УДК 004.43

ЗИЯНДЫ ПРОГРАММАЛЫҚ ҚАМТАМАНЫ ПРАКТИКАЛЫҚ ТАЛДАУ

Сұлтан А. А.
sultan.aiken@gmail.com
7М06111- «Ақпараттық қауіпсіздіктің әдістері мен технологиялары»
Мамандығының 2-курс магистранты
Л. Н. Гумилев атындағы Еуразия Ұлттық Университеті, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – Сауханова Ж.С.

Зерттелетін мәселенің өзектілігі зиянды программалар (ЗП) санының көбеюіне тікелей байланысты. Бұл мақалада зиянды программалық жасақтаманы тарату әдістері және зиянды программалық жасақтаманың таралу жылдамдығына әсер ететін сипаттамалық белгілер зерттеліп, қарастырылады. Мақалада қолданылған материалдар негізінде әртүрлі әдістердің таралу жылдамдығына әсерін ескере отырып, зиянды программалардың таралу модельдері келтірілген.

Кілт сөздер: зиянды программа, тарату әдісі, зиян, таралу жылдамдығы, сипаттамалық белгілер, қорғау шарасы.

Технологиялар дамыған заманда, зиянды программалық қамтамасыз етудің (ПҚ) әсерінен корпоративтік таратылған ақпараттық-есептеу желілерінің қауіпсіздігін қамтамасыз ету көптеген қиындықтар туғызуы әбден мүмкін, сондай-ақ бұл мәселе айқын әрі күрделі мәселердің бірі болып табылады. Деректерге сүйенсек, 2016 жылдың бірінші тоқсанында 249 619 379 зиянды программалар мен желілік құрттар тіркелген екен, бұл көрсеткіш ақпараттық құрылымдарды қорғауды қамтамасыз ету мәселесінің өзектілігін дәлелдей түседі[1].

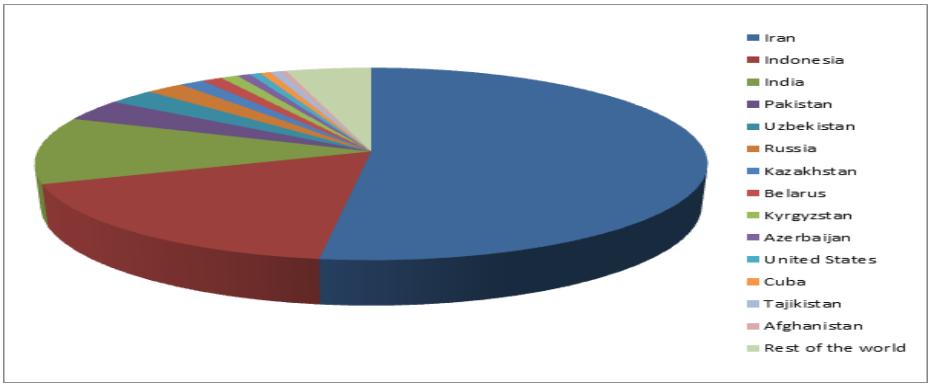
Зиянды программалардан қорғаудың ең көп таралған тәсілдерінің бірі уақытылы қарсы іс – әрекеттер жасай алу мақсатымен олардың таралуын болжайтын әдістерді қарастырып, зерттеу болып есептелінеді. Осы салада жүргізілген зерттеулердің ішінен ұсынылып отырған ғылыми жұмыстарды айрықша көрсетуге болады [2-3]. Алайда, аталған ғылыми зерттеулер негізінен тек зиянды программалардың жіктелуін зерттеуге ғана бағытталған немесе зиянды программалардың бір немесе екі түрінің сипаттамаларын қарастырады. Williamson, M. W. және Leveille, J. ғылыми еңбектерінде зиянды программалардың таралу жылдамдығы сияқты параметрлерді ескеретін тарату модельдері жайлы қарастырылады [4-5], бірақ теріс әсер ету ауқымына қарай зиянды бағдарламаны таратудың әртүрлі әдістерінің мүмкіндіктері жайлы ақпарат жеткілісіз көрсетілген. Жоғарыда көрсетілген ақпаратқа сай, зиянды программалардың таралуында қолданылатын болжау модельдерін нақтылау үшін алдымен зиянды программалық жасақтаманың тарату әдістерін талдау қажет.

Stuxnet, Wiper, Flame, Gauss, Duqu, Icefog зиянды программаларының ерекшеліктері, таралу әдістері зерттелді.

Бірінші қаарстыратын зиянды программа Stuxnet[6].

2010 жылдың 9 шілдесінде Белоруссиялық "ВирусБлокада" антивирустық компаниясының мамандары Stuxnet деп аталатын зиянды программаны тапты.

Оны құрастырған - қазіргі заманғы ақпараттық қауіпсіздік жүйелерінің әлсіз жерлерін жақсы білетін жоғары білікті мамандар тобы болып табылады. 1 – суретте Stuxnet шабуылына ұшыраған елдердің тізімі көрсетілген.



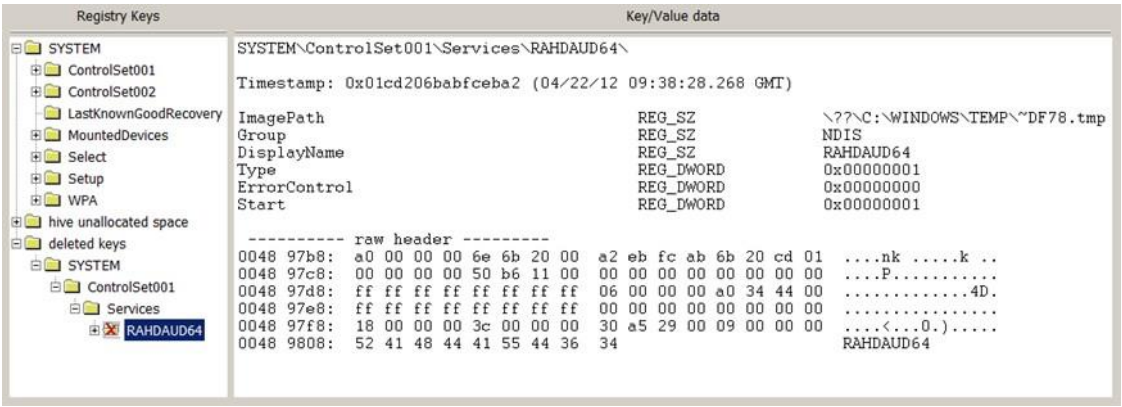
Сурет 1. Stuxnet шабуылына ұшыраған елдердің тізімі

Келесі қарастыратын зиянды программа Wiper [7].

2012 жылы Иранның ондаған ұйымдарының серверлерінде көптеген мәліметтер базасы жойылады Wiper программасының тарихы осыдан басталады.

Wiper ЗП мақсаты - қатты дискідегі деректерді және, ең алдымен, программаны талдау үшін пайдалануға болатын файлдарды біржола жою. Wiper ЗП шабуылынан кейін Касперский зертханасының қызметкерлері қатты дискілердің бірінде қалған деректердің тізімнің ішінен бір бөлігін қалпына келтіре алды 2 –суретте Wiper ЗП шабуылынан кейінгі қалпына келген деректер.

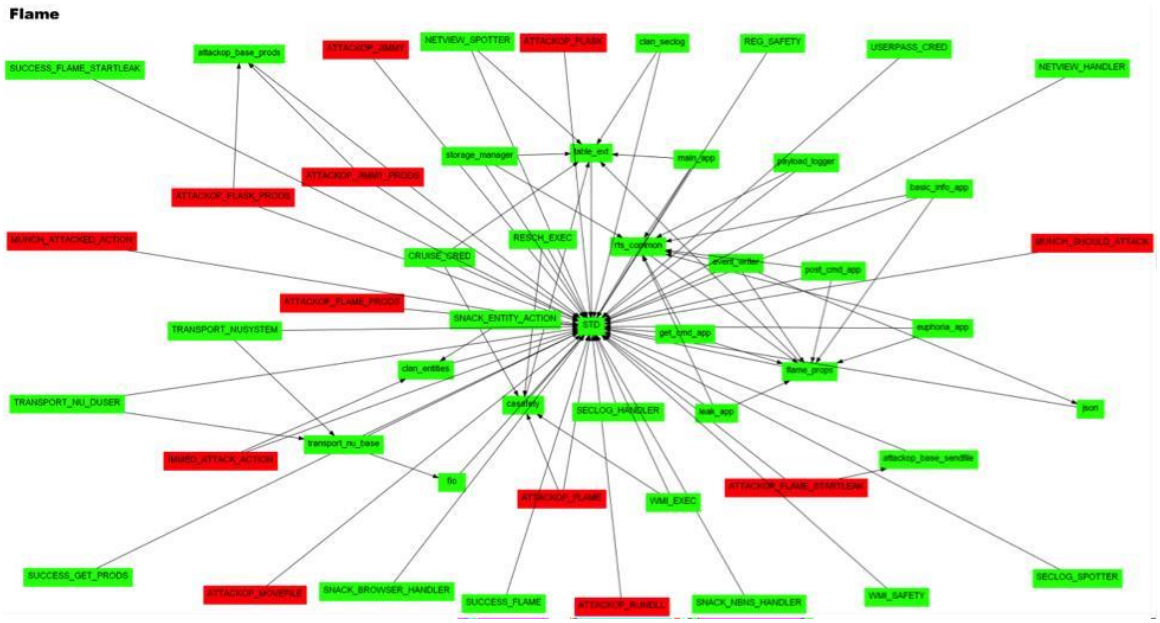
Сурет 2. Wiper ЗП шабуылынан кейінгі қалпына келген деректер



Flame зиянды программасы - Microsoft Windows XP, Vista, 7 нұсқаларының операциялық жүйесінің басқаруындағы компьютерлерді зақымдайтын зиянды программа [8].

Flame-ді 2012 жылдың 28 мамырында Иранда компьютерлерге шабуыл жасаған Wiper вирусын зерттеу кезінде Касперский Зертханасының компьютерлік қауіпсіздік жөніндегі аға ғылыми қызметкері Роэль Шувенберг ашты. Ең көп зардап шеккен елдер - Иран, Израиль, Судан, Сирия, Ливан, Сауд Арабиясы және Египет. Бұл троялық бағдарлама - "backdoor", ол сонымен қатар құрттарға тән қасиеттерге ие және оны иесінен тиісті "бұйрық" алған кезде жергілікті желі мен алынбалы құралдар арқылы таратуға мүмкіндік береді. 3 – суретте Flame

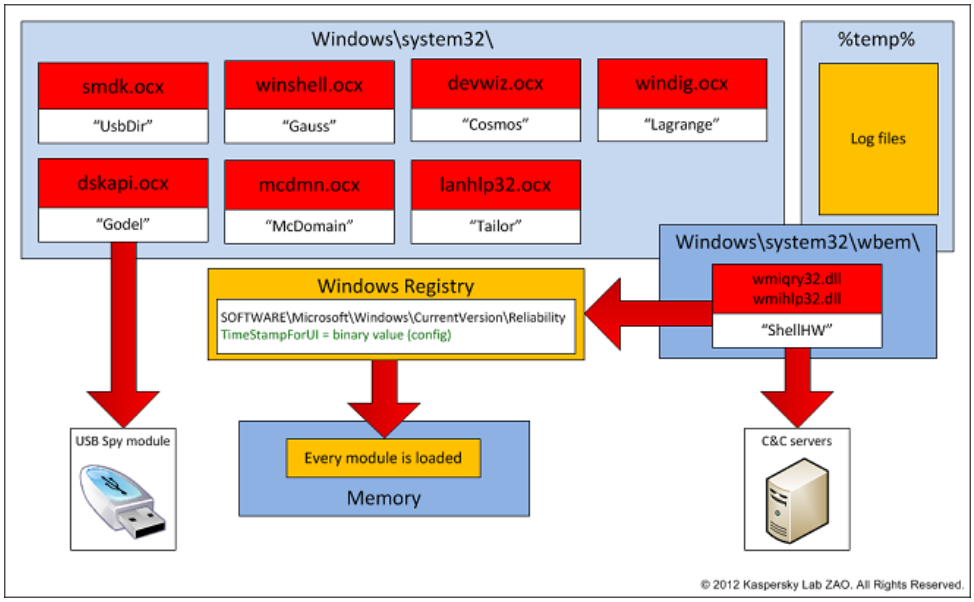
зиянды программасының жұмысы бейнеленген.



Сурет 3. Flame зиянды программасының жұмысы

Gauss зиянды программасы Flame платформасын құрған мамандар тобы жасаған кибершабуылға арналған құралдардың күрделі жиынтығы [9].

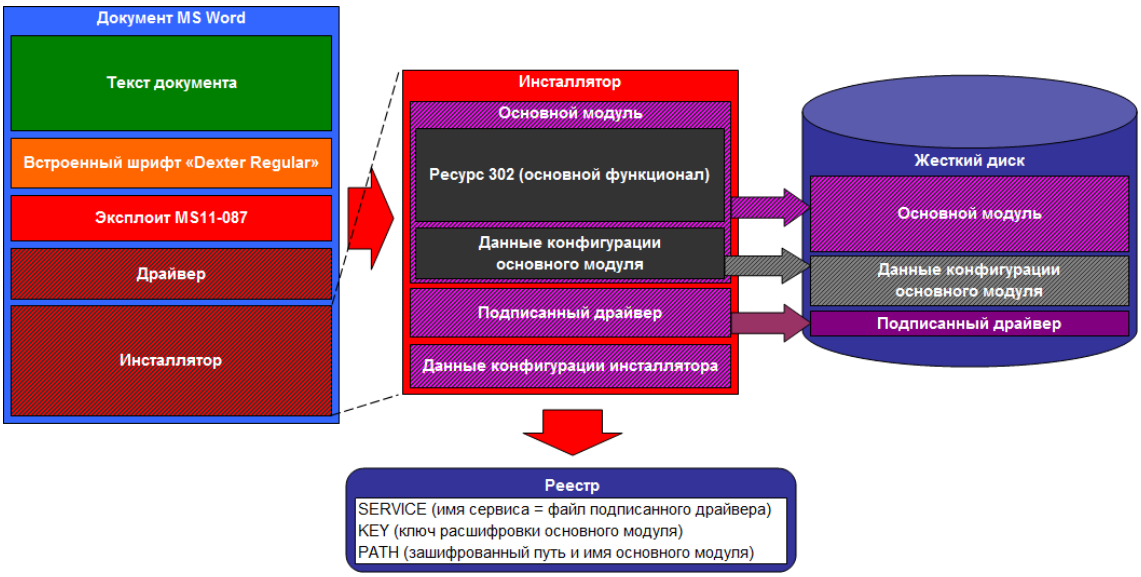
Gauss деп аталатын Модуль зиянды программаның маңызды элементі болып табылады, өйткені ол банктік деректерді ұрлауға байланысты мүмкіндіктерді жүзеге асырады. Осылайша, барлық зиянды кешен осы компоненттің атымен аталады. 4 – суретте Gauss зиянды программасының жүзеге асырылуы кескінделген.



Сурет 4. Gauss зиянды программасының жүзеге асырылуы

Венгр crysys ұйымының мамандары жүргізген зерттеулер (Будапешт технология және экономика университетінің Жүйелік қауіпсіздік және криптография зертханасы) жүйені зақымдайтын орнатушыны (дропперді) ашуға әкелді, жүйені зақымдау Duqu зиянды программасы арқылы жүзеге асырылды.

Бұл TTF шрифттарын визуализациялайтын механизміне жауап беретін win32k.sys драйверінің осалдығын пайдаланған эксплойтты қамтитын Microsoft Word форматындағы файл болды (MS11-087, Microsoft 13 қараша 2011), 5 – суретте Duqu зиянды программасының әрекет ету реті көрсетілген [10].



Сурет 5. Duqu ЗП

2011 жылдан бастап Ақпараттық қауіпсіздік мамандары Icefog деп аталатын киберқылмыскерлер тобымен байланысты бірқатар шабуылдарды қадағалады.

Icefog шабуылдары Microsoft Windows және Apple Mac OS X операциялық жүйелеріне бағытталған арнайы жасалған кибершабуыл құралдарын қолдана отырып жүзеге асырылады [11].

Icefog атауы талдаған зиянды программа үлгілерінің бірінің серверінің атауынан алынған. Сондай-ақ, программалық жасақтамасының атауы қытайша Dagger Three екенін белгілі. 6-суретте Icefog программалық жасақтамасы бейнеленген.

Сурет 6. Icefog программалық жасақтамасы

Қорытындылай келе, қазіргі таңдағы технологиялардың қарқынды даму науқанында, көптеген адамдар компьютердегі зиянды вирустар, трояндық программалар, құрттармен кезігіп жатады, сонымен қатар, сондай зиян келтіру қаупі аса жоғары программалардың кесірінен жеке ақпараттың құпиялылығы мен қол жетімділігіне зақым келуде. Уақыт өте

келе, зиянды программалар, не зиянды вирустар болсын, техникадағы маңызды мәселелердің бірі болып қала береді. Тек, компьютер қолданушысы үшін компьютерді қорғау мақсатында антивирустық бағдарламаны орнатып, соны қолдап отырған өте маңызды болып есептелінеді.

Қолданылған әдебиеттер

1. Развитие информационных угроз во втором квартале 2016 года. Статистика [Электронный ресурс] / Сайт «securelist» – Режим доступа https://securelist.ru/analysis/malware-quarterly/29062/it- threat-evolution-in-q2-2016-statistics/.- 01.11.2016
2. Андреев, Д. А. Вирусы и риски заражения систем: обзор и построение обобщенных вероятностных моделей [Текст] / Д. А. Андреев, А. Е. Брянский // Информационная безопасность. – 2009. - №4. – С.519-536
3. Развитие информационных угроз во втором квартале 2016 года. Статистика [Электронный ресурс] / Сайт «securelist» – Режим доступа https://securelist.ru/analysis/malware-quarterly/29062/it- threat-evolution-in-q2-2016-statistics/.- 01.11.2016
4. Williamson, M. W. and Leveille, J. «An epidemiological model of virus spread and cleanup» HPL-2003-39 [Электронный ресурс] – Режим доступа: http://www.hpl.hp.com/techreports/2003/HPL- 2003-39.pdf
5. Динамические модели распространения вредоносного программного обеспечения на основе теории хаоса [Электронный ресурс]/ – Режим доступа: http://ksi.avo.ru/seminar/25.pdf
6. https://habr.com/ru/post/105964/
7. https://www.kaspersky.ru/blog/vajpery-steret-vsyo/2800/
8. https://eugene.kaspersky.ru/2012/06/14/flame-that-changed-the-world/
9. https://securelist.ru/gauss-gosudarstvennyj-kibershpionazh/2930/
10. https://habr.com/ru/post/159669/