



Europol arresta a 13 personas responsables del RAT Imminent Monitor

Autor: I. Stepanenko

Fecha: Monday 3rd of August 2020 05:42:46 PM



En una operación coordinada de aplicación de la ley internacional, Europol anunció el viernes el cierre de la red mundial de ciberdelitos organizada detrás de Imminent Monitor RAT, otra herramienta de piratería que permite a los piratas informáticos obtener el control completo de la computadora de la víctima de forma remota.

La operación se dirigió tanto a los compradores y vendedores de la IM-RAT (Monitor Inminente Troyano de Acceso Remoto), que fue vendida a más de 14,500 compradores y utilizada contra decenas de miles de víctimas por medio de 124 países.

La infraestructura y el sitio web de venta front-end de Imminent Monitor también se incautaron como parte de la operación, lo que hace que el troyano sea inutilizable para quienes ya lo compraron, y no está disponible para los nuevos usuarios.

Promovida como un marco legítimo de administración remota, la herramienta de piratería se utilizó mucho para acceder sin autorización a las computadoras de los usuarios específicos y robar sus credenciales de inicio de sesión para banca en línea y otras cuentas financieras.

Según el comunicado de prensa de Europol, las autoridades también ejecutaron órdenes de



Europol arresta a 13 personas responsables del RAT Imminent Monitor

Autor: I. Stepanenko

Fecha: Monday 3rd of August 2020 05:42:46 PM

búsqueda en junio de este año en contra del desarrollador y un empleado de IM-RAT en Australia y Bélgica, con el posible objetivo de identificar revendedores y usuarios de la herramienta.

Además, 13 de los clientes más prolíficos de IM-RAT también fueron arrestados en Australia, Colombia, Chequia, Países Bajos, Polonia, España, Suecia y Reino Unido.

Los funcionarios encargados de hacer cumplir la ley también confiscaron más de 430 dispositivos de los clientes y siguieron el análisis forense de una gran cantidad de computadoras y equipos de TI.

Una vez instalado, IM-RAT ofrece a los atacantes un control total sobre las computadoras de las víctimas, permitiéndoles llevar a cabo acciones maliciosas, que se enumeran a continuación, sin el conocimiento de las víctimas:

Grabación de pulsaciones de teclas

Robar datos y contraseñas de los navegadores

Espiar a las víctimas por medio de sus cámaras web

Descargar/ejecutar archivos

Deshabilitar el software antivirus y antimalware

Terminar los procesos de ejecución

Realizar muchas otras acciones

Se consideró que IM-RAT es una amenaza peligrosa debido a sus características, facilidad de uso y bajo costo, de solo 25 dólares con acceso de por vida.

«Ahora vivimos en un mundo donde, por solo 25 dólares, un ciberdelincuente del otro lado del mundo puede, con solo un clic del mouse, acceder a sus datos personales o fotografías de seres queridos o incluso espiarlo», dijo Steven Wilson, Jefe del Centro Europeo de Delitos Cibernéticos de Europol (EC3).



Europol arresta a 13 personas responsables del RAT Imminent Monitor

Autor: I. Stepanenko

Fecha: Monday 3rd of August 2020 05:42:46 PM

«La cooperación mundial en la aplicación de la ley que hemos visto en este caso es esencial para abordar los grupos criminales que desarrollan tales herramientas. También es importante recordar que algunos pasos básicos pueden evitar que seas víctima de este tipo de spyware: seguimos instando al público a garantizar que sus sistemas operativos y software de seguridad estén actualizados», agregó.

La policía cree que el número de víctimas de IM-RAT cae en decenas de miles, *«los investigadores ya han identificado evidencia de datos personales robados, contraseñas, fotografías privadas, videos y datos»*.

En una operación similar por parte de agencias internacionales, la red de delitos informáticos de otro troyano de acceso remoto, llamada Luminosity Link, también fue desmantelada hace dos años.