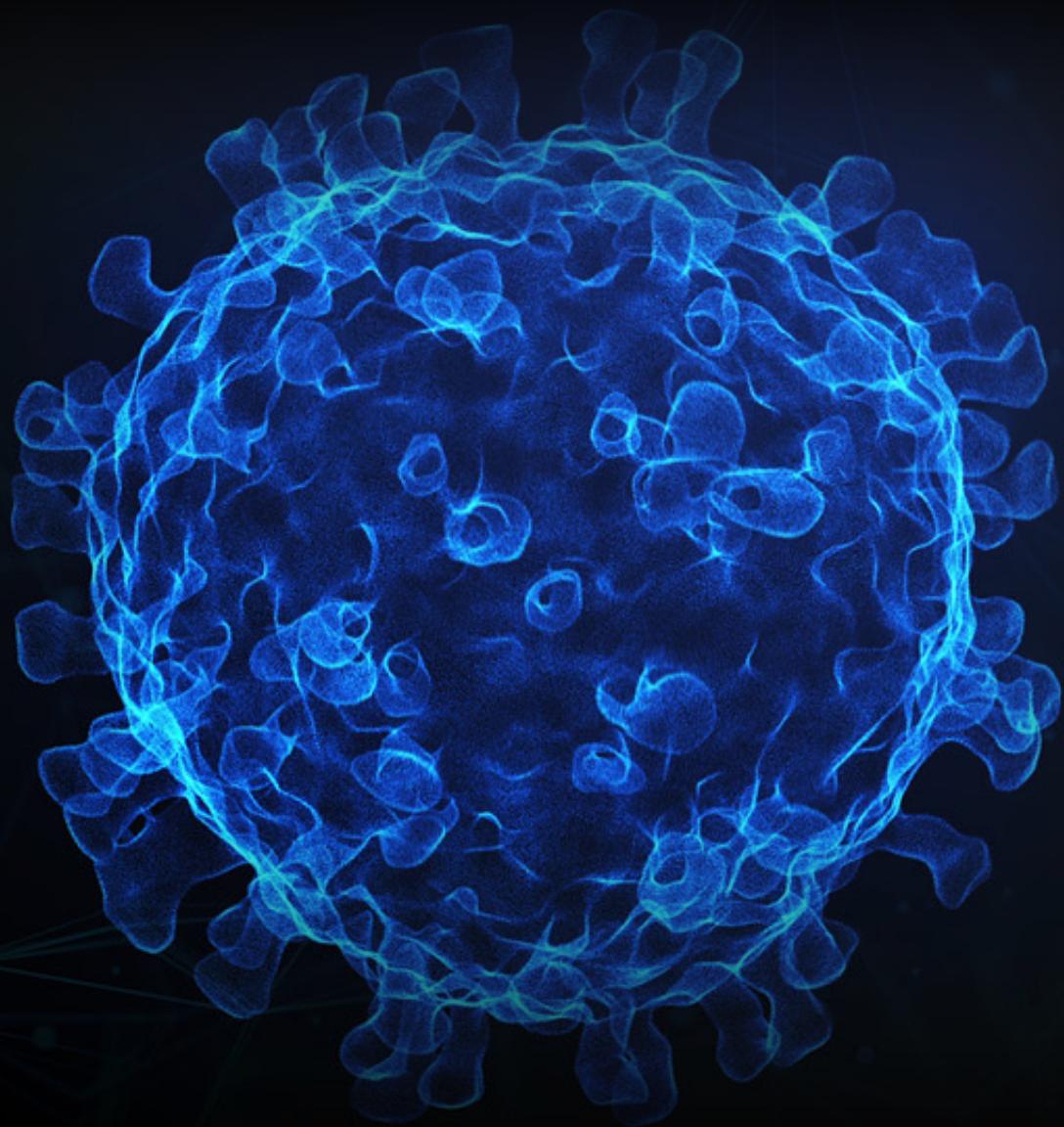




Ilustración en 3D del coronavirus COVID-19 en microscopio electrónico



# REPORTE DE CIBERINTELIGENCIA OPERACIÓN : "APAKUY"

Bono Universal & Bono Independendiente

Mayo 2020 •

# Índice [Mayo]

|  |     |
|--|-----|
| Introducción                                       | [1] |
| Antecedentes                                       | [2] |
| Método para obtener el bono de forma legal         | [3] |
| Método para obtener el bono de forma <b>ilegal</b> | [4] |
| Acciones tomadas                                   | [5] |
| Línea de tiempo                                    | [6] |
| Conclusiones                                       | [7] |
| Consultores  | [8] |

**"APAKUY"**

*Verbo. Llevar algo para sí, con o sin el consentimiento del dueño.*



## Introducción [1]

**DeepSecurity** es una empresa de ciberseguridad con reconocimiento nacional e internacional la cual realiza constantes investigaciones en distintos temas respecto a ciberseguridad y ciberinteligencia.

Es importante indicar que **DeepSecurity** no ha recibido ningún beneficio económico fruto de esta investigación y su único fin es reportar y demostrar fallos de ciberseguridad que venían siendo usados por ciberdelincuentes para beneficiarse con los bonos ofrecidos por el gobierno peruano. **DeepSecurity** es una empresa 100% peruana y de una trayectoria intachable. El presente informe se basa en las buenas prácticas de seguridad para aplicaciones web “OWASP Top 10” como estándar para tipificar las vulnerabilidades presentadas.

**Es importante indicar que DeepSecurity no ha recibido ningún beneficio económico.**

## Antecedentes [2]

Durante nuestras investigaciones de ciberinteligencia, encontramos un grupo en Telegram donde se mencionan distintos temas desde hacking de aplicaciones web hasta el robo de tarjetas (carding). Al realizar el análisis de los indicios encontramos que algunos de los 550 ciberdelincuentes miembros de este grupo publicaban información sobre un fallo en la web del bono universal que permitía apropiarse del bono de los beneficiarios.

Como investigadores profesionales de ciberseguridad, seguimos la ruta de las evidencias dejadas por los ciberdelincuentes para validar si la vulnerabilidad era real.

## Método para obtener el bono de forma legal [3]

### Paso 1

Ingresar: DNI y fecha de emisión del DNI.

**Consulta si eres beneficiario del bono familiar universal.**

 **87654321**

 **29/02/2001**

No soy un robot

  
reCAPTCHA  
Privacidad - Condiciones

Select all squares with traffic lights  
if there are none, click skip

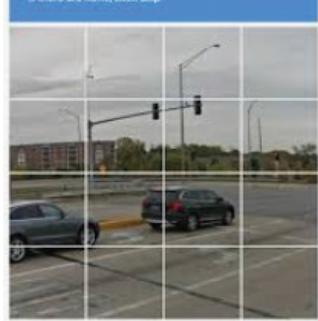


Imagen 1 - Ventana de validación de número DNI y fecha de emisión

### Paso 2

Responder las consultas de autenticación basados en datos de RENIEC, como nombre del padre de la madre y lugar de nacimiento.

Responde las siguientes preguntas para validar tu identidad:

**Mamá**

**Papá**

¿Cuál es tu fecha de nacimiento?



Imagen 2 - Ventana de validación de datos RENIEC

### Paso 3

Ingresar un número de teléfono donde se enviará la clave SMS para el cobro del bono.

Sólo se permiten números telefónicos del Perú.

Operador

# Operador

Escribe tu número de celular

**9909000**

9 / 9

Confirma tu número de celular

**9909000**

9 / 9

Imagen 3 - Ventana para registro de numero de teléfono

### Paso 4

El código SMS enviado es usado en el cajero automatico (ATM) para realizar el retiro del dinero.



Imagen 4 - Envío de SMS con clave para cobro

## Método para obtener el bono de forma **ílegal** [4]

El mayor problema de seguridad que tuvo el sistema del bono está relacionado a la opción de “captcha”, la cual no funcionaba.

### ¿Qué es captcha?

Es ese recuadro con imágenes que dice "No soy un robot".

### ¿Para qué sirve?

Cada vez que vas a enviar la consulta de DNI, la opción “captcha” solicita que resuelvas un desafío basado en imágenes que pertenecen a la misma categoría, una vez que lo resuelves recién el formulario puede ser enviado. Sin embargo, el “captcha” encontrado en el sitio web de Bono Universal (**bonouniversalfamiliar.pe**) y Bono Independiente (**bonodependiente.pe**) no estuvo bien implementando, motivo por el cual se podía enviar el formulario de forma masiva (ilimitada) usando herramientas automatizadas.

### ¿Qué quiere decir esto?

Que un robot (programa que envia peticiones masivas) podría intentar autenticar en el portal N números de DNI sin tener que resolver la adivinanza de imágenes, obteniendo todos los números DNI con bono universal del Perú.

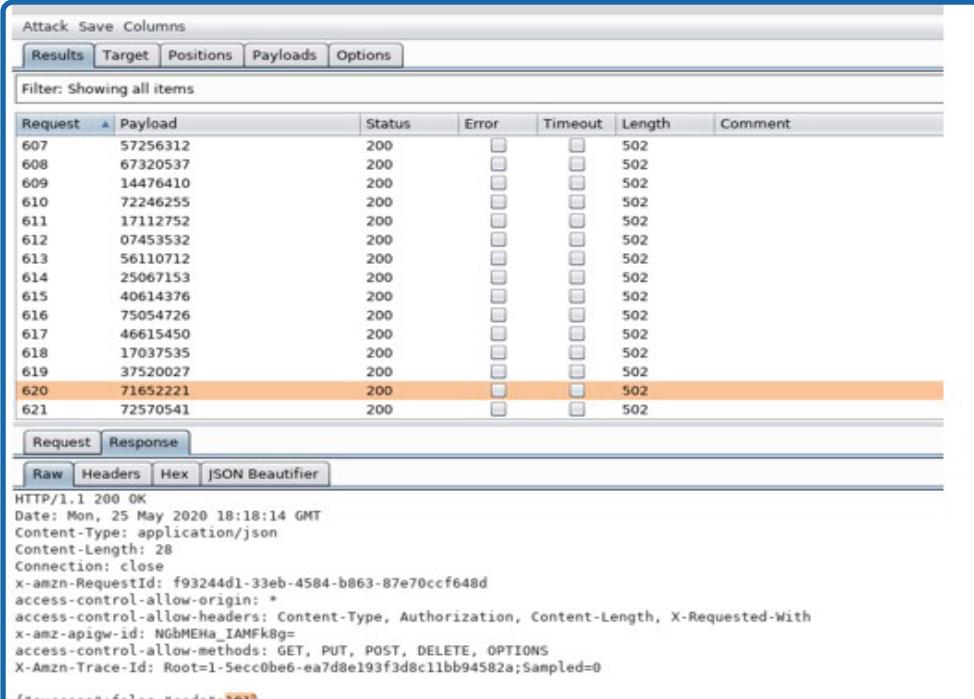
Este tipo de vulnerabilidades se encuentra bien identificada como “Broken Authentication OWASP A2:2017” según lo indicado en las guías de buenas prácticas de seguridad conocidas como “OWASP TOP 10”, que es un estándar reconocido internacionalmente.

[ [https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/Top\\_10-2017\\_A2-Broken\\_Authentication](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication) ]

## Paso 1

El equipo de **DeepSecurity** generó una lista de 2500 números de DNI usando un programa (script) desarrollado en python\*. Envío la lista de 2500 peticiones y en segundos se pudo confirmar la vulnerabilidad. Cuando el servidor del bono recibía un DNI que era beneficiario del bono, se recibía como respuesta el número 101 mientras que cuando se consultaba un DNI no beneficiado devolvía el número 100.

Hasta ese punto, el equipo de **DeepSecurity** podía encontrar los DNI que si eran beneficiarios. Posteriormente hicimos el mismo ataque enfocados en la fecha de emisión del DNI, como el servidor no contaba con la protección anti peticiones robotizadas, realizamos peticiones masivas sobre la fecha de emisión hasta confirmar que pudieron ser halladas. 2500 DNIs y 1500 fechas pueden ser probadas en menos de 5 minutos.



| Request | Payload  | Status | Error                    | Timeout                  | Length | Comment |
|---------|----------|--------|--------------------------|--------------------------|--------|---------|
| 607     | 57256312 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 608     | 67320537 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 609     | 14476410 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 610     | 72246255 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 611     | 17112752 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 612     | 07453532 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 613     | 56110712 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 614     | 25067153 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 615     | 40614376 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 616     | 75054726 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 617     | 46615450 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 618     | 17037535 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 619     | 37520027 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 620     | 71652221 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |
| 621     | 72570541 | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 502    |         |



Imagen 5 - Consulta masiva de 2,500 DNI donde respuesta 101 (confirma bono)

## Paso 2

Hasta este punto se había autenticado al beneficiario (ciberdelincuente) en el sistema del bono universal, posteriormente el sistema te pide que ingreses datos como:

- Nombre del Padre
- Nombre de la Madre
- Fecha de nacimiento

Que en realidad no profundizaremos mucho más en mencionar cómo conseguir esta información dado que el cibercriminal podría inclusive comprar de forma ilegal una ficha de la víctima por menos de S/.20.

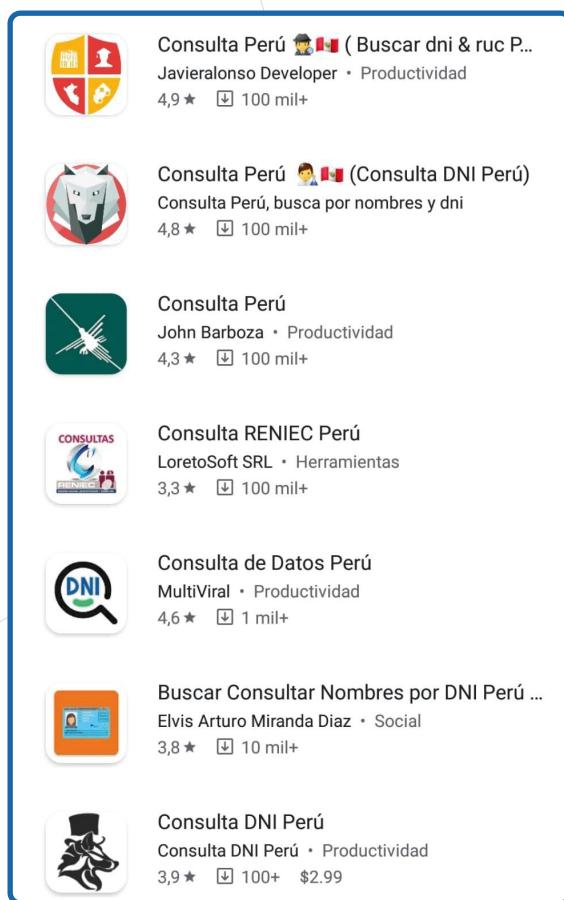


Imagen 6 - Aplicaciones ilegales con información de ciudadanos peruanos.



Imagen 7 - Fuentes información de los beneficiarios conseguida de forma ilegal



Imagen 8 - Búsquedas de fichas reniec en internet.

### Paso 3

El tercer problema de seguridad que tenía el portal era que el teléfono móvil que se debía registrar podía ser de cualquier persona y no necesariamente debía estar a nombre del beneficiario, por lo que el ciberdelincuente podía poner su teléfono y recibir la clave SMS para cobrar el bono. Es importante mencionar en esta parte que OSIPTEL pide al menos un DNI para registrar un teléfono, por lo que podría ser un interesante método de verificación.

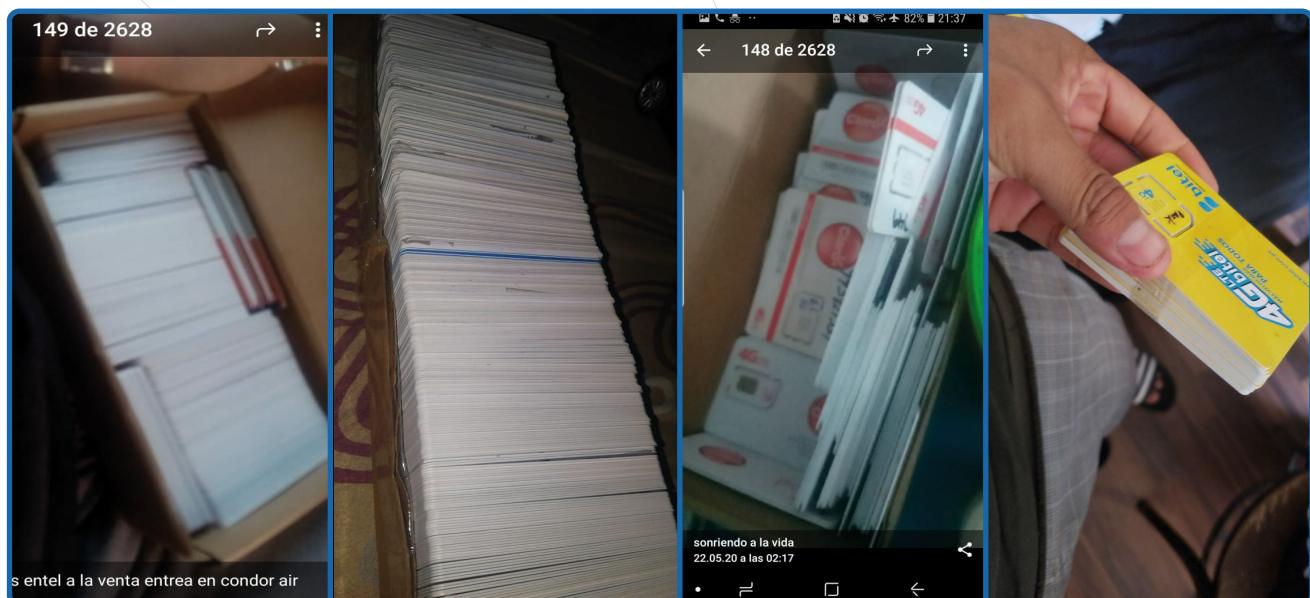


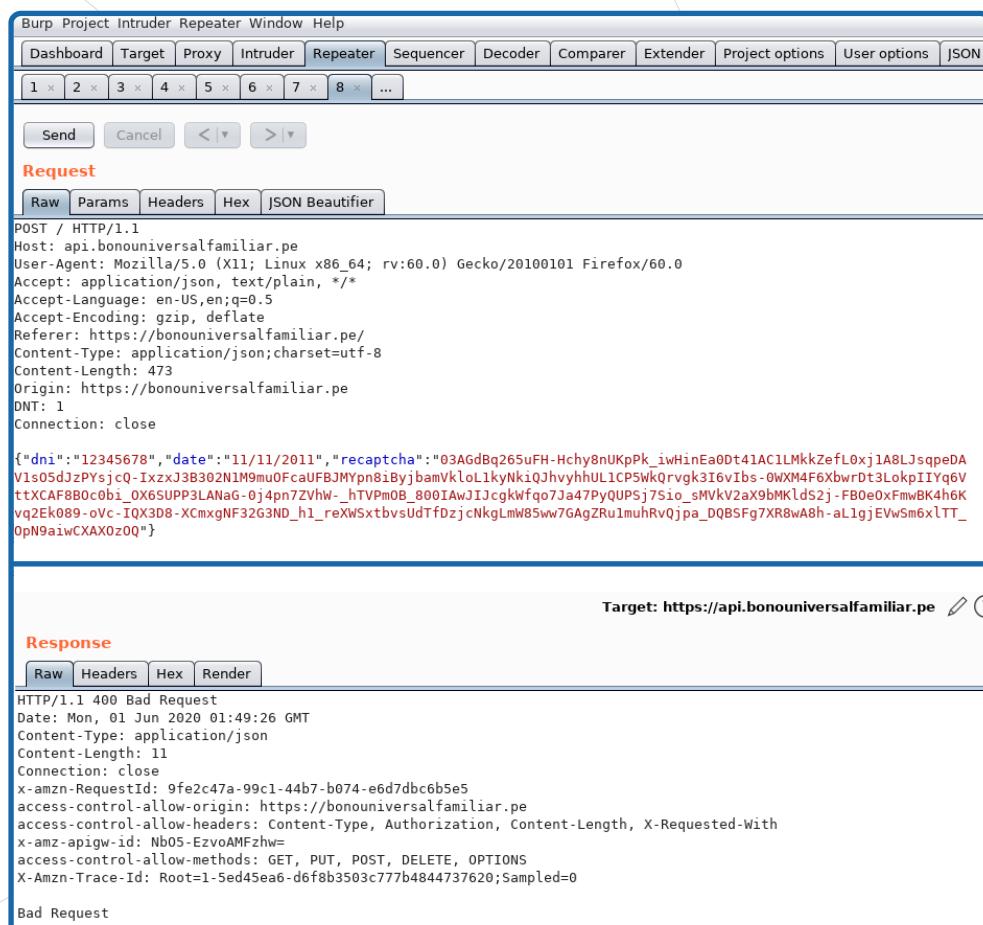
Imagen 9 - Evidencias de chips utilizados y ofrecidos en el canal de ciberdelincuentes.



Imagen 10 - Evidencias de claves de pago divulgadas en el canal de ciberdelincuentes.

## Acciones tomadas [5]

Luego del reporte realizado por **Deepsecurity** al Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional (PECERT), se pudo confirmar el día miércoles 27 de mayo, que la vulnerabilidad relacionada al control de captcha ya había sido solucionada.



The screenshot shows the Burp Suite interface. In the Request tab, a POST request is made to `HTTP/1.1 POST / HTTP/1.1`. The headers include `Host: api.bonouniversalfamiliar.pe`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0`, `Accept: application/json, text/plain, */*`, `Accept-Language: en-US,en;q=0.5`, `Accept-Encoding: gzip, deflate`, `Referer: https://bonouniversalfamiliar.pe/`, `Content-Type: application/json; charset=utf-8`, `Content-Length: 473`, `Origin: https://bonouniversalfamiliar.pe`, `DNT: 1`, and `Connection: close`. The JSON payload is a long string starting with `{"dni": "12345678", "date": "11/11/2011", "recaptcha": "03AGdBq265uFH-Hchy8nUKpPk_iwHinEa0Dt41AC1LMkkZefL0xj1A8LJsqpeDAV1s05d3zPYsjcQ-IxzJ3B302N1M9muOfcaUFBJMYPn81ByjbamVkoL1kyhUlQjhvyhhUL1CP5WkQrvhgk3I6vibs-0WXM4F6XbwrtD3LokpIIYg6VttXCAFBB0cobi_Oj4pn7ZvhW_hTVpmOB_800IAwJ1CgkWfqo7Ja47PyQUPSpj7Sio_sMvkV2ax9bMKlds2j-FB0eo0xFmwBK4h6Kvq2Ek089-oVc-IQX3D8-XCmxgNF32G3ND_h1_reXwSxtbvsUdTfDzjcNkgLmW85ww76AgZRulmuhRvQjpa_DQBSFg7XR8wA8h-aLlgjEVwSm6xlTT_0pN9aiwCXAX0zQ0"}`. In the Response tab, a 400 Bad Request response is shown with the message `Bad Request`.

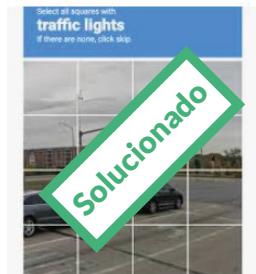


Imagen 11 - Respuesta HTTP "bad request" confirma la vulnerabilidad ya fue solucionada.

También se puede observar que se agregó la opción “Registrar tu caso” en la parte superior de la página bono universal.



Imagen 12 - Página web anterior (cache) descargada de archive.org



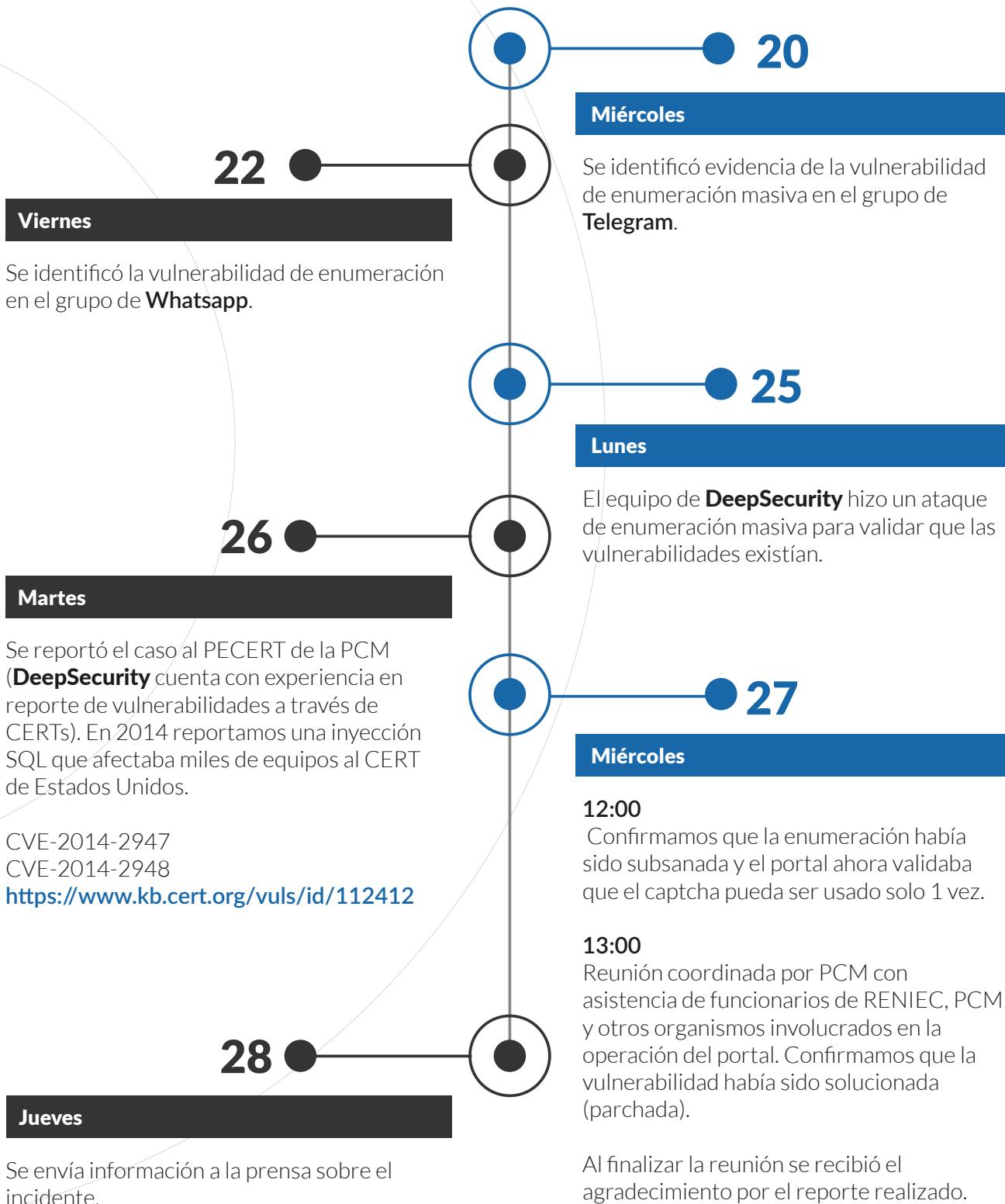
Imagen 13 - Nueva Opción "Registra tu Caso"

 A screenshot of a modal window titled 'REGISTRAR UN CASO - BONO FAMILIAR UNIVERSAL'. The window lists six reasons for case registration, each in a blue box: 1. Beneficiario con problema de salud que requiere cambio de perceptor del bono; 2. Beneficiario en el extranjero que requiere cambio de perceptor del bono; 3. Beneficiario fallecido que requiere cambio de perceptor del bono; 4. Beneficiario preso que requiere cambio de perceptor del bono; 5. Beneficiario con discapacidad que requiere cambio de perceptor del bono; and 6. Beneficiario posiblemente ha sido suplantado. Below these options are two numbered points: 6.1. Nunca registré número de celular y en la plataforma muestra que ya hay un número de celular registrado; and 6.2. Registré mi celular y antes que llegue mi código lo perdí o me lo robaron.

Imagen 14 - Detalle de opciones indica "Beneficiario posiblemente ha sido suplantado"

## Línea de tiempo [6]

**Mayo 2020**



## Conclusiones [7]

1. A fin de evitar que las aplicaciones web puedan ser usadas para conseguir de forma masiva DNI con bono asignado y luego usar la misma página web con el fin de obtener la fecha de emisión o fecha de nacimiento de beneficiario, recomendamos se haga una adecuada implementación de control de CAPTCHA actualmente ya en uso.

El control de captcha presentando en ambos sitios web mencionados;

- **Bono Universal Familiar** (<https://bonouniversalfamiliar.pe>)
- **Bono Independiente** (<https://bonoindependiente.pe>)

Al obtener esta información, se puede iniciar el trámite de registro de datos.

2. Durante el registro del beneficiario, se utiliza como método de validación los datos RENIEC con el objetivo de autenticar el usuario. Sin embargo, estos datos pueden ser encontrados en fuentes abiertas o en distintas aplicaciones de Internet. Este punto hace viable el cambio de datos incluido el nuevo número de celular, al cuál se envía la clave de cobro vía SMS. En ese caso recomendamos implementar controles de información cruzada con otras entidades.
3. Así mismo se hace la observación al registro del número de celular, el que no cuenta con una validación de pertenencia al beneficiario del bono.

Este tipo de vulnerabilidades se encuentra bien identificada como “Configuración de Seguridad Incorrecta OWASP A2:2017” según lo indicado en las guías de buenas prácticas de seguridad conocidas como “OWASP TOP 10” que es un estándar reconocido internacionalmente.

## Consultores [8]

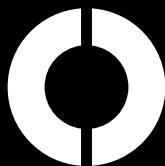
La investigación fue realizada por miembros del equipo de ciberinteligencia de **DeepSecurity** del Perú.

La información y demostraciones que se proporcionan en este documento son solo para fines informativos y educativos.

El mal uso de la información en este documento puede dar lugar a cargos penales contra las personas en cuestión. **DeepSecurity** no será responsable en caso de que se presenten cargos penales contra cualquier persona que utilice indebidamente la información de este documento para infringir la ley.

No deberá hacer un mal uso de la información para obtener acceso no autorizado.

Toda la información en este reporte está destinada ayudar a prevenir los ataques de piratería informática.



**DEEP SECURITY**

### Colaboradores DeepSecurity

#### Investigación Técnica:

Mauricio Urizar y Camilo Galdos

#### Sobre DeepSecurity

DeepSecurity publica artículos originales, informes y publicaciones periódicas que proporcionan información para las empresas, el sector público y sociedad en general. Nuestro objetivo es aprovechar la investigación y la experiencia de toda nuestra organización de servicios profesionales para avanzar en el desarrollo sobre un amplio espectro de temas de interés para ejecutivos y líderes del gobierno.

DeepSecurity 100% peruana.

Sobre esta publicación, no debe utilizarse como base para cualquier decisión o acción que pueda afectar su negocio. Antes de tomar cualquier decisión o tomar cualquier medida que pueda afectar su negocio, debe consultar a un profesor calificado.

La información obtenida durante la encuesta se tomó "tal cual". Deepsecurity no serán responsable de ninguna pérdida sufrida por cualquier persona que tome esta publicación para basar sus decisiones.

Copyright © 2020 Deep Security del Perú SAC. Todos los derechos reservados.