Una nota de Alex Thurber

Preguntas y respuestas comunes sobre Night Dragon **Febrero 11, 2011**

P: ¿Cómo podemos saber si nuestros clientes están infectados?

R: Asegúrese de que sus clientes actualicen los DAT de su antivirus al menos en la versión 6232 y verifique si las exploraciones a petición operan correctamente, y ejecute una exploración completa de virus en el sistema de ficheros. Evalúe ePO y lea los alertas de antivirus y los logs de red para identificar los sistemas comprometidos.

McAfee ofrece herramientas para ayudarle:

- Utilidad de Detección de Remoción del Night Dragon (Stinger)
- Exploración de Vulnerabilidad de Night Dragon

Si ha descubierto la presencia del Night Dragon en sus clientes y quiere reaccionar al incidente u obtener asistencia forense, contacte a McAfee Foundstone Professional Services. Usted también puede enviar cualquier muestra relacionada a Virus_Research@avertlabs.com o, en la Web, por la dirección McAfee Labs WebImmune.

P: ¿Existe alguna detección de red/IDS disponible?

R: Sí. En las comunicaciones de red, quédese atento a esta secuencia que indica una computadora infectada enviando una "guía" a un servidor de mando y control: "\x01\x50\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x68\x57\x24\x13". Contacte con McAfee para obtener más soporte sobre información de red.

P: ¿Es posible encontrar Night Dragon sin un análisis forense de informática?

R: Sí. La DLL es simplemente un atributo de fichero Oculto o Sistema, y se la puede encontrar por el tamaño (19-23kb), en general en la carpeta C:\Windows\System32 o C:\Windows\SysWow64. Existen otros artefactos en el sistema de archivos que pueden identificar cuando el *dropper* instaló la DLL de *backdoor*, así como los tipos de actividades realizadas por el atacante (Escritorio Remoto, Command Shell, etc.)

P: Si encontramos Night Dragon, ¿tenemos que preocuparnos con la infección de otras computadoras?

R: No. Night Dragon no lleva los recursos de infección de un *worm* y propaga a sí mismo. Night Dragon es un troyano instalado en un sistema a través de un archivo *dropper* de troyano (.exe) que un atacante copia en las computadoras – usualmente a través de una compartición de Windows.

Soluciones de McAfee para Combatir Night Dragon

Las APT son ataques sofisticados y multifacéticos que exigen una defensa coordinada y bien concebida. Estamos seguros de que McAfee es la única capaz de manejar las APT (incluso Night Dragon) y otros ataques dirigidos. Y como dije al principio, McAfee **ya añadió la protección contra Night Dragon** a sus tecnologías de seguridad más recientes. Para su consulta, presentamos aquí algunas soluciones de McAfee que, operando juntas, ayudan a combatir los ataques como Night Dragon.

- *McAfee Host Intrusion Prevention* – cuenta con un recurso de detección de APT para correlacionar y detectar RAT y la fuga de datos
- *McAfee Application Control (MAC)* – impide el *malware* porque no permite la ejecución de software que no sea aprobado.
- *McAfee Configuration Control (MCC)* – prohíbe alteraciones de configuración que no sean aprobadas.
- *McAfee Vulnerability Manager (MVM)* – detecta sistemas infectados y las debilidades de seguridad en dichos sistemas.
- *McAfee VirusScan Enterprise (VSE)* – ofrece protección con los DAT antivirus 6263 y posteriores.
- *McAfee Policy Auditor* – detecta las debilidades de seguridad en sistemas comprometidos.
- *McAfee Risk Advisory (MRA)* – permite visualizar los errores de configuración y los fallos de seguridad que permiten explotaciones.
- *McAfee Network Threat Response (NTR)* – detecta el tráfico de mando y control.
- *McAfee Network Security Manager (NSM)* – detecta tráficos malintencionados en la red y alertas, lo cual permite una reacción rápida.
- *McAfee Enterprise Firewall* – atenúa las penetraciones en la red y se puede instalar en capas para reducir los ataques internos a la red.
- *McAfee Web Gateway* – atenúa las operaciones de RAT.
- *McAfee Endpoint Encryption* – reduce la posibilidad de usar información confidencial específica.
- *McAfee Data Loss Protection (DLP)* – impide y detecta la extracción de datos confidenciales.

Los últimos años han sido turbulentos: los ataques al Google y muchas otras empresas con la Operación Aurora, ataques a infraestructuras críticas con Stuxnet, personas con acceso privilegiado robando información que llevaron a la divulgación de documentos por Wikileaks, etc.. Ahora, "Night Dragon" está listo para entrar en la batalla por los titulares.

Si quiere obtener más información sobre Night Dragon, lea el artículo Night Dragon en la bitácora del **CTO de McAfee, George Kurtz**. Allí usted encontrará información básica útil, así como un enlace a un white paper sobre Dragon Noite, escrito por expertos en seguridad de McAfee.

Gracias de antemano por su tiempo y apoyo.

Alex Thurber
Senior Vice President – Worldwide Channels, Commercial and SMB Sales
McAfee, Inc.