MWR InfoSecurity

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Exploitation of novel / 0-day vulnerability

Scenario:

Org2 is a specialist technology company based in the UK. The Org2 IT security operations team responded to an alert from its corporate anti-virus provider that a copy of password stealing malware had been found on three of its domain controllers. This was a serious incident and an investigation was immediately launched.

The investigation found that a regular user had opened a phishing email that contained a link to a malicious site. Examination of the payload found that it hosted an exploit for what was, at the time, a novel remote code execution vulnerability (0-day) in Adobe Flash.

The payload dropped by the exploit had gained high privileges on the user's machine and disabled antivirus, which is a common technique used by malware. The disabled antivirus was flagged by the centralised AV monitoring in Org2 and so a support call was automatically placed. The administrator had then logged into the machine to understand why the AV was not functioning whereby their domain credentials were stolen.

The attacker had then attacked the internal network, including the domain controllers using the stolen credentials. As part of their attacks they had installed credential stealing malware on the domain controllers and gained large numbers of plaintext credentials.

Although a patch from Adobe was relatively quick to be published, Org2 had a period of exposure were there were no patches available and managed this through user awareness, stripping links from email and ceasing the practice of logging onto user systems with domain credentials.

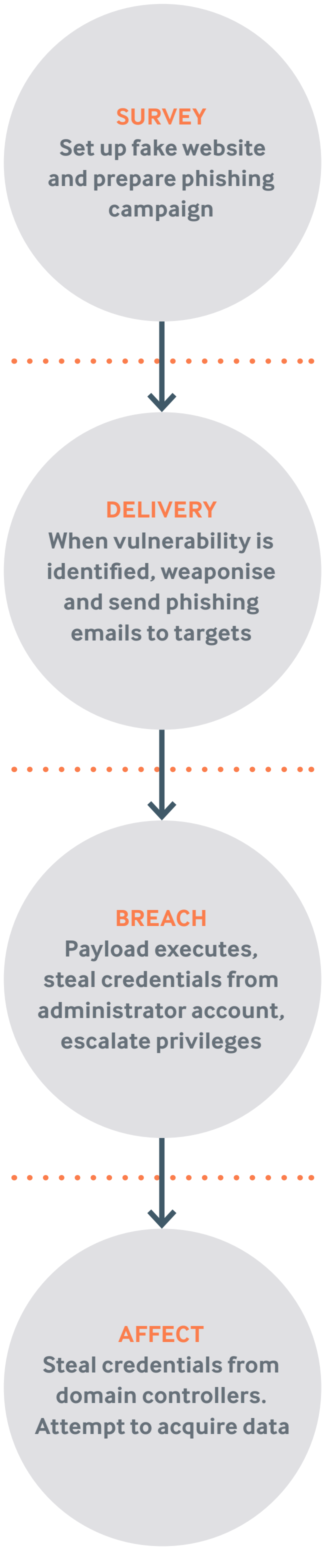
Specific Failures Leading to Compromise

- Flash installed on user PC with no business case for its use
- Administrator interacting with a suspect machine whilst using a domain account
- Users insufficiently aware of risks of links in emails

ATTACK TIMELINE

Targeting to Compromise:	6 weeks (from domain registration & setup)
Compromise to Exfiltration:	4 days
Compromise to Discovery:	4 days
Compromise to Containment:	9 days
Method of Discovery:	Internal - AV triggering on malware found on DCs
Threat Actor:	External – highly targeted
Assets Compromised:	End user system, Domain Credentials, Domain Controllers
Business Impact:	High – IP Informational assets stolen

STAGES OF ATTACK



SURVEY
Set up fake website and prepare phishing campaign

DELIVERY
When vulnerability is identified, weaponise and send phishing emails to targets

BREACH
Payload executes, steal credentials from administrator account, escalate privileges

AFFECT
Steal credentials from domain controllers. Attempt to acquire data

CASE STUDY: ATTACK TYPE – EXPLOITATION OF NOVEL / 0-DAY VULNERABILITY