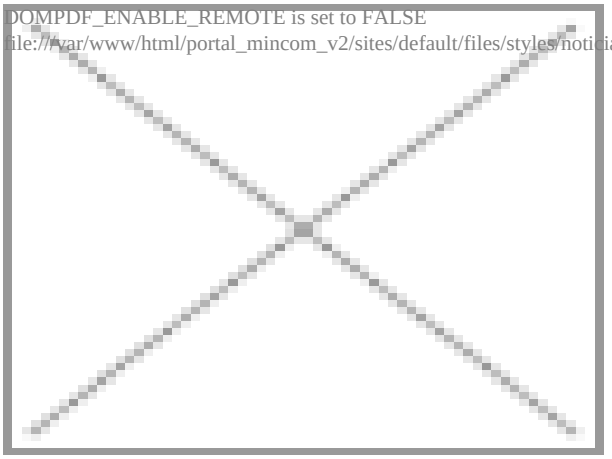
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/1570387332_ciberdelincuencia-tutoriales_en_linea.jpg



Source:
Computer World

La campaña, todavía activa, ha comprometido más de 200 sistemas de infraestructuras críticas y busca hacerse con información sensible para detectar vulnerabilidades.

La última campaña de amenazas persistentes (lo que se conoce como APT en sus siglas inglesas**)** dirigida a los proveedores TI de infraestructuras críticas se ha valido de herramientas gratuitas de Internet para dirigir ataques de *phishing*. Según la empresa CyberX, más de la mitad de las compañías objetivo se encuentran en países como Corea del Sur, China, Tailandia, Japón, Indonesia, Turquía, Alemania, Reino Unido y Ecuador. Pero, en cualquier caso, la cadena de fabricación industrial está interrelacionada en todo el mundo: un incidente en cualquiera de estos países podría exponer datos de clientes de todo el mundo.

Por el momento, se sabe que se han comprometido más de 200 sistemas y que la campaña, denominada Gangman Insudtria Style, está todavía activa. Estos atacantes buscan información. Los archivos robados podrían contener secretos comerciales, esquemas de diseño y otra información que podría permitir planificar futuros ataques, descubrir vulnerabilidades en los productos o ayudar a los clientes a obtener ventajas competitivas.

El *malware* utilizado en el ataque es una variante del famoso Separ, un buscador de credenciales de navegador y correo electrónico que existe al menos desde 2013. La nueva versión es capaz de buscar documentos e imágenes con ciertas extensiones en los sistemas y cargarlos en un servidor FTP.

Por su parte, el ataque se realiza mediante correos electrónicos muy bien diseñados que se hacen pasar por solicitudes de cotización del sector industrial y contienen archivos maliciosos. Tal y como ha informado la firma investigadora, los email incluyen una solicitud de presupuesto para diseñar una planta de energía en la República Checa que supuestamente fue enviada por una subsidiaria de Siemens, una solicitud de presupuesto para una planta en Indonesia y otra de diseño de fábricas de procesamiento de gas.

Disponible en:

https://cso.computerworld.es/cibercrimen/los-ciberdelincuentes-se-valen-... [1]

Links
[1] https://cso.computerworld.es/cibercrimen/los-ciberdelincuentes-se-valen-de-herramientas-gratuitas-en-su-ultima-campana-de-phishing-mundial