SEGOB
SECRETARÍA DE GOBERNACIÓN

CNS
COMISIONADO NACIONAL DE SEGURIDAD

POLICÍA FEDERAL

Policía Federal
División Científica
Coordinación para la Prevención de los Delitos Electrónicos
CERT-MX

Alerta de Seguridad sobre Ransomware WannaCry

12 de Mayo 2017

ALR0517-17

CERT-MX

Centro Nacional de Respuesta a Incidentes Cibernéticos de México

Fecha de publicación: 12 de mayo 2017
Última revisión: 12 de mayo 2017
Fuente: CERT-MX

SISTEMAS AFECTADOS:

- Microsoft Windows
- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 y R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 y R2
- Windows 10
- Windows Server 2016

RESUMEN

El Equipo de Respuesta a Incidentes Cibernéticos de la Policía Federal ha identificado un ataque masivo de ransomware asociado a la vulnerabilidad MS17-010 del sistema operativo Microsoft Windows. De acuerdo con la colaboración con Equipos de Respuesta de España, el malware puede tratarse de una variante del código malicioso llamado WannaCry.

I. DESCRIPCIÓN

El malware infecta el equipo cifrando todos sus archivos y, utilizando la vulnerabilidad mencionada, la cual permite la ejecución remota de código a través del servicio de Samba (SMB) y se distribuye al resto de equipos Windows de la misma red.

De acuerdo con la información compartida con Equipos de Seguridad Cibernética y Agencias de Seguridad Informática, se identificaron direcciones electrónicas IP de donde aparentemente se originaron los primeros ataques, las cuales se comparten a través de la siguiente tabla.

AS	IP	Nombre	País
37560	197.231.221.211	CYBERDYNE	Liberia, LR
3	128.31.0.39	MIT-GATEWAYS - Massachusetts Institute of Technology	Estados Unidos, US
16276	149.202.160.69	OVH	Francia, FR
14061	46.101.166.19	DIGITALOCEAN-ASN - Digital Ocean, Inc.	Estados Unidos, US
201229		DIGITALOCEAN-GERMANY	Alemania, DE
16276	91.121.65.179	OVH	Francia, FR

II. IMPACTO

Cuando un equipo es comprometido a través de un ransomware, la información es secuestrada por un ciberdelincuente, el cual solicita un pago para su rescate, por lo que se pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

III. RECOMENDACIONES

El equipo de Respuesta a Incidentes Cibernéticos de la Policía Federal (CERT-MX) recomienda llevar a cabo las siguientes recomendaciones:

- No abrir archivos adjuntos que provengan de remitentes desconocidos.
- Aplicar la actualización de seguridad recomendada por Microsoft Corp.
- Para los sistemas sin soporte se recomienda aislar los equipos de la red de producción.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP en las redes de las organizaciones.
- Identificar los equipos, dentro de su red, que pueden ser susceptibles de ser atacados a través de Microsoft Windows, en cuyo caso, puedan ser aislados, actualizados y/o apagados.
- Se recomienda realizar un filtro a nivel perímetro de red de las direcciones electrónicas IP mencionadas anteriormente.

IV. REFERENCIAS

- https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

SEGOB
SECRETARÍA DE GOBERNACIÓN

CNS
COMISIONADO NACIONAL DE SEGURIDAD

POLICÍA FEDERAL

¿Qué es el CERT-MX?

El CERT-MX es el Centro Nacional de Respuesta a Incidentes Cibernéticos responsable de atender incidentes de seguridad en cómputo relacionados con redes conectadas a la Internet en México.

CERT-MX

Centro Nacional de Respuesta a Incidentes Cibernéticos de México
Policía Federal / División Científica

Teléfono: +52 55 1103 6000 extensiones
29138, 29147, 29148, 29149, 29150, 29151, 29152, 29153, 29154
Correo electrónico: cert-mx@cns.gob.mx
Reporte Phishing: phishing@cns.gob.mx
Reporte Malware: malware@cns.gob.mx
Llave PGP: 61D2 EA8D A678 EE58 899A 7679 94A0 A8BA 96E8 4DDE