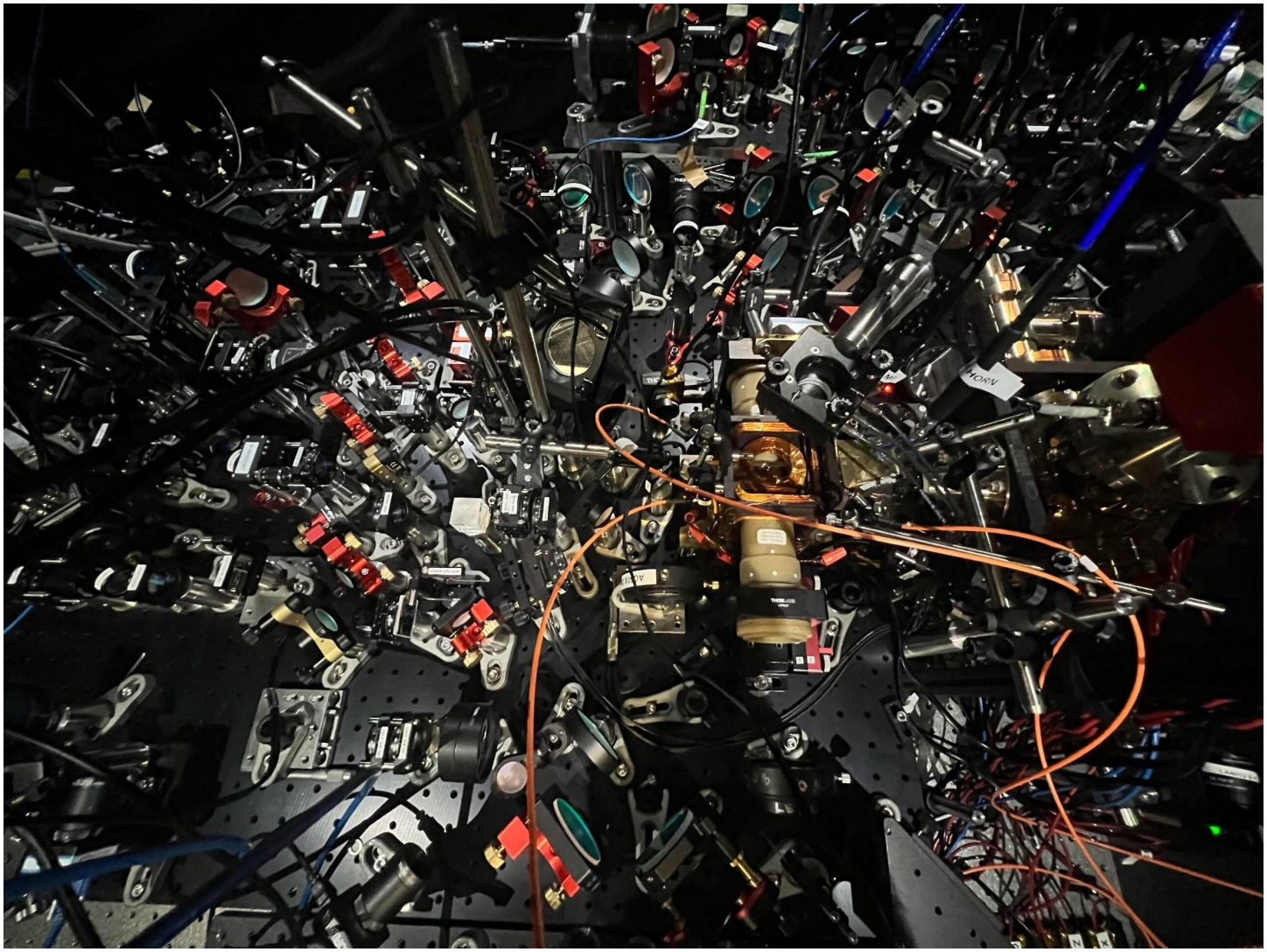
Security Now! #952 - 12-12-23

Quantum Computing Breakthrough

This week on Security Now!

Why is metadata such a problem? What massive new audience just got end-to-end encryption by default? What's the latest on Iran's Cyber Av3ngers? What were the most exploited vulnerabilities of 2023? How are things looking two years after the discovery of the Log4J flaw? Whatever happened with Sony's attempt to force Quad9 to block a music pirate's domain? What exactly is the Dark Web, anyway? And where is it? And after closing the loop with some of our listeners, we're going to examine last week's surprising news of a significant breakthrough in quantum computing!

A breakthrough in quantum computing:



Security News

The underappreciated value of conversation metadata

Last Wednesday, December 6th, one of our favorite privacy-rights crusading senators, Oregon's senator Ron Wyden, addressed a letter to "The Honorable Merrick B. Garland, Attorney General, U.S. Department of Justice. Here's what Wyden wrote:

> *Dear Attorney General Garland:*
>
> *I write to urge the Department of Justice (DOJ) to permit Apple and Google to inform their customers and the general public about demands for smartphone app notification records. In the spring of 2022, my office received a tip that government agencies in foreign countries were demanding smartphone "push" notification records from Google and Apple. My staff have been investigating this tip for the past year, which included contacting Apple and Google. In response to that query, the companies told my staff that information about this practice is restricted from public release by the government.*

That's right... your democracy's tax dollars hard at work tying the hands and gagging companies to prevent them from disclosing what they're being forced to do in what, the name of national security? Ron's letter continues with Ron explaining...

> *Push notifications are the instant alerts delivered to smartphone users by apps, such as a notification about a new text message or a news update. They aren't sent directly from the app provider to users' smartphones. Instead, they pass through a kind of digital post office run by the phone's operating system provider. For iPhones, this service is provided by Apple's Push Notification Service; for Android phones, it's Google's Firebase Cloud Messaging. These services ensure timely and efficient delivery of notifications, but this also means that Apple and Google serve as intermediaries in the transmission process.*
>
> *As with all of the other information these companies store for or about their users, because Apple and Google deliver push notification data, they can be secretly compelled by governments to hand over this information. Importantly, app developers don't have many options; if they want their apps to reliably deliver push notifications on these platforms, they must use the service provided by Apple or Google, respectively. Consequently, Apple and Google are in a unique position to facilitate government surveillance of how users are using particular apps. The data these two companies receive includes metadata, detailing which app received a notification and when, as well as the phone and associated Apple or Google account to which that notification was intended to be delivered. In certain instances, they also might also receive unencrypted content, which could range from backend directives for the app to the actual text displayed to a user in an app notification.*
>
> *Apple and Google should be permitted to be transparent about the legal demands they receive, particularly from foreign governments, just as the companies regularly notify users about other types of government demands for data. These companies should be permitted to generally reveal whether they have been compelled to facilitate this surveillance practice, to publish aggregate statistics about the number of demands they receive, and unless temporarily gagged by a court, to notify specific customers about demands for their data. I would ask that the DOJ repeal or modify any policies that impede this transparency.*

Thank you for your attention to this pressing matter. If you have any questions or require clarification, please contact Chris Soghoian in my office.

Reuters news service followed up on this with some additional reporting, writing:

In a statement, Apple said that Wyden's letter gave them the opening they needed to share more details with the public about how governments monitored push notifications.

Apple wrote: "In this case, the federal government prohibited us from sharing any information. Now that this method has become public we are updating our transparency reporting to detail these kinds of requests." For their part Google said that it "shared Wyden's commitment to keeping users informed about these requests." The Department of Justice declined to comment on the push notification surveillance or whether it had prevented Apple or Google from talking about it.

Wyden's letter cited a "tip" as the source of the information about the surveillance. His staff did not elaborate on the tip, but a source familiar with the matter confirmed that both foreign and U.S. government agencies ***have*** *been asking Apple and Google for metadata related to push notifications to, for example, help tie anonymous users of messaging apps to specific Apple or Google accounts.*

The source declined to identify the foreign governments involved in making the requests but described them as democracies allied to the United States. The source said they did not know how long such information had been gathered in that way.

Most users give push notifications little thought, but they have occasionally attracted attention from technologists because of the difficulty of deploying them without sending data to Google or Apple. Earlier this year French developer David Libeau said users and developers were often unaware of how their apps emitted data to the U.S. tech giants via push notifications, calling them "a privacy nightmare."

We've talked before about the power and value of metadata.

While it may be that Apple and Google's messaging encryption technology deliberately prevents them from being able to comply with lawful government subpoenas – we know quite well that Apple doesn't want to – the ***fact*** that messages are flowing, and between whom they are flowing, is not something that is nearly as easy for Apple to have no way of knowing. These subpoenas doubtless require Apple and Google to provide all information they have of any kind, including specifically metadata, for the individuals targeted by the subpoenas and relating to the apps and other users those targets are interacting with.

Metadata is a pervasive problem. We've talked about how even though today's ISPs are unable to see into today's web connections, the FACT of those connections is not hidden without the use of a VPN to tunnel everything past the ISP's prying eyes. We also talked recently about the move to encrypt the initial TLS handshake packets since they were also carrying metadata. And even the Tor network, whose entire existence is about obscuring endpoint connection metadata, has a difficult time doing so. We've seen that a correlation attack, mounted by examining packets entering and exiting the Tor network – assuming that there's some way to obtain that sort of

near-global visibility, can be surprisingly effective.

So it's significant that Wyden and his team are only, at least in this instance, asking about Apple and Google. It's significant because this is very likely the tip of the iceberg. It would be safe to say that any and all social media enterprises operating inside the US, such as Meta with WhatsApp, are subjected to the same sort of metadata requests accompanied by the same sort of gag orders.

Although law enforcement and other government agencies may be thwarted in their examination of messaging **content**, the social graph networks through which their targets move remains a significant source of valuable and, in fact, vital information. And it's not at all clear how Apple, Google, WhatsApp and the rest can eliminate that loophole, since they are maintaining explicit accounts with the users of those devices. In all of this worry over encryption, backdoors and privacy, the ubiquitous presence of notification, connection and messaging metadata is almost always overlooked.

Facebook Messenger rolling out default E2EE

And while we're on the topic of end-to-end encrypted conversations, also last Wednesday, Facebook announced that their gradual rollout of encryption for Facebook Messenger, which we talked about when it first appeared as an "Encrypted Conversations" option in Messenger, is now switching over to "always on" by default. This took a long time, since it meant that all endpoints would need to have been upgraded. That has happened, so now Facebook is flipping the switch.

Since I was curious about their underlying technology, I did a bit of digging and learned that they had the wisdom to not roll their own encryption system. Facebook Messenger is based on the Signal protocol, even to the extent of borrowing from Signal's open-source libraries at GitHub. Facebook needed to tweak Signal here and there since their platform models are different. But it's nice to know that Messenger's billion+ users will be using a stable and well-proven encryption technology.

Iran's Cyber Av3ngers

Last week we noted that widespread attacks were being seen targeting PLC systems made by the Israeli company Unitronics. These were of particular concern since the systems in question were controlling water management systems in the US and throughout the world. The shocking piece of this was that the systems being "attacked" – and you really need to put the word "attacked" in air quotes here, since given that these systems had never bothered to change their manufacturer's original, factory established password of "1111" connecting remotely to any of the between 500 and 800 systems known to be vulnerable, really amounts to more of a **visit** than an attack. *"Yeah, we're just visiting your system from Iran. What's up?"*

In any event, these Iranians are reportedly continuing to busily scan the Internet for the appearance of any of these PLC systems and we now have the six Iranian IP addresses they're using. I've added them to the show notes for anyone who might be interested in watching their honeypots or their public WAN interfaces for probes from any of these six IPs: 88.135.36.82, 5.144.130.35, 217.144.104.53, 31.7.73.176, 217.144.107.183, 185.143.233.120

Cisco's Talos annual cyber security report

Cisco's Talos group have just published their annual cyber security year in review the thing that caught my eye most was their breakdown of the most targeted vulnerabilities. Before we look at the top 10, here's what the Talos group said about their findings:

In 2023, cyber threat actors exploited older software vulnerabilities in common applications. In many cases, the vulnerabilities were more than 10 years old, consistent with CISA's finding that adversaries have targeted old security flaws more than newly disclosed ones in recent years. In fact, four of the top five most-targeted vulnerabilities we observed were also cited by CISA as being frequently exploited in prior years, further highlighting this point. This underscores the need for entities to regularly install software updates, as many of these systems were likely unpatched given the age of the targeted vulnerabilities.

The top targeted vulnerabilities are found in common applications, like Microsoft Office. This finding is also substantiated by CISA, which noted that actors in 2022 prioritize CVEs that are more prevalent in their targets' networks. Adversaries likely prioritize targeting widespread vulnerabilities because the exploits developed for such CVEs can have long-term use and high impact. Lastly, most of the vulnerabilities on our list would cause substantial impact if exploited, with six receiving a maximum vulnerability risk score of 100 from Cisco Kenna and seven receiving the highest "critical" score from the Common Vulnerability Scoring System (CVSS). Most of the CVEs are also listed in CISA's Known Exploited Vulnerabilities catalog, which is meant to inform users on the security flaws for which they should prioritize remediation. The high frequency of targeting attempts against these CVEs, paired with their severity, underscores the risk to unpatched systems.

Ranking	CVE	Vendor	Product	CISA findings	CISA KEV catalog	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office and WordPad	Routinely exploited in 2022	✓	100/9.3
2	CVE-2017-11882	Microsoft	Exchange server	Routinely exploited in 2022	✓	100/9.3+
3	CVE-2020-1472	Microsoft	Netlogon	Routinely exploited in 2022	✓	100/9.3
4	CVE-2012-1461	Gzip file parser utility	Multiple antivirus products		✗	58/4.3
5	CVE-2012-0158	Microsoft	Office	Commonly exploited by state-sponsored actors from China, Iran, North Korea, and Russia (2016-2019)	✓	100/9.3
6	CVE-2010-1807	Apple	Safari		✗	84/9.3
7	CVE-2021-1675	Microsoft	Windows (print spooler)		✓	100/9.3
8	CVE-2015-1701	Microsoft	Windows (kernel-mode driver)		✓	72/7.2
9	CVE-2012-0507	Oracle	Java SE		✓	100/10
10	CVE-2015-2426	Microsoft	Windows (font driver)		✓	100/9.3

I grabbed the Talos chart of the top ten most often exploited vulnerabilities during this past year. What's astonishing is that this year, the #1 most often exploited vulnerability, with a high CVSS of 9.3, is CVE-2017-0199. That's right, 2017. This is a vulnerability that affects Microsoft Office and Wordpad. This is a remote code execution vulnerability that leverages RTF files and a flaw in Microsoft's equation editor which is exploited through Microsoft Word. We talked about this at time, meaning six year ago, yet still today it distinguishes itself in the list of the top 10 most often exploited vulnerabilities by being #1.

What's absent from these discussions – and from my ability to imagine – are any details about the machines which are, today, still not only running Microsoft's Office software from 2017, unpatched even once since then, but also have no other A/V defense of any kind in place, even Microsoft's free solution. And this is not just one lonely abandoned system somewhere forgotten in a closet. The exploit enters through an eMail attachment. So the systems being compromised not only have no defenses of any kind and haven't received a single update in six years, but they are in active use! And not just a few but a sufficient number to keep the exploitation of this coding mistake in the #1 position.

Want to take a guess at what the #2 problem among the top 10 is? Believe it or not it also has the same high CVSS of 9.3 and its CVE was also issued back in 2017! CVE-2017-11882 ... and that beauty is brought to us by Microsoft's Exchange Server. Obviously the same thing applies as above, although an unattended machine running Exchange Server might well be in some dusty and forgotten back closet.

Lately I've been pushing the idea that automatic updates would solve many of the problems we're seeing in our industry. But Microsoft pioneered the idea of automatic updates – they're enabled by default and have been for a very long time. Yet somehow a huge number of machines are not being patched. It would really be interesting to look at case studies of the machines and the environments that allowed six year old Microsoft flaws to remain present today.

Over 30% of apps are still using a using a vulnerable version the Log4J library

While we're on the topic of long lasting vulnerabilities, it's not only the deep past that seems to be behaving irresponsibly. Two years ago, 2022 was kicked off with the news that a potentially devastating flaw in the Log4J library might rock the Internet. Fortunately, that never happened because the flaw was not readily exploited, so it was never the lowest hanging fruit. But that didn't mean that the flawed library didn't still need to be fixed and replaced, because as long as this known-to-be-vulnerable library was present, a resourceful hacker might find a way to exploit it. Last Sunday, on the 2nd anniversary of the discovery of this flaw, BleepingComputer reported on the findings of the application security company Veracode who took a look at the status of Log4J, today. Here's what BleepingComputer reported:

> ***Roughly 38% of applications*** *using the Apache Log4j library are using a version vulnerable to security issues, including Log4Shell, a critical vulnerability identified as CVE-2021-44228 that carries the maximum severity rating, despite patches being available for more than two years.*

Log4Shell is an unauthenticated remote code execution (RCE) flaw that allows taking complete control over systems using Log4j 2.0-beta9 through 2.15.0. The flaw was discovered as an actively exploited zero-day on December 10, 2021, and its widespread impact, ease of exploitation, and massive security implications acted as an open invitation to threat actors.

The circumstance prompted an extensive campaign to notify affected project maintainers and system administrators, but despite numerous warnings, a significant number of organizations continued to use vulnerable versions long after patches became available. Two years after the vulnerability was disclosed and fixes were released, there are plenty of targets still vulnerable to Log4Shell. A report from application security company Veracode, based on data collected between August 15 and November 15, highlights that old problems can persist for extended periods.

Veracode gathered data for 90 days from 3,866 organizations that use 38,278 applications relying on Log4j with versions between 1.1 and 3.0.0-alpha1.Of those apps, 2.8% use Log4J variants 2.0-beta9 through 2.15.0, which are directly vulnerable to Log4Shell . Another 3.8% use Log4j 2.17.0, which, although not vulnerable to Log4Shell, is susceptible to CVE-2021-44832, a remote code execution flaw that was fixed in version 2.17.1 of the framework. Finally, 32% are using Log4j version 1.2.x, which reached the end of support in August 2015 and all of those versions are vulnerable to multiple severe vulnerabilities published until 2022, including CVE-2022-23307, CVE-2022-23305, and CVE-2022-23302.

In total, Veracode found that about 38% of the apps within its visibility use an insecure Log4j version. This is close to what software supply chain management experts at Sonatype report on their Log4j dashboard, where 25% of the library's downloads in the past week include known vulnerable versions.

The continual use of outdated library versions indicates an ongoing problem, which Veracode attributes to developers wanting to avoid unnecessary complications. Veracode found that 79% of developers choose to never update third-party libraries after their initial inclusion in their code base to avoid breaking functionality. This is true even if 65% of open-source library updates contain minor changes and fixes unlikely to cause functional problems.

Moreover, the study showed that it takes half of all projects over 65 days to address high-severity flaws. It takes 13.7 times longer than usual to fix half of what's in their backlog when understaffed, and over seven months to handle 50% of it when lacking information.

Overall, Veracode's data shows that Log4Shell was not the wake-up call many in the security industry hoped it would be. Instead, Log4j alone continues to be a source of risk in 1 out of 3 cases and may be one of the multiple ways attackers can leverage to compromise a given target. The recommendation for companies is to scan their environment, find the versions of open-source libraries in use, and then develop an emergency upgrade plan for all of them.

There are many places where our industry is limping along and hoping for the best such as with the use of very useful open source libraries. One of the problems is that developers could spend all of their time just keeping their code current with upstream library version changes. I love the Notepad++ application for Windows. It's really terrific. But its developer refuses to leave it alone. So it's constantly wanting to update itself. Since it does everything I want, I finally disabled its checking for updates. But now, if it did have a real problem, I wouldn't know.

So, I can imagine how much chaos there would be if a project was using a large assortment of

open source libraries which were, themselves, dependent upon other libraries, and so on up the dependency tree. It likely would be a full time job just trying to stay current. So it's not difficult to imagine a developer thinking: "Look, everything's working right now. I do not want to rock the boat and risk breaking things that are working... just for the sake of having the latest and greatest version of everything."

Sony loses their suit against Quad 9!

Two years ago we reported on the despicable tactic Sony was undertaking of blaming the DNS resolving service Quad 9 for the fact that they were providing the IP address of a pirate domain whose server was making Sony's copyrighted recordings available. Sony said that the domain owners did not respond and could not be located, so they decided to sue Quad 9. At the time Leo and I were livid at the idea that Sony might prevail since this might set a precedent where anyone with a grievance could sue someone who was providing some of the Internet's infrastructure, regardless of how incidental to the underlying complaint.

Here we are two years later with the news that the German court where Sony brought this case has ruled in favor of the defendant, Quad 9, denying any appeal and instructing Sony to pay all of the defendant's defense costs.

Here's what Quad 9 had to say about all of this:

Today marks a bright moment in the efforts to keep the internet a neutral and trusted resource for everyone. Quad9 has received word from the courts in Dresden, Germany in the appeal of our case versus Sony Entertainment (Germany). The court has ruled in favor of Quad9, clearly and unequivocally. Needless to say, we are elated at the news.

Sony Entertainment (Germany) started a legal proceeding against Quad9 more than two years ago to force Quad9 to stop resolving certain domain names which they claimed were involved in copyright infringement behavior.

We believe this lawsuit was an attempt to set a precedent, such that commercial rights holders could demand that sites on the internet be made unreachable by forcing recursive resolvers to block content. We contended that recursive resolvers have no commercial or even remotely indirect relationship to any of the infringing parties, and that Sony's demand for blocking was ineffective, inappropriately specified, and not related to Quad9.

What made this case more problematic, in our view, was that the servers in question in this case were not located in Germany, and the links they pointed to were on servers also not in Germany. The domain name (canna.to) was not registered in Germany and was under the top-level-domain operated by the nation of Tonga. Sony Entertainment further asserted that we block the domains globally, not just in Germany, as geoIP does not block for users based in Germany with certainty. For that matter, Quad9 has no office or standing in Germany (we are a Swiss entity), but due to the Lugano Convention treaty it was possible for Sony to serve an injunction in Switzerland and drag Quad9 into legal proceedings.

The appeal with the Higher Regional Court in Dresden follows a decision by the Regional Court in Leipzig, in which Sony prevailed, and Quad9 was convicted as a wrongdoer. Before that, Sony successfully obtained a preliminary injunction against Quad9 with the Regional Court in Hamburg. The objection against the preliminary injunction by Quad9 was unsuccessful, and

the appeal with the Higher Regional Court in Hamburg was withdrawn by Quad9 since a decision in the main proceeding was expected to be made earlier than the conclusion of the appeal in the preliminary proceedings.

The court has also ruled that the case cannot be taken to a higher court and their decision is the final word in this particular case. Sony may appeal the appeal closure via a complaint against the denial of leave of appeal and then would have to appeal the case itself with the German Federal Court. So while there is still a possibility that this case could continue, Sony would have to win twice to turn the decision around again.

We would also like to clarify that even though Quad9 benefits from the liability privileges as a mere conduit, it is possible that a DNS resolver operator can be required to block as a matter of last resort if the claiming party has taken appropriate means to go after the wrongdoer and the hosting company unsuccessfully. Such measures could be legal action by applying for a preliminary injunction against a hosting company within the EU. These uncertainties still linger, and we expect that this ongoing question of what circumstances require what actions, by what parties, will continue to be argued in court and in policy circles over the next few years.

We remain committed to the concept that resolving a domain name is not an action that should be prohibited for commercial goals. The DNS does not contain content - it is a system designed for delivery only of pointers, not for data transport.

The courts in Cologne also recently ruled in favor of Cloudflare in a similar case involving DNS recursive resolution (though that case also includes a separate consideration of issues relating to CDN and proxying services.) and we are pleased to have consistent and clear statements from both courts in this matter of DNS recursive resolution.

Today was a significant win in Germany, but there is some disappointment as well. We received a notice from a consortium of Italian rightsholders (Sony Music Italy, Universal Music Italy, Warner Music Italy, and Federation of Italian Music Industry) who have demanded that Quad9 block domains in Italy, and there is potentially another court process ahead of us.

So this is good news, but it's also clear that this is not over yet. Sony is at it again, attempting to use their muscle to force Quad 9, a non-profit DNS resolving company, to bend to their will. Here's the status of this second new lawsuit. Quad 9 wrote:

While our case in Germany has been found in favor of Quad9, we have been served with another demand from commercial interests in an EU nation to block domain names, again based on alleged copyright violations. Italian legal representatives have presented us with a list of domains and a demand for blocking those domains. Now we must again determine the path to take forward fighting this legal battle, in another nation in which we are neither headquartered nor have any offices or corporate presence.

Unsurprisingly, the group of media companies that are represented by the plaintiff (LGV Avvocati, Milan, Italy on behalf of the Federation against Music and Multimedia Piracy) are Sony Music Entertainment Italy s.p.a, Universal Music Italy s.r.l., and Warner Music Italia s.r.l. as well as the Federation of the Italian Music Industry (FIMI).

The short answer from us is that we're going to fight this demand for censorship, but it may take us time to be certain of a full victory and completion of our case in Germany before we

are able to take on another court process. Quad9 can only have a few legal fronts open at once - we are nearly entirely dedicated to operational challenges of running a free, non-profit recursive resolver platform that protects end users against malware and phishing. We are not a for-profit company with lawyers on retainer.

We have complied with the request, and these names are now blocked on Quad9 systems. Since the courts have provided again no guidance on how we determine if a request is made by someone under Italian jurisdiction, we have applied this block globally. The German courts entirely disregarded our use of geo-IP lookups on queries, and asserted that since tests via a VPN were able to resolve the domain, we were in breach of court orders - we wish to avoid that same distraction again for the moment.

We have created an attributed blocking list with these domains on it, and they are searchable on the front page of our website in the search bar, and the results will contain information about the status and origin of the blocking requirements. When Quad9 decides to take action on this issue, we will post updates on this blog and modify our blocklists accordingly.

This is so wrong. I'm so glad that the court in Dresden made Sony responsible for all of the costs of Quad 9's defense, and I hope Quad 9 may be able to use their success in Germany to help with this next case. What Sony, Universal and Warner are doing is so wrong.

The webs we weave

A group known as Searchlight Cyber posted an analysis about the state of the DDoS for Hire business which exists on the so-called Dark Web. That made me realize that while I've referred to the Dark Web in the past, we've really never stopped to talk about it.

For anyone who's unsure, "The Dark Web" is actually a thing, or rather a place – it's not just an expression. And you can't get there from here. It's not just a matter of using some secret URL to bring up a Dark Web site. There are three terms used within the cyber security community to refer to three classes of the web: There's the clear web, the deep web and the dark web.

The web that we all use everyday is more formally known as "The Clear Web." It's what Google indexes and where anyone can easily wander with links that are shared with us either by any public search engine or by other web pages. This is the traditional web that Tim Berners-Lee first conceived at CERN. And interestingly, this "Clear Web" only contains roughly 4% of the entire web's content. So where's the rest? Most of the rest resides in the so-called "Deep Web."

This is web content that's **not** indexed because it requires authenticated access through a portal of some kind. So this includes things like our credit reports, IRS tax records and medical histories, fee-based content, membership websites and confidential corporate web pages. Those are all considered to exist on the "Deep Web." And estimates place this deep web content at roughly 96% of the total browser-accessible web.

And finally, a small subset of this "Deep Web" is known as "The Dark Web." The dark web's servers are deliberately hidden and are accessible only through the Tor browser on the Tor network. It's necessary to use Tor because those servers and the services they offer wish to remain hidden and difficult if not nearly impossible to locate. And it's worth noting that despite

its ominous sounding name, not all the dark web is used for illicit purposes though this is another place where the emergence of cryptocurrency has transformed the place from a backwater hacker curiosity into a significant collection of criminal enterprises.

My advice would be to stay as far away from the dark web as possible. So I won't be offering any guide or tips to accessing this dark underbelly of the Internet. But if you're really curious and want to go poking around down there, you'll find that the clear web contains many step-by-step how-to guides into setting up a secure sandboxed OS, obtaining the Tor browser, putting on your hazmat suit, holding your breath and taking the plunge. Good luck!

And as for what the Searchlight Cyber guys found about DDoS for Hire services being offered on the Dark Web, there was nothing really noteworthy. It's pretty much what we would expect: Portals exist there people can create an account and transfer some of their cryptocurrency into it to create a balance. Then they select the type of DDoS attack they wish to launch, either at OSI stack level 4, which is the transport layer, so either a UDP or TCP flood, or at level 7, which is the application layer, so an HTTP connection and query flood. Then the target IP or URL is provided and the size and duration of the attack is specified... and the site takes care of conducting the attack. One thing that surprised me was that one of these services, named the "Nightmare stresser" claimed to have 566,109 registered users. That number cannot be verified, but it does perhaps support the view from up here in the light of the clear web why and how DDoS attacks have become so prevalent.

Closing the Loop

Mike Ward (via DM)

Hi Steve I just discovered a major privacy and security flaw in the messaging app Telegram.

*Telegram automatically informs users you have joined if that user has your phone number, and has previously uploaded it to Telegram as part of their contacts! Even if you deny Telegram access to **your** contacts!*

I discovered this first hand just now; after downloading and signing up for telegram, and specifically denying it access to my contacts, a friend sitting across the table from me got a notification on his phone and said "you've joined Telegram".

This is a MAJOR privacy and security flaw, as a stalker or domestic abuser could upload a victims number and be automatically notified if that person ever joins Telegram! For that matter, so could any law enforcement or government agency. It may also explain why spam and scams are so prevalent on the services, as malactors are able to upload your phone number acquired from somewhere else, then inundate you with messages the moment you join!

I agree with Mike that this appears to be a significant privacy failing of Telegram. The system ought to require ***mutual*** sharing of intersecting contact information in order to provide any notifications, not just one-way, unilateral contact use. They likely use the less private approach as a means of promoting the further use and adoption of Telegram. But that's not what anyone wants in a secure messaging solution.

Justin Ekis / @jekis

Have you ever seen something like this? Looks like my cell carrier is forcing me to trust an additional root CA. This is unacceptable. I'll be switching at the earliest opportunity. Thought my fellow listeners would like to know.
https://twitter.com/messages/media/1734066118073962718

Justin attached a screenshot of his Xfinity cellular provider asking him to accept a root certificate and to give it full trust on his phone. I agree with him completely. There's only one possible reason for this, which is that Xfinity wishes to insert a transparent proxy into his Internet connections, this decrypting everything that he does with his phone. That should certainly raise warning flags for anyone who understands what's going on. Unfortunately, nearly everyone will simply comply.

Elliot.Alderson / @ElliotAlders369

Instead of pulling all but 6 CAs, couldn't someone make an extension that just shows Green for one of the main 6, Yellow for another CA, Red for HTTP, and a duck for a QWAC cert? May need Blue, Orange, and Pink or something for the color blind.

That's an interesting thought. But my concern would be that this places the burden on the user to observe some visual flag. If our goal in removing the ridiculous number of barely, if ever, needed certificate authority root certs is to improve our security in the event that one of the fringe CAs mints a malicious cert, then I still think that the cost of running with only the top six is likely minimal.

Michael Smithers / @michaelsmithers

Hi Steve, I'm a long-time listener and SpinRite customer. Thankyou for all your work! Can you recommend a hardware VPN solution for home that's not complicated to set up? I need to access my home server from around the world - mainly for version control access - and I presently have some ports internet-facing with port forwarding. Yes, I know this is not good! I can see from the logs that bots are continuously attempting to guess login credentials and are causing user lock-outs for some (more common) usernames. Many thanks for your help. Here's to 1000 and beyond, Michael

VPNs are definitely useful when you want to protect your use of the Internet for example, from your prying ISP. But setting up your own VPN server to provide incoming access is probably no longer the optimal solution. For all of those needs you really want to look at an overlay network. Think "TailScale" or "ZeroTier." Overlay networks is the newer, better, more secure and much more powerful and flexible way to solve this sort of problem. We've talked about these before and I've received a bunch of feedback from our listeners who have said that they have been astounded by how easily the system was to install, setup and get running. And another advantage is that they run through NAT routers without needing any static port forwarding, so no bots are going to be probing for a connection. TailScale has a comparison page with ZeroTier

which I've looked at in the past. It appears to be quite even handed. Since nothing else has claimed GRC's shortcut of the week so far https://grc.sc/952 will take you directly to that page. https://tailscale.com/compare/zerotier/ I'm very glad that Michael asked this question since today's new overlay network solutions really do represent a useful advance and a better way to solve the need for roaming access to a remote network.

Chris Hatch / @chrisbhatch

Steve, very thankful you are continuing SN past 999. Long time listener. Just heard you mention APIMonitor. When I put the URL in firefox Malwarebytes blocked going there with the warning "Website blocked due to Trojan". I checked with Virus Total and it had two A/V's that thought it was malicious. What do you do, to check if a site is safe to visit? Looking forward to upgrading spinrite when 6.1 released. Thanks for a great show. -Chris

Unfortunately, that amazing API Monitor is about ten years old and it hasn't been touched in all that time. It is also not digitally signed since, ten years ago, few things were. And I recognize that many people feel that any software that has apparently been abandoned is automatically worthless. That's not my feeling at all. I strongly prefer software that has become stable because all of its bugs have been found and eliminated, making that software complete and finished. I'm fully aware that's not the way our industry has evolved where many programs are full of bugs or where commercial interests require that software remains forever in flux with people continually paying in the hope that it will finally be finished.

For what it's worth, only triggering two out of all of VirusTotal's A/V scanners, generally about 70, means that there's nothing whatsoever wrong with that code. If the screen had lit up with 20 more out of 70, then, yeah, I would never have let it get near my machine. I just dropped my copy of API-Monitor-Setup.exe which I downloaded and then tested against VirusTotal. I just now received a 0 out of 71 score. So VirusTotal agrees that the code being served by that site, old and unsigned as it is, is clean and safe to use.

Quantum Computing Breakthrough

a breakthrough for the Turbo Encabulator!
or "all your Qubits are belong to us!"

DARPA-funded quantum computing research conducted at Harvard made headlines last Thursday with what those in the know are pretty certain represents a significant step forward in the quest for a practical quantum computer.

One of the big problems, which is currently limiting the practical application of quantum computers, is the need for extensive error correction. One way to think of this is that quantum bits, the so-called qubits, are powerful but imprecise. So when you need precision for things like cryptographic computations, where quantum's fuzziness is a bug not a feature, it's necessary to use a whole bunch of fuzzy qubits in an error-correcting system. The individual fuzzy qubits are referred to as "physical" qubits. But what we want and need for many of the types of calculations that quantum computers promise, are what's known as "logical" qubits. And as I said, traditionally, the number of physical to logical qubits has been around 1000:1. Which is to say that it takes 1000 fuzzy physical quantum bits in an error-correcting mode to reliably obtain a single solid logical bit. And it's only the logical bits that are able to do most of the useful work.

In a minute, I'll share a useful explanation of what was recently accomplished and just published. And that will come from a non-physicist who speaks English as his first language, rather than "quantum". Reading the actual paper, published in "Nature" last Wednesday, written by those who speak "quantum" fluently, I was reminded of our favorite Turbo Encabulator which made good use of those Flambulating differential reverse trunions. So, to give everyone a flavor of just how far out this science has wandered, this is what they wrote for the Abstract of their paper, which was titled: *"Logical quantum processor based on reconfigurable atom arrays"*. They wrote:

> *Suppressing errors is the central challenge for useful quantum computing, requiring quantum error correction for large-scale processing. However, the overhead in the realization of error-corrected "logical" qubits, where information is encoded across many physical qubits for redundancy, poses significant challenges to large-scale logical quantum computing. Here we report the realization of a programmable quantum processor based on encoded logical qubits operating with up to 280 physical qubits. Utilizing logical-level control and a zoned architecture in reconfigurable neutral atom arrays, our system combines high two-qubit gate fidelities, arbitrary connectivity, as well as fully programmable single-qubit rotations and mid-circuit readout. Operating this logical processor with various types of encodings, we demonstrate improvement of a two-qubit logic gate by scaling surface code distance from d = 3 to d = 7, preparation of color code qubits with break-even fidelities, fault-tolerant creation of logical GHZ states and feedforward entanglement teleportation, as well as operation of 40 color code qubits. Finally, using three-dimensional [[8x3x2]] code blocks, we realize computationally complex sampling circuits with up to 48 logical qubits entangled with hypercube connectivity with 228 logical two-qubit gates and 48 logical CCZ gates. We find that this logical encoding substantially improves algorithmic performance with error detection, outperforming physical qubit fidelities at both cross-entropy benchmarking and quantum simulations of fast scrambling. These results herald the advent of early error-corrected quantum computation and chart a path toward large-scale logical processors.*

Well, naturally... because like they said, what you're looking for is high fidelity feedforward entanglement teleportation. Yikes! Since everyone agrees that if this turns out to work as it appears to, it would represent a bonafide breakthrough in quantum computing by dramatically reducing that 1000:1 physical-to-logical qubit ratio thanks to a breakthrough in quantum error correction technology, it immediately became this week's podcast topic. So I now want to share something that was written about this by a non-physicist where there will be no mention of any "feedforward entanglement teleportation." It begins with this powerful claim:

Widespread quantum computing may now come years sooner than widely expected, *thanks to a Pentagon-funded project (as in DARPA which, as we know, also brought the world the Internet), with implications for everything from rapid vaccine development and weather forecasting to cyber warfare and codebreaking.*

If the Harvard-led experiment can be replicated and scaled up, it would still take years to make quantum computers widely available to run new forms of artificial intelligence for medical research, scientific experimentation and military command-and-control. But early adopters would almost certainly include intelligence agencies eager to crack encryption protocols widely used by governments and businesses alike. That makes it all the more urgent to implement the new quantum-resistant encryption algorithms the National Institute of Standards & Technology (NIST) aims to finalize next year in 2024.

On Wednesday afternoon, the Defense Advanced Research Projects Agency (DARPA) and a paper in Nature announced results from a team of almost two dozen scientists, most of them from Harvard, funded by a DARPA program known as ***ONISQ*** *(Optimization with Noisy Intermediate-Scale Quantum devices). By manipulating individual atoms with precise, low-powered laser beams, known in the trade as "laser tweezers," the team was able to create "quantum circuits" that correct for errors much more efficiently than alternative techniques — potentially overcoming the biggest barrier to practical quantum computers.*

DARPA's program manager for ONISQ said "Quantum error correction is fundamentally challenging."

Mikhail Lukin, one of the Harvard scientists, said: "You cannot copy quantum information and you can also not measure the quantum state without destroying it."

Different corporate, government and academic teams have tried various approaches to error correction, but they all waste an "exorbitant" amount of the quantum computer's power. But the Harvard team has found a radically more efficient way to guard against errors.

DARPA's program manager said: "This is truly revolutionary. Having been demonstrated and even validated in this paper ... we are off to the races."

A back-of-the-envelope calculation suggests that the Harvard-team's experimental quantum computer is potentially four times as powerful as the most advanced quantum chip available for purchase, IBM's Condor.

Unveiled on Dec. 4, Condor boasts 1,121 qubits, which is almost a three-fold increase over last year's record-breaking IBM Osprey. So what's a qubit? The term turns out to have multiple meanings.

While a normal "classical" computer uses bits that can represent either 0 or 1, a qubit exploits the fuzzy nature of quantum phenomena to let it represent all the infinite possible values in between. That's a nifty trick that could shortcut previously impossible calculations. But because quantum phenomena are so strange, it's also much harder to figure out whether a qubit is working properly or glitching.

So, all quantum computers to date have had to devote most of their qubits to double-checking each other. That means the number of usable "logical qubits" that can actually do reliable calculations is orders of magnitude smaller than the number of a machine's "physical qubits."

Using current error-correcting methods, it takes more than a thousand physical qubits acting together to form one logical qubit. IBM is now exploring a new, more efficient error-correcting technique it says should allow a mere hundred physical qubits to form a logical qubit. So depending on which technique is used, a high-end chip with a thousand physical qubits, like Condor, could generate as little as one usable logical qubit or as many as ten.

The Harvard team, however, used a radical new approach to error correction that turns a mere 280 physical qubits into 48 logical qubits. That's about 20 times better than what IBM is hoping to achieve in its next-generation chip and ***200 times more efficient*** *than the 1,000-to-one ratio that current techniques try to reach.*

One of the Harvard physicists said: "Up till now, the state-of-the-art people have realized was one logical qubit or maybe two at most … we have done 48. For the first time, we've actually built a processor which operates on these logical qubits. … We demonstrated the key basic elements of this processor, namely the ability to encode, decode, and perform logical gate operations. For the first time ever, we executed algorithms with logical qubits."

Skip Sanzieri, co-founder of QuSecure, which builds software to defend against quantum-powered hacking, said ***logical*** *qubits are the "Holy Grail" for quantum computing. He explained that physical qubits are very ethereal: they can be disturbed easily, which is what leads to errors. Sanzieri said: "With the Harvard team's approach you don't need the thousands, hundreds of thousands, or millions of physical qubits to error-correct. If it works it's a huge speed-up."*

I want to flesh this out a bit more with some additional background and quotes from the researchers. Quoting from some additional coverage of this breakthrough...

The system is the first demonstration of large-scale algorithm execution on an error-corrected quantum computer, heralding the advent of early fault-tolerant, or reliably uninterrupted, quantum computation.

Professor Lukin, who runs the lab at Harvard, described the achievement as a possible inflection point akin to the early days in the field of artificial intelligence: the ideas of quantum error correction and fault tolerance, long theorized, are starting to bear fruit.

He said, "I think this is one of the moments in which it is clear that something very special is coming. Although there are still challenges ahead, we expect that this advance will greatly accelerate the progress toward large-scale, useful quantum computers."

The National Science Foundation's Denise Caldwell, the acting assistant director of the Mathematical and Physical Sciences Directorate which supported the research through the NSF's Physics Frontiers Centers and Quantum Leap Challenge Institutes programs, agrees. She said: "This breakthrough is a tour de force of quantum engineering and design. The team has not only accelerated the development of quantum information processing by using neutral atoms, but opened a new door to explorations of large-scale logical qubit devices, which could enable transformative benefits for science and society as a whole."

In quantum computing, a quantum bit or "qubit" is one unit of information, just like a binary bit in classical computing. For more than two decades, physicists and engineers have shown the world that quantum computing is, in principle, possible by manipulating quantum particles — be they atoms, ions, or photons — to create physical qubits.

But successfully exploiting the weirdness of quantum mechanics for computation is more complicated than simply amassing a large-enough number of qubits, which are inherently unstable and prone to collapse out of their quantum states.

The real coins of the realm are the so-called logical qubits formed from bundles of redundant, error-corrected physical qubits. These can store information for use in a quantum algorithm. Creating logical qubits as controllable units — like classical bits — has been a fundamental obstacle for the field, and it's generally accepted that until quantum computers can run reliably on logical qubits, the technology cannot really take off.

To date, the best computing systems have demonstrated one or two logical qubits, and one quantum gate operation — akin to just one unit of code — between them.

*The Harvard team's breakthrough builds on several years of work on a quantum computing architecture known as a **neutral atom array**, this was also pioneered in Lukin's lab. It is now being commercialized by QuEra, which recently entered into a licensing agreement with Harvard's Office of Technology Development for a patent portfolio based on innovations developed by Lukin's group.*

The key component of the current system is a block of ultra-cold, suspended rubidium atoms, in which the atoms — the system's physical qubits — can move about and be connected into pairs — or "entangled" — mid-computation. Entangled pairs of atoms form gates, which are units of computing power. Previously, the team had demonstrated low error rates in their entangling operations, proving the reliability of their neutral atom array system. With their logical quantum processor, the researchers now demonstrate parallel, multiplexed control of an entire patch of logical qubits, using lasers. This result is more efficient and scalable than having to control individual physical qubits.

The paper's first named author Dolev Bluvstein, a Griffin School of Arts and Sciences Ph.D. student in Lukin's lab said: "We're trying to mark a transition in the field, toward starting to test algorithms with error-corrected qubits instead of physical ones, and thus enabling a path toward larger devices."

So, everyone agrees that this is almost certainly a benchmark on the road to moving quantum computing from a promising curiosity in the lab to a place where it can be commercialized for use in solving previously intractable problems in the real world. Cryptography is not in trouble yet. But that trouble just jumped significantly closer.

Remember that it's not symmetric crypto that's endangered by quantum computing. So algorithms such as the AES's Rijndael cipher and hashing-based solution have always been and will likely continue to be quantum safe. But asymmetric crypto such as RSA, based on the previously intractable problem of factoring a huge number composed of two half-as-huge prime numbers, and elliptic curve crypto are both on the chopping block.

So it was prescient that the academic crypto community began worrying about this years ago and has now generated a series of quantum-safe replacement algorithms that are rapidly being moved toward adoption.

The challenge is that almost everything that's currently being done in the world is still using traditional quantum unsafe asymmetric cryptography. I say almost everything, because remember that three months ago, in September, Signal announced their adoption of quantum-safe crypto running in parallel with traditional time-proven, but now potentially unsafe, crypto.

The other entity that has proven itself to be prescient is the U.S. National Security Agency, our NSA. As we know, having watched them build that massive data center facility out in Utah, they've taken advantage of the astonishing reduction in the cost of electromagnetic storage – or "spinners" as we call them over in GRC's newsgroups and forums – to suck up and store mass quantities of Internet and other communications that they cannot decrypt today... but which they will likely be among the first to be decrypting once they receive their standing order for serial number 1 of a sufficiently powerful quantum computer. I'll bet that facility already has a room set aside and just waiting for something to be installed.

What this means for the industry is that we're not going to be able to enjoy the traditional luxury of upgrading our communications encryption when we eventually get around to it. It will be necessary for the finally approved standards to be moved into preliminary implementations with more speed than normal. The good news is that this is not our first retirement of creaky older crypto in favor of shiny new crypto, so we've gained experience with doing this and can expect it to go smoothly. Once sufficient testing has been done, these next generation algorithms will need to be deployed. And again, not eventually, but as immediately as possible.

The wisdom Signal demonstrated, of running any new and inherently less well proven algorithm alongside a traditional well-proven asymmetric crypto system, may be best in the near term. Requiring that the results from both systems are needed for encrypting and decrypting an ephemeral symmetric key provides protection against the possibility of an unexpected weakness being found in the newer post-quantum system breaking everything. Then later, once the new system has been shown to be entirely safe, the secondary parallel backup system could be dropped to obtain a boost in performance.

This surprise, last week, is yet another reason for taking this podcast past 999! We **definitely** want to be here to chronicle the adventure and the arrival of post-quantum cryptography!