Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-002 Software Malicioso Orientado A Sistemas Punto De Venta

Cuando los consumidores compran bienes o servicios de un vendedor, la transacción es procesada a través de lo que comúnmente se conoce como Sistema Punto de Venta (POS, por sus siglas en inglés). Los sistemas de punto de venta consisten en el hardware (por ejemplo: el equipo utilizado para pasar una tarjeta de crédito o débito y la computadora o dispositivo móvil conectado a él), así como el software que le dice al hardware qué hacer con la información que captura. Al pasar una tarjeta de crédito o débito por un sistema de punto de venta, la información almacenada en la banda magnética de la tarjeta es obtenida y procesada por el ordenador o dispositivo conectado. Los datos almacenados en la banda magnética se conocen como la pista 1 y pista 2. Los datos de la pista 1 son información asociada con la cuenta real; que incluyen elementos como el nombre del titular de la tarjeta y el número de cuenta. Los datos de la pista 2 contienen información como el número de tarjeta de crédito y la fecha de caducidad.

- **Fecha de Liberación:** 2-Ene-2014
- **Ultima Revisión:** 25-Sep-2014
- **Fuente:**
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local y remoto

Sistemas Afectados

1. ## Descripción

   Desde hace algún equipo, los delincuentes cibernéticos se han enfocado a los datos de los consumidores introducidos en los POS. En algunas circunstancias, los delincuentes conectan un dispositivo físico al sistema POS para recolectar datos de la tarjeta, a esta actividad se le conoce como skimming. En otros casos, los criminales cibernéticos distribuyen malware que adquieren los datos de las tarjetas a medida que pasan a través del sistema POS, filtrando la información deseada para después enviarla al criminal. Una vez que el criminal recibe los datos, estos suelen ser traficados a otros sospechosos que utilizan los datos para crear tarjetas de crédito y débito fraudulentas.

   Como los sistemas POS están conectados a computadoras o dispositivos, suelen estar habilitados para acceder a los servicios de Internet y correo electrónico. Por lo tanto, los enlaces maliciosos o archivos adjuntos en mensajes de correo electrónico, así como los sitios web maliciosos pueden ser accedidos, y el malware puede ser descargado por el usuario final del sistema POS. El retorno de la inversión es mucho mayor para un criminal al infectar un sistema POS que recolectará los datos de las tarjetas de varios consumidores.
2. ## Impacto

   Existen varios tipos de malware POS en uso, muchos de los cuales utilizan una técnica conocida como memory scrapping o raspado de memoria para localizar datos específicos de una tarjeta. Dexter, por ejemplo, analiza los volcados de memoria de procesos específicos relacionados con el software del sistema POS que buscan los datos de las pistas 1 y 2. Stardust, una variante de Dexter, no sólo extrae la misma pista de datos de la memoria del sistema, también extrae el mismo tipo de información del tráfico de la red interna. Los investigadores conjeturan que Dexter y algunas de sus variantes podrían ser distribuidos a los sistemas de punto de venta a través de correos electrónicos de

phishing o debido a criminales que podrían estar tomando ventaja de las credenciales predeterminadas para acceder a los sistemas de forma remota, los cuales son vectores de infección comunes. Las vulnerabilidades basadas en red y en el sistema, tal como las credenciales débiles accesibles a través de Escritorio remoto, redes inalámbricas abiertas que incluyen una máquina POS y el acceso físico (no autorizado o mal usado) también pueden ser causantes de la infección.

3. Solución

Los propietarios y operadores de los sistemas POS deben seguir las mejores prácticas para aumentar la seguridad de los sistemas de punto de venta e impedir el acceso no autorizado.

Utilice contraseñas seguras: Durante la instalación de los sistemas de punto de venta, los instaladores a menudo utilizan contraseñas predeterminadas en la configuración inicial por simplicidad. Desafortunadamente, las contraseñas predeterminadas pueden ser fácilmente obtenidas en línea por los ciberdelincuentes. Es altamente recomendable que los dueños de negocios cambien las contraseñas a sus sistemas de punto de venta de forma regular, usando nombres de cuenta únicos y contraseñas complejas.

Actualice el software de las aplicaciones: Asegúrese de que las aplicaciones POS están utilizando las últimas versiones de software y los parches de seguridad. Los sistemas de punto de venta, de la misma forma que las computadoras, son vulnerables a los ataques de malware cuando las actualizaciones requeridas no se descargan e instalan regularmente.

Instale un firewall: Se debe utilizar un firewall para proteger un sistema POS de ataques externos. El firewall puede prevenir el acceso no autorizado hacia, o desde, la red privada filtrando el tráfico proveniente de crackers, virus, gusanos, u otros tipos de programas maliciosos diseñados específicamente para comprometer el sistema POS.

Utilice un antivirus: Los programas antivirus trabajan para reconocer software que se ajuste a la definición actual de malicioso e intenta restringir el acceso del malware en los sistemas. Es importante actualizar continuamente los programas antivirus para que sean efectivos en una red POS.

Restringir el acceso a Internet: Restringir el acceso a las computadoras del POS o a las terminales para impedir que los usuarios expongan accidentalmente el sistema POS a las amenazas de seguridad existentes en Internet. Los sistemas de punto de venta sólo se deben utilizar en línea para llevar a cabo las actividades relacionadas con puntos de venta y no para el uso general de Internet.

No permitir el acceso remoto: El acceso remoto permite a un usuario iniciar sesión en el sistema como usuario autorizado sin estar físicamente presente. Los criminales pueden aprovechar la configuración de acceso remoto a los sistemas de punto de venta para tener acceso a estas redes. Para prevenir el acceso no autorizado, es importante deshabilitar el acceso remoto a la red POS en todo momento.

4. Sugerencias para los usuarios afectados

Los cargos fraudulentos a una tarjeta de crédito a menudo pueden ser remediados rápidamente por la institución financiera emisora, con poco o ningún impacto para el consumidor. Sin embargo, los retiros no autorizados de una tarjeta de débito (que está vinculada a una cuenta de cheques) podrían tener un efecto en cascada sobre cheques sin fondos y cargos por pagos atrasados.

Consumidores deben cambiar constantemente los NIPs de sus tarjetas de débito. Póngase en contacto con o visitar su sitio web las instituciones financieras para obtener más información sobre las obligaciones y los programas de protección contra fraudes disponibles para sus cuentas de tarjetas de débito y crédito. Algunas instituciones ofrecen protecciones para tarjetas de débito que son similares o iguales a las disponibles para tarjetas de crédito.

Si los consumidores tienen razones para creer que la información de su tarjeta de crédito o débito ha sido comprometida, varias medidas de precaución para proteger los fondos y prevenir el robo de identidad incluyen: el cambio de contraseñas en línea y de los NIPs utilizados en los cajeros automáticos y en los sistemas de punto de venta; solicitud de una tarjeta de reemplazo; monitoreo de la actividad de la cuenta; entre otras.

Los consumidores también pueden comunicarse con la policía para denunciar incidentes de robo de identidad.

5. Referencias

All About Skimmers
A look at Point of Sale RAM scraper malware and how it works
A message from CEO Gregg Steinhafel about Target s payment card issues
Dexter and Project Hook Break the Bank (PDF)
VSkimmer trojan steals card data on point-of-sale systems
Dexter Draining blood out of Point of Sales
Point-of-sale malware infections on the rise, researchers warn
New Dexter Point-of-Sale Malware Campaigns Discovered
Happy Holidays: Point of Sale Malware Campaigns Targeting Credit and Debit Cards
Protect your identity from Target security breach
FTC Consumer Information: Identity Theft
US Department of Justice

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Lilia Elena Gonzalez Medina (lgonzalez at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47