УДК 004.056.57

Є. В. Масталярчук
Західноукраїнський національний університет, Україна

СИСТЕМИ РОЗВІДКИ КІБЕРЗАГРОЗ У СЬОГОДЕННІ

Evheniy Mastaliarchuk

CYBER THREAT INTELLIGENCE SYSTEMS TODAY

Аналіз кіберзагроз

При аналізі досвіду кіберзагроз розуміємо, що багато залежить від тріади акторів, намірів і можливостей, з урахуванням їх тактики, техніки та процедур (TTP), мотивації та доступу до намічених цілей. Вивчаючи цю тріаду, часто можна розробити напрямки інформування, стратегічні цілі, оперативну та тактичну оцінки.

— Стратегічний блок оцінює різнорідні фрагменти інформації для формування інтегрованих уявлень. Він інформує тих, хто приймає рішення та політику, щодо широких чи довгострокових питань та/або забезпечує своєчасне попередження про загрози. Аналіз стратегії кіберзагроз формує загальне уявлення про наміри та можливості шкідливих кіберзагроз, включаючи учасників, інструменти та TTP, шляхом визначення тенденцій, закономірностей та нових загроз та ризиків, щоб інформувати тих, хто приймає рішення та встановити інформаційний маркер для своєчасного попередження.

— Оперативна розвідка оцінює конкретні потенційні інциденти, пов’язані з подіями, розслідуваннями та/або діяльністю, і надає інформацію, яка може керувати та підтримувати операції реагування. Оперативна або технічна розвідка про кіберзагрози надає високоспеціалізовані, технічно зосереджені розвідувальні дані для керівництва та підтримки реагування на конкретні інциденти; такі розвідувальні дані часто пов’язані з кампаніями, шкідливим програмним забезпеченням та/або інструментами і можуть надходити у формі експертних звітів.

— Тактична розвідка оцінює події, розслідування та/або дії в реальному часі та надає щоденну оперативну підтримку. Тактична розвідка кіберзагроз забезпечує підтримку повсякденних операцій і подій, таких як розробка підписів та індикаторів компромісу (IOC). Це часто передбачає обмежене застосування традиційних методів аналізу.

Вищевикладений матеріал можна представити у вигляді піраміди рівнів.

Рисунок 1. Піраміда рівнів аналізу кіберзагроз

Розвідка про кіберзагрози виявилася корисною для державних, місцевих, і територіальних структур (SLTT) на всіх рівнях, від вищих керівників до тих, хто працює на місцях.

Найпопулярніші платформи розвідки

Основні функції найкращої платформи розвідки загроз включають консолідацію каналів розвідки загроз із кількох джерел, автоматичну ідентифікацію та стримування нових

атак, аналітику безпеки та інтеграцію з іншими інструментами безпеки, такими як SIEM, брандмауери нового покоління (NGFW) та EDR.

IBM X-Force Exchange — це хмарна платформа для спільного аналізу загроз, яка допомагає аналітикам безпеки досліджувати показники загроз, щоб прискорити час реакцій. Ця TIP поєднує створені людиною розвідувальні дані з глобальною мережею безпеки, пропонуючи унікальний погляд на потенційні загрози. Інструментальну панель X-Force Exchange можна налаштувати, що дозволяє користувачам розставляти пріоритети відповідних розвідувальних даних відповідно до своїх потреб, таких як поради та вразливості.

Anomali ThreatStream об'єднує мільйони індикаторів загроз, щоб виявляти нові атаки, виявляти наявні порушення та давати можливість командам безпеки швидко розуміти та стримувати загрози. Ключовою відмінністю Anomali є його високоточний алгоритм машинного навчання, який призначає оцінки індикаторам компромісу (IOC), щоб команди безпеки могли визначити пріоритети завдань з пом'якшення. ThreatStream також дозволяє інтегруватися з багатьма популярними SIEM та платформами керування.

Palo Alto Networks AutoFocus виконує аналітику загроз з повним контекстом доступною для організацій будь-якого розміру. Ця розміщена служба надає командам з безпеки аналітичних даних, кореляції, контексту та автоматизованих робочих процесів запобігання, які їм необхідні для виявлення та реагування на події в режимі реального часу. AutoFocus також включає доступ до сховища оперативної розвідки Unit 42, внутрішньої групи дослідження загроз Palo Alto Networks.

Кібернапади на світовій арені

Набагато більше держав сьогодні вважають кіберзасоби і сили легітимним і необхідним елементом свого стратегічного набору інструментів поряд з дипломатією, економічною силою і військовою потужністю. Це викликає занепокоєння, чи не станемо ми у найближчому майбутньому свідками повномасштабної війни в кіберпросторі між державами. На додаток ми бачимо, що недержавні дійові особи час від часу виявляють зацікавленість у застосуванні кіберзасобів – хоча наразі є небагато свідчень їх фактичного застосування.

З кожним роком фіксується збільшення кількості кібератак та кіберзагроз в цілому.

Проте науковці, такі як Томас Рід, вважають, що кібервійна не відбудеться. Сучасний досвід фактичного застосування державами кіберзасобів вказує на те, що для таких засобів більш характерні шпигунство або саботаж, що робить більш вірогідним їх застосування нижче порогу, який визначає збройний напад. Попри певну логічність цього аргументу, стає дедалі більш зрозуміло, що деякі держави розглядають кіберзасоби невіддільною частиною своїх оперативних військових сил і засобів і не бояться застосовувати їх в такій якості, навіть якщо вони не схильні до публічного визнання цього.

Література:

1. https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/
2. https://www.esecurityplanet.com/products/threat-intelligence-platforms/
3. https://www.nato.int/docu/review/uk/articles/2016/06/08/zmna-pdhodv-do-kberzahistu/index.html