MICITT-DGD-DRII-AT-126-2022

Alerta sobre IOC asociados con el ransomware BlackCat/ALPHV

Se les comunica a los Directores (as) /Jefes (as) de Tecnologías de Información y a los enlaces de Ciberseguridad, para que tomen las medidas necesarias.

La Oficina Federal de Investigaciones (FBI) ha publicado un informe que detalla los indicadores de compromiso (IOC) asociados con ataques que involucran a BlackCat/ALPHV, un Ransomware-as-a-Service que ha comprometido al menos a 60 entidades en todo el mundo.

Los IoC son:

PowerShell Scripts	
Filename	MD5 Hash
amd - Copy.ps1	861738dd15eb7fb50568f0e39a69e107
ipscan.ps1	9f60dd752e7692a2f5c758de4eab3e6f
Run1.ps1	09bc47d7bc5e40d40d9729cec5e39d73
Additional PowerShell Filenames	
[###].ps1	CME.ps1
[#].ps1	Run1.ps1
mim.ps1	[##].ps1
psexec.ps1	Systems.ps1
System.ps1	

Batch Scripts	
Filename	MD5 Hash
CheckVuln.bat	f5ef5142f044b94ac5010fd883c09aa7
Create-share-RunAsAdmin.bat	84e3b5fe3863d25bb72e25b10760e861
LPE-Exploit-RunAsUser.bat	9f2309285e8a8471fce7330fcade8619
RCE-Exploit-RunAsUser.bat	6c6c46bdac6713c94debbd454d34efd9
est.bat	e7ee8ea6fb7530d1d904cdb2d9745899
runav.bat	815bb1b0c5f0f35f064c55a1b640fca5

Executables and DLLs	
Filename	MD5 Hash
http_x64.exe	6c2874169fdfb30846fe7ffe34635bdb
spider.dll	20855475d20d252dda21287264a6d860
spider_32.dll	82db4c04f5dcda3bfcd75357adf98228
powershell.dll	fcf3a6eeb9f836315954dae03459716d
rpcdump.exe	91625f7f5d590534949ebe08cc728380
Filename	SHA1 Hash
mimikatz.exe	d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
run.exe	4831c1b113df21360ef68c450b5fca278d08fae2
zakrep_plink.exe	fce13da5592e9e120777d82d27e06ed2b44918cf
beacon.exe	3f85f03d33b9fe25bcfac611182da4ab7f06a442
win1999.exe	37178dfaccbc371a04133d26a55127cf4d4382f8
[compromised company].exe	1b2a30776df64fbd7299bd588e21573891dcecbe

Additional Observed Filenames	
test.exe	xxx.exe
Mim.exe	xxxw.exe
crackmapexec.exe	Services.exe
plink.exe	Systems.exe
PsExec64.exe	

BlackCat Ransomware SHA256 Hashes:
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
80dd44226f60ba5403745ba9d18490eb8ca12dbc9be0a317dd2b692ec041da28

C2 IPs:			
89.44.9.243	142.234.157.246	45.134.20.66	185.220.102.253
37.120.238.58	152.89.247.207	198.144.121.93	89.163.252.230
45.153.160.140	23.106.223.97	139.60.161.161	146.0.77.15
94.232.41.155			

Recomendaciones

- Se recomienda a los usuarios y administradores a revisar los IOC y los detalles técnicos en el siguiente enlace:

  https://www.ic3.gov/Media/News/2022/220420.pdf

- Se recomienda incluir estos datos a sus firewalls o sistemas de detección como medida de prevención.

• Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas de usuario nuevas o no reconocidas.

• Realice copias de seguridad periódicas de datos. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos. Recuerde la regla 3-2-1:

- MANTENER **3 COPIAS DE LOS DATOS**
- UTILIZAR PARA EL BACKUP **2 FORMATOS DIFERENTES**
- MANTENER UNA DE LAS COPIAS **OFFLINE**

• Revisar el Programador de tareas para tareas programadas no reconocidas. Además, revise manualmente las tareas programadas reconocidas o definidas por el sistema operativo en busca de "acciones" no reconocidas (por ejemplo: revise los pasos que se espera que realice cada tarea programada).

• Revise los registros del antivirus en busca de indicaciones de que se apagaron inesperadamente.

• Implementar la segmentación de la red.

• Requerir credenciales de administrador para instalar el software.

• Implementar un plan de recuperación para mantener y conservar varias copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (p. ej., disco duro, dispositivo de almacenamiento, la nube).

• Instalar actualizaciones/parches de sistemas operativos, software y firmware tan pronto como se publiquen las actualizaciones/parches.

• Utilice la autenticación multifactor cuando sea posible.

• Cambie periódicamente las contraseñas de los sistemas de red y las cuentas, y evite reutilizar contraseñas para cuentas diferentes.

• Implementar el plazo más corto aceptable para los cambios de contraseña.

Deshabilite los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y controle los registros de acceso remoto/RDP.

• Audite las cuentas de usuario con privilegios administrativos y configure los controles de acceso teniendo en cuenta los privilegios mínimos.

• Instale y actualice periódicamente el software antivirus y antimalware en todos los hosts.

• Utilice únicamente redes seguras y evite el uso de redes Wi-Fi públicas. Considere instalar y usar una red privada virtual (VPN).

• Deshabilitar hipervínculos en los correos electrónicos recibidos cuando sea posible establecerlo

Referencias

https://www.cisa.gov/uscert/ncas/current-activity/2022/04/22/fbi-releases-iocs-associated-blackcatalphv-ransomware

https://www.ic3.gov/Media/News/2022/220420.pdf

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2022.04.23 20:40:40 -06'00'

Jorge Mora Flores
Director de Gobernanza Digital

Firmado digitalmente por ROBERTO PAULO LEMAITRE PICADO (FIRMA)
Ubicación: CSIRT-CR
Fecha: 2022.04.23 20:59:13 -06'00'

Roberto Lemaitre Picado
Coordinador CSIRT-CR