Jefatura para la Protección Presidencial

CSIRT

Equipo de Respuesta a Incidentes de Seguridad de la Información

Presidencia de la República

COLOMBIA POTENCIA DE LA VIDA · COLCERT · TIC

AC-0008-23

IoC Ransomware - MarioLocker

22/09/2023

MITRE ATT&CK TTP's

TA0002 – Ejecución
-T1059 Unix Shell.
Crea una Shell de tipo reverse en ESXI
-T1064 Scripting.
Ejecuta comandos usando el interprete de "esxcli".

TA0005 – Evasión de Defensa
-T1027 Ofuscamiento de Archivos e Información.
Encripta los datos usando RC4 PRGA.
-T1027.005 Remoción de indicadores con herramientas.
Contiene cadenas de pila ofuscadas
-T1064 Scripting.
Ejecuta comandos usando un interprete.

TA0007 - Descubrimiento
-T1083 Descubrimiento de archivos y directorios.
Enumera los Directorios en ESXI.
-T1033 Descubrimiento de Usuarios.
Identifica los usuarios con privilegios y activos en el sistema.

CONTEXTO DE ANÁLISIS

El Software Malicioso Polimórfico denominado MarioLocker que afecto a IFX, se instala y a través de las TTP's ya descritas, descarga un payload de tipo Ransomware, el cual al ejecutarse usa la dirección MAC e IP del equipo para la generación de la clave de cifrado de los volúmenes virtuales.

El malware tiene unas variables de ejecución estrictas, para asegurar su funcionamiento en hypervisores ESXI de VMWare, además de contar con ofuscación de tipo hexadecimal.

ACTIVIDAD DE RED

IP - C2C Relacionadas
20.99.184.37
192.229.211.108

VALORES HASH ASOCIADOS

- 8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973
- b518be7a044c8248a97cdbf8fabcaf36cfd4c0e7d1fe197e2c367c94d38965f4
- bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c
- f059441faa1da0529c87586572c41c57465cc97f2d6d2e1d0aa91ee080aebada
- f7600b701815faeadfa063a8b45cda2746465f0d395cdcfc8c300593ff8aa0e6
- db55383b6521a152492a5767009ad308ac46bc6cfc10e9f3bfee78110e33fdd5
- db55383b6521a152492a5767009ad308ac46bc6cfc10e9f3bfee78110e33fdd5
- 1ee95fc46f676b5a38ed77c997ff88224a302247e448329c6248e3d2a7f6bedd

VECTORES DE ATAQUE

- Descarga desde web
- Ejecución de adjuntos de correo electrónico
- Dispositivos de almacenamiento comprometidos
- Credenciales comprometidas
- Vulnerabilidades de S.O.

CLASIFICACIÓN TLP : CLEAR

Ante cualquier inquietud frente a esta información contáctenos a través:
Teléfono: (601) 5629300 EXT. 3309
Correo electrónico: csirt@presidencia.gov.co

ANÁLISIS CSOC – CSIRT PRESIDENCIA

DOMINIOS

- https://104.168.132.128.nip.io/cae260
- 104.168.132.128.nip.io
- va5vkfdihi5forrzsnmins436z3cbvf3sqqkl4lf6l6kn3t5kc5efrad.onion
- zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion

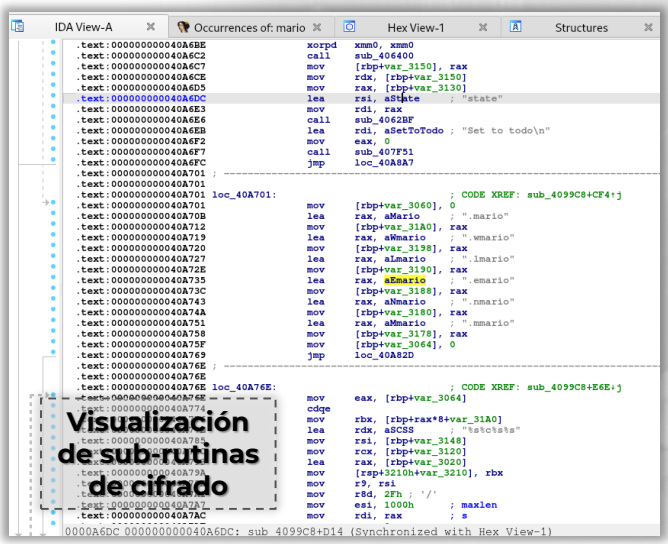
Mensaje de Rescate

APT RELACIONADOS

- RansomHouse

HYPERVISORES

- VMWare ESXI
- Hyper-V



Visualización de sub-rutinas de cifrado

ORIGEN DE LA MUESTRA

La muestra del malware fue suministrada por CSIRT Chile

COMANDOS DE SHELL

- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa "/tmp/marioesxi.zip"
- /usr/lib/p7zip/7z l -slt -bd -y -- "/marioesxi.zip"
- 7z l -slt -bd -y -- "/marioesxi.zip"
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- dpkg --print-architecture
- engrampa "/tmp/MARIOesxi.zip"

TIPOLOGÍA

- Escalada de privilegios.
- Ejecución de código arbitrario
- Manipulación de datos
- Exploración de directorios
- Carga y descarga de archivos
- Exfiltración de datos
- Robo de credenciales
- Capturas de pantalla
- C2C
- Cifrado de archivos en extensión [.]mario

PATHS MODIFICADOS

- /etc/ld.so.nohwcap
- /etc/ld.so.cache
- /etc/ld.so.preload
- USER=root.PYTHONPATH=/tmp/:.OLDPWD=/root/.PATH=/usr/bin:/bin:/usr/sbin:/sbin.PWD=/root/.PYTHONHOME=/tmp/:.MAIL=/var/mail/root.SHELL=/bin/bash.SHLVL=1.LOGNAME=root._=.HOME=/root.
- /etc/localtime
- /root/.cache/dconf/user

CLASIFICACIÓN TLP : CLEAR

ETAPAS DE EJECUCIÓN DEL PAYLOAD

ETAPA 1

Este ransomware esta diseñado para atacar hypervisores en servidores de virtualización; a continuación se muestra la secuencia de instrucciones correspondiente para la identificación de los volúmenes objetivo y los formatos de disco virtual y/o volúmenes físicos o lógicos (RDM) a cifrar:

- GetVMs hmap created find /vmfs/volumes/ -type f -not \(-path /sys -prune \) -not \(-path /proc -prune \) -not \(-path /run - prune \) -not \(-path /var/log -prune \) -name **"*.vmdk*"** -o -name **"*.ovf*"** -o -name **"*.ova*"** -o -name **"*.vmem*"** -o -name **"*.vswp*"** -o -name **"*.vmsd*"** -o -name **"*.vmsn*"** -o -name **"*.vib*"** -o -name **"*.vbk*"** -o -name **"*.vbm*"** vms GetVMs ready for open
- pos slash %s %s %d
- n/a datastoreSize datastoreMountPoint

ETAPA 2

Posteriormente, este ransomware realiza la generación de la clave de cifrado e inicia el proceso de encripción de los volúmenes virtualizados:

CTV start
/etc/init.d/vpxa restart CTV end
date +%s GetId start
uname -a esxcli **--formatter=csv network nic list MACAddress + %02x:%02x:%02x:%02x:%02x:%02x** GetId end
GetHostType start
esxcli GetHost Type end GetIp start
esxcli --formatter=csv network ip interface ipv4 get IPv4Address , ip GetIp end
GetConfig start
welcomeMsg args GetConfig end

UpdateVMs start

df -h -P -x"squashfs" | awk '{print $1"\t"$2"\t"$3"\t"$4"\t"$5"\t"$6}' %s [%s] primary /proc* /boot* /sys* /run* /dev* //proc* //boot* //sys* //run* //dev* * *.?mario

GetVMs end

DelayedProc start
host dropsess passchange welcomeset rmlogs group runIterations runIterationsDelay startIn command pass 1
currentRunIteration 2
Waiting for next iteration...
startsIn Timeout...%d
Starting iteration %d...
5 | 6 | 7
UpdateVMs end

ETAPA 3

Por último, este ransomware después de generar hasta 7 iteraciones de cifrado sobre los volúmenes virtuales objetivo, elimina el proceso en memoria y muestra el mensaje de rescate (Imagen):

Killing pid=%d
Killed
remove quit > welcome.txt

CLASIFICACIÓN TLP : CLEAR