Cutlet Maker: el virus sencillo para robar ATMs

Kaspersky Lab ha descubierto un kit de malware bautizado como **Cutlet Maker** que ayuda a robar cajeros automáticos y que se encuentra disponible en el **DarkNet**. Es un kit de herramientas que "amplía significativamente el alcance de posibles ataques a **ATMs**". Se ha descubierto que **Cutlet Maker consta de tres componentes y permite vaciar el dinero de un cajero automático,** si el atacante obtiene acceso físico a la máquina.

Los cajeros automáticos siguen siendo **objetivos lucrativos para los estafadores**, que utilizan diversos métodos para obtener el máximo beneficio. Mientras que algunos confían en técnicas físicamente destructivas mediante el uso de herramientas de corte de metales, otros eligen la infección con malware, lo que les permite manipular los expendedores de dinero de la máquina desde adentro.

A principios de este año, **un socio de Kaspersky Lab le proporcionó a uno de sus investigadores una muestra maliciosa anteriormente desconocida,** que se presume fue hecha para infectar PCs dentro de los cajeros automáticos. Los investigadores sintieron curiosidad por ver si este malware o algo relacionado se podía comprar en foros subterráneos. Luego buscaron y encontraron artefactos que son únicos del malware: **una oferta publicitaria que describía una variedad de malware para cajeros automáticos en AlphaBay**, un popular sitio de la DarkNet, coincidió con la consulta y reveló que la muestra inicial pertenecía a un kit completo de código malicioso comercial creado para saquear cajeros automáticos.

Tras esto, concretan los investigadores que "una información publicada por el vendedor del malware y encontrada por los investigadores contenía no solo la descripción del software e instrucciones sobre cómo obtenerlo, sino que también proporcionaba una guía paso a paso sobre cómo usar el kit en ataques, con instrucciones y tutoriales en video".

Para comenzar el robo, los delincuentes necesitan obtener acceso directo a los cajeros automáticos para acceder al puerto USB, que se utiliza para cargar el malware. Si tienen éxito, **conectan un dispositivo USB que almacena el juego de herramientas del software**. Como primer paso, los delincuentes instalan Cutlet Maker. Como está protegido por contraseña, utilizan un programa c0decalc, instalado en otro dispositivo, como una computadora portátil o una tableta (este es un tipo de protección de "derechos de autor" instalada por los autores de Cutlet Maker para evitar que otros delincuentes lo usen de forma gratuita), todo esto tal y como concreta un comunicado de

prensa.

Se desconoce quién está detrás de este malware. Respecto a los posibles vendedores del juego de herramientas, el lenguaje, la gramática y los errores estilísticos apuntan a que se trata de personas cuyo idioma nativo no es el inglés. Konstantin Zykov, investigador de seguridad en Kaspersky Lab ha aclarado que “Cutlet Maker no requiere que el delincuente tenga conocimiento avanzado o habilidades informáticas profesionales, transformando así el hackeo de cajeros automáticos de una avanzada operación cibernética ofensiva, en otra manera ilegal más de ganar dinero que está disponible para prácticamente cualquier persona que tenga varios miles de dólares para comprar el malware”.