Як окупанти вбивали "Київстар", який і досі належить путінському "гаманцю"

Читать на русском | Додати як бажане джерело в Google

Як окупанти вбивали "Київстар", який і досі належить путінському "гаманцю"

Хакерська атака рашистів зупинила роботу найбільшого мобільного оператора країни (який й досі опосередковано належить рашисту Фрідману). 24 мільйони абонентів залишилися поза мережею. Як це сталося та коли зможуть повністю відновити зв'язок?

У червні "Київстар" налічував 24,1 млн абонентів мобільного зв'язку та понад 1,1 млн абонентів фіксованого Інтернету, зазначає "ЕКОНОМІЧНА ПРАВДА".

Атака на найбільшого мобільного оператора не просто позбавила зв'язку половину населення України. Напад вдарив по великому колу бізнесів, залежних від зв'язку мобільного оператора, державних установах і навіть конкурентах "Київстару", які не були готові до значного зростання трафіку через перехід до них нових користувачів.

Зранку відсутність зв'язку "Київстар" назвав технічним збоєм, а ближче до вечора – потужною кібератакою, яка значно пошкодила IT-інфраструктуру оператора.

Служба безпеки України припускає, що за атакою можуть стояти спецслужби Росії. З початку великої війни "Київстар" не раз зазнавав кібератак, проте щоразу вдало їх відбивав. Тепер, схоже, ворогу вдалося досягти цілі.

Як усе "лягло"

12 грудня о 8:04 ранку мобільний оператор "Київстар" повідомив про технічний збій і можливі обмеження послуг зв'язку та доступу в Інтернет для частини абонентів. "Спеціалісти компанії працюють над усуненням проблеми", – зазначалося в повідомленні.

У той самий час у внутрішніх чатах співробітників "Київстару" з'явилися повідомлення про кібератаку на ядро мережі та бази даних мобільного оператора. Паралельно анонімні Telegram-канали почали поширювати неправдиву інформацію про нібито обшуки правоохоронців в офісі компанії.

Уже через кілька годин стало очевидно, що масштаб проблеми значно серйозніший. Крім мобільного зв'язку та Інтернету, не працювали мобільний застосунок "Мій Київстар", домашній Інтернет від "Київстару" та сайт оператора.

Українці, які користуються мобільним зв'язком та домашнім Інтернетом від "Київстару", залишися без зв'язку в усій країні. Не допомогли їм і спроби змінити оператора. У Мінцифри повідомили, що абоненти "Київстару" не можуть перейти до інших операторів, оскільки збій у мережі компанії вплинув на національний роумінг.

Пізніше міністр розвитку громад, територій та інфраструктури Олександр Кубраков заявив, що в мережі мобільного оператора відбуваються ремонтні роботи, які можуть тривати чотири-п'ять годин.

Ближче до опівдня компанія визнала, що причиною масштабного збою стала потужна хакерська атака: "Станом на зараз відомо, що персональні дані абонентів не скомпрометовані. На цей час фахівці оператора працюють над усуненням наслідків хакерської атаки для якнайскорішого відновлення зв'язку та надання сервісів".

У компанії також поспішили запевнити, що абоненти, які не мали зв'язку або не могли скористатися сервісами оператора, отримають компенсацію.

Що насправді сталося

Кібератака на "Київстар" призвела до найбільшого збою серед усіх українських операторів за останні роки, зазначив голова підкомітету Верховної Ради з кібербезпеки Олександр Федієнко.

За словами співрозмовника ЕП в уряді, атака на "Київстар" є результатом тривалої і грандіозної роботи хакерів. "Ще до початку великої війни російські хакери не раз намагалися атакувати критичну інфраструктуру України, зокрема і мобільних операторів. При цьому у "Київстарі" сильна система захисту від кібератак, вони вкладали в це багато грошей і в останні два роки показували свою ефективність", – пояснює джерело ЕП.

"Ми фіксували і в нас зросли кібер- та хакерські атаки від початку повномасштабного вторгнення десь на 400%. Ми з цим зіштовхувалися постійно. Наразі це найпотужніша атака від початку великої війни", – повідомила директорка з корпоративних комунікацій "Київстару" Анна Захараш.

Атака на ядро мережі є серйозним ударом по оператору, оскільки саме воно обробляє весь трафік, який передається через мобільну мережу. Цей трафік охоплює голосові дзвінки, смс та мобільний Інтернет.

Щоб зафіксувати обставини та наслідки протиправних дій з втручання в діяльність мережі "Київстару", оператор залучив правоохоронців та спецслужби. У Держспецзв'язку повідомили, що висновки робити рано.

"Триває розслідування інциденту, що спричинив технічний збій у роботі оператора, внаслідок якого тимчасово недоступні послуги зв'язку та доступу в інтернет, фахівцями відповідних служб. Серед інших до цієї роботи залучені фахівці урядової команди реагування на надзвичайні комп'ютерні події CERT-UA", – відповіли у відомстві.

Одна з версій, яку досліджують слідчі СБУ, – причетність до хакерської атаки спецслужб Росії.

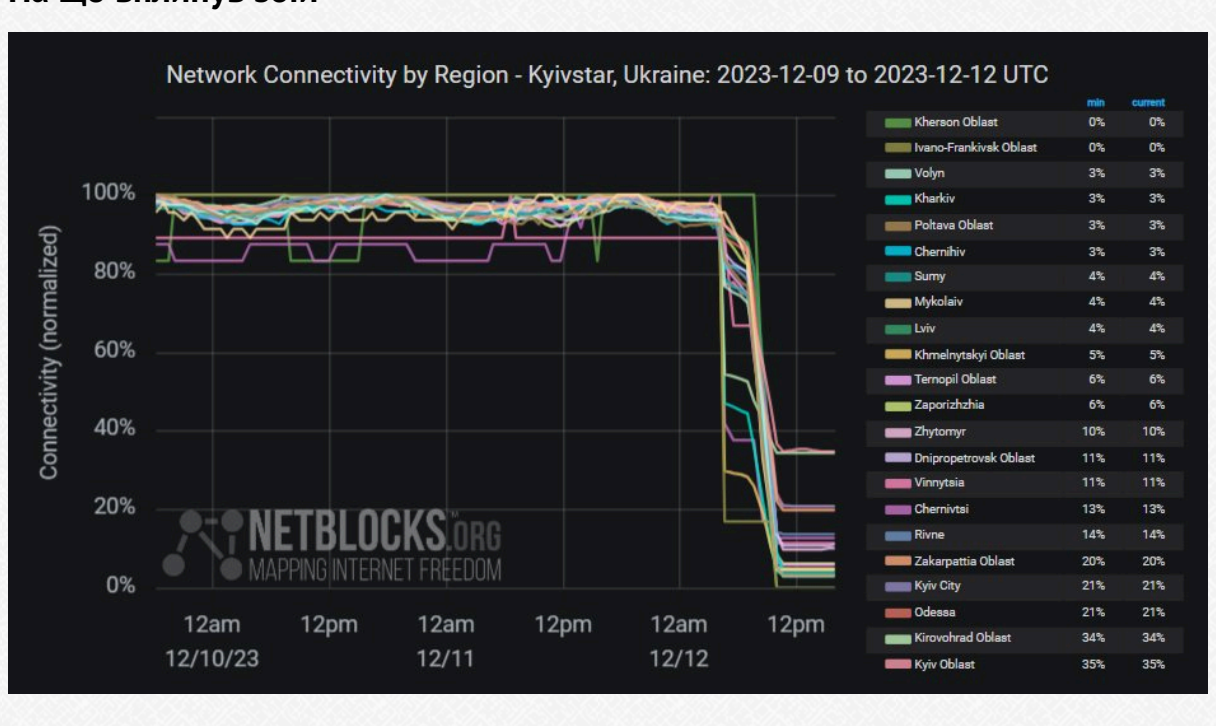
Гендиректор "Київстару" Олександр Комаров наголосив, що кібератака була дуже потужною і через це була частково зруйнована IT-інфраструктура оператора.

"Наші IT-спеціалісти не мали доступу до внутрішніх систем. Весь периметр, який захищається спеціальною директорією, де прописані всі права, повністю зруйнований. Тому нам потрібно було діяти на фізичному рівні, під'єднуючись, умовно, через патч-корди (комутаційні кабелі) до кожного елемента мережі, щоб зрозуміти рівень руйнування мережі на поточний час", – зазначив Комаров.

За фактом хакерської атаки на "Київстар" СБУ відкрила кримінальне провадження за вісьмома статтями кримінального кодексу.

"Після виникнення інциденту в офіси компанії виїхала оперативно-слідча група СБУ, яка документує всі обставини атаки. Крім того, за місцем події працюють кіберфахівці СБУ, які надають допомогу співробітникам "Київстару" і координують зусилля всіх державних установ для якнайшвидшого відновлення мережі", – повідомили ЕП у відомстві.

На що вплинув збій



Мобільні оператори забезпечують функціонування багатьох сфер економіки. Завдяки їхньому Інтернету працює банківська інфраструктура. Про збої в роботі банкоматів та платіжних терміналів повідомили найбільші установи.

"Масштабний збій сервісів компанії "Київстар" призвів до непрацездатності незначної частини банкоматів, POS-терміналів та інформативно-платіжних терміналів "Ощадбанку". Повне відновлення їхньої роботи відбудеться після ліквідації збою сервісів компанії "Київстар", – повідомили в пресслужбі "Ощадбанку".

На проблеми скаржаться і в "ПриватБанку" – найбільшому банку країни: "У зв'язку із складнощами в роботі "Київстару" деякі POS-термінали, банкомати і термінали самообслуговування можуть працювати нестабільно або не мати зв'язку". За даними співрозмовників ЕП у фінансовій установі, від "Київстару" залежить робота до 5% банкоматів, до 10% терміналів самообслуговування та до 30% POS-терміналів.

Про проблеми в роботі розрахункової інфраструктури пише і пресслужба "Райффайзен банку": "Частина POS-терміналів може бути частково недоступною на касах магазинів. Радимо скористатися терміналом іншого банку або зробити розрахунок готівкою".

Інші великі банки через збої в "Київстарі" відчули менші проблеми. ПУМБ повідомив про труднощі з автентифікацією певних операцій: "Клієнти можуть спостерігати деякі проблеми при отриманні смс та push-повідомлень з кодами автентифікації для проведення платіжних операцій".

Крім опосередкованого впливу на банківську систему, протягом дня фіксувалася інтенсифікація роботи хакерів проти банківської інфраструктури. "Масована DDoS атака на "Моно". Об'єкт атаки: точки входу на Amazon (банки, сайт)", – повідомив співзасновник monobank Олег Гороховський близько 13:00. Відбили хакерську атаку менш ніж за годину.

Представники інших банків та НБУ не зафіксували підвищеної хакерської активності. "Усі інформаційні системи Національного банку безперебійно працювали і продовжують працювати. Зокрема – система електронних платежів, якою користуються банки, офіційний сайт та внутрішня комп'ютерна мережа НБУ", – повідомила пресслужба НБУ.

Збій у роботі найбільшого оператора країни вплинув і на інші бізнеси. У службі таксі "Уклон" повідомили про помітне зменшення активності замовлень через те, що значна частина клієнтів залишилася без зв'язку.

"Щоб гарантувати безперебійність адресного обслуговування, ми забезпечили кур'єрів sim-картками альтернативних операторів. Кур'єри зв'язуються з клієнтами усіма можливими способами", – зазначили в пресслужбі "Нової пошти".

Збій у роботі "Київстару" вплинув і на систему цивільного захисту населення. Зокрема, через це тимчасово не працює система оповіщення про повітряні тривоги в Сумській області та деяких містах Київщини: Бучі, Ірпені, Вишневому, Березані, Сквирі, Ржищеві, Тараші та Володарці.

"У населених пунктах, де є проблеми з роботою системи, будуть працювати екіпажі патрульної поліції та ДСНС. Вони через гучномовці сповіщатимуть про повітряну небезпеку, повідомили в Київській обласній військовій адміністрації.

У Львові через проблеми із зв'язком не змогли автоматично вимкнути ліхтарі, тож міським службам довелося відключати лінії вуличного освітлення вручну.

Чому не спрацював національний роумінг

З початку великої війни на випадок збоїв у роботі операторів мобільного зв'язку існує план "Б" – національний роумінг: можливість абонентів одного оператора користуватися інфраструктурою інших. Проте цей план не спрацював.

У Міністерстві цифрової трансформації пояснили, що національний роумінг не діє, бо мережа "Київстару" не може передати інформацію про своїх абонентів мережам інших операторів.

У компанії додали, що скористатися національним роумінгом неможливо через часткову руйнацію системи HLR/HSS – регістрів з абонентськими даними. "Регістри заблоковані, тому не може бути доступу до національного роумінгу. Ми не пускаємо в мережу зовнішні контакти, навіть якщо вони верифіковані як наші партнери", – зазначив Комаров.

У Мінцифри додали, що це тимчасова проблема, над якою активно працюють усі спеціалісти "Київстару".

Що з іншими операторами

Внаслідок збоїв у роботі "Київстару" постраждали й інші оператори – Vodafone та lifecell. Зокрема, через збільшення трафіку ці компанії повідомили про тимчасові проблеми з роботою своїх сайтів та застосунків.

Оскільки багато клієнтів "Київстару" почали переходити до інших операторів, зросло навантаження на інфраструктуру останніх. "Навантаження на мережу збільшилося, також виросло число звернень наших і не наших абонентів щодо ситуації з мобільним зв'язком. Через це в деяких абонентів Vodafone можуть виникати обмеження в доступі до сервісів обслуговування. З мобільними послугами все гаразд, мережа працює як зазвичай", – повідомили у Vodafon.

Про зростання навантаження повідомили і в lifecell. "У мережі lifecell спостерігаються труднощі з поповненням рахунку, активацією нових абонентів, сайтом та застосунком. Водночас робота нашої мережі наразі стабільна. Трафік на наш сайт виріс більш ніж у п'ять разів, попит на eSIM збільшився в десять разів", – зазначили в компанії.

Інші оператори мобільного зв'язку запевняють, що працюють над посиленням захисту від кіберзагроз. Щоправда, деталей такої підготовки не розкривають.

"Наші фахівці щодня фіксують кібератаки. Ми постійно посилюємо і вдосконалюємо захист мережі, адаптуємо нові механізми захисту й технічні рішення, пристосовуємо їх до актуальних загроз, щоб абоненти могли вільно користуватися послугами", – зазначають у пресслужбі lifecell.

Коли відновлять "Київстар"

Коли оператор відновить надання послуг, точно відповісти неможливо. Після 12 годин відсутності зв'язку у "Київстарі" не могли спрогнозувати час відновлення роботи.

Пізніше речниця компанії Ірина Леліченко зазначила, що фахівці "зроблять усе можливе, аби остаточно завершити цю роботу протягом 13 грудня 2023 року". "Відновлення сервісів може відбуватися поступово, про що ми повідомлятимемо додатково", – пояснили в "Київстарі".

Військовослужбовець, інженер і волонтер Сергій Флеш припускає, що відновлення зв'язку можливе через добу: "Того, що сталося, не було ніде і ніколи (за масштабом) за всю історію мобільного зв'язку і не тільки в Україні. Моя оцінка виправлення ситуації – доба з моменту початку робіт. За хорошим прогнозом".

Співрозмовники в уряді припускають, що за найгіршого сценарію на відновлення можуть знадобитися кілька діб.

Гендиректор "Київстару" наголосив, що компанії допомагають найбільші постачальники – Ericsson та Microsoft. "Кожен допомагає як може, тому що на різних елементах мережі працює різне обладнання і різні технології від різних постачальників. Ми кожну годину, коли з'ясовуємо рівень руйнувань, підключаємо цих постачальників, щоб починати домовлятися", – сказав Комаров.

Він додав, що оператор частково надає послугу фіксованого інтернету, але якщо ситуацію не вдасться виправити, то вона перестане працювати орієнтовно опівночі 13 грудня.

На кінець дня 13 грудня, частково став відновлюватись голосовий зв'язок.

Збій перед націоналізацією?

Хакерська атака на "Київстар" сталася тоді, коли держава почала готуватися до його ймовірної націоналізації. "Там зараз відповідні служби вивчають наявність правової ситуації. Думаю, є висока ймовірність прийняття санкцій з подальшою конфіскацією цієї компанії", – пояснював заступник керівника ОП Ростислав Шурма.

Раніше суд арештував усі корпоративні права в Україні, що належали підсанкційним російським олігархам Михайлу Фрідману, Петру Авену та Андрію Косогову, які входять до оточення Путіна та фінансують російську агресію. Серед арештованих судом активів були й частки в "Київстарі", а також менша частка в іншому операторі мобільного зв'язку – lifecell.

У жовтні повідомлялося, що Мін'юст готує позов до Вищого антикорупційного суду стосовно стягнення активів підсанкційного російського олігарха Михайла Фрідмана в дохід України, зокрема – частини мобільного оператора "Київстар".

Теги: кібератаки | Кибератаки | мобільний зв'язок | Мобільні оператори | мобильные операторы | Київстар | Фридман Михаил | Киевстар VEON | Киевстар

Юлія Більченко
ВИПУСКОВИЙ РЕДАКТОР

14 грудня 2023 г., 14:52 | Переглядів: 2995 | Коментарі: 2

Роздрукувати | Надіслати товаришу

Коментарі: