

Złośliwe oprogramowanie — analiza autostartu i procesów

Czas: 2 × 45 min

praca w parach (zamiana VM: jedna osoba ukrywa wpis, druga go szuka)

Cel: Nauczenie się wyszukiwania podejrzanych programów w autostarcie, procesach i połączeniach sieciowych narzędziami Sysinternals oraz usuwania ich i sprawdzania systemu skanerami drugiej opinii.

Po zajęciach potrafisz:

- analizuje wpisy autostartu w Autoruns z weryfikacją podpisów cyfrowych i VirusTotal
- ocenia procesy w Process Explorer (drzewo, ścieżka, podpis, wydawca)
- wiąże procesy z połączeniami sieciowymi w TCPView
- wykrywa i usuwa przygotowany „podejrzany” wpis autostartu
- przeprowadza skanowanie skanerem drugiej opinii i skanowanie offline Microsoft Defender

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i VM Windows 11 z zadania 26 roku 1 (z migawką)

Oprogramowanie

- **Autoruns (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/autoruns
- **Process Explorer (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/process-explorer
- **TCPView (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/tcpview
- **Malwarebytes Free** — skaner drugiej opinii; alternatywa: ESET Online Scanner
<https://www.eset.com/int/home/online-scanner/>
malwarebytes.com/mwb-download
- **Microsoft Defender (Zabezpieczenia Windows)** — wbudowany; skanowanie offline

Przygotowanie przed zajęciami

- Uruchom VM Windows 11 i wykonaj migawkę „przed-malware”. Wszystkie ćwiczenia wykonujesz tylko w VM.

Bezpieczeństwo

- Nie pobieraj prawdziwego złośliwego oprogramowania ani „próbek” z internetu. „Podejrzany” program to Twój własny, nieszkodliwy skrypt.
- Autoruns i Process Explorer pozwalają wyłączać i usuwać wpisy systemowe — w szkolnym systemie i na laptopach tylko przeglądaj, zmiany wykonuj wyłącznie w VM.
- Sprawdzanie w VirusTotal wysyła tylko skróty (hash) plików. Nie używaj opcji wysyłania nieznanych plików — mogą zawierać dane prywatne.
- Po zajęciach przywróć migawkę „przed-malware”.

Przebieg zadania

1 Przygotowanie „podejrzanego” autostartu

Osoba A w swojej VM. Osoba B w tym czasie odwraca się od ekranu.

1. Utwórz plik `%APPDATA%\upd.cmd` z treścią `start notepad.exe` (Notatnik: Zapisz jako, typ „Wszystkie pliki”).
2. Dodaj wpis do rejestru w Wierszu polecenia (`cmd` — w PowerShell zmienna `%APPDATA%` nie zostanie rozwinięta): `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Aktualizator /t REG_SZ /d "%APPDATA%\upd.cmd"`.
3. Dla chętnych drugi wpis: zadanie w Harmonogramie zadań uruchamiane przy logowaniu, o mylącej nazwie.
4. Uruchom ponownie VM i sprawdź, że po zalogowaniu otwiera się Notatnik. Zamieńcie się miejscami.

2 Analiza autostartu — Autoruns

Osoba B szuka wpisów w VM kolegi.

1. Uruchom Autoruns jako administrator. W Options → Scan Options zaznacz weryfikację podpisów (Verify code signatures) i sprawdzanie w VirusTotal.com, przeskanuj ponownie.
2. Włącz Options → Hide Microsoft Entries. Przejrzyj zakładki Logon, Scheduled Tasks i Services.
3. Znajdź podejrzany wpis: zapisz lokalizację w rejestrze, ścieżkę pliku, stan podpisu i wynik VirusTotal. Wyjaśnij, co wzbudziło podejrzenie.
4. Najpierw wyłącz wpis (odznacz pole), uruchom ponownie i sprawdź efekt. Potem usuń wpis (Delete) i plik `upd.cmd`.

3 Procesy i połączenia

1. Uruchom Process Explorer. Dodaj kolumny Verified Signer i VirusTotal (View → Select Columns lub Options). Znajdź procesy bez podpisu.
2. Uruchom ręcznie `upd.cmd` i znajdź w drzewie procesów jego łańcuch (`cmd.exe` → `notepad.exe`). Sprawdź właściwości procesu: ścieżkę, wiersz polecenia, proces nadrzędny.
3. Uruchom TCPView. Otwórz przeglądarkę i znajdź jej połączenia: adres zdalny, port, stan. Znajdź proces nasłuchujący na porcie (Listening) i ustal, czym jest.

4 Skanery drugiej opinii

1. Zainstaluj Malwarebytes Free (bez okresu próbnego wersji Premium, jeśli instalator pozwala), wykonaj skanowanie i zapisz wynik.
2. Uruchom skanowanie offline: Zabezpieczenia Windows → Ochrona przed wirusami i zagrożeniami → Opcje skanowania → skanowanie offline Microsoft Defender → Skanuj teraz. VM uruchomi się ponownie (ok. 15 min) — w tym czasie opracowuj sprawozdanie.
3. Po restarcie sprawdź wynik w Historii ochrony. Przywróć migawkę „przed-malware”.

W sprawozdaniu umieść

- ☐ opis przygotowanego wpisu (lokalizacja, treść) — przez osobę A
- ☐ zrzut Autoruns z odnalezionym wpisem i opis cech, które go zdradziły — przez osobę B
- ☐ zrzut drzewa procesów i właściwości procesu z Process Explorer
- ☐ tabela połączeń z TCPView (2–3 pozycje)
- ☐ wyniki skanowania Malwarebytes i Defender Offline
- ☐ procedura postępowania przy podejrzeniu infekcji (5–7 kroków)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Jakie cechy wpisu autostartu powinny wzbudzić podejrzenie (lokalizacja, podpis, nazwa)?
2. Dlaczego najpierw wyłącza się wpis w Autoruns, a dopiero potem go usuwa?
3. Dlaczego skanowanie offline wykrywa zagrożenia, których nie widzi zwykłe skanowanie?
4. Dlaczego nie należy instalować dwóch programów antywirusowych działających jednocześnie w czasie rzeczywistym?

Kryteria oceny

Kryterium	Punkty
Przygotowanie wpisu i poprawne usunięcie wpisu kolegi	5
Analiza Autoruns z podpisami i VirusTotal	4
Process Explorer i TCPView	4
Skanowanie drugą opinią i offline, procedura postępowania	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).