Security Now! #795 - 12-01-20

DNS Consolidation

This week on Security Now!

This week we look at a couple of new and forthcoming Chrome features, I'll quickly run though some new and notable ransomware casualties, including a couple of follow-ups, we'll look at a critical flaw in the Drupal content management system, the big trouble with generic smart doorbells, an interesting attack on Tesla Model X key fobs, CA's adaptation to single-year browser certs, several instances of leaked credential archives, a critical RCE in a major MDM server, a bit about the Salvation Trilogy, some extremely promising news about SpinRite's future, and then we'll wrap up by taking a look at the consequences of the increasing consolidation of DNS service providers. It's not good if saying on the Internet is important to you.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Browser News

Chrome's Omnibox becomes more Omni

Starting with the current release 87 of Chrome, which we all have now. a range of useful commands can be entered into Chrome's omnibox and directly executed from there. Google is slow-rolling this feature, but anyone interested can enable it immediately.

To enable it, place “chrome://flags” in the URL and then search for “omnibox suggestion”

This will display three hits. You need to enable the first two: “Omnibox suggestion button row” and “Omnibox Pedal suggestions” then click the “restart browser” button that will appear at the lower right. Next, try asking Chrome for things you want to do, such as:

‘clear cache’, ‘delete history’, ‘wipe cookies’, ‘update browser’, ‘incognito’ or ‘launch incognito mode’, ‘edit credit card’, ‘edit passwords’, ‘update credentials’, ‘translate this page’ or ‘translate this’

As you enter the phrase into Chrome's omnibox, various incremental matching guesses will appear as always. But now, at some point, you'll have entered enough for Chrome to guess what you might want and display a button to initiate that action. It's a pretty nifty way to quickly do things without the need to go digging around in Chrome's UI. If you were using someone else's instance of Chrome, you might enter “clear cache” when you were finished to erase your footsteps. Or even better, before starting, type “incognito” when instantly presents an “Open incognito window” button.

Chrome is not the first browser on the block to offer these sorts of omnibox UI-feature access shortcuts, though I think it works better in Chrome. Entering “clear firefox cache” into Firefox will offer a button to choose what to clear. But “clear cache” does nothing in Firefox whereas you get a button in Chrome. It appears that the Mozilla folks decided that they didn’t want to be generating false-positive hits. So the term “firefox” must always be present. But once you know that, the features are similar.

Chrome's open tabs search

And for those of us who are notorious for running with hundreds of open tabs — although I've never tried that in Chrome — next March, Chrome's new “Tab Search” feature will go live. Until then, if Chrome is started with the “--enable-features=TabSearch” command line switch, a little down-arrow will appear to the right of Chrome's tab strip. If it is clicked on, or if Control-Shift-A is entered to “Activate” tab search, an incremental-search drop down box will appear to allow all open tabs to be searched as the search phrase is entered.

I cannot imagine having a huge number of horizontal tabs open. It makes no sense, since tabs are, themselves horizontal. So tabs are desperate to be stacked vertically. Nothing could be more obvious. I've seen previews of Edge's forthcoming vertical tabs feature and they look great. But I have no complaints with Firefox's solution which is highly customizable with CSS. I can make very short itty-bitty tabs and fit a huge number of them — all visible at once — down the left side of my browser’s window.

Ransomware News

Delaware County, Pennsylvania

Delaware County, Pennsylvania has paid a $500,000 ransom after their systems were hit by the DoppelPaymer ransomware last weekend. Being Pennnsylvania, one of the loudly contested states in the Us's recent presidential election, the first question anyone has is whether the ransomware attack had any effect upon the state's election networks. So, Delaware County was quick to state that the Bureau of Elections and the County's Emergency Services Department were not affected and are on a different network than the hacked systems. Sources said the county is in the process of paying the $500,000 ransom since it's insured for such attacks.

So, another instance of the DoppelPaymer ransomware which I have the feeling we're going to be hearing more about in the future. The name "DoppelPaymer" was derived from its predecessor "BitPaymer", with which it shares a large body of code. But DoppelPaymer has been improved to add a multithreaded encryption process for faster operation. Because, of course, that's what you want in your encrypting ransomware. We also know that the gang behind DoppelPaymer often exfiltrates a network's pre-encrypted data, but it's unknown publicly whether this was done to Delaware County.

And in an odd twist, the DoppelPaymer gang apparently advised Delaware County to change all of their passwords and to also modify their Windows domain configuration to include safeguards from the Mimikatz program. Mimikatz is an open-source tool that's been around since 2014. It's commonly used by ransomware gangs to harvest Windows domain credentials on a compromised network. It's on Github where its author explains that he wrote it as a way to learn 'C' and experiment with locating and extracting Windows credentials from the RAM of running systems.

Canon

Also in this week's ransomware news, Canon finally publicly confirmed what we all pretty much knew based upon the evidence: that the cyberattack they suffered back in August was the result of a ransomware attack and that the hackers stole data from company servers. Recall that Canon suffered an outage of their cloud photo and video storage service (at image.canon) and that users lost files. As we noted at the time a large array of related canon domains were also affected.

Shortly after the attack, BleepingComputer obtained information showing that the outage had been caused by Maze ransomware. Maze also told BleepingComputer that they had stolen 10 terabytes of data and private databases before triggering the file-encrypting malware on the 5th of August 5. And, interestingly, the trouble with at least the "image.canon" site was unrelated to the ransomware attack. Maze confirmed that their actions did not extend to Canon's storage service.

US Fertility

"US Fertility", the largest network of fertility centers in the U.S. with 55 locations across 10 states, was hit by an unknown ransomware, encrypting some of its systems two months ago, in September 2020.

Ritzau
Meanwhile, last Tuesday in Denmark, Ritzau, the largest independent news agency in Denmark, which was founded in 1866 by Erik Ritzau, said in a statement that it will not pay the ransom demanded by a ransomware gang that hit its network last Tuesday morning. Their spokesman said: "The Ritzau news agency was subjected to an extensive hacker attack on Tuesday, and the hackers have subsequently demanded a ransom to release data. Ritzau has refused to pay money to the hackers." During the attack, the ransomware group was able to compromise and encrypt roughly one-quarter of more than 100 servers on Ritzau's network. Their IT department immediately set to work restoring the systems and expected to have them back up within two days at the earliest. That's how you do it!

Baltimore County Public Schools
And last Wednesday, the Baltimore County Public Schools posted the news: "BCPS can now confirm we were the victim of a ransomware attack that caused systemic interruption to network information systems. Our BCPS technology team is working to address the situation & we will continue to provide updates as available. For now, please don't use BCPS devices." Of course, this all hits amid the COVID-19 remote learning period.

The Baltimore City Public Schools district — apparently distinct from Baltimore County Public Schools — also published an alert on ITS website, urging students to only use school-issued devices for virtual learning. They wrote: "Students participating in virtual learning should only use City Schools-issued laptops or devices. Do not use devices issued by Baltimore County schools or your personal laptop or computer. Students without access to a City Schools-issued device will be granted an excused absence." Presumably there's some concern that the malware might crawl out onto devices connected to the County network, but not the City network. Or perhaps Baltimore City has additional device protection on their devices.

And here's where it gets even more interesting...

Following last Wednesday's ransomware attack that hit the district's network, Baltimore County Public Schools has now urged students and staff to stop using their school-issued Windows computers and only use Chromebooks and Google accounts. The update on their website say: "We now know that BCPS-issued Chromebooks were not impacted by the cyberattack. You may now safely use: BCPS-issued Chromebooks and BCPS Google accounts for students and staff. Please do not use BCPS-issued Windows-based devices until further notice."

The District also said: "Due to the recent ransomware attack, Baltimore County Public Schools will be closed for students on Monday, November 30, and Tuesday, December 1. BCPS offices will be open and staff will receive additional information about Monday and Tuesday."

So... Interesting that Chromebooks are officially preferred and Windows devices are being told to remain away from the network. Wow.

Banijay Group SAS
The French multinational production and distribution firm Banijay Group SAS, who we better know by the various brands they produce, which include MasterChef, Survivor, Big Brother, The

Kardashians, Mr. Bean, Black Mirror, Extreme Makeover: Home Edition, and Deal or No Deal, among a great many others, was another recent victim of the DoppelPaymer ransomware.

Although Banijay has only shared that they have suffered a cyber-attack and that some of their data might have been compromised, the DoppelPaymer ransomware gang is not only claiming responsibility but also proving their involvement by shared several documents presumably stolen from Banijay's systems. DoppelPaymer is also taunting the French production group by referencing GDPR compliance issues and leaking an internal GDPR compliance document, among others.

Security News

Drupal

Drupal's security advisory is titled: "Drupal core - Critical - Arbitrary PHP code execution"
https://www.drupal.org/sa-core-2020-013

It was issued last Wednesday and if any of our listeners are running Drupal-based systems and you haven't yet updated, do it now! It is a sweeping vulnerability. If you are using:

- Drupal 9.0, update to Drupal 9.0.9
- Drupal 8.9, update to Drupal 8.9.10
- Drupal 8.8 or earlier, update to Drupal 8.8.12
- Drupal 7, update to Drupal 7.75

The Drupal project uses the PEAR Archive_Tar library. The PEAR Archive_Tar library has released a security update that impacts Drupal. This is another case like Google saw with the FreeType font interpreter where their use of a 3rd-party library bit them when a remotely exploitable flaw was discovered there.

The advisory states that "Multiple vulnerabilities are possible if Drupal is configured to allow .tar, .tar.gz, .bz2, or .tlz file uploads and processes them." To mitigate this issue (before fixing it), prevent untrusted users from uploading any of those file types.

What makes this all the more urgent is that there are known exploits against these vulnerabilities and some Drupal configurations are known to be vulnerable. And, Drupal is a popular content management system. As of Friday, over 944,000 websites are using vulnerable Drupal versions out of a total of 1,120,941 according to official stats. But even those stats underestimate the scope and scale of vulnerabilities because only those Drupal sites which are using the Update Status module are included in the data. Thus, many more may be at risk.

Drupal is presently in 4th place among CMS systems on the Internet. WordPress is in the lead with a 63.8% share, followed by Shopify at 5.1%, Joomla at 3.6% and Drupal at 2.5%.

So, again, if you or anyone you care about are using Drupal, be sure to be running the most current release for your major version.

The Revenge of Cheap Smart Doorbells
Hopefully, it won't come as a surprise to any of our listeners to learn that they don't want to have off-brand, even no-name, IoT smart doorbells, the likes of which are sold on Amazon and eBay, anywhere near their homes. Matt Lewis of the NCC Group, and their researchers, took a look at the operation of 11 off-brand "El Cheapo" bargain smart doorbells and found their intelligence lacking.

Matt said: "Our findings could cause issues for consumers and are indicative of a wider culture that favors shortcuts over security in the manufacturing process." [Big surprise, there.]

He added: "However, we are hopeful that the much-anticipated IoT legislation will signal a watershed moment in IoT security. Until this comes into fruition, we must continue to work together to highlight the need for basic security by design principles, and educate consumers about the risks and what they can do to protect themselves."

So, first of all... the IoT legislation Matt is referring to has been moving along since it's 2017 introduction by Senator Mark Warner. It uses the typical carrot and stick of security requirements offered before the government will be allowed to purchase. And it does include a bunch of the stuff we need. The legislation requires vendor commitments that:

1. That their IoT devices are patchable.

2. That the devices don't contain known vulnerabilities.
    - If a vendor identifies vulnerabilities, it must disclose them to an agency, with an explanation of why the device can be considered secure notwithstanding the vulnerability and a description of any compensating controls employed to limit the exploitability/impact of the vulnerability.
    - Based on this information, an agency CIO could issue a waiver to purchase the device.

3. That the devices rely on standard protocols.
    - Outside experts emphasize the importance of having the vendor disclose what network protocols are in use, for instance to assist Department of Homeland Security (DHS)'s Einstein program.

4. That the devices don't contain hard-coded passwords.

However, the bill is not yet law, and there are exemptions that you could drive a large truckload of not-smart-enough doorbells through. So we'll need to take a wait-and-see on that. But it's certainly true that anything would be WAY better than the totally unregulated environment we have today.

And speaking of today two of the devices tested, manufactured by Victure and Ctronics, had critical vulnerabilities that could allow bad guys to steal the user's home network password. The flaws would also allow attackers to hack not only the doorbells and the residential router, but any other smart devices in the home, such as a thermostat, camera or even any of the household computers. And get this: The Victure Smart Video Doorbell was found to be sending customers' home WiFi name and password, unencrypted, to servers in China.

There is ABSOLUTELY no need for a locally-connecting WiFi device to export its local network credentials anywhere. And such devices never should. But that doesn't mean they don't.

Remember that visual we set up when we were talking about this after I attached a few IoT devices to my own network which were phoning home to China. Just visualize all of the hundreds of million of connections reaching across the globe from the US to China. And we hear that we're in what is essentially a cold war with China. And that they have a foothold into probably the majority of US domestic networks. What was that story about the Trojan horse?

Anyway, Matt said: "If stolen, this data could allow a hacker to access people's home WiFi – enabling them to target their private data, and any other smart devices they own."
Yeah, no kidding. A large number of the doorbells tested also used weak, default and easy-to-guess passwords. Matt noted that it's common for less security-conscious consumers to leave the default passwords unchanged on their equipment, potentially exposing them to hackers. Again... uh huh.

The researchers found that another device, bought from eBay and Amazon without any clear brand associated with it, was vulnerable to the critical KRACK exploit — the Key Reinstallation Attack, which was discovered in 2017. So, these devices don't even have up-to-date WiFi stacks. Why would they? This opens any attached network to intrusion by allowing the network's WPA and WPA2 encryption to be cracked.

Of course, none of this comes as any great surprise. But it's nice to examine some specifics since generalities are easily waved off. If you want to buy a smart doorbell, there's very good reason to stick with major brands who proactively support their devices. As we know, that's not to say that they won't have problems, too. But if they do it will make headlines and and the vulnerabilities will be cured promptly — as opposed to never.

Tesla Key Fob Hack #3

And speaking of hacking, even well-designed devices get hacked... As Tesla found out for the third time from one researcher. Lennert Wouters, a PhD student at the Computer Security and Industrial Cryptography (COSIC) group at the Catholic University of Leuven (KU Leuven) in Belgium, discovered a method to overwrite and hijack the firmware of Tesla Model X key fobs. This allowed him to steal any car that isn't running the latest software update. Lennert's attack only takes a few minutes to execute and requires inexpensive hardware. Lennert has previously produced successful attacks against Tesla security in 2018 and 2019. Now he adds 2020.

He explained that this third attack works thanks to a flaw in the firmware update process of Tesla Model X key fobs. The flaw can be exploited using an electronic control unit (ECU) salvaged from an older Model X vehicle, which can be easily acquired online on sites like eBay or any stores or forums selling used Tesla car parts. Wouters said attackers can modify the older ECU to trick a victim's key fob into believing the ECU belonged to its paired vehicle and then push a malicious firmware update to the key fob via Bluetooth. Since this key fob update mechanism was not being properly secured, they were then able to wirelessly compromise the key to take full control over it. Subsequently, they could obtain valid unlock messages to unlock the target car later.

Here's how the attack works, in practice:

1. Attacker approaches the owner of a Tesla Model X vehicle. For this first phase the attack must briefly get within 5 meters of the victim to allow the older modified ECU to wake up and ensnare the victim's original key fob.

2. The attacker then pushes the malicious firmware update to the victim's key fob. Although this second phase requires about 90 seconds to execute, the range during this time increases to 30 meters, allowing the attacker to put some distance between themselves and the targeted Tesla owner, and thus reducing suspicion.

3. Once the victim’s key fob has been hacked, the attacker extracts car unlock messages from the fob.

4. The attacker uses these unlock messages to enter the victim's car.

5. The attacker connects the older ECU to the hacked Tesla car's diagnostics connector — normally used by Tesla technicians to service the car.

6. The attacker uses this connector, and couple of minutes, to pair their own key fob to the car, which they are then later able to use to start the vehicle and drive away.

The only downside of this attack is the relatively bulky attack rig, which would be easy to spot unless concealed inside a backpack, bag, or another car. But that would certainly be feasible.

Nonetheless, the attack rig is not expensive. It requires a $35 Raspberry Pi with a $230 CAN bus shield, a modified key fob, an older ECU from a salvaged vehicle — $100 on eBay, and a $30 Lithium Polymer battery.

Being a responsible lad, after discovering the bug and developing the exploit earlier this summer, Lennert reported it to Tesla's security team in mid-August. And, as you might imagine, after his 2018 and 2019 hacks, they took his call. Only after Tesla began rolling out an over-the-air software update to all Model X cars did Lennert publish his findings. The software update containing the fix is 2020.48. Don’t leave the garage without it!

CA's adapt to single-year certs

As expected, traditional high-reputation non-automated certificate authorities are reacting to the browser industry's decision — initially instigated by Apple but then quickly adopted by everyone else — to enforce a maximum life on browser certs of 398 days. As we know, this went into effect on September 1st of this year, affecting any certificates issued from then on.

This morning I received a notice from my chosen and quite favorite certificate authority, DigiCert, explaining the way their multi-year plans will function. The essence is what we expected: Despite the shortening of individual certificate lifetimes, it's possible to sign up in advance for a multi-year commitment. DigiCert provides for up to six years. And, as you'd expect, a longer commitment results in a lower cost per year which seems fair since we're giving them our money up front.

Once that's set up you're in control of your own certificate renewal, able to reissue certificates at any time needed. In DigiCert's case this is essentially an extension of the system they've had in place for years. I've mentioned on the podcast how convenient it has been to be able to issue a certificate at midnight on the weekend and receive it within minutes.

Of course, all certificate authorities are now needing to compete with ACME certificate automation. As we know, I had traditionally been using EV certs. But when browsers made the decision to de-emphasize the display of extended validation, and also because my use of subdomains has been growing with things like sqrl.grc.com, forums.grc.com, news.grc.com, where EV certs do not support wildcards, it made the most sense to switch from EV to organization validation (OV) certs, which is where I am now.

And given the decidedly mixed blessing of certificate automation, with it's exceedingly high fraudulent issuance rate, I'll be surprised if the CAB Forum doesn't eventually decide to add some sort of indication of whether a certificate was issued by a bot or under human supervision.

Nearly 50,000 Fortinet VPN credentials posted online

Last year it was revealed that the FortiOS which underlies the Fortinet VPN was subject to a path traversal flaw. It was assigned CVE-2018-13379. And the NIST description of the vulnerability reads: "An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests."

On August 28th of 2019, Fortinet posted: "At the recent Black Hat 2019 conference held in Las Vegas this past August 3-8, security researchers discussed their discovery of security vulnerabilities that impacted several security vendors, including Fortinet. All of the vulnerabilities impacting Fortinet were fixed in April and May of 2019."

Naturally, being a responsible company, Fortinet had also worked to notify all of their users to update. We can all probably guess how well that went.

Note that the vulnerability allows Fortinet VPN system files to be obtained remotely and without any of that pesky authentication. This is in the news today, because a massive, nearly 50,000 records worth, of Fortinet VPN logon credential information has recently appeared on the dark web and is being passed around.

This 7 GB archive of individual "sslvpn_websession" files contains session-related information including plain text usernames and passwords and the IPs of Fortinet VPN users. And present among the nearly 50,000 records are the VPN IPs of banks, telecoms, and government organizations from around the world.

Since the aggregated and leaked archive contains all the logon information needed, patching any still-vulnerable Fortinet VPNs at this point won't prevent any of their accounts from still being used. So the only remediation is to patch the VPN then cancel and reissue all VPN accounts. Who said being in charge of IT wasn't fun?

More than 300,000 Spotify accounts hacked

The security industry has renamed what we once called a brute force attack "Credential Stuffing." But it's the same thing. It's typically performed by taking a list of previously used username and passwords and pounding away at some poorly protected service attempting to logon. I say "poorly protected" because any service worth its salt will observe that some attacker at a fixed IP is attempting to brute force their way in. And while, yes, a large multi-IP Botnet could be used, it's trivial — or should be — to quickly blacklist even a large number of IPs making repeated unsuccessful attempts to login. So an attack becomes more diffuse, but detectable and blockable nevertheless.

But, Spotify provides no such protection. And neither do they provide multifactor authentication which would also successfully thwart any "credential stuffing" attacks. So it should come as no surprise that Spotify's history is defined by years of users complaining that their Spotify accounts were hacked after passwords were changed, new playlists would appear in their profiles, or their family accounts had strangers added from other countries. That's what happens in today's world when authentication is weak.

https://www.vpnmentor.com/blog/report-spotify-scam/

VPNMentor's report was titled: "Spotify Targeted in Potential Fraud Scheme"

They wrote: "We unearthed an Elasticsearch database containing over 380 million records, including login credentials and other user data being validated against the Spotify service.

The origins of the database and how the fraudsters were targeting Spotify are both unknown. The hackers were possibly using login credentials stolen from another platform, app, or website and using them to access Spotify accounts.

Working with Spotify, we confirmed that the database belonged to a group or individual using it to defraud Spotify and its users. We also helped the company isolate the issue and ensure its customers were safe from attack."

The researchers believe that the 380 million records contained in the database allowed the attackers to breach between 300,000 to 350,000 individual Spotify accounts. So a hit rate of about 0.1% or 1 in 1000.

VPNMentor contacted Spotify on July 9th of this year, informing them of the exposed database and its threat to accounts and received a response the same day. VPNMentor wrote: "In response to our inquiry, Spotify initiated a 'rolling reset' of passwords for all users affected. As a result, the information in the database would be voided and become useless."

The lesson here for end-users is well understood: Never reuse passwords. Make the passwords we do use long and high-entropy. And always use time-based multi-factor authentication when available.

The lesson for Spotify and other services is: Protect your users by spotting and blocking clearly malicious authentication attempts and immediately offer and promote time-based multi-factor authentication.

MobileIron MDM CVSS 9.8 RCE

MDM is Mobile Device Management. It's a popular means for enterprises to manage the configurations of their mobile phone fleet. Because MDM servers must be publicly accessible to remotely manage those mobile devices, they become a natural target for bad guys. That means that when a remotely exploitable code execution vulnerability is found, enterprises should take heed.

One of the popular MDM services platform, MobileIron, is vulnerable to just such exploitation with a CVSS score of 9.8. The flaw was reported to MobileIron by Orange Tsai from DEVCORE. It exists across various components of this platform: In MobileIron Core, a component of the MobileIron platform that serves as the administrative console; and in MobileIron Connector, a component that adds real-time connectivity to the backend. Also impacted is Sentry, an in-line gateway that manages, encrypts and secures traffic between the mobile-device and back-end enterprise systems; and Monitor and Reporting Database, which provides comprehensive performance management functionality.

It sounds like a big mess, and it's certainly not one that any enterprise wants to have on their network. MobileIron said in an update last week that it has been engaging in "proactive outreach to help customers secure their systems," and estimates that 90 to 95 percent of all devices under mobile management are now being managed on patched and updated versions of software. And the company stated that it will continue following up with the remaining customers where they can determine that they haven't yet patched affected products.

Again, mistakes happen. Maintaining tight lines of communication is the key. And we really do need automated updating — or at the very least, automated update notifications. We're getting there slowly.

Miscellany

"The Salvation Trilogy" — OMG!!

It's been a long slow burn, sometimes even a bit of a slog, since Peter packs his novels with seemingly endless detail. But now I don't ever want it to end. I'm at 92% of book 3 and wow. I'll be rereading what I read last night again. I don't know what Peter has in store, but it feels like there may be a surprise at the end. And although things are beginning to wrap up, there's still time for something more. I'll never forget the breathtaking surprise of the ending of "Fallen Dragon." So I know that he's fully capable of setting us up for something.

SpinRite

The work on the ReadSpeed benchmark is tantalizingly close to completion. I finally published a first release candidate which had the effect of soliciting some additional needed testing. The result was that we discovered a couple of final things that need polishing, which I'll begin on this evening.

But this benchmark has revealed something that's quite exciting. So I reached out to Allyn Malventano to share some of our results with an eMail titled: "Interesting SSD timing reveals... something" and showed him what we were seeing. I know you know Allyn, Leo. He was the

storage editor at PC Perspective for years, and he's now at Intel with the title Storage Technical Analyst.

I'll go into more detail about this as soon as I have something for everyone to play with — which should be soon. But it looks very much as though SpinRite has an extremely bright future in SSD maintenance and repair.

The benchmark provides read timing resolution with an uncertainty of less than 200 picoseconds. And it turns out that this can allow it to spot regions of SSD that are weakening long before they fail. In the time domain, it's akin to having a microscope with extremely high magnification. This reveals the effects of mild regional slowdown which is a natural consequence of SSD management through something known as the FTL — Flash Translation Layer — which is what manages the mapping of the underlying SSD media to its external presentation. Those standard usage effects tend to be mild — but they are now made clearly visible by the benchmark and, depending upon SSD brand, pretty much everyone is seeing them.

But we're also seeing something very different, which reveals when the FTL is having extreme difficulty reading a region of its media. On today's multi-level cells, it may need to tweak its cell voltage threshold to deal with what Allyn terms "cell drift" and/or apply extensive levels of ECC, error correction code, to recover the region's original contents. Some lower end SSD do not have hardware acceleration, so things briefly grind to a halt. Therefore, it may be that identifying and then applying carefully selective block-aligned rewriting will be able to "recharge" and realign the drifting cells to bring a possibly-endangered region back up to speed. And if an area cannot be repaired then, oddly enough, we may be back to the very early concept of marking a region as unreliable and taking it out of the file system. When you think about it, with the crazy size of today's mass storage, it makes a huge amount of sense to remove a tiny fraction of possibly unreliable storage since everyone already has way more than they will ever be able to use.

When I suggested this in my eMail to Allyn, he replied:

> "Actually, there is no need to map out clusters at the file system level, and this is one of the cases where it may be beneficial to go 'old school Spinrite' and re-write successfully (slowly) read sectors. Unlike HDDs, SSDs won't typically do any rewriting on their own, even if a sector was *very* difficult to successfully read, so these very slow reading areas can be remedied by rewriting them. You can minimize an increase in media/FTL fragmentation by ensuring you do these operations in 4KB or 8KB (aligned) chunks and not just single sectors."

Of course, we know that a future SpinRite would do both. It would characterize the overall performance of the media to learn how it performs. It would then identify any regions that are clearly operating far below average. It would first attempt to resolve the trouble with careful selective rewriting. But if a region stubbornly refused to be healed, it would do what SpinRite originally did back at version 1.0 and take that region out of service to preserve the file system's overall data integrity.

I've mentioned that SpinRite will be screamingly fast? The benchmark is reading 544 megabytes/second from a 500 GB Samsung 860 EVO SSD attached to a SATA III port. That means that SpinRite will be able to perform this sort of whole-drive performance scan in 919 seconds, or fewer than 15 and a half minutes.

DNS Consolidation

Despite previous teachable moments, such as when DynDNS was attacked in 2016, with the result that huge swaths of the web became inaccessible, our dependence upon fewer and fewer large providers — in other words, DNS Consolidation — has only grown since then. Today, if Cloudflare, AWS, or GoDaddy were to go down, around 40% of Alexa's Top 100,000 websites would also go down due to a failure of their consolidated DNS.

For those who weren't around this podcast four years ago in 2016, Dyn, a provider of managed DNS services, was the victim of a massive DDoS attack that crippled the company's operations and took down the DNS of more than 175,000 websites. Although some sites managed to remain accessible thanks to well-configured secondary DNS servers that had been wisely kept on different networks, most sites were ill prepared and remained down for nearly a day as Dyn dealt with the attack.

So now a team of researchers at Carnegie Mellon University have conducted a large-scale study of the top 100,000 websites on the internet to see whether and how those responsible for website operations reacted to this attack —if at all— and how many are still operating with a single DNS provider and no backup.

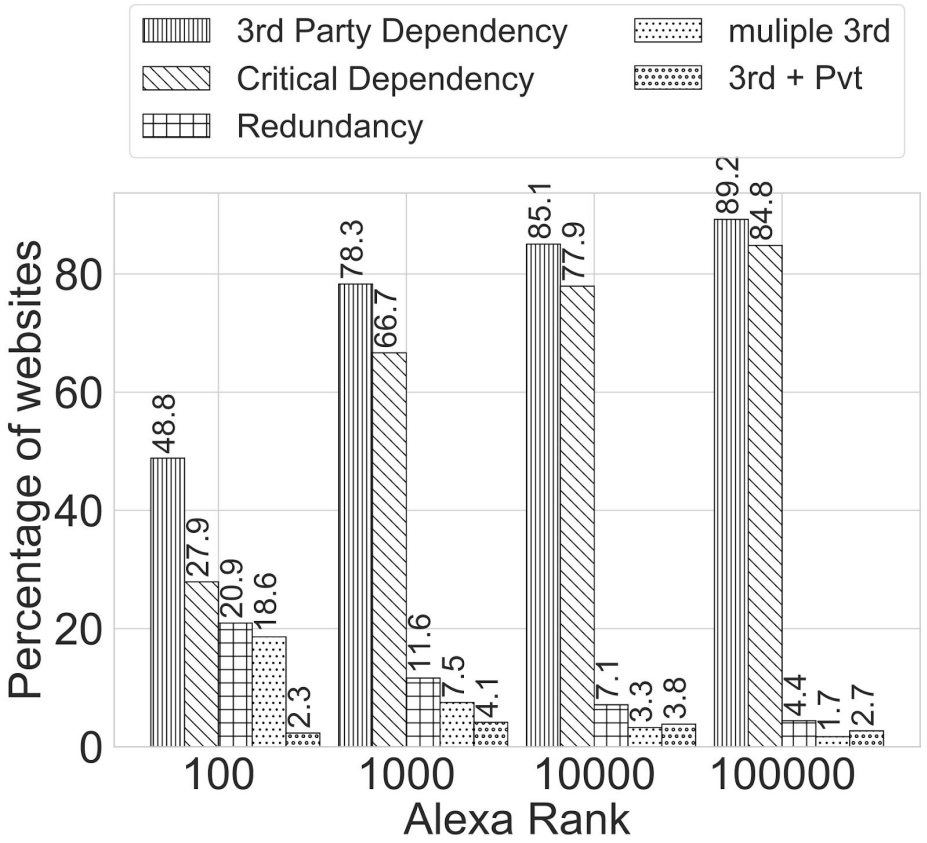
Their 14-page research paper is titled: "Analyzing Third Party Service Dependencies in Modern WebServices: Have We Learned from the Mirai-Dyn Incident?"
https://dl.acm.org/doi/pdf/10.1145/3419394.3423664

The paper was presented during the ACM Internet Measurement Conference last month, and in it they show that today, in 2020, 89.2% of all websites use a third-party DNS provider rather than managing their own DNS server. And to make matters even more fragile, 84.8% of all analyzed websites relied upon a single DNS provider, without any backup redundancy to which they could switch in case of a failure or attack.

The awareness of the need for DNS redundancy dates back to the birth of DNS. We've all seen at least two fields, or a pair of DNS IPs, wherever configured DNS addresses appear. It's regarded as best practice to have redundant DNS servers on non-adjacent IPs, typically on differing class 'C' networks — and for true redundancy, the further apart they are the better. But if the configured servers are actually sitting next to one another in the same rack, any benefit is illusory.

The CMU team says the number of sites having no effective redundancy has increased by 4.7% since 2016, and they suggest that this demonstrates that the lessons website operators might have learned following the Dyn DDoS attack were instead completely lost and soon forgotten.

They pointed out that while two of the top 100 sites DID add backup DNS servers since 2016, smaller websites continued to use a single DNS service provider without any backup, and in most cases, the operators of these smaller sites chose a large well-known provider, thus contributing to the long-observed tendency toward consolidation among ISPs.



CMU researchers say that the Top-3 DNS providers —Cloudflare (24%), AWS (12%), and GoDaddy (4%)— are the single DNS providers of around 38% of the Top 100,000 sites in the Alexa ranking.

In addition, four DNS providers are the lone critical providers for more than half of the Alexa Top 100 website list.

Any intentional attack, or perhaps the accidental network hardware or software failure, at one of these three providers can bring down a large chunk of the internet.

And the researchers also observe that when the much broader Alexa Top 100,000 sites are examined to reveal an apparently much broader base of 10,000 DNS providers, most of those still have indirect dependencies back to only a handful of top-tier providers, such as Cloudflare, AWS, GoDaddy, Namecheap, Oracle (which was formerly Dyn), and others.

Forewarned is forearmed. So, being aware of this is the point. After that, it's a judgement call. If you're a truly mission critical operation, the added overhead of maintaining fully separate truly redundant DNS services is probably justified. The amazing thing about the design of the DNS system is that it **WILL** automatically and transparently find and use them. But if something like the DynDNS outage actually just resulted in an extra unscheduled day off, then... leave things as they are and tell your boss that it was an act of God. :)