Гаманець або життя: як працює бізнес кіберздирництва

Злочинці лютують чимдалі більше, їхні апетити також невпинно зростають.

Світ охопила епідемія кіберздирництва. Мало не щодня надходять повідомлення про атаки на комерційні компанії, школи, лікарні. На нещодавніх президентських виборах у США здирники і завдали удару по базі даних у одному округів штату Джорджія, заблокувавши підрахунок голосів, поданих заочно.

Компанії, які займаються кіберзахистом, стверджують, що кількість здирницьких атак зростає рік за роком, так само, як і втрати від них. За оцінками ***Emsisoft***, у 2019 році глобальні збитки від атак здирників могли сягнути від $6,3 трлн до $25,1 трлн, виходячи з вартості простою на рівні $5,6 тис. за хвилину (згідно з розрахунками ***Gartner***) і середньої тривалості у 16 днів. За основу розрахунків було взято 452 тис. атак — саме таку кількість зафіксував у світі сервіс ***ID Ransomware***, який збирає дані від жертв здирників (при цьому Emsisoft вважає, що лише 25% жертв надають інформацію у цю базу даних). З них 24,77 тис. припало на Сполучені Штати, 11,58 тис. — на Італію і 10,69 тис. — на Німеччину. Як випливає зі звіту компанії ***Deep Instinct***, торік здирники заподіяли у світі шкоди на $11,5 млрд, причому середня атака обійшлася жертвам у в $141 тис. — утричі більше, ніж у 2018-му.

Вектори атак

Компанія ***Coveware***, яка саме спеціалізується на здирниках і також веде статистику атак, на базі даних, отриманих від власної платформи реагування на інциденти, стверджує, що виходячи з понад 1000 інцидентів, зафіксованих з січня по березень цього року, найпоширенішим вектором атак є використання протоколу віддаленого робочого столу — Remote Desktop Protocol (RDP). Це цілком добропорядний засіб, за допомогою якого IT-адміністратори можуть дистанційно керувати різними системами. Проте цей протокол відкриває чудову лазівку для зловмисників. RDP зламують простим підбором паролів, або ж купуючи облікові дані на спеціалізованих торгівельних майданчиках (вартість цих даних цілком дешева, в районі $30), або за допомогою фішингу. «Коли здирники на кшталт Dharma або SamSam завдають удару, це, ймовірно, не перший злам, — зауважує Coveware. — Перший, імовірно, призвів до компрометації облікових даних RDP, які потім було продано здирникам». Загалом на метод компрометації RDP припадає понад половини здирницьких атак, а два роки тому їх частка сягала 90% (**рис. 1**).

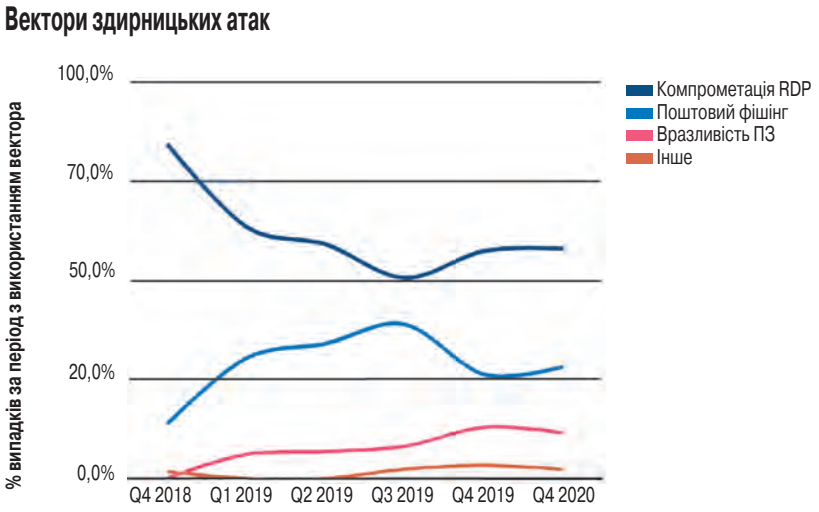

Рис. 1. Найпоширеніші вектори проникнення здирницького ПЗ (за даними Coveware)

Прикметно, що компанія ***Trend Micro*** у травні відзначила тенденцію до поширення послуги Access-as-a-Service («Доступ як послуга»). Її суть в тому, що хакери здійснюють злам компанії, проводять розвідку і крадуть різну інформацію для доступу — у тому числі облікові дані RDP — яку потім продають. Ця послуга існувала і раніше, проте за останній рік кількість продавців зросла у багато разів.

Є й інші дані, які свідчать про те, що більшість заражень відбувається через стару добру електронну пошту. Про це, зокрема, свідчить інформація ***Statista*** за 2019 рік, згідно з якою 67% усіх атак здирників починались з фішингових листів. Компанія ***Group-IB***, що базується в Сингапурі, зі свого боку повідомила, що з 200 зафіксованих нею торік випадків здирництва у більшості з них для початкового проникнення використовувались фішингові листи (а також заражені веб-сайти, які скеровують користувачів на сторінки, що містять зловмисний код). Фішинг не потребує таких технічних навичок, які необхідні для встановлення віддаленого контролю, до того ж продаються готові фішингові пакети, за допомогою яких можна сконструювати сайт-приманку.

Полювання на велику здобич

На додачу фірми, що займаються кібербезпекою, відзначають, що останнім часом у здирництві з'явилося декілька нових трендів. Зокрема, ці злочинці взяли на озброєння деякі прийоми, що їх використовують групи, які стоять за стійкими кіберзагрозами типу APT, а також за їхнім прикладом взялися полювати на «великого звіра» (Big Game Hunting). Торік Group-IB фіксувала атаки через довірених партнерів і постачальників, що є характерним для APT-груп.

Іншим важливим трендом на ниві кіберздирництва є те, що злочинці почали не лише шифрувати дані на комп'ютерах жертв, але й красти ці дані і/або погрожувати їх оприлюдненням. Наприкінці минулого року саме це зробила група Maze. Загалом відомі випадки, коли здирники використовували спеціальні сайти — так звані зливні бачки – для ославлення своїх жертв, а тоді викладали там вкрадену інформацію, якщо ті не поспішали з викупом. Також здирники намагаються продати ці дані на чорному ринку.

Якщо у минулому щойно після зараження починалося шифрування, то зараз здирники можуть проводити в мережі чимало часу, вивчаючи обстановку. Проникнувши всередину, хакери здобувають права адміністратора і відповідні привілеї доступу, за допомогою яких вони можуть відключити антивірус і двофакторну автентифікацію, а також знищити або

зашифрувати резервну копію даних. Окрім того, хакери досліджують топологію мережі, щоб зрозуміти, яким чином компанія реагуватиме на атаку і як можна нейтралізувати цю реакцію. Надалі вони вичікують оптимальний момент і запускають виконуваний файл у найбільш цінній частині мережі. Часто це відбувається вночі або рано вранці, на вихідних чи у свята, або ж у якісь особливі періоди (наприклад, перед терміном подання податкової звітності).

Приміром, за даними ***Microsoft***, оприлюдненими у квітні, атаки здирників, що сталися того місяця, імовірно, почалися на кілька місяців раніше, і відтоді злочинці «вичікували слушний час, щоб монетизувати свої успіхи, запустивши здирницьке ПЗ в той момент, який принесе їм найбільшу фінансову вигоду».

У січні сайт ***Bleeping Computer*** повідомляв, що одна зі здирницьких організацій, Ryuk, почала використовувати функцію Wake-on-Lan, яка дозволяє спеціальною командою віддалено вивести комп'ютер з режиму сну. Цією можливістю послуговуються системні адміністратори для встановлення оновлень або проведення запланованих робіт, проте зловмисники навчилися використовувати її для збільшення обсягу атаки. Зламавши один комп'ютер, вони надалі розсилають команди пробудження іншим ПК і шифрують також їхній вміст. Як зазначає Coveware, якщо інфільтрація відбувається у неробочий час, коли більшість машин не працює, дана функція дозволяє значно збільшити кількість атакованих пристроїв.

Найпривабливішими цілями атак є ті організації, які найбільше постраждають від розкриття своїх даних, а саме юридичні, фінансові і медичні. З 1 січня по 30 червня 2020 року база ID Ransomware отримала 100 тис. повідомлень про атаки, з них у 11 642 випадків дані було поцуплено. Окрім власне переривання роботи організацій, викрадення даних спричиняє більш тривалі проблеми, пов'язані з виплатою штрафів (у Європі відповідно до стандарту захисту персональних даних GDPR, подібне законодавство потроху з'являється і в інших частинах світу), репутаційними втратами, судовими позовами, витоком інтелектуальної власності або іншої інформації, яка надає фірмі конкурентну перевагу.

Медичні заклади і раніше були під ударом, проте у нинішньому році здирники отримали ласий стимул у вигляді пандемії COVID-19. «СіБ» про це писав навесні («Коронавірус атакує комп'ютери», №2/2020). Відтоді ситуація не поліпшилась, надалі під ударом залишаються лікувальні установи і дослідницькі центри. Наприклад, у вересні Ryuk атакував медичну мережу Universal Health Services, яка працює в США, Пуерто-Ріко та Великобританії, заблокувавши комп'ютерні мережі у низці американських лікарень. За повідомленням видання ***Wired***, в результаті частину пацієнтів мусили перевести до інших закладів, а документообіг повернувся до паперової форми. У листопаді — після чергової низки атак на лікарні — губернатор штату Вермонт покликав на допомогу підрозділ кіберзахисту Національної гвардії США.

Страхова заплатить

Суми викупів теж безперервно зростають. Згідно з даними Emsisoft, торік сплатили викуп 33% жертв, а сума того викупу в середньому складала $84 тис. (***Group-IB*** повідомляла, що найбільш жадібні вимагали $800 тис.). При цьому ***Coveware*** за підсумками першого кварталу повідомила, що середня сума викупу збільшилась до $111,6 тис. — на третину порівняно з останнім кварталом 2019-го.

Між тим американська незалежна агенція ***ProPublica***, яка займається розслідуваннями зловживання владою, повідомляє, що в США зростання індустрії кіберстрахування дещо парадоксальним чином спонукає клієнтів платити здирникам, навіть якщо можливе відновлення з бекапу. Для страхувальників це вигідно, оскільки зменшує витрати на відшкодування, адже їм не потрібно компенсувати втрачені прибутки, платню консультантам, що займаються відновленням даних тощо. А також, винагороджуючи злочинців, вони стимулюють нові атаки, в результаті налякані компанії і державні установи купують ще більше страхових полісів.

Наприклад, влітку минулого року внаслідок кібератаки було заблоковано комп'ютери мерії міста Лейк-Сіті, що у штаті Флорида. Мер і міська рада одноголосно вирішили звернутися до страхової компанії Beazley, щоб та покрила виставлений здирниками рахунок у 42 біткойни (на той час це дорівнювало $460 тис.), тоді як місто повинне було сплатити лише $10 тис. Шестизначна сума потрапила до заголовків новин. При цьому IT-персонал намагався відновити файли з резервного архіву, проте, за рекомендацією страхувальника, рада постановила заплатити, позаяк збитки від простою перевищили б $1 млн, а також тому, що прагнула якнайшвидше повернутись до нормальної роботи.

Понад те, ProPolitica стверджує (з посиланням на ФБР), що здирники стали зумисне обирати саме ті компанії, які мають поліс. Після того, як одна з фірм-страхувальників розмістила на своєму веб-сайті імена клієнтів, три з них були атаковані здирниками. Навіть якщо злочинці не знають, застраховані їхні жертви чи ні, численні випадки капітуляцій розпалюють їхню жадобу, що виливається у чимраз більші суми викупу.

Щоправда, здаються теж далеко не всі. Наприклад, у 2019 році місто Атланта, яке мало страховку, відмовилось сплатити здирникам $51 тис. і витратило $8,5 млн на відновлення даних. Минулого ж року американська Конференція мерів ухвалила не платити взагалі нікому. Також страховий поліс не завжди покриває збитки, а якщо й покриває, то отримати компенсацію теж не завжди можливо. У 2018 році виробник продуктів харчування Mondelez International і фармацевтична компанія Merck подавали до суду на страхувальників, які відмовились покривати їхні збитки від атаки NotPetya. Відповідачі заявили, що страховка не поширюється на «ворожі» або «військові» дії, позаяк за атаками ймовірно стояло російське військове відомство.

Здирництво як сервіс

Як і в інших видах діяльності, у кіберздирництві прижилася модна модель SaaS. Гравці, які виступають постачальниками послуг Ransomware-as-a-Service (RaaS), розробляють ПЗ і продають його окремим хакерам або групам, які займаються власне здирництвом. Продаж і просування цього ПЗ відбувається у «темній мережі» (Dark Web) з використанням тих самих маркетингових прийомів, що і у законному бізнесі: існують знижки, пакетні пропозиції, різні рівні підписки, відгуки користувачів і т. ін. У найпростішому випадку користувач отримує код, ключ дешифрування та інструкції з використання. Більш «просунуті» послуги включають цілодобову підтримку, відстеження статусу заражень і платежів тощо.

Як виглядає схема RaaS, можна побачити на **рис. 2**. Розробник створює код шифрувальника і надає його партнерові (здирнику). Той розміщує код на веб-сайті, визначає потрібний вектор зараження і надсилає посилання потенційній жертві. Після того, як та переходить за лінком і зловмисний код шифрує файли на її комп'ютері, жертва отримує повідомлення про суму викупу і інструкції про те, як його сплатити. Відмивач грошей пропускає платіж через серію транзакцій, метою яких є приховати особи як самого здирника, так і розробника. На останньому етапі здирник надсилає жертві ключ для розшифрування (хоча це трапляється не завжди).

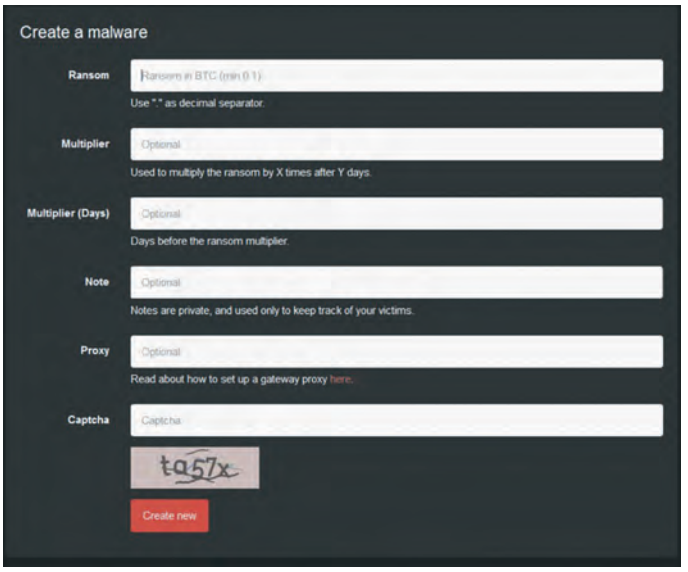

Рис. 3. Налаштування послуги RaaS: можна вказати суму викупу, кількість днів, які даються жертві, і множник, на який буде збільшено викуп, коли цей термін спливе (скріншот з сайту Zvelo)

Як і загалом у SaaS, перевагою моделі є простота користування: потрібно лише зареєструватися і обрати пакет залежно від потреб і ціни (**рис. 3**). Головне ж те, що здирником може стати не лише той, хто пише код, а взагалі будь-хто. У той же час для розробників зменшується ризик, оскільки самі вони здирництвом можуть не займатися.

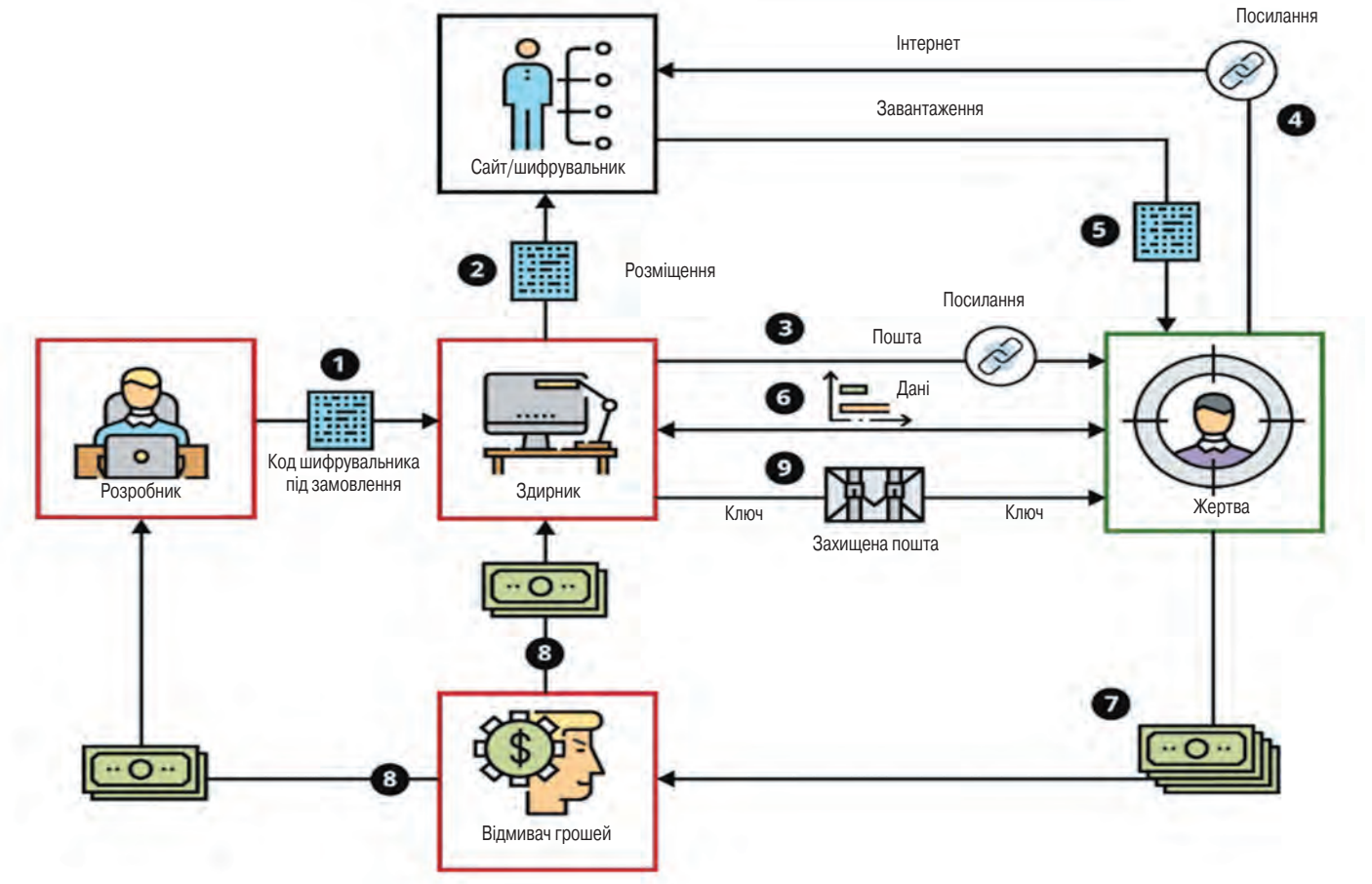

Рис. 2. Схема взаємовідносин за моделлю RaaS (джерело: Інститут Карнегі-Меллон)

За оцінками компанії ***Zvelo***, яка займається кіберрозвідкою, вартість здирницького ПЗ варіюється від $40 до кількох тисяч доларів (за даними іншої компанії, ***Vade Secure***, середній пакет RaaS коштує приблизно $50), проте навіть за максимальної ціни це невеликі гроші, якщо зловмисники бачать можливість трусонути грошовиту компанію.

Деякі постачальники RaaS продають свої продукти за фіксовану ціну або за абонентну плату. Інший поширений варіант передбачає розподіл прибутків (наприклад, здирник отримує 70%, а решту — постачальник, або й навпаки). Хоча рівень успішного здирництва оцінюється як досить низький, зазначає Zvelo, модель розподілу прибутків дозволяє RaaS-постачальникам заробляти більше, проте нерегулярно, але оскільки така схема популярна, можна зробити висновок, що для них бізнес досить вигідний.

Найвідомішою групою, яка надає послуги RaaS (на даний момент, бо гравці постійно змінюються), вважається Sodinokibi. Вона сама здійснює здирницькі атаки, спеціалізуючись на компаніях-аутсорсерах, і продає код колегам-здирникам, зокрема серед її клієнтів є інша відома група Maze, що також атакує аутсорсерів. Дослідники припускають, що Sodinokibi є спадкоємцем групи GandGrab, яка торік хвалилася сумарною здобиччю у $2 млрд і мала 392 замовників.

Дати одкоша здирникам

Для захисту від програм-шифрувальників існує декілька стратегій. Перша полягає власне в тому, щоб не допустити зловмисний код до комп'ютера, це завдання лягає на плечі антивірусів, які мають вбудовані функції захисту від здирництва. Зокрема, сайт ***Techradar.com*** виділяє пакет ***Bitdefender*** Antivirus Plus 2020, який має багаторівневий захист від зловмисних програм і визначає загрози за допомогою евристичного аналізу, хоча й споживає більше ресурсів порівняно з подібними програмами і може конфліктувати з іншим встановленим «софтом». На друге й третє місце дослідники поставили відповідно антивіруси ***AVG*** і ***Avast***.

Захист від здирників підтримують і рішення корпоративного класу, розраховані на протистояння складним атакам. Наприклад, у ***Palo Alto*** це модуль Anti-Ransomware Protection, який входить до складу системи Cortex XDR і викриває здирників на основі поведінкового аналізу. У ***Check Point*** технологія Anti-Ransomware реалізована в пісочниці SandBlast (також є окреме рішення для кінцевих пристроїв ZoneAlarm Anti-Ransomware).

У Bitdefender є дещо екзотичний спеціалізований інструмент Anti-Ransomware, який здійснює «вакцинацію» ПК проти поширених видів шифрувальників. Принцип його дії будується на тому, що більшість шифрувальників оминають комп'ютери, на які вже проникли їхні «колеги»; адже який сенс шифрувати інформацію двічі, якщо її потім не можна буде відновити. Відповідно програма Bitdefender встановлює в системі виконувані файли, які імітують зразки зловмисного ПЗ. Втім, такий «імунітет» безсилий проти тих

програм, які не підтримуються захисником, і тому «вакцина» не замінює повноцінного антивірусу.

«Другий ешелон» оборони становлять рішення, які намагаються не пустити шифрувальника до окремих папок, де зберігаються найцінніші файли. Наприклад, ***Trend Micro*** RansomBuster забороняє будь-яким неавторизованим програмам змінювати файли: тобто, наприклад, з документами можна працювати лише у Microsoft Word. Виявивши хоча б натяк на шифрування, RansomBuster робить резервну копію файлу. Якщо ж спроби повторюються, програма перериває роботу шифрувальника, сповіщає користувача і відновлює файли з архіву. ***Panda*** Dome Security забороняє стороннім програмам навіть читати файли.

Остання, так би мовити, лінія барикад, — це відновлення зашифрованих даних з резервних копій. Є програми, які створені спеціально для цього — наприклад, ***Acronis*** Ransomware Protection відновлює інформацію з локального сховища або з онлайн-бекапу. Цікавий підхід запропонувала компанія ***NewShield*** у своєму рішенні DataSentinel, яке віртуалізує файлову систему, так що будь-які зміни не є постійними. Завдяки цьому шифрування можна просто відмінити. Постійні зміни вносяться раз на добу — таким чином, користувач може втратити щонайбільше один день роботи. При цьому впродовж вихідних постійні зміни повинні підтверджуватися користувачем, оскільки здирники полюбляють робити свою чорну справу у п'ятницю ввечері. Самого шифрувальника можна знищити, відкотивши Windows до попереднього дня.

Втім, технічні винаходи не дають стовідсоткової гарантії захисту, бо зловмисне ПЗ теж розвивається. Загалом фахівці радять вживати профілактичні заходи і зменшувати саму ймовірність зараження. Використовувати VPN для доступу через RDP, створювати складні паролі для рахунків, що використовуються для такого доступу, і регулярно їх змінювати, обмежувати перелік IP-адрес, які можна використовувати для RDP-підключень. Також варто зберігати резервні копії даних десь на окремому пристрої (не кажучи про те, щоб узагалі робити ті копії). Решта рекомендацій загальні для кіберзахисту в цілому: потрібно постійно відстежувати ознаки хакерських атак і компрометації, щоб вчасно їх виявляти і знешкоджувати, а також навчати персонал розпізнавати ознаки фішингу. Щоб не потрапити на гачок.

Василь ТКАЧЕНКО, **Мережі та Бізнес**