում և պարագծում հայտնաբերված սպառնալիքների փնտրում:
- Պետք է հնարավոր լինի աշխատակայանի պաշտպանության ենթահամակարգի ազենտը տեղադրել Windows 7, 8, 10, Windows Server 2008 (R2), 2012 (R2), 2016 (32 և 64-կարգանի տարբերակներ) օպերացիոն համակարգերի վրա:
- Ենթահամակարգը պետք է ունենա ծրագրային ինտերֆեյս (API) ավտոմատացման համար: