Նպատակային հարձակումներից և «Zero day» -ի սպառնալիքներց պաշտպանական համակարգին ներկայացվող տեխնիկական պահանջներ

1. Համակարգի լրակազմին ներկայացվող պահանջներ

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

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

2. ՎԵԲ կոնտենտի դինամիկ վերլուծության ենթահամակարգին ներկայացվող պահանջները

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

- Ենթահամակարգը պետք է իրագործված լինի ապարատա-ծրագրային համալիրի (ԱԾՀ) տեսքով;
- Ինտերֆեյսների աշխատանքի զույգ առ զույգ ապահովում հետևյալ ռեժիմներում և համադրությամբ.
    - Մուտքային մասում «թափանցիկ»(«inline») ռեժիմ՝ սպառնալիքների հայտնաբերման(մոնիթորինգ) և շրջափակման հնարավորությամբ;
- Թրաֆիկի կրկնօրինակների վերլուծության (SPAN, TAP) ռեժիմ՝ սպառնալիքների ավտոմատ հայտնաբերման և TCP-reset и 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 հասանելության ապահովման համար;
    - Կառավարման ինտերֆեյսի կարգաբերումներում «bypass»-ի ստիպողական միացման հնարավորություն;
    - Ջեռքբերվող համակարգի լրակազմում չընգրկված(կարող է ձեռքբերվել 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 ձեռքբերված) առանձին արտաքին ակտիվ մոդուլից եկող HTTPS և FTPS վերծանված ողջ թրաֆիկի՝ այլ ոչ թե առանձին ֆայլերի, վերլուծության ապահովում;
- Պաշտպանության ֆունկցիոնալին ներկայացվող պահանջներ.
    - ՎԵԲ հասանելիությամբ տարածվող «Zero day»-ի «exploit»–ների և վնասաբեր ծրագրային ապահովման ավտոմատ հայտնաբերում;
    - Ցանցի ներսում տարածվող վնասաբեր օրինակների տարածման և տվյալների էքսֆիլտրացիայի ավտոմատ հայտնաբերում;
    - Մոնիթորինգի ռեժիմում՝ «վարակված» համակարգիչներից կառավարման արտաքին սերվերներին (Command and Control, C&C) միանալու փորձերի(ներառյալ նաև՝ HTTP և DNS հարցումները), ավտոմատ հայտնաբերում;
    - «inline» ռեժիմում՝ «վարակված» համակարգիչներից կառավարման արտաքին սերվերներին (Command and Control, 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 (ԱԾՀ) վրա հայտնաբերումից ոչ ուշ քան 5(հինգ) վայրկյանի ընթացքում: Բանկի կորպորատիվ ցանցի APT սպառնալիքներից պաշտպանելու համակարգի մաս հանդիսացող այլ ենթահամակարգերի ապարատա-ծրագրային համալիրների(ԱԾՀ) կողմից նախկինում անհայտ սպառնալիքները՝ հայտնաբերումից ոչ ուշ քան 5(հինգ) րոպեի ընթացքում: Նախկինում անհայտ սպառնալիքները՝ այլ պատվիրատուի(ոչ Բանկի) համակարգերով հայտնաբերումից հետո ոչ ուշ քան 1(մեկ) ժամվա ընթացքում;
- Ապարատա-ծրագրային համալիրի(ԱԾՀ) միջով անցնող ողջ ՎԵԲ- կոնտենտի, ներառյալ՝ ՎԵԲ կայքերը և ֆայլերը, ստատիկ և դինամիկ վերլուծությունը պետք է իրականացվի լոկալ՝ անմիջականորեն Ապարատա-ծրագրային համալիրի(ԱԾՀ) վրա**:**
    - Արգելվում է՝ ստուգման նպատակով, որևէ կոնտենտի ուղարկումը արտադրողի որևէ սերվերի;
    - Արգելվում է՝ կորպորատիվ ցանցում շրջանառվող ցանկացած տվյալների(ներքին փաստաթղթեր, օգտատերերի գրանցումների տվյալներ, ներքին IP հասցեներ և այլն) ուղարկումը արտադրողի որևէ սերվերի;
    - Թույլատրելի է՝ արտադրողի ՎԵԲ-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(ԱԾՀ) կողմից լոկալ հայտնաբերված սպառնալիքների մասին արտադրողի սերվերներին ուղարկել չանհատականացված տվյալներ*;*
- Նախկինում հայտնաբերված սպառնալիքների հայտնաբերման նպատակով Օգտագործողի ողջ INTERNET թրաֆիկի ստատիկ վերլուծության ապահովում(կրկնակի վարակման և C&C բացառում) և դինամիկ վերլուծություն պահանջող նոր, կասկածելի ՎԵԲ կոնտենտի նույնականացում;
- Ուղարկվող ֆայլերի հեշերի ավտոմատ ստուգում VirusTotal բազայով;

- Կասկածելի ՎԵԲ-էջերի դինամիկ վերլուծություն (վիրտուալ միջավայրում ՎԵԲ հասանելիության էմուլյացիա) և «zero day» ներդիրներ պարունակող ՎԵԲ-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;
- Դինամիկ վերլուծության ժամանակ կոնտենտի վտանգավորության աստիճանի գնահատման համակարգի կշիռների ճշտգրտման նպատակով սեփական կանոնների ստեղծում՝ YARA կոնտենտային վերլուծության ալգորիթմական լեզվի օգնությամբ;
- Այլ մշակողների կողմից ստեղծված YARA կանոնների ներմուծման հնարավորություն;
- «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 ՎԵԲ-կոնտենտի (այլ ոչ թե առանձին ֆայլերի) էմուլյացիա;
- Նոր վնասաբեր ծրագրային ապահովման նույնականացում՝ անկախ չարամիտների կողմից օգտագործվող «փաթեթավորման» գործիքներից և կատարվելիք կոդը՝ պոտենցիալ զոհի կայան հասցնելու ընթացքում, քողարկելու մեթոդներից (այդ թվում նաև՝ գաղտնագրված կոդը մաս-մաս ուղարկելու դեպքերը);
- Դինամիկ վերլուծության ժամանակ վնասակար ծրագրային ապահովման կողմից հայտնաբերվելուց պաշտպանված «песочница»-ի համար սեփական մշակման (ոչ OEM) հիպերվիզորի (էմուլյացիայի/վիրտուալիզացիայի միջավայր) օգտագործում: Արգելվում է լայն տարածում գտած ազատ տարածվող և կոմերցիոն հիպերվիզորների՝ ներառյալ VMware, KVM, CitrixXen, VirtualBox օգտագործումը;
- 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(ԱԾՀ) 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) վերսիաների կիրառական ծրագրերի կիրառմամբ (այդ թվում՝ InternetExplorer, Java, MicrosoftWord, Excel, PowerPoint, AdobeReader, Flash, WindowsMediaPlayer, QuickTimePlayer, RealPlayer, VLCMediaPlayer, Windows-ի ստանդարտ հավելվածներ);
- Ապարատա-ծրագրային համալիրի (ԱԾՀ) օգտագործումը չպետք է պահանջի լրացուցիչ լիցենզիաներ՝ «ընդունող» վիրտուալ մեքենաների օպերացիոն համակարգերի և կիրառական ծրագրերի համար;
- «ընդունող» վիրտուալ մեքենաների՝ տեղադրման համար պատրաստ թարմացումները տրամադրվում են Ապարատա-ծրագրային համալիրի (ԱԾՀ) արտադրողի կողմի;
- Ֆայլերի դինամիկ վերլուծության ընթացքում օգտագործողի աշխատանքային էկրանի (desktop) պարունակության ավտոմատ տեսագրման հնարավորություն;
- Ապարատա-ծրագրային համալիրի (ԱԾՀ) արտադրողականությանը ներկայացվող պահանջներ.
    - Ենթահամակարգը չպետք է էական ուշացումներ(ոչ ավել քան 100 միլիվայրկյան) մտցնի Օգտագործողների՝ WEB- հասանելիության ընթացքում;
    - Յուրաքանչյուր WEB- էջի և ֆայլի դինամիկ վերլուծության տևողությունը չպետք է գերազանցի 10(տաս) րոպեն;
    - Կասկածելի ողջ WEB-կոնտենտի վերլուծության համար ենթահամակարգը պետք է օգտագործի՝ Ապարատա-ծրագրային համալիրի(ԱԾՀ) այլ ենթահամակարգերի հետ ընդհանրություն չունեցող սեփական առանձնացված ռեսուրսները;
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և SSHv2 արձանագրություններով;
- Հայտնաբերված սպառնալիքների վիճակագրության, վերլուծվող թրաֆիկի քանակի և ապարատա-ծրագրային համալիրի (ԱԾՀ) հաշվողական ռեսուրսների ծարաբեռնվածության մասին տվյալների ներկայացման համար ապարատա-ծրագրային համալիրի (ԱԾՀ) կառավարման ինտերֆեյսը պետք է տրամադրի վիզուալացման միջոցներ (средства визуализации);
- 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 վերնագրի, 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, ՎԵԲ-հղումները, սկզբնաղբյուրի և վերջնակետի IP-ները, դինամիկ վերլուծության ընթացքում յուրաքանչյուր վիրտուալ մեքենայի օպերացիոն համակարգում և ցանցային ակտիվության հայտնաբերված բոլոր փոփոխությունները ժամանակագրական հերթականությամբ (ներառյալ՝ անհաջող փորձերը) ինչպես նաև՝ պրոցեսսների(ներառյալ կողի 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 էկրանի (desktop) տեսագրության ֆայլերին հասանելիության հղումները;
- C&C և էքսփլոիդ պարունակող վնասաբեր ՎԵԲ-էջի հայտնաբերման դեպքում, կառավարման ինտերֆեյսը պետք է տրամադրի հասանելիություն կորպորատիվ ցանցի համապատասխան կայանի կողմից գեներացված PCAP-ի սկզբնական թրաֆիկին;
- 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 սպառնալիքներց արդյունավետ պաշտպանության համար, ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- Ենթահամակարգը պետք է իրականացված լինի որպես ապարատա- ծրագրային համալիր;
- Ապահովի SMTP և SMTPS (SMTP over SSL) արձանագրություններով աշխատանքը;
- Ֆիշինգային հարձակումների և նոր, անհայտ վնասաբեր ծրագրերի օգտագործմամբ աշխատակայանների կոմպրոմետացիայի փորձերի ոչ միայն հայտնաբերման, այլև՝ կանխարգելման նպատակով փոստային շլյուզի (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 (ԱԾՀ) միջով անցնող ողջ կոնտենտի, ներառյալ՝ էլեկտրոնային նամակները, ՎԵԲ-հղումները և ներդրված ֆայլերը, ստատիկ և դինամիկ վերլուծությունը պետք է իրականացվի լոկալ՝ անմիջականորեն Ապարատա-ծրագրային համալիրի (ԱԾՀ) վրա.
    - Արգելվում է՝ ստուգման նպատակով, որևէ կոնտենտի ուղարկումը արտադրողի որևէ սերվերի;
    - Արգելվում է՝ կորպորատիվ ցանցում շրջանառվող ցանկացած տվյալների (ներքին փաստաթղթեր, օգտատերերի գրանցումների տվյալներ, ներքին IP հասցեներ և այլն) ուղարկումը արտադրողի որևէ սերվերի;
    - Թույլատրելի է՝ արտադրողի ՎԵԲ-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 (ԱԾՀ) կողմից լոկալ հայտնաբերված սպառնալիքների մասին արտադրողի սերվերներին ուղարկել չանհատականացված տվյալներ;
- Էլեկտրոնային հաղորդագրությունների պարունակության, նրանցում առկա ներդիրներում (вложения) և ՎԵԲ հղումներում՝ հայտնի սպառնալիքների առկայության մասով ստատիկ վերլուծության և կասեցման ապահովում;
- VirusTotal բազայով ներդիրների (вложения) հեշերի ավտոմատ ստուգում;
- Կոնտենտային վերլուծության YARA ալգորիթմական լեզվի հետ աշխատանքի ապահովում՝ էլեկտրոնային հաղորդագրությունների պարունակության ստատիկ ստուգումների և կասեցման նպատակով սեփական կանոնների ստեղծման համար, ներառյալ նաև՝ դինամիկ վերլուծության ընթացքում, կոնտենտի վտանգավորության աստիճանի գնահատման կշիռների ճշտգրտումը և կասեցման հավանականության բարձրացումը մակրոս պարունակող ցանկացած փաստաթղթի համար, կատարվող ֆայլերի կասեցում;
- Այլ մշակողների կողմից ստեղծված YARA կանոնների ներմուծման հնարավորություն;
- 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՝ (անկախ «փաթեթավորման» տիպից) դինամիկ (ոչ սիգնատուր մեթոդներով) վերլուծության միջոցով (վիրտուալ միջավայրում

կատարման էմուլյացիայի միջոցով) նոր, անհայտ էքսփլոիտների (эксплойт) և «zero day» վնասաբեր ծրագրային ապահովման (այդ թվում նաև rootkit);
- 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 ՎԵԲ-հղումների (URL) սինտակսիսի վերլուծման ապահովում, նշված հղումներով INTERNET-ից ֆայլերի ավտոմատ ներբեռնում՝առանձնացված ցանցային թրաֆիկի օգտագործմամբ և ներբեռնված ֆայլի դինամիկ վերլուծություն;
- Դինամիկ վերլուծության ժամանակ վնասակար ծրագրային ապահովման կողմից հայտնաբերվելուց պաշտպանված «песочница»-ի համար սեփական մշակման (ոչ OEM) հիպերվիզորի(էմուլյացիայի/վիրտուալիզացիայի միջավայր) օգտագործում: Արգելվում է լայն տարածում գտած ազատ տարածվող և կոմերցիոն հիպերվիզորների՝ ներառյալ VMware, KVM, CitrixXen, VirtualBox օգտագործումը;
- 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 (ԱԾՀ) 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;
- Վիրտուալ 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 (ԱԾՀ) 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;
- Ապարատա-ծրագրային համալիրի (ԱԾՀ) արտադրողականությանը ներկայացվող պահանջներ.
  - Յուրաքանչյուր կասկածելի ֆայլի (WEB-հղումով ներբեռնած ֆայլ, փոստային հաղորդագրության ներդիր) դինամիկ վերլուծության տևողությունը չպետք է գերազանցի 10 (տաս) րոպեն;
  - Յուրաքանչյուր էլեկտրոնային հաղորդագրության՝ ստուգման հերթում գտնվելու ժամանակը չպետք է գերազանցի 30 րոպեն և պետք է կարգավորվի համապատասխան կարգաբերումով;
  - Կասկածելի ողջ կոնտենտի վերլուծության համար ենթահամակարգը պետք է օգտագործի՝ Ապարատա-ծրագրային համալիրի (ԱԾՀ) այլ ենթահամակարգերի հետ ընդհանրություն չունեցող սեփական առանձնացված ռեսուրսները;
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և SSHv2 արձանագրություններով;
- Հայտնաբերված սպառնալիքների վիճակագրության, վերլուծվող թրաֆիկի քանակի և ապարատա-ծրագրային համալիրի (ԱԾՀ) հաշվողական ռեսուրսների ծարաբեռնվածության մասին տվյալների ներկայացման համար ապարատա-ծրագրային համալիրի (ԱԾՀ) կառավարման ինտերֆեյսը պետք է տրամադրի տեսանելի գրաֆիկական միջոցներ(средства визуализации);
- 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, ՎԵԲ-հղումները, սկզբնաղբյուրի և վերջնակետի IP-ները, դինամիկ վերլուծության ընթացքում յուրաքանչյուր վիրտուալ մեքենայի օպերացիոն համակարգում և ցանցային ակտիվության հայտնաբերված բոլոր փոփոխությունները ժամանակագրական հերթականությամբ (ներառյալ՝ անհաջող փորձերը), ինչպես նաև՝ պրոցեսների (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 էկրանի (desktop) 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 (Indicators of Compromise, 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 սպառնալիքներց արդյունավետ պաշտպանության համար, ենթահամակարգին ներկայացվում են հետևյալ պահանջները.

- Ենթահամակարգը պետք է իրականացված լինի որպես ապարատա-ծրագրային համալիր (ԱԾՀ);
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և SSHv2 արձանագրություններով;
- Կենտրոնացված կառավարման համակարգի ՎԵԲ-ինտերֆեյսը պետք է ամբողջովին ունիֆիկացված լինի համակարգի կազմում գտնվող յուրաքանչյուր (ԱԾՀ)-ի լոկալ կառավարման համակարգերի ՎԵԲ-ինտերֆեյսների հետ;
- Կենտրոնացված կառավարման ՎԵԲ-ինտերֆեյսից պետք է տրամադրվի հասանելություն յուրաքանչյուր տիպի կառավարվող ԱԾՀ-ների ենթաբաժիններին՝ կառավարվող ԱԾՀ-ների ամբողջական ֆունկցիոնալի ապահովման պահանջների համաձայն;
- Պետք է ապահովի խմբային և անհատական կարգաբերումների կենտրոնացված կիրառում, այդ թվում նաև՝ ինտերֆեյսի աշխատանքի ռեժիմների, թարմացումների սերվերների, ազդարարման սերվիսների հետ համագործակցության և SIEM-ի հետ ինտեգրացիայի կարգաբեռումները;
- Կառավարվող յուրաքանչյուր տիպի ԱԾՀ-ների համար, կառավարման ինտերֆեյսը պետք է տեսարտացոլման միջոցներ ապահովի՝ հայտնաբերված սպառնալիքների վիճակագրության, վերլուծվող կոնտենտի քանակի և հաշվողական ռեսուրսների ծանրաբեռնվածության արտացոլման համար;
- Ենթահամակարգը պետք է ապահովի կառավարվող տարբեր ԱԾՀ–ներից ստացված լոգերի ավտոմատ կորելյացիա և ՎԵԲ-ինտերֆեյսում հիպերհղումների (hayperlink) կամ իկոնկաների արտացոլման միջոցով դրանց միջև անցումներն ապահովելու 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՝ ԱԾՀ-ի արտադրողի ՎԵԲ-կայքից թարմացումների (սպառնալիքների նոր նկարագրություններ) ավտոմատ կենտրոնացված կիրառումը;

- Պետք է ապահովի՝ պատվիրատուի կորպորատիվ ցանցում հայտնաբերված սպառնալիքների մասին տվյալների, ավտոմատ կենտրոնացված կերպով լոկալ տարածում և ՎԵԲ-թրաֆիկի դինամիկ վերլուծության ենթահամակարգում սպառնալիքների շրջափակման կանոնների թարմացում:

5. Օգտագործողների աշխատատեղերի պաշտպանության ենթահամակարգին ներկայացվող պահանջներ

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

- Ենթահամակարգը պետք է իրագործված լինի ապարատա-ծրագրային համալիրի (ԱԾՀ) տեսքով;
- Ենթահամակարգի կառավարումը պետք է իրականացվի HTTPS և SSHv2 արձանագրություններով;
- Ենթահամակարգը պետք է հայտնաբերի աշխատակայանի վարկաբեկման փորձերը՝ նախապես որոշված վարակման ազդանշաններով (IoC, Indicator of Compromise);
- Ենթահամակարգը պետք է տրամադրի մանրամասն հաշվետվություն՝ աշխատակայանում առկա կասկածելի ակտիվության մասին;
- Աշխատկայանում տեղակայված կլիենտական ծրագրային ապահովումը պետք է ապահովի ագենտի կենտրոնացված կառավարումը և կարգաբերումը, վիճակագրության հավաքագրումը և գրանցամատյաններից տվյալների հավաքագրումը, ինչպես նաև՝ թույլատրի կարգաբերել աշխատակայանի կենտրոնական պրոցեսորի օգտագործումը, օպերացիոն համակարգի փոփոխությունների մասին տվյալների պահոցի ծավալը և հնարավորություն ընձեռնի կասկածելի աշխատակայանը մեկուսացնել ցանցից՝ հետաքննության համար անհրաժեշտ հանգույցների միացման հնարավորությամբ;
- 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 ենքահամակարգի ագենտը տեղադրել Windows 7, 8, 10, Windows Server 2008, 2012, 2016 (32 և 64-կարգանի տարբերակներ) օպերացիոն համակարգերի վրա;
- Ենթահամակարգը պետք է ունենա ծրագրային ինտերֆեյս (API) ավտոմատացման համար;
- Ենթահամակարգը պետք է ապահովի SԱ պատահարների մասին տեղեկատվության հաղորդումը իրադարձությունների կորելացիոն արտաքին համակարգեր (SIEM):