The Ransomware Epidemic

Description: Rather than looking at many small bits of news, this week we take longer looks at a few larger topics. We'll examine several pieces of welcome news from the bug bounty front. We also take a look at Google's Project Zero revelation of a comprehensive multiyear campaign aimed at iOS visitors to specific websites. Then we conclude with a distressingly large array of news from the ransomware front. We figure out how to pronounce Sodinokibi (so-dee'-no-kee-bee) and ponder the future of ransomware.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-730.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-730-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Three big topics today. We're going to talk about bug bounties, all the money going out. That ties right into that zero-day that Google just revealed on iOS. We'll talk about that, too. And of course the ransomware epidemic sweeping the world. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 730, recorded Tuesday, September 3rd, 2019: The Ransomware Epidemic.

It's time for Security Now!, the show where we cover security, privacy, how things work, and a few science fiction shows along the side with Mr. Steve Gibson right here. He's the GRC.com major domo and our regular on here, our security expert. Hi, Steve.

Steve Gibson: Leo, great to be with you once again as we are continuing to plow into our 15th year with no sign of anything letting up. And in fact this week's podcast is titled "The Ransomware Epidemic" because a security firm, Armor, has been tracking what's been going on with ransomware. We of course have been talking about it more over the last few months than we ever have. And a number of things have happened that sort of bring this to the fore. We have a little bit of news from Texas that's been surprisingly quiet. Thirteen new victims last week. The emergence of a - well, okay. There's a new ransomware known by two names. I posted to my Twitter feed this morning, how do people think I should pronounce this for the podcast: S-O-D-I-N-O-K-I-B-I. And the consensus came...

Leo: Well, everybody knows it's Sodinokibi.

Steve: Well, yes. That's what we decided it was, Sodinokibi.

Leo: It's phonetic, Sodinokibi.

Steve: So it's also known as...

Leo: It's probably Japanese, though. It looks like it's Japanese, so I'll have to ask Asako.

Steve: That's what we were thinking, yes. So anyway, rather than looking at lots of small bits of news, as we sometimes do when I talk about like what we're going to do, and it just goes on and on and on, we're going to take longer looks at a few larger topics. We examine several pieces of welcome news from the bug bounty front. We'll also take a look at Google's Project Zero revelation of a comprehensive, multiyear campaign aimed at iOS visitors to specific websites.

And then probably we'll conclude, but with probably at least half of the podcast, talking about this distressingly large array of ransomware news which suggests that we're heading into a new era. I mean, we've sort of been teasing at this for the last few months while we've been looking at these municipalities that have been hit by major ransom demands that have been met, thanks to them being insured, which of course sort of changes the dynamic of all of this. So I think another great podcast for our listeners.

And a rather sobering Picture of the Week, not surprisingly, has a bunch of dots on Florida, where we've been seeing ransomware attacks of late, and Texas, where the same has been happening as a consequence of those 22 different municipalities. This is a diagram of the U.S. produced by Armor, which shows their tracking of ransomware attacks just this year, just 2019. So this is something that is really happening.

And I'll note, and we'll be getting to this later in the show, there are without question many more unreported, less public attacks. The FBI's number, which because they deal with privately reported incidents, is far higher than the number of dots that we see here. So the FBI gets called in when some private company gets attacked, along with local authorities, to see what can be done, what should we do, and so forth. But anyway, so this Picture of the Week went well with the main topic of the show.

But I want to start by talking about the Android Developers blog which was posted last Thursday entitled, by Google of course, "Expanding Bug Bounties on Google Play," which is some welcome news. After some introductory intro stuff in the blog, they explain that the Google Play Security Reward Program, that's the GPSRP, has increased its scope to now include all apps in Google Play Store with 100 million or more installs. So all of those apps. And, you know, I looked around to get some sense for how many apps there were with that count or greater, 100 million or more installs. And I wasn't, in the time that I gave myself, I wasn't able to get some sense for the shape of the curve. We know that there are a gazillion apps with small followings that are just posted and put up by smaller developers. But it'd be interesting to know, and I didn't have a chance to find it, what this means in terms of how many apps are now eligible.

But any apps, Google is announcing, with 100 million or more installs are now covered by their reward program, even if the individual app developers themselves don't have their own vulnerability disclosure or bug bounty programs. Or if they do, then Google will augment those programs in order to meet Google's declared rewards.

Google wrote: "In these scenarios, Google helps responsibly disclose identified vulnerabilities to the affected app developer." They said: "This opens the door for

security researchers to help hundreds of organizations identify and fix vulnerabilities in their apps. If the developers already have their own programs, researchers can collect rewards directly from them on top of the rewards from Google." They said: "We encourage app developers to start their own vulnerability disclosure or bug bounty program to work directly with the vulnerability researcher community."

Then they said: "Vulnerability data from this GPSRP program helps Google create automated checks that scan all apps available in Google Play for similar vulnerabilities," which is sort of clever. So the things that are manually found where researchers have the incentive to find them and report them in return for receiving a bounty, Google will look at those and go, oh, that's interesting. Obviously they hadn't found it from their own automated scanning. Thus human researchers found them.

But then Google would then enhance their automated scanning to help find those in the future and also, of course, look to the lesser highly downloaded apps, scan those in order to see if they're able to find similar vulnerabilities. So it's sort of a win-win-win-win-win.

"Affected app developers," they wrote, "are notified through the Play Console as part of the App Security Improvement program, which provides information on the vulnerability and how to fix it." They said: "Over its lifetime, ASI" - that's the App Security Improvement program - "has helped more than 300,000 developers fix more than a million apps on Google Play. In 2018 alone," they said, "the program helped over 30,000 developers fix over 75,000 apps. The downstream effect means that those 75,000 vulnerable apps are not distributed to users until the issue is fixed." So that's the automated side which benefits from what Google learns from what the human security guys find first.

Then they also said, summing it up: "To date, GPSRP has paid out over $265,000 in bounties." They said: "Recent scope and reward increases have resulted in $75,500 in rewards just across the last two months, July and August." They said: "With these changes, we anticipate even further engagement from the security research community to bolster the success of the program." Obviously, by expanding this, they're creating a much larger, I don't want to really say "target-rich environment," but from the standpoint of the security researcher who would like to see if they could support themselves by finding bugs, many more apps to go looking around in.

Then they also introduced something new, which is the Developer Data Protection Reward Program. They said: "Today we are also launching the Developer Data Protection Reward Program." Again, note the term "data protection." DDPRP is a bounty program which will be run in collaboration with HackerOne, meant to identify and mitigate data abuse issues in Android apps, OAuth projects, and Chrome extensions. So these are technically not bugs. But we've also talked often about how apps are exfiltrating data that is in breach of Google's terms and conditions. So this data protection program is aimed at finding those.

They wrote: "It recognizes the contributions of individuals who help report apps that are violating Google Play, Google API, or Google Chrome Web Store Extensions program policies." So not bugs, but policy violations. They said: "The program aims to reward anyone who can provide verifiably and unambiguous evidence of data abuse, in a similar model as Google's other vulnerability reward programs.

"In particular," they said, "the program aims to identify situations where user data is being used or sold unexpectedly, or repurposed in an illegitimate way without user consent. If data abuse is identified related to an app or Chrome extension, that app or extension will accordingly be removed from Google Play or the Google Chrome Web Store. In the case of an app developer abusing access to Gmail restricted scopes, their API access will be removed. While no reward table or maximum reward is listed at this

time," they said, "depending on impact, a single report could net as large as a $50,000 bounty."

They said: "As 2019 continues, we look forward to seeing what researchers find next." They said: "Thank you to the entire community for contributing to keeping our platforms and ecosystems safe. Happy bug hunting." So Google has expanded the scope of their bug bounty program, not only, as I said, by adding more apps to qualify for bounties, and by encouraging app developers who are able to, to create their own bounty programs, or maybe team up with HackerOne, and also by expanding the range of what qualifies to include not only bugs, but also the abuse of information disclosure.

So as we know, Google has deep pockets, and it's nice to see them using some of that to further strengthen the Play Store. You know, we know that apps are still misbehaving, despite all of the efforts that those who curate their stores, Google in the case of the Play Store and Apple in the case of the App Store there, but stuff still gets through. So it requires just more eyeballs looking at this.

And speaking of the bug bounty industry, we covered back in March the first millionaire, a 19-year-old white hat hacker, Santiago Lopez, who has as his Twitter handle @try_to_hack, was the first to pass the target of $1 million in earnings from HackerOne. He earned himself more than a million dollars by identifying vulnerabilities in the software or systems belonging to Twitter, HackerOne themselves, Automattic, Verizon, a number of private companies who were participating in HackerOne's bug bounty program, and the U.S. government, among others.

Now HackerOne has announced that Santiago is no longer alone. Five additional hackers have joined Santiago to become bug bounty millionaires by finding and reporting security vulnerabilities through HackerOne's vulnerability coordination and bug bounty program. And these new members of this small group are all over the place: Mark Litchfield from the U.K., Nathan Wakelam in Australia, Frans Rosen in Sweden, Ron Chan in Hong Kong, and Tommy DeVoss from the U.S. So now there are six millionaires who have made themselves such by finding and reporting, responsibility disclosing bugs to HackerOne.

And I should also note my thanks to HackerOne for their very kind shout-out about me, as it turns out, in their most recent blog post last Friday, which they titled "HackerOne Praised by an Original Hacker," yours truly. That was cool. They were referring to this podcast 10 weeks ago, number 720, which we titled "The Bug Bounty Business." And as our listeners well know, I consider bug hunting for profit to be an emerging 100% legitimate and very intriguing career. And I've sort of been saying to our listeners, hey, you know, if you'd like to maybe make some extra coin on the side in the evenings, see what you can do. And now, I mean, we really have a new industry here in independent hackers practicing their craft by seeing if they can find problems; and, if so, reporting them and being rewarded. So yay to that.

Leo: Pretty neat. Millionaires, man. That's incredible.

Steve: Yeah, six millionaires. Yeah, so, I mean, that's some serious money. And again, it's interesting, too. I noticed the Asian guy in Hong Kong, he's got some mileage on him. He looked a little more like my age. I thought, wow. Because the other guys are kids, of course, as you typically see.

Leo: Yeah. You don't have to be a kid.

Steve: Don't have to be a kid.

Leo: Right?

Steve: And HackerOne said, hey, Gibson's an original hacker. So, yeah, okay. I'll accept that.

Leo: That's nice.

Steve: Meanwhile, also last Thursday, Google's Project Zero dropped a bit of a bomb on iOS. First of all, everything we're going to talk about has been fixed. So none of this, I mean, you know, Project Zero operates with full responsibility. In some cases where they find something really worrisome, they don't do their 90-day, take your time to fix it. In one instance, they gave Apple seven days.

Leo: And Apple responded. They had an out-of-band fix within seven days, which is pretty impressive.

Steve: Yes, they did. They did it - they were told on the 1st of February, and their patch was out in six days, on the 7th. So yay to them. Certainly they've got good communication back and forth. So what we learned from Project Zero was that for a period of at least several years a small group of websites was successfully infecting anyone who visited them with a RAM-based monitoring malware through the use of a quite sophisticated iOS version-based multistage exploit chain.

And on one hand, as I was digging into this, I was stunned by the work that the group at Project Zero did in order to figure this stuff out. But that has to parallel the work that somebody else did to make this happen. I mean, so the work of figuring out what the malware is doing probably about echoes the work that some agency somewhere went to to figure out that these things could be exploited. So this sort of suggests that there was some serious effort put into creating these exploit chains. As far as everyone knows, all of this finally ended with the emergency jump to iOS v12.1.4, which is what you're referring to, Leo. And not to confuse that with 12.4.1, which is what...

Leo: Another one.

Steve: Which is what we just did when we got the emergency, oops, regression of the jailbreaking problem.

Leo: Jailbreak, yeah.

Steve: So as Project Zero's Ian Beer explained, the story before then, that is, before 12.1.4, is not only troubling due to the exposure created for those who were infected, and we'll talk about what this implant does once you get it, but also more so due to the conclusions Ian draws based upon the exact nature of what he found. So his blog posting was titled "A very deep dive" - and, oh, boy, is it. I mean, it's so deep we're not going to go that deep on this podcast. And as our listeners know, we're not shy of depth here. But

this is beyond anything I could convey through this medium. But there's links to what he posted, for anybody who really wants the nitty-gritty. Anyway, so he says: "A very deep dive into iOS exploit chains found in the wild."

So Ian wrote: "Project Zero's mission is to make zero-days hard. We often work with other companies to find and report security vulnerabilities, with the ultimate goal of advocating for structural security improvements in popular systems to help protect people everywhere." Of course we've been reporting on Project Zero since it began. And I remember when this first happened we were like, wait, they're going to look at other people's stuff, not just theirs? And yes, as we know, they do that. They've fixed all - they've helped to fix all kinds of things.

So Ian said: "Earlier this year, Google's Threat Analysis Group (TAG)" - which I'll be referring to a bit later - "discovered a small collection of hacked websites. The hacked sites were being used in indiscriminate watering hole attacks against their visitors, using iPhone zero-days." Okay. So there's a lot there to unpack. So a small collection of hacked websites. The hacked sites were being used in indiscriminate - meaning anybody who visited would get themselves infected. "Watering hole" suggests that these were set up and then either based on the demographic of who would visit, or other people may have been induced to go there, that is, thus watering hole, that is, the malware was staged on the site, and then something would be used to induce targets to go visit that site - because they were thirsty, thus watering hole - and that would infect their iPhones.

I should note also that this was never - the infection, the malware was never written to non-volatile storage. So it sat in RAM, despite the fact that it was very capable, only until they rebooted their phone. Most people are typically only rebooting when they have an iOS update from Apple. Sometimes you may shut your phone off completely, but that's not the way most people operate. So this thing's going to tend to stay around for quite a while.

He wrote: "There was no target discrimination. Simply visiting the hacked site was enough for the exploit server to attack your device and, if it was successful, install a monitoring implant. We estimate that these sites received thousands of visitors per week." So notice that's not, I mean, thousands of visitors per week, there are sites that are getting thousands of visitors per minute. So these were non-high traffic sites, probably. And at no point does he talk, I mean, he refers a little bit to dissidence, and the presumption is that this was probably a state-backed attack because you certainly needed state-scale resources in order to mount an attack like this.

And he says TAG, that's their Threat Analysis Group, was able to collect five - and this is where things get interesting - five separate, complete, and unique iPhone exploit chains, covering almost every version from iOS 10 through to the latest version at the time of iOS 12. He says: "This indicated a group making a sustained effort to hack the users of iPhones in certain communities over a period of at least two years."

And then he said: "I'll investigate what I assess to be the root causes of the vulnerabilities and discuss some insights we gain into Apple's software development lifecycle." He says: "The root causes I highlight here are not novel and are often overlooked. We'll see cases of code which seems to have never worked, code that likely skipped QA [Quality Analysis] or likely had little testing or review before being shipped to users."

Now, we know that iOS and Android are inherently competitive, that Ian is on Google's team, and that what he wrote here sounds a bit harsh. But when you dig deeper into his work - and it's truly stunning work on Ian's part, and his group - you'll see what he's been working for years is making Apple's iOS better and more secure for everyone, and that comparatively few people are ever going to see and appreciate the work that he's

done. So despite the way that sounds, he's really not attacking Apple. And I have looked at the details of the code. And what he's really only doing is drawing the only conclusion you could from the code that he sees in front of him when he looks at what it was that was being exploited.

So in his posting he has a chart showing moving through time, starting on the 13th of September 2016 through late January of this year, 2019. And the individual stacks of five different exploit chains, which some entity developed in order to move from iOS 10.0.1 and basically get coverage through 10 and through 11 up to the beginning of iOS 12. So through a period of iPhone 7 through the launch of 8, 8+, X, XR, and XS. So a serious bunch of work.

He said: "Working with TAG, the Threat Analysis Group," he wrote, "we discovered exploits for a total of 14 vulnerabilities across these five exploit chains, seven for the iPhone's web browser." And I will get back to it. But I'll also note that, in fairness, he notes that Chrome would have been similarly vulnerable to those, although the attacks were against Safari. And he says: "Five for the kernel and two separate sandbox escapes."

He wrote: "Initial analysis indicated that at least one of the privilege escalation chains was still a zero-day and unpatched at the time of its discovery. We reported these issues to Apple" - and here's what we were talking about before, Leo - "with a seven-day deadline on the 1st of February, 2019, which resulted in the out-of-band release of iOS 12.1.4 on the 7th of February," so just six days later. We also shared the complete details with Apple, which were disclosed publicly on the 7th of February.

He says: "Now, after several months of careful analysis of almost every byte of every one of the exploit chains," he says, "I'm ready to share these insights into the real-world workings of a campaign exploiting iPhones en masse. This post will include" - and actually it's not this post, it's seven subsidiary posts. He says: "...detailed write-ups of all five privilege escalation exploit chains; a teardown of the implant used, including a demo of the implant running," he says, "on my own devices, talking to a reverse-engineered command and control server and demonstrating the capabilities of the implant to steal private data like iMessages, photos, and GPS location in real-time; and analysis by fellow team member Samuel Gross on the browser exploits used as initial entry points." And that's where they noted that Chrome would have also been vulnerable to the same initial entry point exploits.

He says: "Let's also keep in mind that this was a failure case for the attacker," meaning that they were discovered. He says: "For this one campaign that we've seen, there are almost certainly others that are yet to be seen." In other words, they first discovered a website. The way this was found was they discovered a website that was doing this, then followed that trail back into iOS to understand what the site was doing to iOS, thus the exploit chain. But they reasonably assume that there were very likely other websites that were also exploiting the same suite of vulnerabilities, and those were never found.

He says: "Real users may make risk decisions based on the public perception of the security of these devices. The reality remains that security protections will never eliminate the risk of attack if you're being targeted. To be targeted might mean simply being born in a certain geographic region or being part of a certain ethnic group. All that users can do is be conscious of the fact that mass exploitation still exists and behave accordingly, treating their mobile devices as both integral to their modern lives, yet also as devices which, when compromised, can upload their every action to a database to potentially be used against them." And, you know, this demonstrates the truth of that.

He says: "I hope to guide the general discussion around exploitation away from a focus on the million dollar dissident and towards discussion of the marginal cost for monitoring

the n+1'th potential future dissident." He says: "I shall not get into a discussion of whether these exploits cost $1 million, $2 million, or $20 million. I will instead suggest that all of those price tags seem low for the capability to target and monitor the private activities of entire populations in real time."

So he says: "I recommend that these posts be read in the following order." And this is where he now then, in this original anchor posting, has seven links to the details. The first five of them have one extensive amazingly detailed dive into each of these five individual exploit chains that I'm not going to go into because there's just no way to do that in a podcast. It's all there for anyone who is our listener who is interested. I mean, they are amazingly detailed reverse-engineering works. In the sixth of those seven he says: "We examine the WebKit exploits used to attain an initial foothold in iOS." And that's where he notes that, for the record, Chrome on iOS would have also been vulnerable, even though it was Safari that was attacked.

And he says in his final, seventh posting, he examines the operation of the implant that is finally dropped into the device's RAM. He said: "In the earlier posts we examined how the attackers gained un-sandboxed code execution as root on iPhones. At the end of each chain we saw the attackers calling posix_spawn, passing the path to their implant binary which they had dropped into /tmp folder." He says: "This starts the implant running in the background as root. There's no visual indicator on the device that the implant is running." And of course iOS doesn't give users any sense for what's running.

He says: "There's no way for a user on iOS to view a process list. So the implant binary makes no attempt to hide its execution from the system. The implant is primarily focused on stealing files and uploading live location data. The implant" - and of course you maybe wonder why the perpetrator of this wanted that. Who knows. On the other hand, it's in a position to get everything. And that's pretty much what it does.

He says: "The implant requests commands from a command and control server every 60 seconds. Before diving into the code," he says, "let's take a look at some sample data from a test phone running the implant and communicating with a custom command and control server I," he wrote, "developed. To be clear," he says, "I created this test specifically for the purposes of demonstrating what the implant enabled the attacker to do, and the screenshots are from my device."

He says: "The device here is an iPhone 8 running iOS 12. The implant has access to all the database files on the victim's phone used by popular end-to-end encryption apps like WhatsApp, Telegram, and iMessage. We can see here screenshots of the apps on the left, and on the right are the contents of the database files stolen by the implant which contain the unencrypted plaintext messages sent and received using the apps."

And so of course this is what we've often spoken of is that, yes, you've got end-to-end encryption. And so what leaves the device is encrypted strongly, and we know of no means for anyone intercepting that to be able to determine what's being messaged. On the other hand, this demonstrates beautifully that WhatsApp, Telegram, and iMessage have databases of everything that they've been doing in plaintext. In fact, they even added Hangouts. And all of that is available to something that gets into the phone.

He noted that the implant can upload private files used by all apps on the device. He shows the contents of emails sent via Gmail being uploaded to the attacker's server; notes that the implant also takes copies of the user's complete contacts database, takes copies of all of their photos. The implant can also upload the user's location in real-time up to once per minute, if the device is online. He says: "Here's a sample of live location data collected by the implant," he says, "when I took a trip to Amsterdam with the implant running on an iPhone in my pocket." And then that's detailed in his posting.

He says: "The implant uploads the device's keychain, which contains a huge number of credentials and certificates used on and by the device," he says, "for example, the SSIDs and passwords for all saved WiFi access points. The keychain also contains the long-lived tokens used by services such as Google's iOS Single-Sign-On to enable Google apps to access the user's account. These," he notes, "will be uploaded to the attackers and can then be used to maintain access to the user's Google accounts, even once the implant is no longer running."

And he says: "Here's an example using the Google OAuth token stored as [in this case] com.google.sso.optional.1.accessToken in the keychain being used to log into the Gmail web interface on a separate machine." So he took that and actually demonstrated its ability to be used by an attacker to gain persistent access to the accounts that had been exfiltrated.

Finally, he finishes, after he gets way down into the weeds of the way the implant works, and finishes by talking about the impact. He says: "The implant has access to almost all of the personal information available on the device, which it is able to upload, unencrypted, to the attacker's server. The implant binary does not persist on the device. If the phone is rebooted, then the implant will not run until the device is re-exploited when the user visits a compromised site again. Given the breadth of information stolen, the attackers may nevertheless be able to maintain persistent access to various accounts and services by using the stolen authentication tokens from the keychain, even after they lose access to the device."

So there is a deep look inside someone's, we don't know whose, I mean, Google may know based on the sites that were infected. And that's not been made public. But those sites were infected, low-traffic, probably special interest sites. You know, he referred to dissidents, so it's likely that they do know which sites were - we know that they know which sites were infected. They may have some sense for who the perpetrator was who would have wanted the information of people visiting those sites.

Leo: TechCrunch has since had an article that they said it was Uyghur Muslims, and it was the government of China.

Steve: Ah, okay. Wow.

Leo: And there's a company that does this kind of analysis for NGOs and dissidents, and they actually named the sites. And it's the kind of sites that Muslims would go to. But it's a drive-by in the sense that anybody can go to those sites. You might not be inclined to, but anybody could.

Steve: Right. And as they noted, the attacks themselves are indiscriminate. Anybody who goes there picks up this implant. And it just demonstrates, I mean, we know how much time and attention Apple spends on security and has spent, much as Google does. I mean, any of our major suppliers in this day and age, it has to be a focus of your work. Yet even so, cranking out the amount of code that is being produced, mistakes get made.

Leo: And this was also a nontrivial hack. I mean, it would take a government to do it.

Steve: Oh, my goodness, yes, yes. I mean, they're not chaining multiple exploits for fun. They're chaining them because they need each one to perform some little bit of an overall attack in order to achieve their goal. And it's just not easy. But that just also demonstrates, if you put enough focus on this - well, and I've often, and I will be later, talking about how security needs to be viewed as being porous, meaning if you don't put much pressure against it, it's okay. But if you put enough pressure against it, you'll find some leaks.

Leo: Yeah. So Google never did say where they found this, but I think it's kind of escaped out now.

Steve: Yup.

Leo: And it wasn't, by the way, the only attempt by the Chinese government to get this Muslim minority. They hacked OAuth to get Gmail. We actually talked about another example where they put malicious apps on people's phones as they crossed into the country that would monitor everything they did. So they were very active in this.

Steve: Yeah, or proactive, even.

Leo: Proactive.

Steve: Yeah. So the ransomware epidemic. We don't have anything super definitive yet, even now, from Texas, although nine of the reported 22 affected state municipalities have been identified. And I'm still struck by the surprisingly different feel that these attacks have from those that we've covered before. So I continue to think that an attack on a common service provider is the most likely explanation for everything we're seeing, though evidence to support that opinion is still scant.

Meanwhile, we have a bunch, actually 13 new ransomware attack victims which have come to surface in the last week. While most of them are school districts, which of course the timing of that is unfortunate because school is just starting up again, we also have a county in Indiana, a hospice in California, and a newspaper in Watertown, New York.

Armor, the cloud security firm whose data generated our Picture of the Week, has tracked the following new ransomware infections: Lake County, Indiana has been infected with ransomware; the Rockville Center School District in Rockville Center, New York; the Moses Lake School District in Moses Lake, Washington - that attack actually occurred back in July, but was only reported to be ransomware recently; Mineola Public Schools in Mineola, New York; the Stevens Institute of Technology in Hoboken, New Jersey; New Kent County Public Schools in New Kent, Virginia; the Nampa Idaho School District, Nampa, Idaho; Middletown School District, Middletown, Connecticut.

It's odd that there were five in Connecticut because we also have the Wolcott Public Schools, the Wallingford School District, New Haven Public Schools, all in Connecticut. So maybe there again is some common linkage. We have the Watertown Daily Times in Watertown, New York; and the Hospice of San Joaquin in San Joaquin, California.

So again, lots happening in ransomware. And we may be starting to have a clue as to what's going on and why that we will get to in a second. We still don't know what's going

on in Texas, but we do know that our old friend Ryuk, which we now know is pronounced ree-ook - and this week we have a few other pronunciation challenges we'll get to in a second - has been identified as the culprit in at least three of these additional recent attacks.

Newsday reported that the Rockville Center School District in New York initially received a ransom demand of $176,000. The district's insurance company negotiated with the ransomware perpetrator, managing to cut that to essentially half, reducing the payout to $88,000; and the school district then themselves, because they were insured, obviously, by the insurance company, only needed to pay a deductible of $10,000. So the district paid $10,000 against an initial demand of $176,000, and the ransomware guys ended up getting half of that. But on the other hand, this minimizes the impact to the district. The insurance company took a hit. Yet the ransomware guys were certainly encouraged to do this again, netting $88,000.

There's no word on whether other victims have paid any ransoms yet. Back in June, Brian Krebs did some reporting on the Baltimore, Maryland attack which took Baltimore's servers down on May 7th. After communicating with Armor's Joe Stewart, Brian reported that Baltimore was the victim of a ransomware strain known as "RobbinHood," which we've never heard of before. Now here we are four months later, and Baltimore's leadership recently revealed that $6 million of the money needed to cover the city's more than $10 million ransomware cleanup operation would be pulled from funds earmarked for upkeep of city parks and public facilities.

So what's unfortunate is that it looks like Baltimore, it's not clear where they are in terms of paying ransomware. But they're saying that it's going to cost them $10 million to clean up, and more than half of that money gets taken from funds that were earmarked for city parks and public facilities. So this is being expensive for municipalities that are not insured.

They said that so far the RobbinHood ransomware has cost the city over 8 million in lost revenue. So 6 million of the money needed to cover more than 10 million in cost, and it's cost them 8 million in lost revenue and what they termed as "interest on deferred revenue." So as a consequence of all of this, after the fact, they're now considering a contract for a $20 million cyber liability insurance plan. There's a vote planned on the city council proposing an $835,000 contract, which has been deferred. So now we're seeing it costs them $835,000 to get a $20 million coverage cyber liability insurance plan. Yikes.

These 13 new attacks bring the total known publically reported ransomware attacks this year up to a total of 149. So of those, 30 have involved educational institutions. Chris Hinkley, the head of Armor's Threat Resistance Unit, told Ars Technica in their recent reporting of ransomware events, he said: "Just like municipalities, which rely on critical systems to manage records and revenue in a community, school districts host data and systems critical to their community and its students." He said: "Thus hackers know that schools cannot afford to shut down, that budgets are typically stretched thin, and they often have few security protections in place," of course all making them ripe targets. He said: "...all aspects which make them a viable target."

And of course now we know that insurance carriers are indirectly providing these institutions with virtual deep pockets, so they're able to pay up when necessary. Last May, Ars observed that school districts are particularly easy targets for ransomware operators because of their generally low budget for IT and limited security resources. According to data collected by Armor, schools have become the second largest pool of ransomware victims, only second to local governments, and then closely followed by healthcare organizations in third place.

So the ransomware perpetrators are looking at the history of what attacks are being made and are succeeding, and setting their sights accordingly. And we should also note that these numbers, this 149 this year, are only for publicly reported incidents. CNN also reported last week, and we'll be getting into some more details of this in a second, that a firm named PerCSoft and Digital Dental Record are two companies that collaborate to handle the online services in the dental industry.

They reported, and I've got a PDF I'll share in a second, that roughly 400 of their customers, that is, customers of this Digital Dental Record firm connected to individual offices had been infected with ransomware earlier in the week. Dental administrators told CNN they were unable to access basic information such as patient charts, X-ray data, or payment services.

Digital Dental provided a statement. They said that 100 of the affected 400 practices had been restored since the attack. So these more private incidents highlight the fact that many ransomware attacks may be going unreported because, again, if it's not a big - there's no way to hide a municipality or a school district being attacked. But many smaller problems are occurring. The FBI had reported 1,493 ransomware cases last year, which is far more than the number that were publicly known.

Other than New York's Rockville School District, which was insured and negotiated that $88,000 ransom payment, as I just said, cutting it down in about half, it's still too soon to know whether any of the other newly attacked public organizations have cyber insurance in place or yet in place, and whether they even plan to pay the ransoms. We may find out in time. The payouts which ransomware operators have recently received from similar targets, we've covered the Riviera City in Florida paying $600,000 ransom. In Lake City, also in Florida, paying half a million dollars in ransom signaled certainly to attackers that attacking large communities can be quite lucrative.

ProPublica did an investigation which revealed that insurance companies are fueling the rise of ransomware threats as a consequence of covering the cost minus a deductible, and also of course negotiating the value paid to attackers down. So what this essentially does is turning, in fact, we talked about this a few weeks ago, creating a new category of companies that you would almost term "cyber extortion negotiation services," where they're offering their services to negotiate on behalf of the victims and basically handle, serve as an intermediary between victims that have no idea what to do and the attackers who have encrypted all their systems. And of course, as we know, by rewarding the hackers, it encourages more ransomware attacks.

But also in the news last week was this DDS Safe. And what's somewhat ironic, or I guess even maybe more than somewhat, is that this DDS Safe company was specifically talking about how the cloud-based services they were offering were protecting companies from ransomware. And unfortunately, the company that they were using as their cloud services provider, PerCSoft, based in West Allis, Wisconsin, themselves were victims of an attack.

So in his reporting on this, Brian Krebs was unable, as we know I would have also been, to resist titling his coverage "Ransomware Bites the Dental Data Backup Firm." He explained that PerCSoft was this company that manages a remote data backup service relied upon by hundreds of dental offices across the country through its provision of cloud services to Digital Dental Record, and that Digital Dental Record offers an online dental data backup service called "DDS Safe" that archives medical records, charts, insurance documents, and other personal information for dental offices across the U.S.

The ransomware attack hit PerCSoft on the morning of Monday, August 26th, so last week, and encrypted dental records for some, but not all, of the practices that rely on DDS Safe. Brenna Sadler, the director of communications for the Wisconsin Dental

Association, said the ransomware encrypted files for approximately 400 dental practices, and that somewhere between 80 and 100 of those clients have now had their files restored.

Sadler said she did not know whether PerCSoft and/or DDR had paid the ransom demand, although it looks like Bleeping Computer has some updated data on that. And she did not know which ransomware strain was involved or how much the attackers had demanded. But updates to PerCSoft's Facebook page and statements published by both PerCSoft and this Dental Data Record suggest that someone may have paid up. The statements note that both companies worked with a third-party software company and were able to obtain a decryptor to help clients regain access to files that were locked by the ransomware.

In Brian's reporting, several sources were reporting that PerCSoft did pay the ransom, although it's not clear how much was paid. Bleeping Computer did have some ideas. One member of a private Facebook group dedicated to IT professionals serving the dental industry shared a screenshot, which is purportedly from a conversation between PerCSoft and an affected dental office, indicating the cloud provider was planning to pay the ransom.

What's still very unclear, due to conflicting accounts using annoyingly fuzzy reporting, probably because they either don't know or they don't know that there's a difference or a distinction, is whether the infection of PerCSoft's cloud infrastructure allowed the infection to spread down the connection into the individual dental offices which relied upon DDR and PerCSoft. It looks like they're doing cloud-based backup, but there was some indication that they were unable to access the records they use on a daily basis, suggesting that it's not just their backups, but their actual local records that had been infected, which suggests that the malware did in fact get down into their systems.

And some of their documentation suggests that they were using remote management systems. I was able to find a PDF of the media statement that was put out by DentalRecord.com, and they said in their disclosure: "At 8:44 a.m. on Monday, August 26th, we learned that ransomware had been deployed on the remote management software our product uses to back up client data. Immediate action was taken to investigate and contain the threat. Our investigation and remediation efforts continue. Unfortunately, a number of practices have been and continue to be impacted by this attack."

So we know that it was about 400 dental offices spread around the country. And the fact that they said that the ransomware had been deployed on the remote management software product, that suggests to me that whatever it is they're doing to perform this backup uses remote management, which does suggest that maybe malware was able to get down into the networks through remote management software and actually in fact the real-time data of these services. And of course, not surprisingly, cloud data and backup services are a prime target of cybercriminals who deploy ransomware since ransomware encrypts data, and a lot of data is stored in the cloud.

Also, we didn't talk about this at the time, I don't think it had come to light yet, last month attackers hit the QuickBooks cloud hosting firm iNSYNQ and held the data of many of that company's clients hostage. Earlier this year, last February, cloud payroll provider Apex Human Capital Management was taken down for three days following a ransomware attack. And back on Christmas Eve, at the end of last year, the cloud hosting provider DataResolution.net took its systems offline in response to a ransomware outbreak on its internal networks. The company was adamant that it would not pay the ransom demand, but it ended up taking several weeks for customers to fully regain access to all of their data.

So this is happening all the time and everywhere. And we may not be seeing as much of it as is actually happening. As we know, the FBI and many security firms have advised victims not to pay any ransom demands, arguing that doing so encourages the attackers and may not result in their regaining access to encrypted files. But in reality, also, many cybersecurity consulting firms quietly note to their customers that paying up is probably the fastest route back to business as usual. And we've seen that even, I mean, just the disruption of having, as we saw in several of these recent attacks, the disruption of having computers encrypted is not quick to recover from.

In a report published by the cybersecurity firm Fidelis last week, this next major event or malware that we're about to start talking about, which is known as REvil, but also as this Sodinokibi, it has just emerged as the fourth most prevalent strain of ransomware - and we'll talk about why in a second - at 12.5% is this Sodinokibi. Ryuk holds the lead at 23.9%. of incidences, followed by Phobos at 17% and Dharma at 13.6%. So there's a bunch of ransomware out there which is attacking people. Sodinokibi, S-O-D-I-N-O-K-I-B-I. And it's so fun to say. Maybe I'll learn how to say it one of these days. It's also known as REvil, capital R, capital E, v-i-l, as in R-Evil, REvil. Although Sodinokibi - I've got to practice that a few more times.

So Bleeping Computer, who as we know were the first and very early to shine a bright spotlight on the ransomware scene, have a bunch of great information about this newest kid on the block, Sodinokibi. Bleeping Computer notes that although it is relatively new on the ransomware scene, and we have some theories about why, Sodinokibi has already made impressive profits for its administrators and affiliates, some victims paying as much as $240,000 as tracked from their wallet, and network infections netting an average of $150,000.

Now, our listeners may have noted that I used the term "affiliate," which should be a clue to this new terror's distribution and exploitation model. Yes, like GandCrab, it is RaaS, Ransomware as a Service. We talked about back in April the guys behind - I guess we started talking about it in March because they shut down at the end of April. So the guys behind GandCrab, claiming to have made all the money they needed, and having laundered it and reinvested it in legitimate businesses, they decided to shut down their operation. We wondered and speculated at the time what might surface to fill the void left behind by this diabolical network marketing model. And it looks like we have an answer: Sodinokibi. It turns out it's the thing that knocked those 22 towns off the map in Texas.

Leo: Ah.

Steve: Uh-huh. And then nuked those 400-some dental practices. Yes, it is truly REvil. Bleeping Computer reports that the Texas extortion, we now have numbers from them, totaled $2.5 million. So remember that was the 22 townships or municipalities and towns. So the Texas extortion came in at $2.5 million, and the ransom to restore those 400-odd dental offices machines was $5,000 per, now, I wrote "per computer." But I must have meant per office. So somewhere around another $2 million. So since its first appearance in April, meaning that it appeared immediately, I mean, like almost immediately after GandCrab disappeared, Sodinokibi has become prolific and quickly gained a reputation among cybercriminals in the ransomware business and security researchers. And as we know, this is aided by the fact that it's making others among the underworld quite a bit of money in turn.

Although one of the things that really stood out was what a small piece of the action the GandCrab people took. These Sodinokibi guys are taking more, at least initially. After its first month back in mid-May, to put itself more squarely on the map, a Sodinokibi

advertiser, who we now believe is the one behind it, they're going by the forum name UNKN, deposited over $100,000 on underground forums to show that they meant business. Online underground advertisements for the new file-encrypting malware appeared in early July on at least two forums. And this UNKN group said that they were looking to expand their activity; that it was a private operation with a limited number of seats available for experienced individuals.

So again, they're describing their malware as private ransomware, though it is flexible enough to adapt to the Ransomware as a Service business model. UNKN offered their affiliates 60% of the payments, that is, the ransomware, at the beginning, and a 10% increase to 70% after the first three transactions. So the people who indirectly exploited this basically, again, ransomware as a model, meaning that this UNKN would make their ransomware available to third parties, who would then go do the - who would arrange to get victims infected. They would initially receive 60% of the payout, and that would bump to 70% after the first three.

And this actor, this UNKN, also made it clear that they would not be working with English-speaking affiliates as part of this private program. Bleeping Computer posted a screenshot monitoring the ransomware's bitcoin transactions, showing the money pouring in from its victims. Looking at the second one - I have a screenshot here in the show notes. Looking at the second one shows that one victim paid 26.388 bitcoins, which at the time converted to 240,143 USD. And so when the screenshot was taken, that one, that 240,143 USD was 11 hours previously. There was a 0.43 bitcoin, and at the time that was, looks like about 4,000 USD at what was seven hours ago.

Then there were one, two, three, four, five that were 12 hours ago, all about the same amount, that $4,000. Then two days previously there had been a, looks like nearly $20,000. Also two days before about $4,000 and another $4,000. So, I mean, this thing is really making some money. And for affiliates who arrange to infect an entire network, the Sodinokibi developers allow a victim to purchase a decryption tool for the entire fleet of infected computers. According to a forum post shared with Bleeping Computer, those network-wide decryptors have an average cost of $150,000.

So with revenue flooding in, and everybody is able to see what's happening here with the bitcoin wallet, and the people in the underground forums are, I mean, there's a lot of buzz around this, other malware "distributors" are attempting to gain access to the program. But this UNKN group stated that there are currently no available openings for affiliates at this time. Bleeping Computer also reported that the operators behind the Sodinokibi ransomware started searching for affiliates to distribute their software shortly after GandCrab had formally shut down.

The underground reactions toward the new product suggests that there may have been a connection with the administrators or the affiliates of what is now the defunct GandCrab operation and this new Sodinokibi ransomware. Some malware analysts pointed to some code level similarities between the two ransomware strains, although many differences also exist between the two. And you would expect some similarities because one could be just based on some of the way the other works.

However, there was one similarity noted is that the administrators of both malware families are refusing to carry out business in the Commonwealth of Independent States, the so-called CIS area. This is Russia, Ukraine, Moldova, Belarus, Armenia, Turkmenistan, Uzbekistan, and a bunch of other 'stans that I can't even pronounce. Oh, there's Kazakhstan. I know how to say that one. But there's K-Y-R-G-Y-Z-S-T-A-N and T-A-J-I-K-I-S-T-A-N. Whew.

Leo: Tajikistan.

Steve: Tajikistan.

Leo: Tajikistan.

Steve: Anyway, these little breadcrumbs, along with the rapid ascension of this new malware on the scene, do suggest some sort of involvement of the previously well-established GandCrab crew or its affiliates, and that they may already have private connections on these forums that have allowed them to quickly promote Sodinokibi and be selective about their partners. So there's no clear undeniable evidence that Sodinokibi is run by the same individuals that administered GandCrab. But they obviously know the ransomware game and are once again making some serious money from this.

So I guess I'll conclude by observing, again, that everything changed the moment we moved from viruses and malware, which were just being created because they could be for their own sake. You know, Leo, you and I often commented in the early years of this podcast that the viruses were spreading, but they weren't doing anything. I mean, they were just sort of annoying. You didn't want to have it in your computer. But it just, you know, it was being identified by the early AV tools, and it was sort of just there to spread itself. You know, kiddies were messing with it because they could.

But as soon as cryptocurrency exchange - well, first of all, cryptocurrency happened. And that was interesting. Then cryptocurrency exchanges appeared so that cyber currency could then be used to pay the rent and to buy a burger. And so what happened then was that stealing CPU cycles through cryptojacking jumped to the foreground. But then this emergence of cryptocurrencies also meant that there was now a means for ransomware perpetrators to safely receive extortion payments. Remember that, again, in the early years of this podcast, we talked about, like, Western Union payments, right, being made to Russia, I remember. And the problem was wiring money made the funds traceable, given that you had some relationship with the country of destination. But cryptocurrency enabling a much higher degree of anonymity meant that ransomware soon followed.

So today there isn't a malware author alive who isn't aware that it's now possible to live well by finding, infecting, and encrypting the data of the right targets. And this really changes everything. The twisted brilliance of ransomware is that the victim's data is still there. They can see their files, now with a .crypto or other extension appended to the end. The files aren't deleted. They've simply been moved just out of reach, which allows the carrot of full data recovery to be dangled in front of the victim. And as a result, more often than not, though no one wants to knuckle under to extortion, the sanity of self-interest does prevail, and money does flow into the bad guys' cryptocurrency wallets to further encourage them to find another victim.

One of my favorite analogies that I mentioned before for this podcast has been how porous our computer security really is. And I think that this notion of porosity is just the right term, you know, because security does exist. We know it exists. It's kind of there. It's mostly useful. It pretty much protects us. But it isn't absolute protection. And we especially see that when security is put under pressure. And of course pressure is what the emergence of cryptocurrency exchanges has created because now there's a model for bad guys to make a bunch of money.

So what does the future look like? I think we could predict what's going to happen based on what we've seen happen in the past. When the world learned that the NSA had installed data-sucking taps at many of the Internet's major Internet exchange points, our collective reaction was to treat encryption as more than an expensive option. It suddenly became important. And so as we know, today, to a far greater degree than previously,

the entire world's communications are now encrypted end to end. I expect we're going to see something similar happening with system backup imaging. IT departments, just like in the old days with encryption, IT departments have not prioritized the maintenance of good hot and cold backup because they have not had to until now. For the most part, things have been running along just fine.

But that's no longer true. It will no longer be reasonable for a ransomware event to take a municipality or a school district or a corporation offline for months. That won't fly in the future. Storage has become so cheap that there isn't any - there's no reason any longer not to have backups of everything. And where security concerns are paramount, if someone's worried about shipping corporate records into the cloud, there's no need to move backups into the cloud. I mean, that's certainly an advantage for some instances. But it's possible to get a large rack of local storage and secure it and use it.

So I think we're going to start seeing something we haven't really seen yet, which is the emergence of explicitly ransomware-oriented backup protection, where nightly snapshot images of individual workstations are rotated after a day where the computer has been used. And those snapshots will be deliberately kept firmly offline and inaccessible so that, if some malady should hit a machine or machines, those machines can be restored to their previous night's image without a lot of trouble.

I've previously mentioned that this is something I'm already doing using the Windows mountvol command, which allows you to take a volume which is offline and bring it online. And then I also do some registry editing to further hide the unmounted volumes, since mountvol will look at the registry in order to show what it knows is available. And that allows me to transiently bring a well-hidden offline drive online briefly while an image is being made of my main working system, but to keep it hidden otherwise. So I have cold backups which are current. And then of course I have other means for doing incremental backups for the things I'm working on during the day.

And we should also note that, at the operating system level, what ransomware is doing on a system really does stand out. You know, it's unusual behavior for any program to suddenly be performing wholesale encryption of a large number of files. That's something that future OSes themselves should readily be able to observe, detect, and put a stop to. And although whitelisting every program that a system uses can be quite burdensome, whitelisting the few programs that might legitimately need to encrypt large numbers of files is entirely feasible.

So the idea would be that there could be something added, I mean, maybe we'll see future AV doing this, who knows. But the idea of stopping something unknown from suddenly encrypting a bunch of files on the hard drive seems like something that could be added to the OS. And certainly all of our OS vendors are now doing AV and taking responsibility increasingly for malware which is affecting their customers' machines. It's no longer the exception. It's now the rule.

So it really looks to me like we are seeing the beginning of what I titled this podcast, a ransomware epidemic, as a consequence of the fact that it is now possible for bad guys to make some serious money, depending upon the size of the entity that they're able to take down. And it's no longer the case that these are exceptional events. And so I think we're going to have to see IT departments getting very serious about coming up with some countermeasures for allowing quick recovery in the event that that happens.

Leo: Of course remember FileVault and BitLocker are locking all the files, too. I mean, there are some...

Steve: BitLocker doesn't.

Leo: It doesn't encrypt all the files?

Steve: Well, it does, but when you're inside it's decrypted.

Leo: It's unencrypted, yeah, yeah.

Steve: Yeah, yeah.

Leo: I mean, you could distinguish between the two, obviously.

Steve: Well, and if you encrypt the encrypted files, then you can't get them back, either.

Leo: Right. Even better.

Steve: That's right.

Leo: So here is your short URL: twit.to. That's our URL shortener, twit.to, not .tv, twit.to/unlocked. Because that's the name of our event: Cybersecurity & Identity Trends, Unlocked. It is coming Thursday, October 3rd, one month from today, in Boston at the Intercontinental Hotel. Now, don't panic, Steve. I know it says 3:45 p.m. to 8:00 p.m. We will not be onstage that whole time. We're only going to do an hour and a half. But there will be cocktails afterwards, and people can mingle. So they're not going to throw us out until 8:00 p.m. But it will begin around 4:00 p.m., so you want to get there early.

And as I said, there are a limited number of tickets for this. So if you're going to be in the Boston area October 3rd, then please. It's free to go, but every attendee will get a $100 token they can donate to the charity of their choice. This is part of LogMeIn's corporate social responsibility program, Mission Possible. So thank you, LogMeIn, for doing this, and LastPass. Of course I'll be there. You will be there, Steve Gibson.

Steve: Yup.

Leo: Bill Cheswick, "Ches" will be there. And the CISO of LogMeIn, Gerry Beuchelt, will be there, as well. So it's going to be a great panel. I'm really looking forward to it. And you're all invited. It is free to attend. Twit.to/unlocked, if you're going to be in the Boston area October 3rd.

Steve: And I'll just mention, as a courtesy, if your plans change and you can't make it...

Leo: Let us know.

Steve: Please uninvite yourself so that people who are actually able to attend will be able to.

Leo: Always a problem with free tickets. If you made people pay a thousand bucks, they'd show up. You can almost promise. But you give away tickets, sometimes people change their minds. So please, yeah, let us know. That would be a good courtesy. Twit.to/unlocked. I'm going to give you another URL: GRC.com. No shortener needed.

Steve: Oh, I know that one, yay.

Leo: Yeah. No shortener needed for that one. That's as short as can be. That's Steve's home on the Internet, the Gibson Research Corporation. While you're there, pick up SpinRite, the world's best hard drive recovery and maintenance utility. And you can also of course get copies of this show. He makes the unique 16Kb versions available for the bandwidth impaired. Also text versions, human transcribed by Elaine Farris. So that's a really nice feature there at GRC.com. We have audio, but also video, at TWiT.tv/sn. That's our website, TWiT.tv/sn. It's also on YouTube on the Security Now! channel.

You know the best thing to do, why worry about where it is. Subscribe. Get a podcast application and search for Security Now!, press the subscribe button, you'll get it automatically every Tuesday, the minute we're done. Well, give the editors a few minutes to edit it up. We do do the show every Tuesday around 1:30 Pacific, 4:30 Eastern, 20:30 UTC at TWiT.tv/live. You can watch live. The chatroom is irc.twit.tv. Steve?

Steve: Except for next week, when we are...

Leo: We're going to be on Monday.

Steve: We're going to be on Monday at 1:00 p.m., you and I, in order to make lots of room for the big Apple event on Tuesday.

Leo: The following day, yeah.

Steve: Yes.

Leo: So we're going to make it an all-Apple day on Tuesday. 10:00 a.m. the Apple event, right after that MacBreak Weekly, then iOS Today. That squeezes Security Now! out, so we're going to move you to Monday because we know everybody wants their Security Now!. We're not going to put you off. So we'll do it a little early. That way you'll get it a little sooner. So if you want to watch live next Monday, which is September 9th, you can do that. Just watch at 1:00 p.m. Pacific on September 9th, 4:00 p.m. Eastern.

Steve: Will the podcast be available for download a day early? Or will it appear at the same time?

Leo: It's up to you. What do you want?

Steve: I don't care. I just thought, if it was there, our listeners I know are anxious for it. So...

Leo: Subscribe. That way you'll get it the minute it's available.

Steve: Hey, there you go.

Leo: I see no reason not to put it out early, unless there's no editors here.

Steve: Yeah. Yeah, I agree, Leo. I don't see any reason.

Leo: We won't have editors? It's possible we won't have editors because we don't do much on Monday.

Steve: Okay.

Leo: So if we don't, it'll come out Tuesday. But no later than usual.

Steve: And that's useful for Elaine, too, for her planning, because she's got to know when it's going to appear.

Leo: So next Monday. Just once for the Security Now! show. And then you and I, because you're going to Europe soon...

Steve: Yes.

Leo: So you and I are going to do some early Security Nows for your trip.

Steve: Yes. We will be recording on several Saturdays, two successive Saturdays before I leave so that we can keep our Security Nows flowing.

Leo: Yes. I think I have those right in front of me. Saturday September 14th and the 21st.

Steve: Yup.

Leo: We're going to do an evergreen one on the 14th, that'll be for October 1st. We don't want to do it too early because then everything could change by October 1st. So we'll do a more evergreen show then. And on the 21st we're doing it for the week of the 24th, so it's just a couple of days away.

Steve: Yeah. We're going to - I have continued to explore intersystem file synchronization.

Leo: Oh, good, so it's going to be a whole show?

Steve: That's what we're going to talk about. It's Steve's File Sync Destination or conclusion or something. I don't remember what I was going to call it.

Leo: I can't wait. That's going to be very interesting.

Steve: Oh, I think I was going to call it "Sync or Swim."

Leo: "Sync or Swim." I like it. Steve, have a great week. We'll see you next Monday for Security Now!.

Steve: Right-o, my friend.