شركة MITSUBISHI ELECTRIC
قسم العلاقات العامة
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

بالنسبة للنشرة الفورية **رقم ٣١٠٦**

إن هذا النص ترجمة للنص الإنجليزي الرسمي لهذا الإصدار الجديد، وقد تم تزويده للرجوع إليه بسهولة عند الحاجة. يرجى الرجوع إلى النص الإنجليزي الأصلي للحصول على التفاصيل و/أو المواصفات الخاصة. في حال وجود أي تعارض، فيجب اتباع محتوى الإصدار الإنجليزي الأصلي.

استفسارات العملاء

مركز البحث والتطوير لتقنية المعلومات
شركة Mitsubishi Electric
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

الاستفسارات الإعلامية

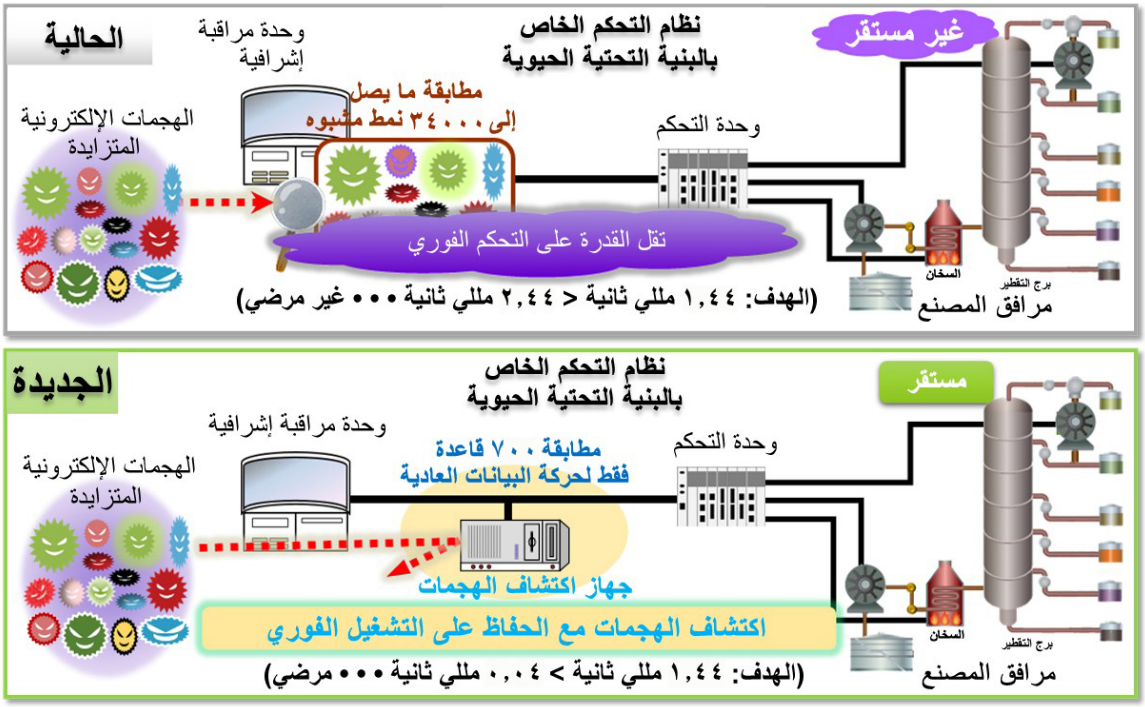
قسم العلاقات العامة
شركة Mitsubishi Electric
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

شركة Mitsubishi Electric تطور تقنية اكتشاف الهجمات الإلكترونية لأنظمة البنية التحتية الحيوية

سوف يسهم الاكتشاف الفوري للهجمات الإلكترونية بأنظمة التحكم في استقرار البنية التحتية

طوكيو، ١٧ مايو ٢٠١٧ – أعلنت شركة Mitsubishi Electric Corporation (طوكيو: ٦٥٠٣) اليوم أنها طوّرت تقنية لاكتشاف الهجمات الإلكترونية يمكنها وبسرعة تحديد حركة بيانات الشبكة التي تنحرف عن مسار الأوامر العادية المحددة مسبقًا في أنظمة التحكم الخاصة بالبنية التحتية الحيوية. وتكتشف هذه التقنية الهجمات الإلكترونية المبتكرة والمتخفية في شكل أوامر عادية تستهدف البنية التحتية الحيوية للطاقة الكهربائية والغاز الطبيعي والمياه والكيماويات والبترول دون الحد من القدرة على التحكم الفوري، ويُتوقع لهذه التقنية أن تساعد على ضمان استقرار البنية التحتية.

من المقرر تسويق البنية التحتية للطاقة الكهربائية تجاريًا بحلول السنة المالية ٢٠١٨ تقريبًا. وسيتم تطوير الاستخدامات الأخرى بالتعاون مع تحدي برامج الترويج الإستراتيجية للابتكارات التقنية (SIP) للأمن السيبراني الخاص بالبنية التحتية الحيوية.



لع به تم .

دعم تنفيذ التقنية الجديدة جزئيًا من خلال نتائج "الأمن السيبراني للبنية التحتية الحيوية" الذي ينفذه مركز Control System Security Center (CSSC). يُعد "الأمن السيبراني للبنية التحتية الحيوية" جزءًا من برنامج Strategic Innovation Promotion Program (SIP)، (برنامج تعزيز الابتكار الاستراتيجي) على مستوى الوزارات، المدعوم من مجلس العلوم، والتقنية، والابتكار، وبتكليف من منظمة New Energy and Industrial Technology Development Organization (NEDO).

الميزات الرئيسية

- تعد هذه التقنية الأولى في العالم، اعتبارًا من ١٧ مايو ٢٠١٧، لتحديد قواعد الاكتشاف استنادًا إلى الأوامر العادية لكل حالة تشغيلية لنظام التحكم وتفسير الانحرافات عن مسار الأوامر العادية كهجوم.
- يتم ضمان التشغيل الفوري لنظام التحكم تحت نظرنا عندما يكون اكتشاف الهجوم قيد الاستخدام لأن هذه التقنية لا تنطوي على عملية مطابقة الأنماط المشبوهة التي تستغرق وقتًا طويلاً.
- تساهم هذه التقنية في استقرار البنية التحتية من خلال خفض وقت الاكتشاف وضمان الحد الأدنى من التأثير على عمليات نظام التحكم التي يجب أن تنتهي في حدود زمنية معينة.

مقارنة مع التقنيات الحالية

	الطريقة	التشغيل الفوري لأنظمة التحكم	الجدوى
الجديدة	تكتشف الانحراف عن مسار قواعد الأوامر العادية التي تحددها الحالة التشغيلية	تأثير محدود بسبب القواعد الموجزة للأوامر العادية	ثبتت فعاليتها في عمليات محاكاة نظام المصنع
الحالية	تطابق الأنماط المشبوهة بمجموعات كبيرة جدًا من القواعد	خطورة وقوع تأثير عالٍ بسبب زيادة الهجمات الإلكترونية	تستخدم حاليًا في الأنظمة المؤسسية

لقد وقعت بالفعل حالات تم خلالها اختراق الهجمات الإلكترونية المتطورة لأنظمة التحكم لتصدر أوامر تبدو عادية ولا يمكن تمييزها عن الأوامر الحقيقية إلى حد كبير. ويمكن أن تخفق طرق الاكتشاف الحالية التي تقارن حركة البيانات الواردة بأنماط مشبوهة معروفة في اكتشاف مثل هذه الهجمات. كما أن المقارنة بمقدار هائل من الأنماط المشبوهة المعروفة يمكن أن تستغرق وقتًا طويلاً وقد تتسبب في تعطل العمليات التشغيلية لنظام التحكم.

لاحظت شركة Mitsubishi Electric أن حركة البيانات العادية لنظام التحكم في البنية التحتية الحيوية تختلف إذا كان النظام يعمل أو لا يعمل أو تحت الصيانة، ومن ثم تستخدم التقنية الجديدة قواعد الاكتشاف المختلفة لكل حالة تشغيلية. ونظرًا لزيادة الهجمات الإلكترونية الحاصلة على نحو مطرد، يستغرق إنشاء الأنماط المشبوهة والبحث عن أنماط متطابقة قدرًا هائلاً من الوقت. غير أن الأوامر العادية في أنظمة التحكم محدودة، ولذلك يمكن أن تكون القواعد محدودة أيضًا، الأمر الذي يتيح للتقنية الجديدة من Mitsubishi Electric البحث عن المتطابقات بسرعة واكتشاف الهجمات مع الحفاظ على التشغيل الفوري لأنظمة التحكم. وقد قامت الشركة بتقييم وقت معالجة اكتشاف الهجوم لنظام التحكم تحت نظرنا. وكشف التقييم أن التقنية الجديدة تستغرق ٠,٠٤ مللي ثانية فقط، مقارنة بـ ٢,٤٤ مللي ثانية للتقنية الحالية، في حين أن الوقت المطلوب للفورية هو ١,٤٤ مللي ثانية.

معلومات عامة

نظرًا لأن إنترنت الأشياء يسيطر على مجال البنى التحتية، يزداد الأمن السيبراني أهمية بالنسبة للبنية التحتية الحيوية التي يستند إليها المجتمع. وحتى وقتنا هذا، تم ضمان سلامة البنية التحتية للطاقة الكهربائية والغاز الطبيعي والمياه والكيماويات والنفط من خلال العزل المادي وجدران الحماية لمراقبة حركة البيانات والإدارة التشغيلية الصارمة. ومع ذلك، في السنوات الأخيرة، ازدادت وتيرة الهجمات الإلكترونية المتطورة التي تخترق أنظمة التحكم في البنية التحتية لإرسال أوامر خبيثة متخفية في شكل أوامر عادية بهدف إلحاق الضرر، مثل انقطاع التيار الكهربائي وتدمير المعدات، وهذا

الأمر ينطبق بشكل خاص في الخارج.

براءات الاختراع

يبلغ عدد براءات الاختراع قيد الانتظار المتعلقة بالتكنولوجيا المعلن عنها في هذه النشرة الإخبارية سبع براءات في اليابان وسبع براءات خارج اليابان.

###

نبذة عن شركة Mitsubishi Electric

مع أكثر من ٩٠ عامًا من الخبرة في مجال توفير منتجات موثوق بها وعالية الجودة، تعد شركة Mitsubishi Electric (طوكيو: ٦٥٠٣) شركة رائدة عالميًا معترف بها في مجال تصنيع وتسويق وبيع المعدات الكهربائية والإلكترونية المستخدمة في معالجة المعلومات والاتصالات وتنمية الفضاء والاتصالات عبر الأقمار الصناعية والإلكترونيات الاستهلاكية والتكنولوجيا الصناعية والطاقة والنقل ومعدات البناء. ومن خلال تبني روح عبارة الشركة، التغيير نحو الأفضل، وعبارتها البيئية، التغييرات البيئية، تسعى شركة Mitsubishi Electric لتكون شركة صديقة للبيئة لإثراء المجتمع بالتكنولوجيا. وقد سجلت الشركة حجم مبيعات إجماليًا للمجموعة بمقدار ٤،٢٣٨،٦ مليار ين (٣٧،٨ مليار دولار أمريكي*) في السنة المالية المنتهية في ٣١ مارس ٢٠١٧. للمزيد من المعلومات تفضل بزيارة:

www.MitsubishiElectric.com

*بسعر صرف ١١٢ ينًا للدولار الأمريكي، سعر الصرف المُعطى من قبل سوق طوكيو لتبادل العملات الأجنبية في ٣١ مارس ٢٠١٧