COVID-19: КЛЮЧОВІ КІБЕРБЕЗПЕКОВІ ТРЕНДИ

Д. В. Дубов, д. політ. н., с. н. с.,
завідувач відділу інформаційної безпеки та кібербезпеки
центру безпекових досліджень Національного інституту стратегічних досліджень

Висновки

1. Експерти виділяють 4 ключові кібербезпекові тренди (які можуть призвести до зростання кіберзагроз) на фоні розгортання пандемії COVID-19: збільшення кількості людей, які працюють віддалено (використовуючи ІТ, але не маючи належних знань та досвіду); збільшення електронних платежів (що збільшує увагу шахраїв); збільшення кількості випадків фішингових атак; потенційна можливість для інформаційних та кібератак з метою дестабілізації ситуації.
2. Ознаки системного деструктивного кібервпливу відсутні (водночас є ознаки дезінформаційного впливу). Занепокоєння, що під час пандемії можуть розпочатись масштабні кібератаки, наразі не справдились. Поодинокі випадки (США, Чехія, Індія, Монголія) не спростовують цей висновок.
3. Очікувано зросла фішингова діяльність хакерських угрупувань. Водночас найбільш небезпечні групи (які є операторами вірусів-вимагачів) намагаються дистанціюватись від такої діяльності на даному етапі (вочевидь, не бажаючи привертати надмірну увагу правоохоронних органів та спецслужб).
4. Найбільшу потенційну небезпеку може становити стрімке збільшення кількості працівників, які працюють віддалено і використовують для цього ІТ – часто такі люди не мають відповідних навичок, а стан кібербезпеки домашніх пристроїв не надто високий. Це веде до потенційного зростання кількості кіберінцидентів (в т.ч. актів кібершпигунства та компрометації інформації).
5. Потенційне зростання інцидентів з електронними платіжними системами наразі не підтверджується доступною статистикою. Водночас слід враховувати а) високий латентний рівень таких злочинів та б) загальну складну безпекову ситуацію.
6. Держави дедалі жорсткіше протидіють поширенню короновірусу, вдаючись при цьому і до порушення традиційного балансу прав і свобод громадян у цифровому просторі (фактично легалізуючи кіберстеження). Слід очікувати, що в

подальшому ця тенденція буде посилюватись і може сформувати «нову норму» в даному питанні.

7. Спостерігається активізація дискусії щодо переліку реальних критичних секторів економіки (критичної інфраструктури), які мають бути першочергово захищені від кібератак. Якщо в попередні роки західні держави відносили до таких секторів енергетику, фінансову систему, оборонну промисловість, шкідливі підприємства та виборчі системи, то тепер до них додалась медична сфера. Важливе зміщення акцентів: від проблеми захисту персональних даних пацієнтів до захисту ключових функцій цієї сфери.

Рекомендації

1. *Національному координаційному центру кібербезпеки РНБО України (НКЦК)* рекомендувати Службі безпеки України, Державній службі спеціального зв'язку та захисту інформації України, Департаменту кіберполіції Національної поліції України, Національному банку України інформувати населення щодо можливих кіберзагроз при використанні цифрових пристроїв при віддаленій роботі та небезпеки фішингових атак.

2. *НКЦК* (з урахуванням реальної епідеміологічної ситуації) ініціювати підготовку рекомендацій щодо посилення кіберзахисту об'єктів медичної сфери.

3. *Міністерству цифрової трансформації України* опрацювати можливість проведення додаткових роз'яснювальних заходів з питань кіберграмотності (кібергігієни) та особистої кібербезпеки для громадян вікових груп 45+, які внаслідок вжиття карантинних заходів можуть перейти на віддалений режим роботи з використанням цифрових засобів. Також інформувати всі вікові категорії про базові правила безпеки використання електронних засобів розрахунків в мережі Інтернет.

Пандемія COVID-19 серед іншого загострила питання кібербезпеки, адже кризові ситуації традиційно викликають активізацію різноманітних хакерських угрупувань. Основні фактори, що потенційно сприяють підвищенню деструктивної (протизаконної) кіберактивності:

практика введення режиму карантину в більшості держав веде до стимулювання роботодавців змінювати характер виробничих відносин з робітниками на умовах дистанційної роботи. В більшості випадків такі взаємодії відбуваються за допомогою мережі Інтернет. Відтак кількість потенційно уразливих з'єднань, які можуть призвести до компрометації інформації або самої організації, або її працівників – збільшується;

обмеження на пересування, максимальне обмеження готівкових розрахунків, а також збільшення часу, який громадяни проводять вдома, призводить не тільки до зростання часу користування мережею Інтернет загалом, але й до інтенсифікації електронних платежів зокрема. Це викликає посилену увагу кіберзловмисників до шахрайської діяльності;

кризи та паніка завжди використовувались хакерами у їх діяльності. У такі періоди традиційно зростає кількість фішингових атак – збільшення фальшивих листів (із malware-вкладеннями) та фальшивих сайтів (для збору персональної та банківської інформації громадян);

додаткове посилення паніки може бути однією з цілей операцій впливу з боку

інших держав, які можуть бажати використати ситуацію у власних інтересах (про це зокрема попереджають спеціальні органи Нової Зеландії, а заяви США та ЄС кажуть про зафіксовану дезінформаційну кампанію щодо коронавірусу).

На даний момент ворожа кіберактивність, яка може бути класифікована як така, що здійснюється іншими державами, повною мірою не підтверджується, хоча занепокоєння мають певну фактичну основу.

США. 16 березня 2020 року Міністерство охорони здоров'я та соціальних служб США (*Department of Health and Human Services*) заявило, що помітило підозрілу активність щодо своїх ІТ-систем. Активність не була спробою зламу, а швидше формою *DDoS*-атаки. Водночас у своїх перших реакціях представники Адміністрації Д.Трампа назвали це «частиною намірів іноземної структури посіяти паніку серед громадян США». Висловлювалось і припущення, що ці атаки є відповіддю Ірану на вбивство К.Сулеймані в ніч з 2 на 3 січня 2020 р. Однак кіберексперти (які досліджували ці атаки більш докладно) вказали на те, що вони мало відрізнялись від аналогічних спроб, які відбуваються майже щодня. За іншими даними атаки на сайти системи охорони здоров'я США тривають – керівник Інформаційного офісу Північної Дакоти Ш.Рілей заявив, що атаки тривають і що мета таких атак – сіяти паніку.

Індія. Експерти відмічають активізацію пакистанського угрупування APT-36 (традиційно ціллю їх атак є уряд Індії), яке розпочало поширення проти індійських агенцій кібершпигунського програмного забезпечення «Crimson RAT» - під виглядом листа індійського уряду про начебто оновлені дані щодо коронавірусу.

Монголія. Ізраїльська компанія Check Point зафіксувала спробу хакерів (яких можливо підтримує неназвана держава) отримати доступ до урядових мереж Монголії, використовуючи для цього начебто новини про коронавірус.

Чехія. В ніч з 12 на 13 березня внаслідок кібератаки шпиталь Університету Брно (*Brno University Hospital*) був вимушений відключити свої системи, припинити операції та перевести пацієнтів у інші лікарні. Варто підкреслити, що ця клініка – найбільший медичний центр Чехії чия тестова лабораторія займалась питанням COVID-19.

Часткове підтвердилися занепокоєння щодо **зростання кількості фішингових атак** та підробних сайтів. Протягом першої декади березня 2020 року з'явилось принаймні декілька підробних сайтів Всесвітньої організації охорони здоров'я (*World Health Organization*) та Центру з контролю та профілактики захворювань США (*Center for Disease Control and Prevention*), однак точно встановити, хто за ними стоїть, виявилось неможливо. Також за даними експертів з кібербезпеки китайські та східноєвропейські хакерські групи вже долучились до фішингової діяльності: надсилаються електронні листи, в яких начебто є оновлена інформація про коронавірус, створюються заражені вірусами інтерактивні карти поширення COVID-19. Вся ця інформація спрямовується співробітникам державних структур та приватних компаній. Експерти компанії *Cynet* на прикладі Італії (яка найбільш постраждала від дії вірусу) показують різке збільшення фішингових атак саме на фоні епідемії (майже у 2,5 разів вище ніж середнє місячне значення).

З іншого боку оператори деяких відомих (наприклад *DoppelPaymer* чи *Maze*) здирницьких вірусів (*ransomware*) заявили, що на період протидії COVID-19 припиняють будь-які атаки проти медичних закладів або тих структур, які намагаються зупинити пандемію. Оператор *DoppelPaymer* відмітив, що якщо в результаті їх діяльності випадково постраждає такий об'єкт, то вони готові надати

їм дешифратор даних безкоштовно. З іншого боку така ініціатива не є загальною – наприклад оператор вірусу *Ryuk* (який нещодавно ефективно атакував ІТ-системи американських міст Новий Орлеан та Дюркхем) таких заяв не робив (цей вірус пов'язують з російськими хакерами). Експерти з кібербезпеки підкреслюють, що такі ініціативи – не альтруїзм хакерів, а стратегія самозбереження, адже реакція правоохоронних органів на такі атаки за поточних обставин може істотно виходити за межі традиційного пошуку зловмисників, а дії хакерів можуть бути класифіковані за тяжчими статтями ніж зазвичай. Так, Офіс Генерального прокурора США вже заявив, що органи юстиції США мають уважніше слідкувати за шахраями в кіберпросторі та переслідувати тих з них, хто намагається отримати зиск від пандемії. Американські сенатори пропонують тих осіб, які спробують атакувати об'єкти системи охорони здоров'я, притягати до відповідальності як терористів.

Відбувається стрімке зростання кількості осіб, що починають вперше працювати віддалено і не зажди знають як це робити – представники компанії *Cisco* кажуть про 10-разове зростання кількості звернень щодо допомоги у налаштуванні таких робочих місць. Все це створює нові ризики безпеці. Крім того, деякі організації використовують тимчасові послаблення режимів доступу до інформації, надаючи його працівникам у віддаленому форматі. При цьому такі працівники часто використовують значно менш захищене телекомунікаційне середовище ніж на своєму робочому місці. Все це збільшує ризики витоків конфіденційної інформації. Ізраїльські фахівці також підкреслюють, що джерелом атаки на домашні системи працівників можуть стати сервіси відеоуроків, якими можуть користуватись їх діти, що також перебувають в умовах карантину (такі сервіси традиційно значно менше захищені ніж інші). **Наразі відсутні достовірні дані про збільшення випадків фактичних інтернет-шахрайств,** пов'язаних із пандемією, однак дедалі більша кількість експертів надає рекомендації громадянам та роботодавцям щодо вжиття завчасних заходів для мінімізації потенційних негативних наслідків. Це, зокрема:

забезпечення належного рівня цифрової гігієни користувачів та поліпшення їх цифрових навичок;

використання VPN (особливо у публічних місцях);

мінімізація використання відкритих (публічних) WiFi;

поліпшення ступеню захисту паролів;

підвищена увага до будь-яких незнайомих листів або таких, що містять «емоційні» заголовки із посиланнями;

використання лише офіційної інформації та даних;

негайне повідомлення роботодавця у випадку якщо було втрачено/викрадено персональний мобільний пристрій з якого працівник міг мати доступ до робочих матеріалів;

завчасне встановлення регламенту віддаленого доступу працівників до їх робочих місць;

постійний контакт між роботодавцями та працівниками щодо кіберінцидентів.

Пандемія COVID-19 загострила ще декілька питань, які можуть мати довгостроковий вимір.

По-перше, кіберспостереження та права людини. Уряди шукають можливості збільшення точності відслідковування як вже заражених людей, так і

тих, з ким вони мали контакти. В тому числі – з використанням сучасних технологій. Однак найбільші можливості для такого виявлення можуть входити в конфлікт із правами людини. Наприклад, МОЗ Ізраїлю використало кіберрозвідувальні можливості контррозвідки «Шін Бет» для відслідковування носіїв та потенційних носіїв вірусу. Це викликало протести активістів, які виступають проти порушення громадянських прав в межах боротьби з коронавірусом. Водночас влада КНР отримала додаткові репутаційні переваги щодо створюваної нею системи всеохоплюючого контролю за життям громадян (включаючи такі її елементи як контрольований кіберпростір, розпізнавання облич, система «Соціальний кредит» тощо) – вони стали одним з інструментів спрощення процесів ідентифікації носіїв вірусу, а відтак і інструментом стримування пандемії. Все це актуалізує питання про межі втручання держави у життя громадян в умовах реальної загрози національній безпеці.

По-друге, система охорони здоров'я (включаючи елементи поставок в ній) набуває нового значення як критична інфраструктура. Хоча і раніше елементи системи охорони здоров'я відносили до критичної інфраструктури, однак зараз фокус такого віднесення зміщується: від розуміння критичності як місця циркуляції чутливих персональних даних пацієнтів до об'єктів, від яких залежить життя значних мас людей. При цьому рівень кіберзахисту таких об'єктів часто є незадовільним. Наприклад, ІТ-системи британської суспільної організації *National Health Service* (NHS), яка я важливою складовою британської системи охорони здоров'я, є уразливими для хакерських атак. Слід визнати, що за оцінками незалежних експертів ІТ української системи охорони здоров'я також не мають належного рівня захисту (водночас рівень залученості ІТ-систем до критичних процесів в українських реаліях менша ніж у розвинених країнах).