UNIVERSIDAD DE CALDAS

FACULTAD DE INGENIERÍAS

DECANATURA

COMUNICADO ABIERTO

Manizales, 27 de Abril de 2018.

La Facultad de Ingenierías como responsable del Sistema de Consulta para la designación de Rector, informa a la comunidad en general, que el día miércoles 25 de abril a las 8:01 minutos el dominio https://votaciones-ucaldas.co, fue atacado por un *bot* informático que afecta la capacidad de respuesta a las solicitudes de acceso. Técnicamente este tipo de ataque es denominado de Denegación de Servicios Distribuido (*DDoS*). Esta secuencia colapsó los servidores con cientos de miles de peticiones por segundo; tales acciones se pueden estimar mas no prevenir con absoluta certeza, pues, ciertamente, este vector de ciberataques ha resultado ser el más exitoso a infraestructuras críticas, sitios de la Registraduría, portales Gubernamentales, DANE, procesos electorales, aplicaciones como Whatsapp, Twitter, Facebook, entre otras.

Gracias a la habilidad de los ingenieros, la arquitectura diseñada, el despliegue en el AWS (Amazon Web Services), la configuración de los protocolos y el modelo de programación, el sistema pudo re-configurarse y recuperarse en un tiempo aproximado de una hora, lo cual resalta el nivel de respuesta de nuestro equipo técnico y humano. Esto, permitió focalizar el esfuerzo para detectar la fuente, la técnica empleada en dicho ataque y así implementar los controles en tiempo real que permitieron contener al máximo la interferencia del servicio.

Cabe aclarar, que el ataque **NO COMPROMETIÓ** el acceso a los datos. **REITERAMOS** que, gracias al modelo de programación, el diseño de infraestructura y el servidor de datos ubicado en un tercer nivel de seguridad (accesible sólo desde grupos de seguridad ubicados dentro del clúster de servidores), el ataque ni siquiera se aproximó a la capa de datos, pero sí que afectó la disponibilidad del FrontEnd que recibe las peticiones, debido a la ráfaga desbordada y concurrente de peticiones (válidas e inválidas).

En los correos de verificación generados después de cada votación, puede consultarse -a través de un código único- el usuario y la hora de registro; estos correos son enviados automáticamente por el sistema, utilizando el servidor de correo Google de uso institucional para dar mayor posibilidad de verificación. El retardo en la recepción de estos mensajes, se debió a las características y límites otorgados por Google en la cuenta de la Universidad de Caldas.

Calle 65 No. 26-10
PBX (57) (6) 878 15 00
ucaldas@ucaldas.edu.co
www.ucaldas.edu.co
Manizales - Colombia

Para posibilitar un mayor control, se ha enviado un informe detallado a las Directivas de la Universidad con las incidencias, los *logs* de los servidores, copia con fechas de creaciones de bases de datos, *logs* de acceso y actualización, con la finalidad de que se remita a la Unidad de Delitos Informáticos Nacional, para que se inicien las investigaciones pertinentes y en correspondencia, un estudio de Informática Forense.

Finalmente, comprendemos el malestar generado en el proceso, pero ninguna autoridad experta en Cibercrimen puede garantizar que **NO** se generen ataques de esta tipología, no obstante, el sistema y el equipo humano demostraron la capacidad de resiliencia ante la incidencia.

Atentamente,

LUIS FERNANDO CASTILLO OSSA
Decano

Calle 65 No. 26-10
PBX (57) (6) 878 15 00
ucaldas@ucaldas.edu.co
www.ucaldas.edu.co
Manizales - Colombia