CVE 2018-8174

Nueva campaña de phishing contra el sector financiero

BCSC_ALERTA_ CVE_2018-8174

www.basquecybersecurity.eus

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Julio 2018

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se facilita a título meramente informativo y orientativo. En ningún caso el Basque Cybersecurity Centre será o podrá ser responsable solidaria o subsidiariamente, de cualesquiera responsabilidades, daños, pérdidas y costos sufridos o incurridos, directos o indirectos, fortuitos o extraordinarios que pudieran derivarse del uso de la información que en el mismo se contiene.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. SOBRE EL BCSC

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en la Agencia Vasca de Desarrollo Empresarial (en adelante Grupo SPRI), sociedad dependiente del Departamento de desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. RESUMEN EJECUTIVO

Se ha identificado una campaña de phishing dirigida a instituciones financieras con documentos maliciosos que explota CVE-2018-8174, una vulnerabilidad de ejecución remota de código en el motor VBScript de Microsoft Windows que se publicó en mayo de 2018.

Se atribuye a COBALT SPIDER con una confianza media, basada en Tácticas, Técnicas y Procedimientos (TTPs) asociados con este grupo.

3. ANÁLISIS TÉCNICO

3.1 Detalles generales

En particular, algunos de los esquemas de phishing, el uso del generador de documentos de explotación y el targeting están en línea con ataques anteriores observados por este grupo.

Confirmados objetivos en Rusia, Turquía, Georgia y Kazajstán. También hay indicios de que esta actividad forma parte de una campaña más amplia dirigida a las víctimas internacionales, incluidas algunas de países occidentales.

Los documentos de explotación se entregan directamente como archivos adjuntos o como segundas etapas que se descargan cuando un usuario busca una URL incrustada en un correo electrónico de phishing.

Los correos electrónicos de phishing están diseñados para atraer a los destinatarios a hacer clic en el enlace o abrir el archivo adjunto mediante el uso de señuelos en varios idiomas relacionados con transacciones financieras fraudulentas, anuncios del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), fraude en cajeros automáticos e infracciones de licencias de software.

Los objetivos identificados son tres bancos rusos, un banco en Turquía, una compañía de seguros en Georgia y un banco en Kazajstán, principalmente en la primera oleada.

Los documentos maliciosos llevan marcas de herramientas que explotan también los CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 y CVE-2018-4878) y también pueden ser una variante del ThreadKit.

ThreadKit son exploits de documentos de Microsoft Office que ofrece una gran variedad de malware y es utilizado por múltiples grupos delictivos. Utiliza VBS y se actualiza con nuevos exploits a medida que se lanzan.

Se ha visto descarga de software ilegal como Smokeloader, Hancitor, y Trickbot, así como payloads específicos de CobaltGang.

En algunos casos, se observó al actor (COBALT SPIDER) entregando correos electrónicos a través de un servidor VPN operado por la empresa sueca AzireVPN. Sin embargo, en la mayoría de los casos, los correos electrónicos fueron enviados desde servidores alojados por Clodo, un proveedor ruso de Servidores Privados Virtuales (VPS).

Los mismos servidores también se utilizaron para alojar documentos de explotación en los casos en que se incluyeron enlaces en los correos electrónicos de suplantación de identidad (phishing), lo que confirma que estos hosts están controlados por el agente con una confianza media a alta.

4. MITIGACIÓN / SOLUCIÓN

• RECOMENDACIÓN

Actualizar los parches de seguridad lanzados por Microsoft, los CVE son:

- CVE-2018-8174
- CVE-2017-11882
- CVE-2018-0802
- CVE-2017-8570
- CVE-2018-4878

4.1. Indicadores de compromiso

- Dominios

  rossgosreestr[.]ru

  mcafeecloud[.]us

  ecb-europa[.]info

  dieboldnixdorf[.]us

- URLs

  http://167.99.249[.]73/2018.txt

  http://cloud-direct[.]biz/2018.txt

  http://documents.total-cloud[.]biz/version.txt

  http://mail.halcyonih[.]com/2018.txt

  http://secure.n-document[.]biz/2018.txt

  http://tlms.com[.]au/2018.txt

- Hash

1d5dff124e56f82e91302e451d914bdc9a0d83b36271df684f9ab8de4f2fccf5

40c69370b87d673e3123814e1d1328ce2078f75bddf72805805b2327923b38ec

7762bfb2c3251aea23fb0553dabb13db730a7e3fc95856d8b7a276000b9be1f5

90fc3b91a67fea6982e59191772c4e88b589f6d4747e8e94ec0234e956daa5f6

a1f3388314c4abd7b1d3ad2aeb863c9c40a56bf438c7a2b71cbcff384d7e7ded

af9ed7de1d9d9d38ee12ea2d3c62ab01a79c6f4b241c02110bac8a53ea9798b5

e4081eb7f47d76c57bbbe36456eaa4108f488ead5022630ad9b383e84129ffa9

e566db9e491fda7a5d28ffe9019be64b4d9bc75014bbe189a9dcb9d

- Regla de YARA

```
CYSOC_BT_SPAIN_CVE_2018_8174 : threatkit exploit cve_2018_8174 delivery_document
{
  meta:
    copyright ="CYSOC BT SPAIN"
    description = "ThreadKit Exploit Document for CVE-2018-8174"
    reports = "CSA-18497"
    version = "201806281416"
    last_modified = "2018-06-28"
  strings:
    $ = "68005400740050003a002f002f00"
    $ = "e 0c9 ea79f9bace118c82 00a a004b"
  condition:
    all of them
}
```

- TAGS

CVE-2018-8174 | COBALT SPIDER | Targeted eCrime | eCrime | Financials | ThreadKit | spear phishing | Insurance | VB Script