наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Резюмуючи викладене вище зазначимо, що пріоритетами та напрямами забезпечення кібербезпеки України є: розвиток безпечного, стабільного і надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом; кіберзахист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки тощо.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15.03.2016 № 96/2016 287 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 04.10.2018).

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287 // БД Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 04.10.2018).

Одержано 05.10.2018

УДК 004.77

Юрій Володимирович КАРГАПОЛОВ,
член правління Інтернет Асоціації України,
генеральний директор Консорціуму «Український Центр підтримки номерів і адрес»

ЗМІНА ПАРАДИГМИ ПРОФІЛАКТИКИ І ПРИПИНЕННЯ ПРАВОПОРУШЕНЬ В ЧАСТИНІ ПОШИРЕННЯ КОНТЕНТУ В СЕРЕДОВИЩІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

1. Існуюча парадигма спрямована на виявлення і подальше блокування ресурсів, на яких або за допомогою яких відбувається поширення контенту, що містить ознаки правопорушень.

Всі зусилля сьогодні зосереджені на питаннях моніторингу та подальшого блокування каналів комунікацій між суб'єктами в електронному середовищі. Це стосується каналів дистрибуції трафіку різного типу - від торгівлі наркотиками, торгівлі людьми до розповсюдження контенту, що містить заклики до екстремізму або порушує права інтелектуальної власності.

У будь-якому випадку практична робота правоохоронних органів виражається і оцінюється відносно успішного або неуспішного результату, направленому на усунення порушення.

2. Чи є така парадигма ефективної з точки зору технологічних можливостей, що надаються електронними комунікаціями?

Використання середовища електронних комунікацій породило абсолютно нові технологічні реалії та можливості, якими можуть скористатися злочинці. Технології дозволяють миттєво змінювати своє фізичне розташування, видаючи в стек відомостей щодо геолокації суб'єкта зв'язку недостовірні дані; використовувати різні за своєю природою мітки (посилання) на використовувані правопорушниками ресурси, чим ускладняються їх ідентифікація; змінювати асоціативні зв'язки між різними типами ідентифікаторів і використовувати механізми резолвінгу для миттєвої зміни розташування ресурсу в мережі і маскування трафіку; задіяти простір DarkNet і розчиняючись за численними серверами маскувати джерело трафіку тощо.

Якщо моніторинг в цих умовах є завданням реальним, оскільки дозволяє відстежувати факти сесій і частково, що дуже важливо підкреслити – частково – фіксувати дані, пов'язані з правопорушенням, то наступні кроки, спрямовані на:

– виявлення ситуаційної локації суб'єкта;

– чіткого визначення мережевого розташування джерела контенту;

– DNS- і IP-адреси джерела трафіку на всіх етапах формування його шляхів;

– деанонімізація номерів в форматі E.164;

– отримання відомостей про персоналії, які зареєстрували сервіси тощо,

практично неможливо здійснити.

Це перш за все пов'язано з:

– відсутністю інструментальної платформи, що дозволяє створювати, аналізувати і прогнозувати профілі цифрових об'єктів;

– відсутністю реальної інструментальної можливості для правоохоронних органів поєднувати і аналізувати дані з мереж на основі стека протоколу СКС-7 та IP-протоколу;

– відсутністю релевантних властивостями мінливості IP-середовища методик аналізу відомостей про цифрових об'єктах;

– пробілами існуючого законодавства, що допускає повну анонімізацію при використанні е-сервісів і відсутністю нормативно-правових актів, спрямованих на структуризацію відомостей про процеси використання е-сервісів.

Всі ці фактори набувають визначальне значення, оскільки електронні комунікації сьогодні орієнтовані на використання IP-протоколу, який визнаний в якості базового для їх розвитку, а отже, з кожним днем розвиток технологій буде приносити все нові форми опору, маскування і догляду

Основна кількість е-сервісів, більше 98%, створено на базі технологій з використанням IP-протоколу і орієнтується на те, що абоненти будуть їх використовувати в Інтернет. Спосіб і метод доступу до мережі стають факторами, які можуть внести ще більше ентропії в процес ідентифікації суб'єкта, оскільки може динамічно змінюватися зловмисником. А без 100% ідентифікації суб'єкта не можна почати аналіз одержуваних під час моніторингу відомостей, оскільки немає впевненості, що ці дані про один суб'єкт і пов’язаний з ним предмет.

3. Факт неможливості використання технологій блокувань або обмежень в середовищі електронних комунікацій.

Практика застосування парадигми блокувань є неефективною.

Недоліки існуючої практики особливо яскраво проявляються на прикладах спроб блокування контенту ресурсів мережі Інтернет, блокувань телеграм та інших чат-каналів та ін.

Результатом зазвичай є килимові бомбометання по хостингам або операторам, які виступають основними потерпілими від таких дій, що в кінцевому підсумку призводить до деградації чи руйнування сегментів ІКТ-ринку.

В ході конференції ENOG-14 в м Мінську 9-10 жовтня 2017 року розгляду цих проблем була присвячена дискусійна панель, з підсумковими результатами якої можна ознайомитися за адресою https://www.enog.org/enog-14/ru/meeting-report.

Ці питання також були обговорені під час спільної секції ІнАУ і УКОС «Новації і виклики законодавства» у доповіді ІнАУ «Про блокування доступу до Інтернету», яка відбулася в рамках конференції УКОС 4-7 жовтня 2017 року в Буковелі.

4. Яка альтернатива? Перехід до парадигми передбачення поведінки цифрового об'єкта і прогнозування його станів.

Перш за все необхідно перейти до розуміння, що в середовищі електронних комунікацій існує поняття цифровий об'єкт, яким можуть бути як фізичні, так і юридичні особи, так і технологічні об'єкти у вигляді серверів, комп'ютерів, телефонів і смартфонів, а також у вигляді масивів даних на зберігачах, об'єднаних по якомусь критерію тощо.

Будь-який цифровий об'єкт має свій профіль, який не є статичним, але динамічним і має свої властиві, притаманні цьому цифровому об'єкту закономірності розвитку і процеси.

Створення інструментальної платформи, орієнтованої на роботу з профілями цифрових об'єктів дозволяє не тільки фіксувати факти правопорушень, використати моніторинг процесів, пов'язаних з ними, але і бути впевненими, що аналіз даних відбувається з дотриманням всіх критеріїв об'єктивності і має гарантовану підставу для створення доказової бази, але й формувати механізми прогнозування поведінки цифрового об'єкта.

Саме в цій точці і відбувається відмова від парадигми блокувань і перехід до парадигми, де з'являється можливість ідентифікації правопорушника і передбачення його поведінки в різних ситуаціях з подальшими кроками, спрямованими на запобігання і припинення правопорушень.

Одержано 12.11.2018

УДК 004[681.518]

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-1020-9399

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Взаємодія між компонентами будь-якої системи характеризується передусім поняттям доступу суб'єктів до об'єктів. Суб'єктом може виступати користувач або процес (завдання, трансакція, запущена програма або сервіс), а об'єктом – логічний або фізичний ресурс системи, такої як файл, набір даних, програма, сервіс, база даних, канал передавання даних тощо. Базовою характеристикою доступу є те, що в результаті його створюється потік інформації від об'єкта до суб'єкта, шляхом виконання операцій, таких як читання, запис, модифікація, пошук та ін.

Управління доступом є ключовим механізмом безпеки в інформаційному просторі. Механізми управління доступом можуть бути класифіковані [2] за рівнями реалізації механізмів безпеки, механізми безпеки – за етапами роботи і компонентами.

За рівнями реалізації виділяють три категорії механізмів безпеки:

– *адміністративні механізми* включають політики, плани, процедури, заходи, що визначені політикою безпеки організації;

– *технічні механізми безпеки* – програмні або апаратні засоби, підсистеми і сервіси інформаційної безпеки;

– *механізми фізичного захисту* – фізичні бар'єри, екрани і засоби контролю доступу.

Механізми безпеки за етапами роботи і компонентами, які реалізують підсистему управління доступом, поділяють на механізми ідентифікації, автентифікації, авторизації та моніторингу.

На етапі ідентифікації визначаються і перевіряються ідентифікатори суб'єкта й об'єкта системи. При автентифікації перевіряється достовірність суб'єкта, чи дійсно він той, за якого себе видає. Якщо суб'єкт автентифікований і має відповідні права на об'єкт, він буде авторизований, тобто йому надається доступ до запрошеного ним об'єкта. Моніторинг передбачає протоколювання й аналіз подій безпеки [1].