Security Now! #817 - 05-04-21

The Ransomware Task Force

This week on Security Now!

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 renown Scripps Health system. We catch up on the multinational takedown of the Emotet botnet and the FBI's contribution of more than 4 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 also ran across a Dan Kaminsky anecdote that I had 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?

Get it??

Ransomware

REvil hacks Apple supplier Quanta Computer

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 "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."

Quanta Computer is a Taiwanese company that assembles a number of Apple laptops and other consumer devices. When Quanta initially refused to negotiate the REvil group, as they promised to, started leaking the data.

The ransomware demand was initially posted just hours before Apple's event, and the hackers say they will release more documents every day, adding: "We recommend that Apple buy back the available data by 1 May." A similar extortion attempt from the same group, aimed at Acer, demanded $50m in exchange for deleting the files.

Groups around the Internet have begun analyzing the details from the leaks. They've noted differences with the current models on sale: a new version of the MacBook Pro is shown without the "Touch Bar", and it appeared that HDMI ports might be staging a comeback along with SD card readers.

What we know of REvil is that they are tough negotiators who do not make idle threats. They are not known for being soft of 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 new Apple logos and as part of this deliberate proof-of-intention data leak. REvil warned Apple that they should buy back the data by May 1st or more would be leaked.

What appears to have happened — for reasons we can only guess — is that Quanta finally responded to REvil and opened a dialog. As part of a private chat, 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, since an updated demand, carrying an expiration date of this coming Friday, May 7th, has reduced the original demand from $50 million down to $20 million — seems like a bargain now, doesn't it?

Various researchers have been quoted stating that this appears to be a pattern: The REvil gang apparently feels that forcing the opening of a dialog is a crucial first step in getting paid. So they may be deliberately establishing a reputation for dramatically reducing their ransom demand once a dialog is established. This provides an incentive for a victim to establish contact in order to obtain the more "real" ransom demand. This also serves to break the ice.

World-famous Scripps Health taken down
Nearly the entire Scripps Health system, a world renown hospital network based in San Diego, was hit by a cyberattack over the weekend, forcing some critical-care patients to be diverted.

Scripps acknowledged the attack in a statement but didn't specify whether it was a ransomware incident. It's also unknown whether the adversaries compromised any patient records or other sensitive data.

An email notice from 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 sent to other medical centers.

As we know, emergencies being sent elsewhere after a ransomware attack is not unheard-of. Last September, employees at Universal Health Services (UHS), the owner of a nationwide network of hospitals, reported widespread outages that resulted in delayed lab results, a fallback to pen and paper, and patients being diverted to other hospitals. The culprit was Ryuk, which locked up hospital systems for days.

A nurse within the system wrote that "No patients died tonight in our [emergency room], but I can surely see how this could happen in large centers due to delay in patient care."

According to reports, outages are widespread across the 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 yesterday's appointments were postponed.

The day-to-day activities of staff have also been interrupted. Nurses, doctors and other personnel have resorted to using manual processes and paper records, since the electronic health records system was disrupted. That's something that also happened in the UHS attack. And, for the time being, the "telemetry at most sites" used for electronic monitoring and alarming (heart monitors, for instance) has become inaccessible, Scripps said, requiring regular manual checks of patients. A source told the paper that medical imaging and other "resources" have been affected.

The Scripps statement said that while the systems are offline, "patient care continues to be delivered safely and effectively at our facilities, utilizing established back-up processes, including offline documentation methods." Naturally, they're attempting to put the best face possible on this nightmare which has been deliberately perpetrated by, almost certainly, attackers located in Russia or China.

There's a sense of "you've seen one ransomware attack you've seen 'em all." But I don't think we should allow ourselves to become complacent about the attacks and numb to them. The question is of course what, if anything, can be done?

But, speaking of what can be done on the topic of massive and pernicious botnets...

Security News

The Big Emotet Botnet Takedown

Somehow we've never talked about Emotet. Perhaps that's because from one standpoint it was just another botnet — though it didn't remain that way. And when it was on the rise we were a bit botnet saturated. But at the beginning of this year, in an effort named "Operation Ladybird" a coordinated global operation which included authorities in Canada, France, Germany, Lithuania, the Netherlands, Ukraine, the United Kingdom and the United States all worked together to take control of the hundreds of botnet servers which supported Emotet. But they didn't stop there. Since at one point as many as 1.6 million active bot infections were believed to be active, the need was to proactively disinfect them. We're finally talking about Emotet today because Sunday before last — April 25th at 1pm — was the date and time set inside a replacement DLL that had previously been injected network wide. At that moment, Sunday before last, more than one million Emotet bot endpoints synchronously shutdown forever. But let's back up a bit to examine the history of this unique network...

Trend Micro was the first group to detect and profile the original Emotet Trojan back in 2014 shortly after its first appearance. What they discovered was at the time a relatively straightforward banking Trojan spread by phishing emails. Banking Trojans sit in a user's machine, patiently waiting for connections to known banking systems. When this is seen they capture and forward the user's authentication credentials, sending them to their bot masters who then typically empty the unwitting user's account.

But through the intervening years Emotet evolved multiple times. Over time it grew into a mature Malware-as-a-Service botnet, offering access to compromised computers for those wishing to pay. And, unfortunately, there were many wishing to pay. Among them were famous ransomware groups such as Ryuk and those pushing the data-stealing trojan, Trickbot. They quickly made the most of the initial access provided by Emotet, picking and choosing into which victims they would deploy additional payloads. Emotet was used by the TA542 threat group (aka Mummy Spider) to deploy second-stage malware payloads, including QBot and Trickbot, onto its victims' compromised computers. TA542's attacks usually led to full network compromise and the deployment of ransomware payloads across all infected systems, including ProLock or Egregor by Qbot, and Ryuk and Conti by TrickBot.

The growing and enduring success of Emotet demonstrated the potential of success through relatively straightforward phishing campaigns that were used to spread the infection. 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's evolving ability to spread laterally to other devices on a network made it among the most resilient pieces of malware seen in recent times. ALL instances of Emotet within a network needed to be killed simultaneously because a single surviving instance would reinfect all other reachable machines. It was a nightmare.

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

At the beginning of this year, 2021, the multinational 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 countries. In coordination with cybersecurity experts, replacement servers were connected to the individual IP addresses of the Emotet's command-and-control machines—many of which were, themselves, hacked PCs which the Emotet gang had been using to manage the botnet and send instructions to its victim computers.

A security researcher who was involved with the operation said: "We took over every critical C2, 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 botnet." [It's over.] Or was it?

Previous botnet takedown operations have had mixed success, the with cybercriminals often rebuilding their networks quickly after a takedown attempt — which were enabled by built-in fallback communications channels. 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 have been learning too. And in their statement about the Emotet takedown, Dutch police note that they discovered and disrupted the infrastructure's backups, too, which they hope will make a possible reconstruction of Emotet seriously 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 use them, and we took all of them, too. 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 that they still observed some detections, since it is 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.

After the takedown operation with the redirection of the network's command and control server IPs to law enforcement control, authorities pushed a new configuration to the million plus active Emotet infections so that the malware would then begin to use command and control servers permanently controlled by Germany's federal police agency.

Once that was done, every Emotet infection was updated with a new benign Emotet module, a 32-bit EmotetLoader.dll which was inserted into all infected systems. This is what caused the entire network of more than one million instances of infected machines to synchronously become inert Sunday before last at 1pm. At that moment, the Windows server startup and autorun registry keys were deleted, and the services terminated their own execution.

Two security researchers with Malwarebytes examined the uninstaller module delivered to the law enforcement controlled Emotet bots. They changed the system clock on a test machine to its April 25th 2021 trigger date and confirmed that it only deleted associated Windows service

definitions and autorun Registry keys, then terminates the process. It leaves everything else on the compromised devices untouched.

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 cautions they could still be hit with secondary malware that Emotet's partners previously downloaded to their computers, such as TrickBot or QakBot.

People are still feeling a bit touchy about the idea of law enforcement being this proactive, so I suppose this is going to take some getting used to. The FBI's subsequent disinfection of US-based Exchange Servers was not without controversy. And in this case not everyone was completely bullish on the Emotet takedown. Malwarebytes' CEO told BleepingComputer: "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. That all 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."

"Intervention" is never something that the intervened welcomes. But it's often the only way to solve a problem — and I suspect that 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, an effective means for kicking it out will be lost.

Emotet's 4,324,770 eMail addresses

In a related public/private partnership, the Dutch authorities and the US FBI have provided 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 to say about this last Tuesday:

Earlier this year, the FBI in partnership with the Dutch National High Technical Crimes Unit (NHTCU), German Federal Criminal Police Office (BKA) and other international law enforcement agencies brought down what Europol referred to as the world's most dangerous malware: Emotet. This strain of malware 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.

Following the takedown, the FBI reached out and asked if Have I Been Pwned (HIBP) might be a viable means of alerting impacted individuals and companies that their accounts had been affected by Emotet. 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 2 separate corpuses of data obtained by the agencies during the takedown:

- *Email credentials stored by Emotet for sending spam via victims' mail providers*
- *Web credentials harvested from browsers that stored them to expedite subsequent logins*

We discussed loading these into HIBP as 2 separate incidents so they could be individually identified, but given the remediation is very similar they've been loaded in as a single "breach".

At this point in Troy's blog, I'm skipping the standard "change your passwords" advice, though I wanted to quote one interesting tidbit that Troy wrote. He said:

- *Keep security software such as antivirus up to date with current definitions. I personally use Microsoft Defender which is free, built into Windows 10 and updates automatically via Windows Update.*

So it's an interesting data point that Troy, who certainly knows his way around security, has come to the same conclusion that Leo and I have when providing for Windows' security: On balance, Microsoft Defender is all that's needed.

Troy concluded: *"I've flagged this incident as sensitive in HIBP 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. 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."*

I'd say that Troy's proactive notification service is super-useful. It's at:

https://haveibeenpwned.com/NotifyMe

And I've signed up using all of my various eMail addresses. You'll receive a notification eMail to confirm your ownership of the eMail address, and when you confirm you'll receive a proactive verification of what that address is currently present in the HIBP database. So, again…

https://haveibeenpwned.com/NotifyMe

One thing Troy did not mention in his blog posting 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.

Have I Been Pwned domain-wide notifications

While we're on the subject of Troy's increasingly excellent service, I should mention its ability to provide domain-wide notification of any and all past and future breaches. Leo, this would be especially of interest to you, as it was to me, and to anyone who controls their own domain. I know from the eMail addresses I've replied to through the years that many of our listeners are masters of their own domain.

When I registered, I received an immediately sobering list of 155 eMail addresses within the GRC.COM domain. After regaining control of my cardiac sinus rhythm, 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 appears that individuals or bots have used a bunch of bogus grc.com accounts that have never belonged to us and for which eMail has never been sent.

But, at the same time, that list also contains a walk down memory lane...

chromazone@grc.com	River City Media Spam List, Verifications.io
cih@grc.com	Verifications.io
cod@grc.com	Data Enrichment Exposure From PDL Customer, River City Media Spam List, Verifications.io
greg@grc.com	Apollo, Cit0day, Data & Leads, Data Enrichment Exposure From PDL Customer, Exactis, Onliner Spambot, Verifications.io
s.gibson@grc.com	B2B USA Businesses, Verifications.io
sgibson@grc.com	Apollo, Data Enrichment Exposure From PDL Customer, Exactis, Verifications.io
sales@grc.com	B2B USA Businesses, River City Media Spam List, Verifications.io
steve@grc.com	Adapt, Covve, Exactis, Lead Hunter, River City Media Spam List, Verifications.io
sue@grc.com	Verifications.io

So I would strongly recommend that anyone who has control of their own domain should register with Troy's domain-wide search and notification system:
https://haveibeenpwned.com/DomainSearch

When you go there you'll need to prove your control of the domain with eMail, web or DNS:

1. For eMail, you'll need to be able to respond to an eMail sent to security, hostmaster, postmaster or webmaster.

2. Or, you can add a custom meta tag to the web page at your domain's root: <meta name="have-i-been-pwned-verification" value="--blah blah blah--">

3. Or, place a file named "have-i-been-pwned-verification.txt" onto the root of the domain containing a specific verification text string.

4. Or, add a specific TXT record to your domain's DNS of the form: "have-i-been-pwned-verification=--blah blah blah--"

QNAP

I don't like QNAP. 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... and I'd recommend this as a general policy. Time and again the company has demonstrated itself to be too irresponsible. They have a well established track record of ignoring security researcher's reports until their users are struck with disaster. Nor do they fess up when they're confronted. They obliquely refer to an "Improper Authorization Vulnerability in HBS 3" (which is their Hybrid Backup Sync offering). And it certainly is. But it would be more correctly described as yet another hardcoded firmware backdoor credential that was discovered, as they will all inevitably be, and has been widely exploited by multiple breeds of ransomware which is now competing to see which can get in first to encrypt all of a user's data.

Despite only asking 500 USD equivalent in bitcoin for decryption, there's clearly no safe way to have any QNAP device publicly exposed to the Internet. And QNAP themselves have begun recommending that their own users should not run on the default port 8080, but should attempt to hide their services elsewhere among the 65 thousand other ports because... that's right... If you **can't** make it secure, then at least make it obscure. No thank you.

Miscellany

Gravity NNTP Newsreader updated to v3.0.11.0:

- Fixs a failure in multipart mime attachments.
- Adds awareness of image/png file attachments.

Just a bit more about Dan

I know that we spent plenty of time remembering Dan Kaminsky last week. But an 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." 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. So they invite a skilled hacker to see whether they're able to get in. According to Dan's mom, Trudy Maurer, he began developing his knack for as a 4-year-old in San Francisco, after his father gave him a computer from Radio Shack. By age 5, Mrs. Maurer said, Dan had taught himself to code.

And at one point his childhood paralleled "War Games", the 1983 movie starring teenage Matthew Broderick who unwittingly accesses a U.S. military supercomputer. When Dan was 11, his mother said 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.

Several decades later, after Dan's comprehensive August 2008 BlackHat presentation of the DNS meltdown that his work had been instrumental in avoiding, Dan was approached by a stranger from the BlackHat audience. It was the administrator who had kicked him off the Internet years earlier. He wanted to thank Dan and to ask for an introduction to "the meanest mother he ever met."

Closing The Loop

Makdaddy / @makdaddy
@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.

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's 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 v6 might not notice anything new and different, but that was no longer any worry. But, for what it's worth, I'll definitely be keeping SpinRite's long-standing textual UI. It's not 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 time frame, 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.

Henrik Schack / @Schack
Hey, long time ago you talked about a very very long scifi series, currently 14 - 15 books, supposed to be 50+ I have forgotten the name, can you help?

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 is asking about: "The Frontiers Saga" by Ryk Brown. The Frontiers Saga is a straight up unapologetic space opera. It's wonderful pulp Sci-Fi. But what distinguishes it from so many others is that it is written well enough that I never find myself wincing. A book I was reading years ago kept referring to the "stygian" blackness of space. That would have been fine once. But this author apparently had no other word for black. So he kept using "stygian." It became tiresome rather quickly. Ryk has a real talent for creating very clear and well defined characters. And once they've been established he never asks them to do something they wouldn't. Since reading fiction is all about building an alternate reality model, the last thing you want is for characters who have been so well and carefully crafted to act out of character. They are all very clear in his mind, and on his pages.

"The Frontier Saga" is one continuous story told 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 books. I reread

the beginning set while waiting for the second set, and I'll confess that I'm now re-reading 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 may have thrown off his schedule a bit, but he's been working all year. As it happens, he just posted this morning, May 4th, starting with: *"I guess I'd better say something, lest I find my picture on the side of a milk carton."* Followed by a summary of what's been going on. He's wrapping up a standalone novel to be titled "The fall of the core" & plans to have the 3rd series starting to appear this summer.

Ryk was also quite unhappy with his books being available through Amazon's Kindle Unlimited plan. So he has also stated that only these first two 15-book arcs will be there. I'm sure I'll buy them wherever they appear, though I hope Amazon will be able to offer them for sale, since the Kindle is far and away my preferred reading platform. For now, all of the first 30 books are free to read as part of the Kindle Unlimited plan, which is $10/month and authors are reimbursed by the actual number of pages of their books that are read. I'll let this podcast's listeners know once the 3rd story arc begins to appear. Ryk has left fans of the Saga with some very interesting dangling loose ends; and I cannot wait to see how he resolves them.

So, let's talk about the new Ransomware Task Force...

The Ransomware Task Force

https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

The Wall Street Journal and CNN appear to have been among the first to obtain and report on a US Justice Department memo which discloses the creation of a new task force dedicated 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 on the works for some time. And, needless to say, it's quite needed. The question is, although a "task force" sounds wonderfully proactive, what can a "task force" actually do?

CNN explained that the new initiative follows what the memo describes as the worst year ever for ransomware 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 Russian-backed SolarWinds hacking campaign and the Microsoft Exchange server vulnerabilities that Microsoft has attributed to Chinese hackers. More recently, it is believed that Chinese hackers exploited vulnerabilities in Pulse Secure's VPN to compromise 'dozens' of agencies and companies in US and Europe.

In a memo from Acting Deputy Attorney General John Carlin to DOJ department heads, US attorneys and the FBI on 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. Actions could include everything from "takedowns of servers used to spread ransomware to seizures of these criminal enterprises' ill-gotten gains. In addition, the DOJ plans to devote more resources to training and intelligence sharing, as well as reaching out to the private sector 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 weak security or an ability to pay.

Brian Krebs covered this news too, opening 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 these crimes."

https://krebsonsecurity.com/2021/04/task-force-seeks-to-disrupt-ransomware-payments/

Brian continued: "In a 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 (DOJ), Europol and the U.K. National 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 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 as 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."

According to security firm Emsisoft, almost 2,400 U.S.-based governments, healthcare facilities and schools were victims of ransomware in 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 while ransomware is profit-driven and 'non-violent' in the traditional sense, that has not stopped ransomware attackers from routinely imperiling lives."

Okay. So now 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. It demonstrates that a lot of thought and work has been going on behind the scenes to get the project to this point.

As all good reports do, it opens with a framing statement that's meant to lay out the problem and the scope of the report's effort. Here's what that says:

We are 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.

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 are 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 criminal enterprise.

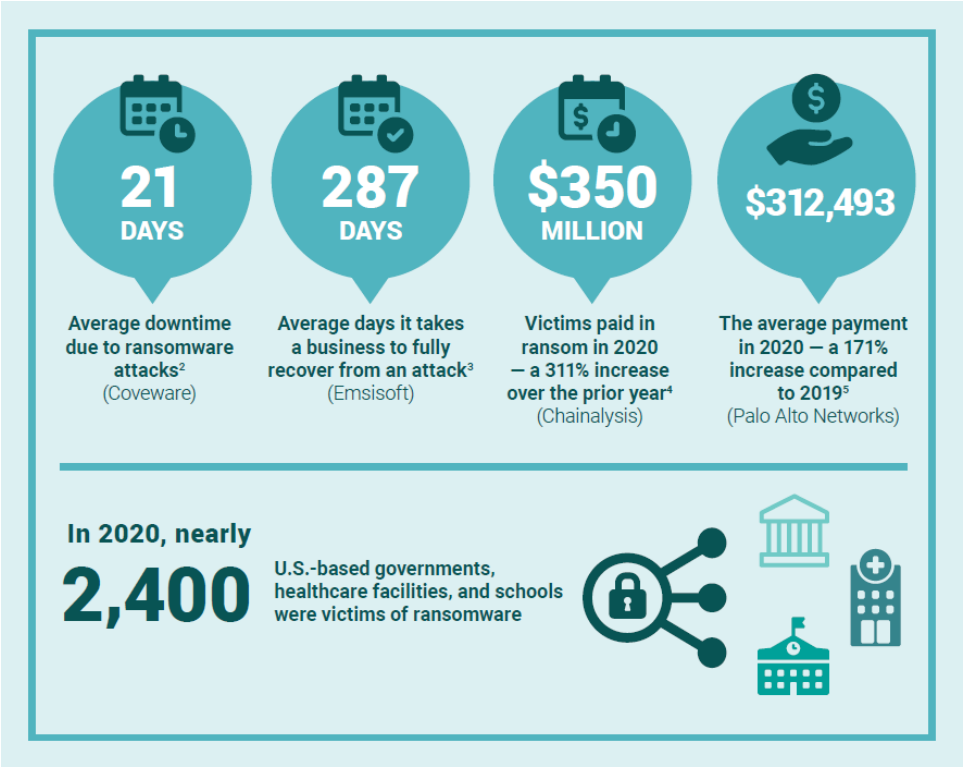
For this reason, we convened the Ransomware Task Force — a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, non-profits, and academic institutions — to develop a comprehensive framework for tackling the ransomware threat. Our goal is not only to help the 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 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 us.

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 depends 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.

This is nothing that we wouldn't 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 the report does contain an interesting and informative infographic:



So, ransomware badly nukes an organization's operation taking them offline for an average of 21 days with 287 days on average to fully recover. The problem is growing very rapidly, showing more than x3 growth in ransom payments during 2020 compared with 2019 with a 1.71 factor increase in the size of individual payments.

I've scanned through the entire report and pulled out some of its most interesting pieces.

When we began this podcast nearly 16 years ago, 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. But as we know, that was then. It occurred to me some time ago, and I've noted it several times on the podcast, that the rise of Cryptocurrency exchanges which support both submitting and extracting payments in local non-cyber currencies, coupled with the inherent anonymity of the blockchain's wallet designations, has been an enabling factor in the growth of ransomware. 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:

> *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 multi-step 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 "chainhopping," 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 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. With 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.

The report discusses the RaaS — Ransomware As A Service threat model and problem, observing that:

Carrying out a ransomware attack does not require technical sophistication. "Ransomware as a service" (RaaS) is a business model that provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware. In 2020, two-thirds of the ransomware attacks analyzed by cybersecurity firm Group-IB were perpetrated by cyber criminals using a RaaS model. This "as a service" 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" business models.

In the RaaS model, there are at least two parties who establish a business relationship: the developer and the 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.

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 Sobinokibi, Phos, Dharma, and GlobeImposter ransomware variants are all known to operate under the RaaS model.

The report also had some sobering things to say about Nation-State actors. 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 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 by other nations]. For example, in an April 2021 announcement 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 and phishing campaigns." *[In other words, we're suffering while they're popping Champagne corks and partying.]*

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.

The Report then distills what I'm sure must have been endless committee meetings and hearings into just four goals:

1. Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy.
2. Disrupt the ransomware business model and decrease criminal profits.
3. Help organizations prepare for ransomware attacks.
4. Respond to ransomware attacks more effectively.

The Report further details each of those four goals with multiple objectives each consisting of one or more specific actions. Since I've provided a 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 list. But suffice to say that it **is** comprehensive and it **is** hopeful.

Long ago on this podcast we observed that 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 spread. So they must have been created by their authors just to see whether they might work. The first botnets 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 also caused far more trouble than he intended.

Compared to when we began looking at and discussing these issues weekly, today's cybercrime world is barely recognizable. "Cybercrime" is no longer the realm of speculative fiction. It exists and it has become nation-state sponsored, revenue-generating big business. With criminals being protected by their own governments, the ability of law enforcement to curtail ransomware attacks seems quite limited.

Unlike Emotet, where the threat was diffuse and significant only because of the size of the network. Ransomware attacks are significant individually. And if the years of this podcast have revealed any truth, it's that were currently unable to reliably create complex **and** secure networked systems.

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 — it's not clear to me that huffing and puffing is going to amount to much.