CIP
CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

PKI and the modern enigma of digital certificates and security

Presentation to European Space Agency Symposium

July 2021

CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

Introduction

ANDY JENKINSON

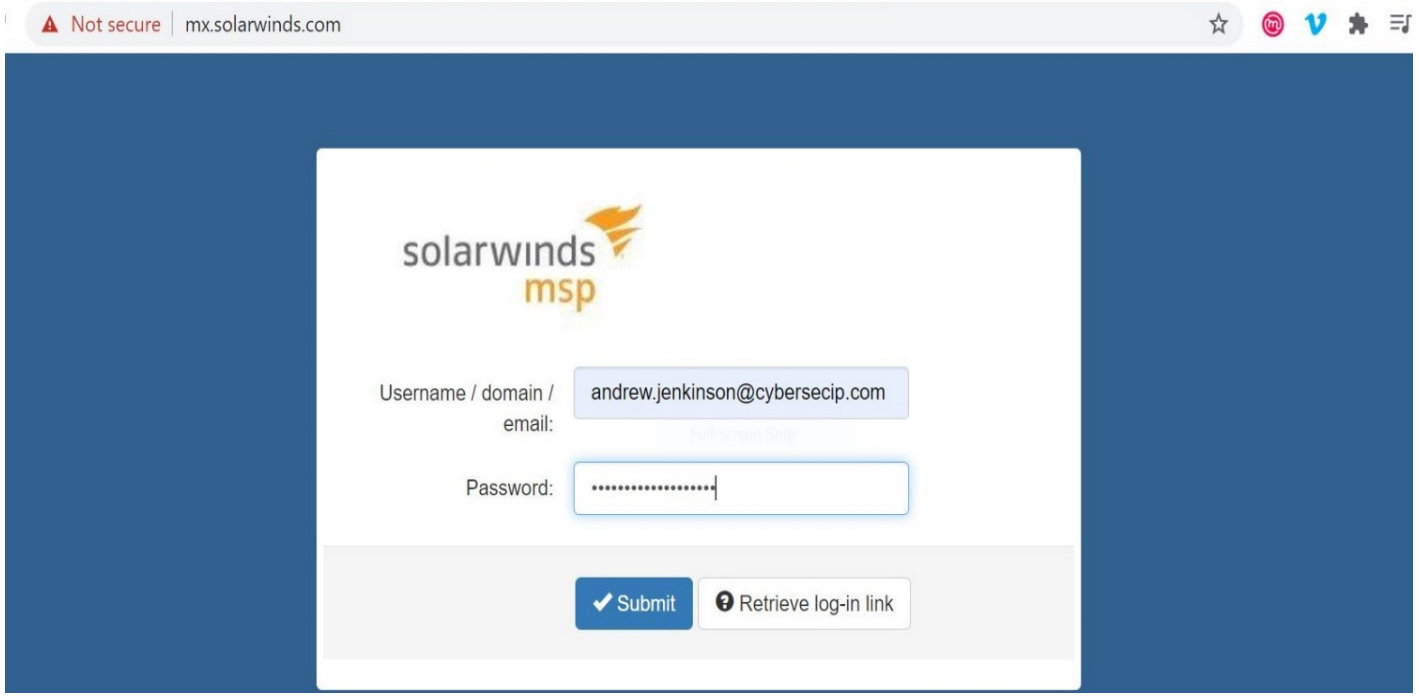
- Senior and seasoned innovative executive with over 30 years' experience as a hands-on lateral thinking CEO, coach, and leader. A 'big deal' business accelerator, and inspirational lateral thinker.
- Crafted, created and been responsible for delivering over £100M of projects within the Cyber, Technical, Risk and Compliance markets with some of the world's largest leading organisations.
- Demonstrable track record of large-scale technical delivery and management within Professional Services, Managed Services and Financial Services environments.

Research & Publications

“TRUST NOTHING, VALIDATE EVERYTHING”

- One of the first, and possibly one of very few people to discover the plethora of insecure SolarWinds domains. It has since been proven that Andy’s version of the attack of an insecure sub domain being hijacked and a nefarious website being stood up, is now common knowledge as being the initial access and root cause of the initial infiltration (Sunburst)
- Research and a paper was presented to the United States Senate Intelligence Committee overseeing the SolarWinds breach earlier this year.
- Just finished writing a second book on his experience and in-depth research of over 1000 companies over the last few years, all of whom have been victims of cyber and ransomware attacks.
- The first book is titled “**Stuxnet to Sunburst”** and the second **“Ransomware and Cybercrime”**

Solarwinds – the lessons of being “not secure”



The initial infiltration was via a Not Secure Website that was hijacked and suffered a Domain takeover that led to full Administration Access.

One of several Not Secure SolarWinds websites as can be clearly shown in the address bar. Furthermore, at the time, a few weeks ago, this site was live 6 months post initial breach.

In December 2020 the infiltration was discovered of SolarWinds. SolarWinds is a US based Global technology and security company that supplies the US government, US Treasury and thousands more.

It is estimated that over 18,000 clients have consequently been infiltrated.

Solarwinds –scan summary

The SolarWinds full website security research CRI (Cyber Rating Index) can be seen as an F and 10/100.

This CRI takes many security metrics into account, some are listed in the next slide.

Suffice to say, the CRI is neither subjective, or opinionated, it is because there are fundamental security issues of the website and/or webservers including subdomains that are connected (sharing data).

CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

Identifying security issues

The table below is just a small selection of the major security issues we look for (as do cyber criminals) using OSINT (Open Source Intelligence).

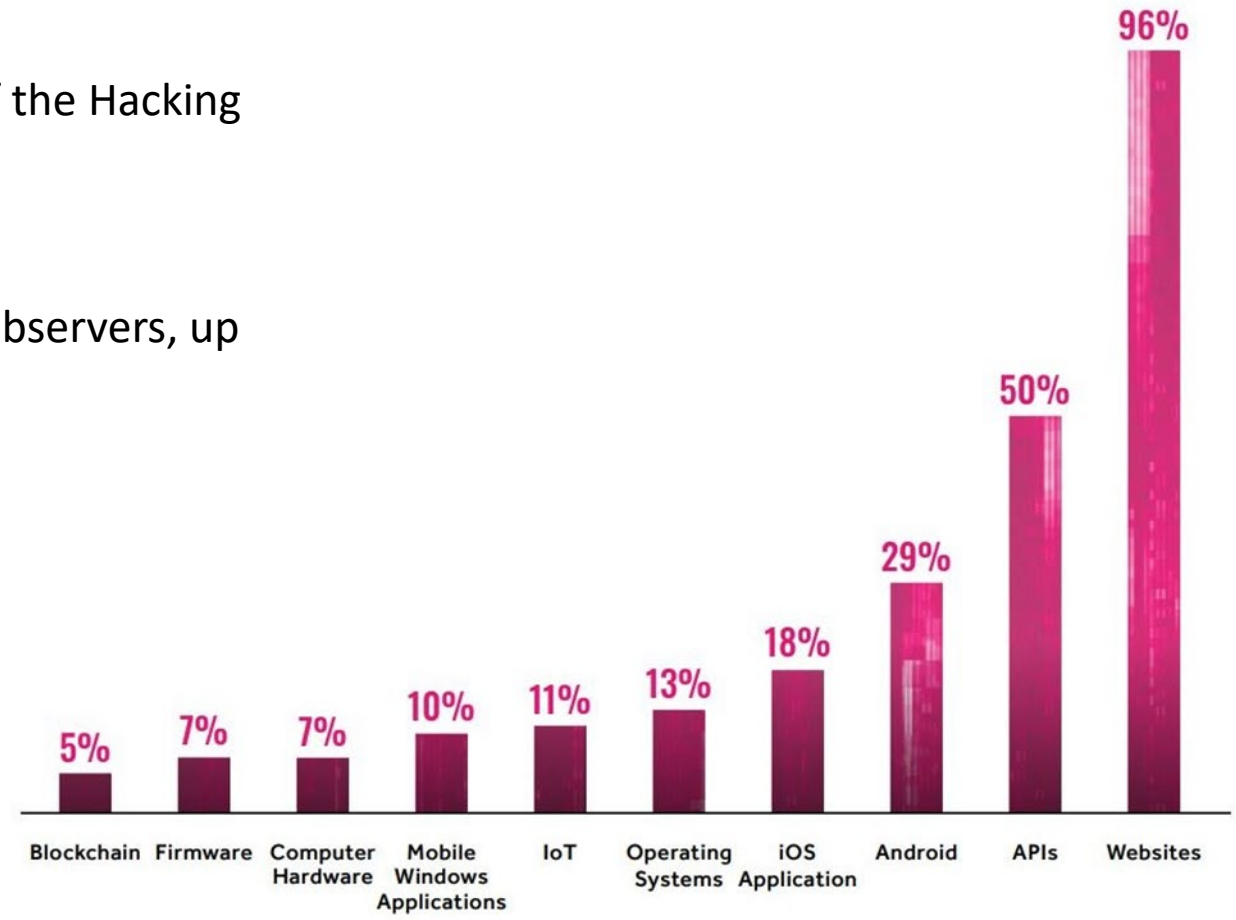
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain
Redirection	✗	-20	Invalid certificate chain encountered during redirection
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via `src="//..."`
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented

We use these methods to provide **Actionable Intelligence**, whereas Cyber criminals use it to identify **weak infiltration access.**

What technologies are hackers working on?

Hacker One, the global leading source of the Hacking World 2021 Report.

96% of all Hackers hack websites and webservers, up from 71% in 2020.



CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

Website security and the ESA

What does all this have to do with the European Space Agency and the sector as a whole?

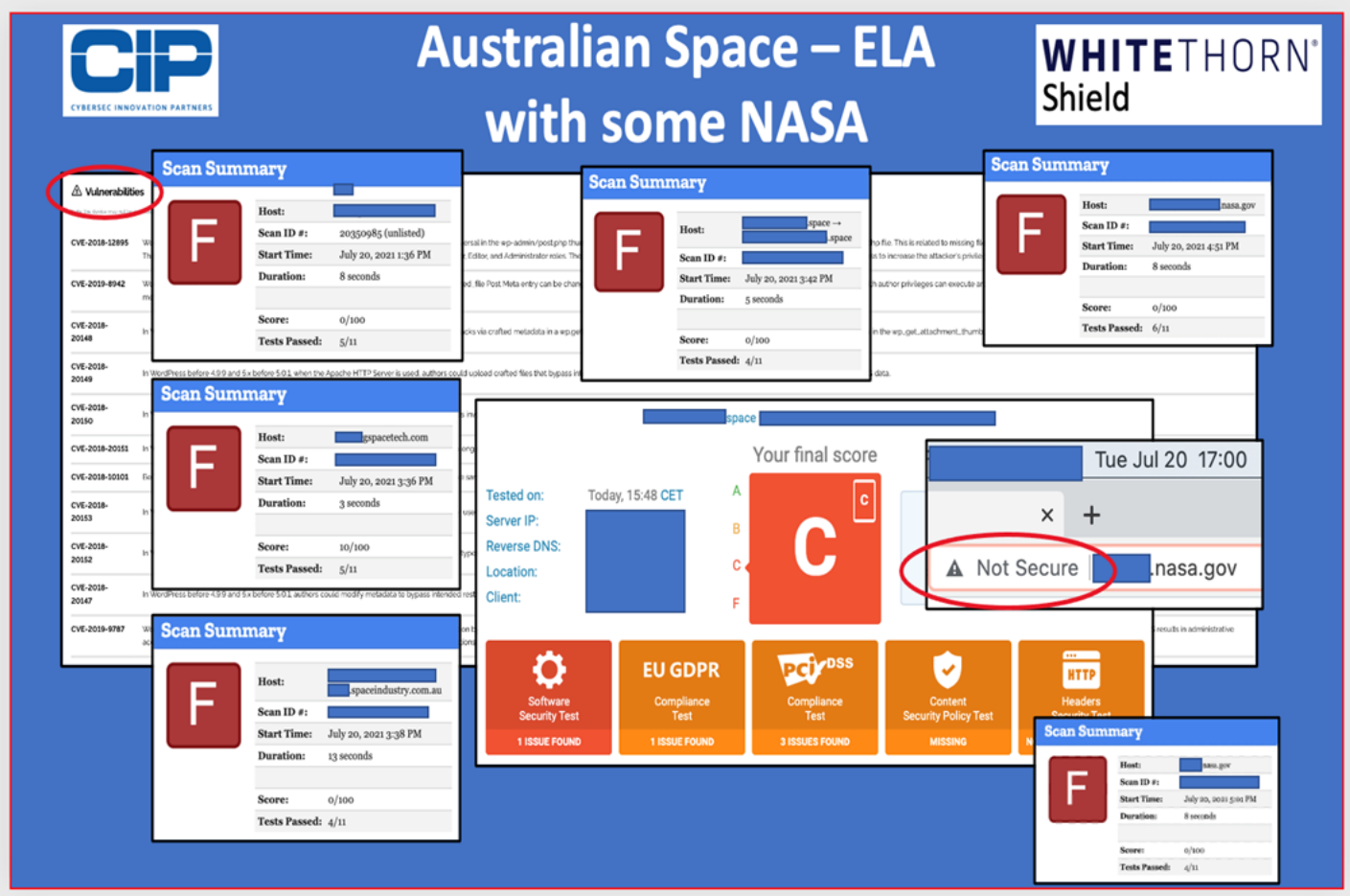
NASA has 23,699 websites, the majority are legacy, the majority are also Not Secure…

The sample on the next slide should make everyone want to ask the question, how secure is our Intellectual Property (IP) and PII (Personal Identifiable Information)?

CIP
CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

Website security and the ESA



Our vulnerability team undertook some basic security research across several Australian Space companies, the results below should act as a wake up call, a catalyst to take website and webserver security seriously.

Currently, the companies below would be as easy to infiltrate as walking into a local Starbucks, taking plain text data (cannon fodder for cyber criminals) and holding the company to Ransom for the encrypted data, or selling to competitors.

Website security and the ESA

Recently, you will possibly all be aware of challenges including technical and access issues that Hubble Telescope has had.

We decided to do some research on the basic, fundamental security position of Hubble and looked at just a few of the websites.

The website www.hubblesite.org again, looks perfectly secure, however is anything but as you can see from the CRI rating below.

Could the challenges be due to operational infiltration? Of course…

CYBERSEC INNOVATION PARTNERS

WHITETHORN®
WHITETHORN® SHIELD

Thank you

QUESTIONS

Contact me:

Andrew.Jenkinson@cybersecip.com

Cybersec Innovation Partners, 24/25 The Shard, 32 London Bridge Street, London SE1 9SG