MWR InfoSecurity

Supported by
CPNI
Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Phishing for Credentials

Scenario:

Org 9 is a multi-national Japanese manufacturing robotics company headquartered in Japan with European operations. Org 9 designs and manufactures robotics used in fabrication and manufacturing facilities throughout the world from automotive production lines to the assembly of micro-electronics.

The UK branch of Org 9 received a notification from its Japanese IT security team that a user had reported a suspicious incident. The incident consisted of emails received from two UK employees, a high level engineer and sales person who were long standing and trusted employees. The recipients were chief design engineers and executives located in Japan.

The suspected emails contained a malicious executable. Since the email was sent internally from employee to employee, the email had not traversed normal email spam filtering which blocks encrypted executable files. When queried regarding the emails, the two employees stated they had not sent the emails which raised suspicion of a suspected compromise of the user's credentials, laptops or the Org 9 UK corporate infrastructure and exchange environment.

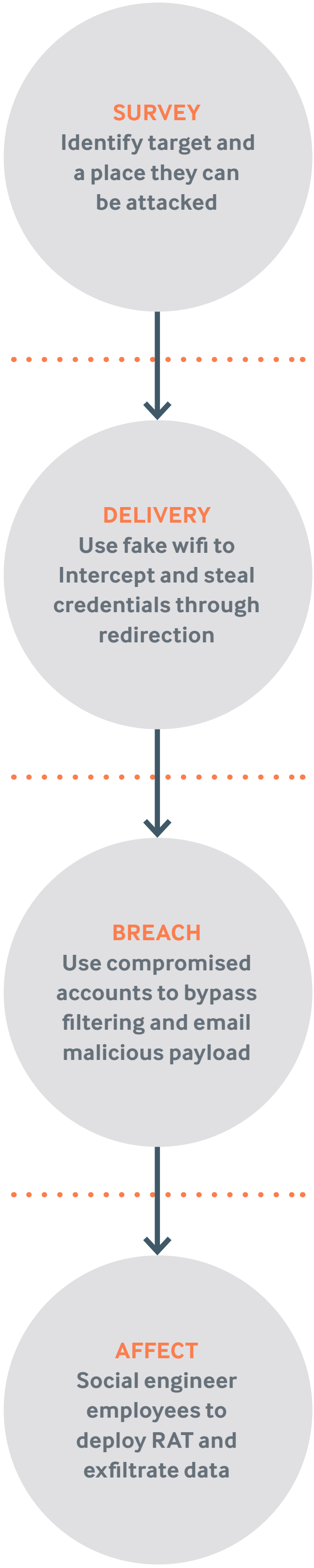
An investigation was carried out on the user laptops, which did not identify any malware or evidence that the emails had been sent from the user's laptops. Upon examination of the email headers and Exchange Server logs, it was determined that the emails had originated from Outlook Web Access (OWA) sessions which allows users to log on and send emails directly from the internet.

The user's accounts did not show high levels of failed password attempts and their passwords were complex and regularly changed. However, upon examination of email logs, it was noted that the two users had logged on to OWA from the same source once week prior to the incident when both employees attended a trade show in Belgium where Org 9 was an exhibitor. Examination of the users' internet cache revealed a fake OWA page that was made to represent the OWA login page. Further analysis indicated that the two laptops authenticated to a wireless access point whilst attending the event that matched the network name, but did not have a hardware (BSSID) address that matched any wireless access points at the event premises. It was subsequently determined that a fake wireless access point had been operating near the Org 9 stand at the event which intercepted requests to the Org 9 domain and redirected to a fake Org 9 OWA page in order to steal user's credentials and conduct further targeted social engineering attacks against Org 9 employees in the Japanese headquarters.

Specific Failures Leading to Compromise

- User awareness training of phishing attacks and use of trusted networks only
- Lack of two factor authentication

STAGES OF ATTACK



SURVEY
Identify target and a place they can be attacked

DELIVERY
Use fake wifi to Intercept and steal credentials through redirection

BREACH
Use compromised accounts to bypass filtering and email malicious payload

AFFECT
Social engineer employees to deploy RAT and exfiltrate data

ATTACK TIMELINE

Targeting to Compromise:	Days (Exact time to plan targeting unknown)
Compromise to Exfiltration:	7 Days
Compromise to Discovery:	8 Days
Compromise to Containment:	8 Days
Method of Discovery:	Internal – employee reported incident
Threat Actor:	External – highly targeted
Assets Compromised:	UK employees email comms, Japanese employees' workstations
Business Impact:	Low – Mail from phished employees compromised but incident caught early