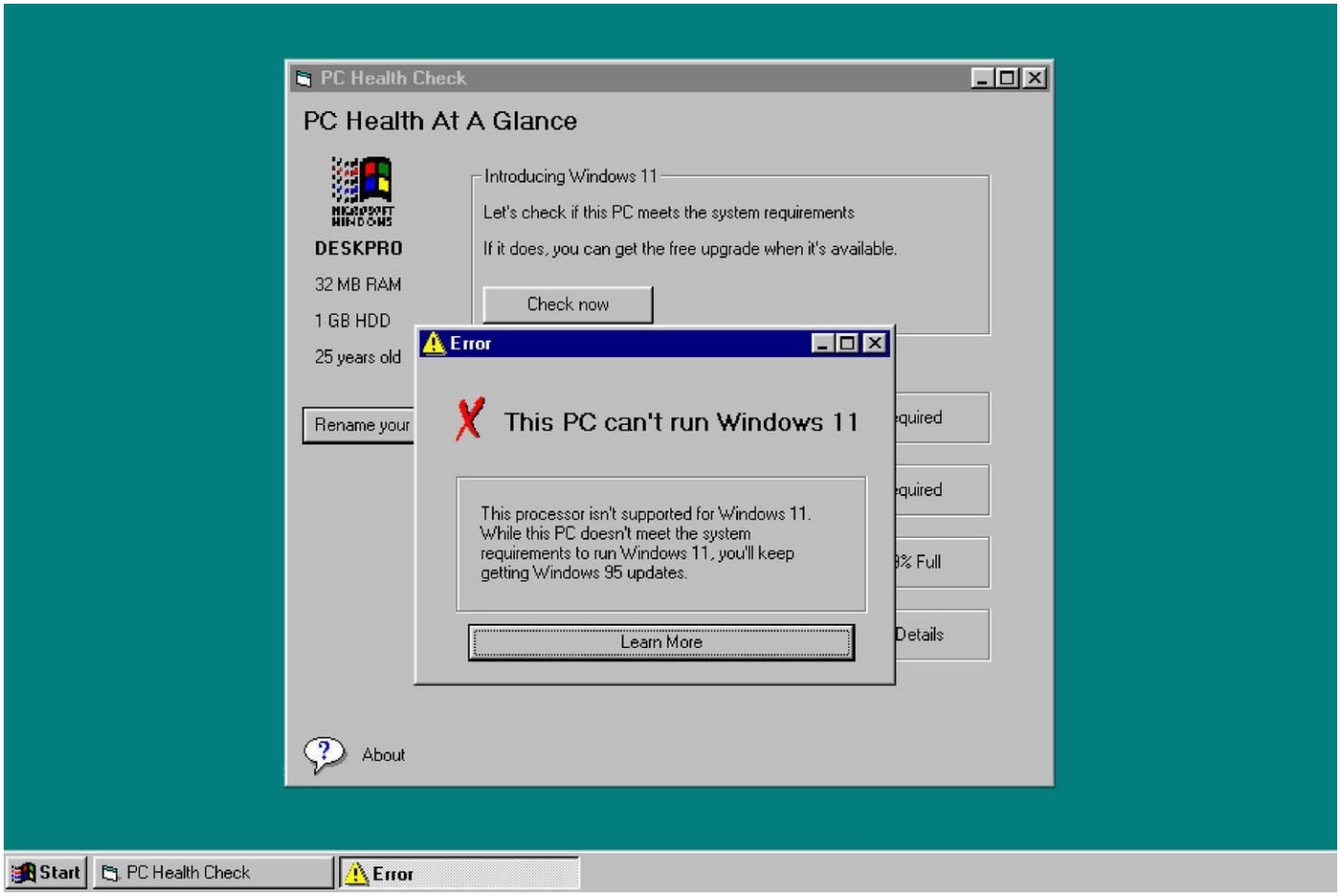
Security Now! #825 - 06-29-21

Halfway through 2021

This week on Security Now!

This week we look at the story behind an important Edge update and revist Google's now-delayed FloC liftoff. We consider the cost of Ireland's recovery from the Conti ransomware attack, and ask who's responsible for the damage and data loss following the remote wiping of many Western Digital My Book NAS devices. We take a moment to observe the passing of an industry legend. Then, we look at the mess surrounding questions of where Windows 11 will run. I share my favorite web browser keyboard shortcut, and also my favorite web site cloning tool, which I just had the occasion to use. We have a worthwhile looking cybersecurity Humble Bundle, then we'll wrap up by responding to two pieces of closing the loop feedback from our terrific listeners. And that will bring us to the end of the first half of an event-filled 2021.

Why place an arbitrary lower bound on Windows 11's minimal requirements??



Web Browser News

On June 3rd, a team of non-Russian speaking hackers who call themselves "Cyber Xplore" were searching for vulnerabilities on the Russian site mail.ru. Mail.ru is, wisely, one of HackerOne's many Bug Bounty program clients and these enterprising hackers were hoping to pay the rent. Their tool of choice for web application security testing is BurpSuite which they run on their browser of choice, which is Firefox.

The trouble was, the web subdomain of mail.ru that they were needing to poke at was all in Russian, which none of them spoke. They knew that Chrome would translate for them, but they didn't want to use Chrome. So they went looking for Firefox extensions for translation but soon discovered that a great many had been removed due to critical security vulnerabilities. Thinking about this further, they realized that any page translator would need to have direct and complete access to the page's entire DOM — its document object model. In other words, it's VERY difficult to make a translator fully secure, and it's very easy not to.

One of the team members had previously found multiple vulnerabilities in Microsoft products so they had some experience dealing with Microsoft. And what captured their attention was that Microsoft's Edge browser now had a built-in translation facility. And since Edge also has a bounty program, they figured that they might be able to get their rent paid. So they decided to switch to Edge, return to the Russian site and use Edge's built-in translator. They were immediately swamped with cross site scripting error pop-ups. They didn't quite believe it, so they did the same with Chrome using its built-in Russian translator... and no pop-ups. Chrome's translation system appeared to be secure, whereas Edge's was looking like a total meltdown.

So they began digging into Edge and they quickly discovered that Edge's translator was failing to properly sanitize HTML image tags. This allowed them to provide their own malicious JavaScript which would run in the context of the origin domain. As web browser security bugs go, it doesn't get much worse. In fact, it's so bad that they realized that they had found a class of XSS known as UXSS for "Universal Cross-Site Scripting."

They then verified that anyone accepting a Friend request on Facebook could be compromised, and that web based applications (for example Instagram) published on the Windows Store would also be vulnerable because the Windows Store operates under the same Microsoft Edge Translator that was responsible for triggering the universal cross-site scripting attack.

And as regards paying their rent, their story had a happy ending. Edge is now significantly more secure and Miccrosoft replied: *"Thank you for taking the time to share your report. Based on the assessment from our engineering team, we have determined that your case 65633 is eligible for a US $20,000 bounty award under the Edge on Chromium Bounty Program. Congratulations!"*

3rd June 2021 : Report sent To Microsoft
7th June 2021 : Reply from Microsoft Reviewing
8th June 2021 : Additional Impact Information Sent
15th June 2021 : Report Triaged
17th June 2021 : Awarded $20000 bounty
19th June 2021 : Pre-Release Patch
24th June 2021 : Patch Update Pushed & CVE ASSIGNED As CVE-2021–34506

So that's not too bad. Microsoft was first notified on June 3rd and the bug was patched and pushed out exactly three weeks later, last Thursday, June 24th. That's not the three days which appears typical or at least possible for the Chromium team, but it sure beats the catastrophic three months during which Microsoft apparently twiddled its thumbs before publishing a patch for the Exchange Server ProxyLogon (https://proxylogon.com/) flaw.

https://cyberxplore.medium.com/how-we-are-able-to-hack-any-company-by-sending-message-including-facebook-google-microsoft-b7773626e447

We're not yet FLoC'd
The future of user profiling remains uncertain.

Back near the start of COVID, the very clever Bluetooth-based privacy enforcing "Exposure Notification" device proximity tracking technology jointly designed and developed by Apple and Google was met with skepticism. No one understood it, so in the immortal words of the Monty Python troop... "Run away!!" And Amazon's recent rollout of their beautifully designed triple-encrypted, multi-layer tunneling, low bandwidth Sidewalk technology was greeted with hysteria by the popular press, claiming that it allows your neighbors to use your WiFi! Gasp! A well-meaning non-technical friend of mine phoned, warning me to "disable Sidewalk immediately!" <Sigh.> Those of us who share this podcast know, that's not at all what it is.

Meanwhile, ***[[Reality Check!!]]*** hundreds of millions of people are blithely plugging all manner of inexpensive IoT devices into their home networks, joining them to their internal LAN WiFi, whereupon those devices immediately connect back to servers in politically hostile foreign lands over which there is absolutely ZERO oversight or security. But trust in Apple, Amazon and Google who all carefully designed super secure solutions? Oh no! "Run Away!!"

In a similar vein, I was, and I continue to be, enamored of Google's FLoC technology. If we MUST have user browser history profiling, it seems to me that being tagged with an amorphous and periodically changing interest-based cohort identifier beats the hell out of having everyone carrying 3rd-party cookies around which uniquely and statically identify them individually — rather than as merely a faceless member of an amorphous cohort.

I would far prefer that legislators simply outlawed all forms of online profiling. We know that the EFF will be satisfied with nothing less. But that doesn't appear to be close to happening. And just like the $5 IoT devices which connect to cloud servers located in hostile countries, many people are missing the forest for the trees, because these days most of us are already being identified by a highly static 32-bit identifier known as an IP address. Some identity blurring occurs thanks to multiple machines located behind NAT routers having a single public IP address. But if IPv6 ever succeeds in giving each and every endpoint its own IP, that blurring will also disappear.

I wanted to briefly revisit FLoC today because, as with those other well-conceived and explicitly well-designed solutions, Google's FLoC has landed with a hard thud. Not one other browser has agreed to adopt FLoC, including those that are based on Chromium's open-source codebase, such as Brave, Edge, Opera, and Vivaldi. And Firefox is a definite "No!" A recent analysis by Digiday discovered that Amazon is already preemptively blocking Google's cookie-free system across its various web properties including WholeFoods, Zappos, ShopBop, and Goodreads.

So... As a result of all of the FLoC pushback, Google recently updated their rollout timeline, which is putting it politely, announcing that they would be delaying FLoC's wider rollout from its originally planned usage starting early next year to late year after next, in 2023. And perhaps not coincidentally, Google has been hit with some new regulatory setbacks in the E.U., after the European Commission opened a wide-ranging investigation into Google's digital advertising business to examine its "plans to prohibit the placement of third party 'cookies' on Chrome and replace them with the 'Privacy Sandbox' set of tools," (meaning FLoC) and assess its "effects on online display advertising and online display advertising intermediation markets." It sure sounds to me as though there's some monied political lobbying going on behind the scenes there. And in a similar move, earlier this month the U.K.'s Competition and Markets Authority (their CMA) announced that it's taking up a "role in the design and development of Google's Privacy Sandbox proposals to ensure they do not distort competition." Again, there are clearly some powerful forces behind these legislative saber rattlings.

Of everything that's happening, the 3rd-party cookie stovepiping that was introduced in Firefox 86's "Strict" privacy mode is the best solution until something better comes along. By breaking the browser's single shared cookie store into individual "stovepiped" per-domain stores, 3rd party cookies will continue to be honored in exactly the way they were originally designed. But when that user visits a different origin domain that 3rd-party cookie will not be returned to the same 3rd party.

Of course, the fact that all of those various queries will be coming from the same IP means that all of the fancy dancing we're doing in the browser, whether with cookies or fingerprinting or FLoC's — amounts to very little. While we run around in circles, the tracking companies are chucking.

Ransomware

Irish Ransomware Attack Recovery Cost Estimate: $600 Million

Back in the middle of last month, about six weeks ago, we covered the news that Ireland's national health system, known as the HSE for "Health Service Executive", was hit by the Conti ransomware gang and that this forced them to take their entire national healthcare IT infrastructure offline. Also recall not only that not only was the Conti gang demanding one thousand dollars shy of $20 million ransom, and Ireland's Prime Minister himself declared that no ransom would paid, but also that the High Court of Ireland then issued an injunction against the Conti Ransomware gang, demanding that the 700 GB of stolen HSE data be returned and neither sold nor published... And, further that having done that, the members of the gang identify themselves by revealing their full and true names, their email addresses, and physical addresses and then turn themselves in to Irish law enforcement immediately!

Today we have an update on the situation in Ireland. First off, it will surprise no one to learn that the Conti gang, doubtless based in Russia, was somehow able to resist the urge to comply with the Irish High Court order and that all gang members remain unidentified and still at large.

What has surprised many is that Paul Reid, the HSE's director general, has estimated the recovery costs to total $600 million. $600 million!! However, upon closer examination, the

great majority of that appears to be more than just recovery. During the hearing, Reid noted that the immediate cost of recovery would total $120 million -- which is still far more than the $20 million requested in ransom. Reid stated that further investments in replacing and upgrading the affected systems, and other expenses, would bring the total cost to an estimated $600 million. I'd sure be interested in seeing an itemization of that. He predicted it would take months for HSE to fully recover from the attack. Among the many expenses was the cost of hiring technical experts. Reid said: "We have also engaged international expertise. There are costs we will incur in the future, and we need to put in place a security operation center to monitor our network on a more comprehensive basis." So it does sound more as if he's softening them up for his forthcoming budget.

He also reported that so far, HSE has decrypted 75% of the affected servers. Despite threats from the Conti group to leak the hacked stolen data, HSE stuck to the Prime Minister's refusal to pay and instead forwarded all the information they had about the attack to Ireland's National Cyber Security Center. And then, a week after the attack, the Conti gang provided a decryptor, which Irish officials began testing.

To me, this leaves many questions unanswered. It's none of our business, but one has to wonder how all of that money is going to be spent.

Security News

"Dude! Where's my data?" — The Western Digital My Book Live Mass Exploitation
Last Friday, Western Digital posted the following:

> *Western Digital has determined that some My Book Live and My Book Live Duo devices are being compromised through exploitation of a remote command execution vulnerability. In some cases, the attackers have triggered a factory reset that appears to erase all data on the device.*
>
> *We are reviewing log files which we have received from affected customers to further characterize the attack and the mechanism of access. The log files we have reviewed show that the attackers directly connected to the affected My Book Live devices from a variety of IP addresses in different countries. This indicates that the affected devices were directly accessible from the Internet, either through direct connection or through port forwarding that was enabled either manually or automatically via UPnP.*
>
> *Additionally, the log files show that on some devices, the attackers installed a trojan with a file named ".nttpd,1-ppc-be-t1-z", which is a Linux ELF binary compiled for the PowerPC architecture used by the My Book Live and Live Duo. A sample of this trojan has been captured for further analysis and it has been uploaded to VirusTotal.*
>
> *Our investigation of this incident has not uncovered any evidence that Western Digital cloud services, firmware update servers, or customer credentials were compromised. As the My Book Live devices can be directly exposed to the internet through port forwarding, the attackers may be able to discover vulnerable devices through port scanning.*

We understand that our customers' data is very important. We do not yet understand why the attacker triggered the factory reset; however, we have obtained a sample of an affected device and are investigating further. Additionally, some customers have reported that data recovery tools may be able to recover data from affected devices, and we are currently investigating the effectiveness of these tools.

The My Book Live series was introduced to the market in 2010 and these devices received their final firmware update in 2015.

So, what we have here is an unfortunate situation. We have an instance of long-abandoned IoT NAS devices continuing to be used for six years past their end-of-support life. You can't really blame WD for retiring support after five years — it's their right to do so. Nor, with two important exceptions, can you really blame the users of those apparently perfectly well-functioning NAS devices for continuing to use them. They appeared to be working well the day after their support ended and even a year after their support ended.

This reminds me of an experience I had as a youngster. Definitely at the end of my teen years. I was responsible for paying for my car insurance, and I received a notice that my insurance had lapsed! I was horrified... but I was also hungry and I wanted to go get some food. So, Leo... I got in my car and to my amazement it still ran!... even without insurance. I guess it didn't know. And neither did those Western Digital My Book Live NAS devices know that their support had ended. They just kept on running.

Now, the plot thickens a bit when three years after that end of support, in 2018, a serious remote command execution vulnerability was found and made public. The flaw was assigned a CVE-2018-18472 which NIST described as: "Western Digital WD My Book Live and WD My Book Live Duo (all versions) have a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. It can be triggered by anyone who knows the IP address of the affected device."

The problem was first identified by WizCase in a 2018 report titled: "Vulnerabilities found on WD My Book, NetGear Stora, SeaGate Home, Medion LifeCloud NAS". The report begins:

NAS devices have become the storage device of choice for many small and medium businesses (SMB). They are inexpensive, easy to operate, and you can add additional storage if you're running low on space. But is it secure enough to protect your company's data? That was the question on our mind when we brought in two security researchers to see whether they could exploit any vulnerabilities in the leading NAS devices.

We focused on discovering only critical vulnerabilities that can be exploited remotely without any user interaction. Meaning, authentication bypasses weren't enough. We wanted to execute commands on the devices remotely with the highest privileges.

We were successful, in all the devices.

All four NAS devices tested suffer from a zero-day, unauthenticated root remote command execution (preauth RCE) vulnerabilities. The vulnerabilities allow hackers, governments, or anyone with malicious intention to read files, add/remove users, add/modify existing data, or

execute commands with highest privileges on all of the devices. It is our belief that there are many other NAS devices that suffer from similar vulnerabilities. Both the vulnerabilities (dubbed CVE-2018-18472 and CVE-2018-18471) remain unpatched at the time of this publication. There are nearly 2 million affected devices online.

We don't know how many of those nearly 2 million online NAS devices were WD My Books at the time. That was 2018 and we're now three years later. What we DO know is that finding such devices has never been easier. The public Internet can be scanned, and it has been. A very recent count revealed 55,348 WD My Book Live devices were located, identified, known to be connected and publicly accessible across the Internet.

Following last week's data destruction derby, we need to collectively ask ourselves where the blame falls? Those forensically reviewing logs have suggested that the owners of the WD NAS devices may have been caught in the crossfire between two warring groups. Given the detection of a Linux Trojan on the devices, it seems likely that any of those WD NAS devices that were still in use had, probably for years, been commandeered into the service of a Botnet. So their subsequent destruction via factory reset wiping may have been the consequence of a rival group wishing to shutdown a rival Botnet.

I said at the top that: "Nor, with two important exceptions, can you really blame the users of those apparently perfectly well-functioning NAS devices for continuing to use them." Those two important exceptions are:

1. *Is it safe to continue to use anything that's connected to the Internet after its ongoing maintenance support has ended?* And at the same time, is it really practical to expect users of an expensive piece of equipment that's apparently working well to all stop using it just because support, which doesn't appear to be needed, is no longer available?

2. We know in this day and age that anyone who is not maintaining **multiple** backups of their important data is inherently placing that data at risk. After last week's disaster, many people were posting that they were totally hosed by the loss of 2 terabytes of irreplaceable data. Many many years ago, I designed an advertisement which, to my surprise, won some acclaim at PC Magazine for being the most responded-to advertisement in the magazine's history to that point. That ad began with the simple headline: "Hard disks die." — then it posed the question: "Ever wonder why?" The point being that all mass storage systems are in a perpetual battle against the forces of entropy... and in the end, entropy **will** win. It always does. Nature abhors a sharp edge.

It would be nice to think that WD might have sent their registered owners of those drives a notice in 2018, warning them to take those drives offline because a critical remote compromise problem had been identified and would not be repaired. I would be surprised if that had been done, since WD had moved on by then, three years earlier, to newer devices.

So I guess I'd conclude that the responsibility falls on the users of those systems. They were obtaining many years of continued service life from an out-of-maintenance device. And in the cases where they were screaming about losing valuable information... it was probably going to happen sooner or later anyway.

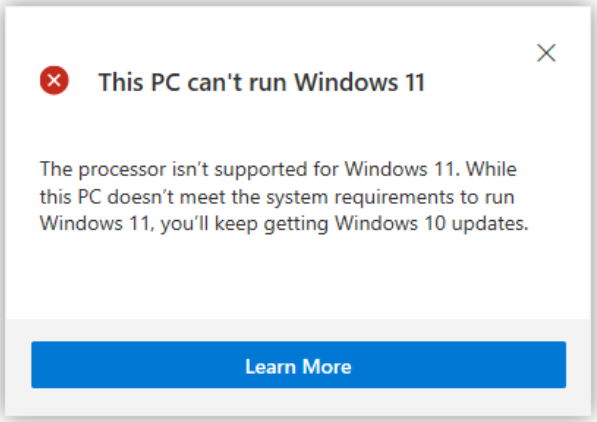
The passing of a living legend
I wanted to note that last Wednesday, John McAfee was found dead by hanging at the age of 75 in his jail cell in Barcelona, Spain. John's extradition to the United States, where he would have been facing a number of legal charges of willful tax evasion had finally been approved by a court in Spain. Despite John's earlier statements that he would never take his own life, and that foul play would definitely be involved if he ever appeared to have done so, everyone assumes that he changed his mind and decided that he was done with life. John's attorney said that his nine months in prison had brought him to despair and attempts to revive him had failed.

As we all know, John was a character and a half, with a life full of antics. I think that the first time we talked about him on this podcast was when he was being sought in connection with the murder of his neighbor, Gregory Faull, who lived next door to John in Belize. Gregory had been found dead, shot in the back of his head by a 9mm bullet. Before that, Gregory had previously confronted John after one of John's quite aggressive dogs had bitten a woman. The dogs were known to get loose and run in packs, terrifying the surrounding community.

John was a source of adventure and controversy. In his earlier years he had worked for NASA, Xerox, and Lockheed Martin before launching the world's first commercial antivirus software in 1987. He and I interacted just once by phone before his launch of McAfee A/V after I had written a series of three columns in InfoWorld which imagined, with as much detail and accuracy as I could, exactly how a theoretical software virus would behave. I don't recall today how clear I made it that this was all conjecture. But a quite animated John McAfee, who was unknown by the PC industry at the time, phoned my office wanting to compare notes and virus samples. He was very disappointed to learn, and it took me some time to convince him, and I'm unsure that I ever did, that my three-column series about software viruses was just written from my imagination as a software developer, not as virus discoverer.

Miscellany

Where will Windows 11 run?
Don’t ask Microsoft because they have no clue.



https://blogs.windows.com/windows-insider/2021/06/28/update-on-windows-11-minimum-system-requirements/

The trouble is, there's no difference between Win11 and Win10 — and everyone knows it. It's the same OS. So Windows 11 **can** run anywhere that Windows 10 runs... unless Microsoft chooses to place arbitrary limits on where they will allow Windows 11 to run. And there's just no way that's going to go down well.

On my own lovely Intel NUC containing a fast 4-core Intel i7-6700HQ Skylake processor with 32 Gigs of RAM, a very large GUID partitioned NVMe mass storage and TPM v2.0. I receive this:

Because there's no actual, legitimate reason why Windows 11 cannot run everywhere and anywhere Windows 10 runs, Microsoft hasn't yet decided where Windows 11 should be **allowed** to run. Their own most recent statement, as of yesterday, essentially admits this, saying:

> *Today, we're releasing the first preview build of Windows 11 to the Windows Insider community. In support of the Windows 11 system requirements, we've set the bar for previewing in our Windows Insider Program to match the minimum system requirements for Windows 11, with the exception for TPM 2.0 and CPU family/model. By providing preview builds to the diverse systems in our Windows Insider Program, we will learn how Windows 11 performs across CPU models more comprehensively, informing any adjustments we should make to our minimum system requirements in the future.* [(What a LOAD!)] *We look forward to the product feedback and learnings as it's an important step to prepare Windows 11 for general availability this year – thank you to the Windows Insider community for your excitement and feedback thus far!*

https://blogs.windows.com/windows-insider/2021/06/28/update-on-windows-11-minimum-system-requirements/

Oh, yes... it's already very exciting! Given the mess and confusion that this is creating, and the clear blowback they're going to be receiving, I think that what should be done is obvious. There's a beautiful compromise available: Unlike Windows 10, Windows 11 should require that any **available** security technologies be enabled on any platform where it runs, but given that, it should run anywhere Win10 runs.

Both of the systems I routinely use have a TPM. One of v1.2 and the other is v2.0. And there's nothing wrong with v1.2 — works just fine. But neither of them are enabled or initialized. Both systems also both offer Secure Boot, but neither have it enabled. Microsoft claims that their telemetry shows that they have seen up to a 60% reduction in malware when TPM-enabled features like Windows Hello and BitLocker encryption are used on supported devices — it's unclear why that would be at all true, unless it's correlation and not causation — people running with those security features enabled tend to be more cautious and careful. But okay. And they also said that <quite> "Devices using the new Windows driver model can achieve a 99.8% crash-free experience." (That's apparently so long as you don't run Windows Update which, as we all know, has the tendency of spoiling one's crash-free experience.)

If the price of allowing me to run Windows 11, on systems that **can** be run with greater security is simply turning on those features, then okay. That's a choice I will make. But tell me that I cannot run Windows 11 on hardware where we know it can run just fine... well, good luck with that. The machine I'm sitting in front of, while we record this podcast, is equipped with an older Haswell processor specifically because Microsoft originally threatened not to support Windows 7 after Haswell. They were later forced to backpedal on that one when corporate America refused

to make the move to Win10, which no one wanted at the time, and insisted upon being able to run Windows 7 on more current hardware.

WhyNot "WhyNotWin11"
There's a new piece of well-intended but very poorly written junk known as "WhyNotWin11."

You can most easily find it by going to https://WhyNotWin11.org. But don't go to http://WhyNotWin11.org (which won't properly redirect to Github) nor to https://WhyNotWin11.com (which is a domain that was grabbed up by someone else who then ignored the author's pleas to synchronize their work). The whole thing is a mess. I'm sure its author means well, and it might eventually provide some useful information. But you'll need to push past Chrome's and Windows' malware alerts, because the app's compiled script is changing minute to minute as its author keeps trying to get it right — thus preventing the code from earning any reputation — and its executable is unsigned. Since the app initially seemed useful, and since I could verify the safety of its operation from its source, I briefly toyed with offering to sign it for the guy, but having watched its subsequent implosion and mismanagement, GRC will have nothing to do with it.

But I did want to put it on everyone's radar: https://github.com/rcmaehl/WhyNotWin11.

I imagine that it will eventually settle down following sufficient community input to help find and eliminate all of its many problems... though by then I expect that Microsoft's own "PC Health Check" tool will have figured out what it wants to say and will become the better choice.

Perhaps the coolest thing about WhyNowWin11 is that it made me aware of a very slick and quite capable 100% FREE Windows scripting tool and environment called: "AutoIt Script" — and that's something that I wanted to put onto our listener's radar:

AutoIt Script:
https://www.autoitscript.com/site/
https://www.autoitscript.com/site/autoit/downloads

It compiles quite capable scripts into standalone and independent EXE's that do not require any **.**NET libraries and it runs under any edition of Windows. The scripting language is extensive, allowing for the Windows UI to be implemented to create quick Windows automation apps and it includes a wonderful and complete 6.8MB old-style compiled Windows Help .CHM files. The help file contains a clear description, tutorials, a language reference, a GUI reference, a COM object reference, and much more. It would probably be just the ticket for enterprise IT admins who need to quickly get something automated to pushed out without resorting to VB.NET or anything heavier. Anyway… "AutoIt Script."

Favorite browser shortcut: CTRL+L - jump to and select URL Bar contents.

Cyotek WebCopy
https://www.cyotek.com/cyotek-webcopy
https://grc.sc/825

Humble Bundle CyberSecurity 2021 by Packt Books
https://www.humblebundle.com/books/cybersecurity-2021-packt-books
https://grc.sc/bundle

$1: 3 books:
- Mastering Azure Security
- Cybersecurity Attacks - Red Team Strategies
- Metasploit 5.0 for Beginners

$10: + 8 (total 11 books)
- CompTIA Security+: SY0-601 Certification Guide
- Cybersecurity Threats, Malware Trends, and Strategies
- Cybersecurity - Attack and Defense Strategies
- Mastering Malware Analysis
- Learn Kubernetes Security
- Learn Wireshark
- Mastering Python for Networking and Security
- Cyber Minds

$18: + 13 (total 24 books)
- Microsoft 365 Security Administration: MS-500 Exam Guide
- AWS Certified Security - Specialty Exam Guide
- Learn Kali Linux 2019
- Mastering Windows Security and Hardening
- Learn Computer Forensics
- Practical Mobile Forensics / Third Edition
- Practical Threat Intelligence and Data-Driven Threat Hunting
- Digital Forensics and Incident Response
- Mastering Linux Security and Hardening / Second Edition
- Practical Hardware Pentesting
- Ghidra Software Reverse Engineering for Beginners
- AWS Penetration Testing
- CISA - Certified Information Systems Auditor Study Guide

Closing The Loop

A frequent and very useful Twitter DM'er sent this: Re: SN 824
Surely "the role of commercial providers" must be the commercial exploit vendors getting their hands on these rather than Google/the Chromium project? I guess they have reason to believe at least some of these 0 days were sold on the open market before exploitation started in the wild.

Mementh / @Mementh
Serious question steve:
Windows 11 might require TPM.
How TNO is it?
Can I trust it to keep the secrets the NSA wants from me from getting out?
Would you put info behind it that would cost you your life if it got broken?
I can't recall what your opinion on it was and I recall the drive you fixed was locked by it.