MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Network Protocol Attack

Scenario:

Org 4 is a mid-sized industrial products distributor with a number of small offices across the UK. In order to keep its telephone operating costs down, Org 4 adopted VoIP (Voice over IP) technology based on session initiation protocol (SIP). This allowed Org4 to roll out IP phones so that all of its staff could call each other at their many distributed offices without any call charges. It also allowed Org 4 to enter arrangements for routing its calls to the outside world. However, one month the bill for external connections was over £15,000, 30 times greater than normal. After a number of possibilities were ruled out, Org4 suspected that a security incident had occurred and commenced an investigation.

SIP addresses work much like email addresses and SIP addresses for Org 4 looked like the following:

sip:JoeBlow@Org 4.com. When routing a call to the outside world, the system is configured to recognise the non-SIP traditional numbers and route the call through to their outbound telephone services provider. Telephone and data traffic traverse the same infrastructure, however org4 strictly segregated VoIP and corporate network traffic by virtual LANs (VLANS).

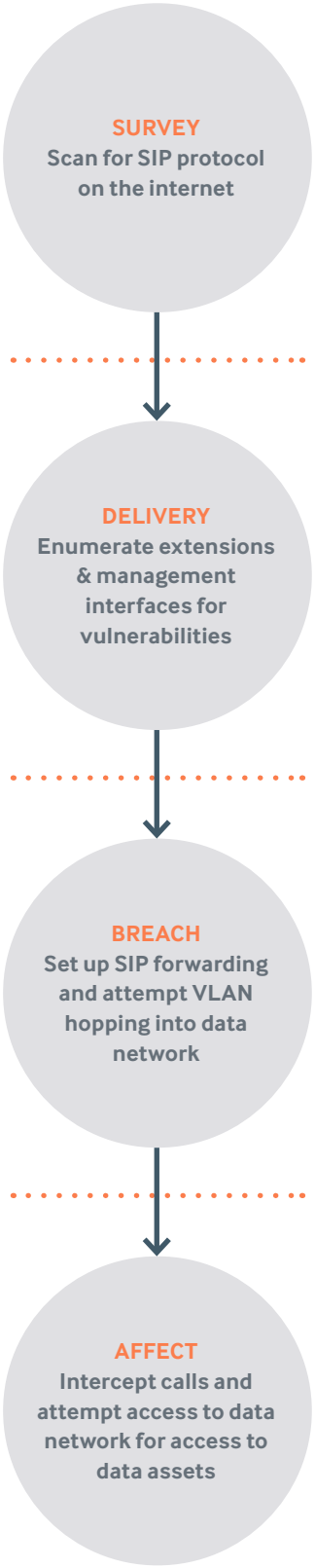
However, investigation of logs showed that attackers had been abusing the system to identify Org4's SIP server and then enumerate extensions. The attackers had realised that Org4 had mistakenly set up their service to allow SIP connections from unknown IP addresses to be forward through their external telephone services provider. The attackers had abused this configuration error to make calls to premium rate numbers that they controlled at a cost to Org4.

The attackers had then gone on to attack the SIP infrastructure and, through exploiting weak credentials, been able to gain access and monitor calls made by Org4's employees. The investigation found that the attackers were trying to gain access to the corporate network but were unsuccessful before their access could be terminated.

Specific Failures Leading to Compromise:

- Misconfiguration of a network service
- Weak credentials

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	4 days
Compromise to Exfiltration:	5 days
Compromise to Discovery:	12 weeks
Compromise to Containment:	14 weeks
Method of Discovery:	Internal – excessive telephone billing
Threat Actor:	External – opportunistic
Assets Compromised:	SIP gateway, Voice comms
Business Impact:	Medium – Fiscal impact and some information loss (phone calls)