MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Application Level Attack

Scenario:

Org 3 is a large organisation in the technology sector that, owing to a large range of products and services, maintains a large number of websites. Suspicious activity had been reported from one of the smaller websites and so Org 3 commenced an investigation.

It was discovered that the website had an SQL injection vulnerability that had not been detected and had been present for over 5 years, despite being a relatively uncomplicated example of an SQL injection. Attackers had exploited the issue and used the SQL injection to upload a web shell, giving them greater access to the hosting server.

The attackers extracted the contents of the database, and then uploaded tools to the web server from which to attack the internal network. The tools had included password extraction tools and privilege escalation exploits. Using these tools, the attackers compromised an account with domain administrator privileges and were attempting to compromise hosts that bridged multiple internal networks when Org 3 identified and stopped them.

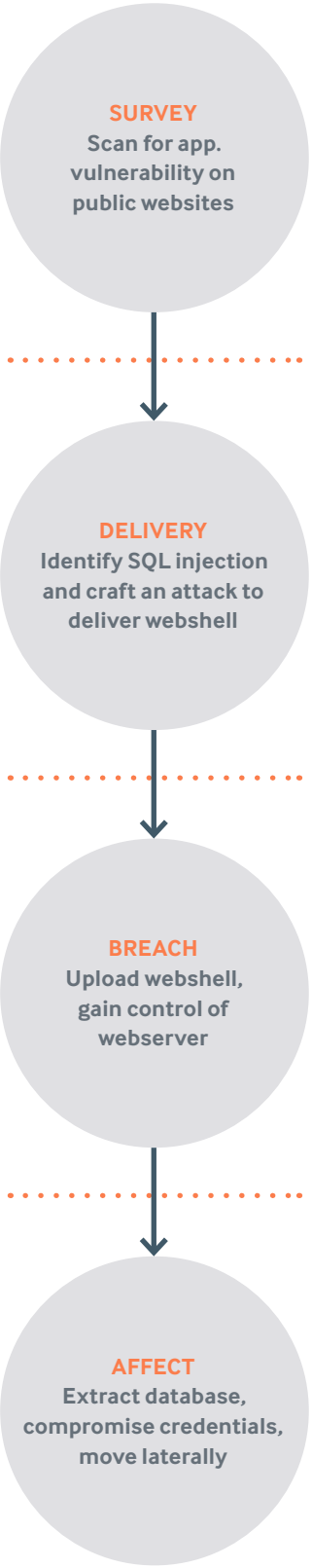
It was found that the attackers had gained access to a number of credit card details, as well as sensitive details around Org 3's clients.

It was also assessed that had they not been stopped when they were, the attackers would have been able to access significant quantities of sensitive data about Org 3 and Org 3's clients.

Specific Failures Leading to Compromise:

- Insufficient code quality and assessment of attack surfaces
- No prevention of malicious tools running or detection of tools

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	1 hour
Compromise to Exfiltration:	3 hours
Compromise to Discovery:	50 days
Compromise to Containment:	54 days
Method of Discovery:	External notification
Threat Actor:	External – targeted
Assets Compromised:	Application Server, Database Server
Business Impact:	Medium – loss of customer sensitive information and business assets