Визначення стану захищеності кіберпростору

Алла Гаврилова
кафедра кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця
Харків, Україна
alla.gavrylova@hneu.net

Determination of cyber space security

Alla Havrylova
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Kharkiv, UKRAINE
alla.gavrylova@hneu.net

***Анотація*—проведено аналіз динаміки кіберзазгроз з точки зору виявлення підозрілих подій, кібератак та кіберінцидентів, запропановано модифікувати алгоритм гешування бази даних паролів та шифрування повідомлень електронної пошти**

***Abstract*—Analysis of the dynamics of cyber threats in terms of detection of suspicious events, cyberattacks and cyber incidents, proposed to modify the algorithm for password database hashing and encryption of e-mails**

Ключові слова—кіберзагрози, гешування, еліптичні криві, алгоритм UMAC, кіберінциденти

Keywords—cyber threats, hashing, elliptic curves, UMAC algorithm, cyber incidents

I. Вступ

Активне переведення співробітників на віддалену роботу і виведення внутрішніх сервісів компаній на мережевий периметр, обумовлені пандемією COVID-19, вплинули на ландшафт кіберзагроз у всьому світі. Лише деякі компанії, які і так практикували роботу у віддаленому режимі, були готові впоратися з усіма складнощами в забезпеченні безпеки, інші зіткнулися з нестачею часу на продумування і реалізацію всіх необхідних заходів захисту.

Зловмисники без зволікання приступили до пошуку вразливостей в сервісах на периметрах компаній, в тому числі в рішеннях, які використовуються для організації віддаленої роботи, перевіряючи їх на міцність. Так, активно експлуатувалися проломи в Pulse Secure VPN, Citrix ADC і Citrix Gateway, в міжмережевому екрані Cisco ASA. Оператори програм-вимагачів, зокрема Netwalker, Clop і REvil, користувалися уразливими сервісами для поширення свого шкідливого програмного забезпечення (ПЗ).

У зв'язку з цим актуальним є дослідження світових тенденцій кібербезпеки та визначення стану з цього питання в Україні.

II. Аналіз стану кібербезпеки в Україні

Система кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури на об’єктах моніторингу за період з початку грудня 2020 р. до кінця травня 2021 р. зафіксувала 46 787 272 підозрілих подій [1]. Розподіл підозрілих подій за групами наведено на рис. 1.

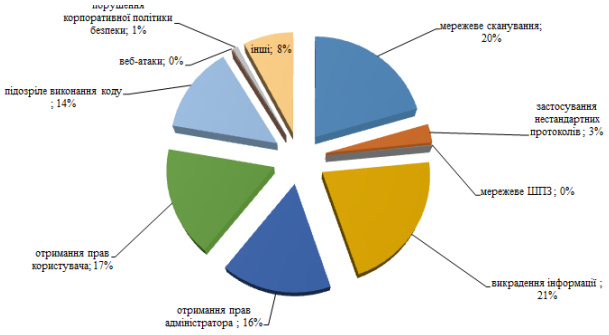

Рис. 1. Кількість підозрілих подій

Система захищеного доступу державних органів до мережі Інтернет за період з початку грудня 2020 р. до кінця травня 2021 р. заблокувала 1 125 783 атак різних видів [1]. Розподіл заблокованих кібератак за групами наведено на рис. 2.

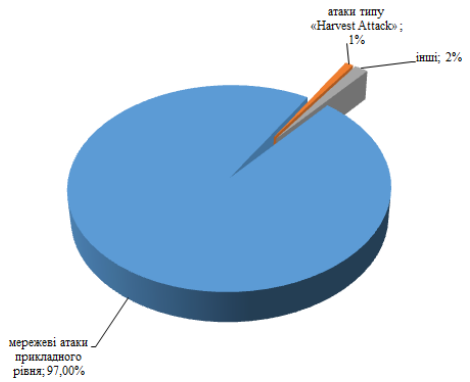

Рис. 2. Кількість кібератак

Також за цей період зафіксовано і заблоковано 287 DDoS-атак, зокрема на вебресурси Офісу Президента України та Держспецзв'язку.

За даними Держспецзв'язку з початку грудня 2020 р. до кінця травня 2021 р. урядовою командою реагування на комп'ютерні надзвичайні події України CERN-UA було виявлено 79 104 кіберінцидентів [1]. Розподіл всіх кіберінцидентів за групами наведено на рис. 3.

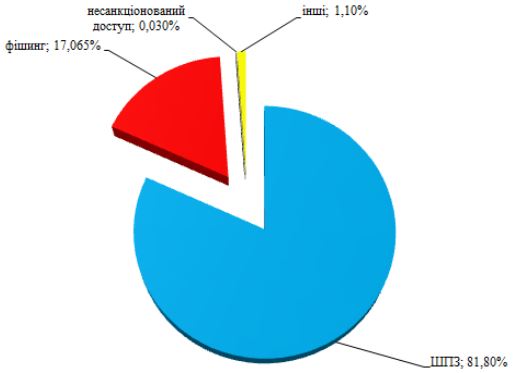

Рис.3. Кількість кіберінцидентів

Дані тенденції характерні й для кіберпростору по всьому світові. Так, в атаках на організації основними векторами доставки шкідливого програмного забезпечення (ПЗ) залишаються електронна пошта (71%) і компрометація комп'ютерів, серверів та мережевого обладнання (24%), а в атаках на приватних осіб хакери віддають перевагу електронній пошті і веб-сайтам (по 32%) [2].

Також можна зазначити, що основним джерелом виникнення кіберінцидентів є канали передачі інформації, в тому числі й електронна пошта.

При автентифікації користувачів в електронній пошті використовується гешування паролів, яке проводиться з використанням алгоритму криптографічного захисту MD5.

При роботі в постквантовому періоді даний алгоритм не володіє необхідною криптостійкістю до зломів, тому постає завдання створення нових алгоритмів або модифікації вже наявних.

При реєстрації користувача в електронній пошті, зазначений їм пароль проходить через геш-функцію і замість пароля в базу даних буде занесений отриманий геш. При кожній спробі авторизації вказаний пароль буде кожен раз проходити через геш-функцію, і отриманий геш-код буде порівнюватися з геш-кодом збереженим в базі даних, і якщо вони будуть ідентичні, то пароль користувачем було вказано вірний.

Алгоритм гешування, який вимагає досить великих ресурсів і великої кількості операцій для обчислення хешу в умовах постквантової криптографії зможе забезпечити належний рівень криптостійкості.

Модифікації, які приведуть до підвищення криптостійкості алгоритмів гешування можуть бути пов'язані з використанням крипто-кодових конструкцій (ККК) на еліптичних кодах Мак-Еліса на підставі алгоритму UMAC.

Також слід зазначити, що використання даного алгоритму може бути застосовано й для підготовки та передачі повідомлень телекомунікаційними каналами, що також повинно сприяти підвищенню рівня криптостійкості повідомлення, що передається.

III. ВИСНОВКИ

В результаті було проаналізовано тенденції щодо зростання різновидів та кількості кіберзагроз як у світові, так й в Україні за останнє півріччя. Згідно із майбутніми змінами в технічному оснащенні зловмисників та появою квантового комп'ютеру, запропоновано використання ККК на модифікованих еліптичних кривих Мак-Еліса за алгоритмом UMAC для проведення гешування при зберіганні паролів користувачів електронної пошти та шифруванні повідомлення, що передається від відправника до отримувача.

ЛІТЕРАТУРА REFERENCES

[1] Сайт Державної служби спеціального зв'язку та захисту інформації України (2021). "Оперативна інформація Держспецзв'язку щодо захисту державних інформаційних ресурсів" [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/fakhivci-derzhspeczv-yazku-z-26-travnya-po-1-chervnya-2021-roku-zablokuvali-44-9-tis-kiberatak-na-derzhavni-informaciini-resursi

[2] Угрозы кибербезопасности – 2020 (2021) Positive technologies, [Электронный ресурс]. Режим доступа:: www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020.