Українці масово отримують небезпечні листи

Читать на русском

Українці масово отримують небезпечні листи

В Україні виявлено нову хвилю кіберзагроз, спрямованих на державні органи, через масове поширення шкідливих електронних листів. Громадянам варто бути особливо уважними до підроблених листів, пов'язаних із сервісами Amazon, Microsoft.

Це повідомляє CERT-UA. Зловмисники використовують теми, пов'язані з інтеграцією сервісів Amazon, Microsoft та впровадженням архітектури "нульової довіри" (Zero trust architecture, ZTA), щоб заманити жертв у пастку.

Один з основних механізмів атаки передбачає використання підроблених електронних листів, які відправляють від імені нібито Генштабу Збройних сил України. У таких листах міститься посилання на сторонній вебсайт, де пропонується завантажити "наказ" чи інші документи. Однак замість безпечних файлів користувач отримує виконуваний файл, що активує шкідливу програму RomCom на комп'ютері.

CERT-UA вказує на можливий зв'язок цієї активності з діяльністю хакерської групи Tropical Scorpius, відомої також як UNC2596. Вона відповідальна за розповсюдження Cuba Ransomware – одного з найнебезпечніших типів програм-здирників, що блокує доступ до файлів користувачів і вимагає викуп за їх відновлення. Ця група використовує шкідливу програму RomCom, яка надає віддалений доступ до системи жертви, дозволяючи зловмисникам красти інформацію та контролювати інфіковані пристрої.

Шкідлива програма, яка запускається після натискання на небезпечне посилання, проходить кілька етапів зараження системи. Після завантаження файла AcroRdrDCx642200120169_uk_UA.exe, що виглядає наче звичайне оновлення програмного забезпечення, на комп'ютері запускається програма, що активує файл "rmtpak.dll". Цей файл дозволяє хакерам отримати доступ до внутрішніх систем жертви, керувати комп'ютером віддалено, копіювати дані та встановлювати додаткові шкідливі програми.

Для виявлення потенційних загроз на комп'ютерах постраждалих CERT-UA публікує індикатори компрометації, які містять назви файлів, хеші та IP-адреси, пов'язані з кібератакою. Зокрема, серед індикаторів компрометації було зафіксовано файли з назвами "Наказ_309.pdf" та "AcroRdrDCx642200120169_uk_UA.exe", а також IP-адреси, пов'язані зі шкідливою активністю: 45[.]158.38.74, 69[.]49.231.103 та інші.

Щоб захистити свої системи, фахівці з кібербезпеки рекомендують вживати низку технічних заходів. Зокрема:

- блокування RDP-з'єднань – закриття можливості віддаленого доступу через RDP протокол зі зовнішніх джерел;
- блокування шкідливих файлів – налаштування поштових шлюзів для блокування файлів ".rdp", які можуть бути використані для віддаленого підключення;
- мережевий моніторинг – перевірка мережевого трафіку на наявність підозрілих з'єднань з зазначеними у попередженнях CERT-UA IP-адресами.

У разі виявлення індикаторів компрометації або підозрілої активності слід негайно звернутися до IT-відділу або фахівців з кібербезпеки. Важливо ізолювати інфіковані системи та негайно розпочати перевірку всієї мережі на наявність інших потенційних загроз. Також потрібно дотримуватись основних правил безпеки, зокрема регулярно оновлювати програмне забезпечення та уникати відкриття підозрілих електронних листів.

Теги: кібератаки | Кибератаки | Письма | листи

Софія Ковальчук
РЕДАКТОРКА СТРІЧКИ НОВИН

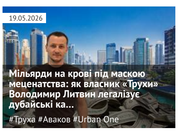
25 жовтня 2024 г., 07:38 | Переглядів: 3178 | Коментарі: 0

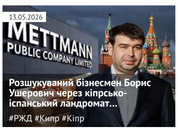
Роздрукувати | Надіслати товаришу

Коментарі:

comments powered by Disqus

Важливі новини





Останні новини

По даті | По переглядам | По коментарям

18:24 Понад 50% поляків незадоволені діяльністю нового президента Кароля Навроцького
18:18 Зеленський провів Ставку: В пріоритеті — антибалістичні ракети, снаряди 155 мм та зміцнення фронту
18:13 Очищення партійних лав руками головного «перебіжчика»: Антон Яценко в Києві вирішував долю черкаських депутатів без журналістів
18:07 Справжнє містобудівне планування: головний архітектор Франківська Мусіловський за ніч «звів» 2 мільйони застави та вийшов із СІЗО
18:01 Травневий наступ РФ провалився: найнижчі темпи просування з жовтня 2023 року, — DeepState

Підписуйтесь на наш канал в Telegram. Оперативно про головне

17:55 Екснардеп Юрій Береза закликав заборонити високопосадовцям обіймати посади, якщо їхні діти ховаються за кордоном
17:50 На Мальті прогримів потужний вибух на фабриці феєрверків: госпіталізовано двох чоловіків, пошкоджено навколишні будинки
17:44 Керівника Львівської обласної прокуратури Миколу Мерета та його заступників звинувачують у шантажі місцевих забудовників
17:38 Заступнику голови Солонківської громади Миколі Пущаку оголосили підозру через ДТП із потерпілим на трасі «Київ-Чоп»
17:33 НАБУ і САП оголосили нову підозру ексзаступнику міністра інфраструктури Василю Лозинському у справі про зловживання
17:28 «Екссмотрящий» за Київрадою Денис Комарницький особисто зустрічає VIP-гостей у власному 5-зірковому готелі у Словенії
17:22 Очільнику Служби відновлення Львівщини Олегу Березі оголосили підозру через нецільове використання 94 мільйонів
17:16 Експеримент із ШІ: Симуляція «світу під управлінням нейромереж» завершилась хаосом і крахом цивілізацій
17:10 «Засуджуємо одне, а робимо те саме»: у Раді прокоментували мовне рішення Полтавської міськради
17:04 Від нарощування вій — до мобілізації: в одеському ТЦК впізнали відомого місцевого б'юті-майстра
16:58 «В усьому винен ретроградний Меркурій»: «ворожка Єрмака» Вероніка "Феншуй" знайшла астрологічну причину зливів у справі Міндіча
16:52 В Одесі стався конфлікт між цивільними, ТЦК та поліцією під час мобілізації
16:48 На півдні Одещини росіяни обстріляли лікарню та пологове відділення: там перебували жінки з немовлятами
16:42 Нікол Пашинян заявив про відсутність підстав для референдуму щодо вибору між ЄС та ЄАЕС
16:37 Новий історичний максимум: НБУ підвищив офіційний курс долара до 44,30 гривні
16:32 Іран виходить із переговорів зі США та оголошує про повне блокування Ормузької протоки
16:27 **Ситуація на фронті: від початку доби росіяни здійснили 62 штурми, найзапекліші бої тривають на Покровському напрямку**

Теги новин

COVID-19 агрессия России Атака **Війна** **Война** ВСУ Вторжение Дональд Трамп Донбасс ДТП Зеленский ЗСУ Киев Київ коронавирус Коррупция **Напад Росії на Україну** Нападение России на Украину оккупанты окупанти Порошенко Путин Росія **Россия** сбу США **Украина** Україна ЧП Эпидемия коронавируса

Наші опитування

Чи вірите ви, що Дональд Трамп зможе зупинити війну між Росією та Україною?

- Так, повністю зможе
- Частково зможе, але не відразу
- Ні, не зможе
- Це залежить від дій інших сторін
- Важко відповісти

Голосувати

Показати результати опитування
Показати всі опитування на сайті