DOI 10.31891/2307-5732-2024-341-5-36
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. 2

Стаття являє собою аналіз помилок компанії CrowdStrike та їх наслідків для кібербезпеки. Сутність проблеми зводиться до того, щоб вивчити технічні аспекти, управлінські рішення та комунікаційні стратегії CrowdStrike. Авторами розглядається вплив на клієнтів та репутацію компанії, вжиті заходи для виправлення ситуації.

Ключові слова: кібербезпека, витік даних, шкідливе програмне забезпечення, 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. 2

This paper examines the devastating consequences of the Falcon detector by the cyber company CrowdStrike, the loss of data, the Windows critical error blue screen of death (BSOD), and the loss of the company's reputation. The article has analyzed many primary sources, articles, and publications to delve as hard as possible into the complex mix of cyber security and reveal the implications for digital security as well. The analysis carried out in this work shows such methods as social engineering, human factors, the carelessness of programmers who released updates, the carelessness of staff during a mass failure, and panic.

The article begins with an hourly diagram of the chronology of events of the mass failure of the company CrowdStrike, how the computers picked up the viral update itself, what had to be done and what methods of countering the threat were proposed in the analysis. The authors then analyzed surface and detailed metric analysis from Sevco Security CEO J.J. Guy between July 19 and 22. Subsequently, reports from the official CrowdStrike website were analyzed a month before the event with decent results from the Falcon detector. Although CrowdStrike's primary focus is to protect customer systems point-to-point. They could not protect themselves from OS updates and critical system errors. Such an incident raises concerns about the effectiveness of existing security protocols. This may signal that there are no universal systems, and no one is immune to human error, updates, or social engineering, as demonstrated in the work.

In addition, the vulnerability of the C++ language was demonstrated in the work. The article analyzes file dumps and analyzes the C++ language, where there was an error in the dump. In the future, it can be assumed that if the company used a newer programming language or at least some means of quarantine and testing on individual systems, such a problem, as this article considers, could be avoided. In conclusion, it should be noted that the field of cyber security is a field of constant innovation, collective awareness, and the ability of personnel to counter everything from phishing spam e-mails to a global failure in the IT field. The purpose of this article is to remind employees in this field to counter the threats of inattention, carelessness, and global panic. Which can be used by cybercriminals. From the mistakes demonstrated in the article, you can learn what happens in one company in the digital world, which can affect everyone's life. It sheds light on the urgent challenge of a collaborative effort to ensure a safe environment for us all.

Keywords: cybersecurity, data breach, malware, cybercrime, CrowdStrike.

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

Світ кібербезпеки, що швидко розвивається, де будь-яка незначна помилка може призвести до фатальних наслідків. Нещодавня подія з критичною помилкою від компанії CrowdStrike яка зацепила 8,5 мільйонів ОС Windows що викликало помилку (синій екран смерті або BSOD) пов'язана з детектором Falcon. В той день від помилки постраждали багато сфер від банківських до фармацевтичних. Такий інцидент викликає побоювання щодо ефективних протоколів безпеки компанії та ставить під сумнів її репутацію. Провідні фахівці з кібербезпеки зазначили що в період з 19 по 22 липня відновлення систем відбувалося дуже повільно. «Чому ж?» спросите ви. Тому що відновлення систем відбувалось в ручну. Дана проблемна ситуація підкреслює критичну важливість надійних заходів безпеки і нагальну потребу в усуненні наслідків таких порушень.

Далі можна зазначити що за місяць до події зі збоєм Falcon, досить не погано себе проявив на CrowdStrike 24 Hours of Spa CUP. Але чому все ж таки через непогані результати детектора у компанії стався такий збій? Це пов'язано з мовою програмування C++. Людина яка використовувала C++ випустила оновлення без відповідних мір. Не використала режим карантинну, не протестувала оновлення на окремих спеціальних машинах і в решті решт просто випустила оновлення. Це не означає що треба відмовлятися від цієї мови, це значить що треба більше нагадувати про це та, проводити тренінги з персоналом на дану тематику.

Аналіз досліджень та публікацій

Авторами вперше [1] розглянуто ситуацію з CrowdStrike, що зіткнулася зі значним збоєм, який залишив

багатьох її користувачів у стані занепокоєння. Збій вплинув на доступність її послуг, зробивши організації вразливими і такими, що відчайдушно потребують рішення. Як і у разі будь-якого серйозного збою в роботі послуг, було розпочато активну діяльність з відновлення нормальної роботи, але це також створило можливості для зловмисників [2]. CEO Sevco Security Джей Джея Гай [3] підкреслює важливість проактивного підходу до кібербезпеки та необхідність інтеграції новітніх технологій для захисту від зростаючих загроз. Автор [4] робить висновок про відновлення сервісу CrowdStrike на 95% завдяки метричному аналізу. Праця [5] стосується спостереження, що сервіс Crowdstrike відновлено приблизно на 95%, але повільний прогрес пояснюється виправленням помилок вручну. В роботі [6] наведено хронологію подій, виявлення помилок та їх знешкодження. Слушним джерелом є статистичний аналіз як детектор Falcon справляється з своєю роботою за місяць до події, а саме 25 червня на «CrowdStrike 24 Hours of Spa CUP» [7]. Корисним є звіт CrowdStrike щодо синього екрану смерті BSOD покрокові дії, як виправити критичну помилку [8]. В праці [9] йдеться про рівні конфіденційності інформації та звіти з помилками/наслідками. Важливим є основне сховище CrowdStrike [10]. В праці [11] йдеться про розширене тлумачення що могла зробити компанія CrowdStrike, типи та розбір помилок що призвели до руйнівного наслідку. Зловмисники намагаються поширювати підроблені виправлення, та вимагають певну суму грошей у BTC [12]. У [13] описано як оновлення програмного забезпечення кіберкомпанії CrowdStrike викликало одне з найбільших у світі відключень IT-ресурсів. В [14] з'ясовано як працюють ядра у комп'ютері, критичні помилки що можуть викликати синій екран смерті (BSOD). У сучасному цифровому світі кібербезпека є критично важливою для захисту інформаційних активів організацій та індивідуальних користувачів. Розуміння мотивів кіберзлочинців, сприятливих факторів, що підвищують ризик атак, а також ефективних методів захисту є ключовим для розробки комплексних стратегій безпеки. [15]. Практичні уроки кібербезпеки для компаній є невід'ємною частиною сучасної стратегії захисту інформації [16].

Формулювання цілей статті

Метою роботи є поглиблений аналіз помилок компанії CrowdStrike та їх розбір.

Виклад основного матеріалу

Майже відразу після збою кіберзлочинці почали розповсюджувати шкідливий файл, замаскований під вирішення проблеми CrowdStrike. Це шкідливе програмне забезпечення, оманливо назване «CrowdStrike_Hotfix.zip», було розроблене для того, щоб використовувати терміновість і занепокоєння, пов'язані зі збоєм у роботі. Користувачі, які прагнуть відновити захист від кібербезпеки, стали жертвами цієї пастки, завантаживши шкідливий файл у спробі захистити свої системи.

Ця тактика не нова. Кіберзлочинці процвітають у хаосі та невизначеності. Вони знають, що в розпал паніки користувачі з більшою ймовірністю втратить пильність і підуть на ризик, якого зазвичай уникають. Імітуючи законне рішення, ці зловмисники використовують довіру та терміновість, які користувачі мають при швидкому вирішенні критичних проблем. [1]

Цей інцидент є яскравим прикладом ширшої стратегії, яку часто використовують кіберзлочинці. Щоразу, коли повідомляється про гучний збій служби або вразливість, ви можете бути впевнені, що зловмисники готові скористатися ситуацією. Будь то фішингові електронні листи, підроблені патчі або шкідливі веб-сайти, мета одна: отримати вигоду зі страху та терміновості [2].

Хронологія подій зображена на рис. 1.

CEO Sevco Security Дж. Гай показує пророблену його відділом роботу, а саме на рисунку 2 можна побачити збій та приблизний аналіз заражених комп'ютерів у відсотковому зображенні на 19 липня.

У результаті вийшов такий показник:

- кількість пристроїв Windows, на яких запущено Crowdstrike онлайн хоча б один раз за 72 години до оновлення поганого контенту, порівняно з

- кількість пристроїв Windows, на яких працює Crowdstrike, не підключені до мережі після оновлення поганого контенту [3].

Тобто скільки ящиків Crowdstrike не зареєструвалося з вчорашнього вечора. Було встановлено інструменти приблизно о 2 годині дня за східним часом і відтоді відстежуємо їх щогодини. Близько 90% машин, які спостерігалися хоча б один раз за 72 години до оновлення шкідливого контенту, тепер активні, і спостерігається повільний, стійкий підйом активності годину за годиною, оскільки сервіс ретельно відновлюється [4].

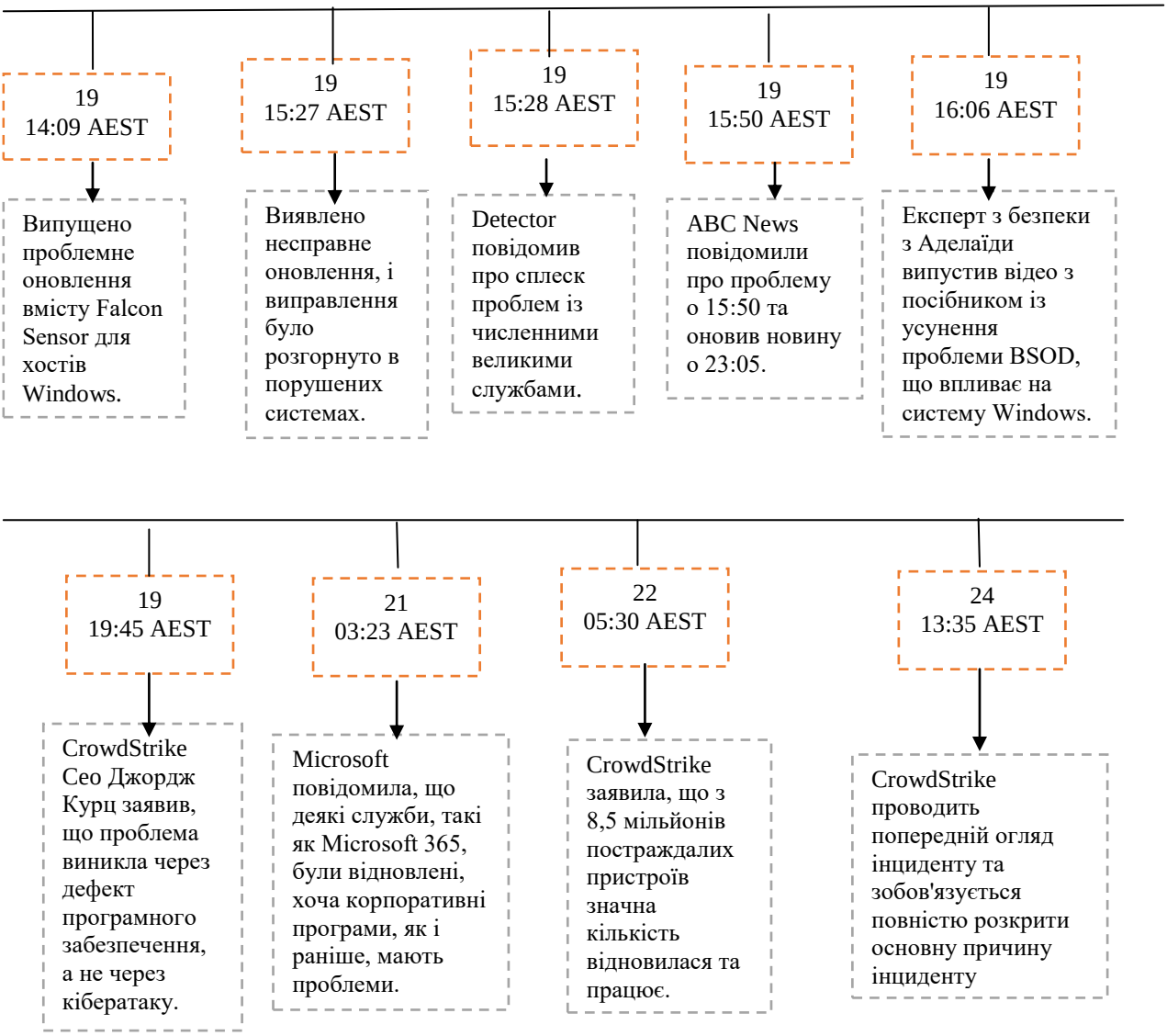


Рис. 1. Хронологія подій 19 липня 2024 року - синій екран смерті Crowdstrike
Джерело: авторська розробка авторів

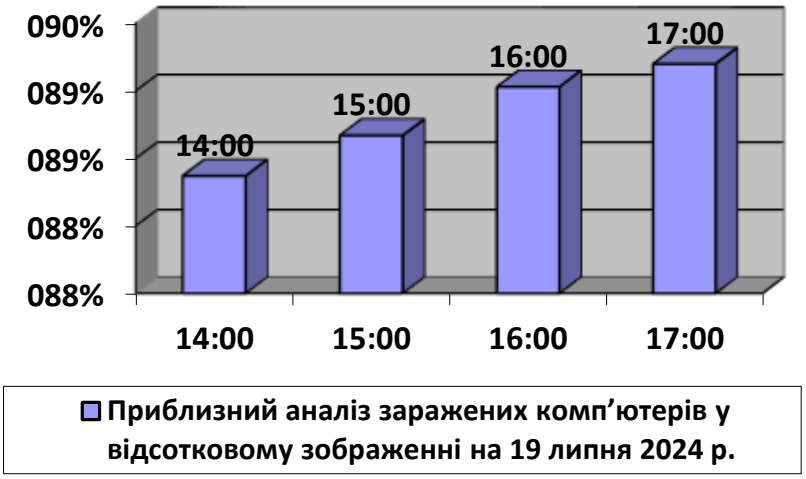


Рис. 2. Зображення проблеми у графіку станом на 19 липня
Джерело: складено автором на основі аналізу [3]

Більш детальний опис CEO Sevco Security Дж. Гай показує на рисунку 3 на період з 19 по 22 липня (рис. 3):

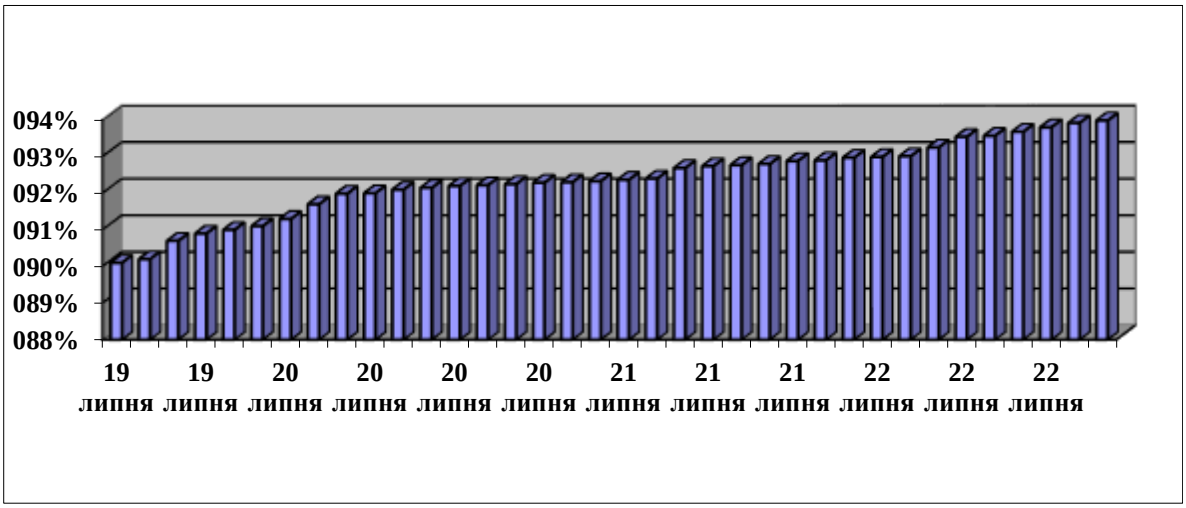


Рис. 3. Детальне зображення відновлення після збою в період з 19 по 22 липня 2024 р.
Джерело: складено автором на основі аналізу [5]

Станом на опівночі робота Crowdstrike відновлена приблизно на 95%, що на 2% більше, ніж у понеділок вранці, і на 5% порівняно з днем п'ятниці.

Ґрунтуючись на оцінці CrowdStrike про 8,5 мільйонів порушених пристроїв, це означає, що приблизно 255 тисяч машин було відновлено за останні ~ 48 годин, причому 425 тисяч машин все ще чекають. Повільний прогрес чітко відбиває втомливі процедури виправлення вручну [5].

На таблиці 1 можна побачити стрічку новин подій коли о 4 ранку почали надходити новини про збій та помилку на ОС Windows.

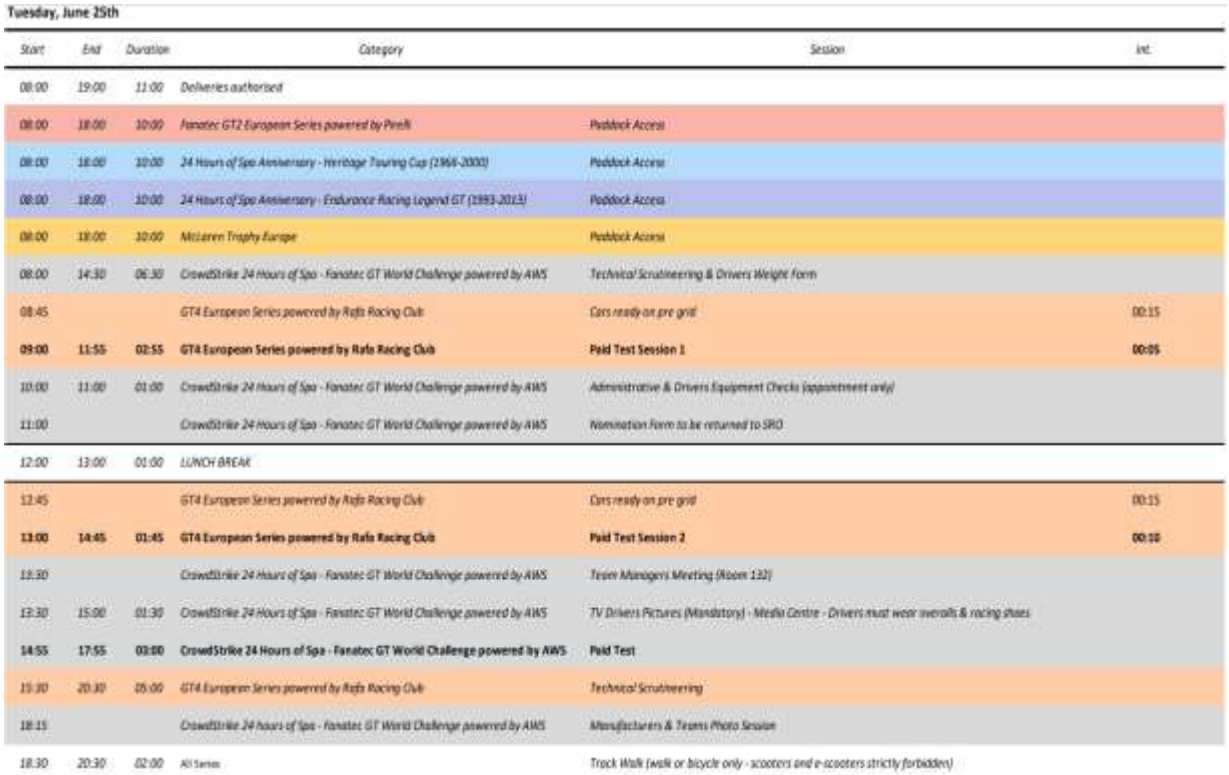
Таблиця 1

Таймінг події

Фаза	Час	Подія
Збій системи (19 липня)	04:09-05:27 UTC	Комп'ютери, що використовують антивірус CrowdStrike версії 7.11 і вище, почали відчувати збої після встановлення помилкового оновлення.
	05:27 UTC	Компанія CrowdStrike виявила проблему і випустила виправлене оновлення
Офіційні заяви (19 липня)	15:30 UTC	Агентство кібербезпеки та інфраструктури США (CISA) випустило попередження про масові збої в роботі IT-систем через оновлення CrowdStrike. Вони підтвердили, що причиною збоїв не була кібератака, і надали рекомендації щодо усунення проблеми.
Оновлення інформації та підтримка клієнтів (20 липня)	21:59 UTC	CrowdStrike оновила інформацію для своїх клієнтів, підтвердивши, що проблема не пов'язана з кібератакою і що системи, які не були оновлені до проблемної версії, працюють нормально.
Рішення від Microsoft (21 липня)	21:22 UTC	Microsoft випустила спеціальний інструмент для відновлення системи, який дозволяє знайти і видалити помилкове оновлення CrowdStrike. За оцінками, це оновлення вплинуло на 8,5 мільйонів пристроїв Windows.
Наслідки для авіакомпанії Delta (23 липня)	23 липня	Департамент транспорту США розпочав розслідування збоїв у роботі авіакомпанії Delta Air Lines, які були пов'язані з масовими відключеннями комп'ютерних систем через оновлення CrowdStrike. Delta скасувала понад 400 рейсів 23 липня і понад 5750 рейсів з 19 по 22 липня.

Джерело: складено автором на основі аналізу [6]

На рисунку 4 можна побачити, що система працює відмінно без всяких нарікань, забезпечуючи високу продуктивність.



Tuesday, June 25th

Start	End	Duration	Category	Session	Int.
08:00	19:00	11:00	Deliveries authorised		
08:00	18:00	10:00	Fanatec GT2 European Series powered by Pirelli	Paddock Access	
08:00	18:00	10:00	24 Hours of Spa Anniversary - Heritage Touring Cup (1966-2000)	Paddock Access	
08:00	18:00	10:00	24 Hours of Spa Anniversary - Endurance Racing Legend GT (1993-2013)	Paddock Access	
08:00	18:00	10:00	McLaren Trophy Europe	Paddock Access	
08:00	14:30	06:30	CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS	Technical Scrutineering & Drivers Weight Form	
08:45			GT4 European Series powered by Rafa Racing Club	Cars ready on pre grid	00:15
09:00	**11:55**	**02:55**	**GT4 European Series powered by Rafa Racing Club**	**Paid Test Session 1**	**00:05**
10:00	11:00	01:00	CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS	Administrative & Drivers Equipment Checks (appointment only)	
11:00			CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS	Nomination Form to be returned to SRO	
12:00	13:00	01:00	LUNCH BREAK		
12:45			GT4 European Series powered by Rafa Racing Club	Cars ready on pre grid	00:15
13:00	**14:45**	**01:45**	**GT4 European Series powered by Rafa Racing Club**	**Paid Test Session 2**	**00:10**
13:30			CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS	Team Managers Meeting (Room 132)	
13:30	15:00	01:30	CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS	TV Drivers Pictures (Mandatory) - Media Centre - Drivers must wear overalls & racing shoes	
14:55	**17:55**	**03:00**	**CrowdStrike 24 Hours of Spa - Fanatec GT World Challenge powered by AWS**	**Paid Test**	
15:30	20:30	05:00	GT4 European Series powered by Rafa Racing Club	Technical Scrutineering	
18:15			CrowdStrike 24 hours of Spa - Fanatec GT World Challenge powered by AWS	Manufacturers & Teams Photo Session	
18:30	20:30	02:00	All Series	Track Walk (walk or bicycle only - scooters and e-scooters strictly forbidden)	

Рис. 4. Перевірка працездатності системи за місяць до інциденту
Джерело: складено автором на основі аналізу [7]

На рисунку 5 можна побачити таблицю TLP системи класифікації для обміну інформацією.

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: backgro
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#00000(
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#00000(
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Рис. 5. TLP система класифікації для обміну інформацією
Джерело: складено автором на основі аналізу [9]

TLP (Traffic Light Protocol) - це система класифікації для обміну інформацією, яка використовується для вказівки на рівень конфіденційності та обмеження розповсюдження інформації. Вона використовується для забезпечення того, що інформація ділиться правильно і безпечно. TLP має чотири рівні:

TLP (Червоний): Інформація є надзвичайно конфіденційною і повинна використовуватися тільки одержувачами, яким вона була призначена. Не може бути поширена далі.

TLP (Помаранчевий): Інформація може бути поширена серед конкретної групи людей або організацій, яким вона була надана. Обмежується доступ у межах організації та потребує обережного поводження.

TLP (Зелений): Інформація може бути поширена в межах спільноти або галузі, але не повинна бути публічно доступною. [8]

TLP (Білий): Інформація не має обмежень щодо розповсюдження і може бути поширена публічно.

За наданим звітом від CrowdStrike: «Одержувачі можуть розповсюджувати цю інформацію по всьому

світу, обмежень на розкриття інформації немає. Джерела можуть використовувати TLP-CLEAR коли інформація несе мінімальний або непередбачений ризик неналежного використання відповідно до застосовних правил та процедурами для публічного розповсюдження. За умови дотримання стандартних правил авторського права інформація TLP-CLEAR може поширюватись без обмежень».

Наприклад, якщо це була б хакерська атака були б застосовані такі методи як:

Вимірювання часу виконання операцій: Атакуючий вимірює час, який система витрачає виконання певних операцій. Ці виміри можуть бути проведені багаторазово, щоб зібрати статистично значущі дані;

Аналіз зібраних даних: Атакуючий аналізує зібрані тимчасові дані, щоб виявити закономірності, які можуть свідчити про виконання певних дій або обробку певних даних;

Вилучення інформації: На основі аналізу часових характеристик атакуючий робить висновки про конфіденційну інформацію, наприклад, про значення ключів шифрування або інших захищених даних.

Та були б застосовані такі методи захисту як:

Уніфікація часу виконання операцій: Робити так, щоб усі критичні операції виконувались за однаковий час, незалежно від даних, що обробляються;

Використання криптографічних алгоритмів, стійких до таймінгових атак: Деякі алгоритми спеціально розробляються так, щоб мінімізувати виток інформації через тимчасові канали;

Обфускація часу виконання: увімкнення випадкових затримок або виконання операцій у випадковому порядку.

Зі звіту CrowdStrike стає зрозуміло що ніякого витоку даних не було, а TLP канали працюють в штатному режимі (вони чисті, прослуховуються, все гаразд) [9].

Датчик Falcon, компонент платформи безпеки CrowdStrike, спричинив глобальний збій. Цей датчик працює локально на пристроях користувачів, скануючи наявність шкідливого ПЗ. Неправильне оновлення викликало збій у роботі, що призвело до масштабних збоїв у системах Microsoft Windows по всьому світу, що зображено на рисунку 7. При скануванні можна побачити, що було помічено «part of the Crowdstrike Application package», що у дампі (репорті) відмічено, що файл був з неофіційного сайту та серверу компанії Crowdstrike.

У п'ятницю оновлення програмного забезпечення, пов'язане з продуктом Falcon від CrowdStrike, викликало каскадний ефект. Falcon розроблений для запобігання кіберзломам з використанням хмарних технологій. На жаль, це оновлення призвело до поширеної проблеми, коли машини перезавантажувалися, викликаючи сумно відому помилку «синій екран смерті» на комп'ютерах Windows [10].

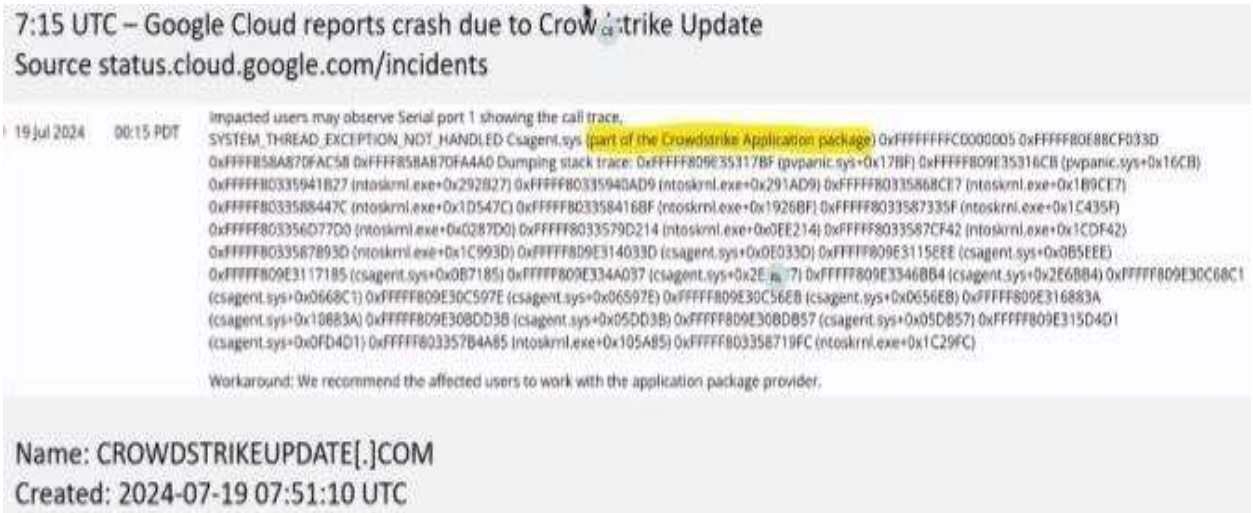


Рис. 6. Дамп файлу з оновленням яке викликало збій
Джерело: складено автором на основі аналізу [10]

Цим як раз могли і скористуватися хакери та під час паніки та закинути файл з вірусним оновленням та поцупити дані користувачів. Приклад такого дампу можна побачити на рисунку 7.

Винуватцем є Channel File 291 (названий шаблоном C-00000291-*.sys), що містить нову логіку виявлення для усунення зловмисного використання іменованих каналів. Повідомляється, що файл обслуговувався тільки протягом короткого вікна за годину між 4 і 5 ранку за всесвітнім координованим часом. За цей час, за оцінками Microsoft, у всьому світі постраждали 8,5 мільйонів пристроїв Windows. Враховуючи природу циклу BSOD, посібник із виправлення порушених пристроїв вимагає завантаження в безпечному режимі та видалення несправного файлу каналу або використання сценаріїв виправлення Microsoft. Якщо пристрій зашифровано за допомогою Bitlocker, для видалення файлу буде потрібно ключ. Мільйони корпоративних систем, що вийшли з ладу, мали каскадні збої у різних галузях, включаючи збої у виробництві, авіаперевезеннях та лікарнях.

Як це часто буває з великими витоками даних, які заслуговують на висвітлення у пресі, кіберзлочинці негайно почали використовувати компоненти на тему CrowdStrike у своїх кампаніях, намагаючись отримати

вигоду з невдач системних адміністраторів і користувачів, які відчайдушно намагаються змусити свої системи працювати. Це включає реєстрацію потенційно шкідливих доменів і присвоєння файлам назв за темами «відновлення CrowdStrike». Ця діяльність залишається низькосортною та опортуністичною.

Після розкриття проблеми CrowdStrike було зареєстровано тисячі (і їх кількість зростає) доменів з тайпсквооттингом, щоб спробувати скористатися жертвами. Ці домени використовуються зловмисниками, щоб заманити жертв для різних можливостей здирництва/шахрайства, включаючи фішинг та розповсюдження шкідливих «виправлень» для цієї проблеми [10].

19 липня 2024 року ZIP-архів з ім'ям crowdstrike-hotfix.zip (SHA256 хеш: c44506fe6elede5a104008755abf5b6ace51f1a84a84ad656a2dccc7f2c39c0eca2) було завантажено до онлайн-сервісу сканування шкідливих програм користувачем із Мексики.

Разом із ZIP-файлом було надано інструкції іспанською мовою, які, схоже, маскуються під утиліту для автоматичного відновлення після проблеми оновлення контенту. Інструкції пропонують користувачеві запустити Setup.exe (SHA256 хеш: 5ae3838d77c2102766538f783d0a4b4205e7d2cdba4e0ad2ab332dc8ab32fea9) для початку встановлення патча.

Зловмисники використовували ці домени, а також загрозливі електронні листи, щоб спробувати вимагати BTC потенційних жертв. Одним із найбільш яскравих прикладів, який швидко з'явився, є створення зловмисниками цих сайтів для прямого запиту оплати за їхнє «виправлення» проблеми.

Наприклад: домен fix-crowdstrike-apocalypse[.]com намагається обдурити жертв, змусивши їх заплатити або за автономний двійковий файл Windows, або за вихідний код виправлення за 500 000 і 1 000 000 євро відповідно (BTC: 0x1AEAe8c6F600d85b3b676ac49bb3816A4eB4455b.) Можна побачити на рис. 7

Ще приклади фейкових «оновлень» називались:

udpate.zip 66fbe2b33e545062a1399a4962b9af4fbbd4b356
crowdstrike-hotfix.zip fef212ec979f2fe2f48641160aadeb86b83f7b35
CrowdStrike Updater.exe 5b2f56953b3c925693386cae5974251479f03928 [11].

Рис. 7. Фейковий сайт складання угоди з CrowdStrike
Джерело: складено автором на основі аналізу [12]

На рисунку 8 можна побачити вразливості і помилки, а також до чого вони привели.

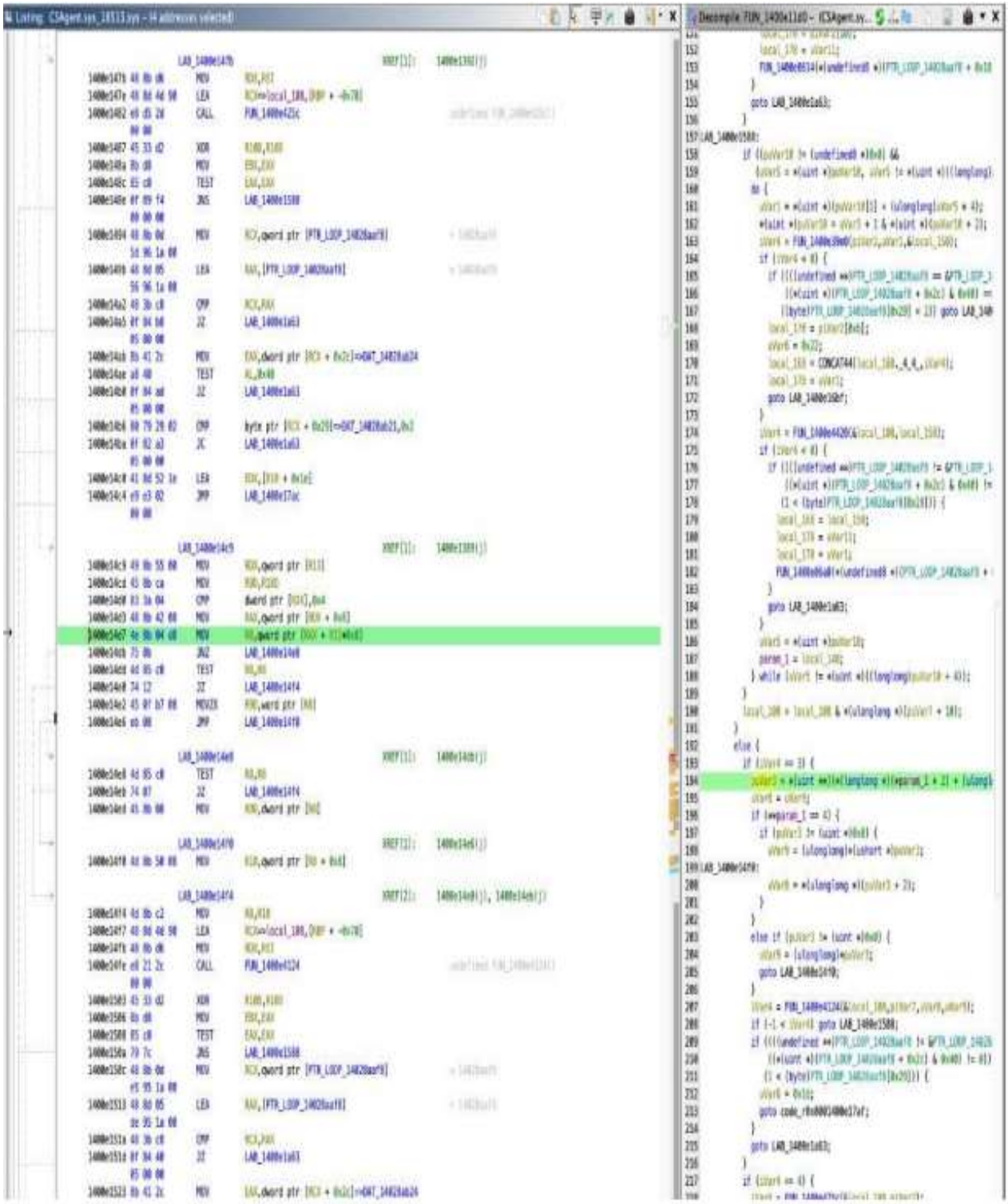


Рис. 8. До чого привели вразливості та помилки
Джерело: складено автором на основі аналізу [11]

C++ є небезпечною для пам'яті мова програмування, відома своїми складнощами в управлінні пам'яттю.

Завантаження файлу каналу передбачає складні операції з пам'яттю, такі як пошук за масивом та зміщенням пошук по масиву та зсуву. Існують побоювання, що CSAgent міг отримати доступ до неініціалізованих ділянок пам'яті.

Поведінка може не одразу вказувати на проблему і потенційно може пройти в залежності від вмісту неініціалізованої пам'яті.

Звіти про те, що на деяких веб-сайтах BSOD виникає на одних машинах, а на інших - ні, викликають занепокоєння щодо варіативності проблеми.

Точна причина, чому проблема пройшла QA-тестування, залишається незрозумілою, і остаточної відповіді може не бути.

Пам'ять у комп'ютері представлена як один гігантський масив чисел. Представляємо ці числа тут у шістнадцятковому вигляді, який має основу 16 (hexadecimal), тому що з ним простіше працювати з низки причин. Так в чому ж проблема? Комп'ютер спробував прочитати адресу пам'яті 0x9c (він же 156).

Чому це погано? Це неприпустима область пам'яті будь-якої програми. Будь-яка програма, яка спробує прочитати з цієї галузі, БУДЕ НЕГАЙНО ЗАВЕРШЕНА WINDOWS. Ось що бачите тут із цим дампом стека. Тобто пам’ять яка не використовується, а на неї посилаєтесь то робота буде негайно завершена з критичною помилкою, а ось який буде результат на рисунку 9 [12]:

Рис. 9. Дамп приклад з CrowdStrike
Джерело: складено автором на основі аналізу [11]

То чому ж адреса пам'яті 0x9c намагається бути прочитаною? Тому що це помилка програміста. C++, мова, яка використовує crowdstrike, любить використовувати адресу 0x0 як особливе значення, щоб позначити «тут нічого немає», не намагайтеся отримати доступ до неї.

Програмісти C++ повинні перевіряти це, коли передають об'єкти, «перевіряючи повне значення null». Зазвичай ви побачите щось на кшталт цього:

```
string * p = get_name ();
if (p == NULL)
{
print("Could not get name");
}
```

Частина string* означає, що ми маємо «покажчик» на початок строкового значення. Якщо він дорівнює null, то там нічого немає, не намагайтеся отримати доступ до нього. Отже, давайте візьмемо універсальний об'єкт із вмістом:

```
struct Obj { int a; int b; };
```

якщо ми створимо вказівник на нього: Obj * obj = new Obj (); Ми можемо отримати його початкову адресу, скажімо, це щось випадкове, наприклад 0x9030=36912. Тоді адреса: obj дорівнює 0x9030 obj->a дорівнює 0x9030 + 0x4 obj->b дорівнює 0x9030 усуненням від початкової адреси.

Тепер припустимо наступне: Obj * obj = NULL; Тоді адреса: obj дорівнює 0 obj->a дорівнює 0 + 4 obj->b дорівнює 0 + 8 Отже, якщо зробимо це з вказівником NULL: print(obj->a); дамп стека програми, як можна побачити вище не зможе прочитати значення 0x000000004.

У цьому стековому дампі на рисунку 12 бачимо, що він намагається прочитати значення пам'яті 0x9c. У людських числах це значення 156. Так ось, що сталося, так це те, що програміст забув перевірити, що об'єкт, з яким він працює, недійсний, він спробував отримати доступ до однієї зі змінних членів об'єкта.

NULL + 0x9C = 0x9C = 156. Це недійсна область пам'яті. І що погано в цьому, так це те, що це спеціальна програма, яка називається системним драйвером, яка має привілейований доступ до комп'ютера. Тому операційна система змушена, з міркувань обережності, негайно аварійно завершити роботу.

Це те, що викликає синій екран смерті. Комп'ютер може відновитися після збою в непривілейованому коді просто завершивши програму, але не системний драйвер. Коли ваш комп'ютер виходить з ладу, у 95% випадків це відбувається через збій у системних драйверах [13].

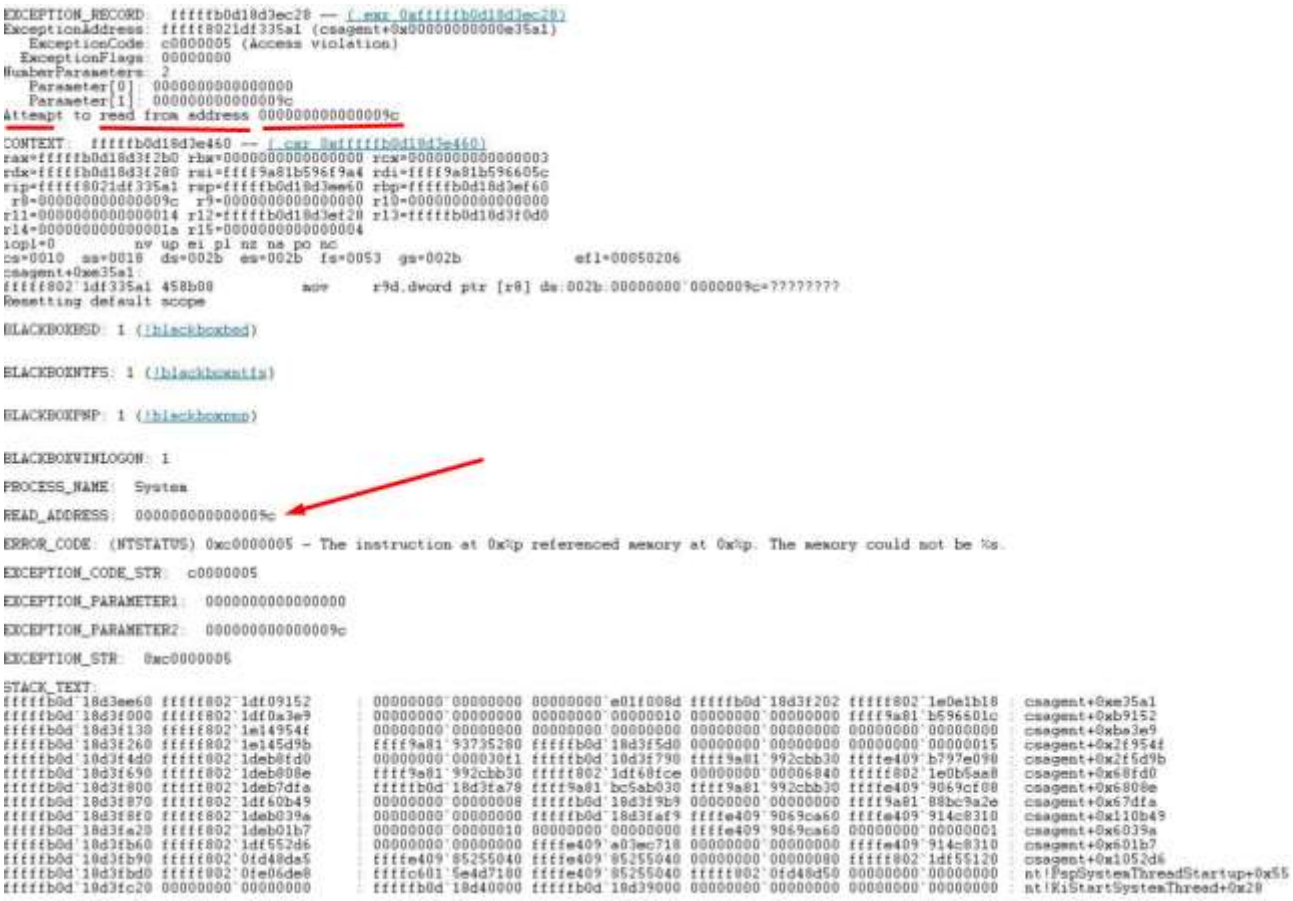


Рис. 10. Стековий дамп
Джерело: складено автором на основі аналізу [11]

Якби програміст зробив перевірку на NULL або якби він використовував сучасні інструменти, які перевіряють такі речі, це може бути виявлено. Але якось це потрапило у виробництво, а потім було відправлено як примусове оновлення Crowdstrike.

Виправлення в майбутньому полягає в тому, що Майкрософт необхідно мати більш досконалі політики для відкату дефектних драйверів, а не тільки для сирих ризикованих оновлень для клієнтів. Crowdstrike, швидше за все, підвищить свого співробітника безпеки коду, щоб він ввів інструменти очищення коду, які будуть автоматично виявляти це.[14] Crowdstrike, швидше за все, уважно розгляне можливість переписування свого системного драйвера з того, що він є зараз, C++, більш сучасною мовою, такою як Rust, в якій цієї проблеми немає. C++ – це складно. Можливо, у них є інженер DEI, який цим займався, але для критично важливого програмного забезпечення, такого як це, Crowdstrike повинен був налаштувати автоматичне тестування з використанням «дезінфікуючого» засобу адрес та засобу потоків, яке запускається при кожному оновленні коду [15].

Це був покажчик NULL із небезпечної для пам'яті мови C++. Це нагадування про те, наскільки критичні оновлення програмного забезпечення та необхідність у їх ретельному тестування перед розгортанням, щоб забезпечити стабільну роботу системи, мінімізувати ризики вразливостей і уникнути можливих проблем у майбутньому [16].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Підсумовуючи інцидент з компанією CrowdStrike, можна зазначити, що все одно це складна багаторівнева проблема яка потребувала свого вирішення. Хоча багато аргументів наведено в статті, що детектор Falcon зарекомендував себе спочатку на досить гідному рівні, а потім допустив зараження 8,5 мільйонів комп’ютерів не можна сказати що його встановлення марне, це не так. Компанія CrowdStrike мобілізувала всіх фахівців, та виклала максимум зусиль для того щоб ліквідувати наслідки, повернути свою репутацію, вибачилась за завдані користувачам незручності. Небайдужі IT компанії теж вирішили допомогти в цьому жахливому для світу кібербезпеки події.

Насамкінець хоча винна сама компанія CrowdStrike не можна не описати того факту, що через

необачність програміста на мові C++, саме це як раз і викликало критичну помилку та синій екран смерті (BSOD). Це не означає що треба відмовитись від C++ і переходити на іншу мову програмування, а треба було в даній ситуації дотримуватись більше карантинних мір, та тестувати оновлення на спеціально взятих системах і не випускати, його занадто рано. Через це багато системних адміністраторів під час збою піддалися частці випадку та почали в інтернеті шукати вирішення проблеми, де могли попасти в пастку соціальної інженерії - під назвою: «crowdstrike-hotfix.zip». Злочинці за певні кошти передавали файл із вирішенням проблеми, а насправді крали данні користувачів і підприємців.

Таким чином збій CrowdStrike показав як комплексна чітко побудована та налаштована система може в мить опинитись у дуже скрутному становищі. Ця праця підкреслює що сфера кібербезпеки та IT потребує постійних нововведень та інновацій. Дані події яскраво показали з якими труднощами стикається чітко налаштована система кібербезпеки, але без колективних зусиль ця робота не коштуватиме нічого.

Література

1. Бевза В.І., Слатвінська В.М. Вплив збою Crowdstrike на мега-витків паролів: чи є зв'язок? Ч. 1. Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. № 4.

2. Wolf R. Navigating the Chaos: Cyber Criminals Exploit CrowdStrike Outage 2024. URL: https://www.linkedin.com/pulse/navigating-chaos-cyber-criminals-exploit-crowdstrike-outage-wolf-aftcc?utm_source=share&utm_medium=member_android&utm_campaign=share_via

3. Guy J.J. Аналіз даних проведений компанією Sevco. 2024. URL: https://www.linkedin.com/posts/jjguy_based-on-sevcos-analysis-of-agent-inventory-activity-7220178636623032321-_1MW?utm_source=share&utm_medium=member_android

4. Метричний аналіз фахівця CEO Sevco Security Джей Джея Гая про відновлення серверів CrowdStrike 2024. URL: https://www.linkedin.com/feed/update/urn:li:activity:7221196423168425987?trk=public_post_comment-text

5. Аналіз від Sevco за весь період подій з критичною помилкою CrowdStrike 2024 URL: https://www.linkedin.com/posts/jjguy_as-of-midnight-crowdstrike-service-is-approximately-activity-7221917327825522689-gHlC?utm_source=share&utm_medium=member_desktop

6. Rawal V. Technical Post-Mortem on the July 19th CrowdStrike Falcon Sensor Outage: A Detailed Overview with Microsoft Architecture Insights 2024. URL: https://medium.com/@vp2005rawal/technical-post-mortem-on-the-july-19th-crowdstrike-falcon-sensor-outage-a-detailed-overview-with-35c148d067ce.

7. CrowdStrike 24 Hours of Spa (Belgium) 2024. URL: https://www.gt-world-challenge-europe.com/images/results/221/2024%20Fanatec%20GT%20World%20Challenge%20-%20CrowdStrike%2024%20Hours%20of%20Spa%20-%20Official%20Detailed%20Timetable%20V1.pdf.

8. CrowdStrike BSOD Loop Issue UPDATE - Version 1.1. 2024. URL: https://www.ncsc.gov.ie/pdfs/CrowdStrike_BSOD_Loop_Issue.pdf

9. Trafic light protocol (TLP) URL: Traffic Light Protocol (TLP) (first.org)

10. Remediation and Guidance Hub: Falcon Content Update for Windows Hosts. 2024. URL: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

11. Case Study : The CrowdStrike Outage 2024. URL: https://www.linkedin.com/pulse/case-study-crowdstrike-outage-vishal-tripathi-zdfbc?utm_source=share&utm_medium=member_android&utm_campaign=share_via

12. CrowdStrike Global Outage – Threat Actor Activity and Risk Mitigation Strategies. 2024. URL: https://www.sentinelone.com/blog/crowdstrike-global-outage-threat-actor-activity-and-risk-mitigation-strategies/

13. Browne R. How a software update from cyber firm CrowdStrike caused one of the world's biggest IT blackouts 2024 URL: https://www.cnbc.com/2024/07/19/what-is-crowdstrike-crwd-and-how-did-it-cause-global-it-outages.html

14. Understanding a Kernel Oops! - Open Source For You (opensourceforu.com). 2024. URL: https://www.opensourceforu.com/2011/01/understanding-a-kernel-oops/

15. Chiong G.M. The rise of ransomware: Motivations, contributing factors, and defenses. 2023. URL: https://www.proquest.com/openview/a23524aec86e67e2b9c4840209690793/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y

16. Daswani N., Elbayadi M., Daswani N., et al. Technology defenses to fight the root causes of breach: Part One, Practical Cybersecurity Lessons for Companies, Springer, 2021. URL: https://www.sciencedirect.com/science/article/pii/S2667345223000561

References

1. Bevza V.I., Slatvinska V.M. Vplyv zboiu Crowdstrike na meha-vytkiv paroliv: chy ye zviazok? Ch. 1. Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Tekhnichni nauky. 2024. № 4.

2. Wolf R. Navigating the Chaos: Cyber Criminals Exploit CrowdStrike Outage 2024. URL: https://www.linkedin.com/pulse/navigating-chaos-cyber-criminals-exploit-crowdstrike-outage-wolf-aftcc?utm_source=share&utm_medium=member_android&utm_campaign=share_via

3. Guy J.J. Analiz danykh provedenyi kompaniieiu Sevco. 2024. URL: https://www.linkedin.com/posts/jjguy_based-on-sevcos-analysis-of-agent-inventory-activity-7220178636623032321-_1MW?utm_source=share&utm_medium=member_android

4. Metrychnyi analiz fakhivtsia SEO Sevco Security Dzhei Dzheia Haia pro vidnovlennia serveriv CrowdStrike 2024. URL: https://www.linkedin.com/feed/update/urn:li:activity:7221196423168425987?trk=public_post_comment-text

5. Analiz vid Sevco za ves period podii z krytychnoiu pomylkoiu CrowdStrike 2024 URL: https://www.linkedin.com/posts/jjguy_as-of-midnight-crowdstrike-service-is-approximately-activity-7221917327825522689-gHlC?utm_source=share&utm_medium=member_desktop

6. Rawal V. Technical Post-Mortem on the July 19th CrowdStrike Falcon Sensor Outage: A Detailed Overview with Microsoft Architecture Insights 2024. URL: https://medium.com/@vp2005rawal/technical-post-mortem-on-the-july-19th-crowdstrike-falcon-sensor-outage-a-detailed-overview-with-35c148d067ce.

7. CrowdStrike 24 Hours of Spa (Belgium) 2024. URL: https://www.gt-world-challenge-europe.com/images/results/221/2024%20Fanatec%20GT%20World%20Challenge%20-%20CrowdStrike%2024%20Hours%20of%20Spa%20-%20Official%20Detailed%20Timetable%20V1.pdf.

8. CrowdStrike BSOD Loop Issue UPDATE - Version 1.1. 2024. URL: https://www.ncsc.gov.ie/pdfs/CrowdStrike_BSOD_Loop_Issue.pdf

9. Trafic light protocol (TLP) URL: Traffic Light Protocol (TLP) (first.org)

10. Remediation and Guidance Hub: Falcon Content Update for Windows Hosts. 2024. URL: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

11. Case Study : The CrowdStrike Outage 2024. URL: https://www.linkedin.com/pulse/case-study-crowdstrike-outage-vishal-tripathi-zdfbc?utm_source=share&utm_medium=member_android&utm_campaign=share_via

12. CrowdStrike Global Outage – Threat Actor Activity and Risk Mitigation Strategies. 2024. URL: https://www.sentinelone.com/blog/crowdstrike-global-outage-threat-actor-activity-and-risk-mitigation-strategies/

13. Browne R. How a software update from cyber firm CrowdStrike caused one of the worlds biggest IT blackouts 2024 URL: https://www.cnbc.com/2024/07/19/what-is-crowdstrike-crwd-and-how-did-it-cause-global-it-outages.html

14. Understanding a Kernel Oops! - Open Source For You (opensourceforu.com). 2024. URL: https://www.opensourceforu.com/2011/01/understanding-a-kernel-oops/

15. Chiong G.M. The rise of ransomware: Motivations, contributing factors, and defenses. 2023. URL: https://www.proquest.com/openview/a23524aec86e67e2b9c4840209690793/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y

16. Daswani N., Elbayadi M., Daswani N., et al. Technology defenses to fight the root causes of breach: Part One, Practical Cybersecurity Lessons for Companies, Springer, 2021. URL: https://www.sciencedirect.com/science/article/pii/S2667345223000561