УДК 004.56

А. Є. Москаленко
Л. М. Куперштейн

АНАЛІЗ ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ПРОГРАМ-ВИМАГАЧІВ ТА МЕТОДИ ЙОГО ВИЯВЛЕННЯ

Вінницький національний технічний університет

Анотація

Розглянуто принципи функціонування програм-вимагачів, що полягають у шифруванні файлів користувача та вимозі викупу за їх розшифрування. Методи виявлення включають спостереження за змінами розширень файлів, активністю центрального процесора та мережевим зв'язком. Для захисту від цих загроз важливо використовувати антивірусне програмне забезпечення, частіше створювати резервні копії даних та бути обережними з електронною поштою та вкладеннями.

Ключові слова:

Принципи, програма-вимагач, ransomware, метод, виявлення, захист, шкідливе ПЗ.

Abstract

The principles of the functioning of ransomware, which consist in encrypting user files and demanding a ransom for their decryption, are considered. Detection methods include monitoring file extension changes, CPU activity, and network traffic. To protect against these threats, it's important to use antivirus software, back up your data more often, and be careful with email and attachments.

Keywords:

Principles, ransomware, ransomware, method, detection, protection, malware.

Вступ

Програма-вимагач – це шкідлива програма, яка шифрує файли в комп’ютерних системах, роблячи їх непридатними для використання [1]. Зловмисники зазвичай погрожують назавжди заблокувати зламані системи або оприлюднити конфіденційні дані, якщо викуп не буде сплачено [1]. Оператори програм-вимагачів шифрують файли та пропонують своїм жертвам ключ розшифрування в обмін на оплату, як правило, у криптовалютах, таких як біткойн (BTC), щоб ускладнити відстеження незаконних коштів [2].

Вперше програма-вимагач була виявлена в 1989 році [6]. Шкідлива програма отримала назву AIDS Trojan. Вона поширювалася через тисячі дискет, які містили інтерактивну базу даних про СНІД і фактори ризику, пов'язані з хворобою. Після запуску шкідлива програма фактично зробила неможливим доступ користувача до більшої частини вмісту на диску.

На даний момент програми-вимагачі є великою та складною проблемою у всьому світі. За даними Gartner, частка країн, які мають закони, що регулюють виплати викупу, штрафи та переговори, збільшиться з менш ніж 1% у 2021 році до 30% до кінця 2025 року [1] . Програми-вимагачі несуть в собі не тільки репутаційні втрати, а й фінансові, наприклад станом до 2031 року вартість програм-вимагачів досягне 265 мільярдів доларів на рік [2].

Результати досліджень

До найпопулярніших методів зараження комп’ютера програмами-вимагачами можна віднести зараження за допомогою соціальної інженерії, такої як фішинг [3]. Також зараження може відбутися через фейковий веб-сайт або ж через додатки, в яких потребується внесення особистих даних. Також варто зазначити, що зростає кількість атак через програми-вимагачі за допомогою віддаленого робочого столу (RDP) [7].

Для того щоб виявити програми-вимагачі потрібно спостерігати за своїм комп’ютером, робочим столом, персональними даними та програмами. Першою ознакою, що ПК заражено є зміна розширень файлів [2]. Також варто звернути увагу на активність центрального процесора, тому що шифруючи дані, програми-вимагачі знижують його швидкодію. Ознакою ще може бути ненормальний мережевий зв’язок, тобто низька, ніж зазвичай, швидкість передачі даних .

Загальний принцип роботи програм-вимагачів полягає в наступному [7]. Спершу відбувається впровадження програми-вимагача в комп’ютер за допомогою фішингових електронних листів, фішингових сайтів, сторонніх додатків. Далі відбувається шифрування даних на жорсткому диску для порушення їх доступності легітимному користувачу. Уже після того, як

уся інформація зашифровані, відбувається вимога викупу в обмін на можливість повернути оригінальні дані. Якщо викуп оплачено, то зловмисники надають можливість розшифрування, але таке буває не завжди. Навіть після оплати злочинці і надалі можуть вимагати кошти.

До визнаних і відомих штамів програм-вимагачів належать Ryuk, NotPetya, Cl0P, Royal та ін. [2]. Cybersecurity Ventures щоквартально відстежує близько 100 банд і штамів програм-вимагачів.

Одним з прикладів програм-вимагачів є WannaCryptor. У травні 2017 року програма-вимагач WannaCryptor або WannaCry швидко розповсюдилася, використовуючи есплойт EternalBlue [3]. Останній використовував вразливість у найпопулярніших версіях операційних систем Windows. Незважаючи на те, що Microsoft випустила виправлення для багатьох вразливих операційних систем більше ніж за два місяці до атаки, файли і системи тисяч організацій у всьому світі постраждали від цього шкідливого програмного забезпечення. Таким чином ця загроза спричинила втрат на суму мільярд доларів.

Ще одна програма-вимагач Petya – мережевий хробак, що вражає комп'ютери під керуванням Microsoft Windows. Перші різновиди вірусу було виявлено у березні 2016 року [4]. 27 червня 2017 року Україна зазнала наймасштабнішої кібератаки в своїй історії. Починаючи з 11:30, комп'ютерні системи українських компанії та установ одна за одною відключалися через ураження невідомим вірусом. У перший день атаки постраждали комп'ютери Кабміну, Мінінфраструктури, Чорнобильської АЕС, Податкової служби, держконцерну Антонов, Ощадбанку та Укртелекому, аеропортів Бориспіль і Жуляни, Укргазвидобування, WOG, ДТЕК, Укрпошти, Укррічфлоту, київського метрополітену, Київенерго, Нової Пошти, Укрзалізниці, медіагруп Інтер, 24 і ICTV та сотні інших компаній і банків [4]. Усього жертвами атаки стали понад дві тисячі установ. За декілька днів вірус заразив більше мільйона комп'ютерів по всьому світу. Найбільш серйозного удару зазнали США, Німеччина та Польща. У Білому домі збитки від кібератак вірусу Petya оцінили у 10 мільярдів доларів [4].

Загальні підходи та рекомендації до захисту від програм-вимагачів [5]:

- Резервне копіювання даних комп’ютера. Потрібно частіше створювати резервні копії системи та інших важливих файлів і регулярно перевіряти резервні копії. Якщо ваш комп’ютер заражений програмою-вимагачем, ви можете відновити систему до попереднього стану за допомогою резервних копій;
- Зберігайте резервні копії окремо. Найкраще зберігати резервні копії на окремому пристрої, до якого неможливо отримати доступ із мережі, наприклад на зовнішньому жорсткому диску. Після завершення резервного копіювання обов’язково від’єднайте зовнішній жорсткий диск або окремий пристрій від мережі чи комп’ютера;
- Потрібно обережно відкривати вкладення електронної пошти. Будьте обережні, відкриваючи вкладення електронної пошти, навіть від відправників, яких ви вважаєте знайомими, особливо якщо вкладення є стисненими файлами або файлами ZIP;
- Встановлюйте програмне забезпечення для захисту. Антивірусне програмне забезпечення та програмне забезпечення для захисту від кінцевих точок можуть допомогти виявити та заблокувати програми-вимагачі;
- Оновлюйте своє програмне забезпечення. Потрібно встановити всі оновлення програмного забезпечення, щоб закрити вразливості, які можуть бути використані програмами-вимагачами;
- Навчання користувачів та працівників. Навчання користувачів тому, як розпізнавати та уникати програм-вимагачів та і в загальному протидії шкідливому ПЗ, може допомогти запобігти зараженню;

Висновки

Програми-вимагачі – це серйозна загроза, яка може мати критичні наслідки для приватних осіб та підприємств. Програми-вимагачі можуть заблокувати доступ до важливих файлів, призвести до втрати даних та до фінансових втрат. Захист від них – це постійна задача, тому важливо бути в курсі нових загроз та регулярно оновлювати свої методи захисту та виконувати базові рекомендації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Kind of Financial Impact Can Ransomware Command? Електронний ресурс] – Режим доступу: https://www.armis.com/faq/how-much-money-does-ransomware-make/ (дата звернення 06.04.2024)

2. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 Електронний ресурс] – Режим доступу: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (дата звернення 06.04.2024)
3. Програми-вимагачі [Електронний ресурс] – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/programma-vymogatel/ (дата звернення 25.03.2024)
4. США пропонують $10 млн за інформацію про організаторів кібератаки NotPetya Електронний ресурс] – Режим доступу: https://suspilne.media/233011-ssa-proponuut-10-mln-za-informaciu-pro-organizatoriv-kiberataki-notpetya/ (дата звернення 06.04.2024)
5. Protecting Against Ransomware Електронний ресурс] – Режим доступу: https://www.cisa.gov/news-events/news/protecting-against-ransomware (дата звернення 06.04.2024)
6. Троян [Електронний ресурс] – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/#:~:text=Одним%20з%20перших%20відомих%20троянів,інтерактивну%20базу%20даних%20про%20СНІД. (дата звернення 02.05.2024)
7. Все, Що Потрібно Знати про Програми-вимагачі (Ransomware) в 2022: Гайд Рекомендацій [Електронний ресурс] – Режим доступу: https://gridinsoft.ua/blogs/vse-scho-potribno-znaty-pro-programy-vymagachi-ransomware/ (дата звернення 02.05.2024)

Москаленко Аліна Євгеніївна- студентка групи 1БКС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: moskalenkoalina56@gmail.com

Moskalenko Alina Evgeniivna- student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: moskalenkoalina56@gmail.com

Куперштейн Леонід Михайлович-доцент кафедри захисту інформації, Вінницький національного технічного університет, Вінниця, e-mail: kupershtein@vntu.edu.ua

Kupershtein Leonid Mykhailovych - associate professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kupershtein@vntu.edu.ua