Silence APT, un grupo de piratas informáticos rusos, conocido por atacar organizaciones financieras principalmente en los antiguos estados soviéticos y países vecinos, ahora se encuentra atacando agresivamente a bancos en más de 30 países de América, Europa, África y Asia.

Activo desde septiembre de 2016 al menos, la campaña exitosa más reciente del grupo Silence APT fue contra el Dutch-Bangla Bank con sede en Bangladesh, que perdió más de 3 millones de dólares durante una serie de retiros de efectivo en cajeros automáticos en un lapso de varios días.

Según un nuevo informe, la empresa de seguridad cibernética con sede en Singapur, Group-IB, el grupo de piratería ya amplió significativamente sus objetivos en los últimos meses, aumentando la frecuencia de sus campañas de ataque y mejorando su arsenal.

El informe también describe la evolución del grupo de piratería de Silence desde *«piratas informáticos jóvenes y altamente motivados»* hasta uno de los grupos de amenazas persistentes avanzadas (APT) más sofisticados que ahora representa amenazas para los bancos de todo el mundo.

El grupo Silence APT actualizó su TTP único (tácticas, técnicas y procedimientos), y cambió sus alfabetos de cifrado, cifrado de cadenas y comandos para que el bot y el módulo principal evadan la detección mediante herramientas de seguridad.

> *«Además, el actor ha reescrito completamente el cargador TrueBot, el módulo de primera etapa, del cual depende el éxito de todo el ataque del grupo. Los hackers también comenzaron a usar Ivoke, un cargador sin archivos y un agente EDA, ambos escritos en PowerShell»,* dijeron los investigadores.

EDA es un agente de PowerShell, diseñado para controlar sistemas comprometidos mediante la realización de tareas a través del shell de comandos y el tráfico de túnel mediante el protocolo DNS, y se basa en los proyectos Empire y dnscat2.

Al igual que la mayoría de los grupos de hackers, Silence también se basa en correos electrónicos de phishing con macros Docs o exploits, archivos CHM y accesos directos .LNK, como archivos adjuntos maliciosos para comprometer inicialmente a sus víctimas.

Una vez en una organización víctima, el grupo aprovecha TTP más sofisticados e implementa malware adicional, ya sea TrueBot o un nuevo cargador PowerShell sin archivos llamado Ivoke, ambos diseñados para recopilar información sobre un sistema infectado y enviarlo a un servidor CnC intermedio.

Para elegir a sus objetivos, el grupo primero crea una *«lista de objetivos»* actualizada de direcciones de correo electrónico activas mediante el envío de *«correos electrónicos de reconocimiento»*, que generalmente contienen una imagen o un enlace sin una carga maliciosa.

> *«Estas campañas ya no se centraron solo en Rusia y los antiguos países soviéticos, sino que se extendieron por Asia y Europa. Desde nuestro último informe público, Silence ha enviado más de 170 mil correos electrónicos de reconocimiento a bancos en Rusia, la ex Unión Soviética, Asia y Europa»,* dice el informe.
>
> *«En noviembre de 2018, Silence trató de apuntar al mercado asiático por primera vez en su historia. En total, Silence envió alrededor de 80 mil correos electrónicos, con más de la mitad de ellos dirigidos a Taiwán, Malasia y Corea del Sur».*

Con las últimas campañas del grupo Silence ATP, desde mayo de 2018 hasta el 1 de agosto de 2019, los investigadores describieron el aumento en el daño de sus operaciones y confirmaron que la cantidad de fondos robados por Silence se multiplicó por cinco desde tu etapa inicial, estimando la pérdida total de 4.2 millones de dólares.

Además, los investigadores de Group-IB, también sospechan que TrueBot (conocido también como Silence.Downloader) y el cargador FlawedAmmyy han sido desarrollados por la misma

persona, ya que ambos malware se firmaron con el mismo certificado digital.

FlawedAmmyy loader es un troyano de acceso remoto (RAT) asociado con TA505, un grupo de amenaza independiente de habla rusa responsable de muchos ataques a gran escala que involucran ataques de correo electrónico altamente dirigidos, así como campañas masivas de mensajes multimillonarios desde al menos 2014.

> *«La creciente amenaza planteada por Silence y su rápida expansión global nos llevaron a hacer públicos ambos informes para ayudar a los especialistas en ciberseguridad a detectar y atribuir correctamente los ataques mundiales de Silence en una etapa temprana»,* agregaron los investigadores.

Los investigadores de Group-IB no compartieron los nombres de los bancos a los que atacó Silence APT, pero dijeron que el grupo atacó con éxito a los bancos en India (agosto de 2018), Rusia (febrero de 2019), Kirguistán (mayo de 2019), Rusia (junio de 2019) y Chile, Ghana, Costa Rica y bulgaria (julio de 2019).

Group-IB publicó sus hallazgos detalladamente en su informe titulado *«Silence 2.0: Going Global».* Puedes verlo aquí para más información.