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

**Temat 4: Zabezpieczenia – rodzaje i podstawy działania**

1. Modelowanie możliwej ścieżka ataku na system informacyjny organizacji z użyciem MITRE ATT&CK..

Celem jest wykradnięcie danych kontaktowych klientów, aby potem wykorzystać je do wysyłania reklam

1. Initial Access:

T1190 Exploit Public-Facing Application – zmieniamy zawartość sesji tak, żeby zalogowało nas jako pracownika systemu.

1. Execution:

T1059.006 Command and Scripting interpreter Python – wprowadzmy skrypt w jezyku Python uzyskujący dane potrzebne do uzyskania sesji pracownika.

1. Persistence

T1078 Valid Accounts – do podtrzymania dalej wykorzystujemy to, że jesteśmy zalogowani jako pracownik. Staramy się zachowywać tak jak typowy pracownik, aby utrudnić wykrycie, regularnie zmieniamy konto z którego działamy.

1. Privilage Escalation

T1078.003 Valid accounts Local Accounts – uzyskujemy dostep do istniejacego konta administratora w celu uzyskania wiekszych uprawnien, regularnie zmieniamy konta z których dzialamy.

1. Defense Evasion

T1601.001 Modify System Image Patch System Image – za pomocą skryptu modyfikujemy system operacyjny atakowanej sieci w celu utrzymania sesji i uprawnień.

1. Credential Access

T1056.001 Input Capture Keylogging – przemycamy do systemu program typu keylogger.

1. Discovery

T1201 Password Policy Discovery – używamy zgromadzonych haseł do uzyskiwania informacji o całym systemie.

1. Collection

T1056.001 Input Capture Keylogging – wykorzystujemy poprzedniego keyloggera do zbierania danych o klientach.

1. Command and Control

T1090.001 Proxy Internal proxy – przy pomocy proxy unikamy wykrycia oraz komunikujemy się z systemem.

1. Exfiltration

T1020.001 Exfiltration Traffic Duplication – pozyskanie danych kontaktowych do klientów.

1. Impact

T1529 System Shutdown/Reboot – Wykorzystując zdobyte uprawnienia zamykamy system po zakończeniu ataku aby utrudnić pozyskanie informacji które potencjalnie zostały przez nas zostawione i mogą być użyte do identyfikacji nas jako napastników.

1. Identyfikacja sposobów detekcji ataku na system informacyjny dla zmodelowaniej ścieżki ataku MITRE ATT&CK.
2. Initial Access:

Mitygacja - M1056 Pre-compromise - zastosowanie protokołu VPN, który uniemożliwia niepodłączonym urządzeniom korzystania z elementów systemu.

1. Execution:

Mitygacja - M1038 Execution Prevention - validacja wprowadzanego pliku wykluczająca możliwość wprowadzania skryptów.

1. Persistence

Mitygacja - M1026 Privileged Account Management - zarządzanie dostępem do logowania, ograniczenie możliwości bycia zalogowanym na większej ilości urządzeń oraz regularnego logowania na kilku urządzeniach.

1. Privilage Escalation

Mitygacja - M1026 Privileged Account Management - ograniczenie dla kont z ponadprzeciętnymi uprawnieniami do wykonywania codziennych czynności.

1. Defense Evasion

Wykrycie:

DS0022 File File Modification:

Regularne sprawdzanie sumy kontrolnej w systemie operacyjnym, porownywanie z zaufana wersja w celu wykrycia nieporzadanych zmian

Przeciwdzialanie:

M1045 Code Signing:

Wersje systemu sa podpisywane, dzieki czemu atakujacy nie może zmodyfikowac systemu bez uzyskania klucza i wygenerowania podpisu

1. Credential Access

Wykrycie i przeciwdzialanie:

Monitorujemy zmiany w rejestrach klawiszy w systemie

1. Discovery

Wykrycie:

Obserwujemy konta które mogą probowac uzyskac dostep do specjalistycznych danych

Przeciwdziałanie:

Uzywamy filtra DLL

1. Collection

Wykrycie i przeciwdzialanie:

Monitorujemy zmiany w rejestrach klawiszy w systemie

1. Command and Control

Wykrycie:

Szukamy podejrzanych ruchow wśród nowych polaczen sieciowych

Wykrycie:

Szukamy podejrzanych ruchow wśród nowych polaczen sieciowych i niezaufanych hostow.

1. Exfiltration

Wykrycie:

Szukamy podejrzanych ruchow wśród nowych polaczen sieciowych i niezaufanych hostow

Przeciwdziałanie:

Szyfrowanie przsylanych informacji

1. Impact

Wykrycie i przeciwdzialanie:

Kontrolowanie wprowadzanych polecen zamykania systemu tak aby były one wykonywane tylko autoryzowane

1. Identyfikacja możliwości mitygacji ataku (przerwania łańcucha ataku MITRE ATT&CK)

Z wykorzystaniem tabeli:

1. Initial Access:

Mitygacja - M1056 Pre-compromise - zastosowanie protokołu VPN, który uniemożliwia niepodłączonym urządzeniom korzystania z elementów systemu.

1. Execution:

Mitygacja - M1038 Execution Prevention - validacja wprowadzanego pliku wykluczająca możliwość wprowadzania skryptów.

1. Persistence

Mitygacja - M1026 Privileged Account Management - zarządzanie dostępem do logowania, ograniczenie możliwości bycia zalogowanym na większej ilości urządzeń oraz regularnego logowania na kilku urządzeniach.

1. Privilage Escalation

Mitygacja - M1026 Privileged Account Management - ograniczenie dla kont z ponadprzeciętnymi uprawnieniami do wykonywania codziennych czynności.

1. Defense Evasion

Przeciwdzialanie:

M1045 Code Signing:

Wersje systemu sa podpisywane, dzieki czemu atakujacy nie może zmodyfikowac systemu bez uzyskania klucza i wygenerowania podpisu

1. Credential Access

Wykrycie i przeciwdzialanie:

Monitorujemy zmiany w rejestrach klawiszy w systemie

1. Discovery

Przeciwdziałanie:

Uzywamy filtra DLL

1. Collection

Wykrycie i przeciwdzialanie:

Monitorujemy zmiany w rejestrach klawiszy w systemie

1. Command and Control

Przeciwdziałanie:

Stosowanie sygnatur w ruchu w sieci. Identyfikacja każdego ruchu który ma miejsce w sieci.

1. Exfiltration

Przeciwdziałanie:

Szyfrowanie przsylanych informacji

1. Impact

Wykrycie i przeciwdzialanie:

Kontrolowanie wprowadzanych polecen zamykania systemu tak aby były one wykonywane tylko autoryzowane

Etapy działań intruza i możliwości przeciwdziałania na atak wg. MITRE ATT&CK

Etapy działań intruza i możliwości przeciwdziałania na atak MITRE ATT&CK /

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **OBRONA**  **ATAK** | **Wykrycie**  *detect* | **Odmowa**  *deny* | **Przerwanie**  *disrupt* | **Osłabienie**  *degrade* | **Zwodzenie**  *deceive* | **Niszczenie**  *destroy* |
| **Initial Access** |  | M1056 Pre-compromise |  |  |  |  |
| **Execution** |  | M1056 Pre-compromise |  |  |  | M1056 Pre-compromise |
| **Persistence** |  |  | M1026 Privileged Account Management | M1026 Privileged Account Management |  |  |
| **Privilege Escalation** |  |  | M1026 Privileged Account Management | M1026 Privileged Account Management |  |  |
| **Defense Evasion** | DS0022 File File Modification | M1045 Code Signing |  |  |  |  |
| **Credential Access** | DS0024 Windows Registry |  |  |  |  |  |
| **Discovery** | DS0002 User Account User Account Metadata | M1027 Password Policies |  |  |  |  |
| **Collection** | DS0024 Windows Registry Windows Registry Key Modification |  |  |  |  |  |
| **Command and Control** | DS0029 Network Traffic Network Connection Creation |  | M1031 Network Intrusion Prevention |  |  |  |
| **Exfiltration** | DS0029 Network Traffic Network Connection Creation |  |  |  | M1041 Encrypt Sensitive Information |  |
| **Impact** | DS0017 Command Command Execution | DS0017 Command Command Execution |  |  |  |  |