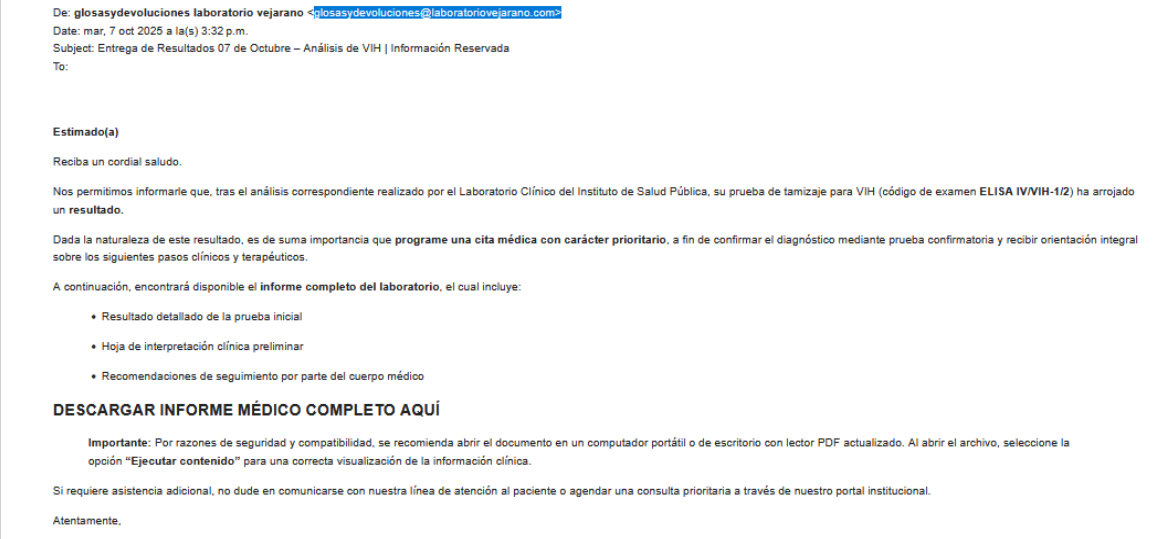
Octubre 08 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	HEUR:Trojan-Downloader.WinINF.Seraph.g
Cuenta de correo del remitente:	glosasydevoluciones@laboratoriovejarano.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



De: **glosasydevoluciones laboratorio vejarano** <glosasydevoluciones@laboratoriovejarano.com>
Date: mar, 7 oct 2025 a la(s) 3:32 p.m.
Subject: Entrega de Resultados 07 de Octubre – Análisis de VIH | Información Reservada
To:

Estimado(a)

Reciba un cordial saludo.

Nos permitimos informarle que, tras el análisis correspondiente realizado por el Laboratorio Clínico del Instituto de Salud Pública, su prueba de tamizaje para VIH (código de examen **ELISA IV/VIH-1/2**) ha arrojado un **resultado**.

Dada la naturaleza de este resultado, es de suma importancia que **programe una cita médica con carácter prioritario**, a fin de confirmar el diagnóstico mediante prueba confirmatoria y recibir orientación integral sobre los siguientes pasos clínicos y terapéuticos.

A continuación, encontrará disponible el **informe completo del laboratorio**, el cual incluye:

- Resultado detallado de la prueba inicial
- Hoja de interpretación clínica preliminar
- Recomendaciones de seguimiento por parte del cuerpo médico

DESCARGAR INFORME MÉDICO COMPLETO AQUÍ

Importante: Por razones de seguridad y compatibilidad, se recomienda abrir el documento en un computador portátil o de escritorio con lector PDF actualizado. Al abrir el archivo, seleccione la opción **"Ejecutar contenido"** para una correcta visualización de la información clínica.

Si requiere asistencia adicional, no dude en comunicarse con nuestra línea de atención al paciente o agendar una consulta prioritaria a través de nuestro portal institucional.

Atentamente,

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	IMG 00329483 Resultados 07 de Octubre – Análisis de VIH Información Reservada.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 08, 2025 at 11:32:04
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	77AF53B803F70736A062F39E91B3A789

SHA1:	89C0D500E80F8A54A17D7234B537DD6A690A4BBC
SHA256:	A6AFEB07A017585EE30EC5E04FFA07583C57F1385865F8D18A36E1397FBACED6
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmrISDXqYyosv:cXaVWfmJtOFJQRzgrDX3yT

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516