|  |  |  |  |
| --- | --- | --- | --- |
| Wykonanwcy: | Radosław Relidzyński | Bartłomiej Pstrągowski |  |
|  |  |  |  |

**Temat 3: Zagrożenia dla informacji i systemów teleinformatycznych.**

1. Zidentyfikować i opisać zakres Framework MITRE ATT&CK oraz możliwość wykorzystania framework-u w procesie oceny zagrożeń w organizacji

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – to dostępna na całym świecie baza wiedzy na temat taktyk i technik stosowanych przez hakerów, oparta na rzeczywistych obserwacjach, wykorzystywana jako podstawa do przewidywania oraz opracowywania rozwiązać dla konkretnych modeli zagrożeń.

Korzystając z modelu Mitre możemy przeanalizować, jakie ataki zostały przeprowadzone, jakimi mechanizmami się kierowali oraz jakie luki w zabezpieczeniu zwiększają możliwość skutecznego przeprowadzenia takiego ataku. Analiza takiego ataku pozwala na określenie, które elementy systemu są mniej lub bardziej narażone na atak oraz które urządzenia lub oprogramowanie może być kluczowe do jego przerwania lub zakłócenia.

Model Mitre w swojej bazie zawiera szczegółowe informacje na temat technik wykorzystywanych przez znane grupy APT . Framework Mitre Att&ck pozwala porównać działania dowolnie wybranych grup APT, w szczególności podobieństwa i różnice w przeprowadzanych atakach oraz stosowanych technikach.

1. Wyjaśnić znaczenie następujących określeń (w kontekście MITRE ATT&CK): domena technologiczna, taktyka, technika, sub-technika, procedury, oprogramowanie.

**Domena technologiczna**:

ATT&CK jest zorganizowany wokół tzw. „domen technologicznych” tworzących środowisko operacyjne dla (wrogich) podmiotów.

**Taktyka**:

Taktyki reprezentują „co” i „dlaczego” poprzez wskazanie podzbiorów technik i subtechnik. Przekładają się one na techniczne cele podmiotów, przesłanki do wykonania określonych akcji i możliwe akcje

**Technika**:

Techniki okreslaja poprzez wykonanie jakich akcji podmioty osiągają założone cele taktyczne

**Sub-technika**:

Subtechniki dostarczają bardziej szczegółowego opisu technik. Nie wszystkie techniki są rozwijalne do subtechnik.

**Procedury**:

Procedury są instancjami sposobów użycia technik.

**Oprogramowanie**:

ogół informacji w postaci zestawu instrukcji, zaimplementowanych interfejsów i zintegrowanych danych przeznaczonych dla komputera do realizacji wyznaczonych celów. Celem oprogramowania jest przetwarzanie danych w wyznaczonym przez twórcę zakresie.

1. Krótko scharakteryzować wszystkie taktyki MITRE ATT&CK, włącznie z wyjaśnieniem znaczenia ATT&CK.

|  |  |
| --- | --- |
| Nazwa angielska | Tłumaczenie i Opis |
| Reconnaissance | Rozpoznanie - Zdobywanie informacji, które mogą być przydatne podczas ataku. |
| Resource Development | Rozbudowa zasobów – pozyskiwanie i utrzymywanie zasobów przydatnych przy ataku np. kont użytkowników |
| Initial Access | Uzyskanie dostępu - pierwsza próba dostania się do atakowanego systemu. |
| Execution | Wykonanie ataku - uruchomienie kodu wykonującego atak |
| Persistence | Utrzymanie dostępu do systemu. |
| Privilege Escalation | Zwiększanie uprawnień atakujących w systemie. |
| Defense Evasion | Unikanie zabezpieczeń (procedur ochronnych systemu). |
| Credential Access | Dostęp do uwierzytelniania - wykradanie danych logowania. |
| Discovery | Odkrywanie systemu - pozyskiwanie wiedzy na temat atakowanego systemu. |
| Lateral Movement | Ruchy poboczne - techniki uzyskiwania dostępu do kolejnych części systemu. |
| Collection | Zbieranie danych - pozyskiwanie danych będących celem ataku. |
| Command and Control | Uzyskanie kontroli – uzyskanie możliwości komunikacji z atakowanym systemem oraz kontroli. |
| Exfiltration | Wykradanie danych z atakowanego systemu. |
| Impact | Wpływanie na system - działania utrudniające lub uniemożliwiające dalsze poprawne działanie systemu. |

1. Charakterystyka wybranej techniki w ramach wskazanej taktyki oraz powiązanych sub-technik.

Uwaga: należy wskazywać pola ID !!!

* 1. (BP)

**Charaktarestyka techniki Proxy w ramach strategii Command and Control:**

**Command and Control:**

Atakujący próbuje komunikować się z atakowanymi systemami, aby je kontrolować.

Command and Control obejmuje techniki, których atakujący mogą używać do komunikowania się z kontrolowanymi przez nich systemami w sieci ofiary. Przeciwnicy często próbują naśladować normalny, oczekiwany ruch, aby uniknąć wykrycia.

**Proxy (T1090):**

Atakujący mogą używać serwera proxy do kierowania ruchem sieciowym do atakowanego systemu lub działać jako pośrednik w komunikacji sieciowej, aby uniknąć bezpośrednich połączeń z ich infrastrukturą. Istnieje wiele narzędzi, które umożliwiają przekierowanie ruchu przez serwery proxy lub przekierowanie portów.

Sub-techniques

|  |  |
| --- | --- |
| **ID** | **Name** |
| T1090.001 | Internal Proxy |
| T1090.002 | External Proxy |
| T1090.003 | Multi-hop Proxy |
| T1090.004 | Domain Fronting |

**Proxy: Internal Proxy (**T1090.001**)**

Atakujący mogą używać wewnętrznego serwera proxy w atakowanej sieci do kierowania ruchem dowodzenia i kontroli między dwoma lub więcej systemami w zagrożonym środowisku. Używają wewnętrznych serwerów proxy do zarządzania komunikacją dowodzenia i kontroli w zaatakowanym środowisku, zmniejszenia liczby jednoczesnych wychodzących połączeń sieciowych, zapewnienia odporności w przypadku utraty połączenia lub omijania istniejących zaufanych ścieżek komunikacyjnych między zainfekowanymi systemami w celu uniknięcia podejrzeń.

**Proxy: External Proxy (T1090.002)**

Atakujący mogą korzystać z zewnętrznego serwera proxy, aby działać jako pośrednik w komunikacji sieciowej z serwerem dowodzenia i kontroli, aby uniknąć bezpośrednich połączeń z ich infrastrukturą. Serwery proxy mogą być wybierane tak, aby było niskie prawdopodobieństwo, że ​​zostanie zbadane połączenie z nimi i z zaatakowanym systemem. Systemy ofiary komunikują się bezpośrednio z zewnętrznym serwerem proxy w Internecie, a następnie serwer proxy przekazuje komunikację do serwera atakującego.

**Proxy: Multi-hop Proxy (**T1090.003**)**

Atakujący tutaj działa podobnie do subtechniki External Proxy, stawia jednak pomiędzy sobą, a atakowanym systemem nie jeden a wiele serwerów proxy. Ofiara jest w stanie zazwyczaj zidentyfikować tylko ostatni serwer proxy po drodze do niego co jeszcze bardziej utrudnia rozpoznanie zagrożenia.

**Proxy: Domain Fronting (**T1090.004**)**

Atakujący

mogą wykorzystywać schematy routingu w sieciach CDN i innych usługach obsługujących wiele domen, aby zaciemniać zamierzone miejsce docelowe ruchu HTTPS.

Atakujący mogą na przykład domenę „a” w nagłówku TLS, a domenę „b” w nagłówku http. W takim przypadku CDN może pokierować ruch na domenę „b” mimo, że ruch będzie wyglądał jak zaadresowany na domenę „a”. Wymaga to jednak aby domeny „a” i „b” były w tym samym CDN.

* 1. (RR)

**Charaktarestyka techniki „Data Encoding” w ramach strategii Command and Control:**

**Command and Control:**

Haker szuka takiej możliwości komunikacji z zaatakowanym systemem, aby móc go kontrolować. Strategia ta obejmuje wszelkiego rodzaju mechanizmy do pozyskania lub wykorzystania możliwości komunikacji i zarządzania systemem. W celu ukrycia swojego działania w systemie, hakerzy starają się nie działać możliwie w sposób najmniej podejrzany, aby utrudnić wykrycie ich działań. Sposoby na uzyskanie oraz otrzymanie dostępu dostosowywane są do danego systemu, jego właściwości oraz jakości zabezpieczeń.

**Data Encoding (T1132):**

Haker, aby jeszcze skuteczniej ukryć swoje działania stosuje szyfrowanie swoich danych. Wykorzystuje się do tego takie kodowania jak chociażby ASCII, Unicode, Base64 oraz MIME. Czasami stosuje się nawet kodowanie stosowane przy kompresji, na przykład gzip.

**Data Encoding: Standard Encoding (**T1090.001**)**

Standardowe kodowanie jest oparte o szyfrowanie danych binarnych do postaci możliwych do wypisania znaków (tekstu). Znajduje to zastosowanie przy transmisji danych, kiedy mamy do czynienia z kanałami dostępu nie akceptującymi nietypowych rozszerzeń lub postaci binarnej danych (na przykład przy protokołach email: SMTP, POP, IMAP, oraz przy pomocy protokołu transportowego NNTP). Takie zabezpieczenia przeciwko transferowi kodu binarnego nazywa się potocznie „ASCII armor”

**Data Encoding: Non-Standard Encoding (**T1090.002**)**

Aby jeszcze bardziej utrudnić możliwość wykrycia działania w systemie stosuje się innych, nietypowych form kodowania, działającym poza standardowymi protokołami. Niestandardowe formy kodowania opierać się mogą o schematy typowego kodowania (popularna jest zmodyfikowana wersja kodowania Base64 dla zawartości strony wysyłanej do serwera poprzez zapytania HTTP). Dodatkowo, istnieje możliwość kodowania informacji w plikach PDF, gdzie można zmieniać znaczenie poszczególnych znaków (co innego jest wyświetlane, a kod znaku symbolizuje zupełnie coś innego – jest to łatwe do wykrycia poprzez kopiowanie zawartości i wklejenie do edytora tekstu, widać wtedy oryginalny tekst).

1. Studium przypadku dla wybranej sub-techniki (minimum jednej, lub więcej technik – podwyższa ocenę). Czy opisywana sub-technika(-i) została(-y) zrealizowana w cyberprzestrzeni (domyślnie w Polsce)?   
   Uwaga: Jako źródło wiedzy wykorzystać publikacje CSIRT MON, CSIRT GOV, CERT NASK (CSIRT NASK) lub innych rzetelnych źródeł.
   1. Spearphishing via Service (T1566.003)

Przykładowa sytuacja:

Użytkownik otrzymuje takiego SMS-a:

Obraz zawierający tekst

Opis wygenerowany automatycznie

Podejrzany nadawca oraz link wskazuje na to, że jest to wiadomość mogąca być typowym atakiem typu phishing, a po wejściu w link możemy być narażeni na atak.

W związku z takimi sytuacjami organizacja CERT Polska przeprowadziła akcję sprawdzania takich wiadomości. Opublikowali oni numer, na który można było przesyłać podejrzane SMS-y:

Obraz zawierający tekst

Opis wygenerowany automatycznie

W Polsce istotnie zdarzają się przypadki tego typu ataków. Do końca roku na Listę trafiło blisko 42 tys. złośliwych domen, z czego aż 33 tys. w 2021 r. Każda z zablokowanych domen była dokładnie weryfikowana przez naszych pracowników przed uznaniem za złośliwą, dzięki czemu stworzyliśmy jedno z najbardziej wiarygodnych źródeł tego typu danych, które może być przetwarzane w sposób automatyczny. W wyniku rosnącego poziomu wdrożenia Listy w różnych systemach filtrowania treści, tylko w 2021 r. udało się powstrzymać blisko 4 miliony prób wejścia na strony oznaczone jako wyłudzające dane.

1. Identyfikacja możliwej ścieżki ataku według MITRE ATT&CK, wraz z uzasadnieniem.

Domena technologiczna **Enterprise**, ***Network Matrix: Network***

1. Initial Access:

Exploit Public-Facing Application – zmieniamy zawartość sesji tak, żeby zalogowało nas jako pracownika.

1. Execution:

Command and Scripting interpreter – wprowadzamy skrypt w języku Python realizujący nasze założenia

1. Persistence

Valid Accounts – do podtrzymania dalej wykorzystujemy to, że jesteśmy zalogowani jako pracownik

1. Privilage Escalation

Valid accounts – nasze konto ma wymagane uprawnienia

1. Defense Evasion

Modify System Image - za pomocą skryptu modyfikujemy system operacyjny atakowanej sieci w celu utrzymania sesji i uprawnień.

1. Credential Access

Input Capture Keylogging - przemycający do systemu program typu keylogger.

1. Discovery

Password Policy Discovery - używamy zgromadzonych haseł do uzyskiwania informacji o całym systemie

1. Collection

Input Capture - wykorzystujemy poprzedniego keyloggera do zbierania danych

1. Command and Control

Wykorzystujemy internal proxy aby uniknąć wykrycia i komunikować się z systemem.

1. Exfiltration

Wykorzystujac technikę Traffic Duplication w celu pozyskania danych wrażliwych z sieci.

1. Impact

Wykorzystując zdobyte uprawnienia zamykamy system po zakończeniu ataku