RAM Scraping: ¿es suficiente con PCI DSS?

Con la masificación del *malware* para TPV (POS) y los incidentes de robo de datos de tarjetas de pago en Target y en las cadenas de hoteles Hilton y Trump (por solo citar algunos), uno de los primeros interrogantes que se plantean en una organización es cómo gestionar el impacto de este código malicioso para evitar la fuga masiva de datos. La respuesta más obvia sería la implementación de los controles de PCI DSS (Payment Card Industry Data Security Standard), pero aun así pueden quedar algunos elementos descubiertos, razón por la cual es indispensable complementar dichos controles con tecnologías adicionales.

David Acosta

Dentro de los diferentes controles para la protección de la confidencialidad de los datos se encuentra la criptografía, que en términos técnicos se implementa durante las fases de almacenamiento y transmisión. No obstante, la funcionalidad de estos controles se ve limitada durante la fase de procesamiento, ya que los tres componentes básicos de la criptografía –claves de cifrado y contraseñas (*passphrases*), texto en claro y texto cifrado– han de ser almacenados temporalmente en un lugar intermedio para que los algoritmos criptográficos puedan ser aplicados. Este lugar intermedio puede ser la memoria RAM (Random Access Memory) o cualquier memoria volátil definida en el sistema. Y es precisamente ese elemento intermedio el talón de Aquiles de todo el proceso y en donde los atacantes están focalizando actualmente sus esfuerzos. Un ejemplo de ello se pudo evidenciar en el ataque **HEARTBLEED** (CVE-2014-0160) [1], que mediante la manipulación de tráfico SSL le permitía a un atacante obtener volcados de segmentos de la memoria RAM de un servidor remoto que podrían contener datos sensibles y que fue causado por fallos de programación en las librerías de OpenSSL [2].

A pesar que el propio sistema operativo implementa controles de acceso para proteger los segmentos de memoria asignados a cada proceso en ejecución, es posible realizar un volcado completo o parcial del contenido de la memoria RAM de un sistema en un fichero para análisis posterior. Esta es una funcionalidad básica dentro del análisis de incidentes y el cómputo forense que permite la captura de evidencia volátil de un sistema involucrado en un incidente. Después de obtenida la información extraída de la memoria RAM se procede con la búsqueda de datos puntuales empleando por lo general expresiones regulares. Pero, ¿qué pasaría si esta misma técnica fuese empleada por un atacante para acceder a la memoria RAM de un equipo en ejecución y extraer los datos confidenciales almacenados temporalmente en texto claro, evadiendo los controles de cifrado en almacenamiento y transmisión?

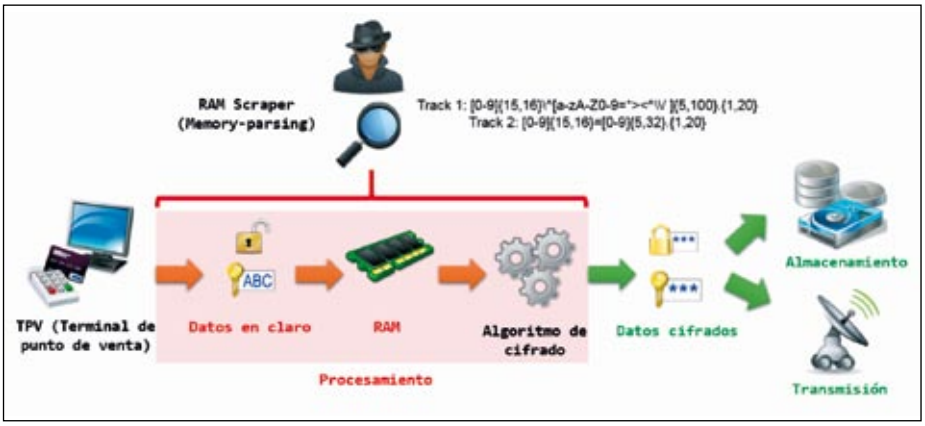

Figura 1.- Captura de datos confidenciales en RAM (RAM Scraping).

RAM Scraper y el *malware* de TPV (PoS)

Aparte de claves de cifrado y contraseñas, algunos de los datos más codiciados por los atacantes son los relacionados con tarjetas de pago (PAN completo, PIN, datos de la banda magnética y chip EMV, códigos de validación, etc.). Imaginemos el siguiente escenario: se tiene un comercio presencial, el cual cuenta con un dispositivo TPV (Terminal de Punto de Venta) conectado a un lector de tarjeta. Cuando el cliente quiere hacer su pago, desliza su tarjeta por el lector. Estos datos son enviados al TPV que a su vez se conecta con el centro autorizador para validar la compra. La comunicación entre el TPV y el centro autorizador están cifrados para prevenir que un atacante con acceso a la red pueda capturar los datos de la tarjeta. Sin embargo, durante todo este proceso los datos de la tarjeta tuvieron que ser procesados y cifrados, lo que **implica un almacenamiento temporal en RAM**. Si el atacante obtiene acceso al sistema operativo del TPV y a su memoria RAM, podría extraer los datos de la tarjeta evitando el cifrado implementado en el almacenamiento y la transmisión. Esto es lo que se denomina "**RAM Scraper**" o "**Memory-parsing**": búsqueda y extracción de datos confidenciales de la memoria RAM.

Actualmente, el crecimiento de este tipo de *malware* ha ido en aumento, perfilando sus objetivos hacia tiendas, supermercados y hoteles y siendo clasificado por las soluciones antivirus dentro de una familia específica: *malware* para TPV (POS). Uno de los más reconocidos debido a la atención mediática que generó en su momento fue **Kaptoxa/BlackPOS**. En 2012, el código fuente de este *malware* fue publicado, lo cual permitió que ciberdelincuentes mejoraran este código y lo emplearan en nuevas generaciones de *malware*. Una de sus variantes se cree que fue la que se empleó en los ataques a Target, identificados en diciembre de 2013 [3].

Siguiendo la misma línea, se han detectado versiones de *malware* para TPV cada vez más complejos, partiendo del básico **Rdasrv** (detectado en 2011) y pasando por **Dexter y Aalina** (2012), **FYSNA/ChewBacca** (2013), **Decebal**, **Soraya y JackPOS** (2014) y **PO-Seidon** (2015) entre otros, que aprovechan el almacenamiento temporal en memoria para extraer datos confidenciales, algunos inclusive empleando de forma irónica software legítimo usado para búsqueda de datos de tarjetas en tareas de cumplimiento normativo (CardRecon de GroundLabs) [4] y herramientas WYSIWYG para la creación de *malware* para TPV como **VSkimmer**. Un análisis detallado de estos pro-

gramas maliciosos y sus componentes puede ser encontrado en el *whitepaper* de Trend Micro "PoS RAM Scraper Malware: Past, Present, and Future" [5].

En junio de 2014, el US CERT publicó el documento "**Alert (TA14-002A) - Malware Targeting Point of Sale Systems**" [6], informando acerca de los problemas provenientes de esta familia de código malicioso, lo cual ya demostraba la criticidad de estos incidentes.

Las marcas de pago y el PCI SSC Vs. los ataques de *RAM Scrapers*

A pesar que los incidentes con *malware* de tipo *RAM Scraper* ya eran conocidos y ampliamente usados por usuarios maliciosos, no fue sino hasta octubre de 2008 cuando VISA –después de múltiples análisis forenses que habían identificado este tipo de código malicioso– emitió un comunicado alertando a sus comercios de una nueva variedad de *malware* que infectaba los dispositivos TPV (PoS) y podía extraer datos de tarjetas de la memoria RAM [7], dando un primer paso dentro de las acciones informativas orientadas a la detección, contención y recuperación de los sistemas infectados con este *malware*. De forma continua, VISA sigue publicando alertas relacionadas con *malware* para POS con el fin de establecer una línea base de trabajo con sus comercios y proveedores de servicio asociados:

- Dexter Malware Targeting Point-of-Sale (POS) Systems (2012) [8]
- Retail Merchants Targeted by Memory-Parsing Malware (2014) [9]
- "CHEWBACCA" POS Malware (2014) [10]
- "BlackPOS" Malware Deconstructed (2014) [11]

Las acciones recomendadas por VISA para la mitigación de este tipo de incidentes se categorizan en 5 acciones principales:

- **Seguridad de red**: desplegar controles de segmentación y separación de redes, filtrado de puertos y protocolos y la protección de sistemas publicados en redes públicas no confiables y bases de datos.
- **Seguridad del sistema TPV**: se recomienda emplear dispositivos homologados PCI PTS [12] con soporte de Secure Reading and Exchange of Data (SRED) en entornos P2PE (Point-to-point Encryption), aplicaciones que cumplan con el estándar PA-DSS, realizar búsquedas periódicas de datos de tarjetas de pago en claro y proceder con su eliminación, actualización de componentes, uso de contraseñas robustas, revisión de la integridad de binarios en el sistema a través de comparación de *checksums* (*hashes*), evitar el uso de RDP (Remote Desktop Protocol) hasta donde sea posible, 'securizar' el sistema (*hardening*), activar el registro de eventos y aplicar controles de "menor privilegio" en las cuentas de usuario.
- **Limitar el acceso administrativo**: usar controles de autenticación basados en dos factores, limitar los privilegios administrativos a los estrictamente requeridos, revisar cuentas no empleadas y evitar el uso de NTLM o LM en sistemas Microsoft.
- **Respuesta a incidentes**: desplegar un sistema SIEM (*Security Information and Event Management*) para la gestión y análisis de registros de eventos, centralizar los registros de eventos *(logs*) en servidores separados y establecer un Plan de Respuesta a Incidentes y probarlo de forma continua.
- **Gestión de terceros**: limitar el acceso únicamente al mínimo necesario a cualquier proveedor tercero al entorno de producción de la organización, establecer una DMZ (*demilitarized zone*) para las conexiones con terceros, revisar las prácticas que emplean los terceros en la gestión de datos confidenciales y analizar el impacto de sus operaciones en la organización.

Por otro lado, el PCI SSC (Payment Card Industry Security Standards Council) a través del estándar PCI DSS ha definido una serie de controles físicos, lógicos, administrativos y documentales para la protección de datos de tarjetas de pago durante el almacenamiento, el procesamiento y la transmisión. Adicionalmente a los controles ya establecidos (cortafuegos, IDS/IPS, anti*malware*, FIM, *logs*, control de acceso, autenticación de dos factores, escaneos de vulnerabilidades y pruebas de penetración, seguridad física, etc.), dicho estándar en su versión 3.1 ha incorporado un nuevo conjunto de controles para minimizar los potenciales ataques de *malware* de *RAM Scraping* desde el punto de vista de desarrollo, entre los que se encuentran:

- **Req. 6.3**: desarrollo de aplicaciones internas y externas de acuerdo con los controles de PCI DSS, basado en mejores prácticas de la industria e incorporando seguridad en el ciclo de vida de desarrollo, haciendo énfasis en el entendimiento de los procesos de gestión de datos sensibles por parte de la aplicación, incluyendo al almacenamiento en memoria.
- **Req. 6.5**: gestionar las vulnerabilidades comunes durante el proceso de desarrollo de software mediante el uso de guías de desarrollo seguro y formación a los desarrolladores, contemplando los controles de seguridad durante el almacenamiento de datos sensibles en memoria.

Controles adicionales a PCI DSS para la gestión de ataques de *RAM Scraping*

A pesar de la complejidad de PCI DSS, algunos vectores de ataque podrían aprovechar debilidades del entorno para ejecutar ataques de *RAM Scraping*, por lo que se recomienda complementar los controles de PCI DSS con los siguientes controles complementarios para minimizar la superficie de ataque y optimizar los procesos de detección:

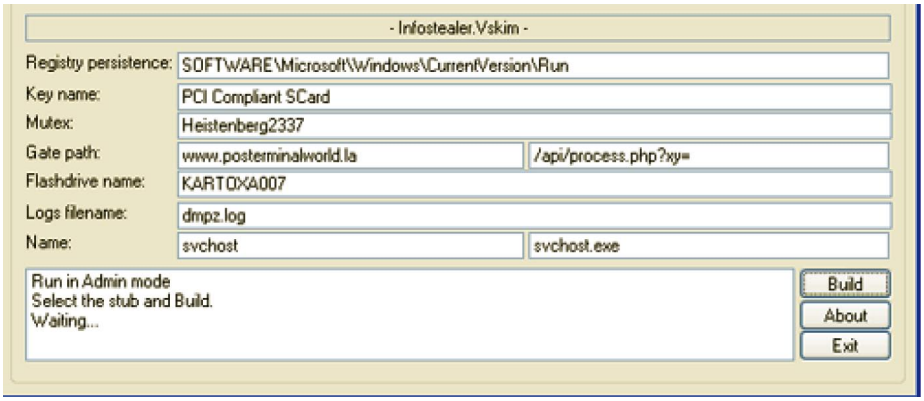

Figura 2.- Pantalla WYSIWYG de VSkimmer.

- **Búsqueda periódica de datos de tarjetas de pago**: a pesar que PCI DSS especifica que es obligatorio el almacenamiento seguro de los datos almacenados (req. 3.4), una forma óptima de identificar potenciales repositorios no autorizados de datos (incluyendo aquellos extraídos por *malware* de *RAM Scraping*) es la ejecución de búsqueda de datos de tarjetas de pago almacenados en texto plano de forma periódica en medios de almacenamiento. Para ello, se puede hacer uso de herramientas *open source* y comerciales y enlazar los resultados con el plan de respuesta a incidentes.
- **Filtrado de URL y análisis de contenido**: uno de los principales problemas en la definición de controles de filtrado de tráfico está en las restricciones del tráfico de salida. Se suele pensar que los ataques pueden venir de fuera y aplican controles restrictivos de entrada y ocurre lo contrario con el tráfico

saliente, que suele ser más permisivo. Esta falencia en controles de tráfico salientes es empleada por los potenciales atacantes para la extracción de datos sensibles (exfiltración) obtenidos mediante RAM Scraping. Para minimizar este problema, se recomienda implementar un sistema de filtrado de URL (lista blanca de URL) y análisis de contenido HTTP, SMTP y FTP, complementando los controles de filtrado e IDS/IPS requeridos por PCI DSS.

• **Uso de herramientas de DLP**: un sistema de DLP (*Data Loss Prevention* – Prevención de pérdida de datos) monitoriza continuamente todas las interfaces de entrada/salida de datos de un sistema (puertos USB, CDROM, DVD, red, discos externos, etc.) en búsqueda de patrones de datos que puedan estar relacionados con fugas de información confidencial. Instalando un sistema de este estilo en un entorno PCI DSS se optimizarán los tiempos de detección de datos extraídos por *malware* de tipo *RAM Scraper* y los controles de contención para evitar exfiltración masiva. Ver [13].

• **Monitorización basada en IoC**: después del análisis del "modus operandi" de un *malware* en particular, a través de IoC (Indicators of Compromise) se puede identificar que un *malware* está instalado en un equipo buscando elementos asociados a su comportamiento (cambios específicos en el registro, hashes de binarios, nombres de ficheros, puertos TCP/UDP abiertos, etc.). Algunas implementaciones de IoC son **OpenIoC** [14], OASIS Cyber Threat Intelligence (CTI) [15] e IODEF (Incident Object Description Exchange Format – RFC 5070 [16]). Ver [17].

• **Uso de soluciones de *whitelisting***: mediante el uso del concepto de ejecución de programas basado en listas blancas ("Whitelisting") se permite la ejecución en el sistema de únicamente aquellos binarios incluidos en una lista específica. De esta forma, cualquier programa que intente ejecutarse y que no esté en dicha lista será bloqueado. Empleando este control se refuerzan las contramedidas basadas en soluciones anti*malware* descritas por PCI DSS. Ver [18].

• **Implementación de controles de protección de datos de transacciones**: mediante el uso de un elemento denominado "**Protected Applet**", que crea un canal seguro para el almacenamiento de datos sensibles, Intel ha desarrollado una solución denominada "Intel Data Protection Technology for Transactions" [19] que evita que los datos de tarjeta puedan ser comprometidos a través de la memoria RAM del equipo o desde el sistema operativo de la terminal de pago (TPV), controlando que *malware* de RAM scraping pueda extraer datos confidenciales. Se trata de una solución que combina cifrado, aislamiento, gestión centralizada y *whitelisting* que a través de políticas gestiona el flujo de datos desde el momento de su captura hasta el envío al centro autorizador. A finales de 2015 esta tecnología empezará a ser ofrecida a través de proveedores de soluciones TPV como NCR.

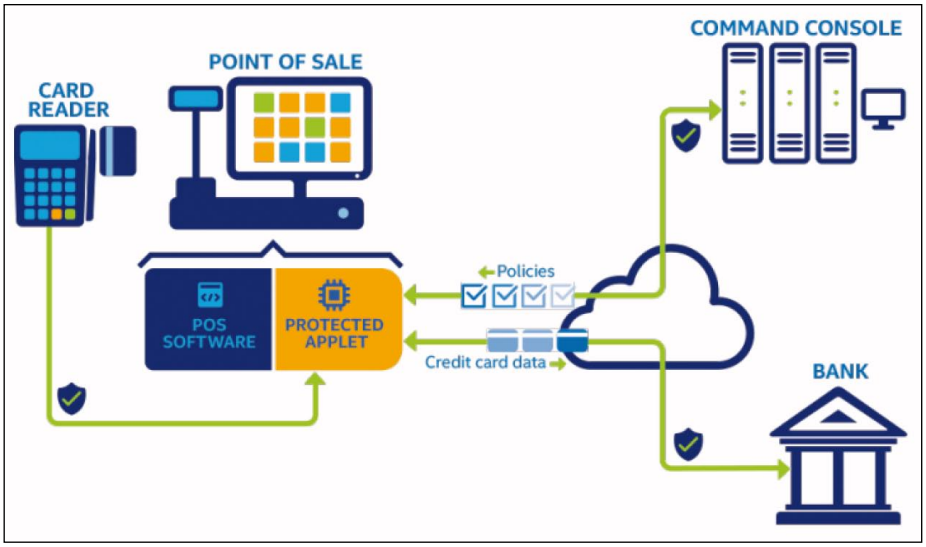

Figura 3.- Esquema de funcionamiento de Intel Data Protection Technology for Transactions.

Conclusión

Uno de los elementos más vulnerables de un sistema es su memoria, ya que es allí en donde se almacenan de forma temporal y en texto claro datos sensibles. Esto lo saben los atacantes y por eso han desarrollado *malware* orientado a la búsqueda y extracción de esta información en memoria (*RAM Scraper*). Este *malware* está atacando de forma masiva terminales de punto de venta (TPV) y cajeros electrónicos en búsqueda de datos de tarjetas de pago. Las marcas de tarjetas –individualmente y a través del PCI SSC– han desarrollado una serie de controles para minimizar el impacto de este *malware*. Sin embargo, dichos controles –a pesar de su complejidad– pueden tener algunas debilidades que deberían ser complementadas con controles adicionales, tales como DLP, uso de listas blancas, filtrado de URL y análisis de contenido y nuevas tecnologías como "protected applets". De esta forma, se reafirma que el cumplimiento de un estándar en particular no es suficiente para gestionar los riesgos que día a día surgen, por lo que es necesario desarrollar acciones adicionales dependiendo del entorno a proteger. ■

David Acosta
Consultor Senior
INTERNET SECURITY AUDITORS

REFERENCIAS

[1] http://heartbleed.com/
[2] https://www.openssl.org/news/secadv/20140407.txt
[3] http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
[4] http://blog.groundlabs.com/unauthorised-copies-of-card-recon-in-circulation
[5] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-pos-ram-scraper-malware
[6] https://www.us-cert.gov/ncas/alerts/TA14-002A
[7] http://usa.visa.com/download/merchants/debugging_software_memory.pdf
[8] http://usa.visa.com/download/merchants/alert-dexter-122012.pdf
[9] http://usa.visa.com/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf
[10] http://usa.visa.com/download/merchants/Alert-ChewbaccaMalware-030614.pdf
[11] http://usa.visa.com/download/merchants/Webinar-BlackPOSMalware-121014.pdf
[12] https://es.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
[13] http://blog.isecauditors.com/2015/07/tecnologias-dlp-y-pcidss.html
[14] www.openioc.org
[15] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[16] www.ietf.org/rfc/rfc5070.txt
[17] http://blog.isecauditors.com/2015/09/papel-de-los-ioc-en-respuesta-incidentes-seguridad-investigacion-forense.html
[18] http://www.pcihispano.com/listas-blancas-de-aplicacion-application-whitelisting-que-son-y-cuando-se-usan/
[19] http://www.intel.com/content/www/us/en/embedded/technology/security/secure-payment-transactions/overview.html