Шапочка С.В., Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України

ЩОДО ПРОТИДІЇ ДЕСТАБІЛІЗУЮЧІЙ ЗЛОЧИННІЙ ДІЯЛЬНОСТІ ТА КІБЕРШАХРАЙСТВУ В ІНФОРМАЦІЙНІЙ СФЕРІ

Нині, коли увага всього Світу прикута до Сходу нашої держави, велике напруження від очікування дотримання мінських угод не спадає - з метою дискредитації української сторони в очах міжнародного співтовариства на сайт Нацгвардії України було здійснено хакерську атаку, внаслідок якої на

ресурсі було розміщено інформацію про нібито атаку бійців Правого сектора в зоні АТО після оголошення режиму повного припинення вогню. А ЗМІ РФ відразу розтиражували цю фейкову новину, намагаючись довести її до широкого загалу та надати можливість на засіданні Радбезу ООН звинуватити Україну в порушенні домовленостей про припинення вогню.

Не обходять зазначені проблеми і державу-агресора. на офіційному сайті РФ для розміщення інформації про проведення торгів 17.02.2015 невідомі розмістили заявку про продаж Кремля. В якості причини термінового продажу в картці лота вказано нестачу коштів для допомоги "Новоросії". Стартова ціна на Кремль встановлена в розмірі 30 руб [1].

Разом із тим, кримінальні угруповання використовують електронні інформаційні технології для комунікації, шифруючи повідомлення (розповсюдження наркотичних засобів), координації своїх дій (організація теракту), полегшення вчинення інших злочинів, підвищуючи ефективність злочинної дестабілізуючої діяльності в інформаційній сфері.

Наприклад, 4 грудня минулого року співробітники СБ України викрили групу осіб, які готували диверсії і терористичні акти на важливих об'єктах інфраструктури [2]. За сприяння бойовиків ДНР, від яких було отримано вибухівку і зброю, злочинна група планувала з метою дестабілізації ситуації в Дніпропетровській області вчинити ряд терактів. Керівник злочинного угруповання, використовуючи соціальні мережі, згуртував злочинну групу з числа осіб, готових вчиняти диверсії, організовувати підпільну роботу.

Кіберзлочинність чинить дієвий вплив на інформаційну безпеку України.

Серед основних видів кіберзагроз для національної, в тому числі й інформаційної безпеки, можна виділити наступні: кібершахрайство, шкідливе програмне забезпечення, бот-мережі та DDoS-атаки, витік персональних даних (блокування інформації, виведення автоматизованих і/або інформаційних систем з ладу, кібершпіонаж, несанкціоноване переведення

грошових коштів тощо). Прикладом є виявлення дослідниками відділу Counter Threat Unit (CTU) компанії Dell нового типу вірусу, що отримав назву Skeleton Key, який обходить захист пароля при авторизації в Active Directory [3].

В кінці січня поточного року на офіційну сторінку Прем'єр-міністра України Арсенія Яценюка http://yatsenyuk.org.ua/ терористичним кіберугрупованням КіберБеркут було вчинено DDoS-атаку та на деякий час блоковано цей веб-ресурс. Зазначене угрупування хактівістів своїми злочинними діями створює імідж повної незахищеності українських владних структур перед хакерами, а значить, і, перед зовнішнім ворогом. Лише в січні 2015 року КіберБеркутом було також заблокувовано роботу сайтів Канцлера ФРН і Бундестагу, отримало доступ до комп'ютерів керівництва військової прокуратури України, юридичної служби і персонального комп'ютера народного депутата України і лідера Правого сектору Дмитра Яроша.

Відбувається активізація кіберзлочинних проявів. У минулому та на початку поточного року було вчинено такі види кібершахрайств. Від кібератак шахраїв лише у листопаді 2014 року постраждали: муніципальні сайти американського міста Форт-Лодердейл, МВС РФ, сайт PlayStation Store, web- сайт PHPBB, шведський уряд, ICANN, промислові підприємства Німеччини, урядові сайти Афганістану, блог Microsoft, Xbox Live і PlayStation Network, компанія Sony, а також користувачі Tor, NVIDIA. Кіберзлочинці також продовжили здійснення атак на ресурси різних організацій, спрямовані на викрадення особистих даних користувачів. Зокрема, рентгенолог з клініки м. Нью-Йорк, США викрав дані 97 тис. пацієнтів. Крім того, в Мережі виявилися дані 130 тисяч користувачів китайського сервісу бронювання квитків.

Хакерське організоване злочинне угруповання Anunak, відповідно до звітів за результатами спільного розслідування експертів компаній Group-IB та Fox-IT, вчинило ряд кібершахрайств в 2014 році стосовно російських банків і

платіжних систем понад 1 млрд руб., використовуючи у якості засобу проникнення цільові фішингові розсилки на ім'я рядових співробітників цих фінустанов, здійснюючи атаки на системи PoS-терминалів торгівельних мереж, медіа-групи, державні органи влади та управління.

У грудні 2014 року хакери продовжили вчиняти атаки з метою викрадення банківських даних, унаслідок чого постраждали такі компанії, як Staples, провайдер платіжних рішень CHARGE Anywhere, а також мережа магазинів Bebe.

Працівники УБКЗ ГУМВС України в Запорізькій області викрили ОЗГ шахраїв, які на Інтернет-сайтах знаходили об'яви про продаж майна, телефонували продавцю товару та повідомляли йому про начебто здійснену оплату, в телефонному режимі представлялися співробітниками банківської установи та, посилаючись на технічні проблеми щодо переведення коштів, "вирішували^ їх тільки дізнавшись номер, код та інші реквізити платіжної картки, гроші з банківської картки заявника зникали. 22 січня 2015 року за місцем проживання членів ОЗГ проведено санкціонований обшук, в результаті якого було вилучено банківські картки з грошовими коштами, сім-карти, мобільні телефони, чорнові записи, що підтверджують злочинну діяльність та відкрито кримінальне провадження за ч. 3 ст. 190 КК України.

В лютому поточного року в спеціальному адміністративному районі КНР, Гонконзі, було вчинено шахрайство, внаслідок якого на місцевій е-біржі злочинці заволоділи криптовалютою Bitcoin у кількості 386,9 млн [4]. Це найбільша сума втрат від кібершахрайства з використанням криптовалют, оскільки загальна кількість Bitcoin у світі не перевищує 3 млрд. Шахраї використали підроблені Bitcoin-торги для залучення інвесторів, закликаючи вигідно вкладати гроші та обіцяючи повернути вклади всім інвесторам одразу після переходу на більш високий рівень, який вимагав залучення нових клієнтів, обіцяючи повернути вклади протягом чотирьох місяців.

Отже, рівень захисту інформаційних ресурсів України як державних, так і недержавних, у тому числі об'єктів критичної інфраструктури, є таким, що не відповідає викликам сьогодення, а інформаційна безпека знаходиться на недостатньому рівні, що є загрозою національній безпеці в інформаційному просторі. Вже понад два роки ведуться дискусії, обговорення законопроектів щодо кібернетичної безпеки України: 2012 року
- 1, 2013 - 2, 2014 - 1. А результатом - є відсутність як профільного закону, стратегії, так і методології, кібернетичної моделі забезпечення кібербезпеки України.

За останні п'ять років позиції України в захисті державних інформаційних ресурсів були істотно ослаблені, зате склалася практика розподілу коштів держбюджету серед пулу приватних компаній, які супроводжують ресурси держорганів. Проблема розпилення бюджетного фінансування потреб інформатизації та захисту інформації вимагає наведення порядку, бо збиток від безладу колосальний: від хакерських атак страждає весь імідж України.

На фоні висвітлених проблем зростає необхідність у не спорадичному, а в системному, наступальному підході до питань протидії й нейтралізації результатів дестабілізуючої діяльності у інформаційній сфері, боротьби зі злочинністю взагалі, злочинами, що вчиняються з використанням мережі Інтернет - кіберзлочинністю та кібершахрайством, зокрема.

Список використаних джерел

1. На сайте госторгов появилось объявление о продаже Кремля / [Электронный ресурс]. - Режим доступа : http://top.rbc.ru/society/17/02/2015/54e328c59a79471edc867.

2. СБУ затримала злочинне угруповання, яке готувало серію вибухів на Дніпропетровщині / [Електронний ресурс]. - Режим доступу : http : //www .sbu.gov .ua/sbu/control/uk/publish/article ?art_id=1 34900&cat_id=39574.

3. Skeleton Key Malware Analysis / [Електронний ресурс]. - Режим доступу :

http : //www .secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis.

4. В Гонконге исчезла биржа Bitcoin с $387 млн на счетах / [Электронный ресурс]. - Режим доступа : http : //news.finance.ua/ru/news/~/344265.