The Ransomware Task Force

Description: This week we touch on several topics surrounding ransomware. We look at the REvil attack that affected Apple, and at this past weekend's attack that brought down Southern California's world-renowned Scripps Health system. We catch up on the multinational takedown of the Emotet botnet and the FBI's contribution of more than four million compromised email addresses to Troy Hunt's Have I Been Pwned. We also look at the two notification services that Troy now offers. I take the opportunity to pound another well-deserved nail into QNAP, and take note of an update I just made to my favorite NNTP newsreader, Gravity. I've also run across a Dan Kaminsky anecdote that I have to share. Then we have two pieces of closing-the-loop listener feedback before we conclude by taking a look at the just-announced task force to combat ransomware. Is there any hope that this scourge can be thwarted?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-817.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-817-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. And unfortunately there's a lot of ransomware to talk about. Scripps Health has been brought down by ransomware. Apple supplier Quanta has also been brought down by the REvil ransomware. And Steve's going to be talking about the Ransomware Task Force, a governmental effort to stop ransomware in its tracks. How good can it be? We'll find out. That and of course a lot more security news, all coming up next. A little sci-fi, too, with Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 817, recorded Tuesday, May the 4th, 2021: The Ransomware Task Force.

It's time for Security Now!, the show where we cover your security and privacy online with this guy right here, Mr. Steve Gibson of GRC.com. Hello, Steve.

Steve Gibson: Yo, Leo.

Leo: How are you?

Steve: Great to be with you as we begin May. Down here we have May Gray. I don't know if you have May Gray in Northern California. That's followed unfortunately...

Leo: We do. They call it the marine layer.

Steve: Ah, yes. And it's followed by June Gloom.

Leo: Right. It's all summer long, let's face it.

Steve: Well, the summer basically tries not to happen. So thanks a lot. I have sort of ambivalent feelings about this, which I will articulate by the end of today's podcast. But because it's happening, and it's a thing, I thought we had to talk about it. And that is the recently announced Ransomware Task Force. I also have mixed feelings about bureaucracies in general. I'm not a big fan of endless committee meetings. I've mentioned before that GRC got to a point where I once years later discovered an outline which I had created to prepare for meetings about our meetings. And I realized, oh, my god, our meetings are having meetings. So I just, like, yeah, that's not the way I wanted to run my company. Consequently we no longer have meetings because I have almost no employees.

Leo: Be a small meeting, yeah. It would be very small.

Steve: Yes. So, but anyway, there were a couple interesting pieces of information we haven't had before, although most of what's going on with the ransomware world is well covered. But still worth talking about. I wanted to sort of plant that flag so that we can then go from there and see if anything develops from it.

We're going to touch on a couple topics surrounding ransomware first. Of course I know you've been talking about it, this REvil attack that affected Apple through one of their suppliers. We're also going to look at just this past weekend's attack that brought down Southern California's world-renowned Scripps Health system. Ouch. We also are going to catch up on something that had been going on, but I was sort of waiting for the other shoe to drop to see what would happen. That happened Sunday before last with a really interesting coordinated multinational takedown of the Emotet Botnet, which has been - like it's a huge botnet. Somehow we just hadn't talked about it, and I'll explain why later. But since 2014 it had been growing.

And as sort of part of that, the FBI contributed more than four million compromised email addresses to Troy Hunt's Have I Been Pwned. We're going to follow up talking about that by looking at two notification services that Troy now offers. And Leo, you're going to want to be poking at one of these because you can now have Have I Been Pwned check for any compromised email addresses by domain, as in *@twit.tv.

Leo: Yeah, that's good.

Steve: And I did that, and I had to get my heart back under control after it returned 155 GRC.com compromised email addresses, which I'll explain. So anyway, you can cheat and scroll ahead if you want to and be ready with how many TWiT.tv were found. Anyway, I'm going to take that opportunity to pound - well, so we have that. Then I'm also going to take the opportunity to pound another well-deserved nail into QNAP, the company that I've come to love to hate because they're just so bad. Also I'm going to talk about an update I just made to my favorite NNTP newsreader, Gravity, whose source I've taken over because it had been abandoned 10 years ago.

And I ran across an anecdote regarding our ex-friend, unfortunately, Dan Kaminsky, whom we celebrated last week. But I had to share this one little bit of fun that also arose from people talking about Dan. We've got two pieces of closing-the-loop feedback from our listeners. And then, as I said, we're going to talk about this Ransomware Task Force. I'm glad it exists. It's good that we're going to, like, an effort is being mounted. But for reasons that we'll talk about, I'm skeptical about whether it can, whether anything can be done. And we have a Picture of the Week that literally brought an LOL out of you the moment you saw it.

Leo: I kind of burst out and said "Oh ho ho ho." It's fun, totally fun.

Steve: Well, and frankly I'm very impressed with how quickly you got it. I think it was instant recognition. So no wonder you're a good chess player.

Leo: Pattern recognition. It's all about pattern recognition.

Steve: Exactly.

Leo: Now let's see how smart they are. Let's see how quickly they grok this.

Steve: Three, two, one.

Leo: You want me to show it? Should I show it?

Steve: Oh, yeah.

Leo: And then this is the Picture of the Week. See how quickly you get it. Silence. So should we describe it, Steve, for people who are listening?

Steve: Yeah. So anyway, this is just fun. I loved it. It is a picture of the classic red Volkswagen Bug, or the Beetle, sometimes referred to as the Beetle, you know, the traditional-shaped VW Bug. And the license plate simply says "FEATURE."

Leo: It's a bug, not a feature. I love it. I wonder, you know, if the guy's driving down the street, how many people see that and go, what?

Steve: I was thinking the same thing. Maybe if you were in Silicon Valley. I don't know where this picture was taken. But you could imagine in a sufficiently techie area people would - he'd be getting some horn toots and people appreciating the fact that it's like, it's not a bug, it's a feature, or vice versa. So, yeah. Anyway, perfect Picture of the Week. So thank you, Twitter listener, follower, tweeter. And all pictures are welcome.

Leo: I guess you get a lot of them now in your Twitter feed. @SGgrc is his Twitter handle.

Steve: Yeah. So two weeks ago, shortly before Apple's big "Spring Loaded" product announcement event, the Sodin group, which is behind the REvil ransomware, began publicly leaking Apple's proprietary designs for its forthcoming Mac laptops. The group's so-called "Happy Blog," as it calls itself, stated: "In order not to wait for the upcoming Apple presentations, today we, the REvil group, will provide data on the upcoming releases of the company so beloved by many. Tim Cook can say, 'Thank you, Quanta.' From our side, a lot of time has been devoted to solving this problem."

Well, okay. So Quanta, Quanta Computer, is a Taiwanese company that assembles a number of Apple laptops and other consumer devices. I know they're watched, as well. And I'm sure you, Leo, are more tuned up on this than I am since you get to talk to your Mac folks.

Leo: Yeah. They do the laptops, I think, is their - yeah.

Steve: Yeah. So when Quanta initially refused to negotiate with the REvil group, Quanta Computer is a large supplier, not only for Apple, but for others. In some of the news coverage I saw that they said "ThinkPad." But I wasn't sure whether that one might have been a typo, or maybe they actually are doing like construction for Lenovo.

Leo: Wow.

Steve: I don't know. But anyway, it was Quanta Computer that was actually compromised by the REvil ransomware.

Leo: It says all 10 top PC companies in the world use Quanta.

Steve: Yeah.

Leo: So that's all of them, including Lenovo, yeah. Wow.

Steve: Exactly. So, and that's not the, well, it is the company that you would want to get inside if you were a ransomware gang. And of course Apple would be particularly sensitive to the disclosure. We know how concerned they are over leaks. So they would be particularly concerned over this disclosure. The ransom demand was initially posted just hours before Apple's event. And the hackers said that they would release more documents every day, adding: "We recommend that Apple buy back the available data by May 1st." And a similar extortion attempt from the same group, aimed at Acer, demanded $50 million in exchange for deleting Acer's files. And I saw the same number, 50 million, was like the opening extortion level also for the Apple stuff.

So groups throughout the Internet began grabbing and analyzing the details from the leaks, and this stuff looked authentic, and there's no reason to believe it wouldn't be. They noted some differences with the current models on sale. A new version of the MacBook Pro was shown without the touch bar, and it appeared that maybe HDMI ports might be staging a comeback along with SD card readers. So, yeah, this early release was providing details that Apple would have rather been releasing themselves.

What we know of REvil from the past is that they are tough negotiators who do not make idle threats. Of course, they don't want to acquire a reputation for not doing what they say they're going to do, or people will start ignoring them. So they're also not known for being soft or for backing down. So something must be going on because last week the REvil gang removed Apple's schematics, drawings, and other data from their data leak site after first warning Quanta that they would leak drawings for the new iPad and the new Apple logos, which I thought was interesting. It's like, what? New Apple logos? So anyway, maybe Apple said, okay, look, Quanta, we need to stop this.

Leo: It did get quiet. They only released two schematics that I saw.

Steve: Right. And so what appears to have happened, for reasons we can only guess, is that Quanta finally responded to REvil and opened a dialogue. As part of a private chat, and I think it was Bleeping Computer who posted some screenshots of that which they got somehow, REvil told Quanta that they hid the data leak page and will stop talking to reporters to allow negotiations to continue. And REvil stated that: "Having started a dialogue with us, you can count on a good discount." And indeed that does appear to be the case. Yeah, the extortion.

Leo: Act today to save 20%.

Steve: Oh, no, that's exactly what happens. So since the demand was updated, it now carries an expiration date of this coming Friday, May 7th. But it's been reduced from the original request of 50 million down to the now much more seemingly affordable 20 million.

Leo: See, I can't see Apple paying a penny. And Quanta shouldn't either. But at the same time I also could see Apple being very concerned.

Steve: Yeah, yeah.

Leo: I mean, this is stuff they're going to announce in June.

Steve: Various researchers have been quoted saying that this appears to be a pattern. The REvil gang apparently feels that forcing the opening of a dialogue with their victim is a crucial first step in getting paid. So what appears to be happening is that we're seeing a pattern of them deliberately establishing a reputation for dramatically reducing their initial ransom demand upon the establishment of a dialogue. So this asking 50 and immediately dropping to 20, that's what people are now coming to expect.

And of course I guess this provides some incentive for a victim to establish contact in order to obtain the more real ransom demand, and also of course in the process serves to break the ice. And it's like, well, now, I mean, of course we're all put in mind of that old joke about prostitution, like okay, well, we've determined what you are, now we're just negotiating a price. So this is the world we're in, and of course we'll be talking about this takedown task force here, or, well, the Ransomware Task Force shortly.

I did want to mention, because it's another significant event, that nearly the entire Scripps Health system, which is a world-renowned hospital network based in San Diego,

was hit over this past weekend by a cyberattack which forced some critical care patients to be diverted. And of course it's particularly galling when any healthcare provider is hit, as so many have been, representing I guess sort of a soft target for whatever reason. Scripps acknowledged the attack in a statement, but did not specify whether it was explicitly a ransomware incident, although in some follow-on reporting everybody seemed to be assuming that, although I wasn't able to track down a specific reference to which ransomware.

It's also unknown whether the adversaries compromised any patient records or other sensitive data, "unknown" meaning just not yet public. An email notice from the County Emergency Services Coordinator Jaime Pitner said that all four of Scripps' main hospitals in Chula Vista, Encinitas, La Jolla, and San Diego implemented emergency care diversions. Stroke, trauma, and heart attack patients were all sent to other medical centers because they were just unable to provide for them while they were completely down.

As we know, emergencies being sent elsewhere after a ransomware attack is not unheard of by any means. Last September employees at Universal Health Services - we talked about this at the time - which is the owner of a nationwide network of hospitals, reported widespread outages that resulted in delayed lab results, a fallback to pen and paper by patient care, as well as patients being diverted to other hospitals. In that case, the culprit was Ryuk, which locked up hospital systems for days.

And one of the interesting stats that we'll get out of this task force is the average number of days that ransomware brings systems down. A nurse within the Scripps system wrote that: "No patients died tonight in our emergency room. But," she wrote, "I can surely see how this could happen in large centers due to delay in patient care." And according to reports, outages are widespread across the whole Scripps system. The San Diego Times-Union newspaper reported that the cyberattack disrupted the organization's backup servers in Arizona; the MyScripps online patient portal was taken offline; and Monday, yesterday, appointments were being postponed.

So the day-to-day activities of staff had also been compromised. Nurses, doctors, and other personnel have resorted to using manual processes and paper records since the electronic health record system was also disrupted. And we know that's something that also happened after the UHS attack. So, oh, also the telemetry being used in real-time at most sites, which is used for electronic monitoring and alarming, heart monitors for instance, had become inaccessible. Scripps said that regular manual checks would then be required because they could no longer count on their telemetry system, which was down. A source told the newspaper that medical imaging and other resources had been affected. So this was a big, comprehensive outage.

The Scripps statement said that, while the systems were offline, "patient care continues to be delivered safely and effectively at our facilities" - not conveniently, but yes, they're managing to work around this - and, they said, "utilizing established backup processes, including offline documentation methods." And of course they're attempting to put the best face possible on this nightmare which has been deliberately perpetrated by almost certainly attackers located in - what we're seeing is they're probably in Russia or China. And we'll be talking about that again at the end of the podcast. And, you know, there's a sense of you've seen one ransomware attack, you've seen them all. But I don't think we should allow ourselves to become complacent about these attacks, and numb to them. The question of course is what, if anything, can be done. So that doesn't look like there's an answer for that at this point.

But speaking of what can be done, on the topic of massive and pernicious botnets, somehow we've really never stopped to take notice of Emotet. Perhaps it's because from one standpoint it was just another botnet, and we've certainly spent a lot of time talking

about botnets in general through the years, though Emotet has not remained "just another botnet." And so I guess while it was on the rise, we were a bit botnet saturated. But something big has been happening. At the beginning of this year, in an effort named "Operation Ladybird," a coordinated global operation which included the law enforcement authorities from Canada, France, Germany, Lithuania, the Netherlands, Ukraine, the U.K., and the United States. All worked together to take control of the hundreds of botnet servers which were supporting the Emotet botnet network.

And they didn't stop there. Since at one point as many as 1.6 million active bot infections were believed to be active, there was a need to then proactively disinfect those infections. We're finally talking about Emotet today because Sunday before last, on April 25th at 1:00 p.m., that was the date and time set inside a replacement DLL that had previously been injected network-wide after the takedown, and I'll explain in more detail in a minute. But at that moment, Sunday before last, more than one million Emotet bots synchronously shut themselves down forever. Okay, but I'm getting ahead of myself.

Leo: Wow, that's cool. I mean interesting, yeah. Synchronized bots.

Steve: Okay. So let's back up a bit and examine the history of what has been literally a historical and unique network. Trend Micro was the first group to detect and profile the original Emotet trojan back in 2014, shortly after it appeared. What they discovered then was at the time a relatively straightforward banking trojan spread by phishing emails. And banking trojans sit in a user's machine - we've talked about them often - patiently waiting for connections to known banking systems. When this is seen, they capture and forward the user's banking authentication credentials, sending them to their bot masters, who then typically empty the unwitting user's account.

Or another thing they might do is, while the user believes they're actually performing some generic standard banking transaction, like log into their bank account and then just do something as benign as check their balance, what these trojans are able to do is establish a shadow connection, using their credentials, to their account. And as soon as they navigate away from the page, that trojan will then transfer, issue on their behalf a transfer of all of their funds to some offshore account somewhere. And then people report, you know, wait, next time they check or a check bounces or something, where did all my money go? Well, it went to a banking trojan.

So as we've always seen, cybercrime has evolved from just sort of a "can we make worms propagate" lark into something which started making money for the bad guys. And of course as soon as the bad guys could start making money, as they said, there's money in them thar hills, and that changed the entire nature of cybercrime.

Okay. So through the intervening years since 2014, because this thing was succeeding, it also evolved multiple times. Over time, it grew into a mature and huge Malware as a Service botnet, offering access to its compromised endpoint bots for those wishing to pay. And unfortunately there were many who wished to pay. Among them were famous ransomware groups such as Ryuk, and those also pushing their own data-stealing trojans such as Trickbot. They quickly made the most of the initial access provided to them for pay by the Emotet network, picking and choosing into which victims they would deploy additional payloads. And Emotet was used by the so-called TA542 threat group, also known as Mummy Spider, to deploy second-stage malware payloads such as Qbot and Trickbot.

It also usually led to full network compromise and often the deployment of ransomware payloads across all infected systems, which a compromised endpoint would allow. So ransomware like ProLock or Egregor by the Qbot people, or Ryuk and Conti by Trickbot.

So this was a big problem. And because we were talking about more than a million endpoints, it was actively being tracked.

This growing and enduring success of Emotet demonstrated among other things the potential of success through nothing more than relatively straightforward phishing campaigns that were the main way that this infection was spread; or, that is, you know, injected into people's computers. It also highlighted the evolution and growing sophistication of the cybercrime economy which was developing its own specialized supply chain. And once inside a single machine, Emotet evolved the ability to then spread laterally to other devices on a network, which made it among the most resilient pieces of malware which had been seen in recent times. All instances of Emotet within a network needed to be killed simultaneously because a single surviving instance would quickly reinfect all other reachable machines. So it was a big nightmare.

Recently, Trend Micro stated that it had grown into one of the largest threats they monitored over the past 10 years, consistently in the top 10 campaigns detected; and with, as I said, according to the U.S. Department of Justice, more than 1.6 million victim machines.

Okay. So at the beginning of this year, 2021, after a very quiet multinational organization, a law enforcement group that had assembled to deal with this global threat was ready, and they made their move. In a coordinated takedown strike this past January, control was taken over the IP addresses of the network's command-and-control servers located throughout more than 90, nine zero, different countries. In coordination with cybersecurity experts, replacement servers were connected to the individual IP addresses of the Emotet's command-and-control machines, hundreds of them, many of them which were themselves hacked PCs which the Emotet gang had been using to manage the botnet and send instructions to its 1.6 million victim endpoint botnet machines.

A security researcher who was involved in the operation said: "We took over every critical C2 [command and control] top, down, left, right. From that point on, if a victim machine reaches out to one of my servers or our partners' servers, they're going to get a payload that's inert and prevents further communication with the original botnet." It's over. Or was it?

Previous botnet takedown operations have had mixed success, with the cybercriminals often being able to rebuild their networks rather quickly after a takedown attempt, which were enabled, this rebuilding, by built-in fallback communications channels. So, for example, a prior attempt to neuter the Trickbot botnet is believed to have resulted in only a short-term setback for its operators, who have since developed new versions of their malware and made progress toward rebuilding. But the good guys had been learning, too, lesson after lesson after lesson. So again, we're in that Spy vs. Spy mode or, yeah.

In their statement about the Emotet takedown, Dutch police noted that they discovered and disrupted the infrastructure's backups, too, which they hope will make a possible reconstruction of Emotet very difficult, if not impossible. The security researcher who participated in the takedown confirmed that the operation also monitored the hackers' backup processes to ensure that there were no unknown hidden recovery techniques. And he believes that all backups were disrupted. He said: "We found their backups and how they used them, and we took all of them, too." So, he said: "It's going to be very hard, if not impossible, for them to recover. And even if they do, we have other tools up our sleeve to combat that."

And indeed, since the January takedown, Trend Micro has reported that there has been no Emotet activity. They said they still observed some detections, since it's nearly

impossible to erase all traces of such a massive infection immediately upon takedown. But as residual infections continue to be cleaned up, they expect to see a gradual elimination of the threat completely.

After the takedown operation, with the redirection of the network's command-and-control server IPs to law enforcement control, authorities then pushed a new configuration to the million-plus active Emotet infections so that the malware would then begin to use permanently command-and-control servers permanently controlled by Germany's federal police agency. So essentially they did a transient IP redirection that allowed them to then push changes to the infections which then told the infections to change the IPs that they subsequently got instructions from, thus permanently commandeering the dynamic Emotet botnet.

Once that was done, every Emotet infection was updated with a new benign Emotet module, which was a 32-bit EmotetLoader.dll, literally, E-M-O-T-E-T-L-O-A-D-E-R dot D-L-L. That was inserted into all infected systems. And that's the thing that had the April 25th time bomb. This is what caused the entire network of more than one million instances of infected machines to synchronously become inert Sunday before last at 1:00 p.m. At that moment the Windows server startup and autorun registry keys were deleted network-wide, and the services self-terminated, and it was over.

Now, two security researchers with Malwarebytes examined the uninstaller module, this thing that was delivered by law enforcement to the now-under-their-control Emotet bots. They did this ahead of time, so they changed the system clock on a test machine to April 25th, 2021, to this trigger moment and confirmed that it only deleted associated Windows service definitions and autorun registry keys, then terminated itself. It leaves everything else on the compromised devices untouched. They did this because, as we saw with the FBI's Exchange Server decontamination that we talked about a couple weeks ago, messing with somebody else's computer is a concern.

Marcus Hutchins, whom we know well on this podcast, has tracked Emotet and other botnets for years. Marcus warned that anyone whose machines were infected should be careful to clean their systems despite the Emotet takedown. He cautioned that they could still be hit with secondary malware that Emotet's partners may have previously downloaded into their computers like Trickbot or Qakbot. So anyway, people are still feeling a bit touchy about the idea of law enforcement being this proactive.

So I suppose this is going to be take some getting used to. As I mentioned, the FBI's subsequent disinfection of U.S.-based Exchange servers was not without controversy. And in this case, not everyone was completely bullish, even on the Emotet takedown. Malwarebytes' CEO told BleepingComputer in an interview: "For this type of approach to be successful over time, it will be important to have as many eyes as possible on these updates; and, if possible, the law enforcement agencies involved should release these updates to the open Internet so analysts can make sure nothing unwanted is being slipped in."

Well, it's nice to wish for that. On the other hand, it really needs to be done in secret because secrets are very difficult to keep. One of the stories I had hoped to get into today's podcast, but I'll catch up with it next week, there just wasn't room, is Microsoft's serious concern that it was their sharing with their industry-wide partnerships that may have led to the early leak of the details of the Exchange Server flaws, which is responsible for it getting loose before they had patches ready. Anyway, we'll talk about that next week.

But that all said, the Malwarebytes CEO said: "We view this specific instance as a unique situation and encourage our industry partners to view this as an isolated event that required a special solution and not as an opportunity to set policy moving forward."

Again, as I said, the concern when this all surfaced about what the FBI did and even here the concern being voiced is people are not comfortable with law enforcement doing essentially what the bad guys have done. My take is we're going to have to get comfortable with it because otherwise law enforcement's hands are tied, and of course the bad guys' hands are not tied.

Intervention is never something that the intervened welcomes. But it's often the only way to solve a problem. And I suspect we're going to be seeing more of it in the future. The Emotet botnet established itself through highly effective email phishing campaigns. Unwitting users clicked on links, which ran macros to infect their machines. So Emotet was being invited in. If we deliberately tie the hands of law enforcement to prevent this sort of lawful remediation, a very effective means for kicking it out of, in this case, 1.6 million infected machines will be lost.

And I'm not arguing that the Malwarebytes CEO was wrong in saying it absolutely has to be done very, very carefully and safely. For example, you would never want to do something that bricked 1.6 million infected machines. But it's certainly possible to test this, and I'm sure it was tested extensively before it was actually done for real. So, yeah, it's dicey, but I think it needs to happen.

So, okay. Among the things that the Emotet botnet was doing was acquiring email addresses. And in a related public/private partnership, the Dutch authorities and the U.S. FBI have provided, get this, 4,324,770 unique email addresses known to have been compromised and used by the Emotet botnet to Troy Hunt's Have I Been Pwned database service. Here's what Troy had to say about this last Tuesday.

He said: "Earlier this year, the FBI, in partnership with the Dutch National High Technical Crimes Unit (NHTCU), the German Federal Crime Police Office (BKA)" - and I can't pronounce that B in German. I looked it for a while, and I thought, no - "and other international law enforcement agencies brought down what Europol referred to as the world's most dangerous malware: Emotet. This strain of malware," writes Troy, "dates back as far as 2014, and it became a gateway into infected machines for other strains of malware ranging from banking trojans to credential stealers to ransomware. Emotet was extremely destructive and wreaked havoc across the globe before eventually being brought to a halt in February."

He said: "Following the takedown, the FBI reached out and asked if Have I Been Pwned might be a viable means of alerting impacted individuals and companies that their accounts had been affected by Emotet." He said: "This isn't the first time HIBP has been used by law enforcement in the wake of criminal activity, with the Estonian Central Police using it for similar purposes a few years earlier. In all, 4,324,770 email addresses were provided which span a wide range of countries and domains. The addresses are actually sourced from two separate corpuses" - would that be corpi? Anyway, "corpuses of data obtained by the agencies during the takedown."

First, email credentials stored by Emotet for sending spam via victims' mail providers. Okay. So among other things, Emotet was a spam agent; right? It sat on victims' computers and used their configured email providers to send out the phishing emails to others. And of course oftentimes it would also compromise their address book, so the email that was outgoing appeared to be coming from people that its recipients knew, meaning the infected victim. And the second source was web credentials harvested from browsers that stored them to expedite subsequent logins. And of course that's something that's always made me a little uncomfortable about storing authentication information in our web browsers is that let's hope that bad guys don't figure out how to get in there.

So Troy wrote: "We discussed loading these into HIBP" - "we" meaning he and the FBI and Dutch authorities - "as two separate incidents so they could be individually identified.

But given the remediation is very similar, they've been loaded in as a single breach." One of the cool things about Troy's Have I Been Pwned is it identifies which breach was associated with the various pieces of information. So, okay, so at this point in Troy's blog I'm skipping the standard "change your password" advice and so forth. He has all that. But I wanted to quote one interesting tidbit that he wrote. He said among his things to do to keep yourself secure was: "Keep security software such as antivirus up to date with current definitions." Troy Hunt wrote: "I personally use Microsoft Defender, which is free, built into Windows 10..."

Leo: Interesting, oh.

Steve: Yes.

Leo: Yeah, I agree with him, but that's really good to hear him say it.

Steve: Yup. And our listeners know that's what you and I have come down finally, Leo, is that it's just...

Leo: You don't need anything more. You just...

Steve: And other things cause more trouble than they're worth.

Leo: Exactly, yeah.

Steve: Yeah. Anyway, he said, so it's free, built into Windows 10, and updates automatically via Windows Update. So that's an interesting data point from Troy. He concluded: "I've flagged this incident as 'sensitive' in HIBP" - again, Have I Been Pwned - "which means it's not publicly searchable. Rather, individuals will either need to verify control of the address via the notification service or perform a domain search to see if they're impacted." And I'm going to explain all that. He said: "I've taken this approach to avoid anyone being targeted as a result of their inclusion in Emotet. All impacted HIBP subscribers have been sent notifications already."

Okay. So the normal thing you do is for non-, what did he call it, sensitive, for non-sensitive issues is you put your email address in, and that's all that you have to do. You click Have I Been Pwned, and it says no, there's nothing here. But of course that allows you to put any email address in, and thereby use Have I Been Pwned to probe whether that email address may have been used in previous attacks. They didn't want to do that here. So there's two URLs. Have I Been Pwned, of course, is H-A-V-E-I-B-E-E-N-P-W-N-E-D dot com. So you do /NotifyMe. That's the standard single email address signup. I've signed up using, before I did the next thing, which was even cooler, I put in a couple of my recent email addresses.

Leo: This isn't the wildcard one. This is just a regular address.

Steve: Correct, yeah.

Leo: Okay, got it.

Steve: This is for people who do not have control of their own domain. So like if you're a Gmail user, or Yahoo, or your own local ISP, but not this is my domain dot com. Then you use this. So you put your email address in, or any that you have been using recently, or back through time, I would say any that still matter, because it needs to be an address on which you still receive email because, when you put it in, you receive at that address a confirmation email which you have to click in order to confirm. And when you click, it takes you back to Have I Been Pwned with the results of whether or not that email address exists in any of the Have I Been Pwned databases, including this one. So again, HaveIBeenPwned.com/NotifyMe.

Okay. One thing Troy did not mention in his blog posting, but I saw it elsewhere, was that 39% of the email addresses provided by law enforcement from the Emotet takedown had already been indexed as part of other data breach incidents. So nearly 40%, 39% of email addresses weren't being well-managed by their users, and they'd already been participating in breach events.

Okay. Now, the domain-wide notifications is very cool. So it's the ability to provide domain-wide notification of any and all past and future breaches. So, for example, TWiT.tv or GRC.com. What I did was I created an alias, a notification alias, because I use aliases a lot since I control my own email server. I created a permanent notification alias where I will receive notices. And, okay. So when I registered, I immediately, as I said, received a sobering list of 155 email addresses.

But first I'll explain about registration. I would strongly recommend that anybody who has control of their own domain should register with this service. I just can't imagine why you wouldn't. If you want to, create an email alias for yourself. So you then need to prove control over your domain with - Troy provides four ways: email, web, or DNS. For email, you'll need to be able to respond to an email sent to, and you get to choose, security at your domain, hostmaster at your domain, postmaster at your domain, or webmaster at your domain.

Or you can add a custom meta tag to the root web page at your domain. And it's, you know, <meta name="have-i-been-pwned-verification" value="long unique token that he provides">. Or you can place a file named "have-i-been-pwned-verification.txt" onto the root of the domain containing a specific verification text string. Or you can add a specific text record to your domain's DNS of the form "have-i-been-pwned-verification=blah blah blah," you know, that same unique string.

And then when you've done one of those, you then say "verify me." And Troy's server will go out, look at your home page, go try to grab that text file from the root of your website, pull a DNS query of your text records and see if the verification string is there, or send you email to one of those four addresses, which you then confirm.

So I did that. And as I mentioned, after regaining control of my cardiac sinus rhythm following seeing 155 email addresses within the GRC.com domain - oh, and he provides them as a web page on his site, as a spreadsheet, somehow I got it as a spreadsheet, or as a JSON file. So you can get it in any of three formats. I settled down to see what was being seen. With a domain like GRC.com, which has been around for so long and which has earned a strong reputation for never having been a source of spam, it's desirable for use by people who are trying to spoof email addresses because they just figure they'll be taken more seriously. So it appears that individuals or bots have used a bunch of always bogus GRC.com "accounts," in quotes, that have never belonged to us, and for which email has never been sent or received. But at the same time, that list also contains a bit of a walk down memory lane.

Leo: I don't know if I want to open this.

Steve: Uh-huh.

Leo: Oh, boy. Do it off camera, yeah.

Steve: That's right.

Leo: Oh, look at that. No results found. But not for TWiT.tv. Not for TWiT.tv. I was using my own personal domain.

Steve: Oh. Oh, oh, oh, okay.

Leo: Which that would make sense nobody would be - that's why I'm not showing it on the screen. Nobody knows what it is.

Steve: Right, right, right. So I found chromazone@grc.com.

Leo: Love it.

Steve: Which, you know, that was an email address I used a long time ago.

Leo: Oh, it was a real address, though. Wow.

Steve: Oh, yeah, because Chromazone was the way I taught myself Windows. I wrote that beautiful, if I do say so myself...

Leo: Oh, I remember that, yeah.

Steve: That screen saver. At the time that flying toaster screen saver, can't remember the name of it...

Leo: Flying Toaster.

Steve: After Dark.

Leo: After Dark, yeah.

Steve: After Dark. They had, I don't remember now how many, like it was megabytes in size, and you got 11 screen savers. Mine was, I think it was a few hundred K, and it came with 400 screen savers because it was a screen saver construction set. I provided you with this editor that allowed you to define and design your own screen savers. Anyway, I called it, of course, Chromazone because it was very colorful. And Troy's site showed that River City Media Spam List and Verifications.io were two breaches where that email address was disclosed.

Also cih@grc.com. That was the virus; remember? CIH was that virus which wiped out the first megabyte of people's hard drives. And I didn't want to charge anything to fix it because it wasn't anybody's fault. So I wrote a custom tool which basically resurrected the entire first megabyte of someone's hard drive in order to reverse the effects of that. Also cod@grc.com. That was the way you and I first met, Leo, Click of Death.

Leo: Oh, yeah. Yeah, yeah.

Steve: Yeah. And so that one was exposed in the Data Enrichment Exposure From PDL Customer. Also the River City Media Spam List and Verifications.io. Not surprisingly, greg@grc.com. We have not used our first names at GRC.com for years. Once upon a time I was steve, Greg was greg, and Sue was sue. But you just can't use a first name at any domain.

Leo: First name, short first name, bad.

Steve: Yes. So, and Greg was there because he would be responding as a tech support provider. Therefore his address would be in all of the email boxes of all of our customers. And so, yeah, it just got loose. Also s.gibson@grc.com. I don't remember ever using that, but I guess I must have. Sgibson@grc.com. Sales@grc.com. Steve, as I mentioned, and Sue. So anyway, so but those, what, one, two, three, four, five, six, seven, eight, nine, there were nine real ones out of 155.

Leo: So the rest were just like joe@grc.com and stuff.

Steve: Exactly. And we never had a Joe. And aaa@grc.com, and just random crap. So anyway, very interesting. And again, the beauty of registering domain-wide is now, if any email address I'm using or Sue's using or Greg's using appear newly in Have I Been Pwned, I will receive a proactive notification saying, hey, this email address for your domain just got breached. So that's super cool. And I would imagine it would be of use to any of our listeners who are responsible for their own enterprise's email.

We know I don't like QNAP. I started off being...

Leo: It's funny because they're really big. And I think people like them. But I'm glad I use Synology after hearing all about this.

Steve: Boy, are you glad, Leo.

Leo: Yeah, yeah.

Steve: You don't know how glad you are.

Leo: Yeah.

Steve: Yeah. I've said it before, but sadly it's worth reminding everyone due to recent events. At this point I'm pretty sure that I will never like nor recommend the use of QNAP's products for any purpose. Maybe if you needed an anchor for your fishing boat, you know, because if it dragged along the bottom it would be pretty good to hold your boat in place.

Leo: That and your bitcoin hard drive, you're set. Sorry.

Steve: Ouch. So time and again the company has demonstrated itself to be just too irresponsible. They have a well-established track record of ignoring security researchers' reports, despite the researchers' responsible attempts to get them to respond within like 90 days or a reasonable length of time. They just do nothing until there's like a catastrophic event affecting their users. Nor do they fess up when they're confronted with reality. They obliquely referred in this instance to a "improper authorization vulnerability in HBS 3," which is their Hybrid Backup Sync offering. Well, it certainly is.

But it would be more correctly described as yet another hard-coded firmware backdoor credential that was discovered as they will all inevitably be. And it's been widely exploited by multiple breeds of ransomware, where there is now a feeding frenzy competition to see which can be the first one to get in and encrypt all of a user's data. Despite only asking 500 USD equivalent in bitcoin for the decryption key, there's clearly no safe way to have any QNAP device publicly exposed to the Internet. And now QNAP themselves have begun recommending that their own users should not run on the default port of 8080, but should rather attempt to hide their services elsewhere.

Leo: That's no good. That's terrible.

Steve: I know. Among the 65,000 other ports because, that's right, if you can't make it secure...

Leo: Just hide it.

Steve: ...then at least make it obscure.

Leo: Yeah. Oh, god.

Steve: No, thank you. No, thank you.

Leo: That's not a solution. The fact that they even suggested that tells you they have no good fix.

Steve: Yes. And they actually do say, you know, put it somewhere else. Boy. Yeah.

Leo: Yikes

Steve: So last time we talked about this I said, if you must use it, if you've got the hardware, move it inside. Don't expose any of it to the public Internet.

Leo: You'd be safe then; right? I mean, because it's, you know...

Steve: Safer, yeah. And if there's alternative firmware, I don't know if there's like a different way, if you can run FreeBSD or Linux. I would say, if you own the QNAP hardware, dig around, see if you can put a real operating system on it and still get the benefit of its mass functions. That would be a cool solution, if that's possible.

Okay. I did want to mention to our listeners that since last week I updated the Gravity Windows NNTP Newsgroup Newsreader. It was at 3.0.10. It's now 3.0.11. Somewhere last week somebody posted a screenshot from their, shoot, I want to say Unisys, or Unison, from their Unison newsreader, which crashed Gravity. A number of us who are Gravity users clicking on the link, it just terminated. It just disappeared from the screen. It turns out there was a bug in the multipart MIME decoder. So I spent an enjoyable couple hours digging into the source, finding the point that was crashing as a consequence, I mean, there was nothing wrong with what the Unison newsreader was posting. Gravity just had a mistake.

So I fixed it. Just wanted to let our listeners know. There's now two entries over in GRC's files page, our freeware page, and also on the discussions page, one for a full new install of Gravity, which now incorporates this new update, and also just Gravity EXE, which is only the updated, because it's only one file that changed. So if you already have Gravity installed, just grab the EXE and move yourself to 3.0.11.

And as I promised, something fun I had to share about Dan Kaminsky. I know we spent plenty of time remembering him last week. But this anecdote from his early life came up that I knew our listeners would appreciate. As we know, Dan was a respected practitioner of pen testing, right, penetration testing being the art of compromising the security of computer systems at the request of their owners who wisely wish to harden their systems from attack by inviting a skilled hacker like Dan to see whether that skilled hacker is able to get in.

According to Dan's mom, Trudy Maurer, M-A-U-R-E-R, he began developing his knack - now, of course this is coming from a mother's loving eyes - when he was a four year old in San Francisco after his father gave him a computer from Radio Shack. We don't know that it was a TRS-80, but one imagines. She said by the age of five he had taught himself to code. And at one point his childhood paralleled "War Games," which of course we all remember the 1983 movie starring then teenage Matthew Broderick, who unwittingly accesses a U.S. military supercomputer. Well, it turns out...

Leo: "Shall we play a game?"

Steve: What was the name of it? It was a...

Leo: WOPR.

Steve: WOPR, yes, WOPR. When Dan, his mother says, was 11, she received an angry phone call from someone who identified himself as a network administrator for the Western United States. The administrator said someone at her residence was "monkeying around in territories where he shouldn't be monkeying around." It seems that Dan had been examining military websites. The administrator vowed to punish him by cutting off the family's Internet access. Mrs. Maurer warned the administrator that, if he made good on his threat, she would take out an advertisement in the San Francisco Chronicle denouncing the Pentagon's security. Mrs. Maurer recalled telling the administrator, "I will take out an ad that says, 'Your security is so crappy, even an 11-year-old can break it.'" They settled on a compromise punishment: three days with no Internet.

Leo: What a good mom. I love it. She stood up for her kid. That's great.

Steve: She said, okay, yup. And actually she's a CEO, so I would imagine that, yeah, it's probably being remembered correctly. Several decades later, after Dan's comprehensive presentation in August of 2008 at Black Hat of the DNS meltdown that his work and then the industry's work were instrumental in avoiding, he was approached by a stranger from the Black Hat audience. It was the administrator who had caused him to lose three days of Internet access when he was 11. He wanted to thank Dan personally, and to ask for an introduction to "the meanest mother he ever knew."

Leo: For purposes of pen testing?

Steve: Anyway, very cool story.

Leo: Oh, I see what you're saying. The meanest mother, his mom.

Steve: Yes. His own mom.

Leo: I know, okay, I was extending the word "mother" beyond the point.

Steve: Right. His actual mom.

Leo: His actual mom, yes. Now I get it.

Steve: Yes, yes. Yeah, he had never forgotten that he got chewed out by the 11-year-old hacker's mother.

Leo: Yeah, don't mess with mama. Isn't that great?

Steve: And backed down to...

Leo: Yes, ma'am. Yes, ma'am. How about three days, ma'am?

Steve: She'll tell him he can't play with his computer over the weekend.

Leo: Yeah, I think - so many great stories about Dan, of course, upon his death, and that's one of them. We actually talked about it on Sunday. He had a great mom. She deserves credit.

Steve: So two pieces of closing-the-loop feedback. Makdaddy sent: "@SGgrc Please don't fancy up SpinRite 6.1 UI. We love the simplicity of ASCII characters for UI. It's super retro and uber cool."

Leo: Super AND uber. Whoo.

Steve: Okay. And I don't know whether something I said may have given the impression that I might be changing anything. I guess that I was talking about updating a bunch of SpinRite screens with the additional data that SpinRite now has available, and that I've also added some new stuff. And I did note that earlier I was worried that those familiar with SpinRite 6 might not notice anything new and different, but that that was no longer any worry. But for what it's worth, I'll definitely be keeping SpinRite's longstanding textual UI.

It's not that I couldn't do or that it couldn't do with a major rework and a move to a bitmapped interface from this century, but mostly that SpinRite is all about performance rather than appearance. If I could have both in the same timeframe, sure. That would be great. But given a choice, since what we have now for a UI works, what it does is the only thing I'm focused on. So, yeah, we get to keep our what did he call it, super retro and uber cool user interface.

Leo: It's actually kind of all the rage in Mac and Linux and Unix communities. They call it a TUI, a Text User Interface. And I have a lot of TUI apps instead of GUI. You don't have all that overhead of a window manager and all that stuff. And it's perfectly informational. It works great. And I agree. I think you've done a good job, that it's really easy to understand. You use colors really well. A lot of the TUIs I use don't use colors nearly as well.

Steve: Yeah, it is really colorful, yeah. Secondly, Henrik Schack said: "Hey, long time ago you talked about a very, very long sci-fi series, currently," he said, "14 to 15 books, supposed to be 50 plus."

Leo: Oh, I know what you're talking about.

Steve: Yup. And so does JammerB. He said: "I have forgotten the name. Can you help?" So we haven't talked about sci-fi much recently, mostly because I've been stuck on my current absolute favorite series, which is what Henrik was asking about. It is, of course, The Frontiers Saga by Ryk, spelled R-Y-K, Brown. And I'll just say that it's a straight-up unapologetic space opera. It's wonderful pulp sci-fi. But what I think distinguishes it from so many others is that it's written well enough that I never find myself wincing. A book I

was reading years ago kept referring to the "stygian" blackness of space. And that would have been fine once. But this author apparently had no other word for black.

Leo: Yeah, no, sorry, such a clich.

Steve: So he kept using "stygian." And it just - it became tiresome very quickly. Ryk has a real talent for creating very clear and very well-defined characters. And once they've been established, he never - and for me this is critical - he never asks them to do something they wouldn't. Since reading science fiction, or any fiction, is all about building an alternative reality model, the last thing you want is for characters who have been so well and carefully crafted to act out of character.

So anyway, it's just a joy to read this. The Frontiers Saga is one continuous story, or the planned saga. I hope he has a chance to finish it. It's in five broad arcs of 15 books each. So far, the first two 15-book arcs have been completed and published. And I've read all 30. I've re-read the beginning set while waiting for the second set. And I'll confess that I am currently rereading them all again. I love to read. And as I reread them, knowing what's coming and how significant this or that newly introduced character will wind up being is fun. It's neat watching everyone else getting to know them for the first time.

Ryk was hospitalized due to complications from COVID-19, which I was worried may have thrown off his schedule a bit. But he's been working all year. As it happens, he just posted this May 4th morning, stating, he says: "I guess I'd better say something, lest I find my picture on the side of a milk carton." So followed by a summary of what's going on, which he posted. Anyway, he's wrapping up a standalone novel, which will be titled "The Fall of the Core," and then plans to have the third series begin, starting to appear this summer. He likes to have a few written ahead of time so that he can sort of do an every three to every four month rate. He started in 2011, so basically 10 years ago. He's got 30 books out in that period of time. So, what, he does three a year, so about one every four months. He was also quite - what?

Leo: Nothing. That's just a lot of books. It's a lot of writing.

Steve: It's a lot of writing. And that's why I hope he does it, like...

Leo: It's the Augean stables where the, yeah, okay, the labors of Hercules.

Steve: I hope he doesn't, like, burn out on this because he's got a bunch of threads which I would love to see him tie up. He was also quite unhappy with his books being available through Amazon's Kindle Unlimited plan. So he has stated that only these first two 15-book arcs, meaning a total of 30, will be there. I'm sure I'll buy them wherever they appear, though I hope Amazon will be able to at least offer them for sale, if not as part of their Kindle Unlimited plan, since Kindle is far and away my preferred reading platform. For the time being, for those who don't know, all of those first 30 books are free to read as part of the Kindle Unlimited plan, which is $10 per month, and authors are reimbursed...

Leo: Means he gets nothing. Right? How much does he get? Nothing.

Steve: Well, I looked. And it looks like maybe a 10th of a penny per page read.

Leo: Oh, geez. Oh, per page. Well, he's written many thousands of pages, so that ain't bad.

Steve: Yes.

Leo: That's all right. Okay.

Steve: Yeah. So anyway, I will post a note, I mean, I'll just make a note. I'll let our podcast listeners know so that JammerB doesn't miss it when the third series begins. But it's not going to be for a few more months.

Leo: Brett in our chat room is suggesting that he gets paid by the word, and that may be the case. I don't know.

Steve: No. I did look. I did look. And the Kindle Unlimited plan makes the royalty reimbursement system very clear. What I did find interesting, though, it isn't books you check out. It's books you actually page through.

Leo: So you have to - yeah, that's why it's by the page. Yeah, that makes sense.

Steve: By the page read.

Leo: That makes sense. So is there a series we should search for? That'd probably be the fastest way to find it; right? Search by series? Because you want to get the first book.

Steve: Oh, yeah, yeah. You have to. It's called "Aurora" is the very first book. But if you just google "The Frontiers Saga."

Leo: Frontiers Saga, Aurora.

Steve: Frontiers as plural. Well, yeah, the Frontiers Saga, Aurora. And I just, you know, I didn't want to take too much time on this, so I sort of rushed through it, but it is really good. I mean, it's not Peter Hamilton; right? That's a caliber all on its own. On the other hand, Peter's books, I will never reread whatever it was he just last put us through because it was a lot of, like, do I care that the guy's buttons, like the third button down he missed, and he needs to polish it? No. I really don't need to know that. So there's no unnecessary detail. But really fun characters.

So, you know, top recommendation: The Frontiers Saga. And of course we've talked about Hamilton and Michael McCollum and the Honor Harrington series. And I enjoy, I guess, reading series, and I'm seeing that that's being done a lot more recently. I think authors like to get you looped in on a series so that you stay with them. And it's just

comfortable being able to continue reading about people you know. And he doesn't spend any time at all, he assumes you are reading this in sequence. You don't, you know, there's no time spent bringing you back up to speed over everything you missed before.

Leo: And you should start at the beginning, obviously. Yes?

Steve: Oh, absolutely. Yes, yes, yes.

Leo: So there are sets. What is the meaning of the sets, then?

Steve: So like the first 15-book set, if you - I know.

Leo: Not a trilogy. It's a quintilogy. Okay.

Steve: It's a "You can't even -ilogy this." When you're done, you're done. But there's a bit of sadness at like the end, and you think, well, wait a minute.

Leo: I want more, yeah.

Steve: Couldn't there be more?

Leo: Oh, there is.

Steve: And what do you know.

Leo: Fifteen more, kids.

Steve: Yes. And when the second or third book is titled "Resurrection," it's like, oh, I think I know maybe what is going to happen here. So, yeah. Anyway, top recommendation.

Okay. So the Ransomware Task Force. The Wall Street Journal and CNN appear to have been the first to obtain and report on a U.S. Justice Department memo which first disclosed the creation of this new task force dedicated to responding to the growing threat of ransomware. Given the maturity of the task force's first 81-page report, selected parts of which I'll be sharing shortly, this appears to have been in the works for some time. And needless to say, it's quite needed. Whether it'll be able to do any good, as I said at the beginning of the show, we'll see, and certainly hope. The question is, although a task force sounds wonderfully proactive, what can it actually do?

CNN explained that the new initiative follows what the memo describes as the worst year ever for ransomware attacks. Of course it coincided with COVID-19 that was the worst year ever for health attacks. It highlights how cybersecurity threats in general have become a major focus of the current administration following other recent high-profile network security incidents such as the now believed to be Russian-backed SolarWinds

hacking campaign and of course the Microsoft Exchange Server vulnerabilities that Microsoft has attributed to Chinese hackers. More recently, it's believed that Chinese hackers exploited vulnerabilities in Pulse Secure's VPN to compromise dozens of agencies and companies in the U.S. and Europe.

In a memo from Acting Deputy Attorney General John Carlin to DoJ department heads, U.S. attorneys, and the FBI last Tuesday, he said: "Although the Department has taken significant steps to address cybercrime, it is imperative that we bring the full authorities and resources of the Department to bear to confront the many dimensions and root causes of this threat."

So this new task force will pull together and unify efforts across the federal government to pursue and disrupt ransomware attackers. And to that I say good luck to you. Actions could include everything from takedowns of servers used to spread ransomware to seizures of these criminal enterprises' ill-gotten gains to the degree that's possible. We'll be talking about that a little bit more in a second. In addition, the DoJ plans to devote more resources to training and intelligence sharing, as well as reaching out to the private sector more than they have to gain insight into ransomware and extortion threats. As we know, during the past few years, ransomware attackers have increasingly targeted schools, hospitals, city governments, and other victims that are perceived to have weaker security or to have an ability to pay.

Brian Krebs covered this news also, and he opened with: "Some of the world's top tech firms are backing a new industry task force focused on disrupting cybercriminal ransomware gangs by limiting their ability to get paid, and targeting the individuals and finances of the organized thieves behind the crimes." Brian continued: "In an 81-page report delivered to the Biden administration this week, top executives from Amazon, Cisco, FireEye, McAfee, Microsoft, and dozens of other firms joined the U.S. Department of Justice, Europol, and the U.K. National Cyber Crime Agency in calling for an international coalition to combat ransomware criminals, and for a global network of ransomware investigation hubs.

"The Ransomware Task Force," he wrote, "urged the White House to make finding, frustrating, and apprehending ransomware crooks a priority within the U.S. intelligence community, and to designate the current scourge of digital extortion a national security threat. An internal DoJ memo reportedly 'calls for developing a strategy that targets the entire criminal ecosystem around ransomware, including prosecutions, disruptions of ongoing attacks, and curbs on services that support the attacks, such as online forums that advertise the sale of ransomware or hosting services that facilitate ransomware campaigns.'"

So according to security firm Emsisoft, whom we've quoted before, almost 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware in just last year, 2020. The task force report observes: "The costs of ransomware go far beyond the ransom payments themselves. Cybercrime is typically seen as a white-collar crime; but although ransomware is profit-driven and non-violent in the traditional sense, that has not stopped ransomware attackers from routinely imperiling lives." And of course we were just talking about last weekend's Scripps attack that brought down four hospitals and all of their ancillary satellite-related services.

Okay. So let's plow into the report to see what this task force is planning. The 81-page document published by the IST, the Institute for Security and Technology's Ransomware Task Force, is titled "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force." And I have to say that the framework is indeed comprehensive. Not that it may make any difference, but okay. We know clearly after looking at this what the problem is. It does demonstrate a lot of

thought and that work has been going on behind the scenes to get the project to this point. So it is not an empty 81 pages.

It opens with a framing statement that's meant to lay out the problem and the scope of the report's effort. It's not long. This is what it has to say. It says - and there was like, I think it was an eight-member committee of mostly industry who wrote this. So they're speaking collectively, saying: "We're honored to present this report from the Ransomware Task Force. This report details a comprehensive strategic framework for tackling the dramatically increasing and evolving threat of ransomware, a widespread form of cybercrime that in just a few years has become a serious national security threat and a public health and safety concern."

They wrote: "Ransomware is not just financial extortion. It is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the healthcare industry during the COVID pandemic and has shut down schools, hospitals, police stations, city governments, and U.S. military facilities. It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction.

"Tackling ransomware will not be easy. There is no silver bullet for solving this challenge. Most ransomware criminals are based in nation-states that are unwilling or unable to prosecute this cybercrime. And because ransoms are paid through cryptocurrency, they're difficult to trace. This global challenge demands an 'all hands on deck' approach, with support from the highest levels of government. Countless people around the world are already working tirelessly to blunt the onslaught of ransomware attacks. But no single entity alone has the requisite resources, skills, capabilities, or authorities to significantly constrain this global crime enterprise.

"For this reason, we convened the Ransomware Task Force a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, nonprofits, and academic institutions to develop a comprehensive framework for tackling the ransomware threat. Our goal is not only to help the world better understand ransomware, but to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions, many of which can be immediately implemented by industry, government, and civil society. Acting upon only a few of these recommendations will not likely shift the trajectory, but the task force is confident that implementing all of them in coordination, with speed and conviction, will make a significant difference.

"While we have strived to be comprehensive, we acknowledge that there will be areas we have not addressed, or on which we could not come to consensus. Prohibition of payments is the most prominent example. The task force agreed that paying ransoms is detrimental in a number of ways, but also recognized the challenges inherent in barring payments. Just as we have been grateful to stand on the shoulders of those that came before us, we hope our efforts and investigations will fuel the thinking and recommendations of those who come after.

"We urge all those with the ability to act to do so immediately. The ransomware threat continues to worsen by the day, and the consequences of waiting to respond could be disastrous. More than money is at stake. Lives, critical infrastructure, public faith in the legitimacy of our institutions, the education system, and in many ways our very way of life depend on taking action. As a final note, we would like to offer our sincere thanks to the members of the Ransomware Task Force, who responded to our call and generously dedicated their time and energy into developing the recommendations included in this report."

Okay. So that's nothing we would not expect. This introduction was followed by an executive summary which I'm going to spare everyone from enduring. It added very little and was largely repetitive. The report does contain an interesting and informative infographic. It pretty much leads with it. This shows three or four factual bullet points. The average downtime due to a ransomware attack is 21 days.

Leo: Yikes. Yikes.

Steve: I know.

Leo: That's a lot of downtime.

Steve: That is, what, three weeks; right? Which means some people get up quicker. Some people get up longer. But three weeks of outage.

Leo: That's really a long time to be out of business.

Steve: Yeah. The average days it takes for a business to fully recover from an attack, 287 days. So, what, like two thirds of a year.

Leo: That's amazing.

Steve: To fully recover.

Leo: Yeah, nine months, yeah.

Steve: Victims paid in ransom in 2020, which is a 311% increase over the prior year, the average amount paid - or, no, I'm sorry, the total amount paid in 2020, $350 million.

Leo: Yeah. And the bigger that is, the more you're going to get because it's lucrative.

Steve: Yes. Talk about incentive. Boy. And here's the average payment in 2020, which represented a 171% increase over 2019, the average ransom, $312,493. So a little over $300,000 paid in ransom.

Leo: And of course this task force is not recommending you pay. This is all about how not to pay.

Steve: Correct.

Leo: How not to get bit. And then, if you do get bit, how to remediate. And I think that needs to be done. I mean, is this for government companies, or is it for everybody?

Steve: So it's largely a call to action. It's sort of like the first steps for beginning to move on this. This went to the Biden administration, an 81-page report. And it has three levels of hierarchy of action items and bullet points that, again, I'm going to spare our listeners because it's what happens when you have a bureaucracy. But I would argue you can't get started without this.

Leo: It needs to be done. It absolutely has to be done.

Steve: Yes. So I scanned the entire report, and I have pulled out some of the most interesting pieces. When we began this podcast, you and I, Leo, nearly 16 years ago, thanks to your insight that this might be something useful, extracting payment from a victim and receiving it without exposure was an unsolved problem for cybercriminals. Sending cash to Russia by Western Union was what we typically saw. And we talked about it on the podcast. But as we know, that was then.

And it occurred to me some time ago, we talked about it, we've noted it a couple times on the podcast, that the rise of cryptocurrency exchanges, which support both submitting and extracting payments in local non-cyber currencies, or so-called "fiat" currencies, coupled with the inherent anonymity of the blockchain's wallet designations, has been an enabling factor in the growth of ransomware. And they touch on that in the report, that the task force agrees.

But it turns out there's much more to it than I knew or than we've ever discussed. Here's what the report explains about the role of cryptocurrency and the complexities its use introduces. They said: "The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions. The use of cryptocurrency adds to the challenge of identifying ransomware criminals, as payments with these currencies are difficult to attribute to any individual. Often the money does not flow straight from ransomware victim to criminal. It travels through a multistep process involving different financial entities, many of which are novel and are not yet part of standardized, regulated financial payments markets.

"Ransomware criminals typically demand that victims send their ransom payments via Bitcoin; but after receiving the payment in a designated digital 'wallet,' the criminals typically obfuscate these funds as quickly as possible to avoid detection and tracking. Their methods include 'chain hopping,' which involves exchanging funds in one cryptocurrency for another using any of a variety of cryptocurrency exchanges. The funds can be extremely difficult to trace after they have been exchanged. And to further shield themselves, ransomware actors may use 'money mule' service providers to set up accounts, or use accounts with false or stolen credentials.

"Ransomware criminals can also obscure their transactions through cryptocurrency 'mixing services,' which muddy the public ledger by mixing in legitimate traffic with illicit ransomware funds. Some groups will also demand payments in currencies known as 'privacy coins,' such as Monero, that are designed for privacy and make payments untraceable. However, privacy coins have not been adopted as widely as might be expected because they are not as liquid as Bitcoin and other cryptocurrencies; and, due in part to regulation, this payment method may become increasingly impractical.

"Cryptocurrencies," they wrote, "add to the challenge of ransomware because they are considered to be 'borderless.' The cryptocurrency community is expressly focused on building a set of technologies designed to reduce compliance and financial processing costs. After obfuscating the extorted funds, ransomware criminals may either withdraw the funds into hard cash or, because cryptocurrencies have become increasingly common and their value has been steadily rising, they may keep their profits in cryptocurrency and use them to pay for other illicit activities.

"While cryptocurrencies are difficult to trace, blockchain analysis can help interpret public blockchain ledgers. And with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies are able to show that a given transaction took place between two different cryptocurrency exchanges, for example, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. Within blockchain analysis tools and Know Your Customer (KYC) information, law enforcement can gain transparency into blockchain activity in ways that are not possible in traditional finance."

So clearly the rise of cryptocurrency, this solves the Western Union loophole or catch that used to be a problem. It's just not so much anymore. Still, it's not as if transferring to bitcoin, as we see, means that it drops into a black hole. We have seen and we've talked on this podcast about how the movement of cryptocurrency from one chain to another can be traced, and how it dropping out of specific wallets can also be seen. What the blockchain is, right, is a transactional ledger which is secure and cannot be spoofed, yet that means it cannot be spoofed. And if you want to get your coin out of a wallet, it will appear on that ledger in order for that to happen.

The report discusses also the rise of RaaS, Ransomware as a Service, that threat model and problem. The report observes that: "Carrying out a ransomware attack does not require technical sophistication. Ransomware as a Service is a business model that provides ransomware capabilities to would-be criminals who do not themselves have the skills or resources to develop their own malware."

Leo: They've made a good start just taking down some of those; right? Those are probably pretty easy to get rid of.

Steve: Right. I did note, I didn't have it in the show notes, but apparently there are some dark websites where law enforcement has begun to post in the dark web forums little warning notes, like sooner or later you're going to make a mistake. We'll be waiting. So it's just to add a little bit of a creep factor. And I'm sure it's like on its face it's blown off. But at some point, as they do make arrests, and I forgot to mention that as part of the Emotet takedown there were individuals in Ukraine who were arrested as part of this. So some of the people behind the Emotet botnet are currently arraigned, and they're moving through the local justice system for them.

In 2020, two-thirds of the ransomware attacks analyzed by the cybersecurity firm Group-IB were perpetrated by cybercriminals using the Ransomware as a Service model. Two-thirds. So this model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from Software as a Service and Infrastructure as a Service in the traditional, on the Internet. It's like, hey, that works. Let's try it. And we've talked about how successful it is.

They wrote: "In the RaaS model, there are at least two parties who establish a business relationship, the developer and an affiliate. The developer writes the malicious program that encrypts and potentially steals the victim's data. The developer then licenses this

malware to the affiliate for a fixed fee or a share of successful ransom payments. The affiliate executes the attack, potentially also including additional business arrangements like purchasing exploits or using cryptocurrency brokers and washers."

And they conclude: "In this model, even a non-technical affiliate can successfully execute ransomware attacks by purchasing the necessary exploits and malware. RaaS can be contrasted with more traditional ransomware gangs in which a cohesive team both builds the malware and executes the attack. The Sodinokibi, Phos, Dharma, and GlobeImposter ransomware variants are all known to operate under the RaaS model."

The report had some sobering things to say about nation-state actors. And to me, this seems like the ultimate problem since proactive protection by one's own local government is pretty strong protection. The report wrote: "Of particular interest to the task force was the relationship between ransomware and national governments. Many ransomware criminals operate with impunity, as their countries' governments are unwilling or unable or uncaring to prosecute this form of crime. In other cases, the organizations executing ransomware attacks may be state-sponsored, and may in fact be helping nations evade economic sanctions imposed upon them by other nations.

"For example, in an April '21 announcement" - so just last month - "of new sanctions against Russia, the U.S. Department of Treasury made a direct connection between Russia's Federal Security Service (FSB) and ransomware hackers, noting that 'to bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks'" - right, against the West - "'and phishing campaigns.'" In other words, we're suffering while they're popping champagne corks and in Russia eating caviar and partying.

Anyway, they finish, saying: "Proceeds from ransomware may help finance terrorism, human trafficking, or the proliferation of weapons of mass destruction. For these reasons, direct affiliation between ransomware attacks and governments is intentionally shrouded in secrecy, making attribution and accountability challenging. Countering state-sponsored attackers will require broad application of carrot-and-stick methods and international cooperation." And unfortunately, to that I say, and good luck to us.

As I mentioned, I don't know what you do about that. The report distills what I'm sure must have been endless committee meetings and hearings into just four goals. The four goals are: deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; disrupt the ransomware business model and decrease criminal profits; help organizations prepare for ransomware attacks; and respond to ransomware attacks more effectively.

As I mentioned, it further details each of those four goals with multiple objectives within each goal, each consisting of one or more specific actions. Since I've provided the link to the 81-page PDF in the show notes at the top of this section, I won't drag everyone through the seemingly endless and mind-numbing hierarchical list. But suffice to say that it is truly comprehensive, and it is hopeful.

Long ago on this podcast we observed that for - and we often talked about it, Leo. For a surprisingly long time, hacking was just mischief. Early on here we were covering email viruses, observing that they didn't do anything other than attempt to procreate. They seemed to exist just to spread. And we also bemoaned for quite some while the fact that Microsoft didn't seem to be taking much action against them. So the only conclusion would have been that they must have been created by their authors just to see whether they might work. The first botnets that we reported on were largely benign.

And even way back in November of 1988, Robert Morris launched his famous worm from a terminal at MIT by leveraging a hole in Sendmail's debug mode, coupled with a buffer overflow in the fingerd network daemon. Robert just wanted to see whether it might work. But because it was so much more effective than he expected, it caused far more trouble than he intended. By the way, he ended up being a tenured professor at MIT. But he also got in trouble. He got himself out of it. His dad was at the NSA, so maybe that helped.

Leo: He actually was quite brilliant. Who was I talking to that was good friends with RTM? Oh, I can't remember. But he said this guy was brilliant, yeah, yeah. Go ahead, sorry.

Steve: So compared to when we began looking at and discussing these issues every week, today's cybercrime world is barely recognizable. I mean, I remember talking about like how it used to seem like science fiction. It's like, really? I mean, even the word "cybercrime." Now no one is laughing. It's no longer the realm of speculative fiction. It exists, and it's become nation-state-sponsored, revenue-generating big business. With criminals being protected by their own governments, the ability of law enforcement I'm worried to curtail ransomware seems quite limited. And unlike Emotet, where the threat was diffuse and significant only because of the size of the network, that could be brought down. But ransomware attacks are different. They're significant individually. Individual attacks like against Scripps are significant.

And if the years of this podcast have revealed any truth, it's that we're currently unable to reliably create complex and secure networked systems. We'd like to be able to do that. We just seem unable to. So I'm glad that this ransomware task force exists. But in the absence of full international anti-ransomware cooperation, including those nations that are hostile to the interests of other nations, like China and Russia against the U.S., it's not clear to me that huffing and puffing is going to amount to much.

I mean, I'm glad that a task force has been assembled. It makes sense that it would be. I mean, these things got to be so recurrent that I stopped talking about them on the podcast because it was just, you know, there is a sense of, well, you've seen one, you've seen them all. But the good news is we have an administration that looks like they're willing to take action. There is a carrot and stick. In their sanctions against Russia they did talk about state-sponsored ransomware crime gangs which had been traced back there. So we'll see if some of this can be dealt with. But again, Leo, as you said, we spotted the problem. The problem is it makes money. And it's difficult to stop something that makes money.

Leo: Yeah, yeah. But I think there's all sorts of things a task force could attack besides the Ransomware as a Service, which clearly makes it way too easy for any idiot to do this. You should have a certain level of skill if you're going to get into this. But also teach companies how to prevent and mitigate ransomware attacks. I mean, you're never going to stop malware ever. But you can do a lot to help people protect against malware. And I think that that's one - I don't know how much the task force is going to work on that. But that's, I think, a huge and very valuable effort.

Steve: Maybe they could do a contract with ITProTV to create an educational video.

Leo: Most of our sponsors help you in one way or the other with this kind of stuff. Certainly on this show anyway. You know, I was thinking about Robert Tappan Morris because every time you think of his name you think of the Morris Worm, and you think of the first computer virus. And that he was the first person ever convicted under the Computer Fraud Act and all that.

Steve: Right, right.

Leo: But really he transcended that. He's a brilliant guy and has done amazing things since then. It's kind of a shame that he's so tarred with that one act that he even says was innocent. He was doing the kind of things that a lot of guys do. He was trying stuff out. He didn't expect it to get away.

Steve: Oh, Leo, it's a good thing that we didn't have the Internet when I was growing up.

Leo: I know, exactly. Exactly.

Steve: That would not have turned out well.

Leo: Like young Dan Kaminsky, your mother would have had to go yell at somebody.

Steve: Well, and given the mischief I got up to without computers, I don't want to think about what would have happened.

Leo: Precisely. It's normal. You have no frontal lobe. You're going to do crazy things. So Morris was the co-founder with Paul Graham of Y Combinator and has done - if you read his Wikipedia entry, you'll get an idea of all the things he's done. That's where I was thinking - Paul Graham wrote an amazing article about RTM and what a great - he's still alive, and he's still very active, but what a great guy he was. So, and I have huge respect for Paul Graham.

Sir, you have completed your duties, your assigned duties for this day. You may go have some fine Italian food, if that's what you desire. Are you still going out every week to the Italian place? That's awesome.

Steve: Yup, we are.

Leo: Isn't it amazing? Life is back. For some of us. Not for all of us.

Steve: Yeah. I'm waiting for my best buddy. He's got his first Moderna. I think he's got it, and Moderna is a four-week interval as opposed to Pfizer there's three. So it was a few weeks ago. So a couple weeks from now he'll be fully vaccinated, then we give him another couple weeks to let that set into his immune system.

Leo: Let's party.

Steve: And Javier's is our Mexican place.

Leo: Can't wait.

Steve: And they're going to look at us and, like, where have you guys been?

Leo: Oh, man. It's exactly right. When we go in...

Steve: We're pretty well known.

Leo: You know those people who were ordering takeout from you for the last year? That's us.

Steve: Uh-huh. That kept you guys afloat.

Leo: Yeah. That was us.

Steve: Yes.

Leo: We're back, baby. So I do hope all of you get the vaccine soon, if you haven't got it already, and we can get back to life. And for people in India and other places where it's just tragic...

Steve: Oh, Leo, boy. Ooh, ouch.

Leo: I feel so bad. And Ontario in Canada they're just suffering. And, wow, I really feel lucky that we have this vaccine and that we've been able to get it to almost half the population now. So it's really, really good.

Thank you, sir. I'm glad you're well, and I'm glad you're here to do this show. Steve joins us every Tuesday, right after MacBreak Weekly. I should warn you we're going to be a little bit late, not next week but the week after. This Week in - not This Week in Google. Just Google. You've heard of them? It's a little company, could do a search engine, has its Google I/O keynote on May 18th at 10:00 a.m. And it's scheduled for two hours, which means we won't get MacBreak Weekly started till about an hour late, which means you might be - you're used to this.

But I just give you a little heads-up, and a heads-up to the audience, if you watch it live. We'll be starting maybe around 2:30, thereabouts. Normally 1:30 p.m. Pacific, 4:30 Eastern, 20:30 UTC on a Tuesday afternoon. You can tune in TWiT.tv/live for the live audio or video feeds. If you're doing that, join us in the chatroom. They're chatting along as Steve talks. That's irc.twit.tv.

We also have, for people who want to listen after the fact, we have copies of the show. Steve's got them at his website, GRC.com. He's got the 16Kb version. If you're really bandwidth-constrained, but you still want to hear it, that's the smallest audio file we've got. He also has an even smaller file, but it's not as fun. You can read because we've got transcripts. I think most people read as they listen, or do what I do, which is use the transcripts to search because it's a great way to jump into a particular part of a show to find the thing you're looking for. And all of that's at GRC.com, along with SpinRite, the world's best mass storage - I said that right this time.

Steve: Thank you, you got it right the first time.

Leo: The world's best mass storage maintenance and recovery utility. 6.0 is out now. You can get it, and we'll get a free upgrade to 6.1, which is in active development and will be out soon. Well worth getting. Everybody who has mass storage of any kind should have SpinRite. While you're there, GRC.com has so many other fun things. All of the rest of it's free, like ShieldsUP! to test your router and, oh, I can go on and on and on. The DNS Benchmark is very valuable if you're choosing a DNS server. Just check it out, GRC.com.

We have audio and video of the show at our site, TWiT.tv/sn for Security Now!. When you get there, you'll also see a link to a YouTube channel. All the shows are there, if you for some reason like YouTube. You can also subscribe in a podcast program. That actually is probably the best way because then you can automatically get it the minute it's available and have it ready for you whenever you're in the mood - Pocket Casts, Stitcher, Overcast, you know, all of the usual suspects. If your podcast player has a review section, please leave us a five-star review. You want everybody to know about Security Now!. This is an important show for everybody to listen to, I think, every week. Thank you so much, Steve Gibson. God bless.

Steve: My pleasure.

Leo: May the 4th be with you.

Steve: Next week we're on time. It's the week after next that you're warning us.

Leo: It's the 18th. The 18th. I just wanted to give you a little heads-up ahead of time.

Steve: In that case, Leo, I'll be here.