Luis Fernández Delgado
Editor
lfernandez@codasic.com

# GRU, mi cibervillano favorito

Irónicamente ha querido la casualidad que la denominación del personaje estelar de la franquicia de animación cinematográfica, **GRU** –tan gamberrete y ladronzuelo él como bien apañado técnicamente– responda al mismo acrónimo que Rusia tiene para su servicio de inteligencia exterior con más pegada: el **G**lavnoe **R**azvedytalnoe **U**pravlenie.

Esta potente unidad –de corte militar– es, según todos los indicios más plausibles de 'atribución', el emisor y, al tiempo, generoso contratante de hordas de villanos digitales que desde tiempo ha vienen hostigando a los perversos lares occidentales. Entre sus envenenados 'regalitos' figuran APT28, CyberBerkut, CyberCaliphate y Sandworm.

Las acciones cometidas por esta facción y otras de cuño similar retratan a Rusia como un incisivo actor muy tempranamente consciente de la importancia de manosear las redes en beneficio propio, ya destruyendo ya distorsionando el normal fluir informativo y digital desafecto con su sentir.

> Ciberbrigadistas internacionales –sean *Hackerberry Finns*, *chiquilihackers*, *hackerveydiles* o *hackermanitas*–, enarbolando causas pretendidamente justas y al margen de coordinarse con el ciberejército de su propio bando, no paran de adentrarse en la tundra 'cibersovietzarista'

Sus trapacerías digitales –y las de sus hermanos de propósito FSB y SVR–, que se remontan ya a un par de décadas, cobran recientemente importancia decisiva por el conflicto de esta 'tropa' con Ucrania y, por derivada, con el bando occidental que sintoniza con el estado soberano ubicado en Europa oriental.

Rememorando el mítico libro de Erich Maria Remarque "Sin novedad en el frente", cabe decir que, paradójica y dolorosamente, ahora sí las hay en esta nueva guerra del siglo XXI. Y no pocas. El conflicto ruso-ucraniano ha desatado, ya desde sus prolegómenos, que la actividad ciberbélica 'oficial' se posicionara madrugadoramente desde todos los frentes y bandos, erigiéndose en perfecto pretexto para probar un descomunal surtido de ciberacciones y arsenal digital emplazado a causar el mayor impacto posible en el contrario y, por otro lado, también a ensayar acciones inéditas de control, rastreo y destrucción cibernéticas.

La realidad percibida –en lo que ha trascendido– muestra que el resultado viene siendo desigual. Junto a mediáticos golpes de efecto con sonadas interrupciones DDoS, acciones de hackeo a 'targets' financieros e IC, sustracción y publicación de archivos, interposición de información y periodistas reivindicativos en telediarios…, también muestra la otra cara, mucho menos exótica. Me refiero al intento, *fake* mediante, de hacer colar que el presidente Zelenski pedía en línea la rendición de su país. Sin duda, el bodrioso intento de servirse de imágenes del mandatario adulteradas por parte de los Josef Goteras y Otiliov, quedará para los anales de la ciberchapucería.

Por otro lado, junto a la panoplia de acciones 'cyberarmy style' por parte de los contendientes –y agentes aliados– esperables en esta poliguerra dimensional, han convergido también otros tipos de respuesta, mucho más informales cuando no frikis, de consecuencias impredecibles. Este hecho, realmente inédito en la historia de las contiendas, hace referencia al protagonizado por hordas de 'hackers' bienintencionados y venidos arriba –ya en grupeto ya en solitario– que en plan despendole estampídico, cibervolando caóticamente por libre con ciberquincallería barata y al son emulador del himno rockero "*We will, we will hack you…*", se han estado abalanzando sobre los activos digitales del enemigo para causar el mayor estropicio posible y, si suena la flauta, también para tratar de pillar alguna de las suculentas recompensas aireadas para identificar artífices rusos de actividades maliciosas.

Lo cierto es que estos ciberbrigadistas internacionales –sean *Hackerberry Finns*, *chiquilihackers*, *hackerveydiles* o *hackermanitas*–, enarbolando sin duda causas pretendidamente justas y al margen de coordinarse con el ciberejército de su propio bando, no paran de adentrarse en la tundra 'cibersovietzarista' sin mensurar las consecuencias derivadas de sus inconscientes e impulsivas incursiones –no siempre adecuadamente anónimas– por las que, por su rastro, podría colegirse las ubicaciones y su país de origen. Y como fruto de ello sobreviniesen contundentes respuestas a fin de causar escarmiento y disuasión a futuro.

Bien está que aflore el talento lateral de la pericia hacker y que coadyuve a la causa. Sin ir más lejos, esta destreza quedó patente en la reciente RootedCON cuando algunos de sus más insignes ponentes mostraron las triquiñuelas para con la app Telegram –casualmente muy usada por la resistencia ucraniana– o las debilidades de IC eléctricas, evidenciadas por espabilados expertos de Tarlogic, ambos dos perfectos ejemplos de aplicabilidad al asunto que nos trae.

Sirva pues como reflexión final que ante los daños colaterales provocados por la oleada de ciberagresiones al por mayor –y por libre– al imperio autárquico ciberzarista, este opte por repelerlas a machete como actos de guerra o más arteramente introduzca topos prorrusos en las filas occidentales, por ejemplo en aquellas empresas de ciberprotección que, tan generosas ellas, con los brazos abiertos se han mostrado dispuestas a acoger a expertos/as ucranianos huidos…

En el sofisticado tablero digital planetario en el que nos hayamos, ¿bastará con cambiar a granel las contraseñas a nivel local y anunciar mesnadas de planes de choque sin concretar o nos pertrechamos de ciberseguridad adulta? A fin de cuentas, se trata de que nosotros también juguemos o de que jueguen con nosotros. Quilosá. ●