Las tres vulnerabilidades zero-day que Apple abordó el 21 de septiembre de 2023 se explotaron como parte de una cadena de ataque dirigida a iPhones en un intento de distribuir una cepa de spyware conocida como Predator, la cual tenía como objetivo al ex miembro del parlamento egipcio, Ahmed Eltantawy, entre los meses de mayo y septiembre de 2023.

> *«El enfoque se produjo después de que Eltantawy hiciera públicos sus planes de postularse para la presidencia en las elecciones egipcias de 2024″,* declaró Citizen Lab, atribuyendo con alta certeza el ataque al gobierno egipcio debido a que era un cliente reconocido de la herramienta de espionaje comercial.

De acuerdo a una investigación conjunta realizada por el laboratorio interdisciplinario canadiense y el Grupo de Análisis de Amenazas de Google (TAG), se informa que esta herramienta de vigilancia mercenaria se envió a través de enlaces enviados a través de SMS y WhatsApp.

> *«En agosto y septiembre de 2023, la conexión móvil de Vodafone Egypt de Eltantawy fue constantemente elegida como objetivo a través de una inyección en la red. Cuando Eltantawy visitó ciertos sitios web que no usaban HTTPS, un dispositivo instalado en el límite de la red de Vodafone Egypt lo redirigió automáticamente a un sitio web malicioso para infectar su teléfono con el spyware Predator de Cytrox»,* explicaron los investigadores de Citizen Lab.

La cadena de ataques aprovechó un conjunto de tres vulnerabilidades: CVE-2023-41991, CVE-2023-41992 y CVE-2023-41993, las cuales permitían a un atacante malicioso evadir la validación de certificados, elevar privilegios y lograr la ejecución de código remoto en los dispositivos objetivo al procesar contenido web especialmente diseñado.

Predator, desarrollado por una empresa llamada Cytrox, es similar a Pegasus de NSO Group, permitiendo a sus clientes espiar a objetivos de interés y recolectar información delicada de

dispositivos comprometidos. Formando parte de un consorcio de proveedores de software espía llamado Intellexa Alliance, fue bloqueado por el gobierno de EE. UU. en julio de 2023 debido a su contribución en campañas de represión y otros abusos a los derechos humanos.

Se dice que el exploit, alojado en un dominio llamado sec-flare[.]com, se entregó después de que Eltantawy fuera redirigido a un sitio web llamado c.betly[.]me mediante un sofisticado ataque de inyección en la red que utilizaba el middlebox PacketLogic de Sandvine ubicado en un enlace entre Telecom Egypt y Vodafone Egypt.

> *«El contenido del sitio web de destino incluía dos iframes, el ID 'if1' contenía contenido aparentemente inofensivo (en este caso, un enlace a un archivo APK que no contenía spyware) y el ID 'if2' era un iframe invisible que contenía un enlace de infección Predator alojado en sec-flare[.]com»,* indicó Citizen Lab.

Maddie Stone, investigadora de Google TAG, caracterizó este ataque como un caso de atacante-en-el-medio (AitM) que se aprovecha de una visita a un sitio web que utiliza HTTP (en lugar de HTTPS) para interceptar y forzar a la víctima a visitar un sitio diferente operado por el actor malicioso.

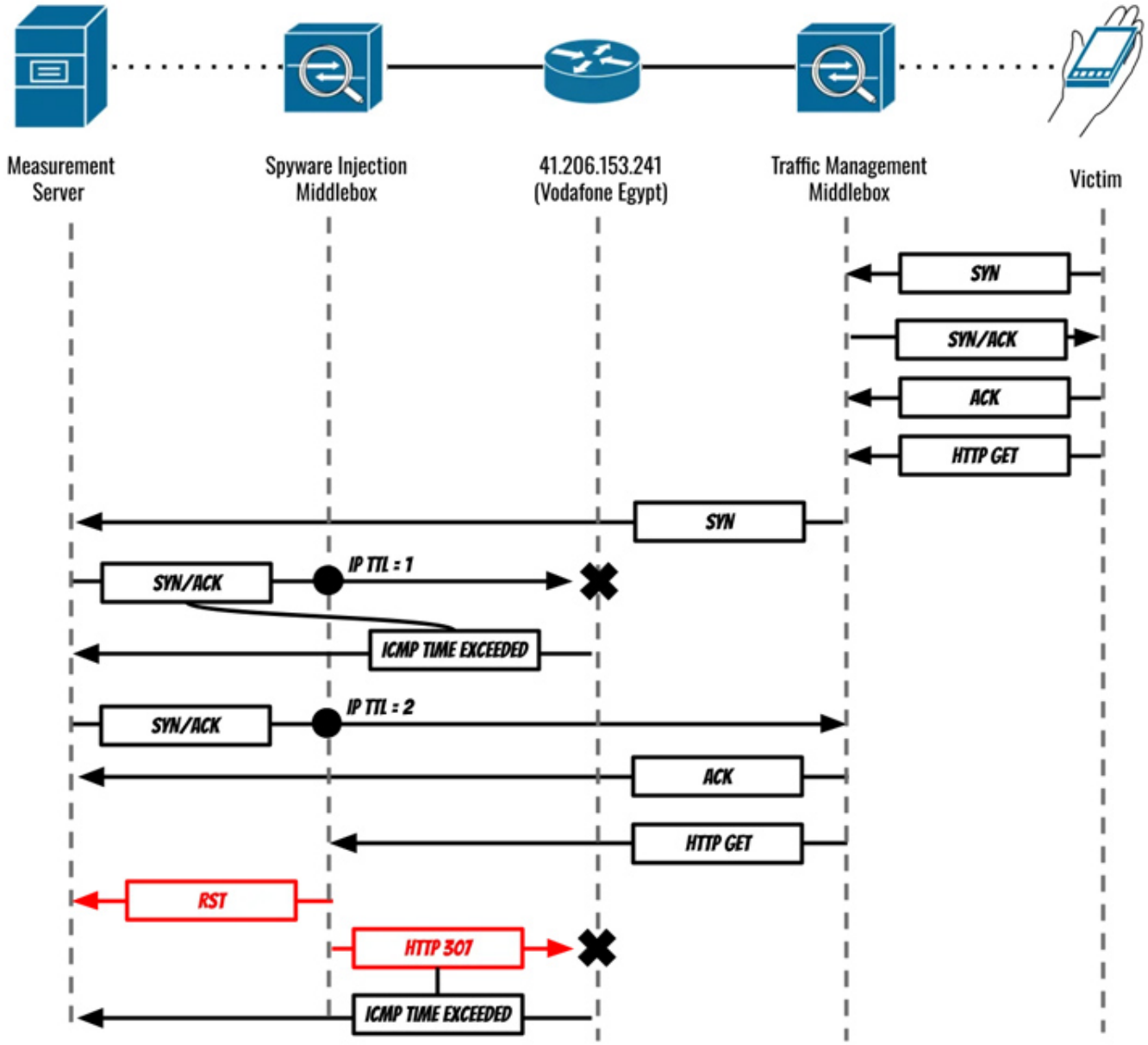
> *«En el caso de esta campaña, si el objetivo visitaba cualquier sitio 'http', los atacantes inyectaban tráfico para redirigirlos silenciosamente a un sitio de Intellexa, c.betly[.]me. Si el usuario era el objetivo esperado, el sitio redirigía al objetivo al servidor de exploit, sec-flare[.]com»,* explicó Stone.

Eltantawy recibió tres mensajes de SMS en septiembre de 2021, mayo de 2023 y septiembre de 2023 que se hacían pasar por alertas de seguridad de WhatsApp, instándolo a hacer clic en un enlace para cerrar una sesión de inicio de sesión sospechosa que supuestamente se originaba desde un dispositivo Windows.

Aunque estos enlaces no coincidían con la huella digital del dominio mencionado anteriormente, la investigación reveló que el spyware Predator se instaló en el dispositivo aproximadamente 2 minutos y 30 segundos después de que Eltantawy leyó el mensaje enviado en septiembre de 2021.

También recibió dos mensajes de WhatsApp el 24 de junio de 2023 y el 12 de julio de 2023, en los que una persona que afirmaba trabajar para la Federación Internacional de Derechos Humanos (FIDH) solicitaba su opinión sobre un artículo que hacía referencia al sitio web sec-flare[.]com. Estos mensajes quedaron sin leer.

Google TAG también informó de una cadena de explotación que utilizó una vulnerabilidad de ejecución de código remoto en el navegador web Chrome (CVE-2023-4762) para distribuir Predator en dispositivos Android utilizando dos métodos: la inyección AitM y mediante enlaces de un solo uso enviados directamente al objetivo.



CVE-2023-4762, una vulnerabilidad de confusión de tipos en el motor V8, fue reportada de forma anónima el 16 de agosto de 2023 y parcheada por Google el 5 de septiembre de 2023, aunque la compañía considera que Cytrox/Intellexa podría haber utilizado esta vulnerabilidad como zero-day.

De acuerdo con una breve descripción en la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST, CVE-2023-4762 se refiere a una *«confusión de tipos en V8 en Google Chrome antes de 116.0.5845.179 [que] permitía a un atacante remoto ejecutar código arbitrario a través de una página HTML manipulada».*

Estos nuevos hallazgos, además de destacar el uso indebido de herramientas de vigilancia para atacar a la sociedad civil, resaltan las debilidades en el ecosistema de telecomunicaciones que podrían ser explotadas para interceptar el tráfico de red e inyectar malware en los dispositivos de las víctimas.

> *«A pesar de los avances significativos logrados en los últimos años en la 'criptografía de la web', todavía hay ocasiones en que los usuarios visitan sitios web sin HTTPS, y una sola visita a un sitio web sin HTTPS puede resultar en una infección por spyware»*, señaló Citizen Lab.

Se recomienda a los usuarios que corren riesgo de amenazas de spyware debido a su identidad o actividades que mantengan sus dispositivos actualizados y habiliten el Modo de Bloqueo en iPhones, iPads y Macs para protegerse contra este tipo de ataques.