SiT Review 2025,
Shumen Institute of Technology
ISSN 2738-7593
NACID ID №: 4112

Концептуален подход за създаване на сценарии за киберучения, базиран на основни модели за анализ на кибератаки и пробиви в сигурността.

Димитър Иванов Николов

Висше военноморско училище „Н. Й. Вапцаров“ – Варна

E-mail: d.nikolov@naval-acad.bg

Абстракт: Настоящата статия разглежда значението и методологията за създаване на реалистични сценарии за киберучения, фокусирайки се върху ефективната подготовка на специалисти по киберсигурност. Основната цел е да се покаже как интегрираното използване на аналитичните модели Cyber Kill Chain, Diamond Model of Intrusion Analysis и MITRE ATT&CK позволява постигането на максимален реализъм при симулирането на сложни кибернетични атаки. Представен е детайлен хипотетичен сценарий, базиран на реален инцидент – сблъсъка на кораба „Дали“ с моста Франсис Скот в Балтимор, САЩ, през март 2024 г. Анализирани са възможностите, при които подобен инцидент би могъл да бъде резултат от кибератака, включваща специфични техники като zero-day експлойти, spear-phishing и атаки срещу индустриални контролни системи. Използваните аналитични модели осигуряват задълбочено разбиране на структурите и процесите при кибератаките, като едновременно с това подобряват способностите за детекция, реакция и комуникация на екипите по сигурност.

1. Въведение

В съвременния свят на нарастващи киберзаплахи и динамично променящи се методи за атака, подготовката на специалисти по киберсигурност се превръща в критичен компонент за защитата на цифровите активи. Киберученията играят ключова роля в този процес, като предоставят възможност за тестване на уменията, подобряване на реакциите при инциденти и валидиране на защитните стратегии в контролирана среда. Те позволяват на участниците – както от защитната, така и от атакуващата страна – да разберат по-добре методите, използвани от злонамерените актьори, и да прилагат ефективни контрамерки.

Киберученията[1] представляват структурирани тренировки, които симулират реални кибератаки с цел оценка и подобряване на защитните механизми в една организация. Тези учения не само развиват технически умения, но и изграждат критично мислене, бързо вземане на решения и ефективна комуникация в кризисни ситуации. В условията на нарастващи заплахи, свързани с държавно подкрепяни APT (Advanced Persistent Threat) групи, финансови киберпрестъпления и атаки срещу критична инфраструктура, обучените киберспециалисти се превръщат в първа линия на защита. Една от основните причини за провеждането на киберучения е способността им да моделират сложни заплахи и да предоставят реалистична среда за тяхното проучване и неутрализиране. Традиционните

ISSN 2738-7593
NACID ID №: 4112

методи за обучение, базирани на теоретични знания, не могат да подготвят специалистите за реалните сценарии, които включват многослойни атаки, комбиниращи различни техники и тактики. Практическите симулации позволяват на защитните екипи да изпробват методите си за детекция, реакция и възстановяване в динамична и интерактивна среда.

За да бъде едно киберучение ефективно, сценарият му трябва да бъде възможно най-близък до реалните тактики, техники и процедури, използвани от атакуващите. Това изисква интеграция на добре разработени аналитични модели като Cyber Kill Chain, Diamond Model и MITRE ATT&CK. Тези методологии предоставят структурирана рамка за анализ и репликиране на атаките, което позволява на обучаемите да разберат и идентифицират различните етапи от атаката и да прилагат съответните защитни мерки.

При Red Team ученията, атакуващите трябва да следват сценарии, базирани на реални APT техники, използвайки разнообразни инструменти като zero-day експлойти, spear-phishing, компрометиране на C2 инфраструктура и други средства за установяване на дълготрайно присъствие в мрежата. От своя страна, Blue Team трябва да реагира, анализира логовете, идентифицира индикаторите за компрометиране (IoCs) и прилага ефективни тактики за детекция и неутрализиране на заплахата.

Използването на реалистични сценарии [2] е особено важно при обучението на екипи, работещи в критична инфраструктура, където компрометирането на системи може да доведе до сериозни последици – например прекъсване на енергийни мрежи, транспортни инциденти или финансови загуби. Именно затова киберученията трябва да се базират на съществуващи заплахови профили и да включват техники, използвани от известни APT групи.

За да се осигури ефективна рамка за анализ и подготовка на киберучения, настоящата статия ще използва три основни методологии. Първата е Cyber Kill Chain[3]. Този модел, разработен от Lockheed Martin, структурира кибератаките като последователност от седем основни фази: Reconnaissance (разузнаване), Weaponization (създаване на експлойт), Delivery (доставка на атаката), Exploitation (експлоатиране на уязвимости), Installation (инсталиране на зловреден код), Command & Control (C2) (създаване на комуникационен канал с атакуващите) и Actions on Objectives (осъществяване на крайната цел на атаката). Този модел е полезен за разбиране на хронологията на атака и идентифициране на критични точки за прекъсването ѝ.

Втората методология е Diamond Model of Intrusion Analysis – прилага релационен подход към анализа на злонамерени събития. Той разделя всяко събитие на четири основни компонента: Adversary (атакуващият), Infrastructure (използваните IP адреси, домейни и сървъри), Capability (инструментите, използвани в атаката, като зловреден софтуер и експлойти) и Victim (компрометираната система или организация). Този модел помага да

ISSN 2738-7593
NACID ID №: 4112

се разберат връзките между атакуващия и инфраструктурата, като позволява предсказване на бъдещи атаки.

Треата методология е MITRE ATT&CK – таксономия на тактиките и техниките, използвани от атакуващите в реални кампании. Включва детайлни описания на техниките, които хакерските групировки прилагат за компрометиране на системи, както и предложени начини за откриване и противодействие. MITRE ATT&CK е особено полезен за идентифициране на тактическите и техническите детайли на атаките, което позволява на защитните екипи да създават ефективни механизми за детекция и превенция.

2. Теоретична рамка за анализ на кибератаки

Три от най-използваните методологии в областта на киберсигурността са Cyber Kill Chain, Diamond Model of Intrusion Analysis и MITRE ATT&CK. Тези рамки предоставят стратегически и тактически инструменти за разбиране на хронологията на атаките, анализа на атакуващата инфраструктура и категоризацията на използваните техники. В тази секция ще бъдат разгледани фазите на всяка методология, възможностите за противодействие и начините, по които трите модела могат да се комбинират за изграждане на ефективна отбранителна стратегия.

Cyber Kill Chain [4] е модел, разработен от Lockheed Martin, който разграничава атаката в седем ключови етапа. Този модел предоставя методология за детекция и спиране на кибернападения чрез идентифициране на критични точки, в които атаката може да бъде неутрализирана.

Фаза	Описание на атаката	Тактики за противодействие
1. Разузнаване (Reconnaissance)	Атакуващият събира информация за жертвата чрез OSINT (Open Source Intelligence), сканира уязвими услуги, домейни, служебни имейли.	Инструменти за мониторинг на трафик (SIEM, IDS), интелигентен анализ на заплахи (Threat Intelligence), блокиране на подозрителни заявки.
2. Въоръжаване (Weaponization)	Създаване на злонамерен код, експлоит, макроси, документи с вграден злонамерен софтуер. Често атакуващият използва 0-day уязвимости.	Стриктни политики за изолирани среди (Sandboxing), анализ на зловреден код, ползийни и поведенческо откриване.
3. Доставка (Delivery)	Изпращане на зловреден софтуер чрез spear-phishing, компрометирани уебсайтове, USB устройства, drive-by	E-mail защита (DMARC, DKIM, SPF), контрол на прикачени файлове, Web Proxy филтриране, DLP системи.

ISSN 2738-7593
NACID ID №: 4112

	downloads.	
4. Експлоатация (Exploitation)	Използване на уязвимости за придобиване на достъп (например T1068 - Exploitation for Privilege Escalation).	Редовно прилагане на пачове, Endpoint Protection (EDR, XDR), принцип на най-малко привилегии.
5. Инсталация (Installation)	Установяване на backdoor, регистрация на зловредни услуги, създаване на нови потребители.	Мониторинг на регистъра (Sysmon, ELK stack), File Integrity Monitoring (FIM), анализ на необичайни процеси.
6. Контрол и управление (Command & Control - C2)	Атакуващият установява връзка с компрометираната система чрез криптирани канали (HTTPS, DNS tunneling, Cobalt Strike).	DNS анализ, Network Traffic Analysis (NTA), Firewall egress rules, YARA правила за зловреден трафик.
7. Действия по целите (Actions on Objectives)	Изпълнение на крайната цел – ексфилтрация, саботаж, криптиране на файлове (ransomware).	SIEM лог анализ, DLP, аномално засичане на файлови операции, Micro-Segmentation.

Diamond Model of Intrusion Analysis [5], разработен от Sergio Caltagirone, Andrew Pendergast и Christopher Betz, Diamond Model of Intrusion Analysis е аналитична рамка, която предоставя детайлен подход към разбирането на кибератаките чрез анализ на взаимоотношенията между основните компоненти на едно злонамерено събитие. Вместо да се разглеждат атаките линейно, както при Cyber Kill Chain, този модел прилага релационен анализ, при който всяко киберсъбитие се разглежда като четиричленна структура, включваща следните основни елементи: Adversary (Атакуващ), Infrastructure (Инфраструктура), Capability (Възможности) и Victim (Жертва).

Основната концепция на модела е, че атакуващият (Adversary) използва определени възможности (Capability) през инфраструктура (Infrastructure), за да компрометира конкретна жертва (Victim). Разкриването и анализът на тези взаимовръзки дава възможност за ефективно проследяване на заплахите, идентифициране на злонамерени актьори и корелация на атаки, дори когато отделните индикатори (IoCs) не са достатъчно ясни сами по себе си.

Компоненти на Diamond Model и тяхната роля:

1. Adversary (Атакуващ)

Този компонент представлява самия атакуващ субект, който може да бъде APT група (Advanced Persistent Threat), хакерска организация, държавно спонсорирана

ISSN 2738-7593
NACID ID №: 4112

кибершпионска група или престъпна мрежа. Анализирането на атакуващите включва оценка на техните мотиви, тактики и почерк (TTPs – Tactics, Techniques, and Procedures), което може да помогне за идентифициране на атакуващата група въз основа на исторически данни. Например, ако атаката включва целево фишинг нападение (Spear Phishing) и използва конкретни злонамерени скриптове, това може да насочи анализаторите към известна група като APT28 (Fancy Bear) или APT29 (Cozy Bear).

2. Infrastructure (Инфраструктура)

Инфраструктурата се състои от техническите ресурси, които атакуващият използва за извършване на атаката. Това включва C2 (Command & Control) сървъри, VPN услуги, Tor мрежи, компрометирани легитимни уебсайтове (watering hole), зловредни IP адреси, домейни и хостове.

Пример за инфраструктура:

Зловреден домейн: Атакуващите могат да използват домейни, които изглеждат като легитимни, напр. update-microsoft-security[.]com за разпространение на фишинг имейли.

C2 сървъри: Често се използват динамични DNS услуги за хостване на управляващи сървъри, например чрез duckdns.org или no-ip.com.

Заразен софтуер (watering hole атака): Атакуващият може да компрометира сайт, посещаван от целевата организация, и да зарази потребителите с JavaScript-или PowerShell-базиран експлойт.

3. Capability (Възможности)

Възможностите се отнасят до конкретните инструменти и техники, които атакуващият използва за осъществяване на пробива. Това могат да бъдат 0-day експлойти, зловреден софтуер (ransomware, троянски коне), PowerShell скриптове, техники за заобикаляне на защита (obfuscation, rootkits).

Примери за зловреден софтуер:

Mimikatz (Credential Dumping – T1003): Извлича идентификационни данни от паметта на Windows.

Cobalt Strike (Beacon C2 Communication – T1071): Платформа за симулирани атаки, използвана и от реални нападатели за C2 управление.

Emotet (Persistence through Scheduled Tasks – T1053): Автоматично презареждане на зловреден код при рестартиране на системата.

4. Victim (Жертва)

ISSN 2738-7593
NACID ID №: 4112

Жертвата може да бъде конкретна организация, инфраструктурен елемент (сървър, мрежа) или индивидуален потребител. Анализът на атакуваната система може да даде информация защо точно тази мишена е била избрана. Например, APT групи често атакуват финансови институции, критична инфраструктура (електроразпределителни мрежи, пристанища), правителствени агенции или медийни компании.

MITRE ATT&CK е таксономия[6], която организира и описва различни техники, използвани от атакуващите в реални инциденти. Моделът е разделен на тактики (Tactics), техники (Techniques) и под-техники (Sub-techniques).

Примерни техники от MITRE ATT&CK:

Persistence: T1543 – Create or Modify System Process (Използване на скриптове за автоматично стартиране).

Privilege Escalation: T1068 – Exploitation for Privilege Escalation (Използване на локални уязвимости).

Defense Evasion: T1036 – Masquerading (Изпълнение на зловреден процес под легитимно име).

Credential Access: T1003 – OS Credential Dumping (Използване на Mimikatz за извличане на пароли).

Комбиниране на Cyber Kill Chain, Diamond Model и MITRE ATT&CK [7]:

Cyber Kill Chain определя последователността на атаката.

Diamond Model анализира отношенията между атакуващите и инфраструктурата.

MITRE ATT&CK осигурява подробна категоризация на техниките за всяка фаза от атаката.

Пример за използване на моделите в анализ на атака:

Чрез Cyber Kill Chain се установява, че атаката е във фаза Delivery.

С помощта на Diamond Model се анализират използваните домейни и IP адреси.

Справка с MITRE ATT&CK показва, че методът на доставка е T1566.001 – Spearphishing Attachment.

Тази тристепенна методология осигурява пълна картина на атаката и позволява бързо и ефективно противодействие.

3.Създаване на реалистични сценарии за киберучения

Създаването на реалистични сценарии за киберучения е ключов компонент за ефективната подготовка на екипите по киберсигурност, включително Red Team (нападателите) и Blue

ISSN 2738-7593
NACID ID №: 4112

Team (защитниците). Реализмът в симулациите се постига чрез използване на доказани модели като Cyber Kill Chain, Diamond Model of Intrusion Analysis и MITRE ATT&CK, чрез специфична техническа информация за действителните средства, тактики и методи на атакуващите групи, използвани за анализ на реални пробиви в сигурността или реални инциденти причина за които би могла да е кибератака.

3.1. Създаване на реалистичен профил на APT група

За създаването на сценарии се дефинират основните компоненти на предполагаема [8] APT (Advanced Persistent Threat) група, която ще бъде емулирана в рамките на ученията. Основните елементи включват:

Adversary (Атакуващ): Избира се фиктивна или реална групировка, като се дефинира мотивът и финансовите възможности – например добре финансирана държавна група (напр. Sandworm Team, свързвана с руската ГРУ), известна с кампании като NotPetya, както и с атаки върху индустриални системи и критична инфраструктура. Профилът включва мотивацията на групата – икономически шпионаж, саботаж или кражба на платежни данни.

Capability (Възможности)

Групата се снабдява с реалистични инструменти като:

- **Zero-day експлойти**, които таргетират широко използван софтуер (например CVE-2024-XYZ срещу VPN инфраструктура).
- **Spear-phishing кампании** с персонализирани имейли, съдържащи зловредни прикачени файлове, които водят до изпълнение на код на целевите системи (напр. MITRE ATT&CK T1566.001 – Spearphishing Attachment).
- **Рансъмуер**, способен да криптира чувствителни данни, като Ryuk, LockerGoga или по-нови щамове, разпространяващи се през мрежата на жертвата след компрометиране на акаунти.

Тези инструменти се подбират с оглед на техния реализъм и честота на използване в реални APT кампании.

Infrastructure

Инфраструктурата на симулираната APT група включва:

- **Command & Control (C2) сървъри**, хоствани на VPS (Virtual Private Server), често наети от посредници, използващи легитимни хостинг доставчици (типично за Sandworm Team и други известни групировки). Например, C2 инфраструктурата може да използва TOR или DNS-тунелиране, за да маскира комуникациите си.

ISSN 2738-7593
NACID ID №: 4112

- **Компрометирани легитимни домейни и IP адреси**, които да минимизират възможността за идентификация от страна на защитните системи (например, „watering hole“ атаки с компрометирани легитимни сайтове, често ползвани от служители на атакуваната организация).

Тази инфраструктура се проектира с оглед на съществуващите техники и инфраструктурни подходи на реални APT групи като Sandworm Team.

Victim (Жертва)

Целта на атаката (жертвата) е организация, подбрана с оглед на значимостта и чувствителността на информацията, която обработва, както и доколко е близка до средата в която трябва да работят обучаемите. В рамките на сценария може да се използва организация с технологичен стек, характерен за индустриалната или финансова инфраструктура (например ICS/SCADA системи, ECDIS, PLC, NMEA протоколи), като например корабната индустрия или морската инфраструктура, по аналогия с хипотетичния сценарий със сблъсъка на кораба „Дали“ с моста Франсис Скот в Балтимор [9], САЩ. Тази цел е избрана поради комбинацията от ICS (индустриални контролни системи), OT (оперативни технологии) и IT инфраструктура, които са характерни за морския сектор и представляват комплексна, но реалистична цел за APT атака.

Изграждане на сценарий за ученето

За да се постигне максимален реализъм, сценарият следва да се изгради според следните стъпки и интегрирайки следните модели:

Cyber Kill Chain

Сценарият проследява атаката през всички фази на Cyber Kill Chain:

- **Reconnaissance** – събиране на OSINT (LinkedIn, DNS данни, WHOIS записи, Shodan сканиране на индустриални системи).
- **Weaponization и Delivery** – подготовка и изпращане на фишинг-атаки, заредени с експлойт кодове.
- **Exploitation и Installation** – използване на zero-day експлойти за получаване на първоначален достъп и инсталиране на рансъмуер или backdoor (напр. Cobalt Strike beacon).
- **Command & Control (C2)** – установяване на C2 комуникации чрез TOR и DNS-тунелиране.
- **Actions on Objectives** – реализиране на атака, целяща отказ на системи, ексфилтрация или криптиране на данни.

ISSN 2738-7593
NACID ID №: 4112

MITRE ATT&CK

Всеки етап от Kill Chain се свързва с конкретни техники от MITRE ATT&CK, например:

- Reconnaissance – T1595 (Active Scanning), T1087 (Account Discovery).
- Delivery – T1566 (Spearphishing).
- Exploitation – T1203 (Exploitation for Client Execution).
- Installation – T1543 (Create or Modify System Process).
- C2 – T1071 (Application Layer Protocol).
- Actions on Objectives – T0813 (PLC манипулации).

Diamond Model

Всяка от фазите от Kill Chain-а допълнително се анализира чрез Diamond Model, където всяко събитие се разбива на четири компонента:

- Adversary (Sandworm, с известни мотиви и методи).
- Infrastructure (конкретни IP-та, домейни и C2).
- Capability (използваните инструменти и експлойти – рансъмуер и zero-day).
- Victim (засегнатите сървъри и инфраструктура).

Очаквани резултати от симулациите

В резултат от интегрирането на тези модели и реализирането на подобен сценарий, се очакват следните практически ползи:

- **Подобряване на детекционните способности** на защитните екипи чрез създаване на правила и сигнатури, базирани на реалистичните TTPs (MITRE ATT&CK).
- **Оптимизиране на реакцията** на Blue Team чрез по-добро разбиране и идентифициране на фазите на атаката (Cyber Kill Chain).
- Подобряване на **оперативната съвместимост** между Red Team и Blue Team, благодарение на единната терминология и стандартизирания подход (Diamond Model), улесняващи комуникацията и обмена на информация.

4. Анализ на инцидент с цел подготовка на сценарий за киберучение: Хипотетична кибератака срещу кораба „Дали“

На 26-и март 2024 година корабът „Дали“ претърпява тежък инцидент [10], сблъсквайки се с моста Франсис Скот в Балтимор, САЩ. Според официалната информация, корабът е загубил контрол над управлението си на около три дължини от моста вследствие на поредица от откази на електрическата система. В резултат на сблъсъка възникват сериозни щети по конструкцията на моста и корпуса на кораба, като са регистрирани и жертви. Макар към момента да няма категорични доказателства за намеса чрез кибератака,

ISSN 2738-7593
NACID ID №: 4112

разглеждането на хипотетична такава е оправдано поради зачестилите заплахи срещу морската критична инфраструктура.

В рамките на този анализ ще приложим моделите Cyber Kill Chain, Diamond Model of Intrusion Analysis и MITRE ATT&CK, за да разгледаме как една кибератака би могла да доведе до подобен инцидент и да очертаем потенциалните методи и тактики, използвани от хипотетична Advanced Persistent Threat (APT) група.

Cyber Kill Chain – хипотетично развитие на атаката срещу кораба „Дали“

1. Reconnaissance (Разузнаване)

Атаката започва с подробно разузнаване на техническите и оперативни системи на кораба. Нападателите събират OSINT информация за корабния оператор, идентифицират използваните навигационни системи (ECDIS), комуникационните протоколи (NMEA), както и потенциалните точки за проникване (имейл сървъри, публично достъпни портове). Могат да се използват техники като Active Scanning (MITRE ATT&CK T1595) и Account Discovery (T1087), за да се идентифицират валидни акаунти и инфраструктурни компоненти, подходящи за последващо компрометиране.

Weaponization (Въоръжаване) – Изработва се зловреден софтуер или zero-day експлойт, специализиран за индустриалните системи на кораба, като вероятна цел е компрометирането на електронната навигационна система (ECDIS), което би довело до загуба на навигационни данни или пълен контрол.

Delivery (Доставка) – Използвайки персонализирани spear-phishing атаки (T1566.001), нападателите могат да доставят зловредния софтуер до системите на кораба чрез компрометиран служителски акаунт или инфектиран USB носител. Тази фаза е критична, тъй като позволява директен достъп до вътрешната корабна мрежа.

Exploitation (Експлоатация) – Използва се конкретен експлойт (например MITRE ATT&CK T1203 – Exploitation for Client Execution или T1210 – Exploitation of Remote Services), насочен срещу ECDIS системата или друг компонент, комуникиращ чрез NMEA протокола. Това може да доведе до първоначално компрометиране на навигационните системи, което от своя страна отваря врата за по-нататъшна експлоатация.

Installation (Инсталиране) – След успешното проникване атакуващите имплантират постоянен backdoor (например чрез T1543 – Create or Modify System Process). Това позволява дългосрочно присъствие в корабната инфраструктура и възможност за отдалечен достъп до системите по всяко време.

Command and Control (C2) – Установява се криптирана комуникация с контролни сървъри чрез DNS тунелиране или TOR мрежа (например T1071 – Application Layer Protocol). Това

ISSN 2738-7593
NACID ID №: 4112

позволява на нападателя дискретно да поддържа контрол над корабните системи и да осъществява комуникация, която е трудна за идентификация.

Actions on Objectives (Действия по целите) – В последната фаза нападателите изпълняват своите основни цели, в този случай – саботаж на PLC контролери (T0813 – Denial of Control), причиняващи отказ на електрическите и навигационни системи, което води до загубата на контрол и крайния сблъсък на кораба с инфраструктурен обект като моста Франсис Скот.

Diamond Model of Intrusion Analysis – анализ на атаката

Чрез използване на Diamond Model е възможно да се определи по-подробен контекст и взаимовръзки на инцидента:

Adversary (Атакуващ) – Вероятният нападател е добре финансирана държавна APT група, например Sandworm Team, свързана с руския GRU, с установен интерес към атаки върху критична инфраструктура, включително електроенергийни и навигационни системи.

Infrastructure (Инфраструктура) – Инфраструктурата за атаката включва компрометирани или наети сървъри, разположени в държави с трудна юрисдикция за проследяване, TOR възли за анонимизация, динамично генерирани домейни, както и легитимни компрометирани сайтове (watering hole), които са трудни за блокиране без съществено влияние върху нормалните операции на корабните системи.

Capability (Възможности) – Конкретните способности и инструменти включват zero-day експлойти, адаптирани към навигационните системи (ECDIS), зловреден софтуер за установяване на трайно присъствие, и рансъмуер за отказ на достъп и унищожаване на критична информация.

Victim (Жертва) – Корабът „Дали“ е целенасочено избран поради своята критична роля и специфичната комбинация от IT, OT и ICS системи, както и поради високата стойност и тежките последствия при успешно атакуване.

Спецификация на използваните техники от MITRE ATT&CK в сценария за атака срещу кораба „Дали“

При изграждането на реалистичен сценарий за киберучения и анализ на кибер инциденти, таксономията на MITRE ATT&CK предоставя необходимата техническа и аналитична дълбочина, която ясно дефинира използваните от атакуващите техники, тактики и процедури (TTPs). В конкретния хипотетичен сценарий, базиран на реалния инцидент с кораба „Дали“ и разглеждан като вероятна цел на кибератака, атакуващата група може да използва следните специфични техники, които са подробно описани в MITRE ATT&CK:

1. Reconnaissance (T1595 – Active Scanning и T1087 – Account Discovery)

ISSN 2738-7593
NACID ID №: 4112

Във фазата на разузнаване атакуващите извършват активни сканирания (Active Scanning - T1595) на корабната инфраструктура с цел да идентифицират публично достъпни интерфейси и услуги, потенциални уязвимости в ICS/SCADA системите и навигационните устройства (ECDIS, NMEA). Същевременно се прилага и Account Discovery (T1087), за да бъдат идентифицирани служебни имейли и акаунти на екипажа, което ще позволи по-късно да бъдат изпратени целеви фишинг имейли.

Техниката Active Scanning включва използване на публични инструменти като Shodan, Nmap и Masscan, които позволяват ефективно идентифициране на уязвими устройства и отворени портове. Допълнително могат да се използват техники за събиране на OSINT информация за служителите на корабната компания чрез социални мрежи и професионални платформи като LinkedIn.

Delivery – Доставка на зловреден код (T1566.001 – Spearphishing Attachment)

На този етап атакуващите изпращат целеви имейли, съдържащи заразени прикачени файлове, които са специално подготвени за компрометиране на целевата система (например офис служител или капитански мостик). В прикачените файлове може да бъде внедрен зловреден макрос, скрипт или експлойт, специализиран за софтуера, използван от корабната инфраструктура (ECDIS).Експлоатация и инсталиране (Exploitation & Installation)

T1203 – Exploitation for Client Execution

Атакуващите използват експлойт на клиентско приложение (например специфична версия на навигационната система ECDIS или NMEA интерфейса), позволяващ изпълнението на неоторизиран код. Този тип атака е често използвана в кампании срещу индустриални системи поради относително ниската осведоменост и слаб контрол на корабната информационна инфраструктура.

T1059 – Command and Scripting Interpreter

При успешна експлоатация атакуващите имплантират специфичен зловреден код (троянец или backdoor), който може да използва легитимни скриптови езици като PowerShell, Python или Bash, за да остане незабелязан за стандартните инструменти за сигурност. Това осигурява възможност за по-дългосрочна и по-дълбока компрометация.

T1543 – Create or Modify System Process

След успешната инсталация зловреднният софтуер е настроен да стартира автоматично чрез модифициране на системни процеси или добавяне на планирани задачи (Scheduled Tasks), осигурявайки устойчивост на достъпа дори след рестартиране или опити за премахване.

Command and Control (T1071 – Application Layer Protocol)

ISSN 2738-7593
NACID ID №: 4112

За да избегнат детекция, нападателите използват комуникация през Application Layer Protocol (например DNS-тунелиране или TOR мрежа), осъществявайки криптирани комуникации с предварително дефиниран C2 сървър. Използването на DNS-тунелиране и TOR позволява на атакуващите да скриват трафика в нормален HTTPS трафик, затруднявайки идентификацията и анализа от страна на защитните екипи.

Actions on Objectives – Постигане на крайна цел

T0813 – Denial of Control (PLC attack)

На финалния етап от атаката злонамереният код влияе директно върху контролерите на програмируемата логика (PLC), управляващи навигационните и енергийни системи. Използването на специфични команди за атака срещу PLC или друга OT инфраструктура позволява атакуващите да предизвикат отказ на системите за управление на кораба, което довежда до неговата загуба на контрол.

T0880 – Data Destruction

С тази техника се цели унищожаване на важни системни данни или конфигурационни файлове на корабните навигационни системи, което пряко води до нарушаване на тяхната нормална работа и гарантира, че корабът няма да може да възстанови нормалното си функциониране навреме, предотвратявайки своевременната реакция от страна на екипажа.

Синергичен ефект от комбинирането на моделите Cyber Kill Chain, Diamond Model и MITRE ATT&CK в сценария:

Използвайки интегриран подход[11], Red и Blue екипите получават яснота за това, на кой етап от атаката се намират (Cyber Kill Chain), кой и с какви ресурси е извършил атаката (Diamond Model) и кои конкретни техники са използвани (MITRE ATT&CK). Тази комбинация осигурява:

- Подобрена способност за ранно засичане на зловредна активност и откриване на конкретни индикатори за компрометиране (IoCs);
- Оптимизиране на бързината и точността на реакция на Blue Team, базирана на ясни и подробни правила за противодействие;
- Ефективна комуникация и координация между Red и Blue Team, базирана на единна терминология и стандартизирана методология за анализ.
- Очаквани резултати и практически ползи от анализа и симулацията

Този подход и детайлен сценарий ще позволи:

- Подобряване на способностите за ранна детекция и превенция – чрез разпознаване на специфични IoCs (IP адреси, домейни, техники за обфускация).

ISSN 2738-7593
NACID ID №: 4112

- Оптимизиране на реакцията на защитните екипи – чрез ясно разпознаване на фазите на атаката и бърза идентификация на критичните точки за контрадействия.
- Изграждане на оперативна съвместимост – между Red и Blue Teams, като се използва единна терминология и съвместна тактическа рамка (Kill Chain, Diamond, ATT&CK).

Заключение

Киберученията са критичен инструмент за подготовката на специалисти по киберсигурност, позволявайки им да тестват и подобряват защитните си способности в среда, максимално близка до реалните условия. Анализираният подход за създаване на реалистични сценарии демонстрира значимостта на използването на утвърдени методологии като Cyber Kill Chain, Diamond Model of Intrusion Analysis и MITRE ATT&CK. Тези модели осигуряват не само структурирана рамка за подробно изучаване на атаките, но и възможности за ефективна емулация на действията на реални APT групи. Използваният хипотетичен сценарий за инцидента с кораба „Дали“ ясно илюстрира практическото приложение на аналитичните модели в реалистична оперативна среда. Чрез комбинация от фазите на Cyber Kill Chain, релационния анализ от Diamond Model и детайлната таксономия на MITRE ATT&CK, бе демонстрирано как една комплексна кибератака може да бъде декомпозирана, разбрана и съответно ефективно контрирана. Включването на специфични технически елементи като zero-day експлойти, Spearphishing атаки, DNS тунелиране и зловреден код за атаки срещу ICS/SCADA системи добави допълнителен реализъм и техническа прецизност на сценария.Практическите ползи от интегрирания подход са особено важни. На първо място, подобрява се способността за навременно идентифициране на индикатори за компрометиране (IoCs) и ранно разпознаване на заплахите. Второ, оптимизира се реакцията на защитните екипи, които могат да действат по-бързо и точно в условия на реални атаки, благодарение на добре отработените процедури и сценарии. Трето, изгражда се оперативна съвместимост между Red и Blue Teams, което е от съществено значение за адекватна защита на критичната инфраструктура.

В обобщение, интегрираният подход за създаване на реалистични сценарии за киберучения, базиран на комбинация от методологиите Cyber Kill Chain, Diamond Model и MITRE ATT&CK, предоставя мощно средство за обучение, анализ и подготовка на специалистите по киберсигурност. Този подход позволява на организациите не само да разберат в дълбочина текущите заплахи, но и да изградят устойчивост срещу бъдещи сложни кибератаки, насочени към критични сектори като морската индустрия.

Литература:

1 Russo, E., Ribaudo, M., Orlich, A., Longo, G., & Armando, A. (2023). Cyber range and cyber defense exercises: Gamification meets university students. In Proceedings of the 2nd

ISSN 2738-7593
NACID ID №: 4112

International Workshop on Gamification in Software Development, Verification, and Validation (Gamify 2023) (pp. 29–37). Association for Computing Machinery. https://doi.org/10.1145/3617553.3617888

2 Holm, H., & Sommestad, T. (2025). Realistic and balanced automated threat emulation. Computers & Security, 151, 104351. https://doi.org/10.1016/j.cose.2025.104351

3. Ahmed, Y., Asyhari, A. T., & Rahman, M. A. (2021). A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. Computers, Materials and Continua, 67(2), 2497-2513. https://doi.org/10.32604/cmc.2021.014223

4. Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In J. Abawajy, S. Mukherjea, S. Thampi, & A. Ruiz-Martínez (Eds.), Security in computing and communications. SSCC 2015. Communications in Computer and Information Science (Vol. 536). Springer, Cham. https://doi.org/10.1007/978-3-319-22915-7_40

5. Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis. Threat Connect, 298(0704), 1-61.

6. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. In Technical report. The MITRE Corporation.

7. Naik, N., Jenkins, P., Grace, P., & Song, J. (2022, October). Comparing attack models for it systems: Lockheed martin's cyber kill chain, mitre att&ck framework and diamond model. In 2022 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-7). IEEE.

8. Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing, 14(7), 9355-9381.

9. Weiss, J. (2024, April 10). Could the Dali container ship incident have been a control system cyberattack? Control Global. https://www.controlglobal.com/blogs/unfettered/article/55017186/could-the-dali-container-ship-incident-have-been-a-control-system-cyberattack

10. National Transportation Safety Board. (2024, May 14). Contact of containership Dali with the Francis Scott Key Bridge and subsequent bridge collapse: Marine investigation preliminary report (Report No. DCA24MM031). https://www.ntsb.gov/investigations/Documents/DCA24MM031_PreliminaryReport%203.pdf

11.Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. Electronics, 13(19), 3867. https://doi.org/10.3390/electronics13193867