MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Watering-Hole Attack

Scenario:

Org 6, globally recognised for innovative research, was informed that suspect traffic had been observed communicating with a known command and control node IP address in September 2013.

An investigation into the incident found that in May 2013, a user had conducted a Google search for an updated driver for a specialist piece of software that facilitated console access to devices used in industrial control systems (ICS). The vendor name, type and the keyword 'driver', was specified as part of the search query. Given the uniqueness of the requested query, the legitimate vendor's website was returned and subsequently the link clicked on, to visit the website. The user proceeded to download the required driver, which was delivered as a zip file. Extraction of this file presented a setup executable, which launched a malicious DLL, and wrote multiple DLLs to the users roaming profile, at which point the user's host became compromised with a remote access trojan (RAT). Once a user's roaming profile has been infected any subsequent machines logged into are at risk of also becoming infected.

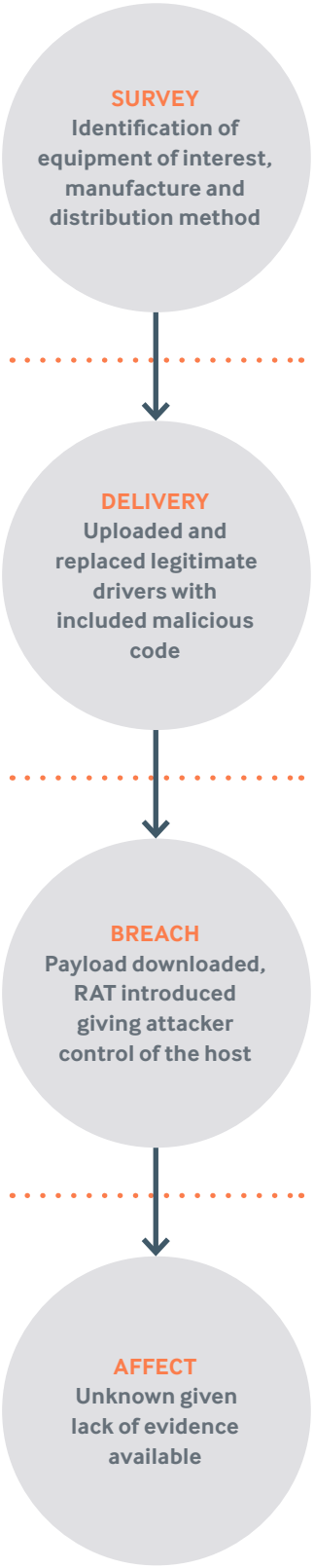
Analysis of the malware found on the user's host was undertaken to determine its capabilities and to extract any further information that could be used to identify other compromised machines. The malware was created in March 2013 and was capable of validating its persistence, checking for, and injecting further malicious code into web browsers on the machine. Additionally, several new command and control servers were also identified through this process.

Lack of reliable logging meant that it was not possible to determine the impact and whether the attacker had been able to acquire data from other systems on the network. If successful, attacks of this nature that take advantage of trusted relationships, such as vendor and consumer, can promptly and efficiently compromise large portions of a particularly niche industry.

Specific Failures Leading to Compromise

- Insufficient Internal Segregation Between Hosts
- Machines used for ICS also used for day-to-day business
- Lack of logging, either centrally or on individual hosts

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	up to 2 months
Compromise to Exfiltration:	< 1 day
Compromise to Discovery:	up to 4 months
Compromise to Containment:	Discovery + 3 days
Method of Discovery:	External – third-party notification
Threat Actor:	External – assessed to be highly targeted
Assets Compromised:	Internal workstations
Business Impact:	Not possible to ascertain