COLLECTION OF SCIENTIFIC PAPERS
SCIENTIA

MAY, 2022

VILNIUS, REPUBLIC OF LITHUANIA

INTERDISCIPLINARY RESEARCH: SCIENTIFIC HORIZONS AND PERSPECTIVES

III INTERNATIONAL SCIENTIFIC AND THEORETICAL CONFERENCE

VOLUME 2

EUROPEAN SCIENTIFIC PLATFORM

DOI 10.36074/scientia-06.05.2022 ISBN 979-8-88526-814-1 *00002*

COLLECTION OF SCIENTIFIC PAPERS
SCIENTIA

6 May, 2022

Vilnius, Republic of Lithuania

INTERDISCIPLINARY RESEARCH: SCIENTIFIC HORIZONS AND PERSPECTIVES

III International Scientific and Theoretical Conference

VOLUME 2

Vilnius, 2022

CONTENT

SECTION 18.
INFORMATION TECHNOLOGIES AND SYSTEMS

Пашнев Дмитро Валентинович
Провідний науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

Демидов Захар Георгійович
Старший науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

АТАКА КРИПТОВАЛЮТНОГО СЕКТОРУ APT-ГРУПОЮ LAZARUS

У середині грудня 2021 року було помічено підозрілий файл, завантажений на VirusTotal[1]. На перший погляд він виглядав, як додаток для роботи з децентралізованими фінансами (DeFi)[2]. Однак при більш ретельному аналізі з'ясувалося, що файл запускає ланцюжок зараження. При запуску програма поміщає в систему і шкідливий файл, і інсталятор легітимної програми. Шкідлива програма виконується за допомогою шляху до протрояненого установника. Потім створений бекдор[3] замінює протроянений додаток на легітимний, щоб приховати сліди першого. Проаналізувавши функції цього бекдору, було виявлено численні збіги з іншими інструментами групи Lazarus[4].

APT-група Lazarus спеціалізується насамперед на отриманні фінансової вигоди. Останнім часом криптовалютний бізнес є її основною метою. У міру того, як вартість криптовалют зростає, а невзаємозамінні токени (NFT)[5] і децентралізовані фінанси (DeFi) привертають все більше уваги, Lazarus продовжує активно атакувати криптовалютний сектор.

Конкретно для цієї атаки оператор шкідливого програмного забезпечення використовував виключно скомпрометовані веб-сервери, розташовані в Південній Кореї. Інфраструктура серверів налаштована для атаки на кілька етапів. Сервери першого етапу поширюють бекдор, а ціль серверів другого етапу - зв'язок з імплантами. Така схема й у інфраструктури Lazarus.

Хоча досі не зрозуміло, як саме зловмисники змушують жертву запускати протроянений додаток (0b9f4612cdfe763b3d8c8a956157474a), припускається, що для цього вони використовують цільові листи фішингу або повідомлення в соціальних мережах. Протроянена програма запускає ланцюжок зараження. Інсталяційний пакет маскується під програму DeFi Wallet і містить легітимний двійковий файл та шкідливий інсталяційний файл.

Після виконання інсталяційний файл отримує розташування шкідливої програми наступного етапу (C: ProgramData \ Microsoft Google Chrome.exe) і дешифрує його за допомогою операції XOR з однобайтовим ключем 0x5D. Під час підготовки до наступного етапу зараження інсталяційний файл записує перші 8 байт, включаючи заголовок MZ, у файл GoogleChrome.exe і витягує решту 71 164 байтів із секції .data протрояненої програми.

Потім створений зловред завантажує ресурс CITRIX_MEETINGS зі свого тіла та зберігає його за адресою :\ProgramData\Microsoft\CM202025.exe. Отриманий файл є легітимною програмою DeFi Wallet. Нарешті, інсталятор виконує раніше створену шкідливу програму, використовуючи ім'я файлу як параметр:

C:\ProgramData\Microsoft\GoogleChrome.exe "[поточне ім'я файлу]"

Зловред (d65509f10b432f9bbeacfc39a3506e23), згенерований вказаною вище протроянеою програмою, маскується під нешкідливий браузер Google Chrome. Після запуску зловред перевіряє, що він був запущений з аргументом, перш ніж почати копіювати легітимну програму C:\ProgramData\Microsoft\CM202025.exe за адресою, представленою у вигляді параметра командного рядка, тобто переписує вихідний протроянений установник. Найімовірніше це спроба приховати сліди присутності цього установника. Потім зловред виконує легітимний файл, щоб приспати пильність жертви, демонструючи процес встановлення невинної програми. Коли користувач запускає нову програму, він бачить програмне забезпечення DeFi Wallet з відкритим кодом. Потім зловред ініціалізує конфігураційні дані, які складаються з прапорів, адрес командних серверів, значення ідентифікатора жертви та значення часу.

Зловред випадковим чином вибирає адресу командного сервера і відправляє на нього сигнал. Цей сигнал є жорстко прописаним і незашифрованим значенням типу DWORD 0x60D49D94. Відповідь від сервера містить те саме значення. Якщо від командного сервера надходить очікуване значення, зловред починає працювати як бекдор. Наслідуючи подальші вказівки командного сервера, бекдор шифрує дані з використанням заздалегідь заданого методу. Для шифрування використовується алгоритм RC4 та жорстко заданий ключ 0xD5A3. Після шифрування дані додатково кодуються методом base64. Бекдор генерує параметри POST із жорстко заданими іменами. Тип запиту (msgID), ідентифікатор жертви та випадково згенероване значення об'єднуються у параметр jsessid. Зловред також створює параметр cookie, в якому містяться чотири випадковим чином згенерованих чотирибайтових значення. Ці значення також шифруються за алгоритмом RC4 з додатковим кодуванням base64. Аналізуючи скрипт командного сервера, було помічено, що зловред використовує як параметр jsessid, а й параметр jcookie. Залежно від відповіді командного сервера, бекдор виконує ту чи іншу приховану дію, спрямовану на збір системної інформації або керування зараженим комп'ютером.

Вважається, з високим ступенем упевненості, що це шкідливе ПЗ пов'язане з групою Lazarus, тому що виявився схожий зловред у кластері шкідливого ПЗ CookieTime (японський центр JPCERT назвав LCPDot). Донедавна кластер активно використовувався групою Lazarus. Бекдор, виявлений у ході останнього розслідування, і знайдений раніше протроянений додаток практично ідентичні. Серед іншого вони використовують один і той же метод зв'язку з командним сервером, одні й ті ж функції бекдору, процедуру генерування випадкових чисел і той самий метод шифрування даних підключення. Цей зловред також згадується у звіті Ahnlab, який розглядає його зв'язок з CookieTime (LCPDot).

У свою чергу з'ясувалося, що кластер CookieTime пов'язаний із кластерами Manuscrypt та ThreatNeedle, які також приписують групі Lazarus. Це стосується не тільки бекдору, але й скриптів командних серверів, які демонструють кілька збігів з кластером ThreatNeedle. У скриптах командних серверів виявились майже всі імена функцій та змінних, а це означає, що оператори повторно використовували базу коду та сгенеровані скрипти командних серверів для шкідливого програмного забезпечення.

Під час попереднього розслідування з'ясувалося, що гурт BlueNoroff, теж пов'язаний з Lazarus, скомпрометував DeFi-гаманець MetaMask. Як продемонстрував останній випадок, групи Lazarus та BlueNoroff намагаються доставити своє шкідливе ПЗ, не привертаючи до нього уваги, та використовують для залучення жертв витончені методи.

Галузь криптовалют та блокчейн-технологій продовжує розвиватися та залучати нові інвестиції. Тому вважається, що інтерес групи Lazarus до неї, як основного джерела прибутку найближчим часом не зменшиться.

Список використаних джерел:

1. Virustotal. Вилучено з: https://uk.wikipedia.org/wiki/ Virustotal
2. Хелен Санс(2022).Что такое DeFi и в какие токены стоит вложить деньги в 2022 году. Вилучено з: https://mc.today/defi
3. Бекдор. Вилучено з: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bekdor/
4. Lazarus. Вилучено з: https://uk.wikipedia.org/wiki/Lazarus
5. Еліна Редіх(2021). Що таке NFT-токени та чому їх купують за тисячі доларів. Вилучено з: https://biz.censor.net/resonance/3260812/scho_take_nfttokeni_ta_chomu_h_kupuyut_za_tisyach_dolarv