ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

мүмкін. Осы мақсатта энергия тұтынуды ескеретін IoT экожүйелерін дамытуға күш салынуда. Осындай архитектуралардың бірі, яғни 2EA архитектурасы balasubramanian et al әзірлеген. Energyaware-Edge-Aware (2EA) архитектурасында IoT сенсорлары өз энергиясын жинай алады. Заттар интернеті желісіндегі әрбір сенсор үшін қуат көрсеткіштері бар энергетикалық профиль сақталады. Энергия таусылған жағдайда, зардап шеккен түйін энергия профилін сұрайды және жақын жерде ең сенімді түйінді табады. Бұл схема тапсырмаларды қабылдау процесіне негізделген ресурстарды оңтайлы пайдалануды қамтамасыз етеді.

Бұл мақалада заттар интернетінің (IoT) өсіп келе жатқан осалдықтары жан-жақты зерттелді және оларды жоюдың түрлі стратегиялары ұсынылды. IoT құрылғыларының күнделікті өмірімізде алатын орны артып келе жатқанына қарамастан, олардың қауіпсіздігі әлі де негізгі алаңдаушылық тудырады. Мақалада талқыланған осалдықтар мен түзету стратегиялары IoT қауіпсіздігін нығайтуға және потенциалды шабуылдарға тиімді жауап беруге бағытталған. IoT құрылғыларын тиімді қорғау үшін үздіксіз зерттеулер мен әзірлемелерді жалғастыру қажеттігі айқын көрінеді. Болашақта IoT қауіпсіздігі саласындағы зерттеулер мен әзірлемелер бұл технологияның әлеуетін толық пайдалануға және кибер қауіптерге қарсы тұра алатын сенімді шешімдер құруға ықпал етуі тиіс.

Қолданылған әдебиеттер тізімі

1. Zanella A. et al. Internet of things for smart cities //IEEE Internet of Things journal. – 2014. – Т. 1. – №. 1. – С. 22-32.

2. Mikko H. et al. The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation//Technology Innovation Management Review. – 2017.

3. Corser G., Fink G., Bielby J. Internet of Things (IoT) Security Best Practices; IEEE Internet Technology Policy Community; White Paper//IEEE: Piscataway, NJ, USA. – 2017.

4. Kolias C. et al. DDoS in the IoT: Mirai and other botnets//Computer. – 2017. – Т. 50. – №. 7. – С. 80-84.

5. Anand P. et al. IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges//IEEE Access. – 2020. – Т. 8. – С. 168825-168853.

6. Makhdoom I. et al. Anatomy of threats to the internet of things //IEEE communications surveys & tutorials. – 2018. – Т. 21. – №. 2. – С. 1636-1675.

7. Rajan A., Jithish J., Sankaran S. Sybil attack in IOT: Modelling and defenses//2017 International conference on advances in computing, communications and informatics (ICACCI). – IEEE, 2017. – С. 2323-2327.

8. Neshenko N. et al. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations//IEEE Communications Surveys & Tutorials. – 2019. – Т. 21. – №. 3. – С. 2702-2733.

9. Mosenia A., Jha N. K. A comprehensive study of security of internet-of-things//IEEE Transactions on emerging topics in computing. – 2016. – Т. 5. – №. 4. – С. 586-602.

ӘОЖ 004.056.57

PORTABLE EXECUTABLE ФОРМАТТЫ ФАЙЛДАР ҚҰРЫЛЫМЫ ЖӘНЕ ОЛАРДЫ ЗИЯНДЫ КОДҚА АЙНАЛДЫРУ ЖОЛДАРЫ

Мукушев Әмірбек Қайратұлы

Amirbek.mukushef@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы магистранты , Астана, Қазақстан

Ғылыми жетекші – Суханова Ж.С.

Аннотация. Windows операциялық жүйесі қолданушылар арасында кең таралған жүйе. Windows жүйесіндегі барлық орындалатын файлдар Portable Executable форматына сәйкес құрастырылады. Оның ішінде зиянды программалар да Portable Executable форматына ие.

Мақалада Portable Executable форматындағы файлдардың форматының құрылымын талдау қарастырылған. Сонымен қатар, статикалық және динамикалық талдау әдістері мен құралдары және зиянды кодқа айналдыру жолдарының сипаттамасы берілген.

Кілт сөздер: Portable Executable, Windows, операциялық жүйе, файл, зиянды код, программа.

Кіріспе. Қазіргі таңда қауіпті вирустық программалардың қарқынды дамуына байланысты компьютерлердің ақпараттық қауіпсіздігін қамтамасыз ету өзекті мәселеге айналды. Қаупсіздікті қамтамасыз ету мақсатында Windows операциялық жүйесіндегі программаларды PE тақырыптары арқылы талдау тиімді әдістерге жатады. PE-форматы файл ішінде жазылған кодты басқару үшін Windows операциялық жүйесіне қажетті ақпаратты қамтиды. Windows операциялық жүйесінде орындалатын барлық файлдар Portable Executable форматында болады [1].

Portable Executable форматты файлдар құрылымы. Portable Executable форматындағы файлдар тақырыптары келесі бөлімдерден құралады:

DOS қосымшасы - MS-DOS және Windows операциялық жүйелері «.exe» кеңейтілімі бар қосымшалармен жұмыс істеуіне байланысты, Windows-қа арналған қосымшалар DOS ішкі кішігірім қосымшасымен бірге орындалады. DOS операциялық жүйесінде Portable Executable форматындағы программа орындалатын болса, «Бұл программа DOS режимінде қосылмайды» хабарламасын шығарады. 0x3c адресінде файл сигнатурасына ығысуы туралы ақпаратты қамтиды және осы ақпарат арқылы Windows операциялық жүйесі программаның дұрыс орнылдауына мүмкіндік береді.

Signature - MS-DOS ығысуы файл сигнатурасы саналатын 4 байтты қолтаңбаны береді. Бұл қолтаңба мәні – «PE\0\0» («P» және «E» әріптері және екі NULL байтынан құралады).

File Header – файл туралы негізгі ақпаратты қамтитын бөлім. Осы бөлім құрылымы кесте 1-де көрсетілген.

Кесте 1.

File Header бөлімінің құрылымы және анықтамасы

Ығысу	Көлемі	Атауы	Анықтамасы
0	2	Machine	Процессор анықтамасы
2	2	NumberOfSections	Файлдағы секциялар саны
4	4	TimeDateStamp	Файлдың құрылу уақыты
8	4	PointerToSymbolTable	Символдар кестесіне дейінгі ығысу немесе 0
12	4	NumberOfSymbols	Символдар кестесіндегі элементтер саны
16	2	SizeOfOptionalHeader	OptionalHeader көлемі
18	2	Characteristics	Файл атрибуттары

Optional Header. «Опционалды тақырып» деп аталатындығына қарамастан құрамындағы ақпарат құнды болып табылады. Optional Header тақырыбының маңызды бөлімдері кесте 2-де қарастырылған.

Кесте 2.

Optional Header тақырыбының маңызды бөлімдерінің атаулары және анықтамасы

Ығысу	Көлемі	Атауы	Анықтамасы
0	2	Magic	Файл кескінінің күйін анықтайтын сан. Кең таралған мәні - 0x10B. 0x10B мәні қарапайым орындалатын файл ретінде анықтауға мүмкіндік береді.
2	1	MajorLinkerVersion	Linker (байланыстырушы құралы) нұсқасының негізгі нөмірі.

3	1	MinorLinkerVersion	Linker (байланыстырушы құралы) нұсқасының қосымша нөмірі.
4	4	SizeOfCode	Код сақталатын секция көлемі.
8	4	SizeOfInitializedData	Деректердің инициализацияланған бөлімінің көлемі.
12	4	SizeOfUninitializedData	Деректердің инициализацияланбаған бөлімінің көлемі.
16	4	AddressOfEntryPoint	Орындалатын файлдың жадыға жүктелуі кезінде программа кескініне сәйкес кіру адресі. Программалар үшін бастапқы адрес болып саналады. Драйверлер үшін инициализация функциясының адресі болып саналады. DLL кітапханалары үшін маңызды емес болып табылады.
20	4	BaseOfCode	Орындалатын файл кодының жадыға жүктелуі кезінде программа кескініне сәйкес кіру адресі.

Section Header. Секция тақырыбы – PE файлдың әр секциясындағы атауы, көлемі, ығысуы және атрибуттары сияқты ақпаратты қамтитын бөлігі. Негізгі секцияларға .text, .data, .rdata, .rsrc, .idata кіреді.

Кесте 3.
Section Header(Секция тақырыптары) құрылымы

Ығысу	**Көлемі**	**Атауы**	**Сипаттамасы**
0	8	Name	Секция атауы
8	4	VirtualSize	Жадыдағы секция көлемі
12	4	VirtualAddress	Орындалатын файлдар кескіні үшін жадыдағы бірінші байтының адресі белгілеу үшін қолданылады
16	4	SizeOfRawData	Файлдағы секция көлемі
20	4	PointerToRawData	Секция деректерінің басталуына дейінгі ығысу мәні
24	4	PointerToRelocations	Секцияның бірінші бөліміне бағыт көрсетуге қолданылады.
28	4	PointerToLinenumbers	Секцияның бастапқы жол нөміріне бағыт көрсету үшін қолданылады
32	2	NumberOfRelocations	Секция үшін орын ауыстыру, ығысу санын көрсетеді. Орындалатын файлдарда үнемі 0-ге тең
34	2	NumberOfLinenumbers	Секцияға қосылатын жолдардың саны.
36	4	Characteristics	Секция атрибуттары

Зиянды кодқа айналдыру жолдары. Орындалатын файлды қауіпті файлға айналдыру үшін оның құрылымына зиянды код енгізіледі. Зиянды код енгізілуі кемінде үш міндетті орындаумен жүзеге асырылады [3]:

1. Файлдың ішіне зиянды кодты енгізу;
2. Негізгі программа орындалуына дейін зиянды кодтың басқаруға келуін қамтамасыз ету;
3. Зиянды кодтың орындалуы үшін керекті жүйелік API-функциялардың адрестерін анықтау.

Файл ішіне зиянды кодты қосу әдістері:

1. Негізгі программа кодының орнына зиянды кодты жазу;
2. Программаның бос жеріне зиянды кодты қосу;
3. Негізгі программа кодын сақтай отырып, файлдың бастапқы бөліміне, ортаңғы немесе соңғы бөліміне зиянды кодты қосу.

Негізгі программа орындалуына дейін зиянды кодтың басқаруға келуі үшін

1. Негізгі кодқа өту адресі сақталған бөлімді зиянды код орналасқан адреске өзгерту;
2. Негізгі кодқа өту нүктесі айналасында зиянды кодқа өту командаларын қосу;
3. Импорт кестесіндегі кейбір элементтерді өзгерту арқылы зиянды кодты орындауға арналған функцияларды шақыру;

Зиянды кодтың орындалуы үшін керекті жүйелік API-функциялардың адресін анықтау жолдары:

1. Файлдың импорт кестесіндегі фунцияларды іздеу;
2. LoadLibrary/GetProcAddress қолдану арқылы иморт кестесіне керекті функцияларды іздеу және қосу;
3. Зиянды кодта көрсетілген жол бойынша қажетті фнукцияларды орындалуын жүзеге асыру;
4. Файлдың импорт кестесіндегі фунцияларды қосу.

PE форматындағы программаларды талдау. PE форматындағы программаларды талдау әртүрлі құралдар мен техникаларды пайдалана отырып жүргізілуі мүмкін.

Статикалық талдау: Файлдың тақырыптарын, секция атрибуттарын және басқа параметрлерін файл орындалуынсыз талдауды жүзеге асырады. Статикалық талдау арқылы программаның қауіп төндіруі мүмкіндігін анықтауға болады. Статикалық талдау тез орындалатын талдау әдісі, бірақ күрделі қауіпті программалық қамтамаларды ьалдауда тиімділігі төмен болып келеді.

Динамикалық талдау: Бағдарламаны бақыланатын ортада іске қосуды және оның орындалуын қадағалауды көздейді. Динамикалық талдау бағдарламаны жөндеуді, жүйелік шақыруларды қадағалауды және желілік трафикті талдауды қамтиды.

Талдау құралдары: Дизассемблерлерді, декомпиляторларды және статикалық талдауға арналған утилиталардан PE файлдарын талдау үшін қолданылатын көптеген құралдар бар. Талдау құралдарына IDA Pro, CFF, OllyDbg, WinDbg және Python программалау тіліне арналған pefile кітапханасын жатқызуға болады.

Қорытынды. PE форматындағы бағдарламаларды талдау ақпараттық қауіпсіздік саласындағы мамандар жұмысының маңызды бөлігі болып табылады. PE файлдарының құрылымы мен тақырыптарын түсіну сараптама жүргізуші мамандарға осалдықтарды анықтауға, зиянды бағдарламалық қамтамасыз етуді талдауға және жүйені шабуылдардан қорғау бойынша шаралар қабылдауға мүмкіндік береді. PE файлдарын сәтті талдау статикалық және динамикалық әдістерді үйлестіруді, сондай-ақ тиісті құралдар мен техникаларды пайдалануды талап етеді.

Пайдаланылған әдебиеттер тізімі

1. M. Sikorski and A. Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 1st edition (March 3 2012), ISBN-10 1593272901
2. Формат PE. https://learn.microsoft.com/ru-ru/windows/win32/debug/pe-format
3. Касперский К., Компьютерные вирусы изнутри и снаружи, СПб: Питер, 2006,С. 114.