Agosto 09 de 2023

**COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING**

| | | |
|---|---|---|
| **Técnica Mitre**: | Phishing - Ransomware | |
| **Malware detectado**: | trojan.olock/msil | |
| **TLP:** | **BLANCO** | |

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:** | DOC002223INFORAD08090001.exe |
| **Veredicto:** | **Actividad maliciosa** |
| **Fecha del análisis:** | Agosto 09 de 2023 - Hora 11:44:09 |
| **MIME:** | application/x-dosexec |
| **Información del archivo:** | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| **MD5:** | 080C8B09E57D1775D1C9E865A57D679B |
| **SHA1:** | FCA175DD6FAF710E26D4DDBD5F68243C3B19373A |
| **SHA256:** | 5AF29832996EDDEA241587FD8F873C67EF9B3B0A448E9DB0E4A94A6894ABB0BB |
| **SSDEEP:** | 24576:Zhq6YRs6CE3jLMpppdpppppUO9Rs6CE3jLMpppdpppppUOTOguFbWROazL2pZaQl:eXRs6CE3jLbO9Rs6CE3jLbO5uFpazCxl |

Fuente. CSIRT Académico UNAD

**Información de proceso**

| CMD | Ruta Comprometida | Proceso Padre |
|---|---|---|
| "C:\Users\admin\AppData\Local\Temp\DOC002223INFORAD08090001.exe" | C:\Users\admin\AppData\Local\Temp\DOC002223INFORAD08090001.exe | explorer.exe |

Fuente. CSIRT Académico UNAD

Cordialmente

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