"El soldado" usa SpyEye para hacerse con "el gordo"

"El soldado" usa SpyEye para hacerse con "el gordo"

El ataque masivo perpetrado por “El soldado” alcanza a las principales corporaciones de Estados Unidos en su red, consigue robar 3,2 millones de dólares en 6 meses y crea vulnerabilidades en organizaciones y usuarios individuales para ataques futuros. Más de otros 90 países heridos por metralla.

Trend Micro lleva investigando durante algún tiempo las operaciones de un ciberdelincuente concreto: se trata de un joven de unos 20 años que reside en Rusia. Durante la investigación, se ha descubierto que el atacante usa varios kits de herramientas delictivos como SpyEye y ZeuS como crimeware, además de kits de explotación de vulnerabilidades como los que hacen que el ataque BlackHat SEO (manipulación en la optimización de motores de búsqueda) propague sus binarios de SpyEye/ZeuS.

Mediante el uso del kit de herramientas delictivo SpyEye, algunos muleros y un cómplice que supuestamente reside en Hollywood (EE.UU.), “El soldado”, apodo por el que se le conoce en los círculos criminales, robó más de 3,2 millones de dólares en 6 meses desde enero de 2011, lo que equivale a unos 533.000 dólares al mes o 17.000 dólares al día.

El objetivo de “El soldado” han sido principalmente usuarios estadounidenses y para aumentar el número de infecciones conseguidas en EE.UU. llegó incluso a comprar tráfico estadounidense de otros ciberdelincuentes. Además de utilizar el malware para sustraer dinero de cuentas pirateadas, también robaba las credenciales de seguridad de los usuarios.

Víctimas destacables

Mediante las direcciones IP de las víctimas que fueron registradas por el servidor de comando y control de SpyEye, se pudo determinar la red a la que se asignó la dirección IP. Entre las víctimas del ataque se ha encontrado que estaban representadas una amplia variedad de grandes organizaciones y multinacionales de EE.UU. de muy diversos sectores.

El equipo de investigación de Trend Micro cree que estas grandes organizaciones y multinacionales estadounidenses fueran el objetivo original del ataque, sino que sufrieron el impacto tras atacar a un usuario final. Los robots (sistemas infectados de las víctimas) se suelen vender a otros delincuentes que realizan otras actividades de robo de datos, por lo que estas redes quedan vulnerables para otros ataques y posibles fraudes posteriores.

Las direcciones IP de las víctimas que se identificaron en el ataque incluían aquellas pertenecientes a los tipos de organizaciones siguientes:

• Gobierno de EE.UU. (local, estatal y federal)
• Ejército de EE.UU.
• Instituciones de educación e investigación
• Bancos
• Aeropuertos
• Otras empresas (automovilísticas, multimedia, tecnológicas)

Infraestructura C&C

Su red de robots pudo comprometer aproximadamente 25.394 sistemas entre el

19 de abril de 2011 y el 29 de junio de 2011. Aunque casi la totalidad de las víctimas residían en Estados Unidos, también encontramos algunas otras repartidas por 90 países.

Además, SpyEye fue creado específicamente para sistemas Windows y Windows XP fue el principal atacado con un 57% de los equipos comprometidos. A pesar de sus mejoras en seguridad, se atacaron cerca de 4.500 equipos Windows 7.

Datos robados

Mientras que SpyEye es conocido como un troyano para datos bancarios, es suficientemente capaz de robar todo tipo de credenciales. Procesamos los datos de servicios bien conocidos y encontramos que se habían robado muchas credenciales, especialmente de Facebook.

La variante de SpyEye usada para las operaciones anteriores se detectó como TSPY_SPYEYE.EXEI. Trend Micro también se ha bloqueado el acceso a sitios remotos relacionados mediante su servicio de reputación Web.

Tal información ofrece una visión más nítida de lo que ocurre con redes robot tan prominentes como las creadas con SpyEye. A medida que se obtenga más información sobre cómo los ciberdelincuentes hacen sus negocios, cuáles son sus objetivos y qué tipos de información buscan, Trend Micro esperamos poder hallar el modo de desmantelar sus operaciones y evitar que roben el dinero, duramente ganado, de los usuarios.

Un ataque de tal escala masiva no es tan inusual para los delincuentes que usan kits de herramientas como SpyEye. Lo verdaderamente alarmante son las cantidades robadas y el número de grandes organizaciones potencialmente afectadas.