Security Now! #826 - 07-06-21

The Kaseya Saga

This week on Security Now!

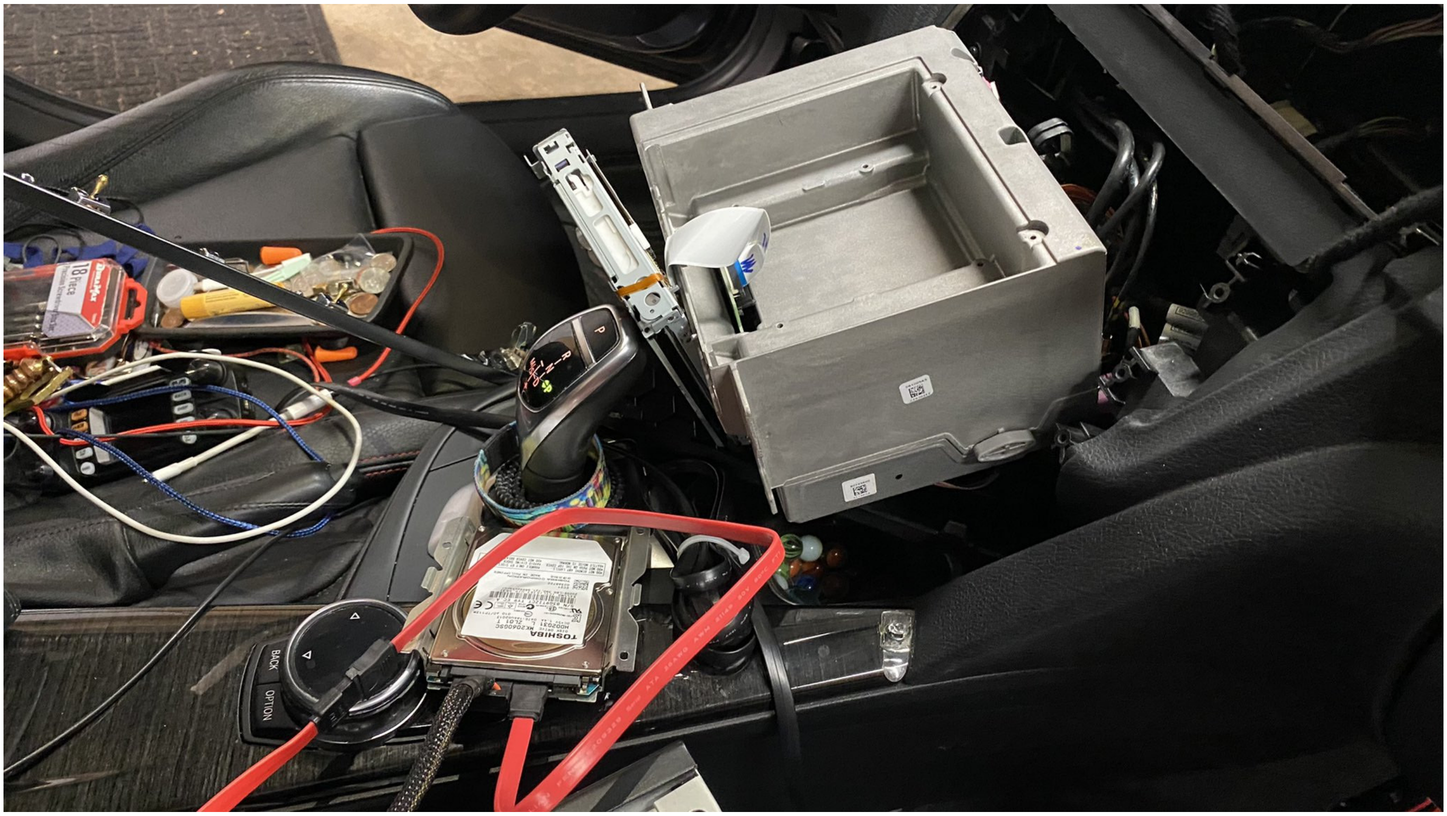
The so-called Windows “PrintNightmare” remote code execution flaw, as bad as it is, was overshadowed by the Sodinokibi malware which the REvil ransomware gang managed to infiltrate into Kaseya, a popular provider of remote network management solutions for managed service providers. Since those MSP's all, in turn, have their own customers, the result was a multiplicative explosion in simultaneous ransomware attacks. Since those attacks reportedly numbered in excess of 1000(!), this makes it the worst ransomware event in history. So, while we'll definitely be covering the PrintNightmare and other events of the week, our topic will be the reconstruction of the timeline and details of the Kaseya Saga.

```
Drive: 1, Item: 2            Graphic Status Display

                                                        sector status key
                           remaining     completed            R recovered
     work                                1,257   .oO analyzing    B defective
megabytes:                 129,482       0.96%    .  unprocessed  U unrecovered
        %:                  99.04%     0:02:08    ■  processed
     time:                 3:39:55
Use the left and right arrow keys to move through the screens at any time, or
```

Life@TerminalVelocity / @lifeattv (https://twitter.com/lifeattv/status/1409982247369850883)

Spinrite saves the day again. My BMW is having fits, has a mechanical hdd. Dealership wants $1500 in parts and $1000 in labor to maybe fix the problem. This is the 2nd pass. 1st pass fixed some issues. Radio now boots. @SGgrc 2:08 PM · Jun 29, 2021 · Twitter for iPhone



Security News

“PrintNightmare” is NOT CVE-2021-1675

Probably the biggest nightmare about PrintNightmare, aside from the fact that it's being exploited in the wild right now, is the incredible amount of confusion surrounding stumbles that Microsoft and well-meaning security researchers have made.

There are two related but separate and independent issues at play which affect ALL current and all previous versions of Windows Print Spooler service which is running by default in Windows and runs with full SYSTEM kernel privileges. Windows' Print Spooler, which has historically been a source of many serious vulnerabilities. Ten years ago, it was the exploitation of an escalation of privilege bug in Windows Printer Spooler that was used by Stuxnet to take over, spin-up and damage the centrifuges being used by Iran's nuclear enrichment program. And here we are today, ten years later with both another Local Privilege Escalation vulnerability and also a separate Remote Code Execution vulnerability.

During last month's June 8th patch Tuesday, Microsoft believed that they had patched and closed the vulnerability, which was identified as CVE-2021-1675, a Local Privilege Escalation. But, as Will Dormann, vulnerability analyst at the CERT coordination center tweeted: *“I've published a vulnerability note on this. I suspect that Microsoft will need to issue a new CVE to capture what PrintNightmare exploits, as it sure isn't what Microsoft patched as CVE-2021-1675.”*

A Chinese researcher with NSFOCUS, who reported the original vulnerability to Microsoft, explained last Thursday in a Tweet: *“CVE-2021-1675 is meant to fix PrintNightmare, but it seems that they just test with the test case in my report, which is more elegant and also more restricted. So, the patch is incomplete. : (”*

Wow. This is NOT the behavior of a Microsoft whose OS the world can depend upon as much as it currently does. The NSFOCUS Tweet suggests that rather than carefully examining the researcher's provided proof-of-concept, and using it to reveal and understand the whole problem that it was intended to reveal, someone at Microsoft apparently quickly applied a patch to shutdown the example, but without resolving the underlying actual problem.

When this research saw what was NOT done last month, he attempted to reach out again to @msftsecresponse. He tweeted: *“My case of #PrintNightmare is closed. And I can't login to MSRC portal because there is no Microsoft account option which I used. Then, how can I report that you not fix CVE-2021-1675 properly (another call is kept vulnerable)? That is your cooperation? @msftsecresponse”*

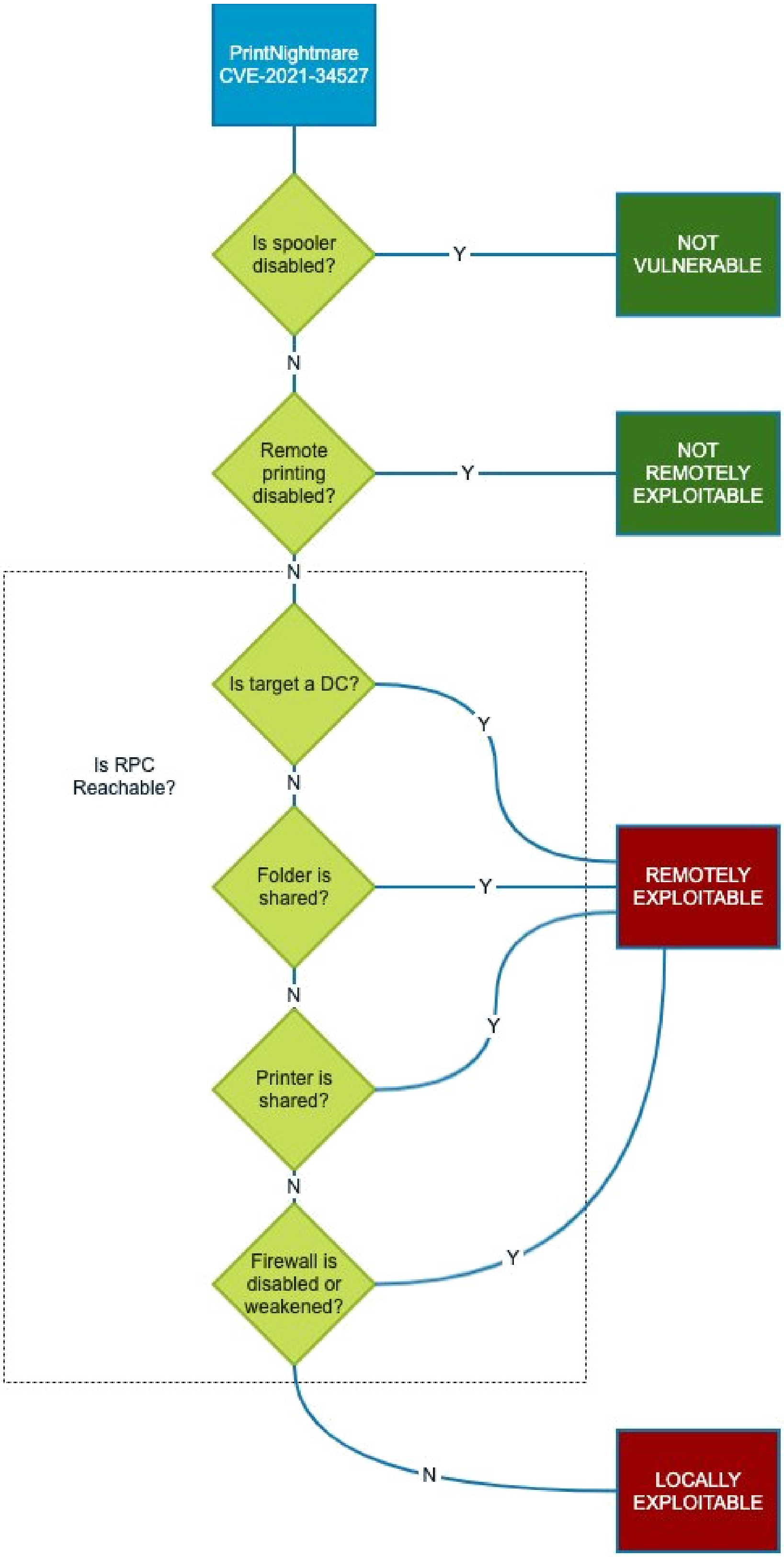
And then the situation even gets worse when, just before the end of June, another Chinese security vendor QiAnXin announced that they found a way to exploit the vulnerability to achieve both local privilege escalation and remote code execution, and published a demo video while deliberately refraining from sharing additional technical details. But the Hong Kong-based cybersecurity company Sangfor published an independent deep-dive of the same vulnerability to GitHub which included fully working proof-of-concept code. The PoC remained publicly accessible for several hours before they thought better of their publication and took the code down. Sangfor’s principal security researcher posted: *“We deleted the PoC of PrintNightmare. To mitigate this vulnerability, please update Windows to the latest version, or disable the Spooler service.”* Unfortunately, updating Windows won’t help. Stopping and disabling the print spooler service is the only sure fire mitigation. And before the PoC was removed the project was forked with variations currently up on two Github locations. The links are in the show notes for anyone who’s curious to review the code:

https://github.com/cube0x0/CVE-2021-1675
https://github.com/afwu/PrintNightmare

So now we all finally know that Microsoft's June 8th patch for CVE-2021-1675 was incomplete, that the PrintNightmare remote code execution exploit works against all up-to-date Windows systems, that ready-to-go proof-of-concept code is available for a still-unpatched CRITICAL Windows RCE 0-day and that it's currently being exploited in the wild. Finally realizing just how badly they had messed up, Microsoft assigned the new and separate CVE-2021-34527 for the remote code execution vulnerability.

And, adding insult to injury, this new technique has already been added to the powerful and popular Mimikatz post-intrusion authentication exploitation toolkit. <sigh>

CERT/CC's Will Dormann created a exploitation and remediation flow chart based upon his own testing of Windows on a currently fully patched system:



CISA has issued a PrintNightmare notification urging admins to disable the Windows Print Spooler service on servers not used for printing, and Microsoft is also recommending that the printing service be disabled on all Domain Controllers and Active Directory admin systems. Their advice takes into consideration that the Windows Print Spooler is enabled by default on most Windows clients and server platforms, thus drastically increasing the risk of future attacks targeting vulnerable systems.

So what about the vulnerability itself? It boils down to the ability of any non-privileged user to bypass the authentication barrier which prevents unprivileged users from installing whatever — possibly malicious — printer drivers they choose. Specifically, any attacker who can bypass the authentication which protects the RpcAddPrinterDriver API can install a malicious print driver. Microsoft's documentation claims that the client needs to hold the "SeLoadDriverPrivilege" for the RpcAddPrinterDriver call to succeed. But that turns out not to be true. A call to "ValidateObject Access" is made, but a mistake in the code that sets up the call's parameters gives a user control and allows the validation check to be skipped. So a non-privileged normal user can bypass the security check and add a driver. If the target is a Windows Domain Controller, a normal domain user can connect to the Spooler service in the DC, install a driver and then fully control the Domain.

Oh... and before signing off, this research noted: *"There are more hidden bombs in Spooler, which are not publicly known. We will share more RCE and LPE vulnerabilities in Windows Spooler. Please stay tuned and await our Blackhat talks 'Diving Into Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer'."*

The 0Patch guys have quickly produced one of their cool micro-patches for this if you need to keep your print spooler online and believe that you might become a victim of this before next Tuesday's patch Tuesday which will, hopefully and presumably, fix this one permanently.

The Authentication Dilemma
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

An 8-page PDF jointly published by the Us's NSA, CISA and FBI and the UK's GCHQ-based National Cyber Security Centre outlined an ongoing brute-force credential stuffing attack being waged against the West by Russia's GRU, their General Staff Main Intelligence Directorate. The executive summary states:

> *Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165, used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide. GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium, and a variety of other identifiers. The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365® cloud services; however, they also targeted other service providers and on-premises email servers using a variety of different protocols. These efforts are almost certainly still ongoing.*
>
> *This brute force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion. The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE 2020-0688 and CVE 2020-17144, for remote code execution and further access to target networks. After gaining remote access, many well-known tactics, techniques, and procedures (TTPs) are combined to move laterally, evade defenses, and collect additional information within target networks.*

> *Network managers should adopt and expand usage of multi-factor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a ZeroTrust security model that uses additional attributes when determining access, and analytics to detect anomalous accesses. Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks (VPNs) and The Onion Router (TOR), where such access is not associated with typical use.*

I absolutely agree with the idea of filtering and blocking any knowable atypical access IPs. As I've often noted, anywhere a relatively static originating IP is knowable, it should absolutely be used as part of a connection qualification filter. Network connections that do not **need** to be accepted from everywhere should never be accepted from everywhere.

We also know that strong security is not provided by simple obscurity. But when you think about it, that's what a password is. It may be very obscure, but many passwords, even today, contain fewer than 128 bits of true entropy. So they are less obscure than a strong cryptographic key.

In a world where the weakest link determines the effective strength of an entire chain, user-chosen passwords remain a problem. From time to time, upon account creation, a web service will pre-assign a super-strong password to me rather than asking me to choose my own. I think that's brilliant. If I don't already have some means for accepting, securely recording, storing and regurgitating-on-demand an arbitrary high-entropy string of characters then I've already lost the game. I'm sure that everyone listening to this podcast has such a facility. But even today not everyone does.

And this brings me to my takeaway conclusion from this news that the Internet's background radiation has inevitably evolved from randomly probing packets to deliberately focused and targeted connections attempting to brute-force their way in. Bad guys are logging into other people's RDP servers using something that someone knows. We really do need to get completely away from the terminally weak "something you know" form of username and password identity authentication. And the sooner the better. Whatever that solution will be, it needs to be free and easy to use, so that everyone will be able to use it. And it doesn't even need to be perfect. It just needs to be a lot better than the decades old mess we're still all using today. I sincerely hope that the right people, somewhere, are giving this the attention it needs. As we all know, I invested seven years of my life creating one complete free solution to this need and problem. FIDO and WebAuthn are useful steps in the right direction, but they both fall short of offering a complete solution. The world doesn't need to use SQRL, but it sure needs to do something.

Western Digital steps up.
https://www.westerndigital.com/support/productsecurity/wdc-21008-recommended-security-measures-wd-mybooklive-wd-mybookliveduo

As we covered last week, many users of Western Digital's My Book Live and My Book Live Duo whose last firmware update was in 2015, and who were consequently unable to patch even if they wanted to after a vulnerability was discovered three years later, which was three years ago in 2018, found themselves to be victims of a recent Internet-wide malicious data wiping campaign. Although direct evidence is not decisive, security industry observers believe that this may be the result of a war between rival botnet groups. We're bringing this up again with the news that Western Digital has stepped up... and I'm very impressed. Last Wednesday, on June 30th, WD updated their coverage of what has been a true disaster for many of their users, by posting:

> *Western Digital has determined that Internet-connected My Book Live and My Book Live Duo devices are under attack by exploitation of multiple vulnerabilities present in the device. In some cases, the attackers have triggered a factory reset that appears to erase all data on the device.*
>
> *To help customers who have lost data as a result of these attacks, Western Digital will provide data recovery services, which will be available beginning in July. My Book Live customers will also be offered a trade-in program to upgrade to a supported My Cloud device.*
>
> *The My Book Live firmware is vulnerable to a remotely exploitable command injection vulnerability when the device has remote access enabled. This vulnerability may be exploited to run arbitrary commands with root privileges. Additionally, the My Book Live is vulnerable to an unauthenticated factory reset operation which allows an attacker to factory reset the device without authentication. The unauthenticated factory reset vulnerability has been assigned CVE-2021-35941.*
>
> *We have heard concerns about the nature of this vulnerability and are sharing technical details to address these questions. We have determined that the unauthenticated factory reset vulnerability was introduced to the My Book Live in April of 2011 as part of a refactor of authentication logic in the device firmware. The refactor centralized the authentication logic into a single file, which is present on the device as includes/component_config.php and contains the authentication type required by each endpoint. In this refactor, the authentication logic in system_factory_restore.php was correctly disabled, but the appropriate authentication type of ADMIN_AUTH_LAN_ALL was not added to component_config.php, resulting in the vulnerability. The same refactor removed authentication logic from other files and correctly added the appropriate authentication type to the component_config.php file.*
>
> *We have reviewed log files which we have received from affected customers to understand and characterize the attack. The log files we reviewed show that the attackers directly connected to the affected My Book Live devices from a variety of IP addresses in different countries. Our investigation shows that in some cases, the same attacker exploited both vulnerabilities on the device, as evidenced by the source IP. The first vulnerability was exploited to install a malicious binary on the device, and the second vulnerability was later exploited to reset the device.*

Later, they reiterate as they conclude their posting:

> *For customers who have lost data as a result of these attacks, Western Digital will provide data recovery services. My Book Live users will also be offered a trade-in program to upgrade to a supported My Cloud device. Both programs will be available beginning in July, and details on how to take advantage of these programs will be made available in a separate announcement.*

This impresses me.

In the first place, we learn how and why that authentication bypass was introduced into the devices. The wholesale commenting-out of the access authentication that was seen last week was troubling in the extreme. But their refactoring explanation makes all the sense in the world, and I can see how a coder could have easily intended, but ultimately failed, to apply the alternative authentication protection which the redesigned system provided. That's exactly the way mistakes are made.

But WD's willingness to take responsibility for a device which it was selling 11 years ago, back in 2010, which has not been supported for the past six years, says a great deal about the company's management — to which I say Bravo! I'm sure they found that the apparent data loss from the Factory Reset was recoverable. So, hat's off to them for stepping up and offering to get their customer's data back for them. I'm impressed.

WD's MyCloud OS3 Troubles

Before we get all choked weepy-eyed up over WD's willingness to help their MyBook NAS users, we need to note that a much larger group of WD's users, those who are still using the MyCloud OS 3 which was built into WD's newer MyCloud NAS devices, are in trouble today...

It turns out that all MyCloud OS 3 devices contain a serious remote code execution flaw, and that, wouldn't you know it, OS 3 is also no longer supported. This came to light when a pair of intrepid security researchers (and several other groups), who were planning to present their discoveries of problems with WD's cloud devices during last year's Pwn2Own competition in Tokyo, had the rug pulled out from under them by WD's release of MyCloud OS 5 shortly before the competition date. Being a complete rewrite, OS 5 inherently eliminated the bug that these researchers and others had hoped to cash-in on. Since the ground rules for Pwn2Own required that qualifying software must be the most current, flaws in OS 3 were no longer prize worthy.

Of course, as we know all too well, the fact that OS 5 appeared doesn't spontaneously cause all of the OS 3's in the world to be updated to the OS 5 firmware and, in fact, it appears that not all of the WD hardware that runs OS 3 will run OS 5, and that even if it did, OS 5's complete rewrite left out a number of OS 3's popular features. So if WD's users of OS 3-based MyCloud devices even knew of the trouble with their current firmware and wanted to update, WD would be asking those customers to accept a feature downgrade in order to repair a previous, badly broken and now out of support OS. Once again, while WD certainly has the legal right to do whatever they wish with their customers, it's not the best way to earn and maintain a reputation for standing behind one's products throughout their entire useful service life. If MyCloud devices were sold under the condition that they would run for exactly five years, then self-destruct, it seems unlikely that many people would choose that solution — though that's essentially what we have here.

In any event, earlier this year, in February, the research team published a detailed YouTube video, which documents how they discovered a chain of weaknesses that allows an attacker to remotely update a vulnerable device's firmware to add a malicious backdoor — using a low-privileged user account with a blank password. Tens of thousands of devices appear to be vulnerable to this attack today.

Last year, before the Pwn2Own competition, there appears to have been some sort of communication mixup, because the researchers said that WD had never responded to any of their reports. Brian Krebs apparently asked WD what the story was, and he was told:

"The communication that came our way confirmed the research team involved planned to release details of the vulnerability and asked us to contact them with any questions. We didn't have any questions so we didn't respond." Really!?! That's what you're going with? *"Since then, we have updated our process and respond to every report in order to avoid any miscommunication like this again."* Well, that's some comfort. *"We take reports from the security research community very seriously* [Uh huh] *and conduct investigations as soon as we receive them."* [Even if we don't mention it!]

And Brain added that Western Digital ignored questions about whether the flaw found by the researchers had ever been addressed in OS 3. Brian reports that a statement published on WD's site, dated March 12, 2021, says that the company will no longer provide further security updates to the MyCloud OS 3 firmware.

"We strongly encourage moving to the My Cloud OS5 firmware," the statement reads. "If your device is not eligible for upgrade to My Cloud OS 5, we recommend that you upgrade to one of our other My Cloud offerings that support My Cloud OS 5."

And we should note that these WD NAS gadgets are not cheap, weighing in at around $500. So telling their users who are stuck with OS 3 for whatever reason to "upgrade" to other WD offerings that support MyCloud OS 5 might be asking a lot.

In order to save some of the value from all of their research, the team developed and released their own patch to fix the vulnerabilities they had found in OS 3. Unfortunately, the patch needs to be reapplied whenever the MyCloud device is rebooted since it will be returned to its previous unpatched and vulnerable state. Western Digital told Brian that they were aware of third parties offering security patches for My Cloud OS 3.

None of this is really confidence inspiring, and NAS devices in general appear to be perennially troubled. I love my Drobos, but no way would I ever consider exposing them to the public Internet. They are permanently linked to each other through SyncThing with both safely tucked away behind multiple layers of NAT routing.

If I had to expose a NAS to the public Internet, I'd use a well-maintained Ubuntu Linux running NextCloud. Take a look at https://nextcloud.com/secure/ if you want to see some guys who have gone way over the top with security. They have multiple code audits and security reviews, and even a live "video verification" option as part of their remote authentication process.

SpinRite

While we're on the subject of mass storage... In addition to this week's utterly amazing picture of the week, I can report having passed another milestone on the road to SpinRite v6.1. At the end of my work day, the day before yesterday on Sunday July 4th, I posted the news to GRC's spinrite.dev newsgroup that I had just finished the work on updating SpinRite's SATA/AHCI driver to add the features SpinRite would need for those controllers. Last Friday I had finished the work on SpinRite's PCI Bus Mastering driver. So that means that all five of SpinRite's new drive-access interface drivers are now written. Recall that I designed a drive-independent IO abstraction layer to be driven by a new SpinRite core. That core will finally switch SpinRite from its traditional track-based orientation to a linear storage model which is what everything today uses. After today's podcast I will begin implementing SpinRite's new core. It's already designed, and the IO abstraction was expressly designed for its use. So I expect the core implementation to go smoothly.

And once that's done... **all** of the parts of SpinRite that needed redesigning and rewriting will be finished. But none of that new code I've been writing has been tested and debugged yet. So I'll set up test cases and work through the live code to watch it work and verify that in every case it does what I intend. Once it all appears to be working correctly, I'll turn the newsgroup gang loose on it for their testing. I'm absolutely certain that we'll discover things that still require some tweaking. But at that point we'll be working on a fully functional pre-release of the finished and final SpinRite v6.1. So things are starting to get exciting!

And speaking of exciting...

Miscellany & Closing The Loop

Last Friday evening after I had finished that work on SpinRite's new PCI Bus Mastering driver, Lorrie and I watched, and thoroughly enjoyed, Amazon's new release of "The Tomorrow War" starring Chris Pratt. Afterward, we had the inevitable discussion about the paradoxes arising whenever someone arranges to travel backward in time. As we all know, traveling forward is no problem at all. But moving into the past creates all sorts of dilemmas. In any event, after the movie I tweeted to my Twitter followers:

"Buckle Up! If you have access to Amazon Prime and enjoy Sci-Fi action movies, I can recommend Chris Pratt in "The Tomorrow War." Non-stop action, fun, astonishing special effects (how'd they do those alien monsters?) and more. I can't imagine that it would disappoint!"

With very few exceptions the replies from those who were motivated to watch the movie were similarly very positive. In fact, Jason Hudson tweeted that he was immediately watching it a second time. And I get that, because it was a romp. There were a few "Meh" replies, but Twitter follower "Houdini7" was the least impressed of all. He wrote: *"I found it so full of plot holes and trivial cliches, I felt it was one of the worst movies I've ever seen."*

So I suppose that "Houdini7" has been quite lucky with his movie choices throughout his life, because I've definitely seen a great many way-worse movies. Nevertheless, IMDB pegs it at a 6.7, which falls below my normal 7.0 threshold of worthiness. So is it, as "Hondini7" says, full of plot holes and trivial cliches? Absolutely!! And yet we still found it to be wonderfully fun. When it comes to **these** kinds of movies, I'm a proud 10 year old.

So, for any other 10 year olds at heart, if you're in search of a deeply cerebral experience you'll likely be as disappointed as Houdini7 was. But if you're looking for a wonderful Sci-Fi romp, I believe that I can safely encourage you not to miss Amazon Prime's "The Tomorrow War"!!

The Kaseya Saga

First, before we plow into The Kaseya Saga, I wanted to share a little bit of interesting trivia: I found a Q&A interview which first appeared on October 23rd of last year. It was conducted between Russian OSINT (open-source intelligence) and a member of the REvil gang. The link to the entire dialog is in the show notes for anyone who's interested: https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/

The interview was titled: "Uncensored Interview with REvil / Sodinokibi Ransomware Operators" and most of what's there we already know. But at one point, the Russian OSINT interviewer asked: *"What does the R prefix in the word Revil mean? Is that the word Reborn?"*

The REvil interviewee replies: *"Ransom Evil. The thought came from Resident Evil."* I'd imagine that gamers are familiar with Resident Evil, also known as Biohazard. It's a Japanese video game series and media franchise which was created by Capcom featuring plot lines about bio-weapons and viral incidents. (And, yes, I also very much enjoyed the many spin-off Resident Evil movies too because, as I said, it's sometimes fun to be 10 years old.)

But a other interesting new tidbits arose from the much longer interview:

Russian OSINT: Have you ever had problems when it was not possible to decrypt encrypted files after receiving a ransom? That is, something went wrong and you yourself could not do anything.

REvil: Yes. If you have previously tried to use third-party data recovery software. If at least 1 bit of the file is modified, the key will be lost. Especially often this happens with antivirus – it simply deletes notes, and they contain keys. I say openly – such cases are extremely rare. I remember only 12 for the entire time of work. And, of course, we never took money. The note contains a warning to the victims. If they don't read it, their difficulties.

Russian OSINT: Which industries are currently the "fattest" for Ransomware attacks? Where is the most profit?

REvil: IT-providers, insurance, legal firms. Manufacturing, especially, oddly enough, the agro-industrial complex.

Russian OSINT: You don't do any hacking and fixing into the infrastructure with your own hands … your partners do it, right?

REvil: We have our own "flying squad", and we also have partners. We do this and that.

Russian OSINT: A recent report from Microsoft said that 2 extremely effective attacks for introducing Ransomware are brute-force and RDP hacking, how do you think, will attack vectors change over time?

REvil: Brute force has been alive for 20 years. And he will be alive. RDP is the best vector. Especially the fresh BlueGate vulnerability will hit him very hard.

Okay. So what’s the backstory behind this biggest-ever record-breaking ransomware event?

Let’s begin with who is Kaseya? They're an international IT solutions provider based in Dublin, Ireland, with their US headquarters located in Miami, Florida and they maintain a physical presence in 10 countries.

Among the IT solutions offered is VSA, a unified remote-monitoring tool for managing networks and endpoints. Their software is aimed at enterprises and managed service providers (MSPs) and Kaseya says that over 40,000 organizations worldwide use at least one of their solutions. Just last week I was noting that MSP's are a potent source of ransomware intrusion since, as we saw in that case of a managed service provider to dental offices, a single intrusion at an MSP could expand downward to all of that company's client/customers. Essentially, all of an MSP's clients have extended their internal networks into that common service provider and, as we often like to rhetorically ask on this podcast, “what could possibly go wrong?”

What went wrong in this instance was that just as MSP's serve many clients, many MSP's are using a single common VSA server provided by Kaseya... and that VSA software contained a number of 0-day vulnerabilities that were being leveraged by clever and determined REvil affiliate.

On July 2 at 2:00 PM Eastern time, Kaseya's CEO Fred Voccola announced “a potential attack against the VSA that has been limited to a small number of on-premise customers.” Uh huh. That has turned out to be nearly 40 of Kaseya's MSP customers each of whom had many clients.

Two days later, by the 4th of July, Kaseya had revised its estimate of this attack severity upward, calling its software the “victim of a sophisticated cyberattack.” Apparently the truth is that Kaseya’s CEO **wishes** that a sophisticated cyberattack was possible but, as we learn in a minute, it was apparently embarrassingly trivial. FireEye's Mandiant team in addition to several other security companies were called in to help get a grip on the situation. Kaseya posted that “Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.”

The FBI described the incident as a “supply chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple MSPs and their customers.”

Huntress has tracked 30 MSPs involved in the breach and believes with "high confidence" that the attack was triggered via an authentication bypass vulnerability in the Kaseya VSA web interface. And in a Reddit explainer they added that an estimated 1,000 companies have had servers and workstations encrypted and noted that it's reasonable to suggest "thousands of small businesses" may have been impacted.

Sophos has said that “This is one of the farthest-reaching criminal ransomware attacks that Sophos has ever seen. At this time, our evidence shows that more than 70 managed service providers were impacted, resulting in more than 350 further impacted organizations. We expect the full scope of victim organizations to be higher than what's being reported by any individual security company.”

The REvil affiliate's discovery of vulnerabilities in Kaseya's VSA offering allowed them to cause malicious update payloads to be sent out to all of the devices being managed by each compromised Kaseya VSA server. Using this malware delivery channel cleverly provided the REvil malware with cover in several ways by supplying the initial compromise through a trusted channel, and leveraging the trust in the VSA agent code. Get a load of this!... Kaseya requires that its software be given anti-malware exclusions for its application and agent “working” folders. That means that, thanks to those exclusions, anything executed by the Kaseya Agent Monitor is allowed and ignored by any antiviral protections. (What could possibly be wrong with doing that?) And it was these explicit exclusions that allowed REvil to deploy its dropper without any scrutiny.

For these reasons, Kaseya's VSA solution platform was a perfect foil for REvil. Among other functionality of VSA is the deployment of software and automation of IT tasks. As such, VSA agents and their actions obtain and run with a high level of trust on customer devices. By infiltrating the VSA Server, any attached client will perform, without question, whatever task the VSA Server requests. Security analysts have suggested that this is probably one of the reasons why Kaseya was targeted. In other words, the REvil affiliate who managed to infiltrate Kaseya almost certainly did it deliberately because they appreciated the size and power of the attack they would be able to achieve.

As we all know by this time, that clever REvil affiliate was quite correct. In one headline grabbing instance, the Swedish supermarket chain Coop was forced to shut down some 500 stores after those stores' retail checkout cash registers stopped functioning.

And now we learn that Kaseya was AWARE of the 0-day vulnerabilities in its systems at the time of these attacks. On Sunday, the Dutch Institute for Vulnerability Disclosure (DIVD) revealed that it had alerted Kaseya to a number of 0-day vulnerabilities in its VSA software that it said WERE being exploited as a conduit to deploy ransomware. DIVD indicated that Kaseya was in the process of testing fixes for VSA under coordinated vulnerability disclosure when the July 2 attacks took place. Although DIVD revealed no specifics about the flaws they had discovered, DIVD's chairman, Victor Gevers, suggested that the 0-days were trivial to exploit. He tweeted: “If I would show you the PoC, you would know how and why. Instantly.”

The attacks, of course, caught these researchers and Kaseya by surprise and probably in horror. Since the immediate solution was to get all Internet-exposed VSA servers offline, DIVD has been providing a list of publicly accessible VSA IP addresses and customer IDs to Kaseya to help that happen. This effort led to a dramatic decrease in publicly accessible servers, from a starting count of over 2200 online servers to only 140 which are known to still be accessible today.

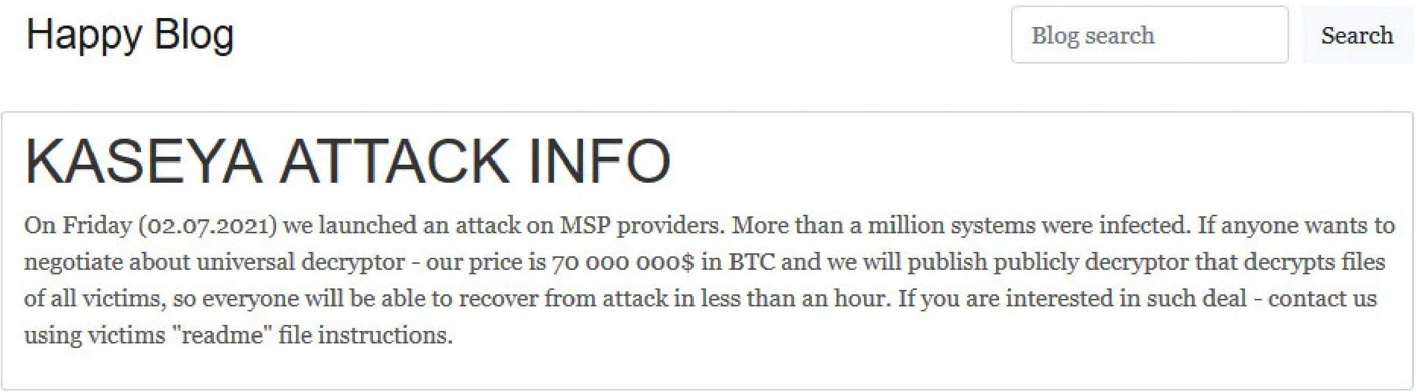
And this brings us to the curious case of the ransom demands which appear to be far more sophisticated than usual. The nature of the ransom offers and negotiations, which appear to center around file extensions, networks and the attack as a whole, raised questions for me about the details of the Sodinokibi ransomware. I was wondering what design architecture would allow them to pull off what they were offering to do in terms of ransom response granularity. So I spent some time digging into it, and I was quite surprised by what I found. As a consequence, next week’s podcast is already titled “Revil's Clever Crypto” where I plan to lay out the amazingly sophisticated cryptographic design of this king of the ransomware hill.

We've learned that the files of the individual MSP victim clients were not exfiltrated before their encryption. And Emsisoft's CTO Fabian Wosar has said that MSP customers who were affected by the attack received ransom demands of $44,999. I was wondering why we were seeing weird pricing of non whole numbers like one thousand dollars shy of $22 million? But when I see $44,999 I'm thinking that it's imitating the retail pricing model. "We're not asking for $45 thousand, only for $44,999! It's a bargain!

Upon closer inspection, however, it appears that $45K ransom is 'per file extension' and that REvil's Sodinokibi often encrypts files with many different extensions. So I don't yet know what that's about. Perhaps they're saying: "You can have all of your DOC files decrypted for $45K, but if you also want your SQL databases back, that'll be another $45K" ... and so on. It's not clear, however, whether the file extensions of the encrypted files are the same as their original extensions, or something assigned by the malware. So this might just be a way of offering to decrypt some specific files or a proportion of all files. But as far as I know, this is the first instance we've seen of "itemized file decryption by extension."

Moving up a level, the REvil affiliate also apparently has the ability to decrypt by MSP customer because ransom payments of $5 million would reportedly allow them to decrypt all of their files regardless of file extension, yet presumably not those belonging to any other MSP's customers. So, you can see what I mean when I say that, if this is true, there's some seriously fancy and cool hierarchical crypto happening here.

And, there's still another level above that! The REvil gang posted the following message to their wonderfully named "Happy Blog":



KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

(There's no indication that anywhere near 1 million systems were infected.) So, decryption can apparently be negotiated not only at the per-victim per-file-type level, and the "all files of a specific victim" level, but also at the all victims of this entire attack level.

One thing should become very clear: Very little of our networked software has been put under the sort of scrutiny and attack that it is being, and will be subjected to, in the future. And unfortunately, this **is** the shape of that future.