МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

УДК [004.383.2:004.738.5:378]:004.056.5

DDOS-АТАКИ НА ОСВІТНІ ВЕБ-РЕСУРСИ

КОРОЛЕВИЧ Є.М.
Наукові керівники: д.т.н., зав. кафедри ІТКБ ПЛОТНІКОВ В. М.,
директор НТБ ЗІНЧЕНКО І. І.
Одеська національна академія харчових технологій

На даний момент більшість компаній зберігає інформацію в електронному форматі на серверах. Таке зберігання даних технологій \має як переваги так, і недоліки. Одним з головних недоліків це кібератаки, адже, щороку їх кількість на веб-ресурси збільшується.

Сучасне зловмисне програмне забезпечення являє собою складну багатофункційну програмну систему та комплекс, який побудований з використанням ефективних методів створення програмних засобів та методів поширення зловмисного коду [1]. Зловмисники найчастіше використовують, для зараження жертв, декілька типів шкідливих програм одночасно[2].

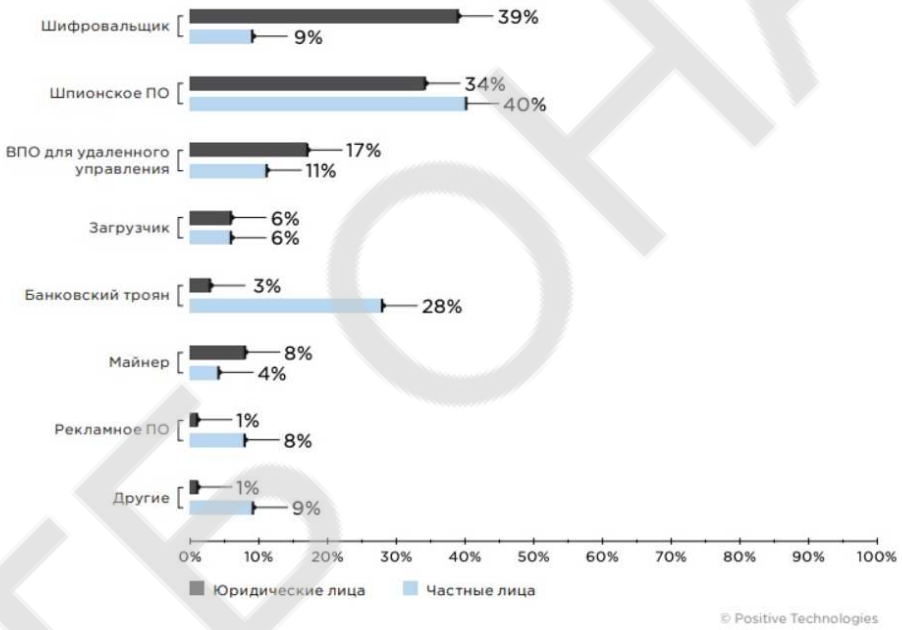

Рис. 1 *"Доля атак з використанням зловмисного програмного забезпечення"*

Сучасні атаки, які завдають великого збитку компаніям, вважаються віддаленні мережеві атаки, серед яких найбільш небезпечною є Distributed Denial of Service (DDoS-атака)[3]. DDoS-атака – «розподілена відмова в обслуговуванні» (англ. – Distributed Denial-of-service attack) – спрямована на обчислювальну систему, з метою створення таких умов, за яких користувачі системи не можуть отримати доступ до деяких ресурсів або сервісів [4].

Оскільки персональні ресурси користувачів мережі зазвичай не мають належного захисту та потужності, щоб протидіяти DDoS-атаці, тому у більшості ситуацій, в яких DDoS-атака здійснюється на особистість, вебсайт людини або ж власне персональний комп'ютер, причинами можуть бути особиста неприязнь зловмисника, розвага або ж використання особистості в якості тренувальної мішені [5].

Окремо можна говорити про використання комп'ютерів користувачів як засобу реалізації DDoS-атаки, перетворення ресурсів користувачів в так звані «зомбі-комп'ютери».

Зазвичай, «зомбування» здійснюється за допомогою троянської програми, що встановлює необхідне зловмиснику фонове завдання. В середньому, інтенсивність DDoS-атаки, що відповідає даному сценарію, складає 100 Мбіт/с. Це еквівалентно, наприклад, тому, що на сайт зайшли 1000 користувачів і вони кожну секунду оновлюють сторінку [5].

Захист від DDoS-атак розділений на три напрямки: запобігання, виявлення та реакція на атаку.

Основною метою запобігання атаці є припинення атак до нанесення нею збитків. Для цього використовують наступні типи, а саме виконують фільтрацію вхідного/вихідного трафіку та на рівні маршрутизаторів, використовують протоколи перевірки адрес джерела.

Методи виявлення атаки спрямовані на контроль та дослідження системи в якої виникають нетипові події. Є такі типи як відстеження активної взаємодії, вкладені поля, на основі хеша, сигнатурні та статистичні.

Методи реакції на атаку в яких жертва реагує на атаку після виявлення. Використовують наступні види StopIt, SIFF, TVA.

У цих методах відповідальність на виявлення і боротьбу з нападом лежить на самій жертві.

Отже, захист інформації відіграє надзвичайно важливу роль, як в забезпеченні безпеки даних підприємств, так і приватних даних користувачів. Також для автоматизації роботи фахівця з кібербезпеки можна використовувати сканери вразливості, основним завданням яких є можливість сканувати мережу для швидкого виявлення вірусу або підозрілих процесів та їх усунення.

Використання сучасних технологій для зберігання даних є зручним способом але вимагає певного комплексу засобів для захисту, але розробка в даному напрямку є дуже перспективною. Отже в майбутньому захист інформації буде ставати більш надійним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Створене посилання: Савенко О. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах : дис. на здобуття наук. ступеня доктор технічних наук : 05.13.05 : захищена 25.10.2019 : затв. naN.NaN.NaN / Савенко Олег . - Львів. - 27 с. Транслітерація: Savenko O. Teoriya ta praktika stvorennya rozpodilenikh sistem viyavlennya zlovmisnoho prohramnoho zabezpechennya v lokal`nikh komp'yuternikh merezhakh : dis. na zdobuttya nauk. stupenya doktor tekhnichnikh nauk : 05.13.05 : zakhishchena 25.10.2019 : zatv. naN.NaN.NaN / Savenko Oleh . - L`viv. - 27 s.

2. Створене посилання: Https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/ // Positive Technologies [Веб-сайт]. - URL: https://www.ptsecurity.com/ (дата звернення: 08.03.2021). Транслітерація: Https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/ // Positive Technologies [Veb-sayt]. - URL: https://www.ptsecurity.com/ (data zvernennya: 08.03.2021).

3. DDoS-атаки: реальна небезпека віртуального світу [Електронний ресурс]. – Режим доступу: http://zillya.ua/ddos-ataki-realna-nebezpeka-virtualnogo-svitu.

4. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.: ил.

5. Створене посилання: ІЄРАРХІЯ ФАКТОРІВ ТИПОВИХ СЦЕНАРІЇВ РЕАЛІЗАЦІЇ DDOS-АТАК - Київ. - 18 с. - (МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ЕКОНОМІЦІ). Транслітерація: IYeRARKhIYa FAKTORIV TIPOVIKh STSENARIYiV REALIZATSIYi DDOS-ATAK - Kiyiv. - 18 s. - (MATEMATIChNE MODELYuVANNYa V EKONOMITSI).

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.