COMISIÓN PARA EL MERCADO FINANCIERO

INCIDENTE DE CYBERSEGURIDAD

INFORME TECNICO

La Comisión para el Mercado Financiero (CMF) comparte con la comunidad detalles técnicos respecto del incidente de ciberseguridad sufrido en su plataforma Microsoft Exchange el pasado 12 de marzo.

De acuerdo con el análisis realizado por el área de seguridad de la información y tecnología de la CMF, junto a la colaboración de apoyo especializado externo, fue posible identificar tanto la magnitud del evento registrado como el impacto que este tuvo en nuestra organización.

Se identificó una webshell en los servidores de Microsoft Exchange producto de la explotación de la vulnerabilidad reportada en la plataforma de correo a nivel mundial. Conforme a los avances de la investigación se identificaron las IP desde donde se realizó la explotación de la vulnerabilidad.

Estas son las siguientes:

- 216.245.221.87
- 216.218.206.67
- 52.97.0.45
- 109.246.19.86
- 125.77.188.204
- 150.255.84.211
- 36.106.167.133
- 118.81.4.171
- 172.81.237.198
- 123.14.253.115
- 113.120.8.186
- 113.88.111.208
- 1.85.216.154
- 36.32.3.146
- 45.155.205.225

Debido a la explotación de la vulnerabilidad la investigación se enfocó en verificar el impacto en la infraestructura tecnológica de la CMF, descartándose otros niveles de compromiso. Se trató de un evento circunscrito a la plataforma de correo.

Los indicadores de compromiso asociados a la explotación son los siguientes:

HASH SHA1	TIPO	DETALLE
0b15c14d0f7c3986744 e83c208429a78769587b5	Webshell .aspx	error_page.aspx
bcb42014b8dd9d9068f 23c573887bf1d5c2fc00e	Webshell .aspx	supp0rt.aspx
0aa3cda37ab80bbe30fa 73a803c984b334d73894	.bat Script	test.bat

Las mitigaciones en la plataforma de Microsoft Exchange ya fueron realizadas estando actualmente operativo.

Ataques de este tipo han sido atribuidos públicamente al grupo de origen chino “HAFNIUM”, registrando numerosas víctimas alrededor del mundo y en sectores tan diversos como laboratorios de enfermedades infecciosas, firmas de abogados, instituciones educacionales, sectores de defensa, policía y organismos reguladores entre otros.

Diagrama simplificado con su forma de operar