Investigadores de seguridad cibernética revelaron hoy un nuevo ataque a la cadena de suministro, dirigido a los jugadores en línea comprometiendo el mecanismo de actualización de NoxPlayer, un emulador gratuito de Android para PC y Mac.

Nombada «Operation NightScout» por la compañía de seguridad cibernética ESET, la campaña de vigilancia altamente dirigida implicó la distribución de tres familias de malware distintas a través de actualizaciones maliciosas personalizadas a víctimas seleccionadas con sede en Taiwán, Hong Kong y Sri Lanka.

NoxPlayer, desarrollado por BigNox con sede en Hong Kong, es un emulador de Android que permite a los usuarios jugar videojuegos móviles en PC, con soporte para teclado, gamepad, grabación de guiones y múltiples instancias. Se estima que cuenta con más de 150 millones de usuarios en más de 150 países.

Las primeras señales del ataque en curso se originaron alrededor de septiembre de 2020, desde entonces el compromiso siguió hasta que se descubrió *«actividad explícitamente maliciosa»* el 25 de enero, lo que llevó a ESET a informar el incidente a BigNox.

> *«Basándonos en el software comprometido en cuestión y el malware entregado que exhibe capacidades de vigilancia, creemos que esto puede indicar la intención de recopilar inteligencia sobre objetivos involucrados en la comunidad de jugadores»,* dijo Ignacio Sanmillan, investigador de ESET.

Para llevar a cabo el ataque, el mecanismo de actualización de NoxPlayer sirvió como vector para entregar versiones troyanizadas del software a los usuarios que, luego de la instalación, entregaron tres cargas útiles maliciosas diferentes como Gh0st RAT para espiar a sus víctimas, capturar pulsaciones de teclas y recopilar información confidencial.

De forma separada, los investigadores también encontraron casos en los que el actualizador BigNox descargó binarios de malware adicionales como Poisonlvy RAT desde servidores remotos controlados por el actor de la amenaza.

> *«Poisonlvy RAT solo se detectó en actividad luego de las actualizaciones maliciosas iniciales y se descargó de la infraestructura controlada por el atacante»,* dijo Sanmillan.

Lanzado por primera vez en 2005, Poisonlvy RAT se ha utilizado en varias campañas de malware de alto perfil, sobre todo en el compromiso de 2011 de los datos RSA SecurID.

Cuando se señaló que los cargadores de malware utilizados en el ataque compartían similitudes con el compromiso del sitio web de la oficina presidencial de Myanmar en 2018 y una violación de seguridad de una universidad de Hong Kong el año pasado, ESET dijo que los operadores detrás del ataque violaron la infraestructura de BigNox para alojar el malware, con evidencia que alude al hecho de que su infraestructura API podría haber sido comprometida.

> *«Para estar seguro, en caso de intrusión, realice una reinstalación estándar desde un medio limpio. Para los usuarios de NoxPlayer no infectados, no descarguen ninguna actualización hasta que BigNox envíe una notificación de que han mitigado la amenaza. Además, la mejor práctica sería desinstalar el software»*, dijo Sanmillan.