МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНУ “ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ”
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
АСОЦІАЦІЯ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ
ПРИВАТНОЇ ФОРМИ ВЛАСНОСТІ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Матеріали

IX Міжнародної науково-практичної конференції

30 березня 2023 р.

Київ
Європейський університет
2023

УДК: 004(063)

Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали IX Міжнарод. наук.-практ. конф., Київ, 30 березня 2023 р. / Редкол.: О. І. Тимошенко та ін. – К.: Вид-во Європейського університету, 2023. – 122 с.

Збірник містить матеріали IX Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації».

Матеріали друкуються за редакцією авторів

ЗМІСТ

моніторинг та фіксацію російської дезінформаційної діяльності, є основними результатами.

Список використаних джерел:

1. Vysotska Olena, Davydenko Anatolii, «Dodatkowe uwierzytelnianie uprawnionych użytkowników według geometrii ich twarzy w systemach informatycznych wykorzystujących technologię single sign-on», XI edycja Konferencji «Inżynier XXI wieku», Part of the Monograph «Przetwarzanie, transmisja i bezpieczeństwo informacji» (10 grudnia 2021), Bielsko – Biała, Polska, 2021, S. 257-268. DOI: https://doi.org/10.53052/9788366249868.27
2. Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов, А.М. Давиденко Управління проектами захисту інформації. Лабораторний практикум для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпека». – К.: НАУ, 2022. – 84 с.
3. Vysotska O., Davydenko A. Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. Advances in Intelligent Systems and Computing, 2020, 938, p. 356–368
4. Патент UA 150034 U; G06N 3/04; Базовий елемент для побудови нейронної мережі, здатної адаптуватися / Давиденко А.М.; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України. – заяв. u 2021 04761, 20.08.2021 р. – Опубл. 22.12.2021, Бюл. № 51.

АНАЛІЗ КІБЕРЗАГРОЗ НА ПОЧАТКУ РОКУ

Демидов З.Г.,
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі,
Хлестков О.В.,
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі,
Харківський національний університет внутрішніх справ

Зловмисники часто використовують поштові розсилки для поширення шкідливого програмного забезпечення (ПЗ). Кількість виявлених у поштовому трафіку вкладень більшою мірою залежить від активності та наполегливості атакуючих і меншою – від дій користувачів: у цій статистиці реєструється факт виявлення листа, що містить шкідливе вкладення, а не спроба його запуску користувачем. Оскільки масові розсилки шкідливого ПЗ відбуваються хвилями, на великому проміжку часу кількість спрацювань поштового компонента то зростає, то падає, хоча має неяскраво виражений висхідний тренд.

У березні цього року захисні рішення компаній виявили рекордну кількість шкідливого програмного забезпечення у поштовому трафіку користувачів – понад 19 мільйонів спрацьовувань. Щоб визначити причину цього зростання, було проаналізовано, які саме файли зробили найбільш значний внесок. Як з'ясувалося, березневий пік у сукупній кількості виявленого шкідливого програмного забезпечення збігся зі збільшенням числа шкідливих офісних документів.

Якщо кількість шкідливих виконуваних файлів, виявлених у поштовому трафіку в березні, збільшилася приблизно на 14% відносно лютого, то кількість шкідливих документів за той же період зросла приблизно вдвічі і виявилася майже на три з половиною мільйони більше, ніж у середньому з травня 2022 року до лютого 2023-го. Тобто саме розсилки з документами спричинили березневий пік.

Розглянемо докладніше, які шкідливі файли розповсюджували поштою у перші майже три місяці 2023 року. Оцінюючи розподілу файлів ми використовуємо поняття «платформи» – середовища, у якому виконується шкідливий програмний код. За цей період в поштовому трафіку було зафіксовано ВПЗ для приблизно п'ятдесяти різних платформ. Розглянемо декілька найпоширеніших із них.

Перше місце ділять платформи, що відносяться до PE-файлів, та скрипти, що виконуються, такі як JavaScript і VisualBasicScript. В обох випадках як вкладення до листа розсилаються файли, що виконуються. Це найбільш простий спосіб атаки, і незважаючи на те, що багато поштових клієнтів і шлюзів блокують такі листи або забороняють запуск таких вкладень, зловмисники продовжують його масово використовувати – майже в половині випадків з 60 мільйонів шкідливе ПЗ в пошті являло собою звичайний PE-файл, що виконується.

На другому місці опинилися шкідливі офісні документи – на них припало близько чверті всіх спрацювань поштових компонентів захисних рішень із початку цього року. За цей період рішення виявили близько 1,9 мільйонів унікальних файлів цього типу. Останні кілька років зловмисники активно використовують офісні програми під час проведення масових атак на користувачів. Зараз розсилання шкідливих офісних документів – це один із основних способів зараження пристрою жертви.

Далі йде платформа Multi – переважно це спрацювання хмарної технології детектування UrgentDetectionSystem. Також сюди потрапляє мультиплатформне шкідливе програмне забезпечення.

Потім у списку йде різне програмне забезпечення: PDF-файли, файли на мові Java, ярлики і т. д., що демонструє широкий спектр засобів, що використовуються зловмисниками.

Тепер подивимося на конкретні загрози, з якими найбільше користувачів зіткнулося. Оскільки офісні документи становлять значну частку шкідливих вкладень, ми відзначимо найпоширеніші загрози цього.

Можна виділити дві групи загроз, що використовують офісні програми: документи, що експлуатують різні вразливості в офісному ПЗ (експлойти) [1], а також документи, що містять шкідливі.

Найчастіше зловмисники намагаються експлуатувати щодо старих вразливостей 2017–2018 років: CVE-2018-0802 та CVE-2017-11882. В обох випадках експлуатація полягає у підготовці атакуючими спеціальних конструкцій, що викликають переповнення стека при обробці в редакторі формул з офісного пакету, що дозволяє виконати в системі довільний код. Обидві вразливості виправлені вже кілька років тому, але, як бачимо, ними все ще активно намагаються скористатися. Зазначимо однак, що хоча в масових атаках поширені старі вразливості, в цільових атаках для зловмисників привабливішими виглядають нещодавно виправлені вразливості та вразливості нульового дня.

До другої групи документів відносяться ті, в яких шкідливі дії здійснюються не внаслідок експлуатації вразливостей, а за рахунок виконання офісним програмним забезпеченням макросів VBA або Excel, що містяться в документі. Зловмисники можуть поєднувати різні макроси в одному документі, обфузувати їх та використовувати додаткові техніки, наприклад, завантаження шаблонів. У більшості випадків документи з макросами завантажують на комп'ютер користувача основне корисне навантаження – інше ВПЗ, яке може належати до будь-якої родини і, відповідно, нести в собі будь-яку функціональність (бекдори, банери, шифрувальники і т.п.). Останнім часом найчастіше такі документи завантажують ВПО сімейства Emotet [2] і є основним способом поширення цієї, можливо, найактуальнішої загрози останніх років – документи, що містять характерні макроси і які детектуються як Trojan.MSOffice.Emotet.gen. Проте зловмисники використовують офісні документи, як вектор розповсюдження далеко не лише цієї родини. Наприклад, цей спосіб застосовується і для розсилки IcedID і Qbot. Також документи з макросами регулярно використовують у цільових атаках, наприклад угрупуванням ScarCruft.

Можна також виділити ще один тип шкідливих документів, що статистично менш поширений і тому не потрапив у TOP 15 поштових загроз. Такі документи не містять експлойти та макроси, але вимагають від користувача виконати якусь дію – наприклад, перейти на посилання в документі, що веде на шкідливий або фішинговий сайт.

Найчастіше поштові компоненти захисних рішень виявляли шкідливі документи в Італії, В'єтнамі та Мексиці. Загалом атаки такого типу відбуваються по всьому світу, у всіх регіонах.

Розсилка шкідливих файлів офісних форматів є одним із найбільш поширених серед зловмисників способів зараження в останні роки, причому вже звично велика кількість таких атак продовжує зростати. Шкідливі документи використовуються, як у масових розсилках «навмання», так і у цільових атаках.

Для захисту від атак через електронну пошту, зокрема з використанням шкідливих документів, компаніям рекомендується:

• використовувати надійне захисне рішення на рівні поштового шлюзу, так і на робочих станціях;

• встановлювати необхідні оновлення безпеки для офісного програмного забезпечення, щоб знизити ризик експлуатації вразливостей зловмисниками;

• навчати працівників правилам інформаційної безпеки, регулярно проводити тренінги, у тому числі, присвячені безпечному поводженню з електронною поштою.

Звичайним користувачам рекомендується з підозрою ставитись до посилань і вкладень у листах, особливо якщо вони прийшли з незнайомої адреси.

Список використаних джерел:

1. Експлойт https://uk.wikipedia.org/wiki/%D0%95%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82
2. Що таке шкідливе програмне забезпечення Emotet і як його видалити з Mac (2021) https://blog.webtech360.com/uk/macos/%D1%89%D0%BE%D1%82%D0%B0%D0%BA%D0%B5-%D1%88%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%B5%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5%D0%B7%D0%B0%D0% B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0% BD%D0%BD%D1%8F-emotet-%D1%96-%D1%8F%D0%BA-%D0%B8%D0%BE%D0%B3%D0%BE%D0%B2%D0%B8%D0%B4%D0%B0%D0%BB%D0%B8%D1%82%D0%B8-%D0%B7-mac-2021/77700407

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Діденко О.В.,
курсант ІІ курсу
Харківського національного університету внутрішніх справ
Світличний В.А.,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ

Побудова інформаційного суспільства є стратегічною метою провідних держав світу: США, Японії, Канади, а також країн-учасниць Європейського Союзу. Розуміючи актуальність та важливість розвитку інформаційної сфери як запоруки конкурентоспроможності, дедалі більше країн обирають аналогічну стратегію, зокрема і Україна.

За даними міжнародного рейтингу конкурентоспроможності держав у цифровому середовищі – World Digital Competitiveness Ranking, Україна в 2021 році посіла 54 місце. Порівняно з 2020 роком показник покращився на чотири