| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00249-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de noviembre de 2021 |
| Última revisión | 15 de noviembre de 2021 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware, los que están circulando en el ciberespacio nacional y representan un riesgo para los sistemas informáticos, así como para los usuarios en general.

**CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso**.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## IoC hash

Hash SHA-256 de los archivos adjuntos en los correos electrónicos:

| N° | HASH | Tipo Malware |
|---|---|---|
| 1 | 17a3f0a447a29ab04d4a194eb79772fe7641da5bbe8b0cf5781bf4e922f55c47 | MSIL/CoinMiner |
| 2 | 1495ed8cf2d45165ddad9769a6585a70f5f2b164639dd6412c08edddd196a70d | MSIL/Kryptik |
| 3 | 93a3a49cd87bcb3d89898fb0d8dfbd448a9b02ca7e5a6fee4b3e4d0104da3d6d | MSIL/CoinMiner |
| 4 | e61b55673e3c393632da298946136f6946f3aa4d6bc95ad7e8e42bdf1234c775 | PossibleThreat |
| 5 | 440928f7612b8ea263648a6cad8aa4fcbbdcf4c2908e2ca3b0427a0c1ed11e4c | MSIL/Kryptik |
| 6 | e22593115e2132bb409ff706cee9341dfbd8990c7ab61b6dae718eec0ac6d019 | MSIL/GenKryptik |
| 7 | be0d20e365851dfb49d756ff9f173bcd952bbe258badd2daf8d68a2ba024e569 | MSIL/GenKryptik |
| 8 | 57fa17734750caa76f4d3fd8cd1ec9db69e54af6dd1603fd4f5a158fc15b958e | MSIL/GenKryptik |
| 9 | d9e316e8a8e478b6e88a76153c0dfcc2f4bcbcbb631ba0516818f3f365cdad45 | MSIL/GenKryptik |
| 10 | 7adcc25316101df9dab7f17a72bcede23253b09e3af4aa1e4472020b8cce8b2a | W32/Agent |
| 11 | 42db0461ac868e01c599a0aed146f50419ba7afc270a6da394900492763a94a8 | W32/Agent |

## IoC nombre de archivo

Nombres de archivos con código malicioso:

| N° | Archivo Malware |
|---|---|
| 1 | Cceeoj9#234.zip |
| 2 | cliff.kuhfeldt's CV.7z |
| 3 | payment request documents.7z |
| 4 | Remittance_advice.zip |
| 5 | specs. in English.r17 |

## IoC servidor SMTP

Direcciones IP de servidor SMTP. Se debe tener consideración que podrían aparecer direcciones de Servicios Cloud reconocidos, ya que este apartado informa desde donde salieron los correos electrónicos maliciosos.

| N° | IP | Etiqueta de sistema autónomo | ASN |
|---|---|---|---|
| 1 | 185.222.57.202 | RootLayer Web Services Ltd. | AS 51447 |
| 2 | 212.193.30.31 | Des Capital B.V. | AS 213035 |
| 3 | 37.0.11.45 | Delis LLC | AS 211252 |
| 4 | 94.130.135.43 | Hetzner Online GmbH | AS 24940 |

## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.15 10:00:00 -03'00'