Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Життєвий цикл кіберзброї

У кіберзброї є свій власний життєвий цикл.

ЖЦ - це процес, який починається з початкової фази, коли кіберзброя є лише концепцією чи ідеєю, і переходить до кінцевої фази, коли кіберзброя існує та застосовується. Практично це відповідає компоненту “Виконання операції” розглянутої моделі.

Можна виділити такі фази життєвого циклу кіберзброї:

Етап I - Визначення проекту: на цьому етапі поняття кіберзброї визначається як зі стратегічної, так і з управлінської точки зору. Тому створюється архітектура кіберзброї та визначається основна функціональність.

Етап II - Розвідка: на цій фазі проводиться дослідження цілі з метою виявлення можливих існуючих вразливостей, які можна використати, збираючи корисні дані та інформацію. Цей етап стосується вивчення та отримання якомога більше інформації про систему, обрану для атаки.

Кіберзброя

Етап III - Проектування: на цьому етапі описується конструкція кіберзброї. Детальні функціональні можливості, технічні характеристики, завдання та терміни для кожного модуля чи компонента перекладаються та представляються, використовуючи різні схеми, моделі та варіанти використання, які допоможуть інженерам зрозуміти, що і як вони повинні реалізувати у проекті.

Етап IV - Розробка: на цьому етапі інженери впровадять код кіберзброї, використовуючи різні мови програмування, технології, сценарії, а також варіанти використання та варіанти тестів, які будуть використовуватися на етапі тестування.

Етап V - Тестування: на цьому етапі інженери перевіряють функціональність за допомогою тестів, які визначено на попередньому етапі, готують тестове середовище, яке повинно бути відображенням якомога ближчим до основної частини чи компонента реального середовища, де буде запущена кіберзброя. Це необхідно для імітації реальної ситуації нападу і встановленню чи буде досягнуто бажаних цілей. Наприклад, хробак Stuxnet був добре протестований у близькому до реального об’єкту середовищі, тому мав найкращій результат.

Кіберзброя

Етап VI - Валідація: на цьому етапі результати з етапу V порівнюються з цілями та функціональними можливостями, визначеними на етапах I та III. Якщо результат цього порівняння позитивний, тоді кіберзброю можна підготувати до використання в цільовій системі, або повернутись до фаз III, IV та V, при негативних результатах перевірки.

Етап VII - Вторгнення та контроль: кіберзброю перевірено і вона готова до запуску за результатами попередніх етапів, тому на цьому етапі виконуються два процеси. Перший процес представляє фактичне вторгнення - кіберзброя потрапляє всередину цільової системи. Вторгнення може бути здійснено шляхом фізичного або віддаленого доступу до системи. Другим процесом є отримання контролю над системою для того, щоб контролювати її і вирішувати, коли настав момент для початку атаки.

Етап VIII - Атака: на цьому етапі атака розпочинається шляхом активації (віддалено чи ні, автоматично чи ні) найважливішої частини кіберзброї, корисного навантаження, яка продовжуватиме виконувати свою мету.

Кіберзброя

Етап IX - Технічне обслуговування: на цьому етапі відстежується дія кіберзброї, щоб переконатися в тому, що досягнуто бажаних ефектів. Якщо трапляються речі, що не відповідають плану, будуть вжиті заходи для вирішення проблеми та продовження атаки або безпосереднього переходу до фази X, коли шанс бути виявленим стає занадто великим.

Етап X - ексфільтрація: на цій фазі закінчується життєвий цикл кіберзброї, і кіберзброя вилучається із цільової системи. Три основні випадки ексфільтрації. У першому випадку відповідно до інтересів дійової особи видаляються будь-які сліди вторгнення та нападу на ціль. У другому випадку, можливо, немає сенсу видаляти сліди дій, оскільки цілі досягнуті, а точно ідентифікувати нападника в кіберпросторі неможливо. У третьому випадку дійова особа не видаляє свої сліди, щоб підкреслити свою присутність та дії. При проведенні цифрових криміналістичних дій з метою виявлення дійову особу кібератаки та впливу його дій час відіграє важливу роль, оскільки він може запропонувати детальну інформацію про процес створення, запуску, використання та зупинки дії кіберзброї. Кібератака української енергетичної установки, для якої було використано Black Energy, прикривалась знищенням слідів методом знищення ключових комп'ютерів. Однак експертам з питань безпеки вдалося визначити дійову особу - російський уряд.

https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

Кіберзброя

Кіберзброя — це комп’ютерна програма, створена та використана для зміни або пошкодження системи(компонента) з метою досягнення (військових) цілей проти супротивників всередині та/або за межами кіберпростору. Комп’ютерна програма може бути як програмним додатком, так і сценарієм, оскільки мови програмування та сценаріїв дозволяють керувати як даними, так і обладнанням, які виконують різні ролі. Вплив може бути обмежений цільовими системами або може поширюватися на інших, навіть на людський домен, змінюючи поведінку людей та організацій.

Структура кіберзброї є багаторівневою і має три складові: перший рівень - доступ, другий - транспорт, а третій - представлений корисним навантаженням.

Рівень доступу базується на вразливості, яку можна використати; це практично вмикач і вхід у систему для кіберзброї для досягнення цілей.
Таким доступом можуть бути:
1) Програмне забезпечення: вразливості (помилки), які не були виправлені, навіть якщо їх існування було відоме або невідоме.
2) Апаратне забезпечення: уразливості в проектуванні апаратного забезпечення або компонентів каналу.

Кіберзброя

3) Конфігурації: помилки під час встановлення, налаштування або оновлення системи.
4) Інше: головним чином пов’язане з людським фактором шляхом надання належного доступу іншому суб’єкту або надання доступу іншому суб’єкту, не знаючи, що система може стати вразливою.

Файли Едварда Сноудена та АНБ показують, що інсайдерська загроза є найбільшою загрозою, оскільки той, хто сильно пов’язаний із системою, може знайти найглибші та найбільш критичні вразливості або скористатися інформацією, яка повинна залишатись таємною всередині компанії чи установи.

Транспортний рівень представляє механізм доставки та розповсюдження програмних компонентів кіберзброї в атаковану систему. Транспорт може бути здійснений на:
a) рівні логіки або даних через веб-сайти, сертифікати, фішинг тощо;
b) фізичному рівні, де транспорт здійснюється за допомогою зовнішніх пристроїв, таких як компакт-диски, DVD-диски, USB-накопичувачі тощо.

Кіберзброя

Рівень корисного навантаження - це програмний додаток або сценарій, розроблений, створений або використаний для компрометації даних або системної цілі. Корисне навантаження може мати одну з наступних архітектур:
a) архітектура з одним модулем: це випадок простої єдиної цілі або функції, якої повинна досягти кіберзброя.
b) мультимодульна архітектура: це випадок складної цілі або декількох цілей або функцій, яких повинна досягти кіберзброя.

Можна визначити такі характеристики кіберзброї:
1) Конкретність цілі: кіберзброя спрямовано на конкретні цілі для досягнення бажаної мети. Stuxnet націлився на іранську уранову програму і напав на ядерну установку з Натанца, що "призвело до поломки центрифуг без будь-якого повідомлення чи видимих причин". За ціллю та завданнями стоять мотивація та інтереси.
2) Нематеріальність: кіберзброя має логічну природу, яка робить її віртуальною та нематеріальною для фізичного світу.

Кіберзброя

3) Різноманітність знань: створюючи та використовуючи кіберзброю, потрібно мати різноманітні та глибокі знання в IT, а також інформацію про її цілі та завдання.
4) Менш коштовна: у багатьох випадках кіберзброя є дешевшою альтернативою звичайній зброї, що має “мінімальні витрати на життя та ресурси”.
5) Здатність до налаштувань: кіберзброя може мати один або декілька варіантів залежно від вразливостей, які вона використовує:
 a) Одиночна: це той випадок, коли лише один варіант кіберзброї створюється на основі наявної вразливості і потім використовується.
 b) Мульти: це той випадок, коли на основі існуючої вразливості створюється та використовується більше варіантів кіберзброї. Можливо, кіберзброя може мати більше варіантів залежно від цілі, цілей та місії.
6) Відсутність повторного використання: кіберзброя має чітко визначені функціональні можливості і після використання їх можна вважати викритими. У разі вжиття належних контрзаходів їх не можна використовувати таким самим чином знову. Однак, якщо не вжити контрзаходів, можна знову використовувати ту саму кіберзброю.

Кіберзброя

Критерії класифікації використання кіберзброї:

За призначенням:
а) Атакуюча: атакувати противника.
б) Захисна: для захисту від супротивника.
в) Багатоцільова: вважається, що існує клас кіберзброї, яку можна використовувати як для атакування, так і для оборони.

За використанням:
а) Одиночне: випадок, коли використовується лише одна кіберзброя.
б) Система: комбінація наступальної, оборонної або багатоцільової кіберзброї, яка розроблена і функціонує як цілісна система.

За складністю:
a) Дуже складна: у разі інвестування великих обсягів ресурсів у процес придбання або впровадження кіберзброї. Створюються та використовуються інноваційні та інтелектуальні методи та технології.
b) Мало складна: у випадку інвестування зменшеної кількості ресурсів у процес придбання або впровадження кіберзброї. Використовуються лише платформи та додатки з відкритим кодом, без інноваційних та інтелектуальних методів.

Кіберзброя

За областю дії:
a) Місцева: це той випадок, коли постраждала лише цільова система.
b) Регіональний: це той випадок, коли ефекти можна спостерігати в більшості систем в країні цільової системи.
в) Глобальний: це той випадок, коли на глобальному рівні постраждало більше систем.

У кіберпросторі важко говорити про кордони. Так мережевий хробак Stuxnet мав глобальний вплив, не зважаючи на те, що він був розроблений для місцевої дії.

Кіберзброя

Три кіберзброї: Stuxnet, Operation Orchard та Black Energy

Stuxnet була викрита в 2010 році білоруською компанією під назвою VirusBlockAda; Після тривалих розслідувань міжнародні експерти дійшли висновку, що цей мережевий хробак мав на меті реагувати на ядерну установку в Натанзі в Ірані та пошкодив близько 1000 центрифуг. Є думка експертів, що його створили та організували США та Ізраїль. Багатоцільова.

Operation Orchard була виявлена в 2007 році в Сирії; після розслідувань міжнародні експерти погодились, що ця кіберзброя використовувалась для нейтралізації сирійських радіолокаційних систем з метою знищення сирійського ядерного об'єкта в районі Дейр-ез-Зор повітряною атакою. Її створив та випробував Ізраїль. Одиночна.

Black Energy була виявлена в 2015 році в Україні; міжнародні експерти дійшли висновку, що вона використовувалась для націлювання на енергетичну установку в Івано-Франківській області, і багато міст на кілька годин залишалися без електропостачання, комп'ютери та телефонні лінії було виведено з ладу. Вона була створена та випробувана російською хакерською групою Sandworm Team. Багатоцільова.

Кіберзброя

Три кіберзброї: Stuxnet, Operation Orchard та Black Energy

Stuxnet
потужна технічна розробка: використано уразливість Windows, передові знання про ПЛК (програмовані логічні контролери) та системи Siemens, ядерні процеси та тестувався в дзеркальному середовищі.

Operation Orchard
потужна технічна розробка: використано передові та конкретні знання з питань радіоелектронної боротьби та протиповітряної оборони

Black Energy
Застосовано сильні технічні та соціальні інженерні навички: використання мережі та отримання доступу до систем ICS (інтегровані комп’ютерні рішення) та UPS, а також передові знання про ICS, енергетичні та електричні системи

Кіберзброя

Три кіберзброї: Stuxnet, Operation Orchard та Black Energy

Stuxnet
Використання — одиночне. Ознаки присутності знайдено у 2009 році, але сам хробак виявлено в червні 2010 року. Область дії: Глобальний: Індонезія, Індія, США та інші країни.

Operation Orchard
Використання — одиночне. Використовувався в 2007 році, але був підсадженим роком раніше. Область дії: Місцевий: Аль-Кабір у Сирії

Black Energy
Використання — системне: направлене на 3 системи розподілення. Використовувався 23 грудня 2015 р. Був швидко виявлений та проаналізований. Область дії: Регіональний: постраждала половина людей з Івано-Франківської області, Україна

Кіберзброя

Stuxnet

написана з поєднанням мов програмування високого та низького рівня: C/C++ та Assembler, з використанням Microsoft Visual Studio 2005 та Microsoft Visual Studio 2008. Для створення задіяно професійну команду інженерів, розробка тривала від півроку до одного року. Команда розробників мала великий обсяг знань та досвіду роботи з промисловими системами управління, найточнішими програмованими логічними контролерами, виробленими Siemens та використовуваними на ядерному комплексі в Натанці. Її відрізняло структурований та системний спосіб мислення та реалізації з метою відображення передової та складної мети до безлічі простих цілей та функцій, які слід виконати. Рівень знань, професіоналізм та інвестиції, що стоять за цією розробкою, виявляють характеристики для державних суб'єктів. З урахуванням сторін напруженості на той час у міжнародній політиці (розвитком ядерної програми в Ірані вкрай стурбованими були США та Ізраїль), саме тому деякі експертні думки свідчать про участь та співпрацю між такими державами, як США та Ізраїль.

Кіберзброя

Stuxnet
Вторгнення:
транспортний рівень - USB-накопичувач та локальна комп’ютерна мережа
рівень доступу - вразливості програмного забезпечення систем, що працюють під управлінням WinCC та спеціального програмного забезпечення Step 7 від SIMATIC, що дозволяє програмувати та контролювати ПЛК фізичних процесів.

Об’єкти та цілі характеризують рівень корисного навантаження. Багатомодульна архітектура містить два компоненти:
перший корисний вантаж - зміна швидкості обертання ядерних центрифуг, нанесення фізичних пошкоджень машинам;
другий корисний вантаж - відкриття та закриття клапанів для подачі газу до інших центрифуг, впливаючи на якість продуктів процесу переробки та непомітний на інтерфейсах оператора.
Stuxnet здатний до оновлення через зв’язок із сервером керування та керування через HTTP або викликом сервера RPC в одноранговому зв'язку. Незважаючи на те, що Stuxnet був цілеспрямованою атакою з точно визначеною метою, розробленою та розробленою для обмеження можливого побічного збитку, він мав глобальний вплив, заразивши 100 000 комп'ютерних систем з таких країн, як Іран, Індонезія, Індія, Пакистан, Узбекистан та інші країни.

Кіберзброя

Таким чином, для аналізу кіберзброї та типу дійових осіб слід визначити наступне:

- Призначення кіберзброї
- Її складність та досконалість
- Специфіку об’єкту та цілі
- Конфігурації кіберзброї
- Потреба в різноманітності знань при її створені та використані
- Застосування
- Час застосування та термін на виявлення та знешкодження
- Локалізацію застосування
- Збитки