SECURITY NOW!

Transcript of Episode #841

Minh Duong's Epic Rickroll

Description: This week we, of course, update on various controversies surrounding Win11 and catch up on the aftermath of last week's Patch Tuesday. We note that REvil's brief reappearance appears to have ended, perhaps this time forever; and we examine, just for the record, the outcome of the big, virtual, 30-nation anti-ransomware meeting where the invitations for China and Russia were apparently lost in the mail. We look at the amazing results of this past weekend's Tianfu Cup 2021 hacking competition in China, at the startling success of a prolific botnet's clipboard hijacking module, and at LinkedIn's decision to dramatically pare down its offerings in China. And then, after quickly sharing Sunday's big news about SpinRite, we're going to take a very fun and detailed look at the sophisticated senior prank orchestrated by Illinois' Minh Duong who miraculously sidestepped his own arrest.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-841.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-841-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. REvil may be gone for good. Steve explains why we might think that. The results from the Tianfu Cup security competition. I wonder who gets the benefit of these security flaws? And then we'll expose, discuss, and break down a very clever senior day prank. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 841, recorded Tuesday, October 19th, 2021: Minh Duong's Epic Rickroll.

It's time for Security Now!, the show where we cover the latest news in security and privacy, and this guy's the guy. Looking over the top of his glasses askance at us, it's Steve Gibson from GRC.com.

Steve Gibson: Yo, Leo.

Leo: How are you, Steve?

Steve: Great to be with you again. I am good. Lots is going on. I have some good news to announce about SpinRite later on. Progress. But something that you caught wind of during last week's podcast was just - I dug into it further, and it was just too fun.

Leo: Yeah.

Steve: So this week's podcast #841 for October 19th is titled Minh Duong's Epic Rickroll. This is an Illinois-based high school senior who got an idea...

Leo: He's actually now at the University of Illinois Urbana.

Steve: Yes. And, well, there's a whole bunch of really cool detail which our particular audience will appreciate, like how he chose to use SSH rather than HTTP and so forth. We have the details of the hack.

Leo: Nice.

Steve: So we're going to talk about that. But of course we're going to update first on various ongoing controversy surrounding Windows 11, catch up on the aftermath of last week's Patch Tuesday. We note that REvil's brief reappearance appears to have ended, perhaps this time forever.

Leo: Oh.

Steve: Yeah. We'll talk about that. And we examine, just for the record, the outcome of the big virtual 30-nation anti-ransomware meeting where the invitations for China and Russia appear to have been lost in the mail. Wonder how that happened?

Leo: Wonder why? Hmm.

Steve: Hello, why is their rectangle blank on that Zoom call? Anyway, we're going to look at the amazing results of this past weekend's Tianfu Cup 2021 hacking competition which took place just last Saturday and Sunday in China; at the startling success which has been sort of under the radar until just recently, well, last week, of a prolific botnet's clipboard hijacking module, we'll remind everybody what that's about; and at LinkedIn's decision to dramatically pare down its offerings in China as a result of a sort of a warning slap they got back in March. And then, after quickly sharing, as I said, Sunday's significant news about SpinRite, we're going to take a very fun and detailed look at the sophisticated senior prank orchestrated by Illinois' Minh Duong, who miraculously sidestepped his own arrest.

Leo: Yeah. I like, by the way, that's a good part of the story, too, yeah.

Steve: Yeah.

Leo: This is going to be fun. I'm looking forward to it.

Steve: Yeah. And of course we do have also a fun Picture of the Week. But just came out of the queue because I thought, you know...

Leo: You get a stack of those by now every week, I bet; right?

Steve: It's wonderful, yeah, yeah.

Leo: All through his Twitter account. DMs are open at @SGgrc.

Steve: Well, this is just one that I got a kick out of. Someone sent me, apropos of technology and the podcast, this shows a sign somewhere in rural America that has some of the movable letters stuck on it that you see in pre-electronic displays. Anyway, so this thing probably stands about, I don't know, three or four feet tall. And it says, "Has anyone tried unplugging the United States and plugging it back in?"

Leo: Just reboot, please. We could use a reboot.

Steve: Yes. That is, of course, the time-honored wisdom when something just doesn't work anymore. Well, when was the last time you rebooted that? Oh. Yeah, that's a good idea.

Okay. So I got a tweet which sort of gave me a platform for something that I did want to follow up on. This was "hickeyj" tweeted, saying: "Hi Steve. Related to your discussions on Windows 11 system requirements, I was interested to see that it was possible to install on" - meaning Windows 11 - "on a 10-year-old PC with a 2nd-gen i5 processor. Running pretty well and seems to be receiving updates."

So I just wanted to close the loop on that question and note that every report is that all machines, regardless of how they have Win11 installed, are reporting that updates are being received. And given the number of people who I've seen citing that not receiving updates is a strong reason not to move to Windows 11 without Microsoft's full blessing, it's clear that just the threat of being cut off from the continual IV drip of Windows improvements and corrections serves as a powerful deterrent, exactly as Microsoft knew it would, while they proceed to deliver updates to every instance of Windows 11, as of course they will. So if anyone's worried, I don't think you need to worry. On the other hand, I don't think there's, as we've said, and as many people are observing, any great need to make the move unless you just, you know, you like pain.

Okay. So last week was October's Patch Tuesday, and it was as eventful as most have been recently for Windows. Threatpost characterized one of last week's updates as: "A PrintNightmare Fix to Fix the Other PrintNightmare Fix." And as it turns out, that fix broke other things. After applying last Tuesday's patches, users and administrators of Windows 10 have started reporting wide-scale network printing problems. And of course this has now become a monthly ritual; right? The culprit this time appears to be KB5006670.

Now, different releases of Windows get different cumulative monthly updates. Windows 11 gets KB5006674. Windows 8 receives '6714. And the oldest Windows 10 supported, which is 1909, receives '6667. But it's '6670, which is used by Windows 10 2004, 20H1 and 21H1, that people are reporting trouble with. Now, given the nature of the trouble, it's more likely, or I would say I guess more than likely, that all releases are actually seeing the same trouble because this seems to be Windows-wide, and that reports are appearing surrounding these three Win10 editions since they are by far the most prevalent Windows 10, being the most recent.

In any event, after installing this '6670, KB5006670, within Win10 networks, users are reporting that they cannot print to network print servers, with some users reporting a 0x00000709 or "Element not found" errors when attempting to print. In online forums, Windows admins have been airing their frustration with the continual printing bugs and have come to a unanimous conclusion: Uninstalling last week's updates solves the problem. And as we know, ever since July, following the PrintNightmare flaws first becoming public in June, although Microsoft, as we know, was informed of them back in March, Microsoft has been scrambling and releasing a stream of what appear to be half-baked security updates intended to fix the various PrintNightmare vulnerabilities as quickly as they can because these are being exploited in the wild. And some of them have been in Windows Print Spooler.

After seeing a bit of this and looking into the nature of the trouble, I made the observation on this podcast some time ago that we appeared to be seeing a true collapse of Windows' printing infrastructure because the bad guys had figured out how to leverage Windows' traditional cross-network print driver auto-installation, which provided Windows with some very popular and cool printing features. Unfortunately, these features had always been exploitable by anyone on the network to elevate their rights and execute their own code. But no one had, until recently.

Ever since then, Microsoft has been attempting to essentially patch the unpatchable. It's unpatchable because it's not a bug. It truly is a feature. Point and Print is just a feature that Microsoft probably now regrets, at least as it's currently implemented. So Microsoft has been attempting to change Windows Point and Print features operation. And while these changes at least somewhat mitigate the vulnerabilities, we've been watching as they have created their own set of new problems for enterprise users.

Imagine being admin of a good-size enterprise whose printing systems keep being broken over and over, month after month. It would become a bit tiresome after a while. And I would wager that the people whose reports we're hearing posted or seeing posted are those whose admins haven't yet stopped hoping. I mean, there must be enterprises where they're just saying, you know, we're going to keep our defenses up for the PrintNightmare problem, but wait until we see a month go by without other enterprises reporting continual problems before we decide to, like, catch up.

Meanwhile, a different issue has beset new Windows 11 users, and guess where it is. Microsoft has confirmed a new and different printing issue for Windows 11. It causes printer installations to fail on systems commonly found in enterprise environments. Microsoft explains that a printer installation might fail when attempted over the network on devices that access printers via print servers using HTTP connections, and that installing printers might also fail when using the Internet Printing Protocol (IPP) in organizations sharing an IPP printer using printer connections.

These problems are said to be specific to Windows 11 because they were fixed in either the September or October updates for the earlier operating systems, which technically predate Windows 11 - except for this October, which update didn't, but did by a week - but not yet for Windows 11. A fix for this is slated for later this month. You know, obviously they know how to do it. It just didn't get into Windows 11 in time.

Last week's release, the good news for Patch Tuesday, it included a fix for CVE-2021 which was numbered 36970. It's a spoofing vulnerability in, yes, Microsoft Windows Print Spooler, that has a pretty high CVSS score of 8.8. Chris Morgan, who's a senior cyberthreat intelligence analyst at Digital Shadows, said that the spoofing vulnerability fix Microsoft pushed out last week is meant to fix new problems that previous patches have introduced.

Okay. Chris said: "While Microsoft provided a fix in their September 2021 update, the patch resulted in a number of new management problems. Certain printers required users to repeatedly input their admin credentials every time an application attempted to print or had a client that connected to a print server." Chris added that: "Other problems included event logs recording error messages and denying users the ability to perform basic prints. As a result, many users skipped the update due to its operational impact" - which is putting it kindly - "ultimately leaving the risk posed by PrintNightmare in place," rather than having them fixed.

So it appears that Windows printing remains tangled. We'll check back next month, see how they're doing. The best news is that none of this affects typical end users who typically just have local printing environments that have never had any of these problems. On the other hand, Microsoft's enterprise customers are obviously where they're keeping their focus.

So a critical remote code execution, a baddie, affecting Word, Office, and SharePoint was fixed, also last week. That's CVE-2021-40486, an RCE which affects, as I said, Word, Office, and some versions of SharePoint Server which can be exploited via the preview pane. The vulnerability is reportedly not completely new to Microsoft, with several other very similar related CVEs documented earlier this year. So it sounds as though this might be another of these recent cases of a partial quick fix that didn't repair the underlying problem, which persisted.

The vulnerability has worried security experts because the attack has very low complexity, meaning very easy to do and get done, merely requiring a user to open a specially crafted file either received by email or via a website. And if from a website, either hosted by the attacker themselves or through a compromised website that accepts or hosts user-provided content. So if you can get this thing to be shown somehow, that's enough. An attacker who successfully exploits the vulnerability may use it to perform actions in the context of the current user. So the code in the opened file would take actions on behalf of the logged-in user under the same permissions as that user. This doesn't give them admin access. But as we know, that's where attacks begin, not where they end.

Okay. So overall there were a total of 74 vulnerabilities of various severities fixed, with one being a true zero-day. The tech press, again, was reporting that there were four zero-days. But there were four critical problems, only one of which was known to be actively exploited. Thus one zero-day. But that one, tracked as 40449, is an elevation of privilege vulnerability in the Win32k.dll. So that's in the kernel. Earlier this year, Kaspersky researchers discovered that an exploit of this vulnerability was being used to elevate privileges and commandeer Windows servers as part of a Chinese-speaking advanced persistent threat campaign from the APT threat actor known as "IronHusky."

The exploit chain was observed to terminate with the installation of a newly discovered Remote Access Trojan (RAT) dubbed "MysterySnail," which put me in mind of those ridiculously named, what were those, vuln something, that was that thing that was spitting out dumb names for vulnerabilities.

Leo: Yeah, the Vulnyms.

Steve: Was it Vulnonyms?

Leo: Vulnonyms, yeah. I don't know.

Steve: Maybe that's a little too...

Leo: Risqu?

Steve: Risqu sounding. Anyway, they were being installed on - this MysterySnail was being installed on compromised servers, with the goal of stealing data. A senior manager of vulnerability and threat research at Qualys said that, if left unpatched: "MysterySnail" - which is a mystery - "has the potential to collect and exfiltrate system information from compromised hosts, in addition to other malicious actors apparently somehow having the ability to gain complete control over the affected system and launch further attacks." I think that quote was a little confused because the other malicious actors are probably those who might also use this Win32sys.dll vulnerability, not others who could somehow jump on the, I don't want to say the tail of the MysterySnail. But there it is. So even though Microsoft appears to be chasing their tail with printing, other good things are being fixed. So yay.

In a little bit of ransomware news, REvil may finally actually be gone for good. The REvil gang has once again shut themselves down for the second time. But if we're to believe its new leader, this is it. In a message posted on an underground Russian-language hacking forum, which was translated into English for the rest of us, the group's new leader, who uses the handle 0_neday which I guess you're supposed to see as Oneday, even though it leads with a zero, so I guess that's supposed to be clever, anyway, we'll call him Oneday posted that they lost control over their Tor-based domains. And of course that ain't supposed to happen.

As we know, the group shut down without any notice previously for the first time on July 13th this year, coincident with one of their affiliates having attacked Kaseya's servers over the 4th of July U.S. holiday weekend and hitting thousands of businesses, thus being called the largest set of ransomware attacks in history, which, not surprisingly, drew a great deal of unwanted attention. Later, we learned that the decision to shut down operations was taken by the group's then-leader known as the four uppercase initials UNKN, I guess thus pronounced "unknown," who took down servers and disappeared. He absconded with the group's finances, which left them unable to pay many of their affiliates, which were other groups who were helping REvil execute attacks and splitting the profits, as we know.

Okay. So then, early last month, the group, minus UNKN, made a formal return using the same name REvil. To prove they were the same group as before, this new REvil incarnation, really just a turned-things-back-on version of the previous one, restored all of their former Tor-hosted portals, such as their victim payment/extortion portal and their data leak site. As soon as they returned, the group's members began launching new attacks, and we talked about the return of REvil.

But last Sunday, two days ago, in a series of messages spotted by an analyst who's with Recorded Future, the group's new admin, that guy calling himself 0_neday, said that a third party had compromised their Tor-based portal. He posted, and this is the English translation: "The server was compromised, and they were looking for me." He said: "To be precise, they deleted the path to my hidden service in the torrc file and raised their own so that I would go there."

Leo: Hmm.

Steve: Yeah.

Leo: Wouldn't they have to have access, physical access to machine, or at least, I mean, to change that rc file they'd have to be in there.

Steve: Yes. Yes. It's a big deal. So 0_neday was saying that someone had created a clone of the legitimate REvil Tor backend panel in the hopes of luring him and then catching him. And that was enough. Already things were not going well for the REvil gang as they were still dealing with the fallout following their July shutdown and the theft of the affiliate funds. Several affiliates were still trying to recover funds stolen by the UNKN guy, and the group's developers were also accused of hiding a backdoor inside their code. The backdoor allegedly allowed the REvil admins to provide decryption keys to victims directly, thus cutting the affiliates out of the loop, both for negotiations and payment.

So basically their cred was in trouble. Since the cybercriminal underworld is primarily driven, such as it is, by reputation and trust - what was that about honor among thieves? - this may have been inevitable, with the writing already being on the wall for what 0_neday decided to do, now declaring that he has shut down the operation permanently, rather than deal with the gang's ever-increasing reputational trouble which probably became unsurvivable.

The Recorded Future analyst who did the decryption of the posting told The Record: "I really hope we just witnessed an offensive operation by the U.S. government. That's how you deal with cybercriminals, using their own methods against them. Release the Hounds."

Leo: It does sound like it might be law enforcement that was setting up a trap; right?

Steve: Yes, yes, yes. I think, you know, we've seen with things like surprising removals of cryptocurrency from wallets which isn't supposed to be possible, you know, it's certainly not easy. And I don't think our government would claim to do something that it didn't do. And the FBI clearly stated that they "recovered" funds that were tied to the Kaseya attacks. So those were REvil and/or affiliate funds.

Leo: Good. I hope it was. I hope it was, yeah.

Steve: Yeah.

Leo: Be nice to know that we can do something about this stuff.

Steve: Yes. Exactly. That we're not entirely, well, incapable. And which brings us perfectly to this next thing I want to talk about, which is this meeting, this virtual 30-country meeting which was held where representatives from the U.S., the EU, and 30 other countries, so 32, have pledged to mitigate the risk of ransomware and harden the financial system from exploitation with the goal of disrupting the ecosystem, calling it, that is, the ransomware attack problem, "an escalating global security threat with serious economic and security consequences."

Now, I'm not a big fan of bureaucracy. I'm highly skeptical about whether anything can have any measurable effect, though it does sound like the behind-the-scenes sort of stuff we can do might be useful. But of course we're all living on top of bureaucracies so it has to do something, too. I wanted to quickly share what was produced and the nature of the saber-rattling. There were also some interesting bitcoin account transaction statistics that are worth airing.

So in a statement released last week following the meeting, officials said, and this is the intro: "From malign operations against local health providers that endanger patient care, to those directed at businesses that limit their ability to provide fuel, groceries, or other goods to the public, ransomware poses a significant risk to critical infrastructure, essential services, public safety, consumer protection and privacy, and economic prosperity." Right. Blah, blah, blah.

Okay. "And to that end, efforts are expected to be made to enhance network resilience by adopting cyber hygiene good practices, such as using strong passwords, securing accounts with multifactor authentication, maintaining periodic offline data backups, keeping software up-to-date, and offering training to prevent clicking suspicious links or opening untrusted documents." And as we know, none of that's bad, but it's also all already well-established best practice. Right? I mean, all of that's what you're supposed to be doing. Yet apparently it's not helping.

Okay. So besides promoting incident information-sharing between ransomware victims and relevant law enforcement and cyber emergency response teams - that's the CERTs - the initiative aims to improve mechanisms put in place to effectively respond to such attacks, while also countering the abuse of financial infrastructure for the sake of laundering ransom payments.

Okay. And again, to me, putting pressure on the payment system makes some sense if you can actually do it. The joint bulletin was issued by ministers and representatives of Australia, Brazil, Bulgaria, Canada, the Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, the Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, the UAE, the U.K., and the U.S. Notably absent, as I said, from the list were China and Russia. And I guess you don't want the fox guarding the chicken coop or the hen house or whatever.

The international counter-ransomware collaboration comes as illicit payments topped nearly $500 million globally in the last two years alone $400 million in 2020 and $81 million in the first quarter of 2021, so I guess they hadn't had recent accounting for the last half or the last two quarters of 2021 necessitating the payment flows that make the activities profitable are subject to anti-money laundering regulations, and the networks that facilitate these payments are held accountable.

In late September 2021, the U.S. Treasury Department imposed sanctions on Russian cryptocurrency exchange "Suex" for helping threat actors launder transactions from at least eight ransomware variants, marking the first instance of such an action against a virtual currency exchange. The U.S. government said: "Treasury will continue to disrupt and hold accountable these ransomware actors and their money laundering networks to reduce the incentive for cybercriminals to continue to conduct these attacks." And, you know, yay. But will that have how much effect? We don't know.

The development also follows an independent report published by the department's Financial Crimes Enforcement Network, that's FinCEN, which potentially tied roughly - now, I'm skeptical about this number, but I'll explain in a second - $5.2 billion worth of outgoing bitcoin transactions to 10 most commonly reported ransomware variants. Okay, now, there's just no way that 10 most commonly reported ransomware variants made $5.2 billion worth in bitcoin.

But in addition they identified 177 unique wallet addresses used for ransomware-related payments based on an analysis of 2,184 suspicious activity reports (SARs) filed between - and here's the question I have - January 1st, 2011, and June 30, 2021. Okay, so that's they're saying a 5.2 billion worth of outgoing bitcoin transactions. But it's spread over a period of the last 10 years. And I wonder whether the historical or the present value of bitcoin was used when calculating that summary. As we know, it's worth way more - I don't know if that's sad or not. But Leo, for us, we have some history. It's worth way more now than it was back then.

At the same time, the bulk of the high-value transactions have been recent when bitcoin has been pricey. In the first half of 2021 alone, ransomware-based financial activity is estimated to have extracted at least 590 million for the threat actors, with a mean average total monthly suspicious amount of ransomware transactions pegged at 66.4 million monthly.

Leo: I wonder, though, where the 5.2 billion number came from.

Steve: Yes, and that's my point.

Leo: That seems like a lot.

Steve: I wonder, yes, I wonder if they summed up all of the bitcoin transactions and then multiplied it by today's...

Leo: Oh, maybe they did, yeah.

Steve: ...bitcoin value.

Leo: That's probably what they did, yeah.

Steve: Exactly. Whereas you know 10 years ago the bad guys would have been immediately taking that money and moving it into their own fiat currency.

Leo: We also know that these guys move money back and forth to make it appear like more transactions are occurring than actually are and things like that. It's, you know, it's a longstanding law enforcement tradition. You stack a hundred bricks of heroin on the table, and you say...

Steve: Then turn the cameras on.

Leo: ... "street value $38 trillion right there. Right there."

Steve: Yeah. So anyway, the most...

Leo: I'm glad they did it.

Steve: Yes. I am, too. The most commonly reported variants are REvil, of course now we think DOA, or RIP, I guess. And that of course was the Sodinokibi software that was really well engineered. But maybe the software will reappear under a new guise. I mean, you know, again, we know that there's been this suspicion that ransomware campaigns, or gangs, rebrand themselves and return. And we've seen clear signs of differently named gangs clearly using ransomware that looked suspiciously similar to previously shut down ware. So, yeah, I wouldn't be at all surprised if some future version of Sodinokibi returns with some new actor's name on it. So anyway, the most commonly reported variants are REvil, Conti, DarkSide, Avaddon, and Phobos. All that we've touched on in the past here.

The Counter-Ransomware Initiative, the CRI, and crying is what people are doing, hopes to drain their funding and take down their operations by disrupting the groups' funding channels. And again, that seems to be the Achilles heel, to whatever degree there actually is one. They said: "We acknowledge that uneven" - this is interesting - "uneven global implementation of the standards of the Financial Action Task Force to virtual assets and virtual asset service providers, creates" - in other words, you can take your money to China or Russia and cash it in there - "creates an environment permissive to jurisdictional arbitrage by malicious actors seeking platforms to move illicit proceeds without being subject to appropriate anti-money laundering and other obligations.

"We are dedicated to enhancing our efforts to disrupt the ransomware business model and associated money-laundering activities, including through ensuring our national AML (Anti-Money Laundering Frameworks) effectively identify and mitigate risks associated with VASPs" - and those are the Virtual Asset Service Providers, oh, we like our acronyms - "and related activities."

Okay. So the efforts to disrupt ransomware groups' abuse of cryptocurrency will include regulators, financial intelligence units, and law enforcement regulating, supervising, investigating, and taking action against virtual asset exploitation. And so, yes, we now know without question that there is somewhere, at some one or multiple locations within the U.S. federal government, someone actively tracking the bitcoin blockchain, looking at what the blockchain ledger reports funds having come in and gone out, and then figuring out what it means. That's happening without question.

And they said: "We will also seek out ways to cooperate with the virtual asset industry to enhance ransom-related information sharing." Reading between the lines there, they're going to bring them all into the fold and say, okay, look, guys, we know you're not bad guys, but we need you to help us with these SARs, these Suspicious Activity Reports. Oh, and the statement noted: "Financial institutions play an important role in protecting the U.S. financial system from ransomware-related threats through compliance with BSA obligations. Financial institutions should determine if an SAR (Suspicious Activity Report) filing is required or appropriate when dealing with a ransomware incident, including ransomware-related payments made by financial institutions that are victims of ransomware."

And remember we just talked about last week how that legislation that had easily passed the Senate and was expected to easily cruise through the House and then be signed into law, would require businesses to report the payment of ransom within, was it - something was said.

Leo: Very quickly, yeah, yeah.

Steve: Was it 24 hours, and something where there was a 24 and there was a 72.

Leo: Right.

Steve: You had to report the event within one of those and the payment within another. But still, so required reporting will be something. And of course if you're then a financial institution that accepted the payment and didn't file a report, then you'd be on the hook, too. So basically the idea is by knitting the government's monitoring into these transactions, people are, you know, very much like the IRS, you know, you'd better pay your taxes, or you can be in trouble. So you'd better file reports or we're going to get you.

So anyway, who knows what'll happen. We've observed that the ransomware scourge has largely been enabled by the existence of a means of securely transferring payment anonymously and nearly untraceably. So attacking that payment chain to whatever degree is possible might at least have some hope for success. But I doubt that telling potential victims to alter their behavior, right - like, oh, don't click those links, we told them already, and they still did - will have any discernible long-term effect. There are just too many potential fish already in the Internet sea. So lots of victims and targets. And Leo, I'm a victim of...

Leo: Great thirst.

Steve: Dehydration.

Leo: Dehydration. Have a drink. Everybody drink when you hear Steve say, "Let's drink."

Steve: Well, we have a lot of fun on this podcast taking a look at the hacking competitions that occur periodically...

Leo: Always enjoy these, yeah.

Steve: ...in our industry, yeah. They are fun. So just this past weekend, this last Saturday and Sunday, the Tianfu Cup 2021 competition occurred. In that competition Windows 10, iOS 15, yes, 15, just still got the paint still drying, Google Chrome, Apple Safari, not surprisingly Exchange Server, and Ubuntu 20 were all successfully hacked, among others. They were broken into and compromised using original, never-before-seen exploits during this just completed 2021 Tianfu Cup. It's the fourth edition of the international cybersecurity contest being held in Chengdu, China.

The competition's targets included Chrome running on Windows 10 21H1; Apple Safari running on MacBook Pro; Adobe PDF Reader, pick your platform; Docker CE; Ubuntu 20 and CentOS 8; Exchange Server 2019; Windows 10; VMware Workstation; VMware ESXi; Parallels Desktop; iPhone 13 Pro running iOS 15; domestic mobile phones running

Android; QEMU VM; the Synology DS220j DiskStation for some reason; and also the ASUS RT-AX56U router.

Our long-time listeners will recall that this Chinese version of Pwn2Own was started three years ago, in 2018, after the Chinese government regulations barred their wonderfully competent and capable homegrown security researchers from participating in international hacking competitions due to national security concerns, as it was said. I wondered if maybe it was perhaps over worries that they might not choose to return home. In any event, Chinese security researchers took home over the weekend $1.88 million.

Leo: Wow.

Steve: Yes.

Leo: Now I know why people participate in these.

Steve: Yeah. After competing and hacking over the past weekend, as I said, the grand winners were researchers from the Chinese security firm Kunlun Lab, who took home $654,500, which was a third of the total purse of 1.88 million.

Okay. So back in July, the organizers of the competition announced a series of targets, that is, those I just listed, and participants had until last weekend to target and prepare exploits that they would execute on the devices provided by the organizers on the contest's stage. Each team had three five-minute attempts to run their exploits, and they could register to hack multiple devices if they wished to increase their winnings. Overall, there were 16 possible targets, and 11 participants mounted successful exploits against 13 of those 16. That is, successful; right? Hacked 13 of those 16, with the exception being the three that weren't, that Synology DS220j NAS, the Xiaomi 11 smartphone, and an unnamed Chinese electric vehicle which for some reason no one elected to target. Maybe they just didn't have them or who knows. Anyway, attacks were successfully mounted against every other target.

Windows 10. And I should say not just once, often. Windows 10 was hacked five times, five different ways. Uh-huh, yeah.

Leo: I'm sure once was through the printer; but okay, go ahead.

Steve: Boy, yes. Adobe PDF Reader, four times. Ubuntu 20, four times. Parallels VM, thrice. iOS 15, also three times. Apple Safari, twice. Chrome, twice. That ASUS AX56U router, twice. Whoops. I hope it wasn't a remote attack. Docker CE, once. VMware ESXi, once. VMware Workstation, once. QEMU VM, once. And Microsoft Exchange Server, once.

Most of the exploits were privilege escalation and remote execution bugs. In other words, the things an attacker would want. Two of the exploits presented stood out. The first was a zero-click, zero-interaction, remote code execution attack against a fully patched iOS 15 on the latest iPhone 13. Yow. Zero-click, zero interaction. Complete remote code execution and takeover.

Leo: Now, I'm just glad they saved it and didn't sell it to the NSO group. I mean, that's the good news.

Steve: Yes.

Leo: I presume this is like Pwn2Own where, if you win, and you use an exploit, you then give it to the company to fix; right?

Steve: Yes.

Leo: Yeah. So that's good.

Steve: Yes. And since this just happened...

Leo: They could have made millions from NSO Group.

Steve: That's right. Since this was just Saturday and Sunday, it isn't incorporated in any of our current iOS 15.0.2.

The second was a simple two-step remote - yeah, two-step, do-si-do - remote code execution chain against Chrome, which is something we've not seen in any hacking competition in years. So there are things that you can get Chrome to do. And as we know, Chrome's at, what was it, 14, I think? Or maybe it was a baker's dozen, I don't remember, of problems so far this year in Chrome, zero-days. But this one was a bad remote code execution that was simple to do.

There were also two competition-related tweets that were noteworthy. One tweet was: "The iPhone 13 Pro Safari escaped from prison remotely, and Chian Pangu won the highest single bonus of $300,000 in history for that one." And again, look at what you get for a highly desirable target with a highly exploitable exploit.

Leo: An iPhone no-click, I mean, millions and millions; right?

Steve: Yes.

Leo: I mean, you'd be - a lot of bidders going for that one. Yeah. Wow.

Steve: Yes. And second tweet: "First confirmed entry for day one of Tianfu Cup, Kunlun Lab pwned Google Chrome to get Windows system kernel level privilege with only two bugs. First time since 2015." And something interesting about this. Aside from the competition, many Western eyes were on this year's contest for another reason. One of the iOS exploits showcased at last year's competition was used in a cyberespionage campaign carried out by the Beijing regime against its Uyghur population.

Leo: Oh. Now, even though this is a Chinese competition, I am hoping the Tianfu Cup doesn't supply the CCP with these exploits. Oh, god. That would be terrible. It doesn't. It can't.

Steve: It could be parallel discovery. But it is the case that an exploit that did appear in last year's competition was being used against the Uyghurs. So that observation has reinforced the belief among Western security experts that Beijing may have forbidden Chinese security researchers from participating in hacking contests held abroad in order to better harness their exploit-creating capabilities for their own purposes.

Leo: Yeah, this is held in Chengdu.

Steve: Yeah.

Leo: Wow. Yikes.

Steve: Yeah. Okay. We've talked about clipboard hijacking, the process whereby malware waits patiently in a system in the background, silently pinging the system-wide clipboard, looking for the sudden appearance of a valid cryptocurrency wallet address and, when found, would wait for the user to paste that content into its target app, then replace the pasted contents on the fly with one of its own addresses that it controlled. In this sneaky way, the unwitting user would be irretrievably sending their cryptocurrency to the hacker's wallet. But just how much cryptocurrency could such attacks net? Would you believe, in the jargon of Maxwell Smart, would you believe $24.7 million in Bitcoin, Ether, and Dogecoin?

Okay. First spotted in 2016, the MyKings botnet, as it's named, or one of its names, has been one of the most sprawling malware operations in recent times. The gang behind this botnet, also referred to as the Smominru or DarkCloud botnet, same, operates by scanning the Internet for exposed Windows or Linux systems running unpatched software. Using known exploits for those unpatched vulnerabilities, the MyKings gang infects these servers and then moves laterally inside their networks. Reports published through the years by Guardicore, Proofpoint, Qihoo 360, VMware's Carbon Black, and Sophos have described MyKings as one of the largest malware botnets that has been created over the past decade, with the number of infected systems sometimes easily totaling more than half a million hacked machines.

In its early years, the botnet was primarily seen deploying a Monero cryptocurrency miner on infected hosts to directly generate profits for the botnet's operators. And a January 2018 report by Proofpoint estimated the group's profits at the time at around $3.6 million, based on the Monero funds they had found in some wallets they linked back to the group. But through the years, the MyKings group operations and malware have evolved from a hack-and-mine operation. The botnet became a Swiss army knife of nastiness, with all sorts of modules for moving across internal networks, spreading like a worm, and carrying out various attacks.

In 2019, Sophos had said that one of the newest modules it had spotted then was that "clipboard hijacker." And at the time, Sophos had concluded that this MyKings clipboard hijacking module probably wasn't that successful or widely used, "never received more than a few dollars," and that stealing cryptocurrency by hijacking the clipboard didn't look like "the most profitable operation of MyKings." But in a report just published last week, Avast said that since 2019, MyKings appears to have perfected this module, which now detects addresses pasted for 20 different cryptocurrencies. The Avast researchers said they had analyzed more than 6,700 samples of the MyKings malware to identify and extract more than 1,300 cryptocurrency addresses used by the gang to collect their funds. In these addresses, researchers said they found more than $24.7 million in Bitcoin, Ether, and Dogecoin.

Leo: Doge. It's Doge.

Steve: Oh, Doge, sorry, Doge.

Leo: It's a meme. It's a little dogey. It's a Shiba Inu doge.

Steve: Oh, yeah, there's no "d." There's no second "d" in Doge.

Leo: Yeah, Doge. It was a joke coin until it started becoming valuable.

Steve: Well, in fact it's the most money here.

Leo: I know.

Steve: Bitcoin, the breakdown of that 24.7 into the top three, Bitcoin is at 6.6 million, Ethereum at 7.4 million, Dogecoin at 10.65.

Leo: What?

Steve: So it's more than the others.

Leo: That's hysterical.

Steve: Yeah. Actually, they must be very low value because that 6.6 bitcoin is only 132 of them, whereas that 10.65 million in Doge is 44.618 billion.

Leo: I just think it's bizarre that a ransomware gang would demand Dogecoin. It's hysterical to me. But it's interesting. So it's not just Bitcoin.

Steve: Yeah. I think one of the reasons may be that it's one means of staying under the radar.

Leo: Yeah, yeah, yeah.

Steve: Although also remember these are not ransomwares. These are currency transfer intercepts. So people buying and selling, using Dogecoin, have lost $10.652 million.

Leo: Oh, I see.

Steve: Where they send payment to someone who says, "When are you going to send it?" And the guy says, "I already did." And the guy's, "I didn't get it."

Leo: Yeah. Now it makes sense. Anybody who's using Dogecoin is probably ripe for the plucking.

Steve: Yeah. So, and what's interesting is that Avast used their AV network to collect the 6,700 samples of malware. So they have a really - they have a great perspective into what's going on. The Avast researcher said: "We can safely assume that this number is in reality higher because the totals we show consist of money gained in only three cryptocurrencies from the more than 20 in total being used by the malware."

While the researchers said that some funds were linked to MyKings' past cryptocurrency mining activity, the vast majority appears to have come from the overwhelming success of the clipboard hijacking module. In other words, intercepting the transfer at the desktop of cryptocurrency payments and receptions. Well, payments aimed at someone changing the destination wallet. And, you know, we use cut-and-paste because who can type that? I mean, of course you're going to use your wallet in order to copy and paste that into a destination field.

So at that point the malware says, aha, and changes it. Avast said that since the beginning of 2020, its own AV software had detected and flagged MyKings malware attacks on more than 144,000 computers. So it's a widespread malware. And I forgot to put in the show notes, but everybody, the takeaway is be careful. If you're actively transacting in cryptocurrency, make sure you don't have a nasty sitting quietly in your machine, playing gotcha. Anyway, but since the users of their AV represent a small fraction of all users, the number of systems attacked is certainly higher, and there's probably a lot of these transactions that Avast was not privy to.

As a result of these just-published findings, malware analysts have completely changed how they are viewing this botnet. With the ability to carry out large-scale exploitation attacks, a way to profit from their operations, a large number of infected hosts, and the ability to download and run any additional payload the MyKings operators may wish, the botnet has now established itself, that is, the MyKings botnet, as one of the most dangerous malware operations going today. So I wanted to put it on all of our listeners' radar.

LinkedIn is going to dramatically pare down its offering in China. They have for some time been the only major American social network allowed to still operate in China. But last Thursday the - as we know, Microsoft bought them - Microsoft-owned company announced that it would be dramatically slimming down its operation, and that until recently, well, it will be slimming down its operation, that it will temporarily pulling up stakes and shuttering its platform until it comes back with something else.

LinkedIn said that "significantly more challenging operating environment and greater compliance requirements" by Beijing authorities were behind the decision. Other social media services, as we know, like Twitter and Facebook, have been blocked in China for years. Those companies' inability to control what's posted on their sites disqualified them for their presence in China. And until now, LinkedIn had been able to maintain its presence only because it was censoring many of the posts being made by its users. They said: "While we found success in helping Chinese members find jobs and economic opportunity, we have not found that same level of success in the more social aspects of sharing and staying informed."

Even so, LinkedIn ran afoul of Chinese Internet content regulators in March when China's Internet watchdog, the Cyberspace Administration of China (CAC) warned LinkedIn that it was failing to control what CAC saw as objectionable political content. The regulator told LinkedIn it had to do better. In response, the company wrote a kind of self-criticism and filed it with the CAC. Around the same time, the company announced publicly that it would "temporarily" suspend new sign-ups. And in their statement yesterday, LinkedIn made clear that while it was trying to abide by local regulations, in the end doing so became too much. They said: "We're also facing a significantly more challenging operating environment and greater compliance requirements in China."

And as I said, LinkedIn is not abandoning China completely. The company said it will eventually offer its 50 million Chinese members a slimmed-down version of the platform, basically an app focused just on job listings. Chinese users will not be able to share or comment on posts, which has been a key social media feature of LinkedIn's platform everywhere else.

In 2014, when LinkedIn began working in China, it said it was a global platform "with an obligation to respect the laws that apply to us, including adhering to Chinese government regulations for our localized version of LinkedIn in China." The company even sold a stake of its Chinese operation to local venture capital partners and said it would be able to abide by local law by using software algorithms and human reviewers to make sure posts did not offend Beijing. But apparently that was insufficient. So it'll just be a shadow of its normal offerings.

I had one really nice closing-the-loop tweet that I saw last week posted by a Fred A. Rhoades III. I grabbed a snap of it as it appeared in my TweetDeck. He had a bunch of fun icons and emojis and then said "!!!BOOM!!!" surrounded by parens. He said: "Anybody out there that deals with MS Windows and hard drives, @SGgrc (Gibson Research Corporation) and his #Insanely #Awesome #SpinRite #Software!"

Leo: He was very happy.

Steve: He was quite happy. He says: "It's a must-have!!! Saved my" - and then we have the "bacon" emoji - "again." And let's see, looks like seven exclamation points. Then the peace symbol, a smiley face with dark glasses, and a thumbs up. Anyway, I publicly replied, thanking him for his posting. To which he replied: "Every time I run into PC geeks, I always tell them about your software and why they need it. It has super powers that I've never experienced from any other software." So Fred, thank you for giving me a perfect lead into my SpinRite update.

Yesterday, oh, actually now it's Sunday. I wrote this yesterday. So Sunday I posted the fourth prerelease of SpinRite to the GRC spinrite.dev newsgroup. The gang there has been having a field day running it on all of their multiple PCs and reporting their results. I have a punch list of things to fix as a result, and I have an idea actually for a cool new surprise feature I haven't even told them about, which will appear on the benchmark's conclusion screen. So I'll be working to get everything resolved and running before I move forward again.

This is a key juncture because everything from here on out builds upon this foundation that we're now working to make bulletproof. In other words, there isn't anything else that can go wrong once a descendant of this fourth release is running for everyone on all their hardware. And actually it looks like I broke something that was running at the end of the third release, the third prerelease, which no longer works. So like when the problems are being reported, they'll run it on the last of the third prerelease, where it works.

And that was at the end of April, so there's been a lot of time, and I've done a lot of rewriting. There was a lot of things I changed. I thought I was making things better, probably was, but I broke something. And it looks like it's around an Intel chipset on Lenovo laptops. So I've got plenty of those around here. I just didn't try it. So I'll do that. I'll fix that. And then I think we're going to be in good shape.

Anyway, we're currently, what we're doing, is locating all of their systems' controllers, wherever they are, and all of the drives attached to each one. We're determining how to best determine - "we" meaning SpinRite - determining how to best communicate with each drive through its controller, then doing so with that method, and performing read and write confidence tests to verify everything. And then finally benchmarking. The fact that we're now performing benchmarks on these drives in SpinRite and seeing hundreds of megabytes per second of throughput means that we'll be seeing many gigabytes per minute and terabytes per hour to deliver vastly faster performance than we've ever had, while also even improving upon SpinRite's ability to recover data from troubled mass storage devices because it'll be so much faster, I'll be able to do basically dig a little bit deeper. So yay.

Leo: Yay, yay, yay.

Steve: And thank you, everybody, for your ongoing support of this work. I really appreciate it.

Leo: Get your copy. Go to GRC.com. Get yourself a copy.

Steve: Here's my water. You know what's going to happen next.

Leo: You're almost out of that gallon jug. You'd better get some more water in there. This one's just for fun, though. I like this story.

Steve: This one is neat. And, yeah. Okay. So just to start us off all on the same page, Wikipedia explains rickrolling as, it says: "Rickrolling, alternatively rick-rolling or rickroll, is a prank and an Internet meme involving an unexpected appearance of the music video for the 1987 song 'Never Gonna Give You Up,' performed by the English singer Rick Astley. The meme is a type of bait and switch using a disguised hyperlink that leads to the music video. When victims click on a seemingly unrelated link, the site with the music video loads instead of what was expected, and in doing so they are said to have been 'Rickrolled.' The meme has also extended to using the song's lyrics, or singing it, in unexpected contexts." And as we'll see, that's what happens in this case.

Upon learning that a quite industrious Illinois high school senior by the name of Minh Duong, he's of Vietnamese descent, had deeply hacked not only his own high school's network, but the networks of his entire high school district, my initial dread was imagining that he'd been immediately arrested by district officials who lacked any sense of perspective or humor. After all, these days apparently just the "View Source" menu item on a web browser...

Leo: Oh, you saw that, yeah.

Steve: ...and then viewing the source is all it takes. And yeah, Leo, I didn't mention this, but many people tweeted this. There was some idiot governor somewhere...

Leo: Missouri, governor of Missouri, yeah. I know, yeah.

Steve: So a reporter clicked View Source on some website and noticed that all, was it the Social Security numbers of a thousand government employees was like, visible on the page, in the source.

Leo: Yeah. The reporter even did everything right. They disclosed it to the state before they printed the story the next day. And still the governor called him a hacker. "He should go to jail for this."

Steve: That's advanced hacking, Leo.

Leo: It's too embarrassing is what it is. It's just he was just embarrassed.

Steve: Wow.

Leo: Anyway, yeah. Everything, the hacking...

Steve: Anyway, the good news is...

Leo: I'm surprised, I am totally surprised that Minh did not go to jail, go directly to jail.

Steve: Yes. And you'll hear both he and I have some caveats about this. The good news is the nature and intent of this prank was kept in perspective, and District 214's cybersecurity was improved as a result.

Leo: Collects on the website videos of this happening. The bell goes off, and [laughter]. Little later in the video he goes down the hall, and you see all the students, it's happened in every classroom in every school in every district. Oh, my gosh. I know you'll talk about what he did. But he did some very clever things to make sure teachers couldn't mute it, couldn't stop it.

Steve: Oh, yeah. We have everything here. And the video you showed started just before the event. It actually, well, I have all that here, so I'll explain it all.

Leo: Yeah.

Steve: Okay. So what did Minh do, and how did he do it? I should first explain that this didn't just happen. The rickrolling event began at 11:55 a.m. on Friday, April 30th. And actually that's a typo. It's 10:55 a.m. on Friday, April 30th, which was a time carefully chosen so as to be minimally disruptive and intrusive. Minh has since graduated and is now studying cybersecurity at the nearby University of Illinois. But the nature, breadth, and depth of his epic hack came to the cybersecurity industry's attention when he for the first time posted the whole back story on his whitehoodhacker.net blog.

Okay. So to discharge the suspense of what Minh's fellow students experienced, this was the culmination of several years of planning. The operation was code-named Big Rick. At 10:55 a.m. on Friday, April 30th, all of the presentation screens and projectors in every class in every high school in the district switched on. If they were motorized projection screens, they'd lowered and deployed themselves with no one doing anything. The remote control was ineffective to move the screen back up. Nothing worked.

The district uses something known as the AvediaPlayer, which is an IoT device, as the common interface for all classroom screens. At first, the only thing displayed simultaneously on every screen in every room in the district was a message stating that an important announcement was forthcoming, with a timer patiently counting down from five minutes. So nothing like this had ever appeared on any of the screens before. So naturally, when the timer hit zero, everyone was waiting to see what the announcement would be.

And in that video that he has on his page and which you're showing, Leo, we see one instructor who's, like, looking at the screen behind him like, what the heck is going on? I mean, he has no idea what's happened. At one point he picks up the remote control and tries to, like, shut it off, but it doesn't work. And so it's like, okay, well. So everyone wanted to see what the announcement would be. They immediately realized that it was a sophisticated prank when Rick Astley appeared on every screen and began crooning the well-known lyrics to "Never Gonna Give You Up." The video ran for 10 minutes, then shut down, and the entire system reverted to its normal operation as though nothing out of the ordinary had happened.

Leo: It's so funny.

Steve: But the prank wasn't quite complete. At 2:05 PM, all of the school bells rang, signaling the end of a class, just as they should. But instead of a bell sound, they played the song again.

Leo: Now, we should explain to non-Americans, and I don't know if this is anywhere else, but in the U.S. there is a tradition of senior pranks for graduating high school seniors. There's always a prank, or two or three. So this is a senior prank. That's what this is.

Steve: Right. It might involve the school bus appearing somehow in a hallway, reassembled overnight.

Leo: Yes, yes. There are far more destructive senior pranks. This isn't as bad as some of them.

Steve: So in this case everyone got rickrolled a second time at the end of the day. After that, Minh immediately sent a 26-page report to the school district, outlining exactly how he and his friends had pulled this off. And because of that, the district decided not to press charges. The director of technology had the class to thank them for finding the flaws in their system.

Okay. So now we know what Minh and company did, let's get his perspective. But before I go any further, for any of our younger listeners, please do not take this one-off success, which fortunately had a very happy ending, as any form of permission to do anything similar. Minh was fortunate. He was not entitled to receive the leniency that he was given. Make no mistake, there are computer and network intrusion laws on the books that Minh absolutely violated. It could so very easily have gone so very wrong for him and his friends. The decision could have been to make an example of them with a zero-tolerance policy, and I would bet that there was some discussion along the way to that end. So I do not mean to be glamorizing something that I myself would never consider doing today. Now, okay.

Leo: But when you were a senior in high school.

Steve: Given my history...

Leo: Yes?

Steve: ...I'm quite certain that I would have been foolish enough to do it when I was 18. Everyone knows the story of the portable dog killer and some of my other youthful antics which I somehow survived without a police record. But it's been 48 years and the Internet since I was 18, and times have really changed since then. The grown-ups are terrified of the technology they don't understand and fear that they cannot control. So poking them with a stick, or with a ping packet these days, is probably not the best idea. Please don't do it. Really.

Okay. With that said, here's how Minh recently described the "Big Rick" hack. I want to share this with our listeners because there are some wonderfully fun techie details that really serve to bring it to life. So he wrote: "On April 30th, 2021, I rickrolled my high school district. Not just my school, but the entirety of Township High School District 214. It's one of the largest high school districts in Illinois, consisting of six different schools with over 11,000 enrolled students.

"This story isn't one of those typical rickrolls where students sneak Rick Astley into presentations, talent shows, or Zoom calls. I did it by hijacking every networked display in every school to broadcast 'Never Gonna Give You Up' in perfect synchronization. Whether it was a TV in a hall, a projector in a classroom, or a jumbotron displaying the lunch menu, as long as it was networked, I hacked it. In this post I'll be explaining how I did it and how I evaded detection, as well as the aftermath when I revealed myself and didn't get into trouble." Okay. Now, clearly recognizing the same danger I recognize, Minh then places into his description a clear disclaimer. He posts: "This post is for educational purposes only. Do not perform similar activities without explicit permission."

He said: "We prepared complete documentation of everything we did, including recommendations to remediate the vulnerabilities we discovered. We sent a comprehensive 26-page penetration test report to the D214 tech team [District 214] and worked with them to help secure their network. With that said, what we did was very illegal, and some administrations may have pressed charges. We are grateful that the D214 administration was so understanding." And actually there's a little bit more. The details of the way they sent the report and when they sent the report, we'll get to at the end.

So under "Initial Access," he writes: "This story starts with my freshman year, when I did not have much technical discipline, a time that I can only describe as the beginning of my script kiddie phase. I didn't understand basic ethics or responsible disclosure, and jumped at every opportunity to break something. So obviously I became curious about the technology at my high school. And by 'curious,' I mean port scanning the entire IP range of the internal district network."

He says: "I had a few friends help out with this project. And, oh, boy, did we scan. Our scanning generated so much traffic that our school's technology supervisor caught wind of it and came in at one point to ask us to stop. Of course we did so immediately. But by then we had finished scanning the first half of the district's 10-dot address space, in other words a total of 8,388,606 IPs." And I presume they scanned the entire port space of every one of those IPs.

He said: "From the results, we found various devices exposed on the district network. These included printers, IP phones, and even security cameras without any password authentication." And he says: "This is where I state the disclaimer again: Never access other systems in an unauthorized manner without permission." He says: "The district tech team was informed about the issue, which they resolved by placing the cameras behind ACL restrictions." ACL meaning Access Control Lists, meaning only some privileged IPs were able to view those IPs. He says: "However, many devices remained exposed to the student network more importantly for this post, the IPTV system."

So I'll just interject here to observe that the phrase "many devices remain exposed to the student network" should horrify any IT administrator. Having high school students sharing a network that also contains administrative functions is insane all by itself. It's about a thousand times worse than having IoT power outlets and light switches phoning home to hostile foreign nations. If ever there was a case to be made for network segmentation, elementary school, junior high, and high schools are it. No one should even consider allowing those precious little darlings anywhere near administrative network functions. Any network that students have access to should be able to touch the Internet and nothing else.

Okay. So continuing with what Minh wrote, he says - I guess that's Exterity, yeah. "Exterity IPTV System. Before moving on, I will briefly explain the IPTV system. The system is composed of three products: AvediaPlayer, AvediaStream, and AvediaServer. AvediaPlayers are small blue boxes that connect to projectors and TVs. They can send serial commands to their respective device to turn the display on and off, change inputs and volume, switch channels, et cetera." And also roll and unroll the screens. "These receivers include both a web interface and an SSH server to execute the serial commands. Additionally, they run embedded Linux with BusyBox tools and use some obscure CPU architecture designed for IoT devices called ARC (Argonaut RISC Core).

"Next, AvediaStream encoders connect to devices that broadcast live video. They encode the live feed coming from these devices to the AvediaPlayer receivers, which display the stream. Encoders are attached to computers that need to broadcast a stream, such as text carousels or morning announcements. These also have embedded software similar to AvediaPlayers. Last but not least, AvediaServers allow administrators to control all receivers and encoders at once. These have typical x86_64 processors and run the enterprise Linux distribution, CentOS. Like the receivers and encoders, they also have web interfaces and SSH servers. Since freshman year, I had complete access to the IPTV system. I only messed around with it a few times and had plans for a senior prank, but it moved to the back of my mind and eventually went forgotten.

"Fast-forward to the second semester of senior year, early 2021. All the schools were doing hybrid instruction because of COVID-19 pandemic. Up to this point, in-person instruction was opt-in, with most students opting to stay remote, myself included. But in March, the superintendent announced that in-person instruction would switch to an opt-out model on April 5th. Since almost all students would be back in school, I realized that a senior prank involving the IPTV system was now worthwhile. A few days later, I decided to share my thoughts with a few close friends. I gathered a small team across the district and started preparing. We began to refer to the operation as 'the Big Rick.'

"The first thing we focused on was figuring out how to control all the projectors at once. While we could send commands to each receiver using a web interface, it would not be ideal spamming HTTP traffic to every receiver simultaneously. Instead, I used the SSH access on each receiver as the command-and-control channel. I developed a simple shell script that would serve as a staged payload to be uploaded in advance to each receiver ahead of time. This script contained various functions that could execute requests to the web interface locally on the receiver. Thanks to the increased flexibility from the payload, I could also back up and restore all receiver settings to the file system after the rickroll was over.

"In the actual payload, I repeatedly looped commands to keep the rickroll running. For example, every 10 seconds, the display would power on and set the maximum volume. This way, if someone" - a teacher - "attempted to power off the projector or mute it, it would revert and continue playing. The only way to shut it off would be to pull the plug or change the input source." He says: "Looping input causes flashes even if the current source is the same as the latest source. I had to rely on a failsafe input switch that activated right before the rickroll started to ensure everyone was tuned in. You can see this flash in the video at the 48-second countdown." In other words, what he meant was he would have loved to be able to also force the input selection to continually refresh every 10 seconds, but he refused to tolerate a 10-second flash interruption. So he decided just to do it once and be satisfied with that. And we're looking at it now in the video that Leo's playing.

Leo: Here it comes.

Steve: 53, 52. So it'll be at 48.

Leo: There it goes.

Steve: Yup, there it is. It blanked out. And that's as he sent the selection to the projector just to make sure that it was on the correct channel. And I'm sure he did it once at the - he did it beforehand at the five-minute, the start of the five-minute countdown, and then again shortly before the video was played.

Leo: It's so impressive that he thought so much of this out. It's really neat.

Steve: Yes. Oh, and wait till you get to the testing, Leo, how he tested this. Because, you know, you wouldn't want anybody to see it happening. And you've got to test that kind of thing. He said: "The vulnerabilities exploited to gain initial access were implementation-specific. In other words, the district's tech team was at fault for using default passwords. However, I discovered vendor privilege escalation vulnerabilities in all of Exterity's IPTV products, allowing me to gain root across all systems. One of these bugs was a simple GTFO-bin, but the other two are novel vulnerabilities that I cannot and should not publish."

Okay. The expression "GTFO-bin" is a reference to a curated list of Unix and Linux binaries that can be used to bypass local security restrictions in misconfigured systems. So Minh found a command, just a standard Linux command, on the system that could be leveraged due a fault in some other security configuration. So he was able to get through.

He said: "The next issue we tackled was setting up a custom video stream to play the rickroll in real-time. We needed to broadcast multicast traffic, but only the AvediaStream encoders or the AvediaServers could do this because of ACL restrictions." Meaning he couldn't do it from some random computer on the network. ACL, you know, there were some Access List Controls that meant you had to be an AvediaServer or AvediaStream encoder.

He said: "Setting up the stream was arguably the most time-consuming part of preparation because testing was an absolute pain. I only needed a single projector for development, but it's not easy when classes are using them during the day. So I tested at night instead. I would remotely connect to one of the PCs in the computer lab with the front camera facing the projector. Then I would record a video to test if the projector displayed the stream correctly." Okay, so just to expand on that a bit, Minh set up a PC in the computer lab, to which he would be able to gain remote access from home in the evening, with its web cam pointed at the classroom's presentation screen to record and capture whatever the screen would show as he was developing the code to take over the entire district remotely.

He said: "The lag seen in the video is one of the earlier issues I faced with the stream. It turned out trying to redirect UDP traffic through the AvediaStream encoders added too much latency. I fixed this by broadcasting to multicast directly from an AV server using ffmpeg." So he ended up hacking one of the AvediaServers and using that as his broadcasting host. And then he said: "Hopefully I didn't scare any late-night staff."

Under "An Unexpected Development," he said: "It was April 27th, a mere three days away from the Big Rick finale, when one of my peers discovered a new IP range full of IoT devices following a scan. It turns out it was the recently installed bell system, called Education Paging and Intercom Communications." Thus EPIC. Thus the Epic Rickroll. "The majority of the devices in this range were speakers found in hallways, classrooms, et cetera. Similar to how AvediaPlayers linked to AvediaServers, each speaker connected to an EPIC server for their respective school. These servers had a web interface locked behind a login page. Only a single EPIC server had been left with its default credentials configured. We were able to modify the bell schedule at will, as well as upload custom audio tones. We could change the bells to play 'Never Gonna Give You Up' instead."

Leo: That's so amazing.

Steve: "However, we only had access to this individual school's EPIC system since it was the only one with vulnerable credentials. Or was it? I discovered that the EPIC server we compromised performed weekly backups of its configuration to an external SMB file share. The credentials for this SMB server were the same default credentials for the EPIC system. Each backup included a SQL dump of account usernames and password hashes. Well, what if the other EPIC systems have backup servers as well? And since these backup servers are separate from the EPIC servers, they might still use default credentials.

This scenario was precisely the case. From there, I was able to access the password hashes for the other EPIC servers and identify a local admin account available across all the EPIC servers. After some password cracking, we effectively had control over all the bell schedules throughout the entire district."

Leo: That's the normal bell. Maybe this is annoying. I'm going to turn it down. It is going to play something eventually; right?

Steve: I don't know. I think that all it played was the rickroll.

Leo: Oh, because this is not - this is just the bell. This is the normal bell. Huh. I'm just playing it off the web page.

Steve: Oh, that's interesting, yeah. So it's there. Huh. I wonder why it's not the modified one.

Leo: It's very annoying. I apologize.

Steve: Yeah. Sorry to the students.

Leo: Yeah, that's a horrible bell. We used to have actual bells in school. I don't understand this.

Steve: Yeah, [mimicking bell], yeah.

Leo: That's a terrible noise.

Steve: So execution. "One of our top priorities was to avoid disrupting classes, meaning we could only pull off the prank before school started, during passing periods, or after school. Before the pandemic, some schools would start earlier, some would start later, some had block scheduling, and some would have all their periods in one day. Conveniently, due to COVID-19, all the high schools in the district were now on the same block schedule, so we didn't have to worry about scheduling on a per-school basis.

"Another thing was that final exams were right around the corner. The biggest concern was standardized testing, which wouldn't have breaks during passing periods. We decided on April 30th, which was the Friday before AP exams started. We surveyed extensively to check if any significant tests were happening on this day. We were fully prepared to abort if we learned any standardized testing was taking place.

"In the weeks before the Big Rick, we staged the C2 payload on all of the AvediaPlayers in an automated manner, carefully spreading our actions to avoid detection. On the day of the Big Rick, we used two of the seven AvediaServers as the C2 masters, which would connect to all the AvediaPlayers and trigger the payloads.

"At 10:40 a.m., rickroll stream goes live with a 20-minute countdown." And elsewhere he said at 10:55 and a five-minute, so I think maybe he changed his numbering. He says: "At 10:55 a.m., AvediaPlayer systems are initialized." Oh, no. So rickroll stream goes live with a 20-minute countdown. For some reason that was just to get everything rolling, but he doesn't actually turn things on until five minutes before.

"At 10:55 a.m., AvediaPlayer streams are initialized, turning on displays and changing the active channel to the rickroll stream. 11:00 a.m., the stream finishes the countdown with the rickroll playing at the end of the first block. 11:10, the payload restores the AvediaPlayer streams to their previous state and removes itself. 2:05 p.m., the end of the third block bell plays a rickroll instead of the dismissal bell. 2:15 p.m., the penetration testing report is automatically sent to the technical supervisors."

We also scheduled another modified bell for 3:25 p.m. If district tech hadn't still figured out what had happened to revert the bells, a one-minute version of the three-second dismissal bell would play at the end of the day. They did figure it out.

Leo: Oh, that's what this was. It's a minute-long dismissal bell. It's not the regular bell, yeah.

Steve: Okay. Okay. So finally, the aftermath. "A few days after sending the report," which again was sent automatically at the end of the blocks bell, automatically sent, and it was actually - "A few days after sending the report through the anonymous email account, we received an email response from D214's Director of Technology."

Leo: What the hell?

Steve: Uh-huh. "The director stated that because of our guidelines," that is, the things that they, like, the limitations they put on this, that is, they weren't going to interrupt the test, they really worked, you know, assiduously for this not to be a big problem, "because of our guidelines and documentation, the district would not be pursuing discipline. In fact, he thanked us for our findings and wanted us to present a debrief to the tech team. Later, he revealed the superintendents themselves reviewed" - I bet they did - "and were impressed by our report."

He said: "I was ecstatic that the administration was open to remediating their problems and auditing them with us. Although the D214 administration communicated good intentions, and they did hold in the future, my peers did not trust the administration and were skeptical of the true nature of the meeting. One of them referred to the whole thing as a sting operation."

Leo: Yeah.

Steve: "We decided I would reveal myself to present our debrief slides, with the others remaining anonymous in the Zoom meeting. I had planned on announcing my involvement from the beginning since I wanted to publish this blog post." He said: "(I was also pretty much the prime suspect anyways.)" So I know how that is.

Leo: Yeah.

Steve: "But just in case," he said, I love this, "I scheduled the debrief to take place after I graduated."

Leo: Yes. Smart.

Steve: "In all seriousness, the debrief went extremely well and was productive for everyone. We answered clarifying questions from the tech team and gave additional tips for remediation. We even managed to get the district to look into expanding the IT cybersecurity program and hopefully sponsoring a D214 CTF," you know, a Capture the Flag competition. He says: "This has been one of the most remarkable experiences I ever had in high school, and I thank everyone who helped support me. Thanks all, and thanks for reading."

Leo: What a great story. And he deserves, you know, of course, he's at a very well-known school for computer science, Marc Andreessen's alma mater. And I'm sure he will go on to great things. He did this perfectly. Beautifully.

Steve: Yeah, he did. He did.

Leo: Yeah, yeah. And he also showed integrity by being willing to take the heat if it turned out the administration wasn't chill about it. Which I admire him for; you know? Good for him, yeah. Pretty hard to punish a guy who comes forward and says, look, you've got problems. I've figured them all out. Yes, I was the one who did it, but I'm going to help you patch those holes. That's good.

Steve: Yeah. And the modifications we made all self-deleted.

Leo: Right.

Steve: We're telling you everything we did. But we left no cruft behind.

Leo: I mean, honestly, senior pranks often involved painting the statue out front purple. I mean, there's all sorts of much more destructive things that happen at the end of every school year. So this, as things go, was just good fun. Amusing. I'm just glad that they had that - it's good that the Governor of Missouri was not present.

Steve: Yes, exactly. I actually, I had that thought when I was writing the note, just like thank goodness that guy was nowhere to be seen.

Leo: And I have no doubt Minh has a great career ahead of him, pretty much can write his own ticket at this point. Very well...

Steve: Well, and as I said to you last week when you first told us about this on the podcast, my first reaction was hire that guy.

Leo: Yeah. This is exactly what you want. Man, what a great pen tester. He should be on somebody's red team, that's for sure.

Steve: Yeah.

Leo: Steve, always fun. I'm glad we could end instead of a scary note on a fun note. There's plenty enough in the show to scare. So it's nice to mix it up sometimes. If you like this show, please, I encourage you to visit Steve's site, GRC.com. He does have copies of the show. He has some unique forms, a 16Kb audio version, so it's pretty small. It's good for the bandwidth-impaired. He also has human-written transcription that's excellent, nice to read along while you listen. A lot of people like to do that. It's all at GRC.com.

While you're there pick up SpinRite, the world's best mass storage maintenance and recovery utility. 6.0 is the current version, but you'll automatically get a free upgrade to 6.1 when that comes out, and you can participate in its development as Steve gets closer and closer. There's also some great forums there. There's SQRL. There's lots of stuff: GRC.com.

Steve's on Twitter at @SGgrc. If you want to DM him, that's a good way to get in touch with him, send him Pictures of the Week submissions, things like that: @SGgrc. We have copies of the show on our website: TWiT.tv/sn for Security Now!. There's also a Security Now! YouTube channel. And of course you can always subscribe in your favorite podcast application and get it automatically. Please, if you do that, leave us a five-star review. Let the world know how valuable Security Now! is, something that you just have to listen to every week.

If you want to watch us do it live, we do have a livestream going at all times, and you can watch any of the shows being produced live at TWiT.tv/live. There's audio and video streams. You can chat live at irc.twit.tv or in our Club TWiT Discord Server. That's it, Steve. Have a wonderful week. Foundation, you still watching it? You moved on?

Steve: Haven't since - I think I've seen three, maybe two.

Leo: They do eventually kind of seem to get to some of the issues...

Steve: Well, in fact, didn't we see some scenes from it during yesterday's Apple presentation?

Leo: Yes, we did.

Steve: There were some beautiful - I've got to see it.

Leo: It was really pretty, yeah.

Steve: I mean just, again, I've got to see it.

Leo: Just turn off the sound and watch the pictures. That's it.

Steve: Perfect.

Leo: Have a great week, Steve. We'll see you next time.

Steve: Thanks, buddy. Bye.