MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Exploitation of publically known vulnerability

Scenario:

Org1 is a large internet service and telecommunications provider with a diverse portfolio of network and data services. In 2014, Org1's operations team responded to a firewall performance issue. On troubleshooting of the device, it was discovered that the cause was an internet facing system that was conducting network scans using NMap, a network scanning tool, which was unauthorised behaviour and the cause of the failure. The system was functioning as a network load balancer to a subversion code repository and did not have an external web interface or much by way of internet facing attack surface.

Upon further investigation, it was determined that the system had been compromised through an internally facing administration web interface that was susceptible to the Shellshock vulnerability (CVE-2014-6271), a vulnerability that had been publically disclosed and a patch made available three months prior.

An investigation ensued and the source system in the attack was identified as an internet facing web server that was also exploited via the Shellshock vulnerability. The web server had the tool Socat deployed which was used by the attacker to forward their shell from one system to another and conduct preliminary internal network scans.

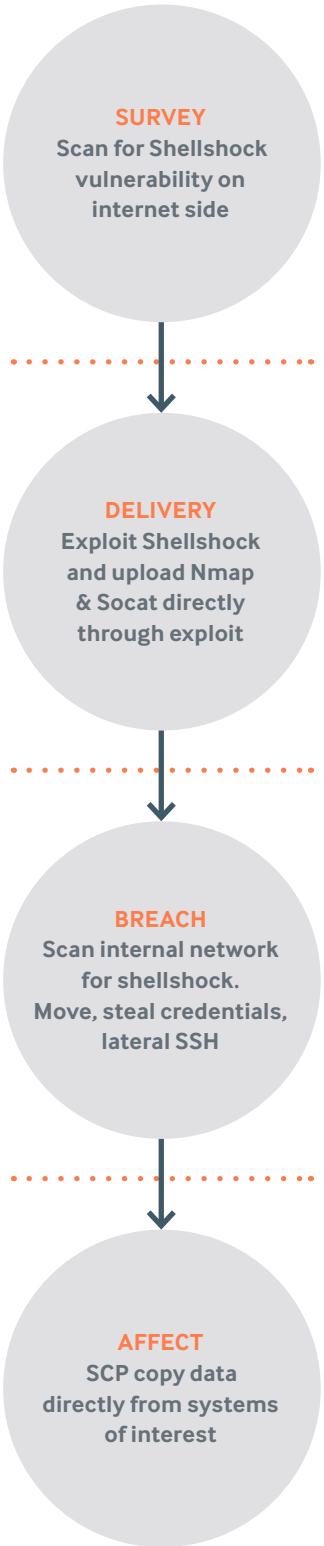
Whilst the organisation had implemented a patch management regimen to deal with Shellshock, individual departments were delegated to assess their own exposure and this was not validated with independent scanning, resulting in incomplete remediation. Of particular note was that at the time of investigation, no internal assets had been patched as they were not considered high risk targets.

As a result, further examination of the web server identified many other load balancers internal to the network that had also been compromised, some of these located in sensitive segments of the network. Since the load balancer administration console was set to run with the highest ("root") privilege, each load balancer that was compromised gave the attacker the opportunity to have unrestricted access allowing exfiltration of data of interest. Credentials were also recovered from load balancers and used for subsequent lateral SSH movements into many other systems resulting in a major incident.

Specific Failures Leading to Compromise:

- Not rapidly patching in response to an actively exploited vulnerability
- Mistakenly assuming internal assets did not need to be urgently patched
- Weak credentials on appliances

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	Seconds
Compromise to Exfiltration:	3 days
Compromise to Discovery:	5 days
Compromise to Containment:	11 days
Method of Discovery:	Internal - operational firewall performance issue
Threat Actor:	External – opportunistic
Assets Compromised:	External Web Servers, Internal Load Balancers, App Servers, SVN code repositories.
Business Impact:	Medium – Compromise of assets but no loss of revenue generation functions or personal information