Boletín Informativo

GPIT

Boletín Informativo por alerta de mensaje falso con virus troyano y suplantación de identidad UNAD 128

UNAD
GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA - GFSI
22/06/2021

Estimada Comunidad UNADISTA:

Advertimos que de manera fraudulenta está llegando a la bandeja de entrada de los correos institucionales de estudiantes y funcionarios de la Universidad, comunicación falsa sobre un supuesto atraso en sus obligaciones como estudiante en el pago de derechos de grado, como se puede observar en la captura siguiente:

---------- Forwarded message ---------
De: [redacted]@unad.edu.co>
Date: mar, 22 jun 2021 a las 11:12
Subject: Procedimiento de embargo por mora en los pagos establecidos en la sucesión.
To:

Bogotá D.C.

Junio 22 del 2021

Cobro 03

En base a la entrada del segundo semestre del año en curso y cumpliendo con el cruce de información, nos hemos dado cuenta que usted no ha pagado las responsabilidades que como estudiantes se deben cancelar, se hace necesario notificar que usted no ha cumplid con su obligación en el pago de los derechos de grados.

Razón por la cual el departamento de cartera procederá a embargar sus cuentas bajo la autoridad que la justicia establece en estos casos, ya es el tercer (3) cobro que se le notifica y no se tiene respuesta alguna por su parte.

Adjunto cobro y el valor del derecho de grado

Adjunto protegido con contraseña: 0022062021

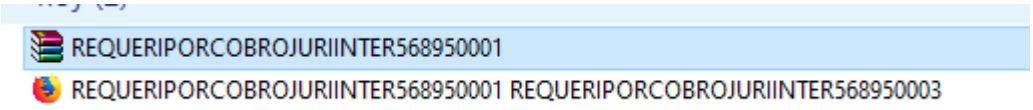
VISUALIZAR COBRO Y VALOR A PAGAR

Mensaje FALSO

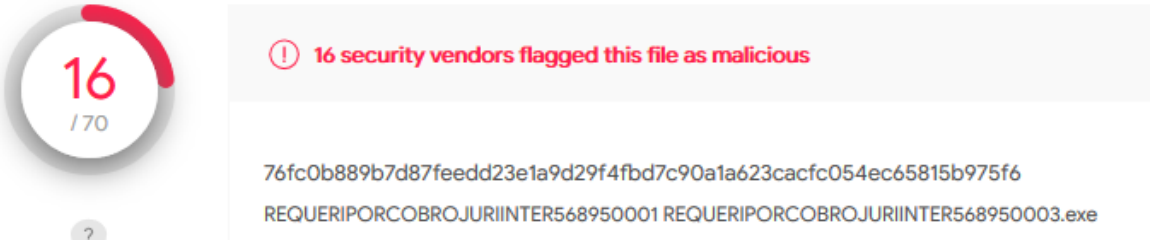
Enlace malicioso archivo con virus troyanos

Por la naturaleza del caso, esto es un claro ejemplo de suplantación de identidad dentro de la Universidad, por tal motivo tengan en cuenta las recomendaciones para minimizar este tipo de actos.

ANALISIS AL ARCHIVO ADJUNTO



Viene un comprimido que resulta ser un archivo contaminado con 16 diferentes tipos de virus troyanos.



VIRUS IDENTIFICADOS EN EL ARCHIVO ADJUNTO:

Malicious	FileRepMetagen [Malware]
FileRepMetagen [Malware]	Win/malicious_confidence_60% (D)
Malicious.015772	Unsafe
Malicious (score: 100)	A Variant Of MSIL/GenKryptik.FGQP
Generic.mg.57650c9d6a37e18b	MSIL/Kryptik.ABOZ!tr
VHO:Trojan.MSIL.Taskun.gen	Trojan.Malware.300983.susgen
Trojan:MSIL/AgentTesla.BOQ!MTB	Trojan.Win32.Save.a
Static AI - Malicious PE	Scr.Malcode!gdn30

Y los delincuentes lo que buscan es contaminar el pc donde se descargue para tomar el control total del mismo.

RECOMENDACIONES A TENER EN CUENTA:

1. No escriba sus credenciales de acceso en alguna parte de su escritorio, podrían suplantar su identidad.

2. Tengan cuidado al abrir mensajes de remitentes desconocidos o conocidos con archivos adjuntos cuya extensión sea ejecutable (exe, com, bat, pdf). O extensiones extrañas.

3. No respondan mensajes que le pidan información personal o financiera desde un formulario.

4. Nunca hagan clic en enlaces dentro de un e-mail.

5. Nunca entren a su entidad bancaria por un enlace enviado desde un email.

6. Introduzcan sus datos confidenciales únicamente en webs seguras.

7. Revisen periódicamente sus cuentas de ahorro de su entidad financiera.

8. Aprendan a identificar correos sospechosos:
   a. *Utilizan nombres y adoptan la imagen de empresas reales.*
   b. *Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa.*
   c. *Incluyen webs que visualmente son iguales a las de empresas reales.*
   d. *Algunos utilizan estrategias como regalos o la pérdida de la propia cuenta existente.*

9. Este tipo de correo están identificados como phishing y lo que buscan son sus credenciales de acceso a su información financiera o tomar el control total del equipo infectado.

10. Activen el doble factor de autenticación para Gmail, este servicio es gratuito y eleva el nivel de seguridad del correo institucional.

11. Mantenga el sistema operativo y antivirus de su computador actualizado.

Atentamente,

Grupo de Seguridad Informática de la UNAD