DOI 10.31891/2307-5732-2024-339-4-52
УДК 65.24

БЕВЗА В'ЯЧЕСЛАВ
Національний університет «Одеська юридична академія»
https://orcid.org/0009-0007-2695-969X
e-mail: viacheslavbevza718@gmail.com
СЛАТВІНСЬКА ВАЛЕРІЯ
Національний університет «Одеська юридична академія»
https://orcid.org/0000-0002-6082-981X
e-mail: slatvinskaya_valeriya@ukr.net

ВПЛИВ ЗБОЮ CROWDSTRIKE НА МЕГА-ВИТІК ПАРОЛІВ: ЧИ Є ЗВ'ЯЗОК? Ч. 1

Стаття аналізує можливий зв'язок між масштабним витоком паролів та збоєм у системі компанії CrowdStrike. Автори досліджують обставини обох подій, розглядає потенційні наслідки та закликають до посилення заходів кібербезпеки як для компаній, так і для користувачів. Основний акцент статті - на взаємозв'язку між кіберзагрозами та необхідністю комплексного підходу до захисту даних.

Ключові слова: кібербезпека, витік даних, інформаційна безпека, кіберзлочинність, CrowdStrike.

VIACHESLAV BEVZA
National University "Odesa Law Academy"
SLATVINSKA VALERIIA
National University "Odesa Law Academy"

THE IMPACT OF THE CROWDSTRIKE FAILURE ON THE MEGA PASSWORD LEAK: IS THERE A CONNECTION? P. 1

This article explores the possible implications of the CrowdStrike incident on the mega password leak. The study draws on various research papers and publications to delve into the complex interplay between cybersecurity breaches and the broader implications for digital safety. The analysis reveals a web of interconnected challenges, highlighting the importance of vigilance and the constant evolution of cybersecurity protocols.

The article begins by recounting the CrowdStrike outage and its aftermath, detailing the actions of the cyber criminals who attempted to capitalize on the situation and the strategies proposed to mitigate risks for affected users. It then discusses the findings of a joint study by FCRF, which uncovered a wave of phishing attacks targeting CrowdStrike clients. The study reveals that the outage was used as a pretext for distributing phishing emails aimed at stealing passwords and other sensitive information.

The connection between the CrowdStrike outage and the mega password leak is not straightforward but indicative of cyber threats' intricate nature. While the primary mission of CrowdStrike is to protect its clients' systems from unauthorized access and data breaches, such an incident raises concerns about the effectiveness of existing security protocols. It serves as a stark reminder of the potential vulnerabilities of even the most reputable cybersecurity firms.

The paper suggests that the relationship between the two events underscores the importance of regular security reviews and the implementation of advanced practices, such as using password managers and two-factor authentication. It emphasizes the need for businesses to remain proactive in updating their security protocols and for individuals to protect their personal information.

Furthermore, the investigation into the outage could have uncovered vulnerabilities in CrowdStrike's systems, which may have contributed to the password leak. However, it is equally plausible that the leak was a result of a separate, unrelated security breach. The article suggests that a thorough analysis of alternative sources of the password leak is essential to gain a comprehensive understanding of the situation.

In conclusion, the potential link between the CrowdStrike outage and the mega password leak is a critical juncture in the ongoing battle against cyber threats. It underscores the necessity for continuous innovation in the realm of cybersecurity, public awareness, and the collective responsibility to manage digital risks effectively. The real story here is the complex interplay between the evolving cyber threat landscape, the challenges it presents, and the urgent need to rethink our approach to password management and digital security.

This article aims to stimulate further research and discussion on the multifaceted nature of cybersecurity incidents and their broader implications. Examining the potential connections between the CrowdStrike outage and the mega password leak sheds light on the intricate dynamics at play in the digital world and the urgent need for a collaborative effort to ensure a secure online environment for all.

Keywords: cybersecurity, data breach, information security, cybercrime, CrowdStrike.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Ландшафт кібербезпеки постійно розвивається, а разом з ним з'являється безліч викликів, на які компанії та приватні особи повинні реагувати, щоб захистити свої цифрові активи. Нещодавнє викриття витоку мега-паролів, в результаті якого було розкрито вражаючі 2,6 мільярда облікових даних користувачів, прокотилося по цифровому світу шоковою хвилею. Оскільки ентузіасти кібербезпеки та широка громадськість намагаються впоратися з наслідками такого колосального витоку даних, цілком природно виникає питання, чи є зв'язок між цією подією та діяльністю CrowdStrike, провідної фірми з кібербезпеки, відомої своїми надійними послугами з реагування на інциденти.

Однією з таких проблем, яка нещодавно опинилася в центрі уваги, є потенційний зв'язок між зломом CrowdStrike і мега-витоком паролів. Проблема, про яку йдеться, полягає у зростаючому занепокоєнні вразливістю конфіденційної інформації перед обличчям все більш витончених кібератак. Ця ситуація підкреслює критичну важливість надійних заходів безпеки і нагальну потребу в усуненні наслідків таких порушень.

Збій CrowdStrike і наступний мега-витік паролів викликали занепокоєння щодо можливого зв'язку

між цими двома подіями. У той час як одні стверджують, що аварія могла поставити під загрозу заходи безпеки, що призвело до витоку, інші припускають, що ці інциденти не пов’язані між собою. 19 липня 2024 року сталася значна подія в кібербезпеці, коли збій у програмному забезпеченні CrowdStrike призвів до глобального IT-збою, що зачепило мільйони пристроїв. Цей інцидент викликав хвилю занепокоєння щодо кібербезпеки, а деякі експерти задаються питанням, чи може він бути пов'язаний з нещодавнім масовим витоком паролів.

4 липня 2024 року хакер на форумі хакерів оприлюднив файл під назвою "rockyou2024.txt", що містить понад 9,9 мільярда унікальних паролів. Цей файл, який, як вважають, є збіркою даних з численних витоків протягом останніх 20 років, став одним із найбільших витоків паролів в історії.

Хоча наразі не встановлено прямого зв'язку між збоєм CrowdStrike та витоком паролів RockYou, деякі експерти вважають, що ці два інциденти можуть бути пов'язані. Збій CrowdStrike зачепив програмне забезпечення Falcon Sensor, яке використовується для захисту від кібератак. Можливо, зловмисники скористалися цим збоєм, щоб отримати доступ до вразливих систем та викрасти дані, включаючи паролі.

Важливо зазначити, що це лише теорія, і наразі немає жодних доказів, які б підтверджували зв'язок між двома інцидентами. Однак цей випадок підкреслює важливість кібербезпеки та необхідність вжиття заходів для захисту своїх паролів та особистої інформації.

Аналіз досліджень та публікацій

В роботі [1] описано глобальний збій CrowdStrike, який стався 19 липня 2024 року, та його вплив на користувачів. Автор описує дії зловмисників, які намагалися скористатися збоєм, а також пропонує стратегії пом'якшення ризиків для користувачів. Стаття також пропонує стратегії пом'якшення ризиків для користувачів, які постраждали від збою. Звіт [2] описує тенденції кіберзагроз у 2024 році, а також методи, які використовують зловмисники для проникнення в системи. Звіт підкреслює, що зловмисники стають все більш спритними та використовують більш складні методи атак. Автори звіту рекомендують організаціям вжити заходів для захисту своїх систем від цих загроз. Стаття [3] описує спільне дослідження FCRF яке виявило хвилю фішингових атак, спрямованих на клієнтів CrowdStrike. Зловмисники використовували збій CrowdStrike як привід для розсилки фішингових електронних листів, намагаючись викрасти паролі та іншу конфіденційну інформацію. Стаття [4] описує збій CrowdStrike, а також інші кібербезпечні новини, що сталися у липні 2024 року. Автор підкреслює важливість кібербезпеки та надає поради щодо захисту себе від кіберзагроз. Стаття [5] описує досвід адміністраторів систем, які постраждали від збою CrowdStrike. Адміністратори поділилися своїми розповідями про те, як збій вплинув на їхні системи та бізнес. Робота [6] описує, як зловмисники використовували збій CrowdStrike для поширення шкідливого програмного забезпечення. Зловмисники створили фальшиві веб-сайти CrowdStrike, які розповсюджували шкідливе програмне забезпечення, коли користувачі намагалися завантажити оновлення. Стаття [7] описує інструмент відновлення, який випустила Microsoft для допомоги користувачам, чиї комп'ютери постраждали від збою CrowdStrike. Інструмент допоможе користувачам відновити свої системи та повернутися до роботи. Стаття [8] описує масштаб збою CrowdStrike, який торкнувся мільйонів пристроїв Microsoft Windows. Збій призвів до "синього екрану смерті" на багатьох комп'ютерах, що спричинило значні перебої в роботі. Праця [9] описує технічні причини збою CrowdStrike, який призвів до "синього екрану смерті" на пристроях Windows. Збій був викликаний помилкою в оновленні CrowdStrike, яке призвело до нестабільності роботи системи. Стаття [10] описує витік 10 мільярдів паролів, який отримав назву RockYou2024. Цей витік є одним із найбільших в історії та підкреслює важливість використання надійних паролів та їх регулярної зміни. Стаття [11] описує наслідки від оновлення ОС Windows, та коментарі CEO що зробили працівники CrowdStrike для виявлення і знешкодження проблеми. Стаття [12] описує витік 10 мільярдів паролів, який є одним з найбільших в історії. Витік включає паролі від багатьох популярних веб-сайтів та онлайн-сервісів. Стаття рекомендує користувачам змінити свої паролі, особливо якщо вони використовуються на кількох сайтах.

Формулювання цілей статті

Метою роботи є: розкрити можливий вплив інциденту з CrowdStrike на мега витік паролів.

Виклад основного матеріалу

CrowdStrike - провідна фірма з кібербезпеки, відома своїми передовими послугами з розвідки загроз та реагування на інциденти. Компанія CrowdStrike, яка потрапила в заголовки газет завдяки своїй участі у розкритті сумнозвісного злому SolarWinds та інших гучних кібервторгнень, є надійним гравцем в індустрії кібербезпеки. Її основна компетенція полягає у виявленні, запобіганні та реагуванні на кіберзагрози, що може наштовхнути на думку про те, що її діяльність ненавмисно спровокувала витік паролів або викрила його. Однак важливо пояснити, що основна місія CrowdStrike - захищати системи своїх клієнтів від несанкціонованого доступу та витоку даних, а не створювати їх [1]. У загальному сенсі, злом такої відомої компанії б'є на сполох щодо ефективності існуючих протоколів безпеки. Якщо організація, покликана захищати інших, може стати жертвою кібератаки, це ставить під сумнів безпеку даних усіх інших. З іншого боку, мега-витік паролів стосується тривожної тенденції масових дампів даних, що містять облікові дані для входу на різні онлайн-платформи. Ці витоки часто відбуваються, коли хакери використовують вразливості веб-сайтів або сервісів для крадіжки інформації про користувачів, яка потім стає загальнодоступною в

темному інтернеті [2].

Взаємодія між CrowdStrike і витоком мега-паролів, швидше за все, має більше нюансів, ніж прямий причинно-наслідковий зв'язок. Після такої значної події фірми з кібербезпеки, такі як CrowdStrike, часто звертаються за допомогою в розслідуванні витоку, виявленні порушників і допомозі постраждалим сторонам зменшити потенційну шкоду. Їх роль полягає в аналізі дампу даних, розумінні обсягу скомпрометованої інформації та наданні рекомендацій щодо посилення заходів безпеки для запобігання подібним випадкам у майбутньому [3].

Хоча участь CrowdStrike у реагуванні на витік паролів може бути значною, дуже важливо відокремити роль фірми в управлінні наслідками від фактичної причини витоку. Зв'язок між CrowdStrike та витоком мега-паролів є радше наслідком їхнього досвіду та позиціонування на ринку, ніж фактором, що спричинив сам витік. Причетність CrowdStrike як лідера в галузі кібербезпеки підкреслює гостру потребу в передових заходах безпеки в сучасному взаємопов'язаному світі.

Зв'язок між витоком CrowdStrike і мега-витоком паролів важливий у кількох аспектах. По-перше, він підкреслює взаємопов'язаний характер кіберзагроз. Злом в одній компанії може мати далекосяжні наслідки, потенційно впливаючи на мільйони користувачів, які могли повторно використовувати свої паролі на різних платформах. По-друге, це підкреслює важливість гігієни паролів і використання унікальних, складних паролів для кожного облікового запису. Повторне використання паролів може створити ефект доміно, коли одне порушення може скомпрометувати кілька облікових записів. По-третє, це ставить під сумнів адекватність нинішніх заходів кібербезпеки та необхідність постійного вдосконалення захисту конфіденційних даних [4].

Зв'язок між цими двома подіями також пов'язаний із ширшими науковими та практичними викликами. Перед дослідниками в галузі кібербезпеки стоїть завдання розробити передові методи виявлення та пом'якшення наслідків таких атак, а також дослідити першопричини цих порушень. Наприклад, розуміння методів, які використовують хакери для обходу систем безпеки, може призвести до створення більш ефективних інструментів і протоколів. Крім того, існує нагальна потреба в інформуванні громадськості про ризики, пов'язані з кіберзагрозами, та важливість впровадження базових практик безпеки, таких як використання менеджерів паролів та двофакторна автентифікація [5].

З практичної точки зору, злом CrowdStrike і мега-витік паролів слугують суворим нагадуванням для бізнесу про необхідність регулярно переглядати і оновлювати свої протоколи безпеки. Це стосується не лише захисту власних систем, але й перевірки сторонніх сервісів, на які вони покладаються. Для приватних осіб ці події підкреслюють важливість залишатися пильними і вживати проактивних заходів для захисту особистої інформації. Регулярна перевірка на предмет витоку паролів та їх оновлення є важливими звичками в цифрову епоху [6].

Розберемо що робити при «смертельному оновленні» (див. Рис. 1):

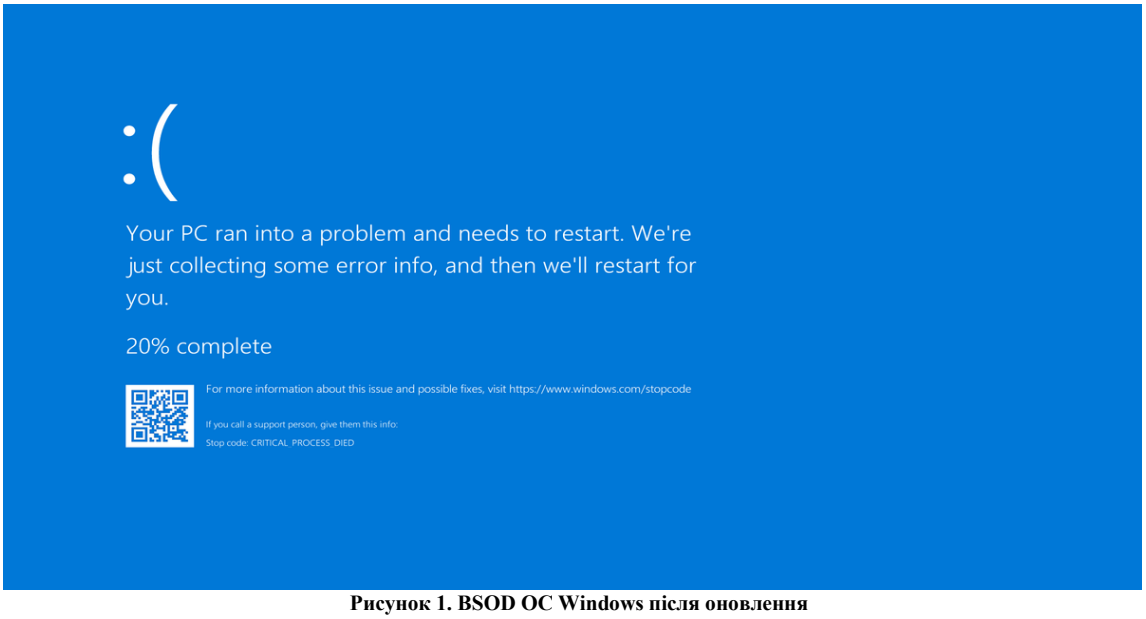

Рисунок 1. BSOD ОС Windows після оновлення

Розглянемо дамп файлу на Рис. 2.

Наведене зображення показує дамп процесу, який зазнав аварії через помилку доступу до пам'яті. Згідно з повідомленням про помилку, помилка сталася, коли процес намагався прочитати значення з адреси пам'яті 0x000000000000009c. Ця адреса не дійсна, оскільки вона не належить жодному виділеному блоку пам'яті. У цьому випадку ймовірно, що помилка викликана не ініціалізованим покажчиком. Це поширена помилка програмування, яку можна легко уникнути, ініціалізуючи всі покажчики перед їх використанням.

```
EXCEPTION_RECORD:  fffffb0d18d3ec28 -- (.exr 0xfffffb0d18d3ec28)
ExceptionAddress: fffff8021df335a1 (csagent+0x000000000000e35a1)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: 000000000000009c
Attempt to read from address 000000000000009c

CONTEXT:  fffffb0d18d3e460 -- (.cxr 0xfffffb0d18d3e460)
rax=fffffb0d18d3f2b0 rbx=0000000000000000 rcx=0000000000000003
rdx=fffffb0d18d3f280 rsi=ffff9a81b596f9a4 rdi=ffff9a81b596605c
rip=fffff8021df335a1 rsp=fffffb0d18d3ee60 rbp=fffffb0d18d3ef60
 r8=000000000000009c  r9=0000000000000000 r10=0000000000000000
r11=0000000000000014 r12=fffffb0d18d3ef28 r13=fffffb0d18d3f0d0
r14=000000000000001a r15=0000000000000004
iopl=0         nv up ei pl nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00050206
csagent+0xe35a1:
fffff802`1df335a1 458b08          mov     r9d,dword ptr [r8] ds:002b:00000000`0000009c=????????
Resetting default scope

BLACKBOXBSD: 1 (!blackboxbsd)


BLACKBOXNTFS: 1 (!blackboxntfs)


BLACKBOXPNP: 1 (!blackboxpnp)


BLACKBOXWINLOGON: 1

PROCESS_NAME:  System

READ_ADDRESS:  000000000000009c

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_CODE_STR:  c0000005

EXCEPTION_PARAMETER1:  0000000000000000

EXCEPTION_PARAMETER2:  000000000000009c

EXCEPTION_STR:  0xc0000005

STACK_TEXT:
fffffb0d`18d3ee60 fffff802`1df09152     : 00000000`00000000 00000000`e01f008d fffffb0d`18d3f202 fffff802`1e0e1b18 : csagent+0xe35a1
fffffb0d`18d3f000 fffff802`1df0a3e9     : 00000000`00000000 00000000`00000010 00000000`00000000 ffff9a81`b596601c : csagent+0xb9152
fffffb0d`18d3f130 fffff802`1e14954f     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : csagent+0xba3e9
fffffb0d`18d3f260 fffff802`1e145d9b     : ffff9a81`93735280 fffffb0d`18d3f5d0 00000000`00000000 00000000`00000015 : csagent+0x2f954f
fffffb0d`18d3f4d0 fffff802`1deb8fd0     : 00000000`000030f1 fffffb0d`18d3f790 ffff9a81`992cbb30 ffffe409`b797e098 : csagent+0x2f5d9b
fffffb0d`18d3f690 fffff802`1deb808e     : ffff9a81`992cbb30 fffff802`1df68fce 00000000`00006840 fffff802`1e0b5aa8 : csagent+0x68fd0
fffffb0d`18d3f800 fffff802`1deb7dfa     : fffffb0d`18d3fa78 ffff9a81`bc5ab030 ffff9a81`992cbb30 ffffe409`9069cf08 : csagent+0x6808e
fffffb0d`18d3f870 fffff802`1df60b49     : 00000000`00000008 fffffb0d`18d3f9b9 00000000`00000000 ffff9a81`88bc9a2e : csagent+0x67dfa
fffffb0d`18d3f8f0 fffff802`1deb039a     : 00000000`00000000 fffffb0d`18d3faf9 ffffe409`9069ca60 ffffe409`914c8310 : csagent+0x110b49
fffffb0d`18d3fa20 fffff802`1deb01b7     : 00000000`00000010 00000000`00000000 ffffe409`9069ca60 00000000`00000001 : csagent+0x6039a
fffffb0d`18d3fb60 fffff802`1df552d6     : 00000000`00000000 ffffe409`a03ec718 00000000`00000000 ffffe409`914c8310 : csagent+0x601b7
fffffb0d`18d3fb90 fffff802`0fd48da5     : ffffe409`85255040 ffffe409`85255040 00000000`00000080 fffff802`1df55120 : csagent+0x1052d6
fffffb0d`18d3fbd0 fffff802`0fe06de8     : ffffc601`5e4d7180 ffffe409`85255040 fffff802`0fd48d50 00000000`00000000 : nt!PspSystemThreadStartup+0x55
fffffb0d`18d3fc20 00000000`00000000     : fffffb0d`18d40000 fffffb0d`18d39000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28
```

Рисунок 2. Дамп файла

Вирішення проблеми

Варіант 1.

Щоб виправити цю помилку, необхідно знайти й виправити код, який використовує не ініціалізований покажчик. Це може бути складно, оскільки помилка може виникнути в будь-якій частині коду. Однак, використовуючи інструменти налагодження та аналізу коду, можна знайти й виправити джерело проблеми.

Варіант 2.

1. Завантажити Windows у безпечному режимі

2. Дотримуватися шляху C:\Windows\System32\drivers\CrowdStrike директорія у провіднику зображено на рисунку 3

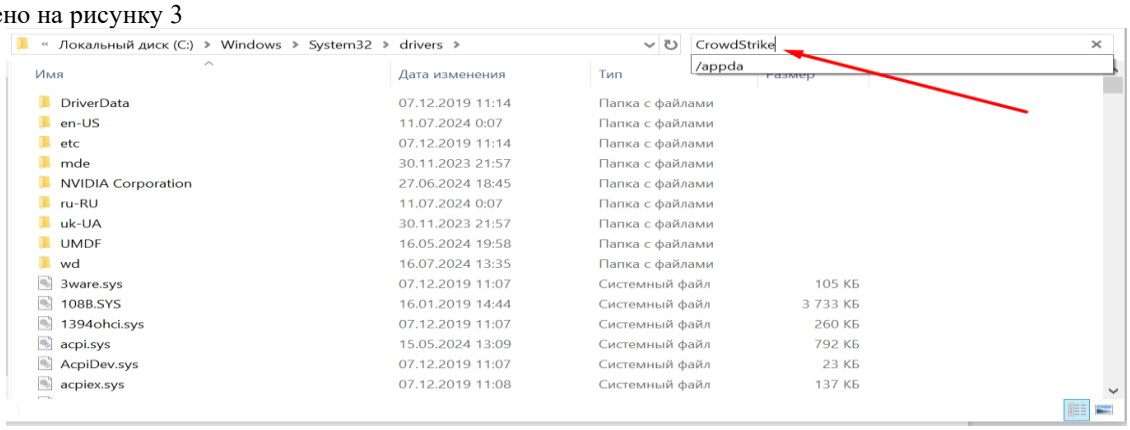

Рисунок 3. Умовний шлях до директорії

3. Знайти файл “C-00000291*.sys” файл, правою кнопкою миші клікнути та перейменувати його в “C-00000291*.renamed”

4. Просто завантажити систему у звичайному режимі.

Варіант 3.

Як ще вважають фахівці CrowdStrike ви можете не заходити в безпечний режим ОС Windows, а наприклад перезавантажити комп’ютер 2-3 рази і тоді проблема може зникнути сама.

Збій CrowdStrike міг поставити під загрозу заходи безпеки, потенційно сприяючи витоку пароля. По-перше, збій міг виявити вразливі місця в системах CrowdStrike, зробивши їх сприйнятливими до використання зловмисниками. Це виявлення слабких місць в інфраструктурі безпеки могло створити можливості для несанкціонованого доступу до конфіденційних даних, включаючи паролі користувачів. Отже, витік паролів може бути прямим наслідком порушення безпеки, спричиненого збоєм [7].

З іншого боку, цілком імовірно, що збій CrowdStrike і витік пароля не пов'язані між собою інциденти. Збій міг бути спровокований технічними проблемами в системах CrowdStrike, які не обов'язково збігаються з факторами, що призвели до витоку пароля. Крім того, витік пароля міг статися через окреме порушення безпеки, незалежно від збою CrowdStrike. Без конкретних доказів зв'язку між цими двома подіями важливо розглянути альтернативні пояснення витоку пароля [8].

Збій CrowdStrike міг вплинути на захист даних, потенційно зігравши роль у мегавитоку паролів. Під час збою заходи захисту даних у системах CrowdStrike могли бути скомпрометовані, що поставило під загрозу цілісність конфіденційної інформації. Збій у протоколах шифрування, які мають вирішальне значення для захисту даних, міг створити лазівки, які сприяли несанкціонованому доступу та викраденню паролів. Як наслідок, скомпрометований захист даних, спричинений збоєм, міг безпосередньо сприяти витоку пароля [9].

Цілком імовірно, що реакція CrowdStrike на збій могла запобігти подальшим витокам даних, включаючи витік пароля. Після збою CrowdStrike, ймовірно, негайно вжив заходів для підвищення безпеки своїх систем, пом'якшивши ризики, пов'язані з подією. Профілактичні заходи безпеки компанії могли ефективно стримувати будь-які потенційні загрози, запобігаючи додаткові витоки даних, у тому числі витік паролів. Таким чином, витік пароля міг статися незалежно від збою, а дії CrowdStrike після збою відіграли вирішальну роль у запобіганні подальшим зламам.

Збій CrowdStrike міг вплинути на конфіденційність користувачів, що потенційно призвело до розголошення конфіденційної інформації користувача, як-от паролі. Конфіденційність користувачів могла бути порушена в результаті збою, що могло сприяти несанкціонованому доступу до даних користувачів, що зберігаються в системах CrowdStrike. Порушення конфіденційності користувача під час збою могло дозволити зловмисникам отримати та витікати паролі, пов'язані з скомпрометованою інформацією користувача, створюючи значні ризики для постраждалих осіб.

Крім того, витік паролю міг виникнути зовсім з іншого джерела, відмінного від збою CrowdStrike. Витік міг бути частиною більшого витоку даних, пов'язаного з іншою компанією чи організацією, не пов'язаною з подіями, пов'язаними з аварією CrowdStrike. Тому вкрай важливо вивчити інші потенційні джерела та фактори, що сприяють витоку пароля, а не пов'язувати це виключно з інцидентом CrowdStrike. Розслідування альтернативних джерел витоку паролів має важливе значення для розуміння повного масштабу витоку даних [10].

CrowdStrike "активно працює з клієнтами, які постраждали від дефекту, виявленого в одному оновленні контенту для хостів Windows", - заявив у п'ятницю генеральний директор Джордж Курц в соціальних мереж X. Він додав, що хости Mac і Linux не торкнулися. «Це не інцидент безпеки чи кібератака. Проблему було виявлено, ізольовано та виправлено», — сказав Курц [11].

Дослідники Cybernews виявили, мабуть, найбільшу добірку паролів, що містить приголомшливі 9948575739 унікальних паролів у вигляді відкритого тексту. Файл із даними під назвою rockyou2024.txt був опублікований 4 липня користувачем форуму ObamaCare.

Хоча користувач зареєструвався наприкінці травня 2024 року, раніше він поділився базою даних співробітників юридичної фірми Simmons & Simmons, інформацією з онлайн-казино AskGamblers та заявами студентів до коледжу Роуена в окрузі Берлінгтон.

Команда зіставила паролі, включені до витоку RockYou2024, з даними засобу перевірки витоку паролів Cybernews, яке показало, (Cybernews зіставили зі своїми базами даними через Leaked Password Checker,) що ці паролі виникли в результаті поєднання старих та нових витоків даних.

«По суті, витік RockYou2024 є добіркою реальних паролів, що використовуються людьми по всьому світу. Виявлення того, що багато паролів зловмисників суттєво підвищують ризик атак із підтасовуванням облікових даних», — кажуть дослідники.

За фактом використання файлу методом перебору є реальна загроза, що хакери можуть отримати доступ до облікових записів користувачів на різних платформах, використовуючи витеклі паролі для зламу інших акаунтів.

Атаки з підстановкою облікових даних можуть завдати серйозних збитків користувачам та підприємствам. Наприклад, недавня хвиля атак на Santander, Ticketmaster, Advance Auto Parts, QuoteWizard та інших стала прямим результатом атак із підстановкою облікових даних проти постачальника хмарних послуг жертви Snowflake.

"Зловмисники можуть використовувати компіляцію паролів RockYou2024 для проведення атак методом перебору та отримання несанкціонованого доступу до різних онлайн-акаунтів, які використовуються особами, які використовують паролі, включені до набору даних", - пояснили в команді [12].

Збірка RockYou2024 не просто так з'явилася. Три роки тому Cybernews опублікував статтю про найбільшу на той момент добірку паролів RockYou2021, що містить 8,4 мільярда простих текстових паролів.

Згідно з аналізом RockYou2024, проведеним командою, зловмисники розробили набір даних,

переглядаючи Інтернет на предмет витоків даних, додавши ще 1,5 мільярда паролів з 2021 по 2024 рік та збільшивши набір даних на 15 відсотків.

Компіляція RockYou2021, що є продовженням витоку даних 2009 року, включала десятки мільйонів паролів для облікових записів соціальних мереж. Проте з того часу обсяг компіляції розрісся в геометричній прогресії. Швидше за все, остання ітерація RockYou містить інформацію, зібрану з більш ніж 4000 баз даних за понад два десятиліття.

Команда Cybernews вважає, що зловмисники можуть використати десяти мільярдну компіляцію RockYou2024 для атаки на будь-яку систему, яка не захищена від атак методом перебору. Сюди входить все: від онлайн-і офлайн-сервісів до інтернет-камер та промислового обладнання. «Більше того, у поєднанні з іншими базами даних, що втекли, на хакерських форумах і торгових майданчиках, які, наприклад, містять адреси електронної пошти користувачів та інші облікові дані, RockYou2024 може сприяти каскаду витоків даних, фінансового шахрайства та крадіжки особистих даних», — заявили в команді [12].

Хоча не існує універсального рішення для захисту користувачів, паролі яких були розкриті, постраждалим особам та організаціям слід вжити заходів щодо пом'якшення наслідків. Дослідницька група Cybernews радить: Негайно скиньте паролі для всіх облікових записів, пов'язаних з паролями. Настійно рекомендується вибирати надійні та унікальні паролі, які не будуть повторно використовуватися на кількох платформах. Увімкніть багатофакторну автентифікацію (MFA), де це можливо. Це підвищує безпеку, вимагаючи додаткової перевірки, крім пароля.

Використовуйте програмне забезпечення менеджера паролів для безпечного створення та зберігання складних паролів. Менеджери паролів знижують ризик повторного використання паролів у різних облікових записах. Cybernews включить дані RockYou2024 у засіб перевірки витоків паролів, що дозволить будь-кому перевірити, чи були його облікові дані розкриті за допомогою останньої компіляції відкритих паролів, яка є рекордсменом.

RockYou2024 став свідком того, як у 2024 році до мережі просочилася друга рекордна компіляція. Раніше цього року Cybernews виявила "Mother of all breaches" (MOAB), що містить разючі 12 терабайт інформації, що охоплює 26 мільярдів записів [12].

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Підсумовуючи, потенційний зв’язок між збоєм CrowdStrike і мегавитоком паролів є складною та багатогранною проблемою. Хоча аргументи свідчать про те, що збій міг поставити під загрозу заходи безпеки, захист даних і конфіденційність користувачів, контраргументи підкреслюють можливість того, що інциденти не були пов’язані, і підкреслюють зусилля CrowdStrike щодо реагування. Необхідні подальші розслідування та аналіз, щоб визначити ступінь впливу збою CrowdStrike на витік паролів, проливаючи світло на складну динаміку подібних інцидентів кібербезпеки.

Насамкінець, хоча масовий витік паролів і подальша участь CrowdStrike можуть здаватися взаємопов'язаними, важливо розмежовувати роль фірми у вирішенні інциденту та джерела витоку. Досвід CrowdStrike, ймовірно, допоможе зорієнтуватися в складнощах цієї ситуації, забезпечити засвоєння уроків і підвищення безпеки цифрової екосистеми. Реальною історією тут є постійно мінливий ландшафт кіберзагроз і необхідність пильності та інновацій у сфері кібербезпеки, а не будь-який прямий зв'язок між двома організаціями, що може свідчити про компрометацію власних систем або операцій CrowdStrike.

Таким чином, потенційний зв'язок між зломом CrowdStrike і мега-витоком паролів є критичним моментом у боротьбі з кіберзагрозами, що триває. Він підкреслює необхідність постійних інновацій у сфері кібербезпеки, важливість обізнаності громадськості та нагальне завдання переоцінки нашого підходу до управління паролями та цифрової безпеки. Взаємозв'язок між цими подіями підкреслює складність викликів, з якими ми стикаємося, і необхідність колективних зусиль для забезпечення безпечного онлайн-середовища для всіх.

Література

1. CrowdStrike Global Outage – Threat Actor Activity and Risk Mitigation Strategies URL: https://sechub.in/view/2915174 (date of access: 22.07.2024).

2. CrowdStrike 2024 Global Threat Report: Adversaries Gain Speed and Stealth URL: https://www.sentinelone.com/blog/crowdstrike-global-outage-threat-actor-activity-and-risk-mitigation-strategies/ (date of access: 22.07.2024).

3. Joint Research by FCRF and mFilterit Reveals Phishing Attacks Targeting CrowdStrike Customers URL: https://www.the420.in/fake-phishing-crowdstrike-websites-outage-2024-mfilterit-fcrf-microsoft/ (date of access: 22.07.2024).

4. CrowdStrike content update causes global IT outage, and other cybersecurity news to know this month URL: https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ (date of access: 22.07.2024).

5. CrowdStrike content update causes global IT outage, and other cybersecurity news to know this month URL: https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ (date of access: 22.07.2024).

6. Angry admins share the CrowdStrike outage experience URL: https://www.theregister.com/2024/07/19/admin_crowdstrike_update_mess/?td=amp-keepreading&_gl=1*1tilbef*_ga*ekxGSllWNHJESnFMMUJSSjAtaGl5V0J3bk1LV1J4U2g2X0Vld25wMDhVU20wY1RUY2VVN2ZUWU5McmFaVnFTSQ..*_ga_JXW44Y23NM*MTcyMTY3NjkzMy4xLjEuMTcyMTY3NzIyNC4wLjAuMA (date of access: 22.07.2024).

7. Cybercriminelen misbruiken CrowdStrike-incident om malware te verspreiden URL: https://www.theregister.com/2024/07/19/admin_crowdstrike_update_mess/?td=amp-keepreading&_gl=1*1tilbef*_ga*ekxGSllWNHJESnFMMUJSSjAtaGl5V0J3bk1LV1J4U2g2X0Vld25wMDhVU20wY1RUY2VVN2ZUWU5McmFaVnFTSQ..*_ga_JXW44Y23NM*MTcyMTY3NjkzMy4xLjEuMTcyMTY3NzIyNC4wLjAuMA (date of access: 22.07.2024).

8. Microsoft випустила інструмент відновлення для комп'ютерів, що постраждали через несправність CrowdStrike URL: https://ms.detector.media/it-kompanii/post/35609/2024-07-22-microsoft-vypustyla-instrument-vidnovlennya-dlya-kompyuteriv-shcho-postrazhdaly-cherez-nespravnist-crowdstrike/ (дата звернення: 22.07.2024).

9. Мільйонні Збої в роботі пристроїв Microsoft Windows Результат оновлення CrowdStrike URL: https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/ (дата звернення: 22.07.2024).

10. Системи Windows одночасно постраждали від «синього екрану смерті» «BSOD» URL: http://www.cicc.gov.ph/ (дата звернення: 22.07.2024).

11. Як оновлення програмного забезпечення кіберфірми CrowdStrike викликало одне з найбільших у світі збоїв IT URL:

12. https://www.cnbc.com/2024/07/19/what-is-crowdstrike-crwd-and-how-did-it-cause-global-it-outages.html

13. RockYou2024: 10 мільярдів паролів витекли в найбільшу компіляцію всіх часів URL: https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/ (дата звернення: 22.07.2024).

References

1. CrowdStrike Global Outage – Threat Actor Activity and Risk Mitigation Strategies Retrieved from https://sechub.in/view/2915174 [in English].

2. CrowdStrike 2024 Global Threat Report: Adversaries Gain Speed and Stealth Retrieved from https://www.sentinelone.com/blog/crowdstrike-global-outage-threat-actor-activity-and-risk-mitigation-strategies/ [in English].

3. Joint Research by FCRF and mFilterit Reveals Phishing Attacks Targeting CrowdStrike Customers Retrieved from https://www.the420.in/fake-phishing-crowdstrike-websites-outage-2024-mfilterit-fcrf-microsoft/ [in English].

4. CrowdStrike content update causes global IT outage, and other cybersecurity news to know this month Retrieved from https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ [in English].

5. CrowdStrike content update causes global IT outage, and other cybersecurity news to know this month Retrieved from https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ [in English].

6. Angry admins share the CrowdStrike outage experience Retrieved from https://www.theregister.com/2024/07/19/admin_crowdstrike_update_mess/?td=amp-keepreading&_gl=1*1tilbef*_ga*ekxGSllWNHJESnFMMUJSSjAtaGl5V0J3bk1LV1J4U2g2X0Vld25wMDhVU20wY1RUY2VVN2ZUWU5McmFaVnFTSQ..*_ga_JXW44Y23NM*MTcyMTY3NjkzMy4xLjEuMTcyMTY3NzIyNC4wLjAuMA [in English].

7. Cybercriminelen misbruiken CrowdStrike-incident om malware te verspreiden Retrieved from https://www.theregister.com/2024/07/19/admin_crowdstrike_update_mess/?td=amp-keepreading&_gl=1*1tilbef*_ga*ekxGSllWNHJESnFMMUJSSjAtaGl5V0J3bk1LV1J4U2g2X0Vld25wMDhVU20wY1RUY2VVN2ZUWU5McmFaVnFTSQ..*_ga_JXW44Y23NM*MTcyMTY3NjkzMy4xLjEuMTcyMTY3NzIyNC4wLjAuMA [in English].

8. Microsoft vypustyla instrument vidnovlennia dlia kompiuteriv, shcho postrazhdaly cherez nespravnist CrowdStrike - Microsoft releases a recovery tool for computers affected by the CrowdStrike flaw. Retrieved from https://ms.detector.media/it-kompanii/post/35609/2024-07-22-microsoft-vypustyla-instrument-vidnovlennya-dlya-kompyuteriv-shcho-postrazhdaly-cherez-nespravnist-crowdstrike/ [in Ukrainian].

9. Milionni Zboi v roboti prystroiv Microsoft Windows Rezultat onovlennia CrowdStrike - 9. Millions of Microsoft Windows device outages as a result of CrowdStrike update. Retrieved from https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/ [in Ukrainian].

10. Systemy Windows odnochasno postrazhdaly vid «synoho ekranu smerti» «BSOD» - 10. Windows systems simultaneously affected by the 'blue screen of death' 'BSOD'. Retrieved from http://www.cicc.gov.ph/ [in Ukrainian].

11. Iak onovlennia programnogo zabespechennia kiberfirmi CrowdStrike viklikalo odne z naibilchih u sviti zboiv IT – 11. How a software update from cyber firm CrowdStrike caused one of the world's biggest IT blackouts Retrieved from https://www.cnbc.com/2024/07/19/what-is-crowdstrike-crwd-and-how-did-it-cause-global-it-outages.html [in Ukrainian].

12. RockYou2024: 10 miliardiv paroliv vytekly v naibilshu kompiliatsiiu vsikh chasiv - 12. RockYou2024: 10 billion passwords leaked in the largest compilation of all time. Retrieved from https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/ [in Ukrainian].