Security Now! #589 - 12-06-16

Q&A #244

This week on Security Now!

- Android meets Gooligan, Windows Upgrades bypass Bitlocker, nearly one million UK routers taken down by a Mirai variant, the popular AirDroid app is "Doing it wrong", researchers invent a clever credit card disclosure hack, Cloudflare reports a new emerging botnet threat, deliberate backdoors discovered in 80 different models of Sony IP cameras, we get some closure on our SanFran MUNI hacker, a fun hack with Amazon's Echo and Google's Home, How to kill a USB port in seconds, a caution about keyless entry (and exit), too-easy-to-spoof fingerprint readers, an extremely troubling report from the UK, and finally some good news: the open-source covert USB hack defeating "BeamGun"!... plus a bunch of fun miscellany, some great Sci-Fi reader/listener book news, and... however many questions we're able to get to by the end of two hours!

From the always wonderful XKCD

http://xkcd.com/1758/

Security News

Gooligan Android Malware compromises 1 million Google accounts

- http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/
- <quote> As a result of a lot of hard work done by our security research teams, we revealed today a new and alarming malware campaign. The attack campaign, named Gooligan, breached the security of over one million Google accounts. The number continues to rise at an additional 13,000 breached devices each day. Our research exposes how the malware roots infected devices and steals authentication tokens that can be used to access data from Google Play, Gmail, Google Photos, Google Docs, G Suite, Google Drive, and more. Gooligan is a new variant of the Android malware campaign found by our researchers in the SnapPea app last year. Check Point reached out to the Google Security team immediately with information on this campaign. Our researchers are working closely with Google to investigate the source of the Gooligan.

- How do Android devices become infected?
    - <CheckPoint> We found traces of the Gooligan malware code in dozens of legitimate-looking apps on THIRD-PARTY Android app stores. These stores are an attractive alternative to Google Play because many of their apps are free, or offer free versions of paid apps. However, the security of these stores and the apps they sell aren't always verified. Gooligan-infected apps can also be installed using phishing scams where attackers broadcast links to infected apps to unsuspecting users via SMS or other messaging services.

- The malware simulates clicks on app advertisements provided by legitimate ad networks, causing the apps to install on the victim's device. Attacker are paid by the ad network when one of these apps is installed successfully.

- Logs collected by Check Point researchers show that every day Gooligan installs at least 30,000 apps fraudulently on breached devices or over 2 million apps since the campaign began.

- Gooligan is active in 86 apps available in third-party marketplaces and sends data about the device: http://www.bbc.com/news/technology-38167453

- Gooligan affects devices on Android 4 (Jelly Bean, KitKat) and 5 (Lollipop), which is over 74% of in-market devices today. About 57% of these devices are located in Asia and about 9% are in Europe.

- How does it all work?
  The infection begins when a user downloads and installs a Gooligan-infected app on a vulnerable Android device. CheckPoint's research team found infected apps on third-party app stores, but they could also be downloaded by Android users directly by tapping malicious links in phishing attack messages.

  After an infected app is installed, it sends data about the device to the campaign's Command and Control (C&C) server.

Gooligan then downloads a rootkit from the C&C server that takes advantage of multiple well-known (but typically unpatched) Android 4 and 5 exploits including VROOT (CVE-2013-6282) and Towelroot (CVE-2014-3153). These exploits still plague many devices today because security patches that fix them may not be available for some versions of Android, or the patches were never installed by the user. If rooting is successful, the attacker has full control of the device and can execute privileged commands remotely.

After achieving root access, Gooligan downloads a new, malicious module from the C&C server and installs it on the infected device. This module injects code into running Google Play or GMS (Google Mobile Services) to mimic user behavior so Gooligan can avoid detection, a technique which was first seen with the mobile malware HummingBad. The module allows Gooligan to:

- Steal a user's Google email account and authentication token information
- Install apps from Google Play and rate them to raise their reputation
- Install adware to generate revenue

Ad servers, which don't know whether an app using its service is malicious or not, send Gooligan the names of the apps to download from Google Play. After an app is installed, the ad service pays the attacker. Then the malware leaves a positive review and a high rating on Google Play using content it receives from the C&C server.

Oopsie!! -- BitLocker bypass on Windows 10 through Windows upgrades

- The root of the problem is unattended upgrades on Windows 10 machines.

- Think about it... How can a locked machine, with Bitlocker-encrypted drives, perform unattended upgrades? By having some means of decrypting the system drive WITHOUT THE USER'S PASSWORD.

- http://www.ghacks.net/2016/11/30/bitlocker-bypass-on-windows-10-through-upgrades/

- Security researcher Sami Laiho discovered an issue in Microsoft's Windows 10 operating system that allows attackers to gain access to BitLocker encrypted data.

- A post on the Win-Fu blog highlights the method. Basically, what the method does is exploit a troubleshooting feature that is enabled during the upgrade process.

- Sami Laiho writes:
  There is a small but CRAZY bug in the way the "Feature Update" (previously known as "Upgrade") is installed. The installation of a new build is done by reimaging the machine and the image installed by a small version of Windows called Windows PE (Preinstallation Environment).

  This has a feature for troubleshooting that allows you to press SHIFT+F10 to get a Command Prompt. This allows for [decrypted] access to [a bitlocker-encrypted] hard disk

[because] , during the upgrade, Microsoft [bypassed] BitLocker.

- If Shift-F10 is pressed at the appropriate time, a command prompt window is opened, allowing full and unrestricted access to the system's storage devices.

  Since BitLocker protection is bypassed during upgrades, it means that anyone exploiting the issue gets access to all files that are usually encrypted by BitLocker.

- The method works when updating the original Windows 10 release build to the November update version 1511 or the Anniversary update version 1607. It also currently works on ANY new Insider Build that Microsoft puts out.

- The main issue, as noted by Sami Laiho, is that anyone with local access to the machine may exploit the issue. Administrative access is not required.

- Since this is a local issue it cannot be exploited remotely. But anyone with local access to a Windows machine may exploit the issue… But LOCAL ACCESS is what Bitlocker and any other full disk encryption solutions are meant to prevent.

- Companies therefore should disallow the switching on of Windows Insider builds for machines running Windows 10.

- Companies may also want to disallow unattended upgrades (not updates necessarily) on Windows 10 machines to prevent the issue from being exploited.

TalkTalk wi-fi router passwords stolen -- And TalkTalk appears to be in panic/denial

- http://www.bbc.com/news/technology-38208958
- http://www.bbc.com/news/technology-38167453

- "An attack on maintenance interfaces is currently taking place worldwide." (Yeah.)

- Last week, Germany's Deutsche Telekom revealed that up to 900,000 of its customers had lost their internet connection as a result of an attack.
- Thousands of TalkTalk and UK Post Office customers have had their internet access cut by an attack targeting certain types of internet routers.
- A spokeswoman for the Post Office told the BBC that the problem began on Sunday and had affected about 100,000 of its customers.
- TalkTalk confirmed that "some of its customers" had been affected, and it was working on a fix.
- This all involves the use of a modified form of the Mirai worm.
- Researchers have observed the worm infecting the router, then stealing the router's SSID and password.
- Then... https://wigle.net/ WIGLE can be used to physically locate the victim based upon their SSID.
- https://wigle.net/enc-large.html

Analysis of multiple vulnerabilities in AirDroid

- https://blog.zimperium.com/analysis-of-multiple-vulnerabilities-in-airdroid/
  (From the people who brought us "StageFright")

- "AirDroid" is a popular Android remote management tool installed in an estimated ~50 million devices.

- Unfortunately, its communications protocol only uses rather weak encryption and NO authentication.

- ... and we know what that means: Without strong authentication, encryption is unable to guarantee any privacy whatsoever.

- AirDroid's communications are encrypted with DES (ECB mode - Electronic Code Book), however the encryption key is hardcoded inside the application itself (thus known to an attacker). Any malicious party on the same network as the target device, or anywhere in the link, could execute a man in the middle attack to obtain authentication credentials and impersonate the user for further requests.

- The key is: "890jklms" (DES has a 56-bit key and a 64-bit block size)

- An attacker performing a MITM attack and redirecting HTTP traffic to a malicious transparent proxy, could modify the response for the /phone/vncupgrade request, which is normally used by the application to check for addons updates... Injecting their own update and thus remotely executing custom code on the target device.

- Disclosure Timeline:
  - May 24 2016 : Initial disclosure email sent.
  - May 30 2016 : Acknowledgment from vendor.
  - Aug 10 2016 : Follow up.
  - Aug 17 2016 : Follow up.
  - Aug 22 2016 : Follow up.
  - Aug 28 2016 : Follow up.
  - Sep 06 2016 : Follow up.
  - Sep 07 2016 : Got reply about new upcoming release.
  - Nov 28 2016: AirDroid 4.0.0 released, still vulnerable.
  - Nov 30: AirDroid 4.0.1 released, still vulnerable.
  - Dec 1 2016: Full disclosure

Credit Card hacking using backend verification

- http://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf

- "Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?"

- Possible Verification Fields:
  - Cardholder Name: the account holderi's name as printed on the card.
  - (They found that no website checks that a name entered is correct.)
  - 16-digit Card Number: The unique identifier printed on the front of the card by the issuing bank. Referred to as the Primary Account Number (PAN), it links the card to the customer's bank account.
  - Card Expiration Date: Printed or embossed on the front of the card. The expiry date and the PAN constitute the minimum set of card authentication data.
  - Card Verification Value (CVV2): a 3-digit number printed on the reverse side of the card. It is meant to be known only to the person possessing the card. It should not be stored electronically anywhere in the payment ecosystem.
  - Cardholder Address: not visible on the card but sometimes used for payment authorization purposes. Address verification is performed only on the numerical values of the street/house and postcode fields; any alphabetical characters

- Sites check varying subsets of the total possible fields
  - 2 fields: PAN + Expiry date (the absolute minimum)
  - 3 fields: PAN + Expiry date + CVV2
  - 4 fields: PAN + Expiry date + CVV2 + Address

- Mastercard's backend is aware of "network wide" guessing and blocks it.
- VISA, the largest network in the world... does not.

Cloudflare reports signs of a Mirai-rivaling DDoS botnet being formed.

- https://blog.cloudflare.com/the-daily-ddos-ten-days-of-massive-attacks/

- They've been watching traffic and spotting patterns.

- On November 23rd, the day before Thanksgiving, they encountered an 8.5 hour, 172 Million packets/sec attack delivering 400 Gbps.

- The following day it repeated, though starting 30 minutes earlier.

- On the third day, the same start time, but ended a bit earlier, after getting up to 200 Mpps and 480Gbps.

- ... and this continued, day after day, through Black Friday, cyber Monday, and into this week... with traffic peaks up to 400Gbps for hours on end.

- Then, a week ago, last Tuesday, the attacker stopped taking breaks and moved to 24 hours per day.

- However... these attacks are not coming from the Mirai botnet. They are using different attack software and are sending very large L3/L4 floods aimed at the TCP protocol. The attacks are also highly concentrated in a small number of locations mostly on the US west coast.

- OSI network model:
    - L1 - Physical Layer
    - L2 - Data Link
    - L3 - Network Layer
    - L4 - Transport
    - L5 - Session
    - L6 - Presentation
    - L7 - Application

Deliberate remote access backdoor discovered in 80 Sony IP camera models:

- Security researchers "SEC Consult" performs a static analysis of a Sony IP camera's firmware.

- Video Security Camera Series: X, C, H, W
    - Minidomes, Fixed, Pan/Tilt/Zoom

- Software analysis discovers two built-in username/password pairs:

- Two application-level backdoor accounts exist:
    - User "debug", Passwort: "popeyeConnection"
    - User "primana", Passwort: "primana"

- The web interface can be used with these to ring up a Telnet / SSH server.

- http://blog.sec-consult.com/2016/12/backdoor-in-sony-ipela-engine-ip-cameras.html

- SEC Consult has found a backdoor in Sony IPELA Engine IP Cameras, mainly used professionally by enterprises and authorities. This backdoor allows an attacker to run arbitrary code on the affected IP cameras. An attacker can use cameras to take a foothold in a network and launch further attacks, disrupt camera functionality, send manipulated images/video, add cameras into a Mirai-like botnet or to just simply spy on you. This vulnerability affects 80 different Sony camera models. Sony was informed by SEC Consult about the vulnerability and has since released updated firmware for the affected models.

- From the Security Advisory: Sony IPELA ENGINE IP Cameras contain multiple backdoors that, among other functionality, allow an attacker to enable the Telnet/SSH service for remote administration over the network. Other available functionality may have undesired effects to the camera image quality or other camera functionality. After enabling Telnet/SSH, another backdoor allows an attacker to gain access to a Linux shell with root privileges!

- The vulnerabilities are exploitable in the default configuration over the network.

- Exploitation over the Internet is possible, if the web interface of the device is exposed.

- SEC Consult writes:
  - Attackers are able to completely takeover the Sony IPELA ENGINE IP Camera
  - products over the network.
  - Sony has provided updated firmware which should be installed immediately.
  - SEC Consult recommends Sony and Sony customers to conduct a thorough security review of the affected products.
  - It is essential to restrict access to IP cameras using VLANs, firewalls etc. Otherwise the risk of being a botnet victim (e.g. Mirai) is high.

- Sony confirms, "thanks", and offers patches to close a remotely accessible Telnet and SSH root access to 80 different IP cameras.

- https://www.sec-consult.com/en/Vulnerability-Lab/Advisories.htm

- [2016-12-06] Backdoor vulnerability in Sony IPELA ENGINE IP Cameras
- Sony IPELA Engine IP Cameras contain multiple backdoors. Those backdoor accounts allow an attacker to run arbitrary code on the affected IP cameras. An attacker can use cameras to take a foothold in a network and launch further attacks, disrupt camera functionality, send manipulated images/video, add cameras into a Mirai-like botnet or spy on people.

- https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20161206-0_Sony_IPELA_Engine_IP_Cameras_Backdoors_v10.txt

- "Users of our network cameras should update now to our latest firmware for improved network security."

- https://www.sony.co.uk/pro/article/sony-new-firmware-for-network-cameras

Our San Francisco MUNI hacker… got hacked!

- http://bgr.com/2016/11/29/sfmta-ransomware-hacker-hacked/

- Hacker's eMail account: "cryptom27@yandex.com"

- A security researcher requesting anonymity correctly guessed the password recovery security question "protecting" the hacker's eMail account, reset the account's password, and obtained access to the account's eMail history.

- He forward his information to Brian Krebs for further analysis and disclosure.

- So now we know more…
  On Nov. 20, hacked emails show that 64 bitcoins (~$45,000 were successfully extorted from a U.S.-based manufacturing firm.
- Brian noted that the attacker appears to be in the habit of switching Bitcoin wallets

randomly every few days or weeks. “For security reasons” he explained to some victims who took several days to decide whether to pay the ransom they’d been demanded.

- A review of more than a dozen Bitcoin wallets this criminal has used since August indicates that he has successfully extorted at least $140,000 in Bitcoin from victim organizations.

- That is almost certainly a conservative estimate of his overall earnings these past few months: My source said he was unable to hack another Yandex inbox used by this attacker between August and October 2016, “w889901665@yandex.com,” and that this email address is tied to many search results for tech help forum postings from people victimized by a strain of ransomware known as Mamba and HDD Cryptor.

- According to a review of email messages from the Cryptom27 accounts shared by my source (writes Brian in his blog), the attacker routinely offered to help victims secure their systems from other hackers for a small number of extra Bitcoins. In one case, a victim who had just forked over a 20 Bitcoin ransom seemed all too eager to pay more for tips on how to plug the security holes that got him hacked. In return, the hacker pasted a link to a Web server, and urged the victim to install a critical security patch for the company’s Java applications.

- <quote> “Read this and install patch before you connect your server to internet again,” the attacker wrote, linking to an advisory Oracle issued for a security hole that it plugged in November 2015.

- For its part, the SFMTA said it never considered paying the ransom.

- But the list of victims indicates that the SFMTA's decision was uncommon. The majority of organizations victimized by this attacker were manufacturing and construction firms based in the United States, and most of those victims ended up paying the entire ransom demanded — generally one Bitcoin (currently USD $756) per encrypted server.

- SFMTA spokesman Paul Rose said: “We have an information technology team in place that can restore our systems and that's what they are doing. Existing backup systems allowed us to get most affected computers up and running, and our information technology team anticipates having the remaining computers functional in two days.”

Atlas Informatics "Atlas Recall"

- https://www.atlas.co/using-atlas/
- Mac and iOS devices now, Win10 on the way...
- A cloud-based store/index of everything you ever do on your computer.

- What is Atlas Recall?
  Atlas Recall is software that makes you smarter and more productive by giving you a searchable photographic memory for your entire digital life. Anything you see on your device can be searched - while keeping you in control of your data.

- How does Atlas Recall work?
  Recall runs in the background as you work, chat, play, and surf, taking note of what is important to you. It remembers everything that you see and interact with on your device, then stores it in a secure cloud, enabling you to return to it from any device where you've installed Recall.

- How Is Atlas Recall Different than searches like Google or Spotlight?
  Google, Spotlight, and Cortana do a great job at helping you find content within a limited sphere. Google specializes in web searches, while Spotlight and Cortana help you find local files on your device. Atlas Recall makes the search services you use every day better, giving you the power to search for anything you see across your entire digital life with one simple search.

- Once I find what I'm looking for, can I open the file?
  Yes. With Recall, you can search for any content you've seen on one device, then open it on the same device - or any other one you have Recall installed on.

- What types of content does Recall remember?
  Anything you see on your screen, Recall remembers. This includes web pages, social media, docs, apps, chats and pretty much everything else. And if you prefer Recall to not remember any element, you're empowered to pause it or block it at any time.

Man Tricks Amazon Echo Dot and Google Home Into a Neverending Conversation

- https://blog.hackster.io/man-tricks-amazon-echo-dot-and-google-home-into-a-neverending-conversation-b5f30bdd7278
- As seen in the video, Jakowenko used the voice-activated devices' calendar features to make the Echo, which answers to the name "Alexa," and the Home, which responds to "Hey Google," converse in an "infinite loop."

"USB Killer", now widely available for $50, allows you to easily fry almost any device...

- Plug the small "USB Dongle" into any USB-equipped device... wait a few seconds, and the victim's USB interface receives a 220volt shock on its USB data lines, typically at least killing the data interface and in some cases, probably depending upon the level of USB-integration present, penetrating deeper into the hardware and also killing non-USB functionality.
- Strong incoming ESD protection would protect against this.
- USB connectors bring up the power and ground first.

Thieves are increasingly using car key jammers

- http://www.bbc.com/news/uk-england-berkshire-38195281
- With the rapid growth of keyless auto entry, thieves are increasingly jamming the remote "lock" signal to gain entry and steal car contents.

- When locking your car, make sure you hear the acknowledging "thunk", "beep", "click" or whatever.

It Only Takes 15 Minutes to Hack a Samsung or Huawei Smartphone Fingerprint Scanner

- http://neurogadget.net/2016/03/13/takes-15-minutes-hack-samsung-huawei-smartphone-fingerprint-scanner/26027/amp?client=ms-android-huawei
- Because their fingerprint scanners will fall for conductive ink on paper...

This seems VERY troubling: UK Police "Mug" a suspect to obtain unlocked phone data

- http://www.bbc.com/news/uk-38183819
- Detectives have developed a new tactic to beat criminals using mobile phone encryption - legally "mug" them.

- This emerged after Scotland Yard's cybercrime unit smashed a fake credit card fraud racket.

- Officers realized crucial evidence in the investigation was concealed on a suspect's iPhone - but it would be unobtainable if the device was locked.

- So a covert team seized it in the street while the suspect was on a call - beating the security settings.

- The "street seizure" of the phone was dreamt up by detectives of "Operation Falcon", a specialist Metropolitan Police team running investigations into major fraud and related crimes organized online. Suspect "Gabriel Yew" had been under investigation for the suspected manufacture of fake cards that gangs were using across Europe to buy luxury goods. Detectives suspected that he was using an iPhone exclusively to communicate to other members of the network, but knew if they arrested him, he could refuse to unlock it and they would never see incriminating evidence.

- They considered whether they could legally force a suspect's finger or thumb on to the device's fingerprint reader to unlock it, but found they had no such power.

- However, they concluded they could stage their own lawful "street robbery" - using a similar snatch technique to a thief - and in June a team set out to do precisely that.

- Undercover surveillance officers trailed Yew and waited for him to unlock his phone to make a call - thereby disabling the encryption.

- One officer then rushed in to seize the phone from Yew's hand - just as would happen in a criminal mugging. As his colleagues restrained the suspect, the officer continually "swiped" through the phone's screens to prevent it from locking before they had downloaded its data.

- Chief Detective Inspector Andrew Gould, who led the operation, said: "The challenges of pin code access and encryption on some phones make it harder to access evidence in a timely fashion than ever before. Officers had to seize Yew's phone from him in the street. This evidence was crucial to the prosecution."

Good news!! BeamGun - A rogue-USB-device defeat program for Windows.

- http://bit.ly/2gKRZx7
- https://jlospinoso.github.io/infosec/usb%20rubber%20ducky/lan%20turtle/c%23/clr/wpf/.net/security/2016/11/30/beamgun-update-poison-tap.html
- https://github.com/JLospinoso/beamgun

- Hacker Terms:
  - "Rubber Duckies" are keystroke injection attack platforms.
  - "LAN Turtles" are USB devices which register themselves as network adapters.

- "BeamGun" is a tiny program that runs in the background listening for USB device insertions.
- When a USB keyboard device is plugged in, Beamgun blocks all keystrokes until it is reset.
- When a USB LAN adapter is plugged in, it is disabled.

Miscellany

MailStore 10 just released and available

George (aka Peabody):
I want to bring up a point regarding Image for Windows. I use Truecrypt whole drive encryption on my computers, and since I don't trust the shadow copy process, I use the Image for Linux CD to both create and restore images. The neat thing about IFL is that they put Truecrypt for Linux on the CD - actually now Veracrypt I guess. So that means I can boot to the CD, mount the Windows partition in question in Truecrypt for Linux using the normal pre-boot password, and then IFL can see the partition in the clear and make the usual smart image (used sectors only, no paging or hibernation files). Of course by default the image which has then been made is also now in the clear, but you can tell IFL to encrypt it.

And all this also works perfectly during a restore: You mount the partition in Truecrypt, then restore the image into the mounted partition, and Truecrypt re-encrypts it on the fly. I've done this several times, and it works.

Amazing "Humble eBook Bundle:

- O'Reilly Unix/Linux eBooks, ending Wednesday night.
  - https://www.humblebundle.com/books/unix-book-bundle
  - PDF, ePub & MOBI
  - $500 worth of eBooks

- Completely free, is:
  - Ten Steps to Linux Survival

- Pay $1 or more, and ALSO unlock:
  - UNIX in a nutshell

    - sed & awk
    - lex & yacc
    - Learning the bash shell
    - Linux Pocket Guide

- Pay $8 or more, and ALSO unlock:
    - bash Cookbook
    - Classic Shell Scripting
    - Learning GNU Emacs
    - UNIX Power Tools
    - Learning the vi and Vim Editors
    - Bash Pocket Reference
    - Learning Unix for OS X

- Pay $15 or more and ALSO unlock:
    - Essential System Administration
    - TCP/IP Network Administration
    - DNS and BIND
    - Network Troubleshooting Tools

- Make: Technology
    - "Make: Fire / The Art and Science of Working with Propane
    - (What could POSSIBLY go wrong??!!)

WestWorld -- OMG!
I'll be re-watching the entire thing in the summer.

A.G. Riddle
A.G. Riddle spent ten years starting internet companies before retiring to pursue his true passion: writing fiction. His debut novel, The Atlantis Gene, is the first book in a trilogy (The Origin Mystery) that has sold over two million copies in the US, has been translated into 18 languages, and is in development to be a major motion picture.

The Origin Mystery - Thriller, Action/Adventure, Mystery, Science Fiction.
- The Atlantis Gene / All Kindle Unlimited & Audible
- The Atlantis Plague
- The Atlantis World

CBS Films is adapting the Atlantis novels for a feature film trilogy (Good luck with that!)

Next up... "Departure"
- FLIGHT 305 TOOK OFF IN 2015... BUT IT CRASHED IN A WORLD VERY DIFFERENT FROM OUR OWN... NOW FIVE STRANGERS MUST UNRAVEL WHY THEY WERE TAKEN... AND HOW TO GET HOME.
- 20th Century Fox adapting for film

- Acquired by HarperCollins for 7-figures
- 250,000+ copies sold in pre-release
- 2,400+ positive reviews

Richard Phillips

- Rho Agenda (Trilogy) - Kindle Unlimited
- The Rho Agenda Assimilation
- The Kasari Nexus
- The Altreian Enigma (Kindle Unlimited)

SpinRite

Scott in Woodland, CA
Subject: SpinRite Guide for New Hard Drives

Hey Steve, I've heard you speak briefly about running SR on brand new drives but what metrics should we be looking at to determine if the drive is healthy or should be returned?