Masterhacks – El hacker detrás de la botnet Andromeda ha sido identificado por las autoridades como Jarets Segey Grigorevich, uno de los piratas informáticos más buscados de Europa del Este. A inicios de la semana, la Europol informó que un ciudadano bielorruso fue detenido en relación con la botnet, pero no ofreció más detalles.

Andromeda, también conocida como Gamarue o Wauchos, es una botnet que ha estado activa desde 2011 y fue publicitada en la Deep Web como un kit criminal para que cualquier hacker compre una «pieza» y distribuya malware, ataques phishing o fraudes por Internet.

Esta botnet se ha vinculado a 80 familias de malware, y se ha detectado o bloqueado en casi 1.1 millones de computadoras cada mes durante los últimos seis meses.

Mientras tanto, la empresa de seguridad informática, Recorded Future, asegura con *«alto grado de certeza»*, que el sujeto arrestado bielorriso probablemente sea Jarets Sergey Grigorevich, de 33 años de edad, también conocido como Ar3s.

El hacker radicaba en Rechitsa, cerca de Gomel, la segunda ciudad más grande de Bielorrusia, antes de ser arrestado por la policía nacional, en conjunto con una coalición mundial donde está la Europol incluida, el FBI y otras agencias de Europa. Empresas como Microsoft y ESET también colaboraron en la operación.

Según Recorded Future, Ar3s es uno de los miembros más antiguos y respetados de la clandestinidad criminal, además de ser un antiguo administrador del foro Damage Lab. Es reconocido como un experto líder en desarrollo de malware e ingeniería inversa, seguridad de redes y tecnología antivirus.

El hacker operaba desde 2004. Fue desarrollador del bot de Win32/Gamaruel HTTP, el SMTP de Windows Bruter v.1.2.3 y el servicio Swf-Inj, que roba tráfico web mediante malware.

Aunque el comité de investigación de Bielorrusia emitió un comunicado de prensa donde informa el arresto, no nombró directamente al sospechoso.