MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Giappone

DA PUBBLICARE IMMEDIATAMENTE **N. 3649**

Il presente testo è una traduzione della versione inglese ufficiale del comunicato stampa e viene fornito unicamente per comodità di consultazione. Fare riferimento al testo inglese originale per conoscere i dettagli e/o le specifiche. In caso di eventuali discrepanze, prevale il contenuto della versione inglese originale.

Richieste dei clienti

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

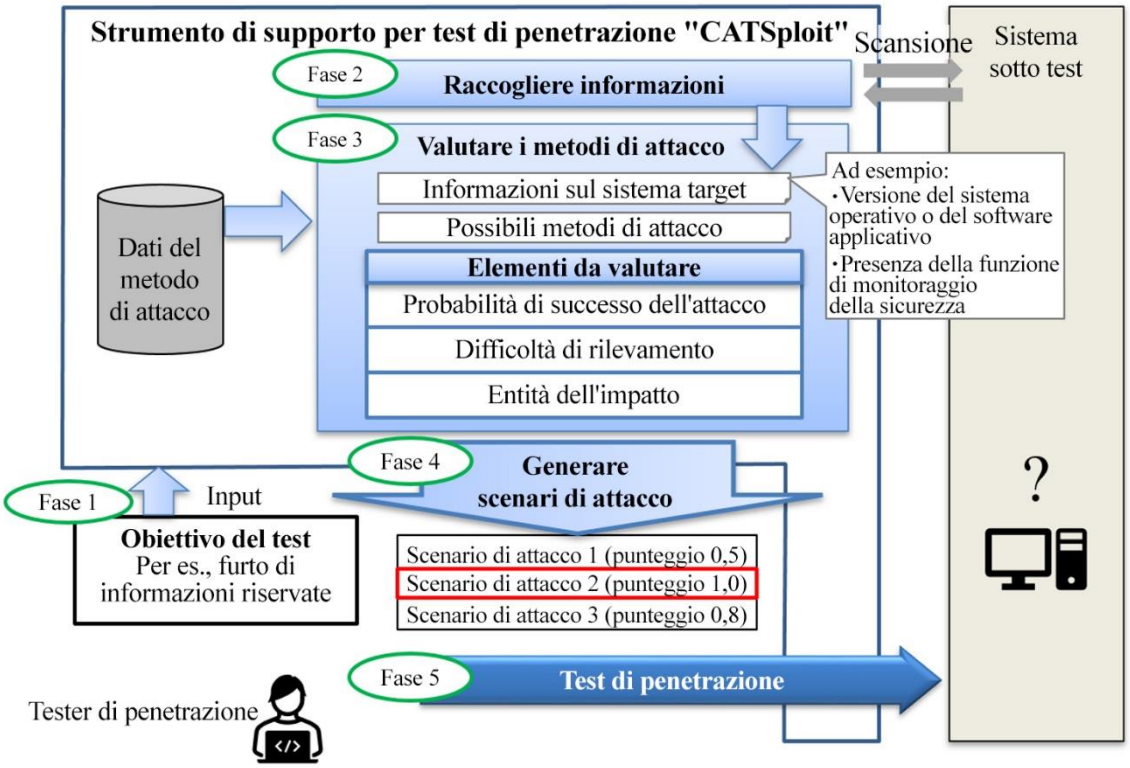
Richieste dei media

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric sviluppa il primo strumento al mondo di supporto per test di penetrazione che genera scenari di attacco dal punto di vista degli hacker

Si prevede che migliori la resistenza agli attacchi informatici di tutti i prodotti connessi alle reti



Esempio di utilizzo dello strumento di supporto durante i test di penetrazione

TOKYO, 5 dicembre 2023 – Mitsubishi Electric Corporation (TOKYO: 6503) ha annunciato oggi di aver sviluppato CATSploit, il primo[1] strumento al mondo di supporto per test di penetrazione[2] che genera automaticamente scenari di attacco basati sugli obiettivi di test di un tester di penetrazione, quali il furto di informazioni riservate, per valutare l'efficacia degli attacchi di test. Tramite gli scenari di attacco e i risultati dei test (punteggi) risultanti, anche gli ingegneri della sicurezza alle prime armi possono facilmente eseguire test di penetrazione.

Negli ultimi anni i sistemi di controllo, tra cui infrastrutture, apparecchiature di fabbrica e via dicendo, sono stati connessi in misura sempre più crescente alle reti, con conseguente aumento del rischio di interruzioni, come interruzioni di corrente o arresto dei trasporti pubblici, a causa di attacchi informatici. La necessità di implementare misure di sicurezza in tali sistemi è diventata urgente. Inoltre, gli standard ISA/IEC 62443[3] richiedono l'esecuzione di test di sicurezza e fuzzing[4] su sistemi e apparecchiature per valutarne la resistenza agli attacchi informatici, incluse le vulnerabilità dovute a errori di implementazione o configurazione. I test di penetrazione sono altamente sofisticati e richiedono il coinvolgimento degli hacker white hat[5] per sferrare l'effettivo attacco al sistema o al prodotto testato; tali individui, tuttavia, devono possedere un livello di competenze molto elevato e, pertanto, sono difficilmente reperibili.

Mitsubishi Electric, concentrando l'attenzione sui fattori che gli hacker considerano nella scelta dei vettori di attacco, ha ora sviluppato uno strumento di supporto per test di penetrazione che genera elenchi di possibili scenari di attacco e la loro efficacia (espressa come punteggi numerici).

I dettagli dello strumento saranno presentati il 6 dicembre (alle 11, ora locale) nel corso del Black Hat Europe 2023 Arsenal a Londra, che si terrà il 6 e il 7 dicembre.

Caratteristiche

1) Genera automaticamente scenari di attacco dal punto di vista di un hacker white hat

- Mitsubishi Electric ha concentrato l'attenzione sui fattori che gli hacker prendono in considerazione nella scelta dei metodi di attacco, quali la probabilità di successo dell'attacco, la difficoltà di rilevamento e l'entità dell'impatto. Adattando gli obiettivi per test specifici, il sistema è in grado di generare automaticamente scenari che evidenziano i passaggi necessari per implementare un attacco mirato a raggiungere tali obiettivi.

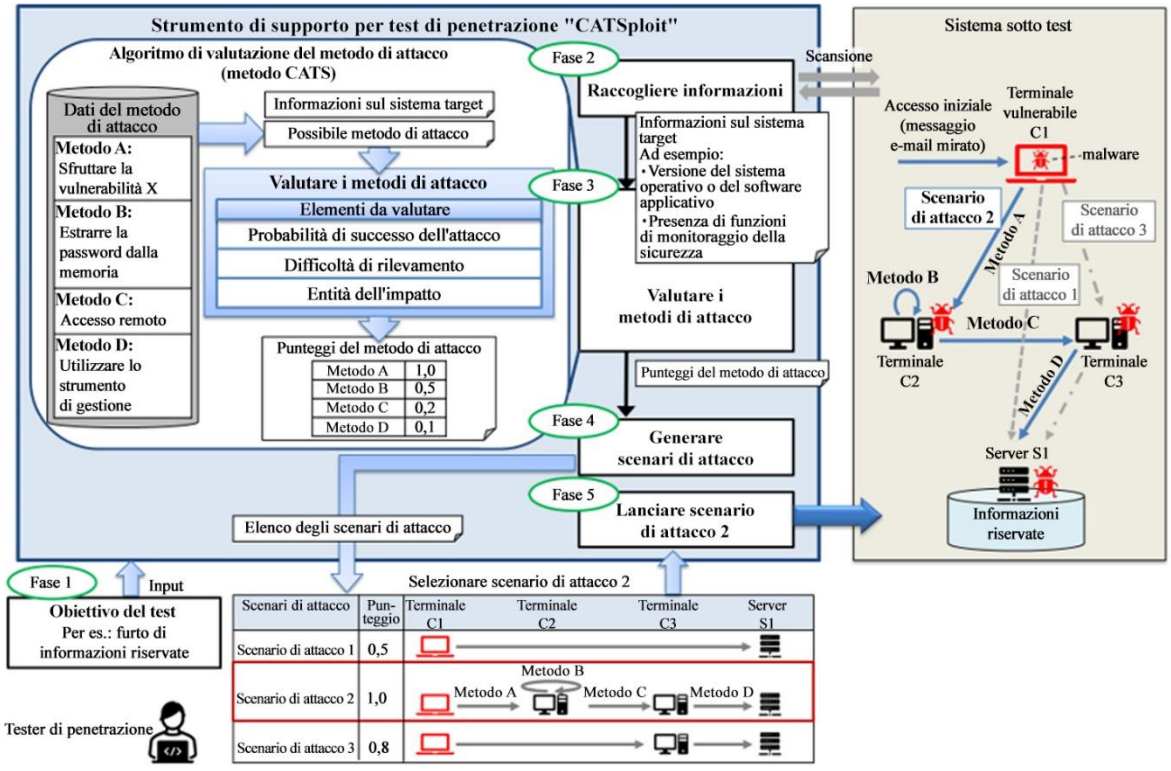
2) Test ottimali valutano l'efficacia degli scenari di attacco dal punto di vista di un hacker white hat

- Il metodo CATS[6] proprietario di Mitsubishi Electric calcola l'efficacia di ciascun metodo di attacco (espressa come punteggio numerico) dal punto di vista di un hacker white hat; viene quindi proposto un elenco di scenari di attacco in modo da poter selezionare quello più efficace (ossia con il punteggio più alto).

---

[1] Secondo le ricerche di Mitsubishi Electric alla data del 5 dicembre 2023
[2] Test che mira a confermare se un sistema o un'apparecchiatura possono essere compromessi da un effettivo attacco
[3] Standard di sicurezza per sistemi di controllo industriali
[4] Metodo di test per rilevare difetti o vulnerabilità software mediante l'immissione di dati non validi o errati
[5] Hacker etici che utilizzano tecnologie informatiche e conoscenze avanzate per identificare problemi di sicurezza e via dicendo
[6] Cyber Attack Techniques Scoring (CATS, punteggio delle tecniche di attacco informatico): metodo proprietario di Mitsubishi Electric per la valutazione dell'efficacia dei vettori di attacco

- La valutazione CATS tiene conto non solo delle informazioni di sistema note, come il sistema operativo, la versione dell'applicazione e i dispositivi di monitoraggio della sicurezza, ma anche delle informazioni mancanti sul sistema, consentendo di realizzare scenari di attacco che replicano fedelmente il punto di vista dell'effettivo autore di un attacco.
- La valutazione automatizzata degli scenari di attacco che potrebbero essere utilizzati dagli hacker white hat consente agli ingegneri della sicurezza meno esperti di eseguire con facilità i test di penetrazione.



Strumento di supporto per test di penetrazione CATSploit

Sviluppi futuri

Per migliorare ulteriormente la resistenza agli attacchi informatici dei sistemi e dei dispositivi sviluppati da Mitsubishi Electric, l'azienda continuerà la ricerca e lo sviluppo di questo nuovo strumento con l'obiettivo di utilizzarlo per i test di sicurezza effettivi dei propri prodotti entro il 2026.

###

Informazioni su Mitsubishi Electric Corporation

Con oltre 100 anni di esperienza nella fornitura di prodotti affidabili e di alta qualità, Mitsubishi Electric Corporation (TOKYO: 6503) è un leader mondiale riconosciuto della produzione, del marketing e della vendita di apparecchi elettrici ed elettronici per i settori informatico e delle comunicazioni, spaziale e delle comunicazioni satellitari, dell'elettronica di consumo, delle tecnologie industriali, energetico, dei trasporti e delle costruzioni. Mitsubishi Electric utilizza la tecnologia per migliorare la società, incarnando lo spirito del concetto "Changes for the Better". L'azienda ha registrato un volume di vendite di 5.003,6 miliardi di yen (37,3 miliardi di dollari USA*) nell'anno fiscale terminato il 31 marzo 2023. Per ulteriori informazioni, visitare il sito www.MitsubishiElectric.com

*Gli importi in dollari statunitensi sono convertiti in yen al tasso di cambio di ¥134 = 1 dollaro statunitense, tasso approssimativo del mercato dei cambi esteri di Tokyo al 31 marzo 2023