OVERVIEW

Welcome to another issue of the Iris Messenger! As you may have noticed, the formatting has slightly changed - this is the result of moving from LaTeX -> PDF to a Markdown -> LaTeX -> PDF conversion. The hope is to make editing future editions an easier process and to allow much easier collaboration.

This issue features hacking and stupidity - two concepts that should never mix.

NEW GLOBAL RANSOMWARE

A new ransomware named "Petya" has been released, despite Petya denying having authored the software. The attack, thought to be targeting Ukraine's infrastructure, has also shut off the sensor system in the Chernobyl radiation area, a Danish shipping company, Russian oil giant, British advertising company and a law firm - although the full extent of the attack is not yet known http://goo.gl/46z4Ny.

Various aspects of the attack are reminiscent of the underlying techniques behind the WannaCry attack, as part of the NSA tools leak of zero day exploits. Despite relatively little media coverage, major shipping networks have been brought to their knees, potentially causing real economic damage to global shipping routes http://goo.gl/Vbs22D.

.FEEDBACK SCAM

ICANN have allowed a new TLD to be registered, the .feedback extension. Shortly after registering the TLD, 5k of the top used domains were pre-registered and host fake feedback websites for their users. The TLD can either be bought for $600 a year or the feedback bought for $20 a month, forcing companies to buy into this service or deal with angry customers http://goo.gl/1AGbu3.

DARK WEB & UK POLICE

Leaflets have been distributed across the UK to spread awareness of suspicious activities in the aid of anti-terrorism. Of the list of suspicious activities, visiting the dark web and ordering unusual items is included http://goo.gl/nw3dik.

STUPIDLY SIMPLE DDOS PROTOCOL

Cloudflare recently detected an attack in excess of 100Gbps, making use of a UDP protocol on port 1900 behind badly configured firewalls. By spoofing the source address, a request asks for a list of devices behind the network. With approximately 10Gbps of spoofing traffic and 940k of "reflector" IPs, attackers see a gain of 10 times to a target address http://goo.gl/Jhszdf.

US NUKE LAB SHUTDOWN

A nuclear lab based in Los Alamos, US, has been shutdown after employees posed 8 handcrafted plutonium rods in close proximity - just for a picture. The lab's safety engineers left in protest of the poor working conditions, including a cover up by managers http://goo.gl/mxJjFz.

JAIL MISTAKES BY BAD SOFTWARE

Judges have refused to order a fix for jail software that incorrectly jails innocent people. Roughly 2k motions have been filed, many of which have served unnecessary jail time http://goo.gl/JouUcF.

CALIFORNIA SOMETIMES TOO GREEN

California has invested heavily in renewable energy in the last few years, with solar power producing *too much energy* on some of the brightest days of the year. The result of this is that they have to pay local states to take the energy, otherwise risk overloading the grid http://goo.gl/LBXxEi.

ARTICLES OF INTEREST

This week's collection of interesting articles:

- http://goo.gl/wBPRFT - 5 days drone flight.
- http://goo.gl/9CFYmE - WhatsApp apology from Guardian.
- http://goo.gl/P9SVWE - 9 line neural network.
- http://goo.gl/DhXmWG - Fitbit data on users sleep data.

Future suggestions welcome.