БАЗА ЗНАНИЙ MITRE ATT&CK ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.Ф. Чаган

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В целях всестороннего построения системы защиты информации в информационных системах и ресурсах необходимо принимать во внимание все возможные угрозы как извне, так и внутри самой системы. Для этого часто прибегают к построению модели нарушителя информационной безопасности.

MITRE ATT&CK [1] является базой знаний, в которой способы описания и категоризация поведения злоумышленника основываются на анализе реальных APT-атак (Advanced Persistent Threat) индивидуальных или организованных преступных групп и написаны правила для автоматизации расследований. Проще говоря, это база знаний о поведении противника, представляющая единый язык для описания одного и того же поведения, который могут использовать различные команды и организации. Данная модель строится с позиции атакующего.

В указанной базе знаний известные поведения злоумышленников разделены на тактики, техники, процедуры и выражаются в виде таблиц (матриц) для различных ситуаций и типов. Тактика показывает, как злоумышленник действует на разных этапах атаки, какая цель или задача у него на каждом этапе. Техника – как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, утилиты, технологии, коды, эксплоиты. Процедура отражает какая техника выполняется и для чего. Поскольку данный список дает комплексное представление о поведении злоумышленника при взломе сетей, он крайне полезен для организации различных защитных мероприятий, мониторинга, обучения и т.д.

Общедоступная база знаний MITRE ATT&CK содержит раздел, посвященный организованным преступным группам, что дает возможность описать поведение злоумышленников в унифицированной форме. Злоумышленники отслеживаются по действиям, характерным именно для них, путем сопоставления с техниками и тактиками в ATT&CK.

Группа – это кластеры действий, которые отслеживаются под общим именем в сообществе безопасности (группы угроз, группы активности и субъекты угроз). В настоящее время (на апрель 2023 г.) база ATT&CK содержит подробную информацию о 135 группах с указанием используемых ими техник и инструментов.

Использование данной базы позволяет отслеживать активности после компрометации, фокусироваться на поведении злоумышленника, а не на единичных флагах, сигнализирующих о нарушениях, а также перейти от реактивных к проактивным действиям.

Список литературы

1. MITRE ATT&CK® [Электронный ресурс]. – Режим доступа: https://attack.mitre.org. – Дата доступа: 04.04.2023.