Investigadores de seguridad cibernética detallaron este viernes una nueva metodología para identificar a los autores de exploits que utilizan sus características únicas como huella digital para rastrear otros exploits desarrollados por ellos mismos.

Al implementar esta técnica, los investigadores pudieron vincular 16 exploits de escalada de privilegios locales (LPE) de Windows a dos vendedores de día cero, Volodya, antes llamado BuggiCorp y PlayBit, también conocido como luxor2008.

> *«En lugar de centrarnos en un malware completo y buscar nuevas muestras de la familia o el actor del malware, queríamos ofrecer otra perspectiva y decidimos concentrarnos en estas pocas funciones que fueron escritas por un desarrollador de exploits»*, dijeron Itay Cohen y Eyal Itkin de Check Point Research.

Esto se basa en crear una huella digital de un exploit para artefactos específicos que pueden vincularla de forma única a un desarrollador. Podría ser el uso de valores codificados, nombres de cadenas o incluso cómo se organiza el código y se implementan algunas funciones.

Check Point dijo que su análisis comenzó en respuesta a un *«ataque complicado»* contra uno de sus clientes cuando se encontraron con un ejecutable de malware de 64 bits que explotaba la vulnerabilidad CVE-2019-0859 para obtener privilegios elevados.

Al darse cuenta de que el exploit y el malware fueron escritos por dos grupos diferentes de personas, los investigadores utilizaron las propiedades del binario como una firma de caza única para encontrar al menos otros 11 exploits desarrollados por el mismo desarrollador llamado «Volodya» o «Volodimir».

> *«Lo más probable es que equipos específicos o personas que se especializan en una función concreta se encarguen de encontrar una vulnerabilidad y explotarla de forma fiable. A los desarrolladores de malware, por su parte, no les importa*

> *realmente cómo funciona, solo quieren integrar este módulo»*, dijeron los investigadores.

Volodya se ha relacionado anteriormente con la venta de 0-days de Windows a grupos de ciberespionaje y bandas de crimeware, por valores que oscilan entre 85,000 y 200,000 dólares.

El principal de los 0-days se trató de un exploit LPE que aprovechó una corrupción de memoria en «NtUserSetWindowLongPtr» (CVE-2016-7255), que ha sido ampliamente utilizado por operadores de ransomware como GrandCrab, Cerber y Magniber. Ahora, se cree que Volodya anunció el LPE de día cero en el foro de piratería Exploit.in en mayo de 2016.

En total, fueron identificados cinco exploits de día cero y seis one-day desarrollador por Volodya durante 2015-2019. Posteriormente, se empleó la misma técnica para identificar cinco exploits LPE más de otro desarrollador conocido como PlayBit.

Al afirmar que las muestras de exploits compartían similitudes en el nivel de código para otorgar privilegios de SISTEMA al proceso deseado, los investigadores dijeron que *«nuestros dos actores fueron muy consistentes en sus respectivas rutinas de explotación, cada uno siguiendo su método favorito».*

Además, Volodya parece haber cambiado sus tácticas durante los años intermedios, y el desarrollador pasó de vender los exploits como código fuente incrustable en el malware a una utilidad externa que acepta una API específica.

Además de los grupos de ransomware, se ha descubierto que Volodya atiende a una clientela extensa, incluido el troyano bancario Ursnif y grupos APT como Turla, APT28 y Buhtrap.

> *«Los clientes de APT, Turla, APT28 y Buhtrap, se atribuyen comúnmente a Rusia y es interesante descubrir que incluso estos grupos avanzados compran exploits en lugar de desarrollarlos internamente. Este es otro punto que refuerza aún más*

> *nuestra hipótesis de que los exploits escritos pueden tratarse como una parte separada y distinta del malware»,* dijo Check Point.

Con los ataques cibernéticos expandiéndose en alcance, frecuencia y magnitud, el uso de la firma de código de un desarrollador de exploits como medio para rastrear a los malos actores podría proporcionar información muy valiosa sobre el mercado negro de exploits.

> *«Cuando Check Point encuentra una vulnerabilidad, demostramos su gravedad, la informamos al proveedor correspondiente y nos aseguramos de que esté parcheada para que no represente una amenaza. Sin embargo, para las personas que comercian con estos exploits, es una historia completamente diferente. Para ellos, encontrar la vulnerabilidad es solo el comienzo. Necesitan explotarla de forma confiable en tantas versiones como sea posible, para monetizarla a satisfacción del cliente»,* dijo Cohen.
>
> *«Esta investigación proporciona información sobre cómo se logra eso y los compradores en este mercado, que a menudo incluyen actores del estado-nación. Creemos que esta metodología de investigación se puede utilizar para identificar autores de exploits adicionales».*