Анализа рачунарског црва Stuxnet

Ђорђе Митровић
Индекс: 42/2025

30. март 2026.

Садржај

1 Увод

Stuxnet представља један од најсложенијих малициозних софтвера икада направљених. Његова примарна сврха била је саботажа индустријских контролних система (ICS).

2 Техничке карактеристике

2.1 Структура кода

Црв је специфичан по томе што комбинује различите методе напада. Његове кључне компоненте укључују:

- **LNK датотеке:** Коришћене за аутоматско извршавање кода са USB стикова.
- **Zero-day рањивости:** Чак четири до тада непозната безбедносна пропуста.
- **PLC rootkit:** Део кода који скрива присуство црва на индустријским контролерима.

SCADA Системи за надзор и контролу.

PLC Програмабилни логички контролери.

Црв је користио чак четири *zero-day* рањивости. Математички модел ширења:

$$P(t) = \frac{1}{1 + e^{-k(t-t_0)}} \tag{1}$$

3 Визуелни приказ и дефиниције

Слика 1: Симболични приказ Stuxnet-а

Дефиниција 1 *Сајбер-оружје је злонамерни код развијен у сврху наношења штете критичној инфраструктури.*

Лема 1 *Сваки софтвер који утиче на PLC може бити оружје.*

Теорема 1 *Ако је код потписан валидним сертификатом, вероватноћа је* $V \approx 1$.

4 Анализа података

Држава	Проценат инфекција	Тип циља
Иран	58.85%	Нуклеарна постројења
Индонезија	18.22%	Енергетика
Индија	8.31%	Индустрија

Табела 1: Дистрибуција инфекције Stuxnet црвом

5 Закључак

Stuxnet је променио начин на који посматрамо модерно ратовање.

1. **Напад на хардвер:** Физичка штета путем софтвера.
2. *Air-gap* изолација није апсолутна заштита.
3. Употреба украдених дигиталних потписа.