Watch this space

Satellites support so much of our business infrastructure, but being in space doesn't make them immune from hackers. Daniel Norman, senior solutions analyst at the Information Security Forum explains why they are vulnerable and attractive targets

Satellite assets are unique; they are often two-to-three years in the making and then stay in space for decades. They underpin a significant number of industries that individuals wouldn't even consider; from timings of financial transactions, to GPS for navigation and shipping, to communications and monitoring. Arguably all organisations are dependent somewhat on satellites somewhere in their supply chain, so the risk of downtime or disruption could potentially be very damaging.

Chris Childers, chief executive officer of the United States National Defence Group, highlighted the fact that most satellites have been orbiting our Earth for many years, which means they have old technology that was made before cyber threats were a real issue. Many satellites also communicate solely through radio-based wireless protocols, which makes them an attractive target for attackers.

If NASA can be hacked, can't everyone?

NASA, the most well-known pioneers of space exploration, are vulnerable to cyber attack. The US government has pumped billions of dollars into satellites but little into protection. Reports say that in 2010 and 2011 there were 5408 computer security incidents at NASA – one incident allowed full functional control of NASA's networks. Hackers also gained access to the Landsat 07 satellite twice, in 2007 and 2008, and gained full control of Terra EOS for two whole minutes on two separate occasions by hacking the ground computers at weak points around the globe.

It's not just weak points around the globe that state-sponsored hackers expose. According to Marc Kolenko, PwC Cyber Security Consultant, "nation states have developed satellites that can park themselves in close proximity of another satellite, and interfere with Telemetry, Tracking, and Command (TTC) uplinks and downlinks. Now, that may not directly equate to a cyber exploit, but if I can insert myself into the uplink or downlink, I can certainly start manipulating the data payloads they carry."

Satellites are integrated into governments, critical national infrastructure and consumers' lives, helping GPS systems function and facilitating communications. Air transport, maritime, financial and business services, as well as weather monitoring and defence systems, all face serious disruption if satellites and space infrastructure are targeted, researchers at Chatham House's International Security Department have said.

'There are now about 1,100 functioning satellites in space, and at least 2,000 non-functioning ones.' This opens up a plethora of potential opportunities for would-be hackers, exacerbated if supported by the financial backing of nation states. Space-based assets could well be interesting targets to nation states: communication systems are heavily reliant on satellites, therefore the best way to knock them out would be to put remote malware on satellites.

The U.S. government and in particular the Department of Defence has satellite-based assets to command and control troops and equipment, or to capture and cultivate intelligence. The Chatham House report states that cyber threats against space-based systems include "state-to-state and military actions; well-resourced organised criminal elements seeking financial gain; terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions; and individual hackers who want to fanfare their skills."

It is not just military implementations. If GPS constellations went down then planes and ships would lose their navigation systems, maps on billions of consumers' smartphones would not work and – something that many people may not realise – clocks around the world would cease to synchronise, disrupting financial trading everywhere. Weather watchers would also be frustrated: the US National Oceanographic and Atmospheric Administration took its Satellite Data Information System offline in September 2014 after an apparent hacking incident, which kept weather agencies around the world from receiving necessary forecasting data for 48 hours.

> Communication systems are heavily reliant on satellites, therefore the best way to knock them out would be to put remote malware on satellites

Soon the expansive networks that link satellites with terrestrial infrastructure is likely to extend to include cars and household appliances, possibly linking to the IoT. "Satellites can play a unique role in the Internet of Things," said David Hartshorn, secretary general of the Global VSAT Forum and companies are now looking to secure their products against these kinds of attack vectors.

What does this all mean? Do you think we are likely to see a major attack on a commercial or military satellite over the next three years? Are you aware of the extent to which your organisation relies on satellites, and what the impact would be if they were taken out of action?

■ **The ISF is a leading authority on cyber, information security and risk management. Its members comprise some of the world's leading organisations featured on the Fortune 500 and Forbes 2000 lists. For more information visit www.securityforum.org**