

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

PARA LANÇAMENTO IMEDIATO

N.º 3106

Este texto é uma tradução da versão em inglês oficial deste comunicado de imprensa, sendo fornecido apenas para referência e conveniência. Consulte a versão em inglês original para obter detalhes e/ou informações específicas. Em caso de discrepância, prevalecerá o conteúdo da versão em inglês original.

Questões de clientes

Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

Questões da imprensa

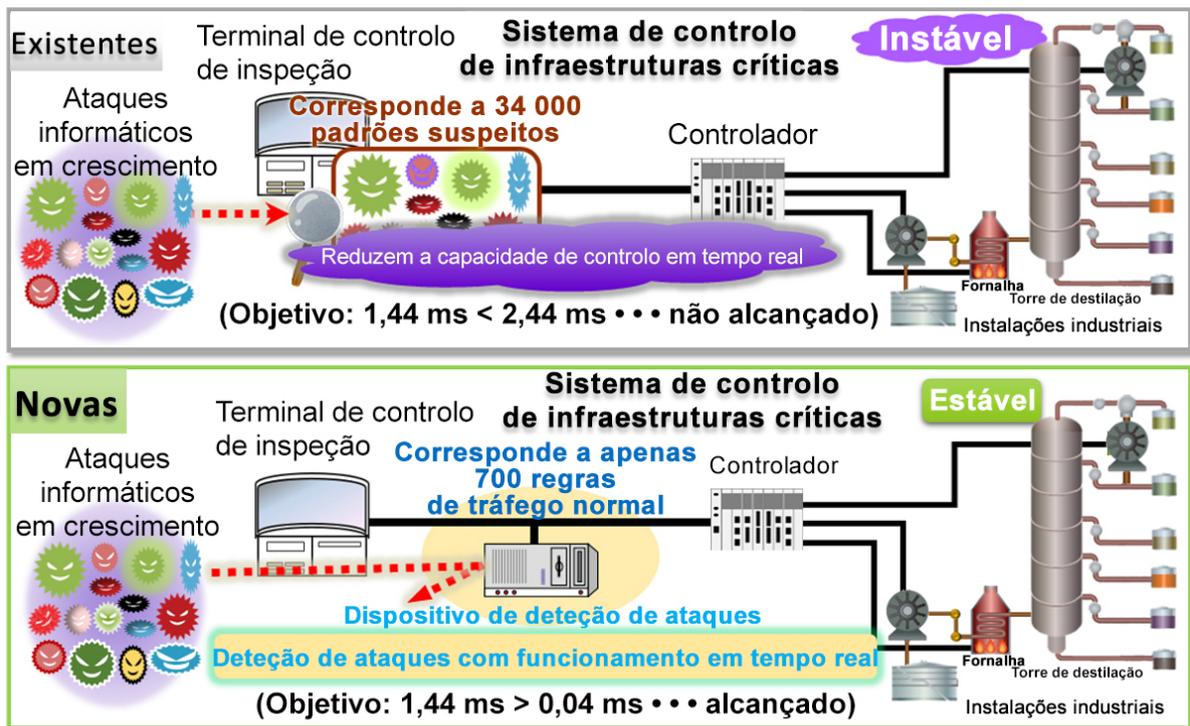
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

A Mitsubishi Electric desenvolve uma tecnologia de deteção de ataques informáticos para sistemas de infraestruturas críticas

A deteção em tempo real de ataques informáticos em sistemas de controlo contribuirá para a estabilidade das infraestruturas

TÓQUIO, 17 de maio de 2017 – A [Mitsubishi Electric Corporation](http://www.MitsubishiElectric.com) (TÓQUIO: 6503) anunciou hoje o desenvolvimento de uma tecnologia de deteção de ataques informáticos que identifica rapidamente o tráfego de rede que se desvia dos comandos normais predefinidos nos sistemas de controlo de infraestruturas críticas. A tecnologia deteta engenhosos ataques informáticos disfarçados de comandos normais identificados em infraestruturas críticas de energia elétrica, gás natural, água, produtos químicos e petróleo, sem reduzir a capacidade de controlo em tempo real, pelo que se espera que venha ajudar a garantir a estabilidade das infraestruturas.

Prevê-se a comercialização desta tecnologia para infraestruturas de energia elétrica a partir do ano fiscal de 2018. Serão desenvolvidas outras aplicações em colaboração com o desafio do Strategic Innovation Promotion Program (SIP) (Programa estratégico de promoção da inovação) para a segurança informática de infraestruturas críticas.



A criação da nova tecnologia foi apoiada pelos resultados da "Segurança informática de infraestruturas críticas" organizada pelo Control System Security Center (CSSC). A "Segurança informática de infraestruturas críticas" faz parte do Cross-ministerial Strategic Innovation Promotion Program (SIP) (Programa estratégico de promoção da inovação) promovido pelo Council for Science, Technology and Innovation, e foi encomendada pela New Energy and Industrial Technology Development Organization (NEDO).

Principais funcionalidades

- A tecnologia é a primeira no mundo, à data de 17 de maio de 2017, a definir as regras de deteção com base nos comandos normais para cada estado operacional do sistema de controlo e a interpretar os desvios dos comandos normais como ataques.
- O sistema de controlo visado tem a garantia de funcionamento em tempo real quando a deteção de ataque é utilizada, uma vez que a tecnologia não envolve um moroso processo de correspondência de padrões suspeitos.
- A tecnologia contribui para a estabilidade das infraestruturas ao reduzir o tempo de deteção e garantir a mínima influência nos processos do sistema de controlo, que, por sua vez, têm prazos de conclusão específicos.

Comparação com as tecnologias existentes

	Método	Funcionamento em tempo real dos sistemas de controlo	Viabilidade
Novas	Detetam desvios das regras dos comandos normais, determinadas pelo estado operacional	Baixo impacto devido a regras concisas dos comandos normais	Eficácia comprovada em simulações em sistemas de instalações industriais
Existentes	Combinam padrões suspeitos com enormes conjuntos de regras	Risco de elevado impacto devido ao aumento dos ataques informáticos	Utilizadas atualmente em sistemas empresariais

Ocorreram casos em que ataques informáticos avançados invadiram sistemas de controlo para emitir comandos que se faziam passar por comandos normais e eram praticamente indistinguíveis de comandos reais. Os métodos de deteção existentes que comparam o tráfego de entrada com padrões suspeitos conhecidos podem não conseguir detetar este tipo de ataques. A comparação com enormes volumes de padrões suspeitos conhecidos pode ser um processo demorado e provocar falhas nas operações do sistema de controlo.

A Mitsubishi Electric constatou que o tráfego normal do sistema de controlo em infraestruturas críticas é diferente se o sistema estiver a funcionar, não estiver a funcionar ou estiver em manutenção. Por conseguinte, a nova tecnologia utiliza regras diferentes de deteção para cada estado operacional. Com o aumento crescente dos ataques informáticos, é necessário muito tempo para gerar padrões suspeitos e procurar correspondências. No entanto, os comandos normais nos sistemas de controlo são limitados e, por isso, as regras podem ser limitadas, o que permite à nova tecnologia da Mitsubishi Electric procurar correspondências com maior rapidez e detetar ataques, ao mesmo tempo que preserva o funcionamento em tempo real dos sistemas de controlo. A empresa avaliou o tempo de processamento da deteção de ataques no sistema de controlo visado. A avaliação revelou que a nova tecnologia demora apenas 0,04 ms, em comparação com os 2,44 de uma tecnologia existente, enquanto o requisito de tempo real é de 1,44 ms.

Enquadramento

À medida que a IdC invade o campo das infraestruturas, a segurança informática torna-se cada vez mais importante para infraestruturas críticas que apoiam a sociedade. Até agora, a segurança das infraestruturas de energia elétrica, gás natural, água, produtos químicos e petróleo tem sido assegurada pelo isolamento físico, firewalls para o controlo do tráfego e por uma gestão operacional rigorosa. Nos últimos anos, contudo, tem-se registado um aumento, especialmente no estrangeiro, de ataques informáticos avançados que invadem sistemas de controlo de infraestruturas para enviar comandos prejudiciais disfarçados de comandos normais

com o intuito de causar danos, como apagões e destruição de equipamento.

Patentes

Patentes pendentes para a tecnologia anunciada neste comunicado de imprensa número sete, no Japão, e sete, no estrangeiro.

###

Sobre a Mitsubishi Electric Corporation

Com mais de 90 anos de experiência no desenvolvimento de produtos fiáveis e de alta qualidade, a Mitsubishi Electric Corporation (TÓQUIO: 6503) é um líder mundial reconhecido ao nível do fabrico, marketing e vendas de equipamento eléctrico e electrónico utilizado em comunicações e processamento de informação, exploração espacial e comunicações por satélite, electrónica de consumidor, tecnologia industrial, energia, equipamento de construção e de transporte. Integrando o espírito do seu lema empresarial, Changes for the Better, e do seu lema ambiental, Eco Changes, a Mitsubishi Electric procura ser uma empresa ecológica líder a nível mundial, enriquecendo a sociedade com tecnologia. A empresa registou vendas de grupo consolidadas no valor de 4 238,6 mil milhões de ienes (37,8 mil milhões de dólares*), no ano fiscal que terminou a 31 de março de 2017. Para obter mais informações, visite:

www.MitsubishiElectric.com

* A uma taxa de câmbio de 112 ienes para o dólar norte-americano, determinada pelo mercado de câmbio de Tóquio a 31 de março de 2017