Pawn Storm Zero-Day Exploit

by javier - Lunes, julio 20, 2015

http://memoriasdeunsysadmin.tk/2015/07/20/pawn-storm-zero-day-exploit/

Para comenzar este artículo y, como acostumbro a hacer, primero voy a explicar las bases:

Qué es un Zero-day?

Los ataques de "Día Cero" son los que aprovechan vulnerabilidades recientemente descubiertas que aún no han sido corregidas, lo que lo convierte en algo muy peligroso que no siempre es fácil de prever o evitar.

Acerca de Pawn Storm

Operation Pawn Storm es el nombre de una operación económica y política de ciberespionaje que ha puesto sus ojos en diversas entidades, tanto militares, de gobierno, defensa, etc; fue detectado por Trend Micro, conocida firma de seguridad informática; mientras investigaban un caso en particular, descubrieron una URL sospechosa alojando un exploit utilizando esta vulnerabilidad. Encontraron también que la URL era similar a la utilizada en el ataque dirigido a la OTAN y Casa Blanca en el pasado mes de enero.

Detrás de estos ataques hay un grupo de hackers y se supone que comenzó sus operaciones en 2007 por lo menos. Se caracterizan por utilizar distintas herramientas y tácticas, en lugar de no centrarse en una sola, al momento de atacar a una víctima. De ahí su nombre, que proviene de una táctica de ajedrez, que busca llegar al rey enemigo utilizando los peones para abrir una defensa sólida.

Cómo decía antes, este grupo se concentró en objetivos militares y políticos, sobre todo los contrarios al gobierno de Rusia, por lo que hay firmes sospechas de una relación con el mismo gobierno de dicha nación. Se supo además de una campaña contra Apple; finalmente, a comienzos de este 2015, el grupo se vio nuevamente en acción, atacando la OTAN, gobiernos de Europa, Asia y Medio Oriente.

La vulnerabilidad:

De acuerdo a Trend Micro, afecta la versión 1.8.0.45 pero no anteriores como 1.6 y 1.7. En sistemas vulnerables, es posible ejecutar código arbitrario sobre java, lo que da un amplio rango de posibilidades al atacante. El exploit es detectado al descargar el archivo troj_droppr.cxc y liberar código en la carpeta del login de usuario. El parche fue publicado por Oracle el pasado 14 de julio y se recomienda instalarlo de manera urgente.

Notas finales:

Si bien no se sabía de 0-day de Java hacía bastante, es un hecho que Java no es seguro. Aún así, no es siempre tan sencillo como simplemente recomendar al usuario que lo desinstale. Por lo tanto, aquí hay

algunas notas a tener en cuenta de manera de utilizar Java sin correr mayores riesgos:

- La mayoría de las amenazas vienen de applets maliciosos que provienen de sitios maliciosos. Si el usuario necesita Java porque un programa lo utiliza, entonces tal vez no sea necesario usarlo en los navegadores y se puede deshabilitar en los mismos sin problemas. Se puede hacer desde el panel de control de java.
- Si necesitas usar Java para acceder a características de un sitio, como una intranet, no es buena idea deshabilitarlo para todos los navegadores. Pero se puede dejar deshabilitado para todos los navegadores, excepto para uno. Lo mejor en este caso es elegir un navegador secundario, que uses solamente para esos sitios que requieren java, pero dejarlo deshabilitado en tu navegador primario. Desde IE y Firefox es bastante sencillo, pero desde Chrome la opción no es tan visible. En este último, podés simplemente tipear chrome://plugins.

Si tenés dudas o necesitás asesoramiento, no dudes en contactarme, puedo ayudarte a asegurar tu equipo.

---

memoriasdeunsysadmin.tk