Dragonblood

Description: This week we discuss a malicious use of the URL tracking "ping" attribute, more on WinRAR, more third-party AV troubles with Microsoft and other new trouble from last week's Patch Tuesday, good things that Patch Tuesday accomplished for Microsoft and for Adobe, another security-tightening change being proposed by Google, Russia's Roskomnadzor finally lowering the boom on Facebook, and the incredible TajMahal APT framework. We touch on a bit of miscellany, answer a SpinRite upgrade question, and share some closing-the-loop feedback from our listeners. We close with a look at Dragonblood, the first effective attack on the new WPA3 protocol (which didn't take long).

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-710.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-710-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. I'm back. We're going to talk about the best version of Windows, one you probably can't get a hold of. We'll also talk about URL ping tracking, a little backtracking from Steve. And then the continuation of the WinRAR nightmare. It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 710, recorded Tuesday, April 16th, 2019: Dragonblood.

It's time for Security Now!, ladies and gentlemen. I give you Steve Gibson, our man of the hour.

Steve Gibson: Welcome back from the sunny equatorial Hawaii; yes?

Leo: Oh, man. I just - it's so nice there, 80 degrees every day. If it rained, it would rain for a few minutes torrentially, and then the sun would come out.

Steve: A little humid for me. I've never been a big fan of humidity. I need evaporative cooling in order to survive, and there's a lack of that down on the Equator.

Leo: I embrace it. Remember, you're wearing shorts and Hawaiian shirts. You're not fully dressed at any given time.

Steve: Okay. That's true.

Leo: So did anything happen while I was gone?

Steve: Oh, my goodness. In fact, one of our stories, it was the topic of last week's podcast, was URL ping tracking. Because it turns out that there's an attribute in the good old <a href>, HTML <a href>, which are the hyperlink click on it that explicitly pings one or more servers when you click on the link. And it was brought to the forefront because the next two versions of Chrome will be removing the ability to disable it. Now, it really doesn't matter because it's enabled by default, and so nobody - I love the term the "tyranny of the default" because, as we know, default is what everyone runs on unless something cataclysmic happens or they're listening to this podcast. But so that was the topic last week.

And so our first topic is the - it turns out I was a little short in my imagination because I said that the only purpose it could possibly have was for tracking. Well, it turns out we have a malicious use of ping tracking in URLs has appeared. We've got more on WinRAR that just is the vulnerability that just keeps on giving. More third-party AV troubles last week with Patch Tuesday with third-party AV and of course Microsoft Windows. We've got other new trouble from last week's Patch Tuesday. We also have good things that Patch Tuesday accomplished, both with Microsoft and also with Adobe, who did a Patch Tuesday.

We've got another security tightening change being proposed by Google. We've got Russia's Roskomnadzor finally lowering the boom, Leo, on Facebook; and the incredible TajMahal APT [Advanced Persistent Threat] framework that Kaspersky has uncovered. We'll then touch on a bit of miscellany, answer a SpinRite upgrade question, share some closing-the-loop feedback from our listeners, and then we take a look at this week's topic, which is Dragonblood. That was the name given to the first effective suite of attacks on the forthcoming WPA3 protocol, which we've looked at briefly.

And our listeners may remember that when I heard about it I was all excited, and I went over to the Wi-Fi Alliance, and it looked like they had changed their stripes, and they were making the specs available. And so I was going to roll up my sleeves and have some fun spec reading. And when I clicked on the links it was like the table of contents was all you got, which was like the worst kind of tease because it's like, ooh, here's all the things we're not going to tell you about the WPA3 protocol because you have to be a member and pay dues and then be in the cloistered community. And of course at the time I commented on what a mistake it was, and what a mistake they continue making by attempting to develop a specification that is as crucial to the health of everything, of the world's networking, as our WiFi protocol, which they insist on keeping closed.

And in fact what's interesting is that these academic researchers - who, by the way, were the people that designed or found the K-R-A-C-K, the KRACK breach in WPA2, so they know their way around WiFi - they comment several times in their 16-page research paper about how this could have all been avoided across the board if this WPA3 development had been done in the open as it should have been, rather than behind closed doors.

So anyway, I think another great podcast for our listeners as we - it's funny because Elaine also corrected me. I misspoke a couple weeks ago I guess about where we were in the history of the podcast. She said, "Steve, just to correct, in four months you'll be ending year 14."

Leo: Yes, yes.

Steve: So I think I keep forgetting that I'm as old as I am.

Leo: This is - we just had the 14th anniversary of TWiT was I think this past weekend, April 15th, so yesterday. And of course I neglected to say a word because I don't really pay attention to that kind of stuff. Been doing it a long time, you and me, Mr. G.

Steve: Indeed.

Leo: But we shall do it for several hundred more.

Steve: Yes.

Leo: Two hundred and eighty-nine, to be precise.

Steve: That ought to do it.

Leo: And then everything will be patched.

Steve: By then, yes, we will have solved the world's security problems, and it'll just be like, okay, did anything happen, Leo? No. Okay. Thanks.

Leo: I did the math at one point. I think it's September 2024. We're here at least, Steve has promised, at least through then. If we can convince him to move to hexadecimal numbering, maybe even longer.

Steve: So I had two pictures this week because I had mentioned to our listeners maybe a month ago, some time ago, that I'd run across - maybe it was listening to Paul and Mary Jo - a comment that the Windows 10 Long Term Service Channel does not come with all of the preloaded crap that you get with the normal consumer Windows 10.

Leo: But not even the consumer, the business Windows 10.

Steve: Well, the professional, Windows 10 Professional.

Leo: Yeah, Pro, yeah.

Steve: And so the first picture here - so what I did was, because I have access as an MSDN developer, for which I pay Microsoft hundreds of dollars a year to have access to all the versions of everything for software testing, I thought, okay, I've got to give this

Long Term Service Channel deal a try. So I took an empty laptop, brand new SSD. And first I installed a clean install of Windows 10 Professional.

Leo: Not even Home. This is the Pro version.

Steve: This is the Pro. I mean, and I put "professional" in quotes in my title because I've never, I mean, this is what I've been complaining about. If they had named it Windows 10 Arcade version, then I would have no problem with it.

Leo: I know, I don't get this, either, yeah.

Steve: You know? We've got sausages and hamburgers, and we've got some guy pruning some hedges with his clippers, and we've got...

Leo: Because the pros love solitaire. Everyone knows. They've got to play Candy Crush.

Steve: Over in the menu we've got two different Candy Crushes. We've got Candy Crush Friends and Candy Crush Saga.

Leo: Yeah, and Cooking Fever.

Steve: It's un-effing-believable.

Leo: I have a PowerShell script I run first thing, before I even open that menu, to delete all that crap. It's terrible, I agree. It's ridiculous.

Steve: It's just unbelievable. And so then I thought, okay. I mean, here I am. Why do I have a screenshot? I hit Print Screen twice.

Leo: And then wipe the drive.

Steve: Then I used 3D Print, which was whatever that is installed automatically. But I pasted the screen and saved it off to an attached drive, wiped the hard drive, and then I used an ISO of LTSC, the Windows 10 Long Term Service Channel. That is the second picture in this week's show notes. And it's just, I mean, it should be called "Ohhh." I mean, it's for...

Leo: Now, how do you get this besides MSDN?

Steve: Or it ought to be called NCSC.

Leo: What's that?

Steve: The No Crap Service Channel. I mean, look at it. It's empty. And look at the menu. Okay, so there's a "D" for Dell because I was doing this on a Dell laptop. There's nothing else. I mean, just under "W" are the various Windows things.

Leo: This is nice. This is clean. This is the way you want it.

Steve: There's no Cortana. That doesn't even have Edge. There's no media crap. I used the "N" version, which is the European version, because of course they're more upset with Microsoft about installing things that they feel is too strong. So, I mean, it's just - there never was anything there. So it is the case that consumers cannot get this. This is an enterprise build, so this is available to enterprises. And the point is that it doesn't do this constant feature updating, although it is constantly rereleased with the updated set of features. And each release has a 10-year commitment from Microsoft for being kept up to date from a security standpoint. So the best thing Microsoft could do would be to give regular people the option to have this. There's no reason, I mean...

Leo: They did for a while do the Windows 10 Signature Edition. And they tried to talk OEMs...

Steve: Do you think Netflix is paying them to...

Leo: Yes. Of course it is.

Steve: I mean, I'm looking at Netflix here on the screen.

Leo: These people aren't there for free. They're all paying for it. And the OEM adds more; right? That's when the OEM puts McAfee or Symantec on there and all that other crap.

Steve: Well, and then you have all these tease-y versions of stuff. You have these stubs where it's like, the first time you click on something it's like, oh, you're interested in this? Hold on a second. We'll download that for you.

Leo: Yeah, because they're not really installed. They're just a picture, yeah, yeah.

Steve: Exactly. And in fact, if you open the Start Menu the instant it boots, what comes up are a whole bunch of blank tiles with download arrows because even the ISO cannot hold all of this crap ware. It won't fit on one disk anymore.

Leo: I have to admit, this looks good. I want this. This is the menu. The only thing I note is there doesn't seem to be a browser. How are you supposed to put Chrome on there, or Firefox?

Steve: Yeah, that's a good question. I guess you'd have to, you know...

Leo: Your network IT guy.

Steve: Yeah, get the network install version and then stick it on a thumb drive in order to bring it over. But, I mean, it's just a breath of fresh air.

Leo: I know.

Steve: It's just like, okay. Although I'm still really happy with 7, I am LTSC man here on out. I mean, I'll pay my MSDN dues in order to have access to this thing because it is just like, oh, look at it. It's just wonderful.

Leo: So, I mean, I can duplicate pretty much this, but I have to run a bunch of scripts, and I have a bunch of tools. And I do notice that, if you delete those big tiles in the Start Menu, your Start Menu slims down. It doesn't stay open that wide.

Steve: Correct.

Leo: It looks like this. So you can get it close to this. But it would be nice to have a version.

Steve: Yes. And until now that's what I've been doing. I first of all go through, I mean...

Leo: You decrapify, yeah.

Steve: Yes. I also run a couple PowerShell scripts to remove all of that junk.

Leo: Right.

Steve: And then you go through and just delete, delete, delete. It takes like, you know, an hour or two in order to prune a system to where it's like, okay, this is what I wish I had been given. But, oh. Anyway, I just wanted to plant this idea somewhere that, you know, there are a bunch of people who would like to own, who would like to have this LTSC. And I guess the problem is no one's buying Windows 10 anymore.

Leo: Yeah, they give it away.

Steve: It comes preinstalled on anything that you get. And so because no one has to pay for it because of all the jumping tiles that you have to tolerate. Yeah.

Leo: Yeah. I know what you mean.

Steve: Okay.

Leo: I just got my ThinkPad Extreme, which I love, my X1 Extreme. Amazing laptop. Love it. But of course the first thing you have to do is decrapify it. And then I got your great TeraByte software Image for Windows.

Steve: Nice.

Leo: And I love that and immediately image it. Fortunately, Microsoft does put a recovery image on the hard drive anyway. So it takes that, makes a recovery USB key, makes it very easy. And now I can get back to the - I basically built my own LTSC.

Steve: Yeah.

Leo: Because you pay, it's like 800 bucks a year for MSDN.

Steve: Yes, that's what it is, yes. I mean, so it's not nothing. But it does, well, for me it pays for itself because I have access to whatever I need when I'm testing software on various platforms.

Leo: Yeah, yeah.

Steve: Okay. So I need to start right out, as I said before, acknowledging a failure of my imagination. Our listeners will recall that last week's podcast, as I mentioned at the top, was URL Ping Tracking, where I described the HTML5 feature of the "ping" term which can be added into the <a href=> anchor tag in order to cause the browser to asynchronously send a ping POST to anywhere. And I commented at the time that - oh, and Leo, you did miss some fun stuff because I looked at the source of a Google search page from Chrome, you know, right-click and then view source. And the URLs were clean because in every one of the URLs was a ping reference in order for Google to track which link I clicked.

And I acknowledge that there are reasons why Google would need to know what we clicked on, other than for just tracking us and profiling us and building up a profile of us for their advertising business. And that is it helps their search results if they present a bunch of URLs, and they see what people tend to choose from a page that a human has never looked at before. Now a human is looking at it. So there's some value there.

If you bring up the same page under, for example, Firefox, what you see is that the URLs do not point to where the link is taking you, but they all of course point back to Google, and in the URL tail is the actual destination. So when you click on the link, you go back to Google. Google registers that, sees where you're actually wanting to go, and then redirects your browser there.

So the point is that, without this ping tracking, we're using URL redirection in order to achieve the same thing. And I got some feedback from my listeners who were disappointed last week in my kind of resignation to the fact of tracking. It's like I said,

you know, well, the browsers are going to end up giving up on this. We are going to have de facto ping tracking because it's now in the HTML5 spec. Chrome is removing it from even the ability to disable it. I did learn that uBlock Origin automatically blocks it, so there's another little benefit of using uBlock Origin. I mean, it comes for free. It just blocks the ping tracking.

Anyway, so back to my failure of imagination. It turns out that the sole purpose of the ping term is not only tracking. It has been used as an effective DDoS attack. It turns out that it allows JavaScript to edit the ping term and to then programmatically click the URL to launch these ping queries at any other website. One of the things that I noted last week is that there is no same-origin protection for this ping. That is, you can ping anywhere, not just the origin from which the page came. And I talked about how at first blush that's like, wait a minute, you know, is that good? Except that I'm sure that people who are working on the spec noted that, well, the URL could go anywhere, so URL redirection has no same-origin restrictions, so why should ping tracking?

Well, one of the consequences of no same-origin enforcement for the ping that has already been done in the wild is that these pings can be aimed at a site that you wish to attack, and JavaScript is able to trigger the URL, which then triggers an offsite ping. What happened was that Imperva Research uncovered a DDoS attack utilizing these HTML pings to perform a distributed denial of service attack on various gaming websites. In one attack which they monitored, which peaked at 7,500 requests per second, a total of 70 million requests were generated from approximately 4,000 IP addresses over the course of four hours, which substantially loaded, basically buried the targeted server under relatively expensive requests.

I mean, they are short queries. But in terms of an HTML request, that's more than, you know, 7,500 per second is more than most sites are equipped to handle. As we know, Safari and Opera, we covered this last week, offer no provision for disabling this behavior. It's enabled by default in Chrome, and Google is planning to, I think we're on 73 now with Chrome; 74 and 75 have removed the option to disable it.

It is still disabled by default under Firefox and Brave. Firefox offers you the option to enable it. Brave doesn't even offer you the option to enable it. So good on them. But it does look like, as a consequence of this kind of abuse, that our browser designers are going to need to come up with some way to preserve this functionality, which they've pretty much all capitulated to.

I also mentioned last week that this ping term, it was familiar to me when I saw that Chrome was removing it, which is what put it back on our radar for last week. It's been around for a decade. But it's sort of like no one was in a hurry to do it because it was just pure and simple tracking. I mean, that's what it was for was for "link auditing" is where it's euphemistically described in some places.

So I think what they're going to need to do is to come up with some way to prevent its abuse. Maybe prevent script from modifying it in the DOM. I don't know what they'll do. Or maybe reconsider not putting a same-origin policy limit on it, as so many other things in our browsers currently have. And we often talk about the same-origin limitation being hugely responsible for security. If you could only ping back to the site which had issued the page, then you could make it that site's responsibility to ping other people if it chose to do so.

And just for the record, Leo, because this is, I mean, the coolness of this is that - and I'm sure it's part of the reason that Google likes it is that it is an asynchronous query. That is, if you use the old-style URL redirection approach, then when you click on a link you go back to the site that issued the page first. And then it redirects you to your target. If you use the ping approach, the browser does both at once. The URL you're clicking on is your

target. So you go directly to that page while, in the background, the browser launches a separate thread which follows the ping reference in the URL to notify the site.

Leo: Yeah, you wouldn't want it to hang things up while it did all that. That would be - yeah.

Steve: Right, right, right. And so if you were to impose a same-origin policy, then you could still get the speed increase of asynchronous operation. But the site that was pinged back to could, if it chose, issue its own pings to other third parties, rather than having it done by the user's browser. So it's actually a little cleaner, too. It'd be nice to see that maybe people will say, oh, whoops, we need to just impose a same-origin policy. I mean, it probably takes half a line of code to do that because all of the logic is already in our browsers for taking care of this.

WinRAR.

Leo: Oh, boy.

Steve: I know. We've been talking about it every single week since it happened. Sophos's Naked Security, the title of their report from yesterday said: "An Ancient WinRAR vulnerability made public in February is now well on its way to becoming one of the most widely and rapidly exploited security flaws of recent times." That's what's happened. And the reason is, as we've discussed before, there are so many copies of this out in the world now, half a billion copies. And there wasn't an upgrade mechanism. And again, I'm not faulting the WinRAR guys. I don't know if it was last week or the week before, Leo, but I did get email from them. I think it may have been last week, so you wouldn't have heard this. But because I'm a registered user and have supported them also because it has been my favorite tool, although I did hear Paul say that he likes 7-Zip now as...

Leo: Yeah, I've been using 7-Zip, too. I haven't used WinRAR in a long time.

Steve: Yeah. Anyway, a lot of people have it, and that's why it's being exploited so widely. So their coverage from yesterday was titled "Flood of exploits targeting ancient WinRAR flaw continues." The latest evidence is a report from Microsoft's Office 365 Threat Research team which identified it as being used by the MuddyWater - there's a name for you, the MuddyWater Advanced Persistent Threat Group, yeah, muddies the water - to target organizations in the satellite and communications industry. And it turns out, as we've said, WinRAR was far too tempting for cybercriminals to ignore, and within days stirred up a hornet's nest of exploits to the tune of 100 exploits or more.

So Microsoft's blog about recent targeted attacks serves as yet another warning to organizations or individuals. If anybody listening to this still hasn't done it, I don't know why, but maybe you missed a few podcasts like, you know, since February. If you haven't updated or removed WinRAR yet, you really do need to do that. We need word to get around as much as possible since, as we've noted previously, unregistered users, or users who no longer maintain their registered email accounts, that is, you may have registered it 10 years ago, and then with an email account you no longer have, so the WinRAR guys who did send out a notification to all the email that they had, you may not have received it because that was so long ago.

So I'm glad that Microsoft has done this because, again, the more attention this gets, the more people will have the opportunity to fix this. Otherwise it's just going to sit there and be a means for bad stuff to get into people's systems. Microsoft detected the threat to their Office 365 early last month, in March. The APT attackers used a Word attachment, claiming to be from the Ministry of Foreign Affairs of the Islamic Republic of Afghanistan.

Leo: Oh, boy.

Steve: So I'm not sure who they're targeting. If I were to receive that email, it's like, I don't think so. But opening it triggers a download from a OneDrive link, which has since been shut down, which downloads an archive containing a second Word file, within which is embedded a macro which initiates the payload in the form of a PowerShell script which opens a command backdoor, allowing the attackers to deliver the malicious ACE file which contains the exploit. That is known as a chain because there are so many steps in it, or so many links in the chain, so many steps involved. So it's a bit convoluted because the attackers need to induce the user via a bogus warning dialog. Apparently they're in a hurry to get the system restarted. So they show a warning dialog, insisting that the user needs to restart their PC. And as we know, the ACE exploit causes something to be put in the user's Startup folder so it doesn't actually get invoked until they do restart their PC.

So as has been noted in the coverage of this, while the entire exploit chain will not succeed every time, it's a numbers game targeting multiple individuals inside a specific organization, thanks to the nature of "This is the Ministry of Foreign Affairs of the Islamic Republic of Afghanistan." So, yeah, not aimed at everybody. Sophos said no one should assume that, just because the attacks detected so far had been connected to nation-state actors, that this will always be the case. Commercial exploits won't be far behind. And they said WinRAR's half a billion reported users is a lot of victims to aim at. So just, again, another reminder.

So it turns out that there were a bunch of problems caused by last Tuesday's patch update, Patch Tuesday update. It resulted in relatively widespread problems for users of a number of major third-party AV systems. As we noted before we began recording, I think we were talking about this, Leo, the widespread problems were predominantly caused, although there were some Windows 10, there were problems under Windows 7, 8.1, Windows Server 2012, and Server 2012 R2, which were causing these systems to freeze, be unable to boot, or to hang on installing updates. And it also appears that some Win10 users were also affected.

According to support articles from Microsoft, Avast, Avira, and Sophos, there is a conflict between some of the recent updates and AV software including Sophos's Endpoint Protection, Arcabit, AVG Business Edition, Avira antivirus, and Avast for Business and CloudCare. In the case of Sophos, in their support article they state that the updates could cause Windows to fail to boot. Reports from users also indicate that the update process may hang at the configuring updates stage. Everybody involved is aware of the problems. And at least in the case of Sophos, Microsoft has written: "To prevent further issues, Microsoft has placed a block on the conflicting updates so that they are not offered to users running Sophos Endpoint until a solution is made available."

I have details in the show notes. But basically it's all of the updates from April 9th, both the security-only update and the monthly rollup affecting Windows 8.1, Windows 7 SP1, Windows Server 2012, in every case both the security-only update and the monthly rollup containing that same update. Avast has looked at the same things, and they've identified the updates which are causing problems, and they are not the same ones that are causing problems for Sophos. So they had actually several different ones. Avira has looked at the problems, and they found that they were having problems both under

Windows 10 in their case and under Windows 7. They suggest uninstalling these Windows updates for now.

And then Sophos needed to provide some support for their customers that were getting stuck when Windows fails to start, freezes, or gets stuck at configuring updates. Their recommendation is to boot into safe mode, disable Sophos antivirus service from safe mode, reboot into normal mode, uninstall the respective Windows Knowledge Base updates, reenable the Sophos antivirus service, and then of course reboot in order to bring everything back together. And they said, if enabled, tamper protection will need to be disabled to reenable the service. So a lot for end users to deal with.

On the other hand, I guess this is what comes with the territory if you want to use a third-party AV now because we have been talking about now an increasing number of problems that third-party AV is having with newer versions of Windows. Also Gnter Born of Borncity reported, based on the version of Windows 10 that you had, that there were various updates for 1709, 1803, 1809, and 1903 which were causing problems. So he enumerated those. I have these in the show notes, for anyone who's interested. BleepingComputer, paraphrasing from their report, they said users are reporting that, after installing this week's Microsoft April 2019 Patch Tuesday updates, that Windows has suddenly become slow, and programs are taking "forever," in quotes, to open.

And I think this was Lawrence who wrote that: "We have received emails and seen reports from users who have stated that this week's updates are also causing Windows to become very slow. The reports have been from users running Windows 10 and Windows 7. The issues that users are experiencing include Windows taking a long time to start or reboot, unable to start programs, a lag in games, excessive disk activity, video streaming issues, and other similar problems."

He said: "For example, in a comment at BleepingComputer a reader has stated that their Windows 10 computer has become extremely slow and that rebooting/starting Windows takes forever. Users on Reddit," and he had six references, "and elsewhere," two references, "are also complaining that Windows has become very slow since installing last week's updates."

He wrote: "Normally, when a user has an antivirus program, Windows Defender will disable its real-time protection." He said: "It seems that, for this user at least, Windows Defender is being enabled automatically, even though the user had Avira installed on the machine. Having two antivirus programs performing real-time protection," he wrote, "could definitely cause slowdowns and other issues." He says: "At this time there's nothing from Microsoft that states they're aware of the reported issues. The only reference to Windows being slow since the updates is from a support article posted yesterday by Avira" - is it Avira? Avira? Anyway - "that is simply titled, 'Why does my system run very slow?' This article states that, if Windows 10 has become slow, you should remove the 509 update. For Windows 7 users, they state you should remove the 472 and the 448 updates for Windows 7."

He says: "As these instructions are for users of their software, it may not apply to everyone." BleepingComputer has reached out to Microsoft, but has not heard back. Two hours after they published that, they updated their article to note that Computer World's Woody Leonard also reported he is seeing users having slowdown issues on Windows 10 after installing these updates. And then two hours after that, they updated again, saying that BleepingComputer has been told by a source familiar with the matter that these issues are being caused by conflicts between the recent updates and AV software. In other words, it's not just complete freezing and failure to reboot or hanging, but it may be that the system finally does get going, but then is operating very slowly.

So it really sounds like, you know, if we step back from this, Microsoft made some changes that caused AV software to no longer interact properly with Windows, not just older ones, but even with Windows 10. So this needs to get sorted out. And just a heads-up if any of our users have encountered this. In the show notes I pretty much captured everything with which updates can be uninstalled in order to get systems running again.

Leo: His point is probably it'd behoove people just to stop using third-party AV; right?

Steve: Well, our listeners know that that's how you and I feel. We have talked about Windows Defender, the fact that, looking at it, it is now doing an at par version, I mean, an at par level of protection. When we most recently looked at it, I think I recall that it was finding everything that others were. It had a slightly higher false positive detection rate. But I've never had it do a false positive. Although actually...

Leo: No, I don't think that's an issue at all. I've never even seen a virus warning ever. Ever.

Steve: Actually, was it last week or the week before, I deobfuscated a URL to something which was in the show notes. And I got reports from our listeners that Windows Defender was calling the show notes, like flagging them as dangerous. So someone is watching.

Leo: That's funny.

Steve: Windows Defender is watching. And yeah, Leo, I mean, I just, I mean, I understand people develop an affection for the AV that they're using. They have come to rely on it. They have a subscription. They've paid for a year of it. But the fact is we saw this before with third-party firewalls where, to do their job, they had to sink their hooks deep into the OS, into the kernel, and it was causing problems. Then, famously, with XP, they had a firewall, but it was disabled by default. But it was there. And then finally with SP2 they enabled it by default. And now third-party firewalls are kind of like, okay, you know, Windows comes with one. Well, Windows comes with a free good AV. And we are now seeing, I mean, I'm not a conspiracy guy; but boy, you know, suddenly there seems to be all of this trouble with third-party AVs.

Leo: Oh, you think Windows ain't done till the AV won't run? Is that it? Aha. I think it's, I mean, in fairness to Microsoft, I think it's more likely that these AVs hook so deep into the OS.

Steve: They do, yes.

Leo: They hook into the kernel. I mean, that's the problem, really.

Steve: Yup.

Leo: Although you've got to wonder, they're not small companies. They're well-known names. And there are hundreds of millions of Avira users and other users. Microsoft knows that. You'd think they'd test with that.

Steve: Well, yes. And Microsoft is, as we know, is releasing these rollups ahead of time. I've already got next month's rollup sitting there. I'm not touching it, lord knows.

Leo: Right, right.

Steve: But, you know, they have the preview...

Leo: Are you on the insider ring? Is that why?

Steve: No, you always get that, you know, under optional updates is the preview of the next month rollup. And so since those are causing problems, you would think that the AV guys are like trying them and saying, whoa, Microsoft, agh. Or working to fix their problem preemptively before Microsoft is able to roll these things out officially. I mean, you have to be way on the inside to know. But boy, for what it's worth, you know, I've got AV. It's scanning all of my stuff all the time, and it's called Windows Defender. And it's not causing Windows any trouble. So, and I know you're in the same position.

Leo: That's so, yeah, yeah. Why should I install those patches, Steve, given what you've told me? Why? Give me 74 good reasons.

Steve: Certainly covering what a disaster, well, especially two out of 74. Last Tuesday's patch did fix some very important things. It repaired 74 security flaws, including two actively exploited Windows zero-days. So our listeners may remember that makes it the second month in a row that a pair of actively exploited zero-days were patched by Patch Tuesday. The two zero-days specifically are very similar. Both are elevation of privilege vulnerabilities impacting the Win32k.dll, which actually should seem familiar or sound familiar because that's what it was also last month, which is of course one of the core components of the Windows OS kernel. Those two problems were discovered and responsibly reported separately by two different security teams, the Alibaba Cloud Intelligence Security Team and Kaspersky Lab, who have been very busy. We'll be hearing more about Kaspersky in a bit.

And Microsoft describes the two zero-days identically in their coverage. They said, and it's a little bone chilling: "An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode," which is even worse.

"An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log onto the system," and as we know, or be under the user's login. They said: "An attacker would then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory." So yay for that.

We have no further details about the exploitation of the vulnerabilities, which is good because we know that it takes people some time to get these things patched, and this would be something bad guys would love to jump on. So, but we do know that they were found in the field being exploited. So thus they are zero-day vulnerabilities. And Kaspersky has reported to Microsoft six Win32k elevation of privilege zero-days in the past six months, all of which they found being exploited by a nation-state-affiliated hacking group.

So we could safely assume that the one Kaspersky found this time is probably number seven in that particular hit parade. And what this suggests is that somebody somewhere has a bunch of potent zero-days which are being found by, in this case Kaspersky, by observing their use in the wild. So who knows how many more exist that have not yet been found. Aside from the Windows zero-days, not surprisingly among the remaining 72 flaws which were fixed, there were three Office Access Connectivity bugs that can allow attackers to execute code on vulnerable systems, all which can be exploited remotely.

Another code execution bug impacts the Windows GDI+ component when parsing EMF files. And that's a worrisome vulnerability since it can be exploited merely by convincing users to visit a website or by emailing users a malicious file because anything that can cause the EMF image to be displayed can potentially invoke this flaw in GDI+. So those are bad, and those are fixed. So yes, despite all the problems with last week's Patch Tuesday - whoops. Sorry about that.

Leo: What does that mean? I've never heard that one. Was that Pebbles?

Steve: That's my "you've got mail," which is a sound file that I got from CompuServe, of all things.

Leo: Oh, man.

Steve: So, yes, I have been around for a while.

Leo: But Steve. By now you surely don't have to note - I turn off mail notifications first thing I do. You've got mail? That's like a big deal? Don't you get mail every three seconds?

Steve: No. No, I only - I get no spam, just like Dvorak.

Leo: You're so smart. You've so smart. If I had announcements every time I got mail, I'd never get anything done.

Steve: Actually, I just turned off Indiegogo email this morning because I got so tired of them just - they've just gone promotion crazy. And I thought, okay, you know...

Leo: I have a folder just for that crap.

Steve: No more. No more.

Leo: Yeah.

Steve: Okay. So anyway, definitely install the Patch Tuesday updates. They're going to fix some things you're going to want fixed. But beware, if you are also using third-party AV, that you may, I mean, the good news is, before Windows does this every month they do a, what is it, a checkpoint, a System Restore point.

Leo: Right.

Steve: And so you can certainly back out and then go, whoops, I think I'll wait awhile until my AV and these most recent updates make peace with each other. And in the meantime, in the interim, just be a little more careful than maybe you would otherwise be.

And not to be left behind, Adobe also released 40 patches last Tuesday. It was a large security update for them, covering their Bridge CC, Adobe Experience Manager Forms, InDesign, Adobe XD, Dreamweaver - get this - Shockwave Player and Adobe Flash Player, and also Acrobat and Acrobat Reader. The vulnerabilities fixed include some which can lead to arbitrary code execution, sensitive information disclosure, and remote code execution in the context of the current user. When I read that Adobe's Shockwave Player was suffering from a total of seven serious security flaws, all critical memory corruption issues, exploitable for the purpose of executing arbitrary code, I thought, Shockwave? You've got to be kidding me.

Leo: Oh, it's around.

Steve: Oh, Leo. We're no longer allowed to use Windows 95, Windows 98, NT, 2000, or XP. But someone somewhere is still using Shockwave? That just doesn't seem right. So actually it turns out, when I dug in a little bit deeper, turns out I spoke too soon, since these were the last updates that Shockwave will ever receive. So Adobe wrote: "Effective April 9, 2019" - which was last Tuesday - "Adobe Shockwave will be discontinued, and the Shockwave Player for Windows will no longer be available for download."

Leo: Oh, my god. Hallelujah.

Steve: I know. But come on.

Leo: I can't believe you still could.

Steve: Last week? Yeah, exactly. They said: "Companies with existing Enterprise licenses..."

Leo: That's the problem, right there.

Steve: "...for Adobe Shockwave continue to receive support until the end of their current contract." So no more contract renewals. So enterprises, I mean, lord knows, I mean, if you're still using Shockwave, you probably are not within reach of this podcast, unfortunately. But, you know, it just had seven remote code execution, arbitrary code execution vulnerabilities fixed last week, which suggests there are probably more because Shockwave, how old is it? Come on.

So anyway, if somehow, I mean, it is way time to switch to HTML5. Anything Shockwave could do, you can do now with JavaScript and HTML5. So hire a programmer; you know? Maybe Rasmus Vind, who did the great work for me with SQRL and the SQRL forums. Maybe you can get him to fix your website or your corporate whatever it is if you need Shockwave because, boy, you really shouldn't.

Also Adobe's Flash Player had an out-of-bounds read and a use-after-free flaw fixed, either of which could result in data leaks or the execution of arbitrary code. Acrobat and Reader also received a substantial update last Tuesday with a total of 21 security issues resolved, 10 leading to information disclosure and 11 other bugs that could be exploited to execute arbitrary code. Which is to say, evil PDFs could be formed which, when viewed with Reader, would execute code on your system. So you absolutely want to update your Acrobat and Reader.

And be careful about, I mean, mostly you want to be careful about what you click on in email that you receive or in sketchy websites that you visit. I mean, the overall best advice is just exercise caution. And it's difficult to always do because sometimes we get excited about something that we're being offered. But really, be careful.

Google, you know, I continue to be impressed with - some things they do don't impress me. Famously we know that their CRL set approach to dealing with certificate revocation is so badly broken that it's not even worth doing. But they do, I mean, they're responsible for many of the improvements that we're seeing on the web. And for that I thank them and salute them. And of course we talked about the changes that they're making to Android in order to improve its security.

In this case Emily Stark with the Chrome branch of Google posted to the World Wide Web Consortium list an item titled "Blocking high-risk non-secure downloads." She wrote: "Hi, webappsec friends." So web application security friends. She said: "Over in Chrome land, we've been considering how to drive down non-secure downloads, particularly high-risk ones like executables." She wrote: "I wanted to see if other browsers would be interested in joining us on this adventure. We want to achieve the right balance between compatibility/user-disruption and security improvements." Of course that's always the challenge is tighten things down, restrict things that have traditionally worked, thus making them not work when they're deemed to be unsafe, yet not cause too much disruption.

She said: "So we will likely start by treating certain high-risk downloads initiated from secure contexts as active mixed content and block them. We're still finalizing our metrics before we can share them publicly, but right now it's looking like it will be feasible to block a set of high-risk file types, meaning executables and archives, as determined by the Content-Type header or sniffed mime-type. We will likely focus on protecting desktop users because Android and Safe Browsing already provide protection against malicious APKs."

She said: "We're not planning to focus on non-secure downloads initiated from non-secure contexts at the moment, because users at least see the 'Not Secure' omnibox badge on those pages." She says: "Feedback welcome. Thanks, Emily." Then in a follow-up reply to someone else's query about which types Google was considering, she wrote:

"We're looking at EXEs, DMGs, and CRXes as executables; and zip, gzip, rar, tar, bzip, et cetera as archives."

In response to a query from ZDNet, a Mozilla spokesperson said: "We are interested in exploring these ideas further in conversation with Google and other interested parties. The general idea aligns with the steps we have previously taken to protect users from insecurely delivered content." Okay. So what she said there is key. She said initiated from secure contexts as active mixed content and block them.

So the idea is that, right now, browsers make a distinction between active and passive mixed content. First of all, "mixed" means from content which is fetched without HTTPS security, so HTTP, from a page which was delivered over HTTPS. So, for example, passive content are things like, for example, an image. Browsers will typically still allow you to fetch an image over HTTP, although some of them complain in very subtle ways; but they don't, like, show it as a broken link and refuse to load it. However, active stuff like, for example, JavaScript will not be tolerated. You cannot load JavaScript from an HTTP URL which exists in an HTTPS content because that's active mixed context.

So what they're considering doing is that moving user-initiated - and that's the other distinction, clicking on something. For example, you can certainly click on an HTTP URL on an HTTPS page. Meaning a user action to switch contexts from HTTPS to HTTP is always permitted. That you can do. But what they're talking about now doing is, if that HTTP link were to download an EXE or a Mac DMG or any of a bunch of archives from an HTTP URL, Chrome is proposing saying, uh, no. Now, maybe it's bypassable. They would bring up an interstitial and say, "Hold on, you're asking to download something from a non-secure source. Are you sure you want to proceed?" Or maybe they're just going to decide to be more heavy-handed and decide there is no case for still allowing that to be done. That seems a little extreme to me.

But it does look like Firefox is interested in following. And what we're seeing overall is a continuous set of incremental moves, moving the entire web over to HTTPS. Of course we have the Let's Encrypt effort, which for the lowest quality of certificate has at least automated those so that you no longer have the excuse of the entry barrier of needing to pay money to be secured. That we have.

So I think it'll be maybe an interstitial at first. That might help people on sites who are pulling things from HTTP. I mean, maybe just laziness. Maybe, for example, that domain already supports security, and they just didn't put an "S" on their URLs because they didn't bother to. And if they did, then it would no longer be a mixed content fetch. So we'll see how this shakes out. But again, I tip my hat to Google. I think that they're moving us in the right direction, and it's all for the best.

So Leo, I said at the top of the show that Russia's Roskomnadzor...

> **Leo:** You just like saying it, that's all.

Steve: Which I do love saying, has finally lowered the boom on Facebook. We covered this pending and growing issue previously. As we noted at the time, last December, Russian Internet watchdog Roskomnadzor send notifications to both Twitter and Facebook, asking them to provide information about the location of servers that store the personal data of its citizens. And we'll remember that Roskomnadzor, also known as the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications - certainly it's easier just to say Roskomnadzor. It's the Russian telecommunications watchdog that runs a huge blacklist of websites banned in Russia. And of course back in 2016 LinkedIn was banned.

So though the social media platforms Twitter and Facebook were given one month to reply back in December, they chose to stick to their guns and to not disclose this information. As a result, Moscow's Tagansky District Court imposed a whopping 3,000 rubles fine...

Leo: How much is that?

Steve: ...on Twitter last week and the same on Facebook today. What is 3,000 rubles in U.S. dollars?

Leo: That sounds like a lot, yeah.

Steve: Yes. Brace yourself: $47.

Leo: Oh, yikes.

Steve: Yup.

Leo: What are they going to do?

Steve: I don't know if Mark fills his tank or if he charges his battery, but less than a tankful of gas these days. That fine, turns out, was the minimum that Russian courts could impose on companies for violating Article 19.1 of the Administrative Code of the Russian Federation: Failure to provide information. The maximum amount of the fine under this article is a whopping 5,000 rubles, or $78. So they probably weren't too concerned either way.

Leo: They didn't even throw the book at them. That's what's funny.

Steve: Now, Twitter and Facebook are not off the hook, however, since Russia law does give them the ability, well, to completely ban non-complying social media companies as they banned LinkedIn back in 2016. So we'll see what happens. Of course Telegram, we covered that fiasco with all of the blocking and other problems, and AWS got blocked, causing all kinds of other sites to get blocked, and it was a mess. So we'll see how this goes. It will be interesting to see because, you know, we're again watching the evolution in so many different directions of what the Internet means to the world.

Kaspersky Lab named the massive APT framework suite TajMahal because the stolen data was transferred to the attacker's command-and-control server in an XML file named "TajMahal." They described this as a state-of-the-art, high-tech, modular-based malware toolkit that not only supports a vast number of malicious plug-ins - and it's funny because, I mean, I looked. If you click on that link on the show notes, Leo, it's SecureList.com at the beginning of the TajMahal article. They enumerate the 80 modules that are contained in this thing. And it is a little chilling to think - and the reason I wanted to share this with our listeners is just to get a sense for just the practical reality of the kind of instrumentation which exists now on the Internet.

Okay. So they describe this as a state-of-the-art, high-tech, modular-based malware toolkit that not only supports a vast number of malicious plug-ins for distinct espionage operations, but also comprises never-before-seen and obscure tricks. So they're learning things, Kaspersky is, from what they see happening out in the world. Evidence shows that the system has been in operation for at least five years, and they only discover it in the autumn of 2018, so late last year. And so that also suggests that who knows how many other similar systems are in use now, and for how long they will be, for how long they have been or will be until they're discovered, because here's one that made it for five years.

Malware samples that they examined suggest that the cyberespionage group behind this attack has been active since at least August of 2014. The system pinged Kaspersky's radar late last year when the attackers used it to spy on the computers of a diplomatic organization belonging to a Central Asian country whose nationality and location have not been disclosed. So presumably they were under some sort of Kaspersky system protection, and Kaspersky's intruder detection system said whoops, what's this?

Kaspersky wrote: "TajMahal is a previously unknown and technically sophisticated APT" - we know that's Advanced Persistent Threat - "framework discovered by Kaspersky Lab in the autumn of 2018. This full-blown spying network consists of two packages named Tokyo and Yokohama. It includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, keyloggers, screen and webcam grabbers, documents and cryptography key stealers, and even its own file indexer for the victim's machine." They wrote: "We discovered up to 80 malicious modules stored in its encrypted Virtual File System." So it installs its own file system, an encrypted virtual file system within the victim file system. And they said: "This was one of the highest numbers of plug-ins we've ever seen for an APT toolset."

They said: "Just to highlight its capabilities, TajMahal is able to steal data from a CD burned by a victim as well as from the printer queue. It can also request to steal a particular file from a previously seen USB stick; next time the USB is connected to the computer, the file will be stolen. TajMahal," they said, "has been developed and used for at least the past five years. The first known legit sample timestamp is from August 2013, and the last one is from April 2018. The first confirmed date when TajMahal samples were seen on a victim's machine is August of 2014."

And I have a picture in the show notes that shows, that sort of depicts this. The first box: Extensive modular APT framework. Initial attacks and infection methods unknown. Then the Stage 1 Tokyo package consists of three modules with backdoors, a PowerShell script, contacts the command-and-control server, and remains in the victim as backup. That then in turn loads Stage 2, which is the Yokohama package consisting of up to 80 modules, installing an encrypted file system within the target system, and containing plug-ins, libraries, configuration files, and more. It's able to hunt for documents, visual and audio files, website cookies, and Apple backup lists. It can also take info from the printer queue, burned CDs, and previously installed USB sticks. Stolen data is sent to the command-and-control in an XML file called "TajMahal," and thus the name of this thing.

So Kaspersky concluded their report saying that: "The TajMahal framework is an intriguing discovery that's of great interest, not the least for its high level of technical sophistication, which is beyond any doubt." They said: "The huge amount of plug-ins that implement a number of features is something we have never seen before in any other APT activity. For example, it has its own indexer, emergency command-and-controls, is capable of stealing specific files from external drives when they become available, and so on. The question is, why go to all that trouble for just one victim?" they ask.

They say: "A likely hypothesis is that there are other victims we haven't found yet. This theory is reinforced by the fact that we couldn't see how one of the files in the VFS

[Virtual File System] was used by the malware, opening the door to the possibility of additional versions of the malware that have yet to be detected."

So anyway, I wanted to just sort of update everybody on this is cyber warfare. This is nation-state-scale advanced persistent penetration targeted attacks. It installs itself in a system, sets up shop, and is incredibly capable. I mean, it's like having an agent of the attacker sitting there in the machine, watching it do things. It can be, once the remote attackers figure out what's going on, what this computer is doing, who it belongs to, what kind of things it's likely to see, they're able to essentially set up triggers which will be triggered when specific files and events occur causing it to spring to life, grab those things, and then send them back to the mothership.

So, I mean, again, at the beginning of this podcast back on the single-digit episodes, this would have seemed like sci-fi. It's just like, oh, really? Come on. And now it's just like, oh, yeah, we're just updating everybody on what's happening out there. Wow.

A little bit of miscellany. I wanted to just mention for Firefox users a handy add-on that I started to use for the first time yesterday. It's called Auto Tab Discard, for those of us who like to run with lots of tabs. One of the things that I've noticed is that restarting Firefox dramatically drops the amount of memory it's using because, as you go to tabs, like bring up a web page, today's web pages are becoming huge. In some cases I'll see that uBlock Origin will have blocked 50, five oh, things from some web page. And even with it in place, this page is multiple megabytes of stuff that it has loaded.

The point is when you switch away from that tab, that page remains in memory. And so as you are doing research, pursuing links, clicking things, kind of building up a list of stuff you want to get back to, which is why my tabs tend to accumulate, so does memory.

And so what I had been doing in the past was just closing Firefox and then reopening it, and Firefox would reload the tabs, but not their contents, not until I brought them to the foreground. Well, Auto Tab Discard does that for me. You can set it up, it's tunable, so it can do it for you continuously in the background. What I do is, because it also has an appearance on the toolbar, I just have it set so that, when I click its toolbar, it'll flush all the memory used for all of the noncurrent tabs. And I've just watched my memory consumption drop, for example, by 4GB, which is just shocking to me to say. But that's the case.

So I just wanted to mention Auto Tab Discard is the name. And if anybody else is a Firefox user and a heavy user of tabs where over the course of a session you visit many different pages, you may want to consider it. And it can also be set up to, like, not do this until it begins to run, your system begins to run short of memory, or some number of tabs have been left open and so forth. So all kinds of settings.

A listener of ours, Andy Weaver in Bath, U.K., with the subject of SpinRite. He said: "Really enjoy Security Now!. The subject coverage is always interesting and just the right level of technical detail for my level of tech knowledge." So I'm glad for that, Andy. He said: "Wondering about the long-awaited SpinRite update. If I buy now, will I be entitled to the promised update features when released?" And he says: "Many thanks. Live long and prosper."

And so I just wanted to mention, yes, absolutely. Not only you, but somebody who bought SpinRite 6.0 15 years ago, in 2004, will also be entitled, for free, to what I do to it moving forward through the 6 series. 6.1 will, as I've been saying, I already know how much faster it will be because I was benchmarking an early version of it before I paused, well, okay, stopped working on it in order to do SQRL. I have had people upset with me for taking this long. But when they've seen what SQRL does and how it works, they've

actually forgiven me. So maybe other people who are impatient waiting for me to get back to SpinRite will also understand why I felt that I just had to get this thing, SQRL, out to the world before I got back to SpinRite. And in return, everybody, I mean, even people who bought SpinRite a long time ago, will be getting a much enhanced product for free.

So yes, anybody who has any version of SpinRite 6 will get all of the updates at no charge. And a little beyond that, another benefit for already owning it is, as I have said recently, I'm going to make the functional pre-release versions available to anybody who has SpinRite 6. And I also think, I'm going to discuss this with my team, but we're already considering no longer offering pre-version 6 upgrades at that point because SpinRite 6 will be 15 years old, and I think that's long enough, especially when the 6.1 release and on are going to be so radically different from what SpinRite 6 had ever been before. So I'm happy to make them all available to owners of SpinRite 6. But I don't think we will continue to upgrade people from beyond 15 years ago. I think that seems more than fair.

A bit of closing the loop with our listeners. Roy in Israel says: "Another reason to use a password manager or SQRL." He says: "Hi, Steve. I've been listening to the show for a few months now. I found this out when one of our support engineers opened a bug about the ability to retrieve the password in our service login page using a simple inspect-and-replace type method within Chrome." He says: "Of course there was nothing we can do about it, but I wanted to share this anyway so people understand how dangerous is the simple password manager which is embedded within our browser." And he gives a link to MakeTechEasier.com/see-password-in-browser. He says: "Thanks for a great show. Roy."

And that actually brought to mind something I did with Lorrie a couple months ago. There was some site that she needed to know her password for, which Chrome knew. And so with her watching, I drilled into just the standard Chrome options and clicked a few times and got to my Chrome's memorized password list and brought up the password and showed it. And her eyes just, like, went wide open, the fact that all the passwords which she had had Chrome memorize for her were right there to anyone, free for the taking, anybody who was sitting in front of her computer. So she said, "What?" And I said, "Oh, yeah, it's convenient to have your browser do that for you. But if you do that, anybody who can access your computer can have all the passwords of all of your accounts."

Leo: They need your login, obviously.

Steve: Yeah.

Leo: They have to log in. They can't just...

Steve: Yeah, if they have access to your computer, then they have access to everything in your browser. Okay. So also, just a reminder to our listeners, Scott in Boston. He says: "Security Now! feedback: uBlock Origin disables ping attribute by default." Oh, and this is how I learned of it. He said: "Hi, Steve. Per your story last week on the formalization of the ping attribute in the HTML spec, it looks like uBlock Origin already blocks sending that info." He says: "It's in the Settings tab under Privacy as 'Disable hyperlink auditing.'" And he says on the tab it reads: "Checking this will prevent hyperlink auditing. Hyperlink auditing is best summarized as 'phone home' feature, or more accurately 'phone anywhere,' meant to inform one or more servers of which links you click on and when."

He says: "The explanatory link goes to a page that defines hyperlink auditing as encompassing the ping attribute as well as a DOM method called 'navigator beacon.'" So he says: "I believe both of those are blocked by uBlock Origin when 'Disable hyperlink auditing' is checked." And I think he said it was done by default. I'll have to check mine to see if it's on by default. But thank you, Scott, for the heads-up, and another nice benefit of uBlock Origin.

Richard in York, U.K. He says: "I've been listening to Security Now! for a few years and absolutely love it. More than that, it's been super useful, as well. But in 709" - meaning last week - "you have revolutionized my working on Windows." He says: "I am forever needing to type in/copy file paths for various things, and I can hardly believe that 'copy as path' has always been there, and I didn't know about it. Thank you so much for letting the world know about that. It seems like a very little thing, but it is so incredibly quick and useful." And then he says, in asterisks, "Mind blown."

And Leo, since you missed it, I never knew that when you right-click on something in Windows to get the properties list of things you can do, if you shift right-click, the right-click menu gets additional things, one of which is "copy as path," which allows you to put the entire file system path onto the clipboard for subsequent pasting somewhere else.

Leo: Very handy. That's nice, yeah.

Steve: Yeah. I explained to our listeners that I used to use, in XP, an add-on - "Send to clipboard as" it was called - and that I missed it because I hadn't yet added that to Windows 7. And it turns out it was there all along. Oh, and I also saw from some other listeners that there are additional things you get in other places when you shift right-click, like the "Send to" option under there also gets a whole bunch more things. Actually, it almost like doubles its size. You get just a gazillion folders and shortcuts that "Send to" can send things to. So additional things to explore with shift right-click. So thank you, everybody, for that. Oh, and that was the next tip I had from an anonymous sender who mentioned that the "Send to" menu is also dramatically enhanced.

So WPA3 is still suffering from being closed. And as I said at the top of the show, I just - it's so critical that something that is as mission critical as WiFi be secure. And the idea that security researchers and academics are unable to examine the protocol while it's in development is unconscionable. And these guys say as much, having just found a bunch of problems with it. So WPA3 is, as it begins to roll out, the actual devices are becoming available. And so in service the researchers are beginning to play with it, and faults are arising.

Leo: So they don't get the code from the Wi-Fi Alliance.

Steve: No.

Leo: They've got to get a device.

Steve: Yup. They got no help. Yup.

Leo: Reverse engineer it, hack it, and then tell them, "Guys, you did it wrong again."

Steve: Yup. So Mathy Vanhoef, a researcher who was at the University of Leuven, KU Leuven, two years ago, where he discovered and revealed a severe flaw in WiFi Protected Access II, which is what we're all still using today, he named that attack KRACK, K-R-A-C-K, for the Key Reinstallation Attack. So today he's now at the New York University Abu Dhabi and working with another researcher at Tel Aviv University and also KU Leuven. Their new research paper is titled "Dragonblood: A Security Analysis of WPA3's SAE Handshake." SAE stands for Simultaneous Authentication of Equals.

Anyway, we've mentioned here in our preliminary discussion of WPA3, that's all we've been able to have because I can't get my hands on a spec in order to comment on it or even describe it to our listeners. Eventually it'll leak out, despite their best efforts, because this is the Internet, and somebody will republish the PDF of the spec. So, you know, someday.

Anyway, so WPA3 Personal is the protocol which replaces WPA2's Pre-Shared Key, the PSK, with that protocol, the Simultaneous Authentication of Equals. It's intended to provide more robust password-based authentication. So that would be the protocol we would use in our homes, for example, where we would come up with a password for our WiFi and then give it to all of our devices. But instead of using the Pre-Shared Key protocol that we have today in WPA2, we'd be using this SAE, the Simultaneous Authentication of Equals protocol. But no users would even know that. They would still be having, like, oh, what's my WiFi password?

So our interface to it would look the same. That protocol, SAE, is known as Dragonfly; and it appears to contain, as these guys have found, a number - and this is what they said - of fundamental design flaws which expose users to password partitioning attacks. In their abstract - it was about a 16-page technical paper. And since I have no access to the spec, I have excerpted sort of the key pieces of this to give our listeners a sense for what they have done and what they found.

So in their abstract they said the WPA3 certification - and that word is important because it turns out it's a certification. "The WPA3 certification aims to secure WiFi networks and provide several advantages over its predecessor WPA2." And they do agree with that. They agree this is better than what we had before. Unfortunately, it could have been better still, had anybody - well, anyway, I'll stop beating that horse. "Such as protection against offline dictionary attacks and forward secrecy." Yay for that.

"Unfortunately," they write, "we show that WPA3 is affected by several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3's Simultaneous Authentication of Equals handshake, commonly known as Dragonfly, is affected by password partitioning attacks. These attacks resemble dictionary attacks and allow an adversary to recover the password by abusing timing or cache-based side-channel leaks. Our side-channel attacks target the protocol's password encoding method. For instance, our cache-based attack exploits SAE's hash-to-curve algorithm.

"The resulting attacks are efficient and low cost. Brute-forcing all eight-character lowercase passwords" - okay, listen to that. "Brute-forcing all eight-character lowercase passwords requires less than $125 in Amazon EC2 instances. In light of ongoing standardization efforts on hash-to-curve, Password-Authenticated Key Exchanges" - so-called PAKEs, that's Password Authenticated Key Exchanges - "and Dragonfly as a TLS handshake, our findings are also of more general interest." That is to say, just beyond its particular use in WPA3. They said: "Finally, we discuss how to mitigate our attacks in backwards-compatible manner and explain how minor changes to the protocol could have prevented most of our attacks."

In their introduction they said: "The Wi-Fi Alliance recently announced WPA3 as the more secure successor to WPA2. Unfortunately" - this is them writing - "it was created without public review, meaning experts could not critique any of WPA3's new features before they were released. Moreover, although the new handshake of WPA3 was designed in an open manner, its security guarantees are unclear. On one hand there is a security proof of a close variant of WPA3's handshake; but, on the other hand, another close variant of the handshake received significant criticism during its standardization. These issues raise the question whether WPA3 is secure in practice. We remark that WPA3 does not define new protocols, but instead mandates which existing protocols a device must support. This means WPA3 is not a specification, but a certification.

"Put differently, devices can now become WPA3-certified, which assures they implement certain protocols in an interoperable manner. The only novelty of the WPA3 certification is a transition mode where WPA2 and WPA3 are simultaneously supported for backward compatibility with WPA2. Although WPA3 follows recommended practice by existing standards, we believe more openness to alternate protocols could have increased its security.

"In this paper we perform a security analysis of WPA3's Simultaneous Authentication of Equals handshake. This handshake was designed to prevent dictionary attacks and constitutes the biggest improvement over WPA2. We systematically analyzed its security by reading specifications, inspecting formal proofs, and auditing open-source implementations. This analysis revealed several design and implementation flaws. For instance, when verifying the assumptions made by the formal proof of the SAE handshake, we discovered both timing and cache-based side-channel vulnerabilities in its password encoding method. We empirically confirmed all our findings against both open source and recently released proprietary implementations of WPA3." Exactly as you said, Leo. Once they had some hardware in their hands, they verified that these problems survived certification.

They said: "All combined, our work resulted in the following contributions," and there are six. They said: "We provide a self-contained and high-level description of WPA3 and its SAE handshake." So basically they have provided what unfortunately the Wi-Fi Alliance has refused to provide, as a consequence of lots of research and reverse engineering and comparing in the field implementations some early open source implementations of the spec and so forth.

They said: "We show" - second contribution - "that the anti-clogging mechanisms of SAE is unable to prevent denial-of-service attacks. In particular, by abusing the overhead of SAE's defense against already known side channels, a resource-constrained device can overload the CPU of a professional Access Point." So something like an infected IoT device could perform a denial of service that would bring down a strong CPU of a high-performance access point running WPA3.

Third contribution: "We present a dictionary attack against WPA3 when it is operating in transition mode. This is accomplished by trying to downgrade clients to WPA2. Although WPA2's four-way handshake detects the downgrade and aborts, the frames sent during the partial four-way handshake provide enough information for a dictionary attack." In other words, this transition mode which is new to WPA3 was not properly designed. They said: "We also present a downgrade attack against SAE, and discuss implementation-specific downgrade attacks when a client improperly auto-connects to a previously used WPA3-only network."

Fourth: "We empirically investigate the feasibility of timing attacks against WPA3's SAE handshake. This confirms timing attacks are possible and leak info about the password." Five: "We present a novel microarchitectural cache-based side-channel attack against the SAE handshake. This attack leaks information about the password being used. Our attack

even works against hash-to-curve algorithm implementations that include countermeasures against side-channel attacks. This type of attack against hash-to-curve algorithms is of independent interest due to current standardization efforts surrounding hash-to-curve methods."

And, finally, sixth: "We show both theoretically and empirically how the recovered timing and cache info can be used to perform an offline password partitioning attack. This enables an adversary to recover the password used by the victim."

So I had here also in the show notes the conclusions and recommendations, but most of it is a rehash in other words of what I already said. So they basically tore WPA3 apart and implemented a practical offline attack on WPA3's personal equivalent, that is, the SAE, the Simultaneous Authentication of Equals protocol, which will be used by all of us in our homes once WPA3 happens. They worked responsibly with the Wi-Fi Alliance, who then of course issued the Security Update April 2019 in a CYA fashion.

The Wi-Fi Alliance wrote: "As with any technology, the robust security research necessary to remain ahead of emerging threats will occasionally uncover new vulnerabilities. Security researchers identified vulnerabilities in a limited number of early implementations of WPA3 Personal and immediately brought their discovery to the WiFi industry." Oh, my goodness. Yeah. Because, of course, the WiFi industry, that is, these guys, didn't make any of this available to these researchers earlier. They had to wait for it to be available.

"There is no evidence," writes the Wi-Fi Alliance, "of the vulnerability being used against WiFi users maliciously" - yeah, because no one has this yet, fortunately - "and Wi-Fi Alliance has taken immediate steps to ensure users can count on WPA3 Personal to deliver even stronger security protections." They have two bullet points. "WiFi CERTIFIED" - in all caps, which is they got a trademark on it - "WPA3 Personal now includes additional testing within our global certification lab network to encourage greater adoption of recommended practices" - yeah, meaning that translation is they've gone "Whoops" and figured out that they need to fix the existing devices against these things that these guys found - "and Wi-Fi Alliance is broadly communicating details on these vulnerabilities and implementation guidance to device vendors as the industry begins to bring WPA3 Personal to market."

They write: "These issues can be resolved through a straightforward software update, a process much like the software updates WiFi users regularly perform on their mobile devices. WPA3 Personal is in the early stages of deployment, and the small number of device manufacturers that are affected have already started to deploy patches to resolve this issue." In other words, we didn't offer it to researchers early enough, so devices are already in the field which are broken and now need to be patched. So whoops, we're doing that. We're making patches available and hoping that people will patch the few devices which are already out there because, as is, they're broken and can have their passwords hacked using this technology, which is now public.

They said: "Users can refer to their device vendors' websites for more information. As always, WiFi users should ensure they have installed the latest recommended updates from device manufacturers. Security is and always will be a dynamic endeavor, and Wi-Fi Alliance will continue to maintain strong security protections for WiFi users through its Wi-Fi CERTIFIED trademark program." Thank you very much. In other words, WPA3 will be made secure despite our efforts to keep it hidden as long as possible. After it becomes deployed, it's no longer possible to hide it. So researchers will then be able to have access to what it actually turned out to be, show us where we made mistakes, and hope then that deployed WPA3 instances will someday be updated to close those problems that we created. Thank you very much. And that, Leo...

Leo: Bravo.

Steve: That, Leo, is our podcast for the week.

Leo: And once again, all is right with the world.

Steve: On that note. I did forget to mention, I should have said, at the end of that "conclusions and recommended" chunk that I removed, they mention that several simple changes could have been made - okay. I should say: "In light of our presented attacks," they wrote, "we believe that WPA3 does not meet the standards of a modern security protocol."

Leo: Oh, boy.

Steve: Whoops. "Moreover, we believe that our attacks could have been avoided if the Wi-Fi Alliance created the WPA3 specification in a more open manner. Notable is also that nearly all of our attacks are against SAE protocol encoding method, in other words, against its hash-to-group and hash-to-curve algorithm.

"Interestingly, a simple change to this algorithm would have prevented most of our attacks. In particular, the peer's MAC address can be excluded from the SAE password encoding algorithm, and instead included later on in the handshake itself. This allows the password element to be computed offline, meaning an adversary can no longer actively trigger executions of the password encoding method." Essentially what they're saying is it dramatically reduces the ability to probe an existing system for clues which they were able to use.

And they said: "Moreover, this would mean that, for a given password, the execution time of the password encoding method would always be identical, limiting the amount of information being leaked. Surprisingly, when the CFRG was reviewing a minor variant of Dragonfly, they actively discussed these types of modifications. However, to our surprise, this change was not incorporated into any of the Dragonfly variants. We also conjecture that resource-constrained devices may not implement all the side-channel countermeasures, as these may be too costly on lightweight processors. Additionally, correctly implementing our suggested backwards-compatible side-channel countermeasures is non-trivial."

Meaning in some sense the cat is out of the bag; and, if anybody was implementing WPA3 in resource-constrained implementations, it may not be practical, as the Wi-Fi Alliance said, to fix this through a software update.

Leo: Wow.

Steve: Yes. They said: "This is worrisome because security protocols are normally designed to reduce the chance of implementation vulnerabilities. Finally," they said, "we believe that a more open process would have prevented, or at least clarified, the possibility of downgrade attacks against WPA3 transition mode. Nevertheless, although WPA3 has flaws, we still consider it an improvement over WPA2."

So eventually we'll get there. And again, as I said before all this happened, this idea of developing a protocol this important to the Internet in the dark, behind closed doors, it's just wrong. And here we're seeing a perfect example of that happening as soon as WPA3 began to creep out into the world.

Leo: Do you know, when they say "resource constrained," if they mean CPU or RAM or what?

Steve: Yeah. They must mean a processing attack.

Leo: Processing power.

Steve: Yeah, processing power.

Leo: Yeah, because a lot of routers are just, you know, very low...

Steve: Oh, my god, they barely get off the ground, yes.

Leo: Yeah, yeah. On the other hand...

Steve: Well, and light bulbs.

Leo: Yeah, light bulbs.

Steve: Yeah, not even routers.

Leo: That's true, the WPA3 client needs to be updated, too; right?

Steve: Exactly.

Leo: Oh, that's a problem.

Steve: Yeah.

Leo: I don't expect a lot of processor in my light bulb.

Steve: No. I mean, the good news is they caught this fast. And so let's hope that this gets fixed. And eventually...

Leo: Yeah. I don't know how many, you know, WPA3 devices there even are so far; right?

Steve: Yeah. I'm aware of none so far.

Leo: Yeah. So maybe they can fix it.

Steve: Whew.

Leo: But this is why this process was so broken. You called it. You said this would happen.

Steve: Yup.

Leo: You can't develop in secret. You can't, especially an encryption protocol, you just can't do it in secret. That just doesn't work. They should have known from WEP, let alone WPA3.

Steve: From WEP. From WPA1. From WPA, I mean, every single one of these...

Leo: Every single one.

Steve: ...this has happened. And it has been a disaster.

Leo: Just nuts. Thank you, Wi-Fi Alliance. Well, Steve, once again we've come to the end of a fabulous episode of "Game of Thrones." We will be back next week with more Dragonblood, more fire, and another very uncomfortable seat of swords.

Steve is the man in charge here at GRC.com. That's where you'll find SpinRite, the world's best hard drive recovery and maintenance utility. Also find the show. He's got audio versions of the show and transcripts, very good transcripts by Elaine Farris. So that's a good place to go. That's all free. Everything's free except SpinRite. So buy SpinRite and then use everything else. That's kind of how it works. You can also leave him questions. He's on the Twitter at @SGgrc. And you could go to GRC.com/feedback. There's a form there. There are also great forums if you want to participate in the creation of SQRL. We're getting close.

Steve: Yup.

Leo: GRC.com. We are at TWiT.tv, and you'll find audio and video of the show at TWiT.tv/sn, or you could subscribe in your favorite podcast application. You'll get a copy of everything the minute it's available. We will do the next episode as we always do, on Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. Thanks so much to Jason Howell for filling in last week, and I'll be back for the foreseeable future.

Steve: Yay.

Leo: Yay. Thank you, Steve.

Steve: Okay, my friend. Talk to you next week for Episode 711. Bye.