РЕЗОЛЮЦІЯ
Позачергового з'їзду нотаріусів України від 22-23 квітня 2016 року з приводу низки сторонніх втручань до ДРРП шляхом використання логіну, пароля, ключа ЕЦП нотаріуса та заходи протидії кіберзлочинам у сфері державної реєстрації прав

Впродовж тривалого часу (розпочинаючи *з квітня 2015 р.* - травень 2016 р.) спостерігаються випадки стороннього втручання до Державного Реєстру речових прав (надалі - *ДРРП*) шляхом використання логіну, пароля, ключа ЕЦП нотаріуса. В результаті здійснюються неправомірні реєстраційні дії, пов'язані із *припинення обтяжень, арештів та іпотек, а також подальшої незаконної перереєстрації права власності*.

За наявною, хоча і неповною інформацією, внаслідок цього проведено біля 300 сторонніх втручань, внаслідок чого вже постраждало більше 20 (двадцяти) нотаріусів, в т.ч.:

- Київ та Київська область – 6,
- Рівненська область – 5,
- Харків – 3,
- Дніпропетровська область – 2,
- Запорізька область, Житомир, Чернігів, м. Каховка Херсонської області, м. Суми тощо – по 1^{му} нотаріусу.

Реально таких випадків значно більше, оскільки між сторонніми втручаннями до ДРРП і виявленням такого факту проходить досить тривалий час (іноді – декілька місяців), а перші інциденти, пов'язані із використанням комп'ютерів нотаріусів для проведення незаконних реєстраційних дій в ДРРП датовані листопадом-груднем 2014 р.

Серед найбільших резонансних «хакерських атак» на ДРРП - припинення обтяження, зареєстрованого в інтересах іпотекодержателя ПАТ «Укргазбанк», та подальша протиправна перереєстрація права власності з ТДВ «ЖЛ» на ЗАТ «Житомирські ласощі», вчинені в лютому-березні 2016 р.

В першому випадку кримінальне провадження порушено ГУ контррозвідки СБУ, посадовим особам «Укргазбанку» пред'явлено підозру про вчинення злочину, котрі в свою чергу «вектор звинувачення» активно перекладають на нотаріуса, під логіном, паролем, ЕЦП якого здійснювалося припинення обтяжень.

Щодо другого випадку, то нотаріус Дніпропетровського МНО Прокоф'єва О.Ю., від імені якої начебто вчинялися реєстраційній дії, тричі безрезультатно подавала до правоохоронних органів заяву щодо несанкціонованого втручання. Проте попри очевидні факти і докази, кримінальне провадження порушено було_тільки 21.04.2016 р. лише після відповідної ухвали суду, котра зобов'язала правоохоронні органи вчинити передбачену КПК України процесуальну дію.

У вкрай складній ситуації перебувають ті українські нотаріуси, котрі попри процесуальну казуїстику та добре відомий «суб'єктивний фактор» правоохоронної системи таки домоглися відкриття кримінального провадження за фактами злочинного використання їх особистого логіну, пароля, ключа ЕЦП тощо.

Так, за заявою приватного нотаріуса Житомирського МНО Стражник Т.О. постановою слідчого 24.10.2015 р. було відкрито кримінальне провадження, а нотаріуса – визнано потерпілим. Проте всупереч фактам, логіці і здоровому глузду, Вищий спеціалізований адміністративний суд в своїй ухвалі *(№ К/800/1830/16 від 31.03.2016 р.)* дійшов висновку, що наявність кримінального провадження за заявою нотаріуса і його статус як потерпілого не можуть бути підставою для відмови у задоволенні позовних вимог про визнання дій нотаріуса протиправними.

Натомість, нотаріусу Стражник Т.О. доводиться самотужки відстоювати свою невинуватість і правоту в судових органах, будучи відповідачем у 4 (чотирьох) судових провадженнях одночасно. При цьому вартість одних лише судових зборів в одному провадженні сягає 42 (сорока двох) тисяч грн.

Безпосередньо проведення незаконних реєстраційних дій відбувається зазвичай у період низької активності нотаріуса-державного реєстратора (*відпустка, курси підвищення кваліфікації,*

вечірній чи нічний час, свята або вихідні тощо). Так, здійснення перереєстрації 10 (десяти) об'єктів нерухомого майна від імені ПН Дніпропетровського МНО Прокоф'євої О.Ю здійснювалося 25.02.2015 р. в дуже короткий проміжок часу – менше 1 (однієї) години: із 20^{47} до 21^{45}.

Після чого, по виведеним із заборони/арешту/іпотеки об'єктам в іншому регіоні України іншим нотаріусом вчиняються нотаріальні та/або реєстраційні дії щодо зміни права власності.

Технологічно кібератака на комп'ютер нотаріуса відбувається непомітно у декілька етапів, а використання у такий спосіб викраденого ЕЦП/ключа доступу до відповідного реєстру жодним чином не пов'язані ні місцем, ні часом. Схема атаки та аналітична довідка з цього питання, підготовлена фахівцями ТОВ «Лабораторія комп'ютерної криміналістики» (надалі - *CyberLab),* (*додаток 1)*.

Так, у наданому *CyberLab* висновку зазначається про встановлення на обрані для хакерської атаки комп'ютери шкідливого програмного забезпечення LiteManager, основними функціями якого є віддалене управління комп'ютером, викрадення даних облікових записів користувачів, передача файлів на сервер в мережі інтернет. Ймовірно, що зараження відбувалося шляхом відкриття файлу, котрий містив у собі шкідливий код, що надходив на досліджуваний комп'ютер нотаріуса в якості вкладеного файла у повідомленні електронної пошти. Також спеціалістами CyberLab було встановлено, що з пошти "хакера" зазвичай направлялося декілька листів від імені Міністерства юстиції України з використанням домену. Зважаючи на частотність розсилок, кількість адресатів та конверсію (коефіцієнт зараження), експерти вважають, що на даний час постійно зараженими є орієнтовно 1000 (одна тисяча) комп'ютерів нотаріусів, державних виконавців та інших уповноважених на здійснення реєстраційних дій осіб, котрі в будь-який момент можуть бути обрані в якості чергової «жертви», від імені та з використанням ідентифікатора доступу до ДРРП якої буде здійснено чергова низка протиправних реєстраційних дій.

При цьому фахівці CyberLab не виключають, що кібератака може вестися безпосередньо на сервері. Проте технічно дослідити це припущення не мають можливості через брак достатнього рівня співпраці та взаємодії із персоналом Державного підприємства «Національні інформаційні системи» (надалі – *ДП «НаІС*»), що є технічним адміністратором ДРРП.

Проте, попри швидкість проведення протиправного несанкціонованого втручання до ДРРП, технологічна підготовка кібератаки може тривати значний період часу. А сам нотаріус, від імені якого комп'ютерні злочинці здійснили протиправні реєстраційні дії, може і не здогадуватися про наявний факт використання третіми особами його ідентифікатора для роботи із ДРРП (ключа, пароля, ЕЦП тощо). Зокрема, ПН Житомирського МНО Стражник Т.О. лише 21.10.2015 р. і тільки після надходження до Мін'юсту України скарги з приводу нібито вчинених нею реєстраційних дій із припинення обтяжень, арештів та іпотек дізналася про факт незаконного доступу до ДРРП. А саме-про 50 (п'ятдесят) випадків несанкціонованих, протиправних реєстраційних дій, що здійснювалися від її імені та під її логіном, паролем та ключем ЕЦП невстановленими досі правоохоронними органами зловмисниками в період з 22.09.2015 р. по 18.10.2015 р. Наразі задокументовано 7 (сім) тривалих у часі випадків несанкціонованого втручання, під час яких знімалися іпотеки/заборони/обтяження по різній кількості об'єктів нерухомості (*від 2 до 17 за одне втручання*) з різноманітною географією: м. Миколаїв, Харків, Одеса, Київ, Слов'янськ тощо. Аналогічна ситуація трапилася і в м. Каховці Херсонської області, де факт несанкціонованого доступу мав місце 12 квітня 2016 р., а виявлено несанкціоновані реєстраційні дії рівно за місяць – 12 травня 2016 р.

Наразі невідомо, хто саме і коли стане наступною жертвою комп'ютерних зловмисників, оскільки одні із останніх задокументованих втручань у ДРРП шляхом використання логіна, пароля та ключа ЕЦП нотаріуса мали місце в Чернігові, Каховці Херсонської області та в Сумах впродовж квітня-травня 2016 р., коли вже працював оновлений реєстр UB.

30.03.2016 р. Громадською організацією «Асоціація нотаріусів м. Харкова та Харківської області» направлено ґрунтовні «*Пропозиції щодо вирішення проблем несанкціонованого доступу до Єдиних та державних реєстрів*» Міністрові юстиції України. Суть проблематики потребує ґрунтовного дослідження з залученням широкого кола фахівців (*експертів у галузі кіберзахисту, розробників програмного забезпечення ДРРП, науковців, нотаріусів, слідчих, суддів, представників ЗМІ* тощо). На цей час правоохоронні органи зосередились переважно або

й виключно на питанні так званого «людського фактору» і, відповідно, апріорі «винного» нотаріуса, чий ідентифікатор доступу до ДРРП зловмисники використали.

Але факти уперта річ, бо більш ніж за 15 попередніх років роботи з Єдиними та Державними реєстрами не було зафіксовано жодного випадку вчинення від імені нотаріуса реєстраційної дії, авторство якої не визнавалось би ним самим. Тому акцентування уваги саме на «людському факторі» та нечистоплотності (непорядності) нотаріуса - це хибний шлях і втрата дорогоцінного часу.

Насправді нотаріуси України були, є і залишатимуться сумлінними користувачами Єдиних та Державних реєстрів, з року в рік напрацьовуючи довіру до себе як до професіоналів з чистими руками й світлими помислами шляхом вчинення реєстраційних дій від імені Держави Україна.

Сама ж ситуація із не розслідуваними і тому безкарними сторонніми втручаннями щодо реєстраційних дій в ДРРП від імені нотаріусів створює реальну загрозу існуванню як інституту нотаріату та виконавчих проваджень, так і національній безпеці України в цілому.

Зважаючи на ознаки системності втручань до електронних реєстрів нерухомого майна, не контрольованість їх масштабів (ні кількісно, ні географічно), правову незахищеність нотаріусів - державних реєстраторів, потужний суспільний резонанс даної проблематики, а також її спотворене висвітлення у ЗМІ, що завдає непоправної шкоди репутації кожного нотаріуса, нотаріальна спільнота України в особі Позачергового з'їзду нотаріусів, що проходив у м. Києві 22-23 квітня 2016 р., вважає за необхідне:

1. Звернутися до Міністерства юстиції України, котре *забезпечує формування та реалізацію державної політики у сфері державної реєстрації прав, створення і функціонування ДРРП та є його держателем* (ст. 7 ЗУ «Про ДРРП») з питань:

- розробки комплексу заходів задля підвищення ступенів захисту інформації, яка міститься в Єдиних та Державних реєстрах МЮУ, правового захисту нотаріусів, які постраждали від несанкціонованого втручання у їхню роботу з боку третіх осіб;

- модернізації Програмного забезпечення ДРП шляхом «прив'язки» /закріплення/ АРМ/UB до конкретного ПК конкретного нотаріуса з метою унеможливлення здійснення несанкціонованих реєстраційних дій третіми особами під ЕЦП нотаріуса за допомогою т.зв. «віддаленого доступу», поставивши задля цього відповідне завдання ДП «НаІС» як технічному адміністратору ДРРП (п. 7 ч. 1 ст. 2 ЗУ «Про ДРРП»);

- забезпечення співпраці ДП «НаІС» як технічного адміністратора ДРРП із провідними фахівцями в галузі боротьби із кіберзлочинністю (в т.ч., але не тільки – експертами CyberLab);

- організації та проведення «круглих столів» (із залученням до участі в них *експертів у галузі кіберзахисту, розробників програмного забезпечення ДРРП, науковців, нотаріусів, слідчих, суддів, представників ЗМІ тощо)* та інших форм взаємодії й співпраці із правоохоронними органами (Генеральна прокуратура, МВС, СБУ тощо), відповідними комітетами Верховної Ради України, Вищою радою юстиції з метою переведення проблематики питання несанкціонованого доступу з позиції виключно «суб'єктивного фактору» в площину пошуків ефективних шляхів захисту й відновлення прав громадян та юридичних осіб, що постраждали внаслідок несанкціонованого доступу до ДРРП, на стадіях розслідування кримінальних справ відповідними слідчими підрозділами та їх судового розгляду;

- направлення відповідних листів до правоохоронних органів (*Міністерства внутрішніх справ України, Генеральної прокуратури України, Служби Безпеки України* тощо) щодо необхідності оперативного та всебічного розслідування кримінальних справ, порушених за фактами несанкціонованого доступу до ДРРП, невідкладного вжиття заходів щодо відновлення порушених прав не лише осіб, які безпосередньо постраждали від несанкціонованого втручання, але й нотаріусів.

Йдеться, зокрема, як про невідкладне накладення арешту на майно, яке було предметом несанкціонованих дій, так і про необхідність проведення допитів не виключно нотаріусів, під чиїм ЕЦП/паролем здійснювався несанкціонований доступ, а й інших суб'єктів правовідносин, пов'язаних із нерухомим майном, котре внаслідок кібератаки на ДРРП було незаконно виведено з-під обтяження, а саме:

- заявника, в інтересах якого здійснювалися протиправні реєстраційні дії,
- його ж та/або власника майна, котрий одразу ж після несанкціонованих реєстраційних дій здійснював відчуження майна, обтяженого забороною, арештом чи іпотекою,
- набувача, на ім'я якого здійснювалася протиправна реєстрація права власності (наприклад, ЗАТ «Житомирські ласощі»),
- нотаріуса, який безпосередньо за злочинним припиненням обтяжень посвідчував відповідний правочин щодо вказаного майна на ім'я третіх осіб тощо.
- звернення до Вищої ради юстиції, а також до Колегії з адміністративних справ Верховного суду з проханням щодо неупередженого та об'єктивного розгляду справ за позовами до нотаріусів як державних реєстраторів шляхом доведення інформації про численні факти несанкціонованого втручання до ДРРП з боку невстановлених досі зловмисників, а також рекомендації щодо зупинення провадження з адміністративних справ до закінчення кримінального провадження щодо пов'язаних з ними кримінальних справ, за яким нотаріус визнаний потерпілим.

2. Президенту та Раді НПУ створити постійно діючий робочий орган НПУ - комісію з питань кібербезпеки, забезпечивши відповідне фінансування даного напрямку і оперативне напрацювання відповідних рекомендації і технічних рішень задля гарантування інформаційної безпеки нотаріусів-державних реєстраторів.

3. Від імені НПУ надати рекомендації організаційно-технічного характеру державним та приватним нотаріусам у сфері безпеки використання ДРРП, як-то:
- невідкладна заміна персональної ідентифікації доступу до ДРРП (ЕЦП, паролі тощо);
- наявність окремого ПК для роботи виключно із ДРРП, іншими Єдиними та/або Державними реєстрами;
- систематичне формування відомості виконаних в ДРРП дій з обтяженнями (щоденно);
- здійснення доступу до інтернет-мережі (в т.ч. користання електроною поштою) із ПК, на яких не встановлені ДРРП та інші Єдині та/або Державні реєстри;
- при використанні WiFi обов'язково налаштовувати т.зв. «*гостьовий вхід*»;
- використання виключно ліцензійного програмного забезпечення, сучасних антивірусних програм, кріптографа, інших технічних напрацювань у сфері протидії кіберзлочинам (окремі програмні засоби захисту робочого місця нотаріуса-державного реєстратора) ;

4. Раді НПУ та відділенням НПУ в областях організувати та проводити системну роботу із центральними та місцевими ЗМІ (*телебачення, радіо, преса, інтернет-видання* тощо) щодо активної протидії численним спробам дискредитації та паплюження іміджу професії нотаріуса із використанням неперевіреної та/або недостовірної інформації в аспекті вчинення злочинів у сфері державної реєстрації прав (*умовна рубрика - «чорні нотаріуси»)* та формування позитивного іміджу нотаріуса – державного реєстратора

Додаток: 1. висновок ТОВ «Лабораторія комп'ютерної криміналістики» CyberLab від 22 квітня 2016 року вих. № 14 на 4 арк.