MWR InfoSecurity

Supported by

CPNI
Centre for the Protection of National Infrastructure

CASE STUDY: ATTACK TYPE – BRUTEFORCE (PASSWORD GUESSING)

CASE STUDY:

Attack Type – Bruteforce (Password Guessing)

Scenario:

Org 7, an African based manufacturing company became the victim of a bruteforce attack of their corporate email service. During a feedback session regarding a failed bid for a significant tender between Org 7 and the potential purchaser, Org 7 was informed that their submission was essentially identical to one of their competitors although more expensive. Org 7 were of the understanding that their offering and proposed strategy was unique to them as a company.

In response, Org 7 decided to investigate this incident further, realising this was unlikely to be coincidental given they had recently laid off several employees. As the lay-offs occurred prior to the completion of the bid process, investigations initially focused on identifying key individuals involved in the bid, and critical assets responsible for transmitting and storing the related confidential data. After a few days of assessing the sources and accessibility of data, the compromise of their corporate email service was confirmed.

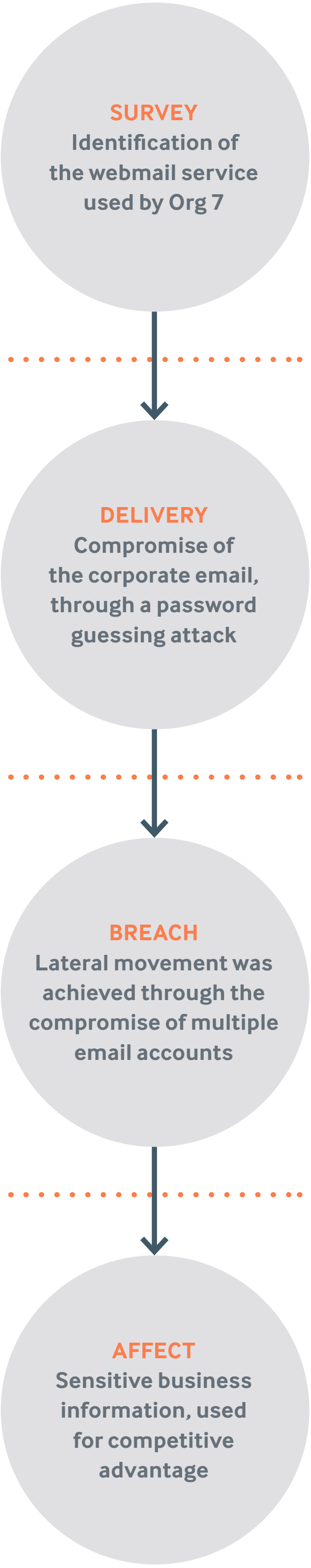
The email service provider was immediately contacted and asked to supply information that would assist with the investigation. In response to the request, Org 7 was provided with the available access logs, the past 20 days, which was in-line with the service they had purchased. A review of the limited log data identified an unknown IP address having accessed five employee email accounts across a number of weeks. Each of the unauthorised accesses was found to exceed 45 minutes in length and often occurred for several hours. Lookups on the unknown IP address found it to be registered to a competitor. In attempt to contain the incident the passwords were immediately changed on the five email accounts identified. Log data provided for the following weeks showed failed login attempts on the date the passwords were changed and an additional log on attempt for a previously unidentified email account.

Overall, twenty email accounts were found to be using the compromised password. Limited visibility meant Org 7 was unable to determine how many of the twenty accounts were compromised as well as exactly what had been taken from them. It was assessed that a competitor had gained access to sensitive emails and likely used this information for the purposes of commercial advantage during the bid process.

Specific Failures Leading to Compromise

- Weak passwords
- Default passwords not changed
- Insufficient logging

STAGES OF ATTACK



SURVEY
Identification of the webmail service used by Org 7

DELIVERY
Compromise of the corporate email, through a password guessing attack

BREACH
Lateral movement was achieved through the compromise of multiple email accounts

AFFECT
Sensitive business information, used for competitive advantage

ATTACK TIMELINE

Targeting to Compromise:	Immediate
Compromise to Exfiltration:	Immediate
Compromise to Discovery:	> 1 month
Compromise to Containment:	< 1 hours from discovery
Method of Discovery:	External – third-party notification due to loss of bid
Threat Actor:	External – assessed to be targeted/competitor
Assets Compromised:	Corporate Email – third party hosted service
Business Impact:	High – Bid lost and unique selling point lost