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

DA PUBBLICARE IMMEDIATAMENTE **N. 3106**

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
www.MitsubishiElectric.com/company/rd/

Richieste dei media

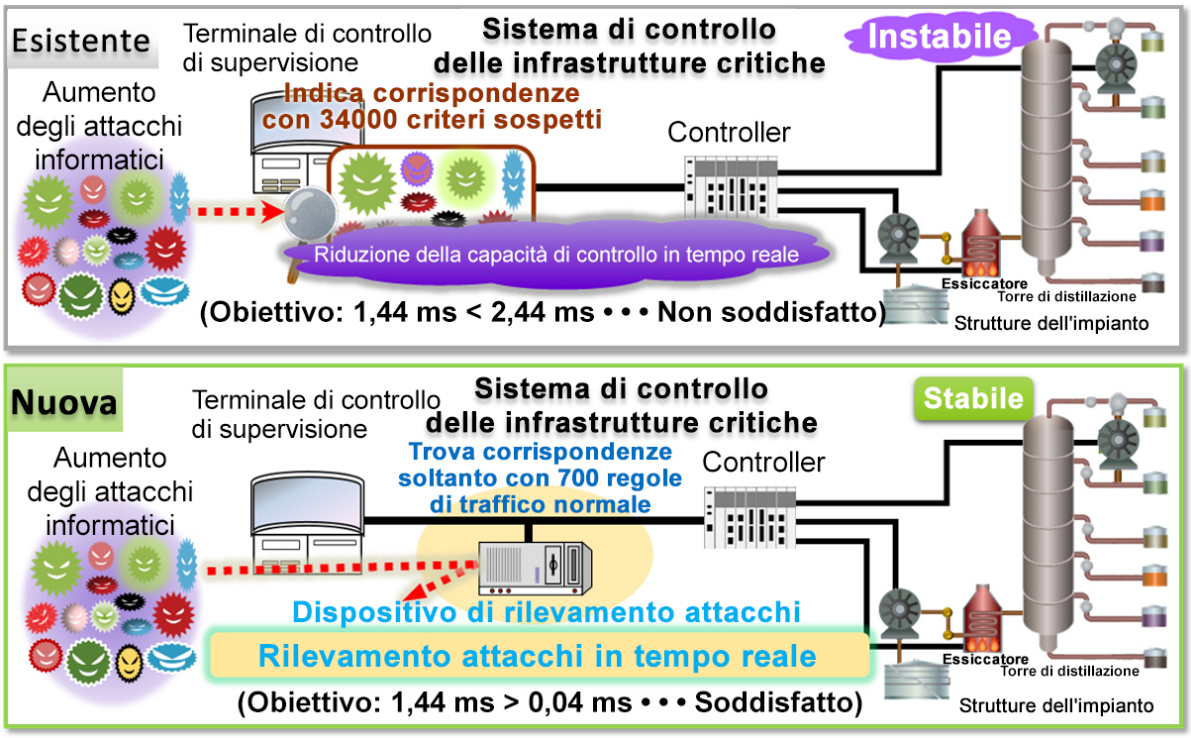
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric sviluppa una tecnologia di rilevamento degli attacchi informatici per i sistemi di infrastrutture critiche

Il rilevamento in tempo reale degli attacchi informatici ai sistemi di controllo contribuirà a favorire la stabilità delle infrastrutture

TOKYO, 17 maggio 2017 – Mitsubishi Electric Corporation (TOKYO: 6503) ha annunciato oggi di avere sviluppato una tecnologia di rilevamento degli attacchi informatici che consente di identificare rapidamente il traffico di rete che non corrisponde ai normali comandi predefiniti nei sistemi di controllo delle infrastrutture critiche. Questa tecnologia rileva elaborati attacchi informatici mascherati da normali comandi che mirano a colpire le infrastrutture critiche di produzione di energia elettrica, gas naturale, acqua, sostanze chimiche e petrolio, senza ridurre la capacità di controllo in tempo reale; si prevede che il suo impiego aiuterà a garantire la stabilità delle infrastrutture.

La commercializzazione per l'infrastruttura di produzione di energia elettrica è prevista approssimativamente per l'anno fiscale 2018. Altre applicazioni per la sicurezza informatica dell'infrastruttura critica saranno sviluppate in collaborazione con il comitato dello Strategic Innovation Promotion Program (SIP, ovvero Programma di promozione delle innovazioni strategiche).



La realizzazione della nuova tecnologia è stata supportata, in parte, dai risultati ottenuti dal progetto "Cyber-Security for Critical Infrastructure" (Sicurezza informatica per infrastrutture critiche) intrapreso dal Control System Security Center (CSSC). Il progetto "Cyber-Security for Critical Infrastructure" fa parte del Cross-ministerial Strategic Innovation Promotion Program (SIP, ovvero Programma interministeriale di promozione delle innovazioni strategiche), promosso dal Council for Science, Technology and Innovation (il Consiglio per la scienza, le tecnologie e le innovazioni) ed è stato commissionato dalla New Energy and Industrial Technology Development Organization (NEDO).

Caratteristiche principali

- A partire dal 17 maggio 2017, questa tecnologia è la prima al mondo in grado di definire le regole di rilevamento sulla base dei normali comandi per ogni stato operativo del sistema di controllo, inoltre interpreta come attacchi le deviazioni dai normali comandi.
- Quando il rilevamento degli attacchi è in uso, il funzionamento in tempo reale del sistema di controllo preso in esame è garantito, poiché questa tecnologia non implica un lungo processo di ricerca di corrispondenze con i criteri sospetti.
- Questa tecnologia contribuisce alla stabilità delle infrastrutture poiché riduce i tempi di rilevamento e garantisce il minimo impatto sui processi del sistema di controllo che devono terminare entro limiti di tempo stabiliti.

Confronto con le tecnologie esistenti

	Metodo	Funzionamento in tempo reale dei sistemi di controllo	Fattibilità
Nuova	Rileva le deviazioni dalle regole dei normali comandi determinate dallo stato operativo	Basso impatto grazie alle regole concise per i normali comandi	Collaudata e dimostrata efficace nelle simulazioni dei sistemi degli impianti
Esistente	Indica corrispondenze con i criteri sospetti confrontandoli con una massiccia quantità di set di regole	Rischio di impatto elevato a causa degli attacchi informatici in aumento	Attualmente utilizzata nei sistemi aziendali

Si sono verificati casi in cui degli attacchi informatici avanzati siano riusciti a penetrare nei sistemi di controllo per eseguire comandi che fingono di essere normali e che difficilmente sono distinguibili dai comandi reali. I metodi di rilevamento esistenti che confrontano il traffico in entrata con i criteri sospetti conosciuti potrebbero non riuscire a individuare questo tipo di attacchi. Il confronto con gli enormi volumi di criteri sospetti conosciuti richiede molto tempo e può causare errori delle operazioni del sistema di controllo.

Mitsubishi Electric ha osservato che il normale traffico del sistema di controllo nelle infrastrutture critiche è differente se il sistema è operativo, non è operativo o se è in manutenzione, pertanto, la nuova tecnologia utilizza regole di rilevamento diverse per ciascuno stato operativo. Con l'aumento crescente degli attacchi informatici, il tempo necessario per generare i criteri sospetti e cercare corrispondenze è veramente eccessivo. Tuttavia, poiché i comandi nei sistemi di controllo sono limitati, anche le regole possono essere limitate; ciò permette alla nuova tecnologia di Mitsubishi Electric di cercare rapidamente le corrispondenze e di rilevare gli attacchi, pur consentendo il funzionamento in tempo reale dei sistemi di controllo. L'azienda ha stimato il tempo di elaborazione per il rilevamento di attacchi del sistema di controllo preso in esame. La stima effettuata ha rivelato che la nuova tecnologia richiede soltanto 0,04 ms, rispetto ai 2,44 ms di una tecnologia esistente, mentre il requisito in tempo reale è di 1,44 ms.

Contesto

Con l'espansione dell'IoT nel campo delle infrastrutture, la sicurezza informatica sta diventando sempre più importante per le infrastrutture critiche che sostengono la nostra società. Fino a oggi, la sicurezza delle infrastrutture relative alla produzione di energia elettrica, gas naturale, acqua, sostanze chimiche e petrolio è stata garantita per mezzo di isolamento fisico, firewall di controllo del traffico e di una gestione operativa inflessibile. Tuttavia, negli ultimi anni e in particolar modo oltreoceano, è stato registrato un aumento di attacchi informatici avanzati che riescono a penetrare nei sistemi di controllo delle infrastrutture per inviare

comandi dannosi mascherati da comandi normali al fine di arrecare danni, quali blackout energetici e distruzione di apparecchiature.

Brevetti

I brevetti in corso di registrazione, relativi alla tecnologia annunciata nel presente comunicato, sono sette in Giappone e sette all'estero.

###

Informazioni su Mitsubishi Electric Corporation

Con oltre 90 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. Incarnando lo spirito del motto aziendale "Changes for the Better" e della visione ambientale "Eco Changes", Mitsubishi Electric si impegna a essere un'azienda "green" leader a livello mondiale, con l'obiettivo di migliorare la società con la tecnologia. L'azienda ha registrato un volume di vendite consolidato del gruppo di 4.238,6 miliardi di yen (37,8 miliardi di dollari USA*) nell'anno fiscale terminato il 31 marzo 2017. Per ulteriori informazioni, visitare:
www.MitsubishiElectric.com

*Al tasso di cambio di 112 yen per dollaro USA fornito dal mercato dei cambi esteri di Tokyo il 31 marzo 2017