Дослідження сучасних методів кібер-атак

УДК 004.056.53

Каріна Безверха

Національний авіаційний університет, karina0kira@ukr.net

«Кіберзлочинність», «кібер-атаки», «кіберзахист» за останні декілька років, особливо в нашій країні, набули масштабного поширення та розуміння. На сам перед це пов'язано звичайно з продовженням активного розвитку інформаційних технологій, які поглиблюють всі сфери життєдіяльності людства та держав в цілому. Однак, розвиток інформаційних технологій, зі всіма позитивними результатами їх впровадження, одразу ж створюють підґрунтя для зловживання шахраями. Злочинність в кіберпросторі - одна з найгостріших проблем, з якою зіткнувся весь світ протягом останніх років. Цей метод злочинності стає більш витонченим та не передбачуваним та на сьогоднішній день є однією з найбільш серйозних загроз в інформаційній сфері. З кожним роком хакерські атаки стають все більш складними і досконалими: зловмисники створюють потужні інфраструктури для здійснення і підтримки своїх шкідливих кампаній, постійно вдосконалюють свої технології і способи здійснення атак. В результаті чого, проваджені в організаціях засоби та заходи захисту виявляються недієвими. Тому дослідження методів кіберзлочинності є актуальною темою, яка дозволить проаналізувати актуальні вектори діяльності злочинців в кіберпросторі та затуляти дірки в існуючі методи та системи захисту на всіх рівнях.

В ході роботи було проаналізовано щорічні звіти з інформаційної безпеки за 2016-2017 роки компаній Cisco, Ernst&Young, Microsoft, Imperva та ін., результати міжнародних конференцій за останній рік, в результаті чого було зроблено наступні висновки:

Найпоширенішими залишаються DDos-атаки (SYN-DDoS, TCP-DDoS, HTTP-DDoS, DDos-атаки «на замовлення»): DDos-атак мережевого рівня, DDos-атаки прикладного рівня з великим об'ємом трафіку (8,7 Gbps). Також набирають обертів DDos-атаки з використанням HTTPS з'єднання для маскування своєї діяльності (drown, freak та ін.). Набирає обертів також атака типу програми–вимагачі, програми – шифрувальники, які за допомогою шкідливого програмного забезпечення шифрують дані на комп'ютерах, на веб-ресурсах та ін. з подальшими шантажем та вимогами викупу (WannaCrypt, KeRanger, Hailstorm, Snowshoe, Conficker, Dork bot). Ще одним типом атак, що прогресують є рекламне програмне забезпечення, тип атаки, діяльність якої направлена на зміну параметрів браузерів та операційної системи з метою ослаблення захисту, виведення з ладу антивірусних систем і інших засобів безпеки, контроль та встановлення іншого шкідливого програмного забезпечення, збір та крадіжка інформації (троян DNSChanger).

Рівень кібер-атак зростає щороку. Аналіз показав,що основна кількість атак припадає саме на виявлені вразливості в системах захисту інформації. Тому залишається важливим питання вдосконалення існуючих систем захисту.

Науковий керівник – к.т.н.,доцент кафедри БІТ Кінзерявий В.М.