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

POUR DIFFUSION IMMÉDIATE **n° 3649**

Ce texte est une traduction de la version anglaise officielle de ce communiqué de presse. Il est fourni à titre de référence et pour votre confort uniquement. Pour plus de détails ou de précisions, veuillez vous reporter à la version originale en anglais. En cas de divergence, la version originale en anglais prévaut.

Demandes de renseignements des clients

Information Technology R&D Center
Mitsubishi Electric Corporation

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

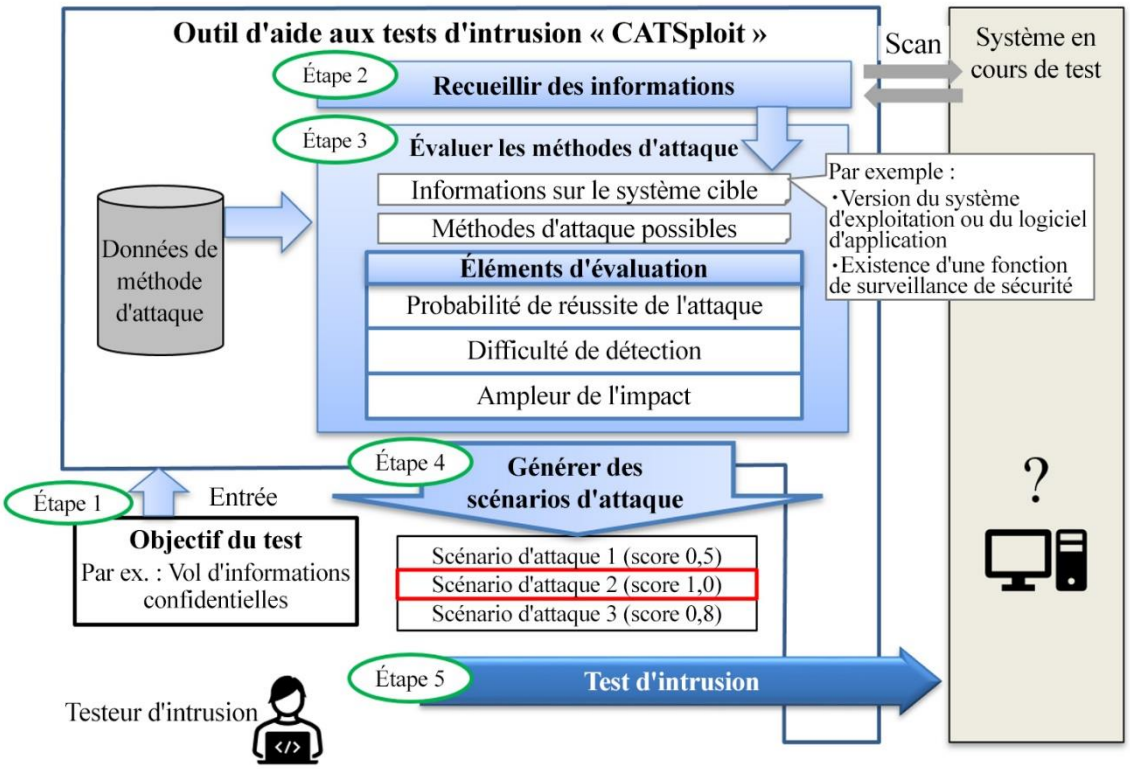
Demandes de renseignements des médias

Public Relations Division
Mitsubishi Electric Corporation

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

Mitsubishi Electric développe le premier outil d'aide aux tests d'intrusion au monde qui génère des scénarios d'attaque développés par des hackers

A pour but d'améliorer la résistance aux cyberattaques de tous les produits connectés aux réseaux



Exemple d'utilisation de l'outil pendant les tests d'intrusion

TOKYO, 5 décembre 2023 – Mitsubishi Electric Corporation (TOKYO : 6503) a annoncé aujourd'hui avoir développé le premier[1] outil de test d'intrusion[2] au monde, CATSploit, qui génère automatiquement des scénarios d'attaque basés sur les objectifs d'un testeur d'intrusion, tels que le vol d'informations confidentielles, afin d'évaluer l'efficacité des attaques tests. Grâce aux scénarios d'attaque et aux résultats des tests (scores) qui en résultent, même des ingénieurs de sécurité inexpérimentés peuvent facilement effectuer des tests d'intrusion.
Depuis ces dernières années, les systèmes de contrôle, notamment les infrastructures, les équipements d'usine, etc., sont de plus en plus connectés aux réseaux en ligne, ce qui augmente le risque de perturbations, telles que les pannes d'électricité ou les arrêts des transports publics, causés par des cyberattaques. La nécessité de mettre en œuvre des mesures de sécurité dans ces systèmes est par conséquent devenue urgente. En outre, les normes ISA/IEC 62443[3] exigent que les tests de sécurité dits fuzzing[4] et les tests d'intrusion soient effectués sur les systèmes et les équipements pour évaluer leur résistance aux cyberattaques, y compris les vulnérabilités dues à des erreurs de mise en œuvre ou de configuration. Les tests d'intrusion sont extrêmement sophistiqués et nécessitent l'intervention de hackers éthiques[5] pour attaquer le système ou le produit testé, mais ces personnes, qui doivent posséder un niveau d'expertise très élevé, sont rares et difficiles à trouver.
Mitsubishi Electric, en se concentrant sur les facteurs pris en compte par les hackers éthiques lors de la sélection de leurs vecteurs d'attaque, a développé un outil de test d'intrusion qui génère des listes de scénarios d'attaque possibles et leur efficacité (exprimées sous forme de scores numériques).
Les détails de cet outil seront présentés le 6 décembre (à 11 h, heure locale) à l'Arsenal de la Black Hat Europe 2023, qui aura lieu les 6 et 7 décembre à Londres.

Caractéristiques

1) *Génère automatiquement des scénarios d'attaque du point de vue de hackers éthiques*

- Mitsubishi Electric s'est concentré sur des facteurs pris en compte par les hackers éthiques lors du choix de leurs méthodes d'attaque, tels que la probabilité d'une attaque réussie, la difficulté de détection et l'ampleur de l'impact. Les hackers peuvent ajuster les objectifs pour des tests spécifiques et le système est en mesure de générer automatiquement des scénarios qui montrent les étapes nécessaires à la mise en œuvre d'une attaque pour atteindre ces objectifs.

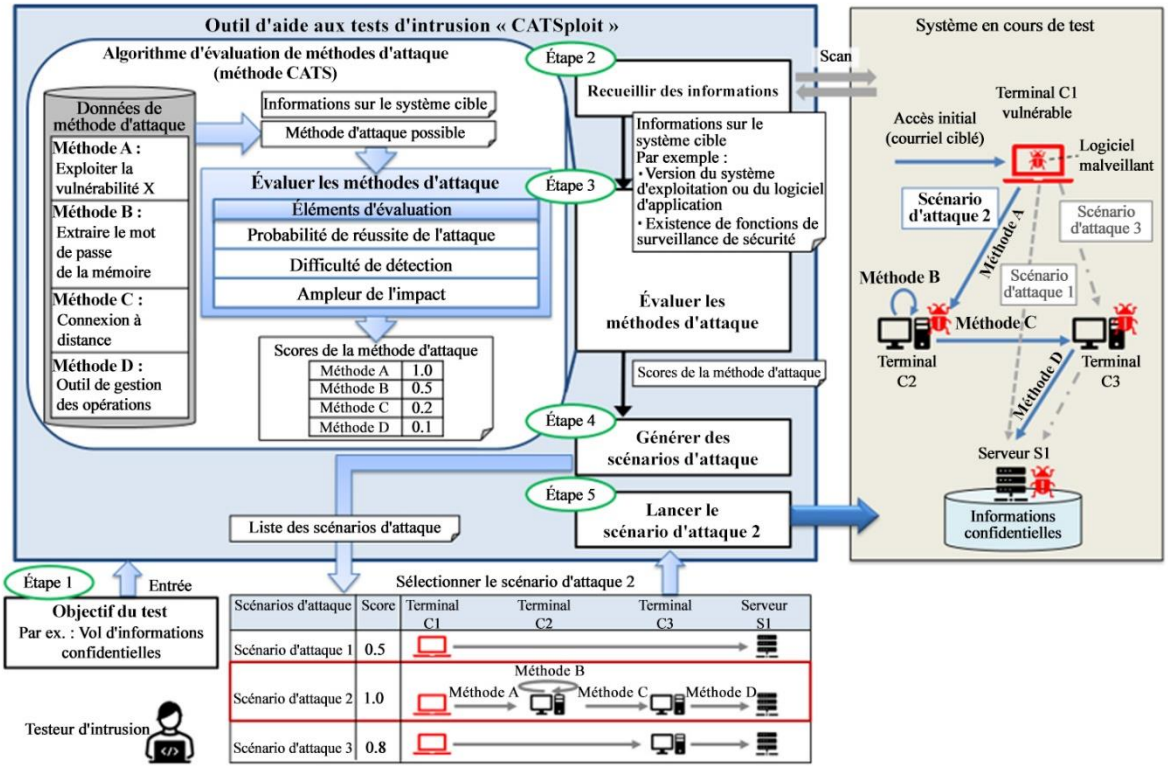
2) *Des tests sophistiqués évaluent l'efficacité des scénarios d'attaque du point de vue de hackers éthiques*

- La méthode CATS[6] exclusive de Mitsubishi Electric calcule l'efficacité de chaque méthode d'attaque (exprimée sous forme de score numérique) du point de vue d'un hacker éthique, en fonction de laquelle une liste de scénarios d'attaque est proposée afin que le scénario le plus efficace (score le plus élevé) puisse être sélectionné.

---

[1] Selon une étude réalisée par Mitsubishi Electric, au 5 décembre 2023
[2] Test pour confirmer qu'un système ou un équipement peut être compromis par une attaque réelle
[3] Normes de sécurité pour les systèmes de contrôle industriels
[4] Méthode de test permettant de détecter les défauts ou vulnérabilités de logiciels et qui consiste à y injecter des données incorrectes ou non valides
[5] Pirates éthiques qui utilisent des connaissances et technologies informatiques avancées pour identifier les problèmes de sécurité, etc.
[6] Évaluation des techniques de cyberattaque : méthode propriétaire de Mitsubishi Electric pour évaluer l'efficacité des vecteurs d'attaque

- L'évaluation CATS prend en compte non seulement les informations système connues, telles que le système d'exploitation, la version de l'application et les dispositifs de surveillance de sécurité, mais également les informations système manquantes, ce qui permet de réaliser des scénarios d'attaque qui reproduisent de près le point de vue d'un véritable pirate.
- L'évaluation automatisée des scénarios d'attaque susceptibles d'être utilisés par des hackers éthiques permet aux ingénieurs de sécurité moins expérimentés d'effectuer facilement des tests d'intrusion.



Outil d'aide aux tests d'intrusion CATSploit

Prochaines étapes du développement

Afin d'améliorer encore la résistance aux cyberattaques des systèmes et appareils développés par Mitsubishi Electric, l'entreprise continuera de rechercher et de développer ce nouvel outil dans le but de l'utiliser pour les tests de sécurité réels des produits de l'entreprise d'ici 2026.

###

À propos de Mitsubishi Electric Corporation

Forte de plus de 100 années d'expérience dans la création de produits fiables et de haute qualité, Mitsubishi Electric Corporation (TOKYO : 6503) est un leader mondial reconnu pour la fabrication, la mise sur le marché et la vente d'équipements électriques et électroniques utilisés dans les domaines du traitement de l'information et des communications, du développement spatial et des communications par satellite, des appareils électroniques grand public, de la technologie industrielle, de l'énergie, du transport et de l'équipement de construction. Mitsubishi Electric enrichit la société par la technologie dans l'esprit de sa devise « Changes for the Better ». L'entreprise a enregistré un chiffre d'affaires de 5 003,6 milliards de yens (37,3 milliards de dollars US*) au cours du dernier exercice qui a pris fin le 31 mars 2023. Pour plus d'informations, veuillez consulter le site www.MitsubishiElectric.com

*Les montants en dollars américains sont convertis à partir du yen au taux de ¥134 yens = 1 dollar US, taux approximatif indiqué par le Tokyo Foreign Exchange Market au 31 mars 2023