Encrypting DNS

Description: This week we cover a few bullet points from last Tuesday's monthly Windows patches, as well as some annoyance that the patches caused for Windows 7 users. We track some interesting ongoing ransomware news and look at the mixed blessing of fining companies for self-reporting breaches. We check out a survey of enterprise malware headaches, update some Mozilla/Firefox news, and examine yet another (and kind of obvious) way of exfiltrating information from a PC. We address a bit of errata, some miscellany, and closing-the-loop feedback with our listeners. We then conclude with a closer look at all the progress that's been occurring quietly with DNS encryption.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-723.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-723-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He has an update on Microsoft's Patch Tuesday update. He also talks about LaPorte County. It was struck by Ryuk. And are IT professionals prepared for ransomware? Plus we'll talk about, in more detail, DNS over HTTPS. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 723, recorded Tuesday, July 16th, 2019: Encrypting DNS.

It's time for Security Now!. Ladies and gentlemen, here he is, the star of our show, Steven Gibson of the Gibson Research Corporation, king of the hill when it comes to security NOW. Hi, Steve.

Steve Gibson: Hey, Leo. It's great to be with you again. Episode 723. And in my errata I have a note from Elaine because she heard me stumbling over what year this was. And so she just said, "By the way, you will be beginning year 15 on August 20th." So we're closing in on the end of our 14th year. And last week's mention, you know, we talked about Mozilla's adoption of encrypting DNS for privacy and the U.K.'s pushback, the ISPA, whatever that was, the association of Internet service providers...

Leo: They called them the "Villain of the Year."

Steve: The villain of the year, yes, one of three nominated as Villain of the Year. And my conversation about that generated as much interest as we've seen in a long time. So I decided, okay, let's sort of take a look at where we are because we haven't talked about

this since the early days of OpenDNS and DNSCrypt, which, I mean, we've touched on it a little bit here and there, but not given it any time. So today's topic is "Encrypting DNS," which we will get to.

But first we're going to talk about a few bullet points from last Tuesday's Patch Tuesday, which, interestingly, Adobe chose not to synchronize themselves with. Normally they're doing their patches on the same Tuesday as Microsoft, but not this time. Also there was a little bit of upset caused for some Windows 7 users. I just wanted to mention it in passing because it was interesting that Microsoft has probably deliberately done something they said they would not do. We'll track some interesting ongoing ransomware news. And there's even a county with your name, Leo, that has been attacked, LaPorte County.

Leo: Oh, those Laportes get around, I tell you.

Steve: Ah, they do. We're going to look at the mixed blessing of fining companies for self-reporting breaches, why I'm not that sanguine about the idea of major fines being levied against, well, in this case it's Marriott, and it's big, and it's the GDPR regulation being used against them. Which, I don't know, it feels wrong, but we'll see.

Oh, there was an interesting survey that Sophos commissioned, an independent survey of 3,100 IT execs about the problems they have, which produces some interesting statistics and graphs that we'll take a look at. Also some update on additional Mozilla Firefox news.

A paper being released in two days at the, I don't know, 84th - could it be 84th? Maybe not. Anyway, I have it in the notes, IEEE conference on something or other about yet another way of exfiltrating data from a PC. And it's annoyingly obvious. But to these guys' credit, they really wrestled this thing to the ground. I mean, so there's, like, no stone unturned in dealing with something obvious. And I'm thinking that next we want to have them research the optimal Dixie cup size for connecting two paper cups together by string. But we'll see. And also what should the tensile strength be and maybe a less elastic medium than cloth string and so forth because I'm sure they could really do that justice for setting up a simple telephone system.

Anyway, we also have bit of errata, some miscellany, closing-the-loop feedback with our listeners. And then we, as I said, will take a look at where the world stands with encrypting DNS. So I think another great podcast for our listeners.

Leo: Lots to talk about.

Steve: Our Picture of the Week pretty much sums up what you were just saying, Leo.

Leo: Yeah, it does. We've always said security's a binary issue.

Steve: That's right. We have someone giving a presentation to a group with - he's got a front-projecting screen and a little pointer, and we have the caption: "We've narrowed our security risks down to these two groups." And we have the first group: Everyone who works here. The second group: Everyone who doesn't work here.

Leo: That's it. They've narrowed it down. That's the threat. That's the threat.

Steve: So that pretty much covers the territory. So last Tuesday was Patch Tuesday. And there were your typical bunch of things. There were two zero-days which were being exploited by Russian hackers at the time, in addition to 15 critical flaws that were fixed. A total of 77 vulnerabilities which affected Windows, a range of, well, IE, DirectX, and the graphical subsystem. Of those 77 vulnerabilities, as I mentioned, 16 of those were critical, 60 were acclaimed to be important, and one was given moderate severity.

Most of the critical vulnerabilities allow the attackers to execute remote code, so those were RCEs, remote code execution vulnerabilities on the user system. And 19 of the only important vulnerabilities could be used for local privilege elevation. However, as we've seen, although sort of privilege elevation seems like less of a big deal than remote code execution, they are very valuable. And in fact these two zero-days were privilege elevation exploits that were important enough to be in active use. That one moderate problem which resolved was an authentication bypass for applications using Windows Communication Foundation and the Identity Foundation API. So of the two that were zero-days, one was an elevation of privilege, as I mentioned, in the Win32k component, a null pointer dereference. And the other was in the printer spooler, of all things.

So anyway, what was interesting was the attacker gets elevated, or they were able to get in for the purpose of elevating their privilege with any of six browser memory corruption vulnerabilities or five Chakra engine vulnerabilities. So again, the privilege of elevation sort of allowed them to gain a foothold after these basically 11 different browser vulnerabilities which Microsoft fixed allowed them to get in in the first place. So I'm sorry I sound a little bit fragmented. I got distracted by something else going on in my environment.

Anyway, if an attacker were to cause a victim to visit a malicious website, they could execute remote code in the context of the user's browser, then gain full control over the machine using either of these two zero-days. So anyway, those patches have been applied. And as I said, Adobe for whatever reason did not synchronize their updates. We saw some significant updates to Adobe that we talked about a couple weeks ago, so I guess they just weren't ready for another round.

And I mentioned that there was one thing that happened that upset some stalwart Windows 7 users who, based on the reporting, got pretty worked up and annoyed to receive a non-security update, after specifically asking Microsoft only to deliver security updates, that is, Microsoft gave them a Windows telemetry update on Windows 7 machines, even though it was labeled as a security-only monthly patch. Recall back in 2016 when Microsoft simplified its patching of Windows versions by offering Windows 7 and 8.1 users two types of updates. You could either get the monthly rollup, which is what I do because it's, you know, why not, which is both security and non-security patches. So for IE, like for bugs and for reliability. But the second option was to say I don't want any feature changes. I don't want anything other than security patches for my system. So you could ask for security-only updates and receive a minimal package.

Well, it turns out that last week, on July 9th, Patch Tuesday, there was a security-only update, KB4507456, which actually contained something called the Compatibility Appraiser tool which was slipped in. And our friend Woody Leonard, writing in his "Woody on Windows" column for Computer World, posted under the title "New Windows 7 'security only' update installs telemetry/snooping feature." And the subhead of his piece says: "Three years ago, Microsoft promised to keep Windows 7 and 8.1 updated with two tracks of patches, monthly rollups that include everything, and security-only patches that are supposed to be limited to security fixes." And he says: "Guess what happened?"

Anyway, for anyone who's interested, Woody's article has a ton of good information for people who want to know more. And he cites a security expert who tweets as @VessOnSecurity, Dr. Vess Bontchev, who tweeted: "I have officially stopped updating my Win7 machine." This guy tweets: "I no longer trust Microsoft's updating process. I'll protect it from any existing and future vulnerabilities with my other defenses as well as I can." And he signed off with: "Eff you" - and he didn't say "eff" - "Microsoft." And Woody politely left that ending out of his copying of this guy's tweet.

My feeling is that all we can be is informed; right? I mean, that's what we do on this podcast. That's why we're here. I choose to use Windows 7, which I do with my eyes wide open. The job Microsoft is doing, frankly, I think is impossible. I don't want that job. No one wants it. And given the messy legacy of Windows code, the fact that it is using a barely Windows-literate user base, I mean, I know we techies who listen to this podcast, when we're trying to help our other Windows friends, we're like, okay, do you understand what this button does? No. Just, you know, they don't want to know. And as we talk about every week, there is an incredibly and increasingly hostile environment for which Windows attempts to protect its users.

So I give Microsoft a lot of credit for doing, all things considered, I think an amazing job. And clearly whatever this compatibility appraisal tool thing was is something that they felt they needed to put into, for whatever reason, some telemetry in preparation for the fact that, as we know, Windows 7 will stop receiving any of these things in six months, in February of 2020.

So I feel like I should take a moment to talk about Windows 7 and Windows 10 and me because security updates will stop flowing to Windows 7 six months from now, in February. That is, unless Microsoft changes their mind again and pushes that deadline further back, which could still happen. We've seen them do it before. It was going to be cut off earlier, but Windows 7 was still the majority operating system, despite all their efforts to push people to Windows 10. So we know that, at the beginning of this year, only just between the snapshot in December of 2018 and January 2019, Windows 10 finally outpaced Windows 7. There were finally, based on a snapshot of installs in the world, 7 and 10 traded places.

But even today, six months later, seven months later, they're still neck and neck. Windows 10 sits at 40.61%, with Windows 7 at 38.06% of market share. So they're still near parity. Over time we're going to see Windows 7 systems disappear, but probably only because you can't buy any new hardware that runs Windows 7. Windows 7, you have to jump through real hoops to install Windows 7 on a machine that supports USB3. And all, I mean, every machine for a long time has. So it's very difficult to get Windows 7 running on contemporary hardware, and the newer chipsets don't support it at all. So as hardware dies or gets recycled or replaced just because of its age, even though Windows 7 is just fine, it's going to have to be running Windows 10. It won't have any choice.

And as our long-term Security Now! listeners know, I won't be moving my main workstations. I have two at each of my main residential locations. I won't be moving them to Windows 10, even after Windows 7 stops being supported. I do have Windows 10 laptops for testing. When I go out to present SQRL to a group, that laptop is running Windows 10. You and I, Leo, are Skyping over a Windows 10 machine. But I know from long, loving, and trouble-free experience with XP that this Windows 7 machine I'm sitting in front of with its five high-resolution screens, and everything is installed in...

Leo: Five?

Steve: Yeah, yeah. I'm looking around, I've got, like, everything is all - I love this environment. It will continue to happily purr away for many years, even without constant nursing from Microsoft. Windows Defender has never found anything on any of my machines other than false-positive annoyances from my own code that I've written that it doesn't know about that it protects me from. or old well-marked viruses in email archives. Sometimes it fires off, and I think, oh crap, it found something. And I look and say, oh, no, for some reason it went and sniffed some old directory somewhere where I have some virus repositories that I'm keeping, and they're well marked and known. And besides, I'm not even sure they infect anything like Windows 7 or 10 any longer. I mean, they're really old.

But it will stop being updated in six months, and I'll miss it. It's nice to have Defender sort of watching my back, even though it's never found anything. But I think I'll be okay. And we just talked about all of the ways bad stuff was getting in, which Microsoft just patched last week, were browser vulnerabilities in IE and Edge. And I will continue not using them in the future. So I'll stick with Firefox, and I'll probably be okay. And as I've said before, my backups have backups. And I also keep a rolling off-machine incremental file change backup of all the projects I'm working on, as well as monthly static offline deep-freeze snapshot images. So I'm well protected. On the other hand, I'm not your average user. And for what it's worth, neither are the listeners of this podcast.

Also, I love so many of the apps that I have running on Windows. I'm just like, I'm extraordinarily happy with them. There are apps that I've been moving forward through the years from machine to machine. The move away from XP and the loss of native 16-bit support was traumatic for me, but it finally had to be done because even Firefox and Chrome finally were refusing to update themselves on XP. So I thought, okay, fine. I'll do that. But I'll continue using Windows 7, and Firefox and Chrome will continue to keep me being safe.

But the one thing I want to say - because I get the sense that maybe people believe I'm suggesting this is okay for everyone, and so I'm not saying that. I know that there are listeners within our audience that feel the way I do. I mean, look, half the world is, I mean, literally half of the Windows systems even today are running Windows 7 as opposed to 10, despite all the pressure that there is and there has been to move to 10. And of course that's going to ratchet up through the rest of this year until, I imagine, there will be people who don't feel as I do that it is, for whatever reason, safe to continue using Windows 7 without this constant drip-drip-drip of fixes to things that Microsoft finds that are wrong.

So I am not suggesting that anyone else follow my example. And one of the reasons is, and I've said this before, is my use of Windows is boring compared to most others. I don't use my machine for entertainment or gaming. I don't watch YouTube videos or just follow random link trails to see what's out there on the Internet. I'm really not very interested in most of what is out there. So my main Win7 workstations are, while they're not technically air-gapped from the Internet, they are Steve-gapped because I just don't do much with them. You know, I assemble my own code and design PC circuit boards and, I mean, I use it as a workstation rather than as a toy. And so my exposure to danger is, I think, reduced from the typical Windows machine.

But anyway, I just wanted to say that here we are, six months away from end of updates for Windows 7. I think it is remarkable that Windows 7 versus 10 is at 38% versus not quite 41%. I mean, people just don't want Windows 10. So it'll be fun to track this as we move forward, and we certainly will.

And Leo? LaPorte County, Indiana. No relation.

Leo: You know there's a city of LaPorte in every state of the union.

Steve: Is that true?

Leo: Yeah. We were fur traders, and we got around. That's all I'm going to say about that.

Steve: Anyway, LaPorte County. The Michigan City News Dispatch reported last Tuesday, the 9th, their headline was "Malware attack on county computers. LaPorte County website, government email servers out of operation."

Leo: They're besmirching the family name.

Steve: Oh, my goodness. Well, and it'll be interesting to see how this goes. Paraphrasing and trimmed down from this article, the report was all LaPorte County government email and the county website remained out of commission late Tuesday - that is, last Tuesday - following a malware virus attack that affected the system on Saturday morning. The LaPorte County Board of Commissioners President, someone by the name of...

Leo: You're just doing this to irk me, aren't you.

Steve: No, no, no, no.

Leo: Just wait till Gibson Township goes down. I'm just telling you.

Steve: That's right. Dr. Vidya Kora said Saturday evening: "The system will be inoperable as authorities respond to 'a malicious malware attack that has disabled our computer and email systems.'" Then, a few days later, last Tuesday, County Attorney Shaw Friedman confirmed that county government computers were "impacted by a sophisticated ransomware virus early Saturday morning."

Leo: Must be sophisticated or we wouldn't have fallen prey.

Steve: That's right. It was a baddy. He said: "Fortunately, our IT team reacted quickly."

Leo: Unplug them. Unplug them, quick.

Steve: Although after the fact, of course, and shut down much of the system.

Leo: They did, they unplugged it.

Steve: I know. They did. They unplugged them. Even though it was a weekend. So yes, our IT team is on the job.

Leo: On the job.

Steve: Even on the weekend. He said: "Less than 7% of our laptops have been infected; however, it did hit our two domain controllers, which means no server can access network services." Whoops.

Leo: OMG.

Steve: And actually, Leo, it also got their backups.

Leo: Uh-huh.

Steve: Yeah, uh-huh. An insurance policy taken out last year, Kora said, will help the county recover. He said: "Fortunately, our county liability agent of record, John Jones, last year recommended a cybersecurity insurance policy" - I bet there's a lot of those recommendations going around right now.

Leo: Yeah. You ought to get an insurance policy.

Steve: "Which the county commissioners authorized from Travelers Insurance." He said: "We informed Travelers Insurance late Saturday" - while we were still busily unplugging machines, no, he didn't say that - "of the malware attack, and they immediately referred us to the Wayne, Pennsylvania incident-response law firm of Mullen Coughlin LLC that specializes in responses to such cyberattacks and coordinates system repairs and protection of our computers from such virus infections."

Friedman said: "The forensic investigation firm has been retained to determine the nature and scope of the incident, including how the county could have been infected." Actually, they never did find out. But, he says: "We're developing a game plan to respond to the attack..."

Leo: Oh, that's reassuring.

Steve: I know, got to have a game plan, "and come up with an approach to repair our systems and protect them from further damage." Right.

Leo: A little late for that.

Steve: After we've plugged them back in. After we plug them back in. "The county's IT department has been working long hours" - oh, we're pumping that up - "long hours to try and get things operational."

Leo: So please don't fire us. Please.

Steve: Oh, get this. Exactly. Please, please.

Leo: Please don't fire us.

Steve: We don't want to follow, what was his name, Brian somebody, Brian...

Leo: Yeah, he's gone, but he's looking for work.

Steve: Yeah, he's looking. Yeah, don't hire him.

Leo: I hope he goes to Gibson County. I just pray, I pray that he goes to Gibson County.

Steve: It says they've been working long hours to try and get things operational, including, Leo, spending Sunday...

Leo: Oh, no.

Steve: Even on Sunday. They never get to rest, those IT people - to ensure that the courts and prosecutor's office remain functional. Because we've got to prosecute somebody.

Leo: Well, yeah.

Steve: After we figure out who did this to us. So "This particular ransomware variant, known as Ryuk" - no kidding.

Leo: Oh, yeah? Oh, where have we heard that name before?

Steve: Yeah, R-Y-U-K, "is especially insidious as it seeks to delete or encrypt system backups." Whoops.

Leo: How dare they?

Steve: But Leo, he said: "We are exhausting all possibilities." We're going to be exhausted, as are our IT people.

Leo: Maybe there's a hard drive in the closet somebody forgot to connect.

Steve: He said: "We're even tapping the FBI cybersecurity unit and reviewing all workarounds" - we're going to review those workarounds - "in order to determine how to restore the county to a full operational status." So, you know, we're glad we voted for this guy because, you know, even on Sunday. So staff from this firm, the law firm Mullen Coughlin, arrived in LaPorte - at LaPorte? In LaPorte? I don't know - on Sunday night. Night, even, Leo.

Leo: Oh, traveled on a Sunday to get there.

Steve: No sleeping, to assist.

Leo: No, took a Greyhound.

Steve: They will help prepare documentation to report the attack to the FBI and other appropriate law enforcement agencies. Kora and Friedman both praised the efforts of the IT department. Kora said: "I commend our Director Darlene Hale" - while she still has her job - "and her team..."

Leo: Don't fire me, please.

Steve: "...for shutting down our systems Saturday afternoon" - she came right in - "as soon as the malware virus was detected. Unfortunately..."

Leo: It was way too late.

Steve: "...at least half our servers have been infected." Because you know that malware is quick.

Leo: Speed of light, my friend, speed of light.

Steve: That's so unfortunate, "and it will take some time to fully restore service. I ask for patience from the public as we seek to become fully operational again." They like that phrase. Friedman echoed that sentiment, saying: "Darlene Hale and her team have been working 15-hour days," Leo, 15 hours, "since this virus hit to try to restore portions" - okay, we're getting a little more modest now - "portions of our system that can be restored." Because of course you cannot restore those portions that can't be restored because they can't be restored. "We ask for patience from all concerned."

Okay. So that was the incident reporting. Then, a week later, BleepingComputer reports: "A forensic investigation firm and the FBI were involved, but attempts to recover the data encrypted by the malware without paying the ransom were fruitless. The cybercriminals got about $130,000 in Bitcoin..."

Leo: Oh, they paid them. Oh, boy.

Steve: "...from this attack, with $100,000 being covered by insurance. So the impact may not be immediate," they write, "but it does create some ripples in the long run. The decision to pay the cybercriminals came after seeing that the decryption keys from the FBI" - I guess they must have had some from previous...

Leo: Ryuk cyber is one of those malwares that sometimes can be reversed.

Steve: I don't think so. I don't think Ryuk can.

Leo: No?

Steve: No.

Leo: Somebody sent us an email saying, yeah, we do this, and sometimes you can reverse it.

Steve: Ah. Well, actually I do think there were some versions. I may be confusing it with a different one. But anyway, according to a local report from WSBT, a local station, the county had backup servers, but the malware encrypted them. So you don't want your backup servers to be on your network all the time. So we now know that insurance companies are bearing the brunt of the payouts for these attacks.

So I'll bet that we're not far from the time when the conditions of continued insurance require regular training and reviews, periodic security audits, and more reliable backup solutions. I'll bet that we're, I mean, in other words, we're going to be hearing from insurance companies, quote, something like, "We'll insure your municipality; but unless you want the insurance premiums to be really sky high, you need to get much more proactive about protecting yourself from these threats. And when you come calling for a payout, the first thing we will do is audit to figure out why none of the multiple safeguards you promised to put in place and to maintain were effective in this instance. And only if we find that you were not at fault, given the terms of this insurance, are we going to pay." So I think we're going to see something happen.

And then I got a kick out of this. Also in the news, U.S. mayors adopted a resolution not to pay any more ransoms to hackers. Whoo. They have adopted a resolution, Leo. It turns out that just happened. The 2019 Adopted Resolutions of the 87th Annual Meeting - oh, that's the 87 I was probably thinking of, not the IEEE because that'd be a long time to have IEEE meetings. But the 87th Annual Meeting of the United States Conference of Mayors, of the Committee for Criminal and Social Justice, included the resolution to "oppose payment to ransomware attack perpetrators."

And actually the proposal adopted resolutions stuff is pretty humorous, so I've put a link in the show notes. And I had to scroll down through, like, endless adopted things. Finally got down to opposing payment to ransomware attack perpetrators.

And so there are seven points. They said: "One, whereas targeted ransomware attacks on local U.S. government entities are on the rise; and, two, whereas at least 170 county, city, or state government systems have experienced a ransomware attack since 2013; and, three, whereas 22 of those attacks have occurred in 2019 alone, including the cities of Baltimore and Albany and the counties of Fisher, Texas and Genesee, Michigan; and, four, whereas ransomware attacks can cost localities millions of dollars and lead to

months of work to repair disrupted technology systems and files; and, five, whereas paying ransomware attackers encourages continued attacks on other government systems, as perpetrators financially benefit; and, six, whereas the United States Conference of Mayors has a vested interest in de-incentivizing these attacks to prevent further harm" - yeah - "seven, now therefore be it resolved that the United States Conference of Mayors stands united" - yes, united - "against paying ransoms in the event of an IT security breach." In other words, we're saying don't do it anymore.

Leo: We stand agin it.

Steve: We stand united against paying what we're going to be paying. We're not happy. So, uh-huh. Anyway.

Leo: Ransomware, I'm agin it.

Steve: That's right.

Leo: I don't like it.

Steve: So basically they're all definitely, Leo...

Leo: We are all in against it.

Steve: ...unhappy. We're really, really not happy.

Leo: Somebody's got to get these guys some help. So we got an email from a guy, and I can't vet it, so maybe, I don't know, you can or something, named Brett Callow. He works for a company, a New Zealand company called Emsisoft. His point was that Ryuk uses hard-coded keys that sometimes are reused.

Steve: Ah.

Leo: And so those are the keys probably referred to by the FBI. It was unclear. He wanted to get the word out that, you know, they offer a downloader that will check it against the keys that are known. This is the website. I don't know anything about it. They say it's free of charge. But the point being that he said, "I just want to get the word out that sometimes you can get a key to decrypt it that's been reused."

Steve: And it may work.

Leo: And it may work. And certainly should do that before you pay anybody any money.

Steve: Yeah, especially, you know, lots of bitcoin.

Leo: Oh, man, that's a lot of money. Wow. You know, how long is insurance going to be offered? I mean, it's going to either...

Steve: That's exactly right. I mean, the premiums are going to start going up. And the fact that the insurance company paid the round number $100,000 makes it sound like that was the cap on their payout for this particular county. So, in fact, the county may have decided, well, boy, you know, to get full coverage it's going to cost - the premiums are going to be too high. So we'll accept a cap of $100,000 because, you know, whatever. Anyway, believe it or not, Leo, this problem, not surprisingly, actually, has created, well, we already saw they've created a law firm that specializes now.

Leo: Isn't that interesting? Yeah.

Steve: Yes. And now we have Coveware.com, ransomware remediation. It's C-O-V-E-W-A-R-E dot com. "We are the first responders to your ransomware recovery. Coveware aggregates global ransomware data to minimize your ransomware-related costs and downtime. Let our IT security professionals manage your ransomware incident response."

They say: "How do we restore your encrypted data?" Well, "One, explore free remediation options. Identify ransomware type. Find free decryptor tools," like what you were just talking about. "Free initial assessment risk. Identify the threat actor group." Then second main point: "Threat actor negotiations. Secure and safe negotiations. Complete and transparent communications. Determine risks and outcomes."

So basically we now have an industry which is establishing itself as professional ransomware remediation and negotiation, I mean, they have experience with this. So I'm sure they have the threat actors' number and know how to contact them and say, okay, look, let's see what we can do here.

Then number three: "Ransomware settlement. 100% transparency, reimbursed costs, transparent documentation, compliance checks." I presume that means that they get paid out of what they, like, out of insurance or settlement. And then, four: "Restore data and end downtime. Professional IT support. Insurance documentation." So they're able to have their costs paid by the municipality's insurance and roll experts in who are able to apply the decryption tools and bring the systems back up. So if your local IT staff are not up to it, now there's Coveware that you can contact. Then they sign off on their web page saying: "Minimize your ransomware downtime. Let us manage your ransomware recovery." Unbelievable.

Leo: Wow. It's really a business.

Steve: It really is a business.

Leo: I want to ask this one more time. I feel like I've asked this many times. Is it not the case that you could probably prevent this with good IT? I know you might get infected; right? I mean, sometimes they'll sneak through. But if you have good cold backups, I mean, it seems to me this would be avoidable. But maybe not.

Steve: I've had a lot of feedback from our listeners while we've been talking about this. I mean, from our listeners who are on the IT front line and who say, you know, you guys need to stop saying that this is as easy as backing up all the systems. There are real logistical problems to doing that. For example, there are servers that, I mean, so I don't have those jobs. I can't definitively say. But what I'm hearing from our listeners is that there are servers that can't be taken down. There are workstations that for whatever reason can't be logged off of. The backups cannot be done on the fly. There are, like, open files that prevent themselves from being backed up.

And we know that that can happen where you just - you can't take a snapshot of a system that's in use. You have to stop it in order to snapshot it in some instances. And there are systems that can't be taken down. For what it's worth, Leo, I'm absolutely sure that it is not an impossible problem to solve. But it probably takes a lot more than is practical given the resources that these people have. And in fact this takes us perfectly into the next topic, which is this survey that Sophos commissioned from a U.K. research-based firm. After our second break we will talk about it.

Leo: Yeah, I don't mean to diminish the efforts and the difficult of this. It seems like it would be worth doing it, somehow preventing it; right?

Steve: I really do think that it's a tradeoff. You know, how much time and effort and money and staff do you commit to mitigating...

Leo: But you're looking down the barrel of a gun that's going to hit you.

Steve: I know, I know. But I'm sure the IT people are saying at every meeting, the CIO, we need more money. We need more money. And the boss says, okay, yeah, but, you know, you've got to do what you can with what you've got because we don't have any more to give you. And I'm sure they're saying, look, everything was good yesterday. Everything is good today. We're going to hope that everything's good tomorrow. And of course...

Leo: It ain't gonna be, though.

Steve: I know.

Leo: It ain't gonna be.

Steve: That's true.

Leo: You're going to be the next one. So we've not been hit by ransomware, knock on wood.

Steve: Knock on wood, I know.

Leo: You've not been hit by ransomware, knock on wood. We're in a worse - you have one person opening your email. We have 20 employees opening emails. We probably have been targeted. I would imagine we have.

Steve: Well, Leo, I live in fear. I would love to have servers statically mapped, and I'm disconnecting from them all the time because, I mean, this is the problem that we face today. And so, I mean, it is really, I mean, it is the problem is that something gets in and encrypts the data.

Leo: And also ransomware's more sophisticated than it used to be. We've got two people in the chatroom who are saying - Web108 says, "We had two ransomware attacks in 2017. We contained them. We restored. No loss of time or data." Beta4a says, "My company's been infected by cryptoware twice. We have wiped, rebuilt, and restored with a loss of a maximum of one day's work." So, but it may be the case also, ransomware, thanks to Blue, what is it, Blue Heaven? Blue, you know, and various tools that are now out there that make it easy...

Steve: Oh, BlueKeep, BlueKeep, yeah.

Leo: BlueKeep, to worm its way through your network. Maybe it's more virulent than it used to be. It feels like there's things you should do. Maybe you can't prevent it 100%. But it feels like it's well understood what you need to do.

Steve: Well, for example, as I've said, I mean, my computer could explode, and I'd be up. I have an entirely separate physical redundant machine just sitting here waiting to be commissioned.

Leo: But, yeah, you don't, you're not - you're not running an active server that's doing 100 transactions a second or anything like that, either.

Steve: No. And I said a long time ago I don't want the job of keeping Sony safe. Nobody wants that job.

Leo: I told you we had the guy who protects the cybersecurity for West Point, the military academy at West Point. And he said it's tough because "we only have to make one mistake." Right? They're attacking all the time. It only takes one mistake. Now, he's lucky because the army's Cyber Defense Command is also there, so they help out a little bit. But still, you're right. I wouldn't want that job. We're not saying you guys are dopes.

Steve: No. No, no. I mean, and I know IT people who their lives are, you know, it's like that mailman we talked about last week. He's happy. He's delivering the mail.

Leo: It's easy. Life is easy. All you have to worry about is occasional dogs, yeah. Well, and I won't talk about what we do. But we have a fairly, I mean, we have a number of barriers to the outside world. We use Gmail, which says that, you know, Google says, "We filter against known malware attacks." I don't know. I feel like - I

don't know. Watch, because tomorrow I'll be saying, Steve, we can't do the show. All our servers are encrypted. Do you know any good malware authors?

Steve: Get one of those Dixie cups with string so we can talk to each other.

Leo: Yeah.

Steve: So Sophos commissioned an independent survey of 3,100 IT managers. They used the U.K.-based research house Vanson Bourne. And this survey was conducted at the end of last year to the beginning of this year, so December 2018 to January 2019. To provide a representative size split, they chose the same number of organizations between 100 and 1,000 people, and 1,000 and 5,000 people, so an even mix of smaller and larger organizations. What they found was - none of it was really very surprising, but we have some nice numbers.

Respondents who had been victims of a cyberattack in the last year were asked how the most significant cyberattack got into their environment. The results revealed that where respondents knew how the attack got in - and they didn't always know - not surprisingly email was the number one most common attack vector, which was used in one third, 33% of the attacks. And of course we know that that's conducted with phishing, where email is sent that is designed for someone to think that it's authentic. Typically in targeted attacks somebody clicks the link. And in some cases, like somebody else's email account could get compromised, so the email is actually coming from someone you trust, but it's malicious. And the rest is what we talk about all the time.

The web is also a major vector, which was used in three out of 10 attacks, so 30%, just slightly less than email. So again, as we've often said, the browser is today's attack surface. It's why I made the comment when I talked about continuing to use Windows 7 in the future, I'll be using Firefox or Chrome - well, Firefox probably, which is being kept constantly updated - even after Windows 7 stops being updated because, well, and for that matter Thunderbird for email, both that are being constantly maintained, even if the underlying OS isn't.

IT managers, however, cannot just focus on email and the web. 23% of attacks got in via a software vulnerability of some kind, and 14% through a USB stick or external attached device. So those things, we don't really talk about those very much, but those are still happening. Back at the beginning of the podcast, Windows was infamous for running a program when you stuck a USB device onto the machine. So it was very easy back then to do drive-by attacks. Anyway, so 33% email, 30% through the web, 23% through some software vulnerability, and 14% through USB or some other device.

And in one out of five instances, no one knew. They did not know how something got in. They were unable to identify the way something happened. And, you know, in a sufficiently large organization, I can understand where something happens, and you just say, well, you know, we looked everywhere, and we were never able to determine how something happened. I mean, even "I don't know" is, you know, you'd like to know, but it's hard to know in every case.

Also what was interesting is that these cyberattacks that we're seeing, as you said, Leo, they are becoming increasingly sophisticated, which says they may not just use one thing. They may be multistage and coordinated and blended. Respondents whose organizations had been victim of a cyberattack revealed that they had suffered a range of attacks. So, for example, the second graphic that I have shows 53% phishing, 41% data

breach, 35% malicious code, 35% software exploit, 30% ransomware, and 21% credential theft.

Well, 53, 41, 35, 35, 30, 21, that adds up to way more than 100%, meaning that what they were seeing was that many of these attacks used multiple means of obtaining their goals, not just one type of vulnerability. It could be phishing email that then leveraged a software exploit. And of course we see that, for example, where phishing email leverages scripting in Word, where there's a vulnerability in Word, where if you coax the user to taking it out of protected mode, it will run the Word macro and then leverage one or two other vulnerabilities that exist somewhere. So it's a complex sort of multiprong attack because no one thing anymore is sufficient because our systems overall, the various ways that things can happen are increasing in their security; but, by combining multiple vulnerabilities, people are still able to get in.

Of the 2,109 - okay. So 3,100 organizations were surveyed. 2,109 of those were hit by a cyberattack in 2018. Over half, 53%, were victims of phishing. So that is still the most lucrative, the most high return attack across all of the survey. And there was some variation based on country on the nature of software exploits. Over a third, 35%, suffered from an exploit taking advantage of a vulnerability in software they were using. Interestingly, in Mexico, over half the organizations that fell victim to a cyberattack experienced a software exploit which was double the number of those in Brazil, at 22, and South Africa and Japan, both at 23. So there is, for whatever reason, there was like a statistically significant difference by country.

And the survey asked the question, as I mentioned, about technology, talent, and time, and concluded that they were in short supply. In this report they said: "As we've seen, organizations face a wide range of attacks and need to secure multiple threat vectors." They revealed that, on average, IT teams spend 26%, so just 1% over a quarter, 26% of their time managing cybersecurity. So think about that: 26% of the IT team time is cybersecurity related. And they concluded that, for the majority of respondents, this is not the correct ratio, meaning that it should be higher.

And then again, there was some variation by country. Organizations in India spent the most time, at 32%, and Japanese teams the least at 19%. Organizations that have been hit by a cyberattack, I guess not surprisingly, spent a little more time now on IT security, 28%, over those who had never experienced an attack, yet were still spending substantial time, 23%. So maybe that accounts for the fact that they had not yet been hit.

And the report said: "Given the variety and complexity of threats, it's not surprising that 86% of respondents said they need greater cybersecurity skills within their organization. Those organizations that had experienced an attack have even greater need for cybersecurity experience than those that hadn't, 89% versus 79%." But still, even those who had not been hit, 79% of those organizations said we need to be doing more than we are able to.

Anyway, so they said that bringing the expertise to fill these gaps is a major challenge. Eight in 10 organizations say they struggle to recruit the right skills. So they're struggling to find people who have the skill set. They said when it comes to recruitment, India faces the greatest challenge at 89% of the organizations saying they cannot find people who have the skills they need, and Germany the least. But still, two out of three German IT managers, so 66%, say they struggle to bring in the right skills.

So anyway, I just thought that was interesting, to get some sense for the fact that, I mean, given all the stuff that we cover and the way we cover it, this fits everything that we believe in terms of the major threats that we're seeing, the way these threats get in, and how difficult it is in practice to counteract them. And the fact that IT organizations, it

may just be that there's a bit of a brain drain, too. I know that a lot of our listeners sometimes ask, you know, are there jobs in security? I think it's very clear that somebody who focuses on security can increasingly find work there in the future.

And we're seeing that fines are beginning to happen, where mistakes are starting to cost organizations more than just reputation damage. And I'm of two minds about fines. We really do want major organizations to act responsibly with the personal and abusable data that they collect about us through their normal course of justifiable business operations. But we also want and need them to self-report when, despite their best efforts, they fail to live up to their and our hopes for their ability to keep our data safe. And given that responsible self-reporting is inherently voluntary, unless a breach is discovered externally, which is much less common than internal discovery, levying burdensome and abusive fines on those organizations may not actually improve end-user security and privacy.

Which, you know, the reason I'm talking about this is that, as I mentioned at the top of the show, the U.K.'s Information Commissioner's Office, the ICO, has announced that it intends to impose a hefty fine. It's 99,200,396 euros - or, no, I'm sorry, pounds, which is in this case $123,705,870. Nearly $124 million fine on Marriott, the hotel chain, over last year's data breach.

As we know and reported at the time, last November 2018, Marriott self-reported that hackers had had access to the Starwood guess reservation database over a period of four years, since 2014. Starwood was a different chain of hotels which Marriott had acquired in 2016. So the breach occurred two years before Marriott acquired it. Marriott initially reported that hackers had stolen the details of, and it was a rough estimate, half a billion, so a big breach, 500 million hotel guests, which they subsequently reduced to 383 million after a more thorough investigation.

And remember that there are also passports involved. There were 383 million guest records, 18.5 million encrypted passport numbers, 5.25 million unencrypted passport numbers, 9.1 million encrypted payment card numbers, and 385,000 card numbers that were still valid at the time of the breach and had not been encrypted.

So unfortunately in this day and age, class-action lawsuits began piling up within hours of Marriott's announced security breach. And I suppose not surprisingly now, with the GDPR, the U.K.'s Information Commissioner's Office, which is in charge of such things, has stated that Marriott's security practices are in violation of the EU's GDPR. And it'll be interesting to follow this to see whether that's actually the case. I have no opinion one way or the other. We don't, without much more information. The good news is that Marriott has stated that they are going to oppose this fine. They filed a note with the U.S. Securities Exchange Commission that they're going to formally oppose it.

Marriott International's President and CEO, Arne Sorenson, said: "We are disappointed with this notice of intent from the ICO, which we will contest. We deeply regret this incident happened. We take the privacy and security of guest information very seriously and continue to work hard to meet the standard of excellence that our guests expect from Marriott." And he did say that Marriott had retired, and we mentioned it at the time, the Starwood guest reservation system earlier this year. So it's no longer in use.

So I don't know how - I guess I don't know how to feel about the EU stomping on Marriott for a violation of GDPR which occurred over a period of time, involved an organization that they didn't own at the time, that they're now slapping them with a big fine over. And again, we want organizations to responsibly disclose breaches, rather than to fix them quietly and not acknowledge that there was a leak that could affect their customers. Yet having the GDPR used in this way really seems to put cold water on that. So it'll be interesting to see.

Oh, the day before that also, by the way, the ICO in the U.K. also announced plans to hit British Airways with a $230 million fine after they failed, British Airways failed to protect their website, which was infected with a web-based card skimmer which was collecting payment card details from British Airways customers for, let's see, April, May, and June, for three months back in 2018.

Leo: Oh, I didn't know there was such a thing as a web-based card skimmer. That's awesome.

Steve: Yeah. It was infected JavaScript which got in there and was capturing all of their credit card information while they were putting it in. So I don't know. It seems...

Leo: You feel like they're being scapegoated because they're big names?

Steve: Yeah. And they've got deep pockets.

Leo: I liked OutofSync's idea. Instead of fining them and collecting it and lining your coffers, make them spend that money on security. Say, like, good, now you're going to spend $99 million to make your system more secure, and we want to see the receipts.

Steve: Yes. I think that makes a lot of sense.

Leo: I think that would be better.

Steve: Yeah.

Leo: I guess if they're not sitting up and paying attention to the hacks, maybe the fine would get companies to pay attention. But it doesn't feel like that.

Steve: No. And this Information Commissioner Elizabeth Denham in the U.K., she said: "The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess, not only what personal data has been acquired, but also how it is protected. Personal data," she says, "has a real value; so organizations have a legal duty to ensure its security, just like they do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."

So I guess, I hope, that they can't simply levy a fine. I hope that, for example in this case, Marriott says, no, prove that we were negligent. Then there will have to be an investigation that the ICO has to undertake in order to demonstrate Marriott's negligence post-acquisition. Because she's saying that they have an obligation, even for organizations that they acquire. So you imagine Marriott did something. I mean, we talked about it at the time, that there was some looking at what it is that they're getting. They missed it, clearly. But everyone makes mistakes. Anyway, it'll be interesting to see how this plays out. But I agree, Leo, just telling them we're going to force you to spend

this money to make yourself stronger. It's like, well, okay. We didn't want to spend it that way, but it's better than you guys having it. As you said, Leo, lining the coffers. That doesn't seem right.

And speaking of fines, although in this case it's a different nature because it was a policy decision that they're being hit with, remember a few months ago when we talked about Mark Zuckerberg addressing his shareholders and stating that they had "set aside," I think those were his words, some billions with a "b" of dollars for an expected Federal Trade Commission fine in a settlement in the infamous Cambridge Analytica-tied privacy violations. Well, the Wall Street Journal just reported that FTC commissioners have voted and approved a $5 billion settlement with Facebook. So there's a slap. And certainly in this case no one would argue that these guys - this wasn't a mistake. This was Facebook selling their information. So they're paying the price.

Mozilla, actually it was you mentioned it while I was talking about the ISPA because it was just happening as we were recording the podcast, you mentioned last week that the ISPA had reversed their position on Mozilla.

Leo: Yeah.

Steve: Paul Ducklin, who is a writer for Sophos "Naked Security," he followed up his earlier column about that nutty ISPA nomination of Mozilla as Internet Villain of the Year with a column titled: "Mozilla aren't villains after all." And in his piece he nicely summarized, which is why I'm quoting it, why unprotected DNS over UDP is a problem in the first place.

He wrote: "If I unlawfully sniff your DNS traffic so I know where you went, I'm violating your privacy. Merely by knowing where you surfed, without getting any details of what you actually surfed, I can infer an awful lot about you. I can probably piece together your daily routine, both at work and at home; figure out your likes and fears; learn which companies you do business with, which bank you use, the shops you frequent, the clubs you belong to, the hobbies you enjoy, the medical surgery you're registered with, the sports teams you support, and much more."

So anyway, I liked that brief summary. As we all know, there are many other means for blocking access to unwanted sites. I just sort of wanted to follow up on this before, and we'll be talking about encrypting DNS in a minute. But what we know is that the U.K. is unhappy with Mozilla for making it so easy, is the only way I can read this, making it so easy to blind their ISPs to the DNS queries that Mozilla's customers are making.

And so I thought I'd just say for a minute, since DNS to IP mapping sometimes changes, an ISP's content blocking device, rather than doing a match on DNS queries, could periodically make the same DNS queries their customers make, retrieve the DNS lookup IP, and dynamically manage an IP filter blocking list in order to keep those connections from being completed after the user's browser tries to make them. Or redirect them to a "prohibited content" page or whatever. Or some concerned organization could perform the lookups and communicate IP address additions and removals to concerned ISPs. Or ISPs could subscribe to a published block list in the same way as spam has been thwarted since way back in 1997 with RBLs, real-time blacklists of the IPs of known spammers.

So my point is there are a great many ways to solve this problem that are just as robust as filtering on DNS. And certainly those organizations being filtered, that is, the ones that are being blocked, know, already know that by changing their domain names, they can sidestep the filtering until it again catches up with them. So, you know, yeah. Enhancing

the privacy of all web browsing users by encrypting DNS at the expense of asking ISPs to change the details of the way they selectively block access so that some domains which haven't yet changed their names to avoid the blocking get blocked, to me makes a great deal of sense. And I'm glad the ISPA came to their senses on this.

And speaking of Mozilla, recall that we previously covered that shady organization who chose to name themselves DarkMatter, which was petitioning Mozilla to include their root CA certificate in Firefox's Trusted Certs store.

Leo: What could possibly go wrong?

Steve: What could possibly go wrong? At the time, cybersecurity experts and privacy advocates were strongly cautioning and urging Mozilla against doing so, stating that DarkMatter could abuse its position - yeah - to help its surveillance operations. Remember, it is a manufacturer of those middleboxes, which are used to intercept HTTPS connections. And right now, if its middlebox certificate is not trusted, then users would get a warning and/or have to trust its certificate. But if they are able to get into the root store, then their middleboxes could be issued certificates which would raise no alarm, which we don't want.

Some of these operations, that is, of DarkMatter, these surveillance operations, have been previously reported. So it's not just it could happen. This is what DarkMatter has done in the past. Reports from Reuters, The New York Times, the Intercept, and other sources have detailed alleged DarkMatter-orchestrated hacking operations against human rights activists, journalists, and foreign governments, which DarkMatter carried out at the behest of the UAE, United Arab Emirate government. So these guys don't sound like anybody you want to have in your root store. I mean, Hong Kong Post Office, that's benign compared to these guys.

So get this, Leo. Just recently, in a last-ditch effort to find a way to get its certificates trusted inside Firefox, DarkMatter attempted to create a spinoff certificate authority business called DigitalTrust.

Leo: Oh, much better. I like that.

Steve: Much better. Much better. They're digital, and they're trustworthy. That's right.

Leo: Yeah.

Steve: Unfortunately, both DarkMatter and DigitalTrust were run by the same CEO. These guys seem kind of clueless. If you're going to set up, try to have a different organization, it's really not your name. We don't like your name DarkMatter, but that's not why we said no. So creating a spinoff run by the same guy called DigitalTrust, oh, yeah, trust us. No.

So taking everything into consideration, having given plenty of time for contemplation, and because they really don't want to deny anybody who should have this privilege out of hand, Mozilla has finally announced its decision last week in a Google Groups discussion. Wayne Thayer, Certificate Authority Program Manager at Mozilla, said: "Our foremost responsibility is to protect individuals who rely on Mozilla products." He said, "I believe

this framing strongly supports a decision to revoke trust in DarkMatter's existing intermediate certificates."

He says: "While there are solid arguments on both sides of this decision" - I guess the argument on the pro side is, well, maybe they aren't bad. He says: "It is reasonable to conclude that continuing to place trust in DarkMatter is a significant risk to our users." He says: "I will be opening a bug requesting the distrust of DarkMatter's subordinate CAs" - that is, the intermediate certificates - "and will also recommend denial of the pending inclusion request and any new requests from DigitalTrust."

So anyway, the distrust of the subordinate CAs that Wayne was referring to was something we also talked about before. DarkMatter had been issuing certificates, which would be trusted by Firefox, using an intermediate CA certificate which had been signed by QuoVadis, which is trusted. So those certificates, that intermediate CA, is going to be killed, as well. Once Mozilla removes the QuoVadis intermediate certificates from Firefox in a future update, all websites that use TLS certificates acquired from DarkMatter will show the standard illegal certificate warnings in Firefox, warning and blocking users from accessing their content.

So what I'm wondering now, because we don't know, I haven't seen, is what Windows and other root stores are going to do. Recall that in order to prevent problems with third-party AV, Mozilla stated that in some conditions they will be importing the Windows CA root and trusting certs signed by those roots. So the specific conditions are, if you're on Windows 8 or Windows 10 with a recent Firefox, and who isn't recent, anything since 66, and I think we're at 68 now, and you have a non-Windows Defender AV registered with the system, in those cases, Windows 8 or 10, and you're using a non-Windows Defender AV, then Firefox may be, and I think is, but I can't test it here because I don't have a non-Windows Defender AV, Firefox may be turning on the option to trust the Windows root store.

If Windows is trusting DarkMatter certs, and I don't know whether it is either way, or their previously issued QuoVadis intermediate cert, then your Firefox would, too. There is the switch, the option switch that we talked about before. Maybe you can inspect it and see if it is set, if your situation matches that, that is, you're probably using Windows 10, and if you're using a non-Windows Defender AV. Go to about:config in your address bar and put in security.enterprise. That will bring up one entry, security.enterprise_roots.enabled. I checked it, and for me, it was set to the default of "false."

But as I understand it, Firefox in those circumstances, because they don't want to be causing problems with not recognizing certs that are installed by these AVs, which are wanting to filter HTTPS TLS connections, they will be bringing the roots which are registered with Windows into the Firefox store. And that switch will be set to "true." So it'll be interesting to find out whether other roots follow Mozilla's lead and do not trust DarkMatter certs.

Oh, and one other nice forthcoming Mozilla feature, the next release of Firefox, 69, will add a tracker blocking report. When we get 69, and I'm not sure when that's scheduled, putting about:protections into the URL will bring up a graphical display showing how many and of what type of trackers Firefox has autoblocked during the previous seven days. We didn't talk about this when it happened since so much was happening that particular week. But it was last month.

Mozilla has decided, I guess, pretty clearly, to differentiate itself from the Chromium-based browsers by focusing upon privacy through proactive anti-tracking. They released the full version of their enhanced tracking protection they call ETP, in Firefox 67 last month. It added default blocking for cross-site tracking, which are, as we know, small

bits of JavaScript embedded in websites by advertisers. Those bits of code send back our location to monitor what we're doing across the web for the purposes of generating profiles.

At the same time, Firefox released an updated version of its Facebook container, which stops Facebook from tracking people in the same way. So all of those Share and Like buttons which appear ubiquitously across the web, which report back to Facebook even if they are never clicked, are now also completely blocked by the updated Firefox container, along with all the other connections to Facebook's servers that might happen. So in May, oh, and also in May Firefox began blocking cryptomining for us and also is now blocking fingerprinting.

So all of those things are now being handled by default by Firefox. And in Firefox 69 we'll get a very nice graphic. I have a picture, a snapshot from the proposed graphic in the show notes for anyone who's interested. And it breaks out all of the different types of blocking and how many of these trackers have been blocked over the course of the last seven days.

So Chrome is a great browser, and it now, as we know, has the majority of the Internet. But we also know how Google makes its money. I love their search engine. And this show notes document was created using their very slick online tools. But I am more closely aligned with Firefox's philosophy. I love having its tiny tabs down along the sidebar. And Firefox works perfectly for me. So I expect to be sticking with Firefox for the foreseeable future.

And now, Leo, in this week's installment of Wrestling a Simple Idea to the Ground, we have the paper which will be delivered this Thursday during - ah, it was the 43rd. I knew it couldn't be 87th. It was the IEEE 43rd Annual Computer Software and Applications Conference, which is COMPSAC, C-O-M-P-S-A-C, titled "CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs."

My first thought about hearing this was that it should have been named, rather than CTRL-ALT-LED, CTRL-ALT-DUH because, okay, it's obvious to all of us that, if software can blink a keyboard's LEDs, you know how keyboards have, what, Caps-Lock, Scroll-Lock, and Num-Lock LEDs. So if you can put those under software control, and you can, and you can install malicious software in a computer, and we know that happens, and you can arrange to have something watching the LEDs over time, obviously at a time when there's no one sitting there because otherwise they'll think, what the heck? What the hell? My computer's just gone berserk. My lights are blinking on my keyboard like crazy. If all of those preconditions can be set up, then, yeah, you could send data, you could exfiltrate data from the computer.

Now, to their credit - and Leo, you're scrolling this on the screen right now. I have it in the show notes. They really did solve the problem. And as I said, I want to put them on the task of figuring out what the best communications medium to use is between the bottoms of two Dixie cups which are stretched so that, when we talk, we get the most clear communication. And for that matter, since it's really not a really clear communication, maybe which language would be best used for increasing intelligibility of a Dixie cup telephone because these are the guys you want to put on that project. They really wrestled this thing to the ground.

They have looked at the nature of the radiation pattern as a function of angle from dead-on, the Lambertian radiation pattern, the transmitted power as a function of how far off of the axis you are from the LED. If you have a camera lens which is imaging multiple LEDs, to what degree are you able to differentiate between the LEDs spatially when the LED illumination falls onto the camera sensor. They have a wide range of camera types that they have experimented with. And what about if you have a non-imaging receiver?

If you have something that can only detect the illumination, but doesn't have a focusing lens, so all you can detect is a subtle change in brightness in the room, for example.

And they wrestled it all the way down to which keyboards produced the highest bit-rate, believe it or not, looking at Dell with a single LED versus multiple LED, Lenovo the same conditions, Logitech keyboards, or Silverline. And for anyone who is worried about this, the Silverline keyboards allowed them, at a relatively low bit error rate of 3.10%, they were able to very cleverly manage an exfiltration of a little more than 5 kbps. So that's, you know, that's not bad. That's way over Morse code. Anyway, for anyone who's interested or worried, I guess you could, I mean, I never really use those lights on my keyboard. You could not only stick a Post-it note over your...

Leo: One more thing to tape up.

Steve: ...webcam, exactly. And these guys are the blinking light experts. They're the people we've talked about before who worried that hard drive activity lights could be used for exfiltrating data. And remember we talked about them saying that the lights on routers could be used. And I said, "What?" You know, maybe if the data bits were exposed on the LED. But routers don't put the data bits. They, like, sort of aggregate them together and just blink the light slowly if anything is happening at all. So I don't know. They do tend to push the limit.

Leo: Ilya says: "What about the flash on your camera?" That could probably be used to...

Steve: Yeah.

Leo: On your camera phone; right?

Steve: Yeah. Wow. Anyway, so they really wrestled the problem to the ground.

Leo: These guys are the kings.

Steve: They are. So I have the note in Errata that I already mentioned was that Elaine, hearing us talk about how long we've been doing the show, corrected me, saying, no, Steve. I think maybe I said we were in year 13 or something. She said no, year 15 will begin next month, on August 20th. So we'll be right here.

Leo: You can listen to Security Now! #1 right at TWiT.tv/sn1.

Steve: That's every one from then on is available.

Leo: Yup, they're all there. And I try to keep numeric numbering, so sn1, sn2, sn3, sn4, all the way up to sn, what is it, 723.

Steve: 723. Yes, my friend. And I did want to just make a mention that Lorrie and I managed to slug our way through "Stranger Things 3." Ugh.

Leo: Oh, that's too bad.

Steve: Yeah, yeah. It was a disappointment.

Leo: It was so good, the first two. It would be hard, you know, it's hard to keep up that quality.

Steve: Yes. And the other thing that was really annoying was it seemed like such a commercial play. You know, there were clear product placements throughout the entire thing. I mean, the fact that it was held in a mall where you were seeing the various stores advertised.

Leo: A lot of those stores were '80s vintage stores that no longer exist.

Steve: Some of them, yes.

Leo: They rebuilt that whole mall. They created it, yeah.

Steve: Yeah, yeah. So anyway, a couple pieces of closing the loop. Oh, and this is relevant to our topic today. Chuck posted to GRC's Security Now! newsgroup. He said: "I enjoyed show 722 yesterday. Last night I checked the Firefox setting to 'Enable DNS over HTTPS' (DOH)."

Leo: Doh.

Steve: Doh. He said: "I chose a VPN location in Europe and started browsing." He says: "There was a dramatic improvement in speed with which websites started loading on the screen." He says: "I mean really fast." He says: "Tonight I'm going to do some unchecking and rechecking to confirm that DOH is responsible. Is DOH improving the efficiency of a VPN connection?" And then he followed up exactly 24 hours later with: "I disabled DNS over HTTPS (DOH) in Firefox last night. Web page loading performance slowed considerably." He says: "Naturally I turned it back on, and the joy of quickly loading web pages returned."

Leo: Well, that company has a slow DNS server, I guess; right?

Steve: Yes, exactly. And so it may well be that by turning the tunneling on, you are avoiding the slow DNS service you were using by default, and you got a big acceleration.

Leo: Yeah. A lot of ISPs have crap DNS servers.

Steve: Yes. It's sort of an afterthought; you know? It's not like, you know, we've got the best DNS. It's like, yeah, we had to plug one in, so it's over there in the corner. I mean, it's not very glamorous. So it is often the case that even though the ISP's DNS service is almost by definition the closest server to you in terms of the connection, it may not be the fastest one to deliver a response.

Leo: Well, that's why you wrote your DNS Benchmark.

Steve: The Benchmark, yup.

Leo: You can easily test it.

Steve: So our topic, "Encrypting DNS." There's four things we have. We have DNSSEC; DNSCrypt; technically we have DNS Curve, but that never, that's sort of been replaced by Crypt; DNS over HTTPS; and DNS over TLS. So let's talk about each of those to sort of clarify where they stand, what's going on, what they do. DNSSEC first because it's not encryption. It provides cryptographically signed DNS records, which allows DNSSEC-aware OSes to verify that the DNS response which was received, which may have been cached and forwarded from its originating authoritative DNS server, has not been tampered with or altered in any way. So it's just a signature. That's all it is. Since it's signed with a private key, which no forger can have, this essentially means that we're assured that the received DNS reply is authentic. It hasn't been tampered with. So that's all good.

But what DNSSEC does not do is encrypt. It was never intended to provide privacy, only authenticity. So the records are signed; and as I said, they cannot be tampered with. But anyone watching the traffic will still see the DNS client's queries and their replies just as if DNSSEC was not in use because all it does is it adds a signature record to the existing DNS reply, which allows a DNSSEC-aware client to check the signature. Oh. But before I go on, I'll note that all three of the full encryption options, that is, the other three things - DNSCrypt, DNS over HTTPS, and DNS over TLS - all three of those are now compatible with DNSSEC. The earliest versions of DNSCrypt were not compatible with DNSSEC, which is what you remembered from our original coverage of this, Leo, back in the old days.

But an update to DNSCrypt allowed essentially a full encapsulation of DNS so it became DNSSEC-compatible. So that while that's not been true all the time, it is true now. So DNSSEC can be used with all of the three encryption solutions. So we first discussed DNSCrypt back in the context of OpenDNS, which was subsequently purchased by Cisco. DNSCrypt uses the same fast, lean, and secure crypto that I chose to use with SQRL. That's Dan Bernstein's Elliptic Curve 25519. It successfully provides encryption for privacy, but it is not nearly as attack and hack resistant as we would wish a contemporary protocol to be, since it does not use any of the existing public certificate infrastructure. The server's public key is published over DNS, and it's implicitly trusted, though it can be verified with DNSSEC.

So when DNSCrypt added DNSSEC, then it does allow for privacy and protection, and you can verify the server's public key in order to provide protection. But what it really means is that DNSCrypt was simple and lightweight. It was the progenitor of these later full tunneling protocols. It could ride atop either UDP or TCP, which was a benefit. Unlike the connection-oriented protocols, it required much lighter server resources. So it was very easy to implement, did not require a full TLS stack and the security troubles that we have, as we know, that implementing full TLS can bring with it. But it never made it to

the IETF standards, does not have an RFC, and was never taken up by the IETF for standardization.

So it's there. There are providers for it. It was a pioneer in encrypting DNS. But my sense is that it sort of wasn't the right solution. There is a tool known as DNSCrypt-Proxy which is written by Frank Denis. He wrote it in GoLang. It supports both DNSCrypt and DNS over HTTPS. And we're going to be referring to that in a minute because it ends up being probably the right solution. It provides client services for Linux, BSD, Windows, macOS, Android, and others. And there are a whole bunch of binary distributions ready to run. I've got the link to it, the GitHub link, in the show notes. Again, it's DNSCrypt-Proxy, so I'm sure if you just google "dnscrypt-proxy" you'll be able to find it. And there is, if you are a Windows user, there is a simple configuration tool for it called Simple DNSCrypt, which provides a very nice-looking front end.

Okay. So the second to the last is DNS over TLS. And as we know, HTTPS runs over TLS, which runs on top of TCP. So DNS over TLS is, as it sounds, a protocol for encrypting and wrapping DNS queries and their replies in a TLS tunnel. So that means that we get both privacy via TLS's encryption and authentication via TLS's support for the entire public key infrastructure, all the root certs and certificates and all. So this prevents eavesdropping, thanks to encryption, and any manipulation of DNS via man-in-the-middle attacks which, as we know, simple DNS over UDP is extremely prone to.

Cloudflare, IBM's Quad9, Google. There's a company, Quadrant Information Security, and CleanBrowsing are providing public DNS resolver services via DNS over TLS. So it's broadly available from some big, well-connected services - Cloudflare, Quad9, and Google. Back in April of 2018, Google announced that Android Pie would include support for DNS over TLS, and it does. I'll get to that in a second. There's DNSDist from PowerDNS also announced support for DNS over TLS in its latest version. Users of the older BIND DNS server can get DNS over TLS by proxying it through stunnel. So that is to say, it's just DNS running through a TLS tunnel. That's all it is. And the newer unbound DNS server, which is in the various BSDs now, it has supported DNS over TLS natively since early last year.

So that's definitely something to consider. DNS over TLS is a nice option, especially if your client platform, like Android Pie, supports it natively. There's a link in the show notes here to a Cloudflare post about doing exactly that. They say first, in Android Pie and probably subsequent, go to Settings. Under Network and Security, Advanced; and you'll find under Advanced, Private DNS. Select the Private DNS provider hostname option. Enter one.one.one.one or 1dot1dot1dot1.cloudflare-dns.com and hit Save. Then visit 1.1.1.1/help to verify DNS over TLS is enabled. And it's just that simple. So my goodness. If you're an Android user, why would you not turn this on and immediately have all of your Android smartphone or other Android device DNS tunneled through DNS over TLS to Cloudflare?

Oh, and last week I misspoke about the pfSense firewall support. I said it was DNS over HTTPS. That's what we were talking about last week. It wasn't. It's DNS over TLS. But again, there's plenty of support for it. And it essentially provides all of the same services as DNS over HTTPS, as long as you have a provider on the other end, and there are plenty of providers.

And so finally this brings us to DNS over HTTPS. It is a proposed IETF standard, as I mentioned last week, specified under RFC 8484. It uses HTTP/2 or HTTPS, and supports the on-the-wire format of DNS responses. So exactly as are returned by existing UDP responses, meaning that you just take exactly what a standard DNS server would send back in a UDP packet, you stick that - you reply over HTTPS the same thing. That means that it is extremely simple to bring up on a web server, to allow a web server to host

DNS over its existing protocols. It defines a new HTTPS payload type with a MIME type of application/dns-message.

So you know how MIME types typically are like plain/text or application/something, Excel or Word or something, this is application/dns-message to identify it as DNS content. When HTTP/2 is used, because of the features of HTTP/2, the server can even push DNS answers that haven't been queried yet because remember that HTTP allows you to do send ahead. So it's able to push values that it anticipates the client may find useful in advance.

So it feels to me like either DNS over TLS or DNS over HTTPS, depending upon your platform, is the one you want to use. And the client I mentioned before, even though it still has the name DNSCrypt, DNSCrypt supports DoH, DNS over HTTPS. So for users, like for Windows, well, actually it's widely supported - Linux, BSD, Windows, Mac, Android, and more. You can install DNSCrypt-Proxy, which you can get a binary from, making it easy, you don't have to build it yourself, from GitHub. You install that and configure it on your OS, and you will get - because it also not only supports DNSCrypt but full DNS over HTTPS.

And there are plenty of all of those other providers, all of the big DNS providers also support, like Cloudflare and Quad9 and Google, support DNS over HTTPS. And if you are a Windows user, you can use SimpleDNSCrypt.org, https://simplednscrypt.org, a front end, very nice configuration front end for the DNSCrypt-Proxy on Windows. And so what that essentially means, and the reason I wanted to discuss this, is that not only with a Firefox browser can you now flip a switch and have your Firefox DNS protected from snooping. But it is entirely practical to install DNSCrypt on any OS platform, configure it to use the big DNS provider of your choice, and you go dark to anyone, your ISP or anybody else who may be sniffing your traffic. And it sure looks like you suffer nothing in terms of performance loss.

Leo: So, well, not anybody else, but anybody else in between you and the DNS server at that point.

Steve: Correct. Exactly. All of your queries are emerging and are known to, for example, Google. Or Goog.

Leo: Right, the Goog. The Goog knows all.

Steve: The Goog. The Goog knows all. Especially if you choose them as your DNS over HTTPS endpoint.

Leo: Right, right. Well, yeah, then there's Verizon. You could choose them. They're known for their privacy policies.

Steve: Ah, yes.

Leo: I would use - Quad9, we still don't know. Who is running Quad9?

Steve: IBM.

Leo: Oh, it's IBM. Well, I trust them.

Steve: They offered it as the service. Yeah, I do, too. They have...

Leo: Cloudflare is good. Quad1, yeah.

Steve: Yup, yup, for sure.

Leo: Yeah. And you know, I was just again talking to Ilya, who's been a font of information in here. Google's Pixel phones come with a similar, like 1.1.1.1 built into the phone, so you can turn that on to make DNS queries.

Steve: Nice.

Leo: But it goes back to Quad8. It goes back to Google. It's basically Quad8.

Steve: Right.

ILYA: But you can change it.

Leo: You can change it? Oh, I'll have to look in the settings. You can change it to something else, if you want Quad1 instead.

Steve: Away from the Goog.

Leo: The Goog. The Goog knows way too much. Why give them more? That's my philosophy. Steve, great episode. I'm going to run home and watch the mall episode of "Stranger Things."

Steve: Please don't.

Leo: You said one aisle you can see one brand of cereal. You could see it all clearly. And across the aisle everything's blurred out.

Steve: Yes, yes. I mean, it was obnoxious.

Leo: That's pretty bad, yeah.

Steve: And it was all cereal, all by one manufacturer.

Leo: Well, Netflix is running low on money. You've got to help them out a little bit here.

Steve: Yeah.

Leo: Yeah. We do this show every Tuesday. We try to get in here about 1:30 Pacific. We're usually pretty good. But if we're a little late, well, you'll understand. That's 4:30 Eastern time, 20:30 UTC Tuesdays. You can watch it live at TWiT.tv/live, or listen. We've got live audio and video streams there. If you're doing that, chat with us at irc.twit.tv. Always a good bunch of people in the chatroom during Security Now!, smart people.

Also, often, really great people in the studio audience. It was nice to have Ilya here. If you want to be in our studio audience - he's waving at you, Steve - all you have to do is email tickets@twit.tv. Steve's waving back. And we'll be glad to put a chair out for you. This is a pretty small studio. So any of the shows like Windows Weekly, Security Now!, The Tech Guy show that I do in here, it's a very good idea to email ahead because sometimes it can fill up, and we don't really have an overflow studio for you. The big studio, well, we can always get one more person in there.

If you want to get versions of this show after the fact, there are several places you can go. Start with Steve's site, GRC.com. In fact, while you're there, pick up - you've got transcripts. You've got audio. And you can also pick up a copy of SpinRite, the world's best hard drive recovery and maintenance utility, and Steve's bread and butter. That's the best way to support Steve. And by the way, you get some value out of that, some real value out of that. SQRL's there, too, a lot of other great stuff: GRC.com. Steve is @SGgrc on Twitter. You can DM him there. He's open to DMs, if you have a suggestion or a question you'd like him to answer. You can also go to GRC.com/feedback for the feedback form.

We have audio and video at our site, TWiT.tv/sn. And of course, as always, you can subscribe. Probably the best way to do it. Find your favorite podcast application. Search for Security Now! - 15 years, we should be in there by now - and subscribe. That way you'll get it every time it's available, the minute it's available. Stay on the line, Steve, because we've got to do some future planning. But thanks for being here, and I'll see you next time.

Steve: Yes, good.

Leo: On Security Now!.

Steve: Perfect.