El kit de explotación RIG (EK) alcanzó una tasa de explotación exitosa históricamente alta de casi 30% en 2022, según nuevas investigaciones.

«RIG EK es un programa motivado financieramente que ha estado activo desde 2014», dijo la empresa suiza de seguridad cibernética PRODAFT.

> *«Aunque aún se tiene que cambiar sustancialmente sus exploits en su actividad más reciente, el tipo y la versión del malware que distribuyen cambia constantemente. La frecuencia de actualización de muestras varía de actualizaciones semanales a diarias».*

Los kits de explotación son programas que se usan para distribuir malware a un gran número de víctimas aprovechando las vulnerabilidades de seguridad conocidas en el software de uso común, como los navegadores web.

El hecho de que RIG EK se ejecute como un modelo de servicio significa que los hackers pueden compensar financieramente al administrador de RIG EK por instalar el malware de su elección en las máquinas de las víctimas. Los operadores de RIG EK emplean principalmente publicidad maliciosa para garantizar una alta tasa de infección y una cobertura a gran escala.

Como resultado, los visitantes que usan una versión vulnerable de un navegador para acceder a una página web controlada por un hacker o a un sitio web comprometido pero legítimo, son redirigidos mediante un código JavaScript malicioso a un servidor proxy, que a su vez, se comunica con un servidor de explotación para entregar el exploit de navegador apropiado.

El servidor de exploits, por su parte, detecta el navegador del usuario analizando la cadena User-Agent y devuelve el exploit que *«coincide con las versiones de navegador vulnerables predefinidas».*

> *«El ingenioso diseño del Exploit Kit le permite infectar dispositivos con poca o ninguna interacción por parte del usuario final. Mientras tanto, su uso de servidores proxy hace que las infecciones sean más difíciles de detectar»*, dijeron los investigadores.

Desde que apareció en escena en 2014, se ha observado que RIG EK ofrece una amplia gama de troyanos financieros, ladrones y ransomware como AZORult, CryptoBit, Dridex, Raccoon Stealer y WastedLoader. La operación recibió un gran golpe en 2017 después de una acción coordinada que desmanteló su infraestructura.

Las campañas recientes de RIG EK se han centrado en una vulnerabilidad de corrupción de memoria que afecta a Internet Explorer (CVE-2021-26411, puntuación CVSS: 8.8) para implementar RedLine Stealer.

Otras vulnerabilidades del navegador armadas por el malware incluyen CVE-2013-2551, CVE-2014-6332, CVE-2015-0313, CVE-2015-2419, CVE-2016-0189, CVE-2018-8174, CVE-2019-0752 y CVE-2020-0674.

Según datos recabados por PRODAFT, el 45% de las infecciones exitosas en 2022 explotaron CVE-2021-26411, seguido de CVE-2016-0189 (29%), CVE-2019-0752 (10%), CVE-2018-8174 (9%) y CVE-2020-0674 (6%).

Además de Dridex, Raccoon y RedLine Stealer, algunas de las familias de malware notables distribuidas mediante RIG EK son SmokeLoader, PureCrypter, IceID, ZLoader, TrueBot, Ursnif y Royal Ransomware.

Además, se dice que el kit de explotación atrajo tráfico de 207 países, reportando una tasa de éxito del 22% solo en los últimos dos meses. La mayor cantidad de compromisos se encuentran en Rusia, Egipto, México, Brasil, Arabia Saudita, Turquía y varios países de Europa.

> *«Curiosamente, las tasas de intentos de explotación fueron las más altas los martes, miércoles y jueves, y las infecciones exitosas tuvieron lugar los mismos días de la semana»,* dijeron los investigadores.

PRODAFT, que también logró obtener visibilidad en el panel de control del kit, dijo que hay unos seis usuarios distintos, dos de los cuales (admin y vipr) tienen privilegios de administrador. Un perfil de usuario con el alias «pit» o «pitty» tiene permisos de subadministrador y otros tres (lyr, ump y test1) tienen privilegios de usuario.

«admin» también es un usuario ficticio reservado principalmente para crear otros usuarios. El panel de administración, que funciona con una suscripción, se controla mediante el usuario *«pitty».*

Sin embargo, un error de seguridad operacional que expuso el servidor git llevó a PRODAFT a eliminar el anonimato de dos de los hackers: un ciudadano de Uzbekistán de 31 años llamado Oleg Lukyanov y un ruso que se hace llamar Vladimir Nikonov.

También se evaluó con mucha confianza que el desarrollador del malware Dridex tiene una *«relación cercana»* con los administradores de RIG EK, debido al manual adicional.

> *«En general, RIG EK ejecuta un negocio muy fructífero de exploit-as-a-service, con víctimas en todo el mundo, un arsenal de exploits altamente efectivo y numerosos clientes con malware en constante actualización»,* dijeron los investigadores.