

# CYBERSECURITY INCIDENT

## TECHNICAL REPORT

**March 22, 2021** – The Financial Market Commission (CMF) shares with the community technical details regarding the cybersecurity incident that affected its Microsoft Exchange platform on March 12, 2021.

According to the analysis carried out by its Information Security & Continuity area alongside special externalized support, it was possible to identify both the magnitude of this event and the impact it had in the Commission.

A webshell was identified in Microsoft Exchange servers because of the exploit of the vulnerability reported worldwide in this email platform. As the Commission's investigation progressed, it identified the following IP addresses from which the vulnerability was exploited:

216.245.221.87	150.255.84.211	113.120.8.186
216.218.206.67	36.106.167.133	113.88.111.208
52.97.0.45	118.81.4.171	1.85.216.254
109.246.19.86	172.81.237.198	36.32.3.146
125.77.188.204	123.14.253.115	45.155.205.225

Due to this vulnerability's exploit, the investigation focused on verifying the impact on the CMF's technological infrastructure, ruling out other levels of compromise. The incident was limited to the email platform.

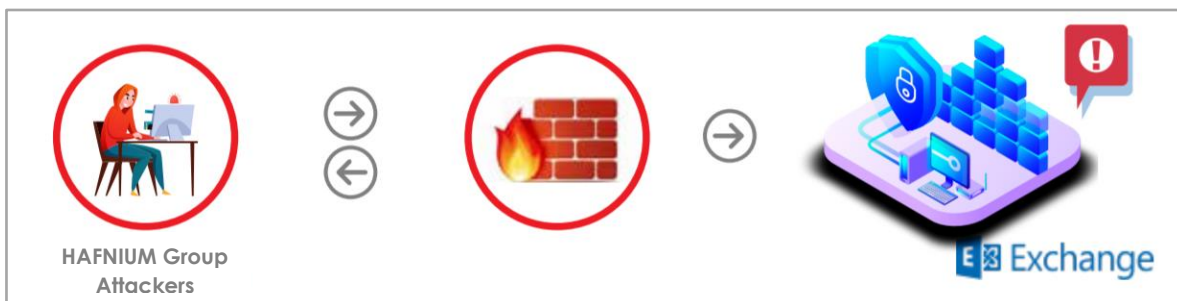
The compromise indicators related to the exploit are as follows:

HASH SHA1	Type	Detail
0b15c14d0f7c3986744e83c208429a78769587b5	Webshell.aspx	error_page.aspx
bcb42014b8dd9d9068f23c573887bf1d5c2fc00e	Webshell.aspx	supp0rt.aspx
0aa3cda37ab80bbe30fa73a803c984b334d73894	.bat Script	test.bat

Mitigations in the Microsoft Exchange platform have already been carried out, and it is currently operational.

This type of attacks has been attributed to the China-based "HAFNIUM Group," hitting numerous institutions around the world. Affected sectors include, among others, infectious disease laboratories; law firms; educational institutions; defense; police forces; and regulatory agencies.

## A simplified diagram on how the exploit works



\*\*\*\*

Area of Communications, Education & Image – Financial Market Commission (CMF)

Contact: [prensa@cmfchile.cl](mailto:prensa@cmfchile.cl) | [Press Room](#) | Twitter: [@CMFChile](#) [@CMF Educa](#)  
[@CMF HEsenciales](#) | LinkedIn: [CMF](#)