

WHITETHORN° WHITETHORN° SHIELD

+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
+	+ D k	+ 1	+ nd	+ + h	+		+	+	+ nia	+		+	+	+	+	+	
+			nd al c										+	+	+	+	
+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
+	+ Droe	+ sentat	+ tion to	+ Euro	+	+ Snace	+ Δσοη	+	+ mnosi	+	+	+	+	+	+	+	
+	+		+	+	+	- +	+ +	+ +	+	+	+	+	+	+	+	+	

- July 2021
- + + + + + + + + + + + + + + + +



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"

| Not secure mx.solarwinds.com | ☆ | 0 | V | * | =J |
|--|---|---|---|---|----|
| | | | | | |
| solarwinds
msp | | | | | |
| Username / domain /
email:
Password: | | | | | |
| rasswiru. | | | | | |

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

WHITETHORN[®] WHITETHORN[®] SHIELD

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

Scan Summary

| Host: | solarwinds.com →
www.solarwinds.com |
|-------------|--|
| Scan ID #: | 20350459 (unlisted) |
| Start Time: | July 20, 2021 12:53 PM |
| Duration: | 4 seconds |
| Score: | 10/100 |

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).



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 |

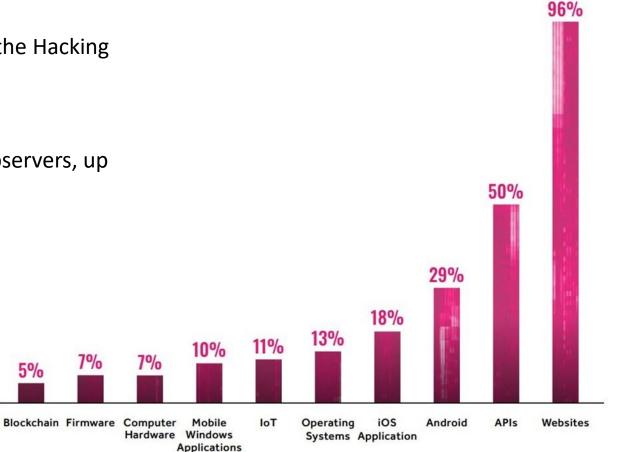
We use these methods to provide Actionable Intelligence, whereas Cyber criminals use it to identify weak infiltration access.



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.





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)?



WHITETHORN° WHITETHORN° SHIELD

Website security and the ESA

| CYBERSEC INNOVATION PARTNERS | | lian Space – E
1 some NASA | Shield |
|--|--|---------------------------------------|--|
| Scan Summary | | Scan Summary | Scan Summary |
| CVE-2016-12895 With The Start Time: | 20350985 (unlisted)
ersti in the ep-admin/pod prop th
July 20, 2021 1:36 PM
t Editor, and Administrator raise. Th | Host: space → | No file. This is restand to missing file
is to nervase the attacker's pade
Duration: 8 seconds |
| CVE-2019-0942 W Duration:
CVE-2019-0942 W Score:
20148 In Tests Passed: | 8 seconds ed. Be Post Meta entry can be cha | Duration: 5 seconds | h autro privileges can execute a Score: 0/100 n Bw vp.get.sttadmett.Bune Tests Passed: 6/11 |
| CVE-2018-
20149 In WordPress before 4.9.9 and 5.4 before 5.0.1 when the Ap
CVE-2018-
20169 In International Content of the Ap | coche HTTP Server is used authors could usload orafted files that bypass i
a ina | Tests Passed: 4/11 | dra. |
| CV6-2016-20161 10
CV6-2016-20161 10
CV6-2016-10101 fo
CV6-2016-10101 fo
CV6-2016-10101 fo
Duration: | July 20, 2021 3:36 PM 3:56
3 seconds Tested on: | Your final scor
Today, 15:48 CET A | |
| 20153 in
CVE-2018-
20152 in
Tests Passed: | 10/100 by Reverse DNS:
5/11 Location: | | × + |
| CVE-2018-
2017 In WordPress before 4.99 and 5x before 5.01 authors cour
CVE-2018-9787 W Scan Summary | ac modify metadata to bypass intended rest Client: | F | retubi in administrative |
| Host:
Scan ID #: | spaceindustry.com.au
Software
Security Tes
Yaly 20, 2021 3:38 PM | | Content
Security Policy Test
Missing N |
| Start Time: J | | | |

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

Scan Summary

| ſ | 7 | |
|---|---|--|
| | | |
| | | |

| Host: | hubblesite.org |
|-------------|-----------------------|
| Scan ID #: | 19923726 (unlisted) |
| Start Time: | June 29, 2021 1:53 PM |
| Duration: | 5 seconds |
| | |
| Score: | 0/100 |

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 <u>www.hubblesite.org</u> 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...



| + | + + | + | + | + | + | + | + | + | + | + | + | + | + | + | + · |
|---|---------------------------------------|--------------------|----------------------|---------------------|---------------------|-------------|------------|---|---|---|---|---|---|---|-----|
| + | Thank | yo | U, | + | + | + | + | + | + | + | + | + | + | + | + • |
| + | | | +
\ \ | + | + | + | + | + | + | + | + | + | + | + | + · |
| + | + + | + | + | + | + | + | + | + | + | + | + | + | + | + | + · |
| + | Contact me: | + | + | + | + | + | + | + | + | + | + | + | + | + | + • |
| | Andrew.Jenkinson@cybersecip.com | | | | | | | | | | | | | | |
| + | + + | + | + | + | + | + | + | + | + | + | + | + | + | + | + · |
| + | Cybersec Innovation Pa | rtners, 24/2 | 25 The Share | d, <u>3</u> 2 Londo | on Bridge St | reet, Londo | on SE1 9SG | + | + | + | + | + | + | + | + · |
| | Registered in England & Wales No 1146 | 5050. Registered O | ffice: Linden House, | Linden Close, Tunb | ridge Wells, TN4 8H | н | | | | | | | | | |
| + | + + | + | + | + | + | + | + | + | + | + | + | + | + | + | + · |