УДК 004.056.53

ВОПРОСЫ ОПИСАНИЯ ВОЗМОЖНЫХ СЦЕНАРИЕВ УГРОЗ ПРИ РАЗРАБОТКЕ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Иван Евгеньевич Дорошенко
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (996)377-34-08, e-mail: vaas2202@gmail.com

Мидат Олегович Максудов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (909)529-82-33, e-mail: zaki.anarchist@gmail.com

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

В статье рассмотрен вопрос описания сценариев угроз безопасности информации при разработке модели угроз по методике оценки угроз безопасности информации, вопрос использования зарубежных ресурсов при описании сценария угроз безопасности и вопрос совмещения зарубежных и отечественных ресурсов при описании сценариев угроз безопасности информации.

Ключевые слова: методика оценки угроз безопасности, модель угроз, тактики и техники угроз

QUESTIONS OF DESCRIBING POSSIBLE THREAT SCENARIOS IN DEVELOPMENT OF THREAT MODELS TO INFORMATION SECURITY

Ivan E. Doroshenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (996)377-34-08, e-mail: vaas2202@gmail.com

Midat M. Maxudov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (909)529-82-33, e-mail: zaki.anarchist@gmail.com

Valentine V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

The article considers the question of describing possible threats scenarios by developing models of threats to information security by developing a threat model based on the method of assessing threats to information security, the issue of using foreign resources in describing a scenario of security threats, and the issue of combining foreign and domestic resources when describing scenarios of threats to information security.

Keywords: security threats assessing methodology, threats model, tactics, technics and procedures

В феврале 2021 года ФСТЭК утвердила методику оценки угроз безопасности информации, в которой, помимо прочих, содержится требование к описанию возможных сценариев угроз [1].

В данный момент крайне сложно составить подобный перечень сценариев угроз безопасности информации [2]. Это напрямую связано с техниками атак, так как сценариев может быть множество, а техник в ТТУ от ФСТЭК всего 145, а в TTP от MITRE ATT&CK – 200 [7]. Также это связано с неоднозначной правовой базой при описании сценариев угроз безопасности информации [4].

Требование к описанию возможных сценариев угроз трудноосуществимо ввиду следующих факторов:

– отсутствуют средства автоматизации, позволяющие составить перечень возможных сценариев угроз, ввиду чего проблематично составить модель угроз;

– необходимо досконально знать все методы злоумышленника [3];

– крайне сложно подобрать средства защиты, ввиду отсутствия перечня сценариев угроз безопасности информации [5].

Описание возможных сценариев угроз бессмысленно на данный момент, ввиду вышеупомянутых факторов и бесконечного множества сценариев [10]. Однако, вместо описания сценариев и последующего создания средств противодействия им, возможно использование техник и тактик угроз, которых существует конечное множество, что позволяет описать модель угроз, а также составить модель нарушителя. Также возможно подобрать средства защиты информации, так как техники и тактики угроз известны и систематизированы [9].

Проект MITRE ATT&CK имеет матрицу тактик и техник атак, список APT-групп с присущими ими TTP (tactics, technics and procedures), список защитных мер, которые связаны с нейтрализуемыми тактиками и техниками [8]. Многие производители средств защиты внутри своих продуктов не только делают отсылки на TTP, но и предоставляют своим заказчикам матрицы соответствия своих решений защитным мерам по ATT&CK. К примеру, CISCO предоставляет следующую матрицу соответствия, что помогает при построении модели угроз (рис. 1).

С другой стороны, не только зарубежные компании пользуются базой MITRE ATT&CK, но и лицензиат ФСТЭК, компания Positive Technologies (рис. 2). Они не пытаются описывать сценарии угроз или же сопоставить тактики угроз со сценариями, а лишь указывают, какими техниками пользуются злоумышленники [13].

ФСТЭК также озаботился описанием тактик и техник атак и адаптировал TTP от MITRE ATT&CK, дав название ТТУ (тактики и техники угроз). По сути это переписанный TTP со множеством изменений, совмещений и разделений [7]. Если попробовать сопоставить ТТУ от ФСТЭК и TTP от MITRE, окажется, что 10 тактик ФСТЭК – это объединение нескольких тактик MITRE. С техниками дела обстоят хуже, они сильно перемешаны. Например, техника T1.7 у ФСТЭК описывает сбор данных, предоставляемых DNS-сервисами. В ATT&CK это уже две техники – T1590.002 (сбор сетевой информации о цели – DNS) и T1596.001 (поиск в открытых базах данных – DNS/Passive DNS) [11].

Рис. 1. Матрица соответствия решений защитным мерам по CISCO

ID	Название	Описание
Execution		
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Группа Calypso использует cmd.exe для исполнения команд в системе
Persistence		
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	BAT-скрипт Install в составе ВПО группы Calypso позволяет закрепиться в системе через ключ автозагрузки реестра системы: "HKCU\Software\Microsoft\Windows\CurrentVersion\Run key"

Рис. 2. Тактики из MITRE ATT&CK группировки Calypso

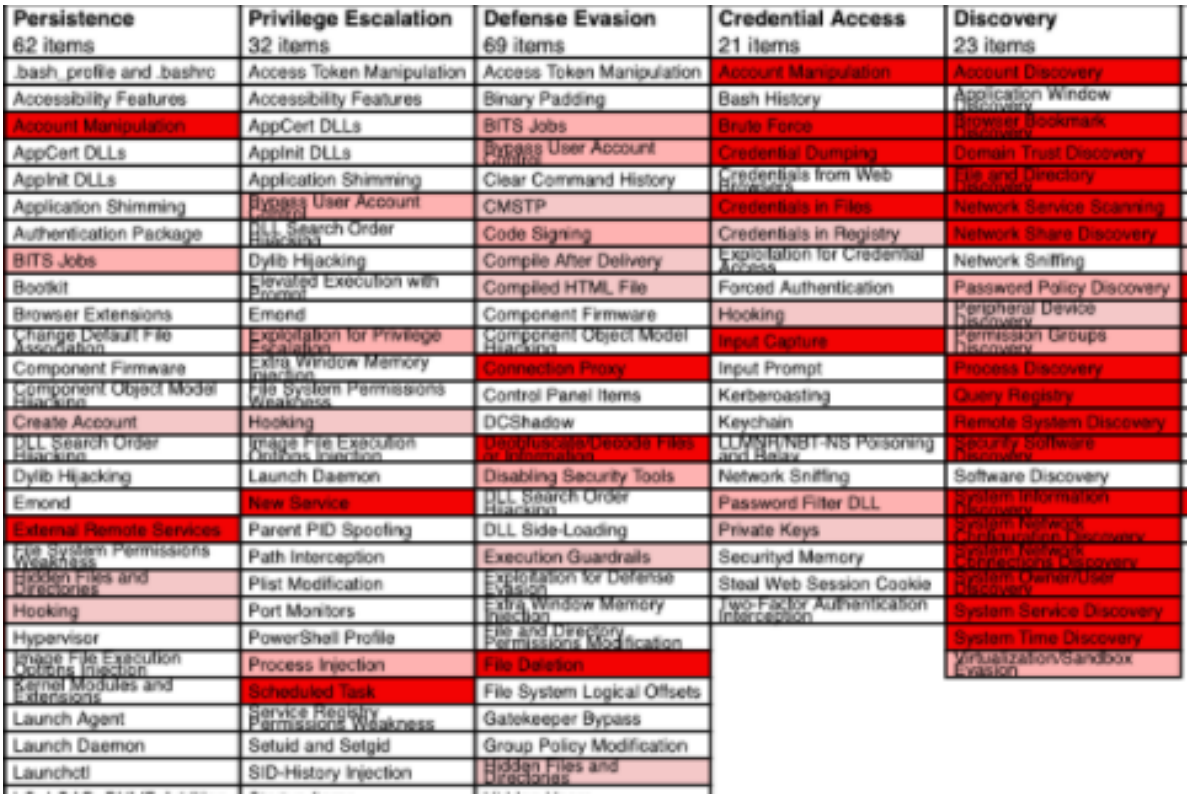
Если бы ТТУ ФСТЭК были бы простым переводом TTP, тогда было бы возможно задействовать инструменты, базирующиеся на MITRE ATT&CK, например, attack navigator, облегчающий работу с тактиками и техниками, позволяющий описывать сценарии атак, описывать сценарии, не закрывающиеся текущими методами защиты, проводить тесты средств защиты [10].

На данный момент крайне сложно, опираясь на ТТУ ФСТЭК, написать аналитику и модель угроз безопасности информации, так как все отечественные и зарубежные вендоры работают только с TTP от MITRE ATT&CK. Сама по себе ТТУ от ФСТЭК представляет собой таблицу, написанную в Microsoft Excel, в то время как TTP – это централизованная база данных с автоматизацией, IPI, позволяющий создавать свои продукты на его основе [9].

Предположим, что регулятор создаст сервис с автоматизацией, IPI и поддержкой российских продуктов. Тогда отечественным производителям решений понадобится адаптировать свои продукты как на отечественный рынок, опираясь на ТТУ ФСТЭК, так и на зарубежный, работая с TTP от MITRE ATT&CK. Или же сопоставить ТТУ от ФСТЭК и TTP от MITRE таким образом, чтобы была возможность создать средство автоматизации на базе ТТУ, но содержащее актуальную информацию о киберпреступниках, их техниках, тактиках и угрозах, как например сервис CARET, построенный на ATT&CK, позволяющий при вводе в него набора техник выдать возможные группировки киберпреступников, стоящих за атакой [12].

Однако, в таком случае остаются открытыми вопросы, как именно пользоваться результатами работы зарубежных компаний, опирающихся именно на MITTRE ATT&CK, кто именно будет сопоставлять TTP с ТТУ, и как будет происходить обновление баз данных ТТУ в таком случае? Также остается открытым еще один вопрос, как быть с киберпреступниками или же их техниками и методами, которые уже попали в базу данных TTP от MITTRE ATT&CK, но еще неизвестны для ТТУ от ФСТЭК. К примеру, сервис CARET на базе ATT&CK способен при вводе в него набора выявленных техник выдать перечень группировок, подходящих по определенным параметрам. И наоборот. Если в процессе моделирования нарушителей определены актуальные, сервис CARET поможет определить, какие техники используются, сокращая при этом время на анализ (рис. 3) [12].

На данный момент выполнить требование к описанию возможных сценариев угроз по методике оценки угроз безопасности информации крайне сложно в полной мере. Вместо описания сценариев и последующего создания средств противодействия им возможно использование техник и тактик угроз, однако использование ТТУ от ФСТЭК на данный момент также создает большие трудности. Согласно методике оценки угроз безопасности информации, ФСТЭК разрешает использование зарубежных баз данных, потому вместо ТТУ от ФСТЭК возможно использование проекта MITRE ATT&CK с его TTP, позволяющего подробно описать тактики угроз, описать модель нарушителя, а также подобрать соответствующие средства защиты информации.



Persistence 62 items	Privilege Escalation 32 items	Defense Evasion 69 items	Credential Access 21 items	Discovery 23 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery
Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery
AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery
AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery
Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning
Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery
BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing
Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery
Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery
Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery
Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery
Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry
Create Account	Hooking	DCShadow	Keychain	Remote System Discovery
DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery
Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery
Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery
External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery
File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery
Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery
Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery
Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery
Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion
Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets		
Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass		
Launch Daemon	Setuid and Setgid	Group Policy Modification		
Launchctl	SID-History Injection	Hidden Files and Directories		

Рис. 3. Описание части техник, используемых одним из нарушителей по ATT&CK

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Методика определения угроз безопасности информации: методич. материал – Москва, ФСТЭК, 2021. – 83 с.

2. Лесько С.А. Модели и сценарии реализации угроз для интернет-ресурсов. – 2020. – [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=44514882 (дата обращения: 17.04.2021).

3. Ганздюк Т. М., Поршнев С.В. Анализ угроз безопасности информации. возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации. – 2018. – [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=37142357 (дата обращения: 17.04.2021).

4. Размыслов Е.В., Якунин А. Г. Анализ нормативно-правовой базы в области оценки угроз безопасности информации. – 2020. – [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=44682896 (дата обращения: 17.04.2021).

5. Калач А.В., Пеев Д.Н., Зыбин Д.Г. Анализ и оценка современных угроз безопасности информации. – 2017. – [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=37158195 (дата обращения: 17.04.2021).

6. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя. – 2017. – [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=27537410 (дата обращения: 17.04.2021).

7. Моделирование угроз по ФСТЭК [Электронный ресурс]. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/350566.php (дата обращения: 17.04.2021).

8. Enterprise Matrix [Электронный ресурс]. – URL: https://attack.mitre.org/matrices/ enterprise/ (дата обращения: 17.04.2021).

9. Методика оценки угроз ФСТЭК: первая попытка применить ее на практике [Электронный ресурс]. – URL: https://www.securitylab.ru/blog/personal/ Business_without_danger/ 350559.php (дата обращения: 17.04.2021).

10. Краткий обзор новой методики оценки угроз ФСТЭК [Электронный ресурс]. URL: https://bis-expert.ru/blog/660/72838 (дата обращения: 17.04.2021).

11. Enterprise tactics [Электронный ресурс]. – URL: https://attack.mitre.org/tactics/ enterprise/ (дата обращения: 17.04.2021).

12. Caret analytics [Электронный ресурс]. URL: https://mitre-attack.github.io/caret/#/ (дата обращения: 17.04.2021).

13. Calypso APT: изучаем новую группировку, атакующую госучреждения [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/calypso-apt-2019/ (дата обращения: 17.04.2021).