Dentro de la operación cibernética que quebró el liderazgo de Assad

por **K.Almassian**

A medida que avanzamos hacia una nueva fase de guerra híbrida, ya no basta con controlar los cielos o las calles. También es necesario controlar el código.

Lo ocurrido en Alepo el 27 de noviembre de 2024 no fue solo un suceso en el campo de batalla, sino un terremoto político. La rápida caída de la ciudad, y con ella, la columna vertebral de la presencia militar del gobierno de Asad en el norte de Siria, conmocionó a la región. La velocidad con la que se desintegró fue sorpresiva(..) Muchos sabían que se estaba llevando a cabo una operación militar, pero pocos comprendían la guerra invisible que se desarrollaba tras las líneas del frente.
Ahora, podemos hacerlo.

Según una investigación publicada por la revista New Lines, el colapso del Ejército Árabe Sirio en Alepo no fue simplemente resultado de ataques terrestres o con drones, sino de una ciberoperación encubierta. En el centro de este engaño no se encontraba un cohete ni un tanque, sino algo mucho más insidioso: una aplicación móvil.

“Fondo Sirio para el Desarrollo”: Un caballo de Troya.

Lanzada bajo la apariencia de una iniciativa humanitaria, la aplicación llamada STFD-686 (Syria Trust for Development), apareció en el verano de 2024. Supuestamente estaba vinculada a la primera dama Asma al-Assad y se promocionaba como un programa benéfico para apoyar a los soldados sirios con un estipendio mensual de 400.000 libras sirias (aprox. 40 dólares).

La oferta a muchos soldados que vivían en condiciones desesperadas [tras 14 años de guerra económica de EEUU contra Siria] era irresistible.

Para reclamar el pago, los usuarios debían introducir una serie de datos personales aparentemente inofensivos: nombre, fecha de nacimiento y número de integrantes de la familia. Pero luego se les solicitaba información más sensible: rango militar, designación de la unidad, coordenadas de despliegue y afiliaciones a la cadena de mando. Un experto en software, familiarizado con la operación, declaró a New Lines que la aplicación estaba diseñada para extraer suficientes datos para mapear toda la estructura del ejército sirio en tiempo real.

Pero no se detuvo allí.

La aplicación requería la integración con Facebook, lo que otorgaba acceso a gráficos sociales, mensajes privados y credenciales. Una vez instalado, se activaba el software espía "Spy Max", que otorgaba a sus operadores acceso ilimitado a llamadas telefónicas, archivos, fotos e incluso transmisiones en vivo de la cámara y el micrófono del dispositivo.
Cada teléfono con la aplicación se convirtió en un centro de vigilancia móvil, desde dentro de las propias filas del ejército.

Ataques selectivos, cadenas de mando interrumpidas

Lo que vino después fue devastador. Las fuerzas de Julani, ahora equipadas con un mapa digital de las vulnerabilidades más críticas del ejército sirio, actuaron con precisión quirúrgica. Las unidades remotas quedaron aisladas y privadas de suministros. Oficiales de alto rango vieron sus órdenes

interceptadas o revocadas. Líneas defensivas enteras en Alepo se derrumbaron no por falta de personal, sino por sabotaje estratégico .

Los soldados no tenían ni idea de que ellos mismos habían entregado las llaves.

Esto no fue un ciberataque en el sentido convencional. Fue una guerra psicológica , ejecutada mediante tecnología, que explotó la desesperación con la promesa de ayuda.

¿Quién estuvo detrás de esto?

Esa sigue siendo la pregunta del millón.

Las huellas digitales son turbias. Uno de los dominios de la aplicación estaba alojado en un servidor estadounidense, lo que genera sospechas obvias, dado el largo historial de Washington de apoyo a las facciones de Julani. Pero las pruebas están lejos de ser concluyentes. Puede haber sido una falsa bandera intencionada, destinada a despistar a los investigadores y desviar la culpa.

¿La realidad más probable? Se trató de una operación con múltiples actores, que combinó inteligencia de la oposición local, activos regionales y posiblemente experiencia cibernética extranjera. Israel, Turquía, Qatar... ninguno de ellos es ajeno a la guerra cibernética, y todos tenían un interés estratégico en debilitar a Damasco.

La nueva era de la guerra

Si algo demuestra esta operación es lo siguiente: el campo de batalla ya no es sólo un espacio físico. La guerra cibernética ya no es un complemento del poder militar convencional, sino su elemento central.

Recordemos 2020: el teléfono olvidado de un soldado sirio dentro de una unidad de defensa antiaérea rusa Pantsir permitió a Israel triangular y eliminar el sistema mediante un ataque aéreo. Eso fue una advertencia.

Lo que ocurrió en Alepo fue el cumplimiento de esa advertencia.

El ejército sirio no sólo fue superado en armamento, sino también en ataques. Y a medida que avanzamos hacia una nueva fase de la guerra híbrida, ya no basta con controlar el cielo o las calles. También hay que controlar el código.

Y en noviembre de 2024, el código ganó.

Traducción realizada con la versión gratuita del traductor DeepL.com

https://kevorkalmassian.substack.com/p/inside-the-cyber-operation-that-cracked?utm_medium=android&triedRedirect=true