Список бібліографічних посилань

1. Погребняк К А., Повтарєв Д. В. Аналіз безпеки сервісів зберігання даних у хмарі. Прикладная радиоэлектроника. 2013. Том 12, № 2. С. 202–208.

2. Хмарна безпека: чи згущуються хмари над захистом даних? // ООО «Видавничий дім "МЕДІА-ДК"». 12 грудня 2017 16:14. URL: https://biz.nv.ua/ukr/kibervoiny_i_biznes/hmarna-bezpeku-zgushchujutsja-chi-hmari-nad-zahistom-danih-2331588.html (дата звернення: 30.10.2018).

Одержано 30.10.2018

УДК 004.056.53

Михайло Юрійович БУРДІН,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-6748-3321;
Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-9017-9635;
Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії
кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3946-0189

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРАТАКАМ НОВОГО ПОКОЛІННЯ

Останнім часом фахівцями з кібербезпеки було відзначено значне зростання рівня небезпечності атак у кіберпросторі, що дало привід зробити висновки про появу кібератак нового покоління.

У лютому 2018 р. аналітики антивірусної компанії McAfee підрахували, що в 2017 р. світовий збиток від кіберзлочинів склав близько $ 600 млрд., або 0,8 % від світового ВВП, збільшившись приблизно на 35 % у порівнянні з оцінкою за 2014 рік, яка становила $ 445 млрд. Серед факторів, що зумовили зростання, фахівці перерахували таке: дедалі витонченіші хакерські атаки, розширення ринку кіберкримінальних послуг і поширення криптовалют. Експерти визнали, що найбільш швидко зростає такий вид кіберзлочинів, як атаки за допомогою вірусів-шифрувальників. Хакери все частіше вдаються до цього методу на тлі зростаючої доступності сервісів, побудованих за моделлю Ransomware-as-a-Service (RaaS, «Вимагання як послуга»). У McAfee нарахували понад 6 тис. кримінальних онлайн-ресурсів, які пропонують віруси-вимагачі та послуги з організації атак за їх допомогою.

Згідно зі звітом 2018 Security Report, який опублікувала компанія Check Point Software Technologies, більш ніж 300 мобільних програмних продуктів, що поширюються через офіційні магазини, містять у собі шкідливий програмний код. Це свідчить про недостатню захищеність офіційних онлайн-крамниць від проникнення шкідливого програмного забезпечення.

За інформацією Check Point, 2018 Security Report спирається на дані численних досліджень серед IT-директорів і керівників бізнесу, а також звітів Check Point's Threat Cloud і Threat Intelligence Report. Дослідження охоплює всі сучасні загрози, спрямовані на такі галузі, як охорона здоров'я, промисловість і державні структури. Пітер Александер, директор по маркетингу Check Point Software Technologies, зауважив, що все наше суспільство знаходиться під загрозою масштабних кібератак наступного покоління (Gen V). Нове покоління кібератак відрізняється від попередніх поколінь своєю масштабністю, багатовекторністю і швидкістю розповсюдження. Щоб отримати більше інформації про сучасний ландшафт кіберзагроз, Check Point опитав 443 фахівців з інформаційної безпеки по всьому світу про виклики, з якими вони стикаються, відбиваючи кібератаки нового покоління. Результати дослідження показали, що захист більшості компаній відстає на 10 років і як мінімум на два покоління від сучасних кібератак Gen V. 77 % опитаних висловили стурбованість тим, що організації не готові до таких сучасних кібератак і що переважна більшість інфраструктур безпеки компаній є безнадійно застарілими. Близько 97 % компаній не мають рішень, що здатні протистояти кібератакам Gen V. У групі ризику опинилися всі: банки, медичні установи, державні структури, великі корпорації, малі та середні підприємства. Це свідчить про глобальну уразливість сучасної інфраструктури перед атаками «П'ятого покоління».

Наприклад, на початку квітня 2018 р. стало відомо про хакерські атаки на чотири американські газові компанії. В результаті кібернападу деякі IT-системи на кілька днів були зупинені з метою безпеки. Невідомі кіберзлочинці напали на Boardwalk Pipeline Partners, Eastern Shore Natural Gas, Oneok і Energy Transfer, які займаються обслуговуванням газопроводів. Атаки були здійснені в кінці березня. У компанії Oneok, яка управляє газовими магістралями в пермському нафтогазоносному басейні в Техасі і Скелястих горах (західна частина Північної Америки), заявили, що як запобіжний захід було ухвалено рішення відключити комп'ютерну систему після того, як стало очевидно, що підрядник став жертвою кібератаки. Oneok не уточнила, робота якої системи була заморожена, але сам факт відключення системи свідчить про недостатній рівень інформаційної безпеки на цих підприємствах.

У Energy Transfer розповіли, що компанія відключила платформу для обміну даними (EDI; через неї передають замовлення на поставку, рахунки тощо) з клієнтами, яку розробила дочірня Energy Services

Group для прискорення передачі документів і скорочення витрат. На думку експерта з кібербезпеки промислових систем Філа Нерая (Phil Neray), хакерська атака на газопровідні компанії була проведена з метою фінансового збагачення, однак не варто виключати, що за цим могли стояти владні структури будь-яких країн.

Жертвами кібератак стають підприємства й організації всіх масштабів, а економічний збиток від подібних зловмисних дій до 2022 р. може досягти $ 8 трлн. При цьому багато корпорацій вже задумалися над шляхами вирішення проблеми – про це свідчать сплановані на наступні роки бюджети. Так, за прогнозами Cybersecurity Ventures, протягом наступних чотирьох років глобальні витрати на кібербезпеку складуть близько $ 1 трлн.

Найбільша кількість кібератак спрямована на банківські структури та різноманітні фінансові інститути, як найпривабливіші з точки зору отриманих злочинцями прибутків. Експерти з кібербезпеки Threat Intelligence з початку року зафіксували значну активність хакерської групи Cobalt, спрямовану на банківські системи відразу в близько 40 країнах світу. Атаки цієї групи дуже небезпечні завдяки добре скоординованим діям зловмисників з різних куточків світу та використанню ними найбільш сучасних програмних засобів, таких як Carbanak, Cobalt Strike, Anunak. Хоча ватажка цієї групи було заарештовано в Іспанії ще у 2017 р., його спільники продовжують свою злочинну діяльність і ще завдадуть світовій фінансовій сфері чималих збитків.

Протистояти міжнародній хакерській злочинній дяльності зараз можливо лише сумісними зусиллями правоохоронних органів усіх держав світу, державних служб, служб безпеки приватних компаній та об’єднань фахівців з кібербезпеки.

У зв’язку з цим 17 квітня 2018 р. 34 компанії в сфері технологій і забезпечення безпеки підписали Технологічну угоду з кібербезпеки (Cybersecurity Tech Accord) – договір між найбільшою в історії групою компаній, які зобов'язуються захищати клієнтів по всьому світу від зловмисних дій кіберзлочинців. У число 34 компаній-підписантів увійшли ABB, Bitdefender, Cisco, ARM, BT, Cloudflare, Avast!, CA Technologies, DataStax, Dell, HPE, SAP, DocuSign, Intuit, Stripe, Facebook, Juniper Networks, Symantec, Fastly, LinkedIn, Telefonica, FireEye, Microsoft, Tenable, F-Secure, Nielsen, Trend Micro, GitHub, Nokia, VMware, Guardtime, Oracle, HP Inc., RSA. Разом ці підприємства представляють творців і користувачів технологій, що забезпечують роботу світової комунікаційної та інформаційної інфраструктури. Технологічна угода залишається відкритою для інших компаній незалежно від масштабів або спеціалізації їх діяльності, які користуються високою репутацією, суворими стандартами кібербезпеки і згодні безумовно дотримуватися принципів документа.

Компанії-підписанти створять більш потужну систему захисту від кібератак. У рамках цієї угоди вони зобов'язалися захищати клієнтів по

всьому світу незалежно від мотивів і цілей онлайн-атак. Компанії не сприятимуть урядам у нанесенні кібератак і вживатимуть заходів щодо захисту своїх продуктів і сервісів від зламу або некоректного використання на всіх етапах технологічної розробки та дистрибуції.

Підприємства будуть докладати додаткових зусиль для підтримки розробників, компаній і приватних користувачів своїх технологій, допомагаючи їм розширювати свою здатність до самозахисту. Такі зусилля можуть включати спільну розробку нових практичних стандартів забезпечення безпеки та нових функцій, які компанії зможуть впроваджувати у свої продукти і сервіси.

Компанії будуть розвивати існуючі зв'язки і спільно створювати нові формальні й неформальні партнерства з іншими представниками галузі, громадянського суспільства і дослідницьких кіл з метою нарощування масштабів технічного співробітництва, виявлення чинників вразливості, спільного аналізу ризиків і зведення до мінімуму потенційну можливість появи шкідливих кодів у кіберпросторі.

Звичайно, цього недостатньо, щоб зупинити бурхливе зростання кіберзлочинів у світі, але це може стати першим кроком до об'єднання всього небайдужого до проблем кібербезпеки суспільства задля протидії злочинцям у кіберпросторі.

Одержано 02.11.2018

УДК 004.056.5

Антон Вікторович ВОЛКОВ,
курсант 1 курсу групи Ф4-102 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

НАЙБІЛЬШ РОЗПОВСЮДЖЕНІ ЗЛОЧИНИ У КІБЕРПРОСТОРІ

Вступ і постановка проблеми.

Широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Через збільшення ролі комп'ютеризації в житті громадянина і держави, збільшується і можлива шкода завдана зловмисниками шляхом злочинів в кіберпросторі. Інтернет став ефективною зброєю в руках злочинців. За оцінками експертів Міжнародної торгової палати, число злочинів, які вчиняються за допомогою глобальної комп'ютерної мережі Інтернет, зростає, причому пропорційно числу користувачів. За даними Інтерполу, Інтернет став тією сферою, де рівень злочинності зростає найшвидшими темпами.

Наразі жодна країна не здатна протистояти цим загрозам самостійно, в повній мірі. Саме тому провідні країни і організації співпрацюють для боротьби з кіберзагрозами. За останні роки вже не