tapmışdır.Doğru şəkildə aşkarlanmış şəbəkə təhlüksizliyi bir necə hissədən ibarətdir.Bunlara aid edə bilərik, firewallar,müdaxilənin üzə çıxma sistemlərindən vs xidmətlərdən istifadə edilir.Əvvəlcədən təhlükəsizlik halları üçün sistemlərin əldə edilməsi təhlükəsizlik halarını artırır.Təşkilatların əldə etdikləri məlumatların təhlükəsizliklərini minimum etmək üçün əlverişki protokollar və bir sıra təlimatlar lazımdır.Bundan əlavə şəbəkə təhlükəsizliyi zamanı istifadə edilən avadanlıqlarda şəbəkədə baş verə biləcək təhlükələri artıra bilir.Şəbəkəyə edilən hücumların qarşısını ən effektiv şəkildə necə azalda və hansı yollarla qarşısını ala bilərik.Şəbəkə yaradan yazaman ilk öncə güclü parollrdan istifadə etmək, müxtəlif simvollardan istifadə edərək şəbəkənin təhlükəsizliyini təmin edə bilərik.Effektiv şəbəkə təhlükəsizliyi sistemə qeyri-qanuni şəkildə daxil olan girişlərin qarşısını alır və şəbəkədə mövcut olan məlumatları qoruyur.

**Ədəbiyyat**


[1] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paperon Network Security and Cryptography." Advances in Computational Sciences and Technology, vol. 10 (5), pp. 763-770, 2017.

[2] R. Khan, and M. Hasan, "Network threats, attacks and security measures: A review." International Journal of Advanced Research in Computer Science, vol. 8 (8), pp. 116-120, 2017.

[3] ]A. Tayal, N. Mishra, and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey." International Journal of Electronics and Information Engineering, vol. 6 (1), pp. 49-59, 2017.

[4] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions." Informationsciences, vol. 421pp. 43-69, 2017.

[5] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements." IEEE access, vol. 5pp. 1872-1899, 2017.

[6] D. Barrera, I. Molloy, and H. Huang "Standardizing IoT network security policy enforcement," In: Workshop on Decentralized IoT Security and Standards (DISS). p 6, 2018.

[7] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani, "An enhanced WLAN security system with FPGA implementation for multimediaapplications." IEEE Systems Journal, vol. 11 (4), pp. 2536-2545, 2015.

[8] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan "Security vulnerabilities attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," In: 2017 International Conference on Signal Processing and Communication (ICSPC). IEEE, pp. 288-293, 2017.

[9] S. Zheng, Z. Li, and B. Li "Implementation and application of ACL in campus network," In: AIP Conference Proceedings. vol 1. AIP Publishing LLC, p 090014, 2017.

[10] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik "Network Layers Threats & its Countermeasures in WSNs," In: 2019 International Conference on Computing, Communication, and Intelligent Systems(ICCCIS). IEEE, pp. 156-163, 2019.


## ZƏRƏRLİ PROQRAM VASİTƏLƏRİ


**Seyidsoylu Sevil**

**Azərbaycan Dövlər Neft Və Sənaye Universiteti**



**Xülasə**

Məqalənin əsası zərərli proqramlar və onların təhlili təşkil edir.Təhlil üsullarından istifadə etməklə proqramı baş verəcək təhlükələrdən qorunma məsələlərinini əhatə edir.Burada əsas məqsədlərdən biri odur ki, kompüterin və yaxud faylın hakerlər tərəfindən hücumuna məruz qalmağının qarşısını almaqdır.Həmçinin məqalədə zərərli proqramları təhlil olunaraq,ən əlverişli üsullarla qorunmaqdan da bəhs olunur.



**Açar sözlər**-Zərərli proqram, zərərli proqramların aşkarlanması, təhlili, yoluxmanın qarşısının alınması, spyware,təhlil alətləri.


**Giriş**

Müasir dövrdə zərərli proqramların sayı daha da inkişaf edir.Müəyyən metodlardan istifadə etməklə bu cür təhlükələrdən qoruna bilərik.Əks halda daha böyük fəsadlara səbəb olacaqdır,faylların öz-özünə çoxalması,reklamların görsənməsi,kompüterdə ləngimələrin baş verməsi,hətta kompüterin idarəolunması hakerlərin nəzarəti altına keçə bilər.Bu tip təhlükələrdən qorunmaq üçün kompüterdə daima antivirus proqramlarını aktiv saxlamalıyıq,həmçinin zərərli proqramlar haqqında məlumatımız olmalıdır.Bu məqalədə zərərli proqramın tipləri,onlardan qorunma üsulları,aşkar olunması,həmçinin təhlili haqqında geniş müzakirə edəcik.

**Məqsəd**

Bu məqalədə əsas məqsəd qarşıya çıxmış zərərli proqramın tipini müəyyən etmək və təhlükəsizlik üçün tədbirlərin görülməsidir.Lakin günümüzdə inkişaf edən bu tip təhlükələrin sayı artmaqdadır.Təhlükəyə davamlı ola biləcək addımlar seçməklə məlumatların yayılması və təhlükələrin daha çox yayılmasının qarşısını ala bilərik.

**Metod**

**Zərərli proqram**. Zərərli proqram-kompüter daxilində mövcud olan məlumatların oğurlanması,kompüter sistemlərinə ciddi ziyan vura biləcək potensialda olan proqramlardır ki,bu proqramlar müxtəlif kibercinayətkarlar tərəfindən yaradılır.Bu tip proqramlar həssas məlumatları rahat şəkildə ələ keçirib,onları silə bilər,həmçinin kompüterin nəzarəti başqalarının nəzarəti altına keçib,faylları rahat şəkildə yaya bilər.Zərərli proqram yalnız cihaz və fayllara zədələməklə qalmır,şəbəkəyə yoluxduğu zaman xoşa gəlməz hadisələr baş verə bilər.Zərərli proqram vasitələrinə misal olaraq aşağıdakılar aiddir:

1. Viruslar
2. Qurdlar
3. Troyan virusları
4. Casus proqramları
5. Reklam proqramları və s.

Virus-ən geniş yayılmış zərərli proqramdır ki,özü həyata keçirilərək fayllara və proqramlara rahat şəkildə yoluxa bilir.Viruslar istifadəçinin xəbəri və icazəsi olmadan kompüterin işini dəyişmək üçün yazılan kiçik proqramlar toplusudur.Viruslar iki əsas meyarın şərtlərini ödəməlidir:

1) İlk olaraq özünü icra etməlidir ki,o başqa proqramın icrasında öz kodunu yerləşdirsin.

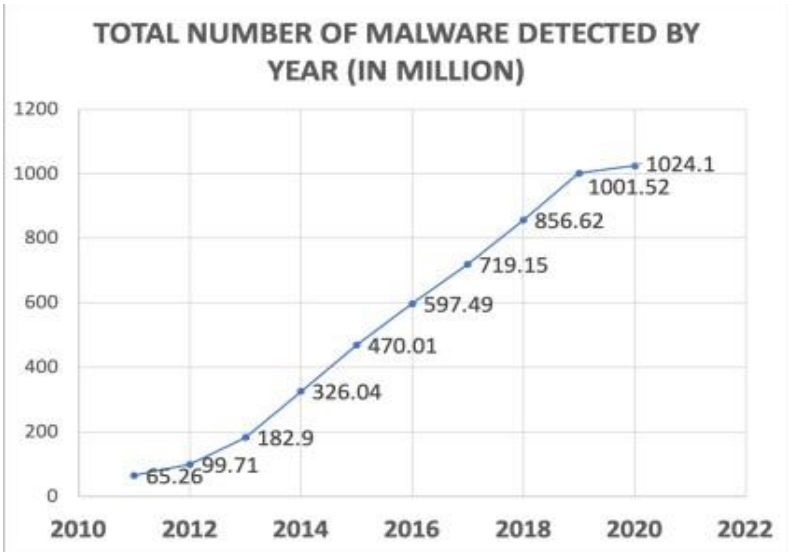
2) Özünü təkrarlatmağı bacarmalıdır.Digər icra olunan faylları virusa yoluxmuş faylın surəti ilə əvəz etməlidir.

Viruslar həm masaüstü kompüterlərə,həm də şəbəkə serverlərinə yoluxur.Bir çox viruslar faylların silinməsinə,proqramların zədələnməsinə və yaxud mövcüd diskin yaddaşının azalmasına səbəb ola bilir. Qurdlar-host proqramı,həmçinin zərərli proqram müəlliflərinin əlaqəsi olmadanda yayıla bilir.Qurdlar öz şəbəkələri vasitəsilə kompüterdə təkrarların çoxalması ilə internetdə sürətli şəkildə yayır.Bu təhlükəli viruslar çox vaxt fayllarda mövcud olsa belə,ən çox Excel və ya Word sənədlərinin daxilində rast gəlinir.PrettyPark ən geniş yayılmış nümunələrindən biridir. Troyan virisları-ən təhlükəli hesab edilən virusdur,öz hücumlarını kompüterlərdə gizlətməyə çalışır.Bu viruslar özlərini yararlı bir proqram və yaxud sayt kimi göstərərək,istifadəçinin bu məlumata daxil olmasına və həmin məlumatlardakı şərtləri yerinə yetirməyə şərait yaradır.İstifadəçinin bu proqram və yaxud sayta girişi nəticəsində bütün məlumatlar ələ keçirilir.Qurdlardan fərqli olaraq özünü təkrarlaya bilmə qabiliyyəti yoxdur.

Ransomware-istifadəçini sistemini asanlıqla yoluxdurur və bütün məlumatları şifrələyir.Kibercinayətkarlar məlumatların şifrəsini açmaq üçün istifadəçidən fidye ödənməsini tələb edir.

Rookit-termini "kök"və "kit" sözlərinin birləşməsindən əmələ gəlib.Digərlərindən fərqli olaraq,bu üsuldan istifadə edən kibercinayətkarlar özünü administrator səviyyəsində aparır.Lakin burada zərərli proqram təminatı mövcud deyil.Rookitlər antivirus proqramları tərəfindən aşkarlanmasında və silinməsində kənarda qala bilər.Bu zərərli proqramının əsas məqsədi aşkara çıxmaması və kompüterə

davamlı olaraq girişin təmin edilməsidir. Arxa qapı virusu və yaxud RAT virusu-gizli şəkildə yoluxmuş virus kompüter sistemində arxa qapı yaradır,bu da təhlükə iştirakçılarına istifadəçinin xəbəri olmadan uzaqdan daxil olma imkanını yaradır.[1]
Reklam proqramları-hücum iştirakçıları istifadəçinin tarixçəsini izləyir və onu alış-veriş etməyə sövq edə biləcək reklamları ekranda əks etdirir.Sistem monitoru-istifadəçinin e-poçt adresslərini,açılmış web saytlarını,həmçinin istifadə edilmiş bütün düymə vuruşlarını rahatlıqla izləyə bilir. Spyware və ya casus proqramları-bu tip proqramlar şəxsiyyət oğurluöunun baş verməsinə,fişinqlər kimi zərərli hücumların baş verməsi üçün istifadə olunur.Həmçinin istifadəçilərin bank hesablarınından və bizneslərindən pul oğurlamaq üçün yaradılmış təhdidlərdir.Casus proqramları adından göründüyü kimi sizin gün ərzində ziyarət etdiyiniz vebsaytlara,istifadə etdiyiniz fayllara rahat şəkildə daxil olaraq casusluq edə bilir. Casus proqramlarının bir növü olan key-loggers(açar qeyd edənlər) istifadəçinin klaviaturada işlətdiyi düymələri gizli şəkildə qeyd edərək,məlumatları fırıldaqçıya geri göndərir,bu yol vasitəsilə fırıldaqçı onlayn bank hesablarını oğurlaya bilər,həmçinin istifadəçinin fayllarına daxil olaraq şəxsi məlumatlardan istifadə edə bilər.Bu tip halların baş verməsi üçün çoxlu hiylələr vardır ki,fırıldaqçı spam xarakterli e-poçt keçidləri,müxtəlif veb-saytlara giriş təmin üçün müxtəlif yollara əl ata bilər.




Şəkil 1.İllər üzrə aşkar edilmiş virusların sayı(milyonlarla) [3].

**Zərərli proqramlarda təhlükəsizlik tədbirləri**
Bəs zərərli proqramın yoluxmanın qarşısını almaq üçün hansı ehtiyat tədbirlərini görmək olar?[2]

1. Tanımadığınız şəxslər tərəfindən göndərilmiş e-poçtları və yaxud daxil olunmuş keçidlərə daxil olmayın.Bunlar təhlükəli və şübhəli ola bilər.
2. Veb saytlarında gəzərkən ehtiyatlı olun,qarşınıza çıxan reklam xarakterli məlumatlara daxil olmayın.
3. Naməlum USB portlarını kompüterə daxil etməyin,bir çox hallarda viruslar məhz USB vasitəsilə ötürülür.
4. Təhlükəsizlik yenilənmələrini vaxtında yerinə yetirin.Həmçinin kompüter sistem yenilənməsini həmin vaxt ərzində icra etmək olduqca vacibdir.

5. Antivirus proqramlarından istifadə etməyi unutmayın.İnternetə daxil olmamışdan əvvəl antivirus proqramını aktivləşdirin.

**Zərərli proqramların aşkar olunması.** Zərərli proqramlarını neçə aşkar etmək olar?

Zərərli proqram təminatını aşkar etmək etmək üçün həmin proqram vasitələrinin təhlili,təsnifati,aşkarlanması və saxlanması kimi hissələrə ayırmaq olar.Zərərli proqramların təhlili dedikdə,həmin zərərli proqramın xüsusiyyətlərindən istifadə etməklə müxtəlif təsnifat üsullarına əsasən onun müəyyən edilməsidir.Təsnifat müəyyən əlamətlərinə görə kataloqlaşdırılır ki,buda həmin virusların daha asan tanınması üçün əlverişli bir yoldur.Zərərli proqramın aşkarlanması isə daha çox zərərin qarşısını almaq üçün istifadə olunur.Həmçinin zərərli proqramın hər hansısa bir nümunəsini gizlədə və yaxud təsdiq edə bilər.Bəzi aşkarlama üsulları vardı,onlarla tanış olaq.

1) İmza əsaslı zərərli proqramların aşkarlanması.Bu tip proqramların aşkarlanması əsasən antivirus proqramları tərəfindən geniş istifadə olunur,bunun vasitəsi ilə skaner zərərli kodu aşkar edir və hesabat üçün proqram daxilində bayt ardıcıllığını skan edir.İmza verilənlər bazası daima yenilənməlidir,çünki zərərli proqramının aşkarlanması üçün onun son versiyasına nəzər yetirilir.Bu üsul təhlil etməklə kod təlimatı sintaktik səviyyədə aparılır.Zərərli proqramı çaşdırmaqla onun işləməsinə təlimat verən prosesi məhdudlaşdırır.

2) Spesifikasiyaya əsaslanan zərərli proqramların aşkarlanması. Bu üsullardan əsasən nümunə üçün verilmiş uyğunluğun çatışmamazlığını aradan qaldırmaq və çaşqınlıq yaradan üsullara daha yüksək davamlılıq təmin etmək üçün xüsusi aloqirtmdən istifadə olunur.

3) Davranışa əsaslanan zərərli proqramların aşkarlanması. Davranışa əsaslanan aşkarlanma səthi skan edir və zərərli proqramların davranışlarını verilənlər bazasına yığaraq,onların hərəkətini müəyyən edir.Burada əsas məqsəd ondan ibarətdir ki,qarşıya çıxmış zərərli proqramların məxsus olduğu ailələri təsnifləşdirsin.Data mining texnikası həm zərərli,həm də qeyri-zərərli proqramları daha asan şəkildə fərqləndirmək üçün dəstək vektor maşınları texnikasındanistifadə edir.Bu da öz növbəsində daha yüksək olan metaforik ərərli proqramların aşkar edilməsində çox sərfəlidir.

**Zərərli proqramların təhlili.** Zərərli proqramların təhlil edilməsi.Zərərli proqramlar üçün imzalar yaradılmamışdan əvvəl riskləri və niyyətləri başa düşüb təhlil etməliyik.Təhlil zərərli proqramları və onun bütün imkanlarnı yoxluyaraq,daha təhlükəsiz bir mühitdə icra etməklə təcrübələr əldə edə bilərik.Əsasən iki cür təhlildən istifadə olunur:[4]

1) Statik təhlil
2) Dinamik təhlil

1) Statik təhlil

Zərərli proqramının təminatını icra etmədən təhlil olunmasına statik təhlil adlanır.Statik təhlildə istifadə edəcəyimiz nümunələrə misal olaraq,sətir imzasını,sintaktik kitabxana çağırışını,bayt ardıcılllığının n-qramları daxildir.Statik təhlil edilməmişdəm əvvəl fayl mövcüd olduğu yerdən çıxarılmalı və şifrəsi açılmalıdır.Bler/debugger icra sənədlərinin geri qaytarılması üçün istifadə olunur,LordPe [5] və OllyDump [6] yaddaş alətləri sistemdə yerləşən qoruyucu kodu əldə etmək üçün,həmçinin onu fayla daxil etmək üçün istifadə olunur.Bu təhlil texnikası təhlil edilməsi çətin olan yüklənmiş icra sənədlərinin təhlil etmək üçün istifadə olunan ən yaxşı texnikadır.Lakin statik təhlilin müəyyən çatışmamazlıqları mövcud idi ki,bu da dinamik analizin yaradılmasına səbəb oldu.Statik təhlil zərərli proqramların aşkar olunması,həmçinin onların təsnifi üçün kifayət qədər yetərli olmadığı üçün dinamik təhlil ilə əlaqələndirilməyə başlanmışdır.Dinamik təhlil bir növ statik təhlilin tamamlayıcısı kimi həyata keçirildir.

2) Dinamik təhlil. Zərərli proqramın kodunun idarə olunan mühitində(virtual maşın,simulyator və s) icrası zamanı onun sistemlə qarşılıqlı əlaqəsinin təhlilinə dinmaik təhlil deyilir.İlk olaraq Process Monitor və Capture Bat[6],Process Explorer[7] və Process Hackerreplace kimi monitorinq alətlərini quraşdırıb aktivləşdirmək lazımdır.Dinamik təhlili icra etmək üçün müxtəlif funksiyaların çağırış monitoringi,parametrlərin təhlili,məlumatların axınının izlənməsi və s daxildir.Dinamik təhlil statik təhlilə görə daha keyfiyyətlidir və burada icra olunan faylın dağıdılması tələb olunmur.O,analiz təhlilə

nisbətən daha davamlı təbiət davranışa malikdir.Lakin bu çox vaxtın itirilməsinə,daha çox resurslardan istifadə tələb edir.Zərərli proqramın istifadə olunduğu mühit virtual mühitdən çox fərqlidir.O həmçinin dəqiq deyil,süni davranışla yranan müxtəlif üsullarla özünü büruzə verə bilər.Zərərli proqram üçün bir sıra onlayn avtomatlaşdırılmış alətlər mövcuddur,məsələn:Norman Sandbox,CWSandbox,TTAnalyzer və s.Bu proqramlar mövcud olan zərərli proqramın davranışını daha tez başa düşür və hərəkətləri dərindən analiz edir.Bundan əlavə hər gün minlərlə zərərli proqram vasitələrini avtomatlaşdırılmış şəkildə yanaşma tələb olunur.

**Zərərli proqramların təhlil alətləri.** Zərərli proqram vasitələrinin təhlil alətləri**.** Gələcəkdə baş verə biləcək hücumlardan qorunmaq və proqnozlaşdırmaq üçün zərərli proqramın təhlili üçün bir sıra müxtəlif alətlərdən istifadə edirlər.Tədqiqatçılar açıq mənbəli zərərli proqramın təhlili alətlərindən istifadə etməklə hücumun həyat dövrünü təhlil edərək baş verə biləcək təhlükələri nəzarət edir.Lakin getdikcə zərərli proqrmların mürəkkəbliyi artdı,bu da həmin prosesi təhlil etməyə,həmçinin müqayisə etməkdə çətinlik yaradırdı.Buna görədə hər bir zərərli proqramın növünü təhlil etmək üçün həm düzgün alət tapılmalıdır,həm də tədqiqatçılar bu işin öhdəsindən gəlməyi bacarmalıdır.Bir sıra alətlər ilə tanış olaq.

1) Açıq mənbəli zərərli proqramların təhlili alətləri

Google Rapid Pesponse(GRR)-bu platforma Google-də təhlükəsizlik tədqiqatçıları tərəfindən yaradılmış,insedentlərə cavab verən bir sistemdir.Həmçinin agent və serverilə əlaqənin saxlanılması üçün quraşdırılmış proqramdır.GRR aləti həm agenti,həm də müştəriləri idarə edir,onlarla danışa bilmə bacarığıda mövcuddur.Agent və server quraşdırıldıqdan sonra onlar GRR müştərisinə çevrilərək mesajlar almağa başlaya bilərlər.Platformanın əsas məqsədi baş verən hadisələri daha tez təhlil etsin və uzaqda təhlil aparmaq mümkün qədər sadə və çevik şəkildə yerinə yetirə bilməkdir. Remnux-pulsuz Linux aətlər dəstinə aiddir.Platforma zərərli proqramların nümunələrini axtaran bir pəncərə interfeysindədir.REMnux Ubuntu üzərində yaradılmışdır,həmçinin Linux və Windows əsasında təhlilin daha tez yerinə yetirilməsi üçün bir neçə resurs ilə birləşdirilmişdir.Burada əsas məqsəd qeyri-adi mətn faylarını araşdırmaq,zərərli obyektləri təyin edib,silmək

Zeek-Şəbəkə təhlükəsizliyi monitoru şəbəkə axınını hadisələrə çevirən çoxyönlü şəbəkədən asılı olan analtik sistemdir.O,imza əsaslı və anomaliya əsaslı monitrinqdən istifadə edərək şəbəkəyə baxış icra edir.Şəbəkə təhlükəsizliyinə diqqət yetirməkdən əlavə şəbəkə axınının təhlilində hər tərəfli nəzarət edir.Zeek platforması 20 ildən çoxdur ki istifadə olunur və yarandığı müddət ərzində əməliyyatlar arasında boşluğu aradan qaldırmaqda çox müvəffəqətlidir. Cuckoo Sandbox-2010-cu ildə Google Summer of code yaradıcılığı ilə könüllülər komandası bu analtik aləti yaratmışdır.Bwu Windows,linux və Andorid üçün zərərli faylları analiz edən,onları avtomatlaşdıran və həmin faylların necə işlədiyinə aid bütün faktları özündə saxlayan platformadır.Həmçinin baş verə biləcək bütün zərərli proqramların hücumlarının gərginliyini də azaltmaq üçün çox əlverişlidir.Son illərdə,istifadəşilər üçün vazkeçilməz bir sistemə çevrildi.2012-ci ildə Cuckoo toplanmış məlumatların istifadəsinin asan olması üçün Malwr alətini yaratdı.

2) Mobil zərərli proqramlarınn təhlili alətləri. APKTool -ikili Andoridlər üçün işləmək,qapalı sistemə malik olan alətdir.Bir sıra dəyişikliklər etməklə orjinal formayı deçifrə etmək,əvvəlki halını bərpa etmək mümkündür.Bu alət faylların yaradılması,onların apk yaratmaq kimi bir sıra layihə sayəsində cihazla işləməyi çox asanlaşdırır.APKTool-un üstün cəhətlərindən biri də mənbənin kodunu tez bir zamanda dəyişə bilərik,həmçinin deşifrə edilmiş resursları apk formatına qaytara bilərik. Dex2Jar -Android ".dex" və Java ".class" faylları ilə işləmək üçün yaradılmış pulsuz istifadə olunan alətdir.Android proqramlarını ".dex" skreiptlərinə bənzəyir və o Java-da yazılmış tərtib olunmuş proqramlara çevirir.Daha sonra bütün məlumatlar ".dex" qovluğunda saxlanılır.Dex2Jar alətinin əsas xüsusiyyəti APK classes.dex faylını classes.jar və yaxud əksinə çevirməkdir. Mobile Sandbox-platforma Android OS smartfonları üçün həm statik,həmdə dinamik analizlərini yerinə yetirir.Sistem bu analizləri iki istiqamətdə aparır: [10]

1) statik və dinamik analizi birləşdirir,yəni statik analizin nəticələrini dinamik təhlilə istiqamətləndirir.
2) Müxtəlif girişlər ümün müxtəlif API proqramlarından istifadə olunur.

Statik təhlil də VirusTotal xidmətindən istifadə etməklə bir neçə antivirus proqramlarını skan edərək,onların içərisində ən yaxşı olanını seçir.Dinamik analiz də isə tətbiqi əməliyyatları işlədə və onları qeyd edə bilər.

**Nəticə**

Zərərli proqram vasitələrindən qorunmaq üçün ən yaxşı təhlükəsizlik proqramları seçim edilməlidir.Zərərli proqramın təhlükələrini əvvəlcədən müəyyənləşdirilməsi,və onlardan qorunmağı bacarmaq lazımdır.Bu cür təhlükələrə qarşı tədqiqatçılar bir neçə fikirlər irəli sürmüş və həmin fikirlər əsasında müvəffəqiyyətli üsullar tapılıbdır.Doğru şəkildə qəbul edilmiş qərarlar istifadəçinin öz şəxsi məlumatlarının təhlükəsiz şəkildə saxlayacaqdır.Həmçinin bu məqalədə bu təhlükələrin araşdırılması üçün müxtəlif texnika və vasitələri də araşdırdıq.

**Ədəbiyyat**


[1] Ben Lutkevinc-"Malware" https://www.techtarget.com/searchsecurity/definition/malware
[2] Protecting against malware-VigiTrust-Free-course-Protecting-Against Malware_compressed.pdf
[3] Sajedul Talukder-"Malware_Survey_arxxiv"
[4] I. Lapowsky, "Malware last 10 years," AV-TEST, shorturl.at/yzN01, 2020
[5] B. Anderson, C. Storlie, and T. Lane, "Improving malware classification: bridging the static/dynamic gap," in Proceedings of the 5th ACM workshop on Security and artificial intelligence, 2012, pp. 3–14.
[6] S. Talukder, S. Witherspoon, K. Srivastava, and R. Thompson, "Mobile technology in healthcare environment: Security vulnerabilities and countermeasures," arXiv preprint arXiv:1807.11086, 2018.
[7] J. Sexton, C. Storlie, and B. Anderson, "Subroutine based detection of apt malware," Journal of Computer Virology and Hacking Techniques, vol. 12, no. 4, pp. 225–233, 2016
[8] P. Khodamoradi, M. Fazlali, F. Mardukhi, and M. Nosrati, "Heuristic metamorphic malware detection based on statistics of assembly instructions using classification algorithms," in 2015 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS). IEEE, 2015, pp. 1–6.
[9] S. Talukder and B. Carbunar, "Abusniff: Automatic detection and defenses against abusive facebook friends," in Twelfth International AAAI Conference on Web and Social Media, 2018.
[10] X. Xiao, S. Zhang, F. Mercaldo, G. Hu, and A. K. Sangaiah, "Android malware detection based on system call sequences and lstm," Multimedia Tools and Applications, vol. 78, no. 4, pp. 3979–3999, 2019.


## ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ ДЛЯ ОПТИМИЗАЦИИ ЭНЕРГОЭФФЕКТИВНОСТИ В УМНЫХ ГОРОДАХ


**Джамиль Алиев**
**ЗАО "Azərbaycan Hava Yolları"**



Абстракт

В эпоху глобальных изменений и растущего давления на природные ресурсы, устойчивое развитие городов приобретает особую актуальность. Города по всему миру сталкиваются с многочисленными вызовами, включая урбанизацию, изменение климата и необходимость обеспечения качества жизни своих жителей при одновременном снижении воздействия на окружающую среду. В этом контексте технологии умных городов и аналитика больших данных выступают в качестве ключевых инструментов для реализации энергоэффективности и устойчивого городского развития.