Security Now! #623 - 08-08-17

Inching Forward

This week on Security Now!

This week we discuss and look into DigiCert's acquisition of Symantec's certificate authority business unit, LogMeIn's LastPass Premium price hike, the troubling case of Marcus Hutchins' post-Defcon arrest, another instance of WannaCry-style SMBv1 propagation, this week's horrific IoT example, some hopeful IoT legislation, the consequences of rooting early Amazon Echoes, the drip drip drip of Wikileaks Vault 7 drips again, Mozilla's VERY interesting easy-to-use secure large file encrypted store and forward service, the need to know what your VPN service is really up to, a bit of errata, miscellany, and some closing-the-loop feedback from our always-attentive terrific listeners.

"GSM Cell Providers before and during BlackHat & DefCon"

Before <--------> During

Security News

DigiCert purchases Symantec's CA business unit.
https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0802_01
https://www.digicert.com/news/digicert-to-acquire-symantec-website-security-business

Before I comment I want to be ABSOLUTELY clear with everyone: I have ZERO inside knowledge about this transaction. I have spoke with no one at DigiCert or Symantec about this. So any and all conclusions are solely my own.

All of our listeners know that I could not be more bullish on and delighted with the quality of DigiCert's services and their support. And our long time listeners will recall that I was driven away from the Symantec/Verisign duet, into the arms of DigiCert, because I was so unhappy with Symantec's performance.

And our listeners also know that DigiCert has been uniquely able to meet some of my weirder requests, such as minting a pair of certs with specific year-end expirations and signature hash lengths to satisfy Chrome while keeping GRC available as long as possible to older web clients. And I cannot imagine having obtained that sort of attention from Symantec.

So I'm not going to pretend for an instant to be an unbiased objective observer... though my biases are public and, I believe, well earned and well deserved.

If Symantec had purchased DigiCert (much as LogMeIn purchased LastPass, which we'll discuss next) I would be heartsick right now, since being able to work with and depend upon a high quality certificate authority is way up there in my own hierarchy of needs. It's probably only second to Level3 being GRC's bandwidth provider. But, thank goodness, the acquisition was the other way around.

DigiCert purchased Symantec's entire Certificate Authority business for... $950 million in cash plus a 30 percent stake in DigiCert.

In eMail from DigiCert John Merrill…

> Also, some of you may be wondering about any implications our announced acquisition will have on the ongoing debate between Symantec and the browser community about trust in their certificates.
>
> Earlier this year, the browsers proposed a plan to limit trust in Symantec certificates after discovering issues with how they were validating and issuing digital certificates. Importantly, we feel confident that this agreement will satisfy the needs of the browser community.
>
> DigiCert is communicating this deal and its intentions to the browser community and will continue to work closely with them during the period leading up to our closing the transaction. DigiCert appreciates and shares the browsers’ commitment to engendering trust in digital certificates and protecting all users.

Garrett Bekker, the principal security analyst at 451 Research said "Symantec's certificate business will immediately increase DigiCert's market share and make the company one of the biggest players in the PKI and SSL markets. This will make DigiCert pretty much one of the leaders in terms of revenues in the digital certificate business."

Okay... In retrospect this makes SO MUCH SENSE.

A certificate authority lives and dies by its attention to detail, and the earned trust in the integrity of the assertions made by its signed certificates. As we know, that trust is, as it should be, hard won and easily lost... and Symantec lost the industry's trust.

But, having acquired the business from Verisign, Symantec was a huge going concern with a large customer base... which it could no longer effectively leverage. So this transfer of "trust requiring" assets from an untrusted owner who could no longer effectively leverage them, to a highly trusted owner who can, makes total sense.

It will be interesting to watch how DigiCert handles this. the good news is that the certificate minting business is inherently scalable and DigiCert should be able to acquire and transfer Symantec's certificate customer base without needing to massively expand.

LogMeIn, who purchased LastPass, has doubled its Premium pricing from $12/year to $24/year.

There have been a class of users who were willingly paying $1/month to support Joe back in the beginning and inertia -- and LastPass's value at $1/month -- kept them subscribed. It remains to be seen how those people will feel about the jump.

The LastPass Free offering remains fully functional and useful.

What I care most about are the security guarantees that LastPass offers and the quality of their service. As with the CA business, trust is hard earned and easily lost. And so far Joe & Company, even since the LogMeIn acquisition, has never let us down. They have continually responded with such speed that Tavis was barely dried off after his shower before LastPass had fixed the obscure bug that Tavis' ruminating had uncovered. That's all we could ever ask and it's much more than is commonly delivered.

If THAT ever changes we'll have serious cause for concern. But we have none yet.

I'll be remaining with LastPass, while also completely understanding if paying users are sufficiently annoyed to terminate their double-price subscription and either drop back to LastPass FREE, or look around for other solutions.

Marcus Hutchins who stopped the WannaCry worm by registering the DNS domain it was checking was arrested
https://arstechnica.com/tech-policy/2017/08/researcher-who-stopped-wcry-worm-detained-under-mysterious-circumstances/
https://www.wired.com/story/wannacry-malwaretech-arrest

As we'll recall, Marcus Hutchins was the white-hat hacker who reverse engineered enough of the WannaCry work to spot its attempt to retrieve a web asset from a bizarrely named and, at the time, unregistered domain. Upon registering that domain the worm's fetches resolved and all copies of the massively-spreading worm ceased scanning and reproducing themselves.

Then, Last Wednesday, as Wired wrote: ... authorities detained 22-year-old [Marcus] Hutchins (ArsTechnica says he's 23 which is confirmed by a screen shot of the City of Herderson, Las Vegas booking information.) after the Defcon hacker conference in Las Vegas as he attempted to fly home to the UK, where he works as a researcher for the security firm Kryptos Logic. Upon his arrest, the Department of Justice unsealed an indictment against Hutchins, charging that he created the Kronos banking trojan, a widespread piece of malware used to steal banking credentials for fraud. He's accused of intentionally creating that banking malware for criminal use, as well as being part of a conspiracy to sell it for $3,000 between 2014 and 2015 on cybercrime market sites such as the now-defunct AlphaBay dark web market.

(Note that last Friday Marcus denied any wrongdoing and pleaded not guilty to the charges against him. He has a court date in Milwaukee set for TODAY (August 8, 2017) and was being held in Las Vegas jail.)

(Also note that using the alias "MalwareTech" and using the Twitter handle "@MalwareTechBlog" may not be helpful.)

[Paraphrasing Wired a bit for length] But the short, eight-page indictment against Hutchins has already raised questions and skepticism in both legal and cybersecurity circles. Orin Kerr, a law professor at George Washington University who has written extensively about cybersecurity and hacking cases, says that based on the indictment alone, the charges look like "a stretch." Although the indictment claims Hutchins wrote the Kronos malware, nothing in the document illustrates that Hutchins possessed actual intent for the malware he allegedly created to be used in the criminal "conspiracy" he's accused of.

Kerr said: "It’s not a crime to create malware. It’s not a crime to sell malware. It’s a crime to sell malware with the intent to further someone else’s crime. This story alone doesn’t really fit. There's got to be more to it, or it’s going to run into legal problems."

Some associates of Hutchins defended him Thursday on Twitter, even arguing that he has worked directly with US law enforcement. Kevin Beaumont, a UK-based security architect wrote: "I know Marcus. He has a business which fights against exactly this (bot malware), it's all he does. He feeds that info to US law enforcement. The DoJ has seriously F'ed this up."

Jake Williams, another well-known researcher with the security firm, Rendition Infosec said he'd worked with Hutchins multiple times since 2013, met him in person at last year's Defcon, and shared malware samples. At one point in 2014, Williams says Hutchins refused his offer of

payment for help on an educational project. And, even when Hutchins was awarded a $10,000 "bug bounty" from security firm HackerOne for his work on stopping WannaCry... he gave it away to charity. Williams wrote: "I have pretty good black hat radar. It NEVER went off when talking to Marcus or exchanging stuff with him."

Wired finishes, writing: For the moment, neither the FBI nor the Department of Justice is commenting further on Hutchins' case beyond the DOJ's statement and the facts of the indictment. A spokesperson for the Electronic Frontier Foundation, which often offers legal representation to embattled hackers, wrote in a statement to WIRED that it's "deeply concerned" about Hutchins' arrest and are reaching out to him.

The EFF tweeted: EFF is deeply concerned about security researcher Marcus Hutchins' arrest. We are looking into the matter, and reaching out to Hutchins.
— EFF (@EFF) August 3, 2017

Legal Defense Fund accepting donations:

- https://secure.lawpay.com/pages/torekeland/hutchinsldf

WannaCry Inspires Banking Trojan to Add Self-Spreading Ability
http://thehackernews.com/2017/08/trickbot-banking-trojan.html

Researchers at Flashpoint have discovered that the TrickBot Banking Malware Trojan has just been evolved to add WannaCry-style SMBv1 LAN scanning and propagation. It doesn't yet have the capability of scanning out into the public Internet, which was WannaCry's claim to fame. But it does probe LAN-based servers via the NetServerEnum Windows API and enumerate other computers on the network via Lightweight Directory Access Protocol (LDAP). So if it gets inside an enterprise network which has not yet administratively and globally disabled SMBv1 (do it now!) it could create a real mess. And it's foreseeable that this won't be the last re-use of the SMBv1 vulnerability we encounter.

This Week in IoT (where the "S" in IoT stands for Security)
Approximately 175,000 Chinese Internet connected security cameras made by one manufacturer can be easily located with Shodan and then hacked.
http://securityaffairs.co/wordpress/61595/iot/security-cameras-flaws.html
https://drive.google.com/file/d/0BytbxOde47O6VGxjMFh0VWIybWs/view

The guys at Bitdefender, after doing some poking around with the Shodan Internet device search service, identified approximately 175,000 currently online and connected security cameras with what can only be described as blatant remote access vulnerabilities.

The vulnerable cameras are manufactured by a Chinese company Shenzhen Neo Electronics who offer surveillance and security solutions, including IP cameras, sensors and alarms.

The Bitdefender researchers discovered several buffer overflow vulnerabilities in two models of their cameras: the iDoorbell and the NIP-22 models. Because many of Shenzhen Neo's devices reuse the same firmware the researchers believe that other models are also certainly vulnerable.

The security cameras use UPnP (Universal Plug and Play) to automatically open ports through their user's firewall/router to allow incoming access from the Internet. Querying the Shodan search engine for vulnerable devices the researchers discovered between 100,000 and 140,000 vulnerable devices worldwide.

Note that this is the easiest, least caring, least careful and sloppiest way of doing this: simply creating Internet-exposed TCP servers.

The proper way to do this is for such devices to occasionally send a single UDP packet out to a publicly-accessible remote server. The outbound UDP packet automatically creates return-packet mapping through any and all NAT routers along the way, denying incoming traffic from any but the single remote IP. Then the remote server can send instructions back to the camera when it wishes to enable audio and video streaming.

Instead, these cretins were utterly lazy. They use UPnP to open static incoming ports through the user's router, allowing ANYONE and EVERYONE to access the camera.

On top of this, Bitdefender found that both security camera models are vulnerable to two different remote attacks, one that affects the web server service running on cameras and another that affects the RSTP (Real Time Streaming Protocol) server. They showed that it was quite easy to exploit the flaws in the security cameras, anyone can hack access the livestream by simply logging in with default credentials (i.e. "user," "user," and "guest," "guest"). They also found several buffer overflow vulnerabilities that could be exploited to take control of the cameras remotely.

An example of one vulnerability is in the publicly exposed HTTP service. It is triggered by an error in the way the application processes the username and password information at login. As the user attempts to authenticate, the credentials are passed in a GET request with name=value parameter pairs: "http://<ip>/?usr=<user>&pwd=<password>". But when the web authentication function parses these values, the "libs_parsedata" function copies the content of the two arguments onto the stack without checking their actual size. Thus allowing for an out of bound data write onto the device's stack.

Shenzhen Neo did not comment about the discovery.

The full Bitdefender report is linked in the show notes for anyone who is curious to know more.

But, in VERY good IoT news, a new US Senate bill proposes security standards for Internet-connected smart devices
http://thehackernews.com/2017/08/iot-bill-security-standard.html
https://www.techdirt.com/articles/20170804/11060637926/us-senators-unveil-their-attempt-to-secure-internet-very-broken-things.shtml

A pair of US Senators, one from each political party, Virginia's Democratic Senator Mark Warner and Colorado's Republican Senator Cory Gardner have introduced a new bill titled "The Internet of Things Cybersecurity Improvement Act of 2017.

It forbids any Internet connected devices purchased by the US government from having hard-coded (unchangeable) usernames and passwords in their devices.

The legislation also require vendors to ensure that their devices are patchable, and, at the time they are purchased, are free from already known vulnerabilities.

Firmware updates must have an effective authentication mechanism, such as a secure digital signature, which prevents unauthorized updates.

The device must use only non-deprecated, industry-standard protocols and technologies for communications, encryption, and interconnection with other devices or peripherals.

The device be updatable: <quoting from the legislation> Requires such Internet-connected device software or firmware component to be updated or replaced, consistent with other provisions in the contract governing the term of support, in a manner that allows for any future security vulnerability or defect in any part of the software or firmware to be patched in order to fix or remove a vulnerability or defect in the software or firmware component in a properly authenticated and secure manner.

And it must be repaired in a timely fashion: Requires the contractor to provide a repair or replacement in a timely manner in respect to any new security vulnerability discovered through any of the NIST and other relevant security databases or from the coordinated disclosure program.

Rooting an Amazon Echo is now (or was) a thing...
Mark Barnes, 1 August 2017: Alexa, are you listening?
MWR Info Security
https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening
http://thehackernews.com/2017/08/hacking-amazon-echo-spying.html

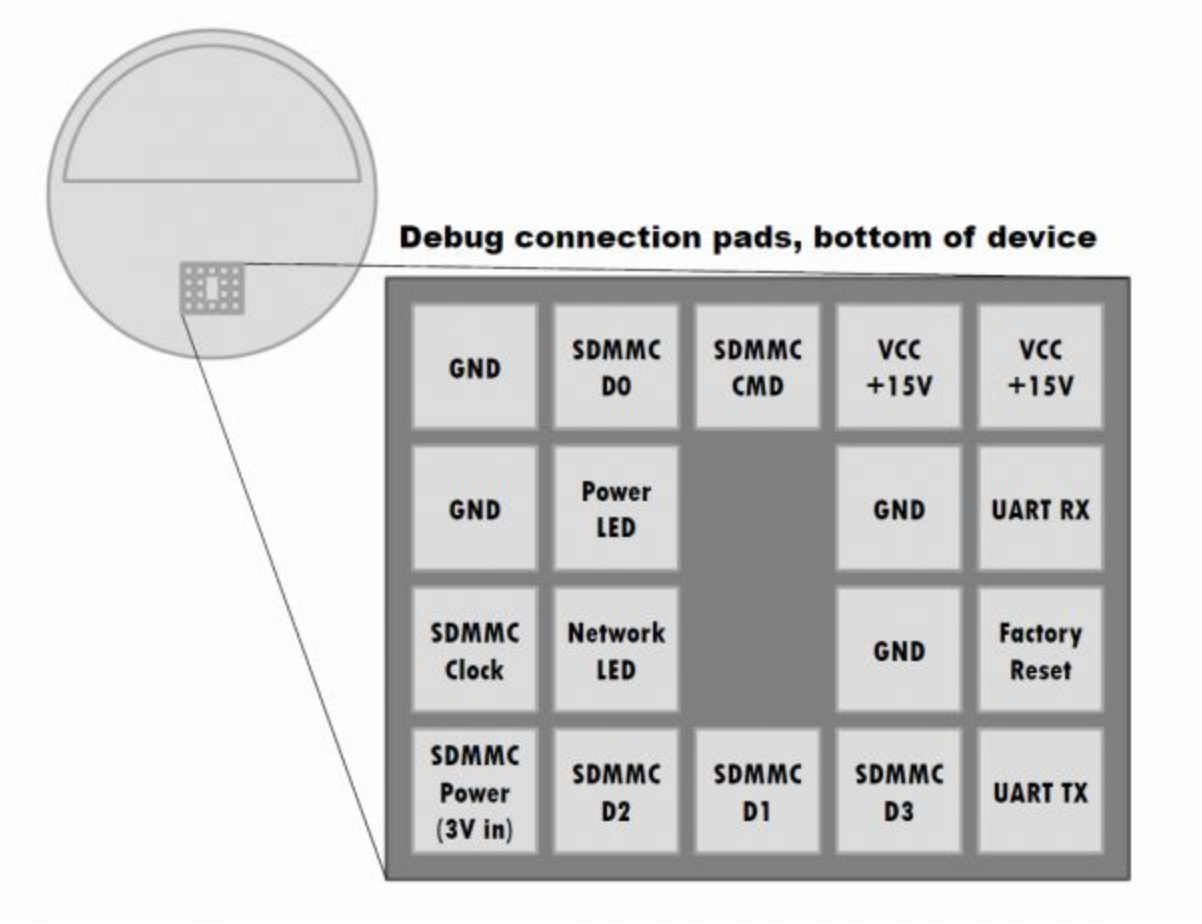
An interesting but not overly alarming physical access (aka Evil Maid) hack of early 2015 and 2016 model Amazon Echoes.

Under the rubber base of the earlier Echoes is an 18-connection debugging and access pad providing a serial terminal interface and remote SD card booting interconnect *(see next page for a diagram of the exposed interface)*. Together, they allow the device to be monitored, probed, and fully commandeered without opening the Echo any further.

Mark Barnes said that his team developed scripts that leveraged tools embedded on the Amazon Echo to continuously stream the raw microphone audio over TCP/IP to a remote server without affecting the actual functionality of the device itself... thus turning it into an always-on home surveillance device.

Thus, in a fully developed attack scenario, an "Evil Maid" would disconnect the Echo's power, remove the rubber footing, press a square connector pad against the exposed 18-connection debugging surface, power-up the Echo and wait while it boots. The external SD memory would take over, modify and rewrite the Echo's internal firmware, turning the device into anything the

attackers wished. Then the boot-override would be removed, the rubber base reaffixed, and the Echo returned to its original location.



Users owning this year's 2017 models of the device are not affected by this latest hack, as the new models introduced a mitigation that joins two of the crucial debugging pads in a way that prevents the device from external booting.

The takeaway here is that while this is an interesting attack, we've seen these before, such as with the Samsung television attack which, similarly, required that a USB thumb drive be physically inserted into the television.

The drip drip drip of WikiLeaks Vault 7 CIA Leaks continues
This is How CIA Disables Security Cameras During Hollywood-Style Operations
http://thehackernews.com/2017/08/surveillance-camera-hacking.html
https://wikileaks.org/vault7/#Dumbo

Requirements:

- Dumbo program requires SYSTEM level privilege to run.
- The USB drive must remain plugged into the system throughout the operation to maintain control over connected surveillance devices.

Capabilities:

- Mute all microphones
- Disables all network adapters
- Suspends any processes using a camera recording device
- Selectively corrupted or delete recordings

This has the feeling of something that was originally purpose-specific, created to address a specific need somewhere. Agents needed to shut down a audio/video surveillance facility where a blackout was preferable to being seen and recorded. So this tool was commissioned and created for that purpose... and it was then added to the arsenal of possible useful tools.

Firefox's VERY INTERESTING new "Send" service
https://send.firefox.com/
Firefox Test Pilot / web experiment
All public and open source on Github.
Uses AWS for file storage.

1. Drop a file into the page.
2. JavaScript running in the browser generates a random symmetric key and encrypts the file.
3. Gets a unique file identifier token from the server & uploads the encrypted file to the server.
4. The browser displays a URL containing the server-provided file ID plus the decryption key following a # pound sign.
5. This URL is then sent to someone else who may use it to:
6. Download the encrypted file and decrypt it on the user's machine.
7. Once downloaded the file is deleted from the server.
8. After 24 hours the file is deleted from the server.

"For the most reliable operation, it's best to keep your file under 1GB"
Quote: "Send lets you upload and encrypt large files (up to 1GB) to share online. When you upload a file, Send creates a link to pass along to whoever you want. Each link created by Send will expire after 1 download or 24 hours, and all sent files will be automatically deleted from the Send server.

Unlike other Test Pilot experiments, Send does not require an add-on, and can be used in any modern browser."

https://send.firefox.com/download/10cb15a779/#MH-CW3onPdrrswDShACgVA
download / {file identifier} /# {symmetric encryption key}

VERY CLEVER: The data folllowing the '#" pound sign is never sent to the server.
Wikipedia says: The fragment identifier functions differently than the rest of the URI: namely, its processing is exclusively client-side with no participation from the server. When an agent (such as a Web browser) requests a resource from a Web server, the agent sends the URI to the server, but does not send the fragment. Instead, the agent waits for the server to send the resource, and then the agent processes the resource according to the fragment value. In the most common case, the agent scrolls a Web page down to the anchor element which has an attribute string equal to the fragment value. Other client behaviors are possible.

The IETF says: 4.1. Fragment Identifier

> When a URI reference is used to perform a retrieval action on the identified resource, the optional fragment identifier, separated from the URI by a crosshatch ("#") character, consists of additional reference information to be interpreted by the user agent after the retrieval action has been successfully completed. As such, it is not part of a URI, but is often used in conjunction with a URI.

Hotspot Shield VPN accused of spying on its users and selling

Developed by Anchorfree GmbH, Hotspot Shield is a free VPN service available on the Windows, Windows Phone, Mac, iOS, Android, Chrome.

An estimated 500 million users around the world.

But, sometimes you get what you pay for. The Centre for Democracy and Technology, a US-based non-profit advocacy group, working with Carnegie Mellon University who carefully examined the Hotspot Shield system and clients, yesterday filed a 14-page complaint with the US Federal Trade Commission alleging that it is willfully violating its own privacy policy of providing "complete anonymity".

The Hotspot Shield VPN app promises to "secure all online activities," hide users' IP addresses and their identities, protect them from tracking, and keep no connections logs while protecting its user's internet traffic using an encrypted channel.

However, according to research conducted by the CDT along with Carnegie Mellon University, the Hotspot Shield app fails to live up to all promises and instead logs all connections, monitors users' browsing habits, redirects online traffic and sells customer data to advertisers.

Hotspot Shield was also found injecting Javascript code using iframes for advertising and tracking purposes.

Reverse engineering of the app's code revealed that the VPN uses more than five different third-party tracking libraries.

Researchers found that the VPN app discloses sensitive data, including names of wireless networks (via SSID/BSSID info), along with unique identifiers such as its users unique Ethernet MAC addresses and mobile device IMEI numbers.

And, the VPN service sometimes redirects e-commerce traffic to partnering domains. If users visit commercial websites, the VPN app redirects that traffic to partner sites, including ad companies, to generate revenue. For example, when a user connects through the VPN to access specific commercial web domains, including major online retailers like www.target.com and www.macys.com, the application can intercept and redirect HTTP requests to partner websites that include online advertising companies."

Now... as we know, this is ALL tempered by the fact that not even a VPN can peer into HTTPS traffic. But they can still monitor IP addresses

And note that disclosing things like their users' MAC address and IMEI number cannot be dismissed as inadvertent and benign. it HAD to have been deliberate since neither of those unique identifiers would ever normally travel across and IP connection. Both MAC and MEI are strictly local-link network identifiers. So the Hotspot Shield client-side app needed to deliberately seek and send that information.

Once again, my refrain on this will be familiar to our listeners: Hotspot Shield has the right to whatever they choose. But they cannot misrepresent what they are doing. That's the CDT's only complaint. If users are truthfully informed about WHY their apps and its services are free, and how Hotspot Shield is monetizing their use of the free service, then I (and the CDT and FTC) would have no problem with that. But it's NOT okay to be offering a service which claims to provide absolute privacy enforcement while deliberately and by design violating that promise.

Our takeaway is that trust and reputation really matters for a VPN service provider, and understanding the provider's economic model is crucial.

Errata

Ed Moreau (@edmoreau)
@SGgrc re: SN 622 "not famous" "Bond actor" in "Colossus" has starred in "The Young and the Restless" (soap opera) for decades.

Miscellany

- The Rho Agenda Inception Trilogy (the backstory of Jack and Jane)
- The Original Rho Agenda Trilogy with the teenagers
- The Rho Agenda Assimilation Trilogy
    - The final book of trilogy #3 "The Meridian Ascent" was released yesterday.

(I am currently on book #14 of my re-read of the 19-book Frontiers Saga series.)

SpinRite

Darren in Brisbane, Australia
Subject: SpinRite SMART data and relative drive performance
Date: 15 Jul 2017 20:14:11

Hey Steve,
I have been using SpinRite on my Seagate NAS drives for years, each month or so picking the next drive to check. A few months ago I had a couple of drives give up completely so I replaced them with Western Digital Red drives.

I have been keeping track of the ECC corrected and Seek error counts and I've noticed a correlation between SpinRite's reported ECC counts and the time required to perform a full Level 4 SpinRite pass -- the more errors the longer SpinRite takes. The slowest remaining Seagate drive reports 1,350 million ECC errors, the next faster drive, which is still slow, shows around

850 million. But the new WD drives report 0 ECC and Seek errors and they also run MUCH faster under SpinRite.

So does this difference in ECC counts indicate that the WD drives overall performance will be much better than the Seagate drives?

I will also be very curious how these drives perform with the new version of SpinRite so I will join your news group when you get SQRL completed and are back to SpinRite development.

Love the podcast, have been listening during my commute to work for years, keep up the great work.

Closing The Loop

Chris Beattie (@jabbrwcky)
@SGgrc Why are enterprises fussing over TLS1.3 PFS when they're surely doing MITM for internal traffic inspection anyway? What am I missing?

Craig Naples (@crgn)
@SGgrc If we're mainly relying on ISPs to block ports exploited in SMB hacks, would using VPNs to bypass ISPs leave us more exposed?

Anthony Headley (@hossimo)
@SGgrc from the latest SN, you should probably switch to this CLI aws.amazon.com/cli/

AWS Command Line Interface
The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon S3.
Windows, Mac and Linux
https://aws.amazon.com/cli/

Seth Meister (@SethZero1)
@SGgrc - Love Spinrite! Is there an easy way to run it on an external HDD while actually using the Win computer it's plugged in to? Thanks.

Yes... It's possible to (and many people do) run SpinRite in a VM, giving it exclusive access to the external drive. This is FAR more practical that it might seem at first, since SpinRite and DOS can run in a VM with 640K of RAM. And it will use virtually ZERO of your hosting machine's CPU. We've seen photos of people running multiple

Rene Feliu (@renefeliu)
@SGgrc if Ransomware attacks a system, does it upload your data? If I get attacked should I assume my files could be copied to the bad guys?

Gary S. Martin (@GaryScottMartin)
@SGgrc RE: S3 Storage // What encryption solution are you using? You mentioned Duplicati in 2012 and Boxcryptor in 2014. Either of these?

CloudBerry Lab - One time fee for the software, not a "plan".
All the crypto was done right. And they have a full range of offerings from individual ($30) to enterprise. It's what I use to securely backup GRC's servers at Level 3.

Jeremy Malone (@garfwiz)
@SGgrc what we need for your barcoded voting paper is a "turbo entabulator" so the results are even faster

Someone noted that human unreadable barcode could also be hacked... So wouldn't a better solution be a human readable paper output?

Norbert Boron (@NorbertBoron)
@SGgrc if you rename special ep #85a to #85 and decrease all prior to that one by 1, you'll have ep #0 :)

(We have the best listeners! :)

~30~