ДОСЛІДЖЕННЯ ІМОВІРНОСТІ ВИНИКНЕННЯ РИЗИКУ ТА АНАЛІЗ ЗЛОВМИСНИХ ПРОГРАМ

Пестєрєва С. Є.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. IMI, тел. (057) 702-14-29)

The technological advances in computing devices have created great impact for wide range of application. Since computing devices may be coupled with third-party software applications, so, many security and privacy difficultiescan be stimulated by malwares.

Object of research – methods to improve safety for computer systems as for home users and business users.

The purpose of this work is a research malware and threat analysis. Build classification certain malware.

Мета роботи – дослідження тенденції розвитку зловмисних програм у світі за останні роки.

У ході роботи були розглянуті 10 актуальних вірусів (а саме GoBot2, Formbook, Joao, TrojanDownloader.FakejQuery, Remaiten, Prikormka, Mooze/AdWare.LoadMoney, Mumblehard, Aibatook) та розглянуто методи та етапи їх розповсюдження, встановлення, запуск та виконання зловмисних програм (команд)

У ході дослідження було проаналізовано 5 вірусів (GoBot2, Remaiten, Prikormka, Mooze, AdWare.LoadMoney, які мають більш обширні відомості) за такими факторами: імовірність, складність реалізації та застосовність.

Під імовірністю розуміється ймовірність підхоплень та розраховується, як 0,1 за актуальність ресурсу та 0,5 від кількості вразливостей, а саме на що він спрямован (файл, тека, виконання команд та ін.).

Під складністю реалізації розуміється необхідність наявності у порушника режиму ІБ та залежить від кількості етапів встановлення один етап має вагу 0,05, якщо встановлення вірусу потребує 4 етапи, то складність реалізації 0,2.

Під застосовністю розуміється можливість застосовувати кібератаку на рівні різних архітектур, фреймворків, операційних систем, мов програмування. В нашому випадку від актуальності операційної системи для звичайного користувача та її версії. Коефіцієнти я розділила так, що для ОС Linux=0,05; для Win32=0,1; для Win64=0,15.

Було побудовано таблицю з розрахунком імовірність виникнення ризику, яка наведена в табл. 1

Таблиця 1 – Розрахунок імовірності виникнення ризику

Фактор	Класифікатор	Коефіцієнт	Назва вірусу				
			GoBot2	Remaiten	Prikormka	Mooze	AdWare.LoadMoney
Імовірність	Актуальність						
	Торент-файл	0,05	+				
	Браузер	0,1		+	+	+	+
	Кількість вразливостей						
	Тека	0,05	+		+		
	Файл			+	+		
	Виконання файлів		+				
	Запис реєстра		+			+	
	Виконання команд					+	
	Крадіжка облікових даних			+	+		+
Сума			0,2	0,2	0,25	0,2	0,15
Складність реалізації	Кількість етапів встановлення	0,05	5	1	2	4	1
Сума			0,25	0,05	0,1	0,2	0,5
Застосовність	Операційна система						
	Linux	0,05		+			
	Win32	0,1			+	+	+
	Win64	0,15	+		+		
Сума			0,15	0,05	0,25	0,1	0,1
Загальна сума			0,6	0,3	0,6	0,5	0,3

За результатами проведеного дослідження були розглянуті різноманітні віруси та проаналізувала імовірність виникнення ризику в залежності від різних умов.

Перелік джерел:

1. SECURITY REPORT 2017/18 [Електронний ресурс] // https://www.av-test.org/en/news/. – 2018.

2. Threat Encyclopaedia [Електронний ресурс] // https://www.virusradar.com/en/threat_encyclopaedia/filter?page=. – 2019.

3. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] // Постанова Національного банку України. – 2017.