



Современные подходы к моделированию
угроз безопасности информации.

Источники информации об угрозах
безопасности информации

Часть 1

■ Аксененко Ю.И, Сидак А.А.

Содержание

Введение	2
База знаний об известных тактиках и приемах нарушителей безопасности MITRE ATT&CK™	3
1. Тактики действий нарушителей /Tactics/	4
1.1 Тактики действий нарушителей, связанные с подготовительными действиями к атакам /PRE-ATT&CK Tactics/	5
1.2 Тактики действий нарушителей в корпоративной сети /Enterprise Tactics/	6
1.3 Тактики действий нарушителей, связанных с использованием мобильных устройств /Mobile Tactics/	7
2. Техники действий нарушителей /Techniques/	8
3. Группы нарушителей /Groups/	9
4. Программное обеспечение для реализации угроз /Software/	10
Список литературы	11

Введение



Нормативными правовыми актами ФСТЭК России определены требования по разработке моделей угроз безопасности информации для информационных систем.

1,2

БИ – безопасность информации
ИС – информационные системы

Основным источником исходных данных для определения угроз безопасности информации в информационной системе является банк данных угроз безопасности информации [а](#), ведение которого осуществляется ФСТЭК России /БДУ ФСТЭК России/. ФСТЭК России постоянно развивает банк данных угроз и регулярно доводит информацию об особенностях и перспективах его использования на различных форумах, конференциях и семинарах.

Также при определении угроз БИ и разработке модели угроз БИ для ИС, в дополнение к БДУ ФСТЭК России, могут использоваться иные источники, содержащие сведения об угрозах БИ. [1,2](#)

В качестве наиболее известных дополнительных /по отношению к БДУ ФСТЭК России/ источников информации об угрозах можно привести следующие:

- 1) база знаний об известных тактиках и приемах нарушителей безопасности MITRE ATT&CK™ [б](#)
- 2) каталог шаблонов атак CAPEC™ [в](#)
- 3) каталог угроз БИ германского федерального ведомства по информационной безопасности BSI /BSI IT-Grundschutz Kataloge/ [г](#)

а) <https://bdu.fstec.ru/threat>

б) <https://attack.mitre.org/>

в) <https://capec.mitre.org/index.html>

г) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompodium/elementare_gefaehrdungen/elementare_Gefaehrdungen_Uebersicht_node.html?sessionId=E6E1263DFF2ABCC406C35285E7D37BC1.2_cid360

База знаний об известных тактиках и приемах нарушителей безопасности MITRE ATT&CK™

ATT&CK™

ПОЛНОЕ НАЗВАНИЕ –
Adversarial Tactics,
Techniques, and Common
Knowledge
/Тактики, техники действий
нарушителей и общая информация
о нарушителях/

Интернет-ресурс 

База знаний ATT&CK™ была создана компанией MITRE /The MITRE Corporation/ в целях систематической классификации поведения нарушителей в рамках деятельности по практическому моделированию действий нарушителей БИ в ИС.

Основой базы знаний ATT&CK™ является каталог действий /техник/, которые нарушители ИБ в ИС могут выполнять для достижения своих целей /тактик/. Первая версия базы знаний ATT&CK™ была разработана в 2013 года и была ориентирована в основном на корпоративную сеть /Enterprise/, функционирующую на платформе Windows.

В дальнейшем каталог ATT&CK™ был доработан и опубликован в 2015 году в составе 96 техник /techniques/, сгруппированных в относительно 9 тактик /tactics/. К настоящему времени каталог ATT&CK™ был существенно расширен, в том числе за счет вклада сообщества экспертов по кибербезопасности. 

База знаний ATT&CK™ включает следующие основные разделы:

- тактики действий нарушителей /Tactics/;
- техники действий нарушителей /Techniques/;
- группы нарушителей /Groups/;
- программное обеспечение для реализации угроз /Software/.

Тактики и техники в базе знаний MITRE ATT&CK™ сгруппированы по следующим областям деятельности нарушителей:

- область деятельности PRE-ATT&CK Tactics /подготовительная деятельности нарушителя до непосредственного проникновения в систему/;
- технологическая область Enterprise /корпоративные сети/;
- технологическая область Mobile /использование мобильных устройств/.

Тактики действий нарушителей /Tactics/ представляют собой цели /задачи/, которые достигаются /решаются/ нарушителем.

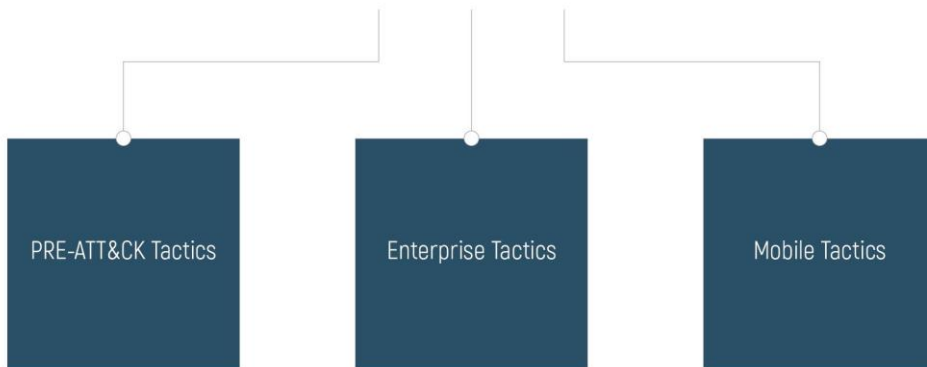
В то же время техники действий нарушителей /Techniques/ – это непосредственные действия, которые осуществляет нарушитель для достижения своих целей /решения задач/.

В технологической области Enterprise выделены следующие платформы: Linux, macOS, Windows; в технологической области Mobile – Android, iOS. Ожидается, что по мере развития базы знаний MITRE ATT&CK™ число платформ, для которых будут моделироваться действия нарушителей, будет расширяться.

1

Тактики действий нарушителей /Tactics/

Как отмечалось выше, тактики действий нарушителей /Tactics/ представляют собой цели /задачи/ деятельности нарушителей и сгруппированы в базе знаний MITRE ATT&CK™ по следующим областям:



1.1

Тактики действий нарушителей, связанные с подготовительными действиями к атакам /PRE-ATT&CK Tactics/

В базе знаний MITRE ATT&CK™ определены следующие категории тактик действий нарушителей, связанных с подготовительными действиями к атакам /PRE-ATT&CK Tactics/:

- планирование определения приоритетов /Priority Definition Planning/;
- определение приоритетов /Priority Definition Direction/;
- выбор объектов атаки /Target Selection/;
- сбор технической информации /Technical Information Gathering/;
- сбор информации о персонале /People Information Gathering/;
- сбор информации о функционировании организации /Organizational Information Gathering/;
- выявление технических недостатков /Technical Weakness Identification/;
- выявление слабых сторон у персонала /People Weakness Identification/;



- выявление слабых сторон функционирования организации /Organizational Weakness Identification/;
- обеспечение скрытности действий нарушителя /Adversary OPSEC/;
- создание и поддержка инфраструктуры проведения атак /Establish & Maintain Infrastructure/;
- создание ложной личности /Persona Development/;
- создание возможностей /потенциала/ нарушителя /Build Capabilities/;
- опробование возможностей /Test Capabilities/;
- обеспечение использования возможностей /Stage Capabilities/.

1.2 Тактики действий нарушителей в корпоративной сети /Enterprise Tactics/

В базе знаний MITRE ATT&CK™ определены следующие категории тактик действий нарушителей в корпоративной сети /Enterprise Tactics/:

исходное проникновение в информационную инфраструктуру /Initial Access/;

исполнение вредоносного кода /Execution/;

сохранение доступа /Persistence/;

повышение привилегий /Privilege Escalation/;

обход защиты /Defense Evasion/;

доступ к учетным данным /Credential Access/;

получение знаний об информационной инфраструктуре /Discovery/;

перемещение в информационной инфраструктуре /Lateral Movement/;

сбор интересующих данных /Collection/;

взаимодействие со скомпрометированными системами /Command and Control/;

вывод собранных данных /Exfiltration/;

нарушение целостности и доступности систем и данных /Impact/.

1.3 Тактики действий нарушителей, связанных с использованием мобильных устройств /Mobile Tactics/

В базе знаний MITRE ATT&CK™ определены следующие категории тактик действий нарушителей, связанных с использованием мобильных устройств /Mobile Tactics/:

- исходное проникновение в мобильное устройство /Initial Access/;
- сохранение доступа /Persistence/;
- повышение привилегий /Privilege Escalation/;
- обход защиты /Defense Evasion/;
- доступ к учетным данным /Credential Access/;
- получение знаний о характеристика мобильного устройства /Discovery/;
- перемещение в информационной инфраструктуре /Lateral Movement/;
- негативное воздействие /Impact/;
- сбор интересующих данных /Collection/;
- вывод собранных данных /Exfiltration/;
- взаимодействие со скомпрометированными системами /Command and Control/;
- негативные воздействия, связанные с сетевым взаимодействием /Network Effects/;
- негативные воздействия, связанные со службами удаленного доступа /Remote Service Effects/.



Техники действий нарушителей

/Techniques/

Техники /Techniques/ представляют собой непосредственные действия нарушителей, направленные на достижение целей /решение задач/ нарушителей, сформулированных в базе знаний MITRE ATT&CK™ в виде тактик /Tactics/.
Техники /Techniques/ соотносятся с Тактиками /Tactics/ как «одна-ко-многим». Таким образом, одна и та же техника может использоваться для решения сразу нескольких задач нарушителя, сформулированных в базе знаний MITRE ATT&CK™ в виде соответствующих тактик.

Представление техник в базе знаний MITRE ATT&CK™ включает:

- идентификатор метода /ID/;
- наименование метода;
- общее описание метода;
- наименование тактики или тактик, которые могут быть осуществлены с использованием метода /Tactic/;
- идентификатор платформы по типу используемой операционной системы /Platform/;
- требования к условиям реализации /System Requirements/;
- права в системе, которые минимально необходимы нарушителю для выполнения техники /Required Permissions/;
- права, полученные при выполнении техники в результате повышения привилегий /Effective Permissions/;
- источники данных, с использованием которых можно обнаружить атаку в конкретной системе /Data Sources/;
- признак того, техника может быть использована для обхода механизмов защиты информации /Defense Bypass/;
- идентификатор соответствующего шаблона атак в каталог шаблонов атак CAPEC™ /CAPEC ID/;
- примеры реализации /Examples/ с указанием наименования /Name/ известных нарушителей или групп нарушителей /Groups/, вредоносного программного обеспечения или иного инструментария нарушителя /Software/ и описания совершенной атаки /Description/;
- способы обнаружения /Detection/;
- способы /меры/ предотвращения реализации техники или уменьшения последствий /Mitigation/;
- наименования подтехник /планируется в новой редакции/;
- описание подтехник /планируется в новой редакции/;
- составители описания техники /Contributors/.
- номер редакции описания техники /Version/.



3 Группы нарушителей /Groups/

Представление групп нарушителей /Groups/ в базе знаний MITRE ATT&CK™ включает:

- идентификатор группы /ID/;
- наименование группы нарушителей /Name/;
- альтернативные наименования группы, встречающиеся в отчетах по анализу угроз /Associated Groups/, включая их описания /Description/;
- описание группы нарушителей /Description/;
- использованные техники /Techniques Used/, включая для каждой техники область деятельности /PRE-ATT&CK, Enterprise, Mobile/, идентификатор техники /ID/, наименование техники /Name/, описание использования и ссылку на источник информации /Use/;
- программное обеспечение для реализации угроз /Software/, включая для каждого программного обеспечения идентификатор программного обеспечения /ID/, наименование программного обеспечения /Name/, ссылки на информацию о программном обеспечении и /или/ об его использовании /References/, наименование техник, при выполнении которых использовалось программное обеспечение /Techniques/;
- перечень источников информации, на которые есть ссылки в описании группы нарушителей /References/.

4

Программное обеспечение для реализации угроз /Software/

Представление программного обеспечения для реализации угроз /Software/ в базе знаний MITRE ATT&CK™ включает:

- идентификатор программного обеспечения /ID/;
- наименование программного обеспечения /Name/;
- тип программного обеспечения /Type/;
- инструментальное средство /Tool/ или вредоносное программное обеспечение /Malware/;
- альтернативные наименования программного обеспечения /Associated Software/;
- описание программного обеспечения /Description/;
- техники, для которых может использоваться программное обеспечение /Techniques Used/, включая для каждой техники: область деятельности /PRE-ATT&CK, Enterprise, Mobile/, идентификатор техники /ID/, наименование техники /Name/, описание использования программного обеспечения для реализации техники и ссылку на источник информации /Use/;
- группы нарушителей /Groups/, которые используют данное программное обеспечение;
- перечень источников информации, на которые есть ссылки в описании программного обеспечения /References/.

На момент написания настоящей статьи в базе знаний MITRE ATT&CK™ была размещена информация о

40

тактиках

485

техниках

91


группе нарушителей

397

наименованиях программного обеспечения для реализации угроз БИ

(продолжение следует)

Список литературы

- 1** Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 № 28608 // СПС КонсультантПлюс.
- 2** Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», зарегистрирован в Минюсте России 26.03.2018 № 50524 // СПС КонсультантПлюс.
- 3** Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas MITRE ATT&CK™: Design and Philosophy, July 2018// MITRE ATT&CK™  /дата обращения: 02.09.2019/.

Материал поступил для публикации 09.09.2019.