УДК 004.491.42

Олександр Євгенійович ПАКРИШ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

ШАНТАЖ З ВИКОРИСТАННЯМ ПРОГРАМ-ВИМАГАЧІВ І МЕТОДИ ЗАХИСТУ

Програма-вимагач (англ. ransomware) – тип шкідливого програмного забезпечення, яке блокує доступ до комп'ютерної системи або запобігає зчитуванню записаних в ній даних, а потім вимагає від жертви викуп для відновлення початкового стану.

Програми-вимагачі шифрують інформацію жертви, що потенційно може призвести до незворотної втрати даних.

Малий та середній бізнес найбільше вразливий щодо атак за допомогою ransomware. Статистика останніх років оцінює середній розмір викупу за кожен інцидент у 2500 доларів США [1]. Тільки у США атаки програм-вимагачів за 2019 рік коштували біля 7,5 мільярдів доларів.

Не зважаючи на те, що більшість фахівців з питань інформаційної безпеки вважають сплату викупу поганою ідеєю, майже 40% жертв вибирають цей шлях [2].

При цьому, згідно з дослідженнями [3], майже 33 відсотки компаній, які сплачують викуп, не отримують доступ до своїх даних.

Ускладнює проблему програм-вимагачів те, що розробка деяких з них (зокрема WannaCry та NotPetya) фінансувалась, можливо, на державному рівні [4]. Ці програми маскувались під ransomware, але мали на меті незворотнє знищення інформації, а не отримання фінансової вигоди.

Загальний алгоритм злочинного використання програми-вимагача становить послідовність наступних кроків:

1. Інфікування комп'ютера жертви під час відкриття шкідливого вкладення, що розповсюджується шляхом спам-розсилки, або під час відвідування вебсторінки, яка інфікована пакетами експлойтів.

2. Потрапивши на комп'ютер жертви, програма-вимагач зберігає себе на жорсткому диску та створює ключ автозавантаження в реєстрі

для забезпечення власного запуска під час старту системи. Після цього програма шукає на диску файли за певним шаблоном та здійснює їх шифрування.

3. Програма-вимагач встановлює зв'язок з командним центром (сервером C&C) та інформує жертву про факт шифрування її файлів та щодо розміру і порядку передачі викупу. Більшість програм-вимагачів використовує для зв'язку з C&C сервером анонімні мережі

4. Після переведення коштів, жертва, в ідеалі, отримує ключ для розшифровки файлів. Для оплати зазвичай використовують одну з криптовалют (найчастіше біткоін).

Використання анонімних мереж та криптовалют забезпечує анонімність зловмисника і робить проблематичним притягнення його до відповідальності.

Епідемія коронавірусу викликала велику кількість спам-розсилок, що містять ransomware, та тематично пов'язані з питаннями пандемії. Також кіберзлочинці масово реєструють домени, пов'язані з пандемією та використовують їх для кібератак. Наприклад, зовсім анекдотичний сайт antivirus-covid19.site пропонував завантажити і встановити на свій комп'ютер програмне забезпечення Corona Antivirus для захисту від зараження [5].

Таким чином, виходячи з вищезазначеного, основні зусилля щодо захисту від програм-вимагачів пропонується зосередити, по-перше, на створенні умов, в яких програма-вимагач не зможе інфікувати комп'ютер, по-друге, на забезпеченні резервного копіювання критичної інформації [6]. Цього можна досягти, виконуючи наступні заходи:

- своєчасне оновлення операційної системи, браузерів та антивірусних баз;
- упереджене ставлення до вкладень листів електроної пошти та невідомих вебсайтів. Використання ресурсу VirusTotal для перевірки підозрілих файлів та вебадрес;
- контроль за мережевими підключеннями і дозвіл мережевого обміну тільки довіреним програмам (деякі програми-вимагачі починають шифрування тільки після встановлення зв'язку з C&C сервером);
- присвоєння атрибуту «тільки для читання» файлам, які не повинні змінюватись;

– організація резервного копіювання засобами, які не входять до складу операційної системи. При цьому права доступу до резервних копій повинні мати тільки програми резервного копіювання (для виключення можливого шифрування файлів резервних копій).

Список бібліографічних посилань

1. Cook S. 2018-2020 Ransomware statistics and facts // Comparitech Limited. 24.01.2020. URL: https://www.comparitech.com/antivirus/ransomware-statistics/ (дата звернення: 26.04.2020).
2. Understanding the Depth of the Global Ransomware Problem : survey report // Osterman Research, Inc. August 2016. URL: https://www.malwarebytes.com/pdf/white-papers/UnderstandingTheDepthOfRansomwareIntheUS.pdf (дата звернення: 26.04.2020).
3. Paying for ransomware could cost you more than just the ransom // Trend Micro Incorporated. 22.03.2017. URL: https://blog.trendmicro.com/paying-for-ransomware-could-cost-you-more-than-just-the-ransom/ (дата звернення: 26.04.2020).
4. Hern A. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 // Guardian News&Media Limited. 30.12.2017. URL: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (дата звернення: 04.04.2020).
5. Как киберпреступники используют пандемию коронавируса в своих целях // ХАБР : сайт. 24.04.2020. URL: https://habr.com/ru/company/trendmicro/blog/498854/ (дата звернення: 04.04.2020).
6. Дроботун Е. Б. Анализ активности и тенденций развития вредоносных программ типа «блокиратор-шифровальщик файлов». *Программные продукты и системы*. 2016. № 2 (114). С. 77–81.

Одержано 27.04.2020