The EvilProxy Service

Description: This week we look at an unusual and disturbing escalation of a cyberattack. I also note that crypto heists have become so pervasive that I'm not mentioning them much anymore. The White House conducted a "listening session" to dump on today's powerful tech platforms, and a government regulator in The Netherlands quit his position and tells us why. There's another QNAP mess which is bad enough to exceed my already quite high QNAP mess threshold, and D-Link routers need to be sure they are running their very latest firmware. I have another comment about my latest sci-fi author discovery, and two quick bits of feedback from our listeners. Then we're going to examine EvilProxy, the conceptual cousin to Ransomware-as-a-Service.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-888.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-888-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. The White House has a listening session that drives my blood pressure up. We'll find out why one Netherlands regulator quit his job in protest. Another QNAP mess. And finally, it had to happen someday, Phishing-as-a-Service. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 888, recorded 13 September, 2022: The EvilProxy Service.

It's time for Security Now!. Yes, he's here, ladies and gentlemen, Steve Gibson. He didn't sleep well last night, but he's going to sleep like a baby tonight because it's Security Now! day. Hello, Steve.

Steve Gibson: That's right.

Leo: He told me he sleeps better when the show's done. Like you put a lot of stress into this; right?

Steve: Well, okay. So I monitor the phases of my sleep. Remember the Zeos that I had you get?

Leo: Yeah, yeah, yeah.

Steve: Like years ago?

Leo: I still have it.

Steve: Well, it may come in handy. It turns out that the amount of slow wave sleep we get, which is the deepest level of sleep, it correlates with - basically it's a response from the previous day's cognitive memorization-related work.

Leo: Hmm.

Steve: And they've done tests where they've taken two groups of people who are well mixed and had them both spend the day doing two different types of task, one which involves memorization, and the other also a mental task but did not require memory. And the amount of slow wave sleep obtained by the group who were trying to memorize things is significantly larger than the group that did an equal amount of work, but didn't require memory. It's during slow wave sleep that memories are transferred from temporary storage into permanent storage. And what's interesting is that that's also the only cycle, the only phase of our sleep where the toxic proteins, the amyloid betas and the tau proteins, are swept out of our brain.

So one wonders whether the old adage about like learning a language or exposing yourself to novelty, if the reason that tends to keep your brain healthy is that our brain's response to that load we're putting on it, like a memorization load, learning something new, is to give us more slow wave sleep, which has the effect of clearing out the metabolic debris from the previous day's work.

Leo: Hence, you should never stop doing the show. This show is good for you.

Steve: Oh, hence I need to keep finding authors like the new author that I've found. Oh, my.

Leo: Oh, good books will work, too.

Steve: Oh. But anyway.

Leo: Are you still reading him? You're crazing about him? We'll talk about him later.

Steve: Oh, I've got a section of our show notes to talk about him.

Leo: Oh, good. Can't wait.

Steve: Yes.

Leo: What else we going to cover?

Steve: So we're at Episode 888 for the 13th of September. This one's titled The EvilProxy Service. And oh, boy. Bruce Schneier's words about attacks never getting worse, they only ever get better or stronger, they really ring true here. Anyway, we've got something really interesting and upsetting to talk about. But first we're going to look at an unusual and disturbing escalation of a cyberattack. I hope not an indicator of things to come. I also note that crypto heists have become so pervasive that I'm not mentioning them much anymore. They're just - it's ridiculous. We'll talk about that.

Leo: Like breaches. It's the same thing. It's just so many.

Steve: Yes.

Leo: Yes.

Steve: Also the White House last Thursday conducted a "listening session," as they called it, to dump on today's powerful tech platforms. Some of what came from that was interesting. And a government regulator in the Netherlands quit his position and then told us why. Also there's another QNAP mess which is bad enough to exceed my already quite high QNAP mess discussion threshold. Normally I just don't talk about it anymore because it's like, okay, yeah, again. Anyway, also D-Link routers need to be very sure that they are now running the latest firmware. I'll explain why. I've got, as I mentioned, another comment about my latest sci-fi author discovery; two quick bits of feedback from our listeners, and then we're going to examine this - essentially Phishing-as-a-Service...

Leo: Oh, golly.

Steve: ...has happened.

Leo: Inevitable. Inevitable.

Steve: In the same way - yes. It is exactly that, Leo. In the same way we had Ransomware-as-a-Service, now we have Phishing-as-a-Service. And this service can bypass all of our multifactor authentication safeguards.

Leo: Oh, boy. That's not good. Oy.

Steve: So it is essentially the conceptual cousin of Ransomware-as-a-Service. And, oh, do we have a Picture of the Week.

Leo: I burst out laughing when I saw it. It's good. It's good. We get to see that thing that made me laugh out loud.

Steve: So the residential version of this is that old story - you'd have to be our age or older, probably, Leo, to remember when fuses were screw-in base in homes; right? The

actual fuse, there weren't circuit breakers so much back then, they were very much like a lamp socket, but you would screw a fuse which was round and would have a little piece of copper there in the middle. And of course the point was that if something downstream of the fuse was drawing so much current that the little fuse, thus it's called a "fuse," would overheat and melt. Well, you wanted that to happen because the melting opened the circuit and...

Leo: Protected you, yes.

Steve: ...turned off the current. And so as an engineer, you know, as a technical person, the idea - and what people would do, of course, is like, you know, things would happen. The fuses could be pulled; right?

Leo: You don't have a fuse, yeah.

Steve: It could just sort of, yeah, you don't have a fuse handy because you used them up. You used a fuse the last time it blew. That was your last fuse. And so you forgot to go get some more. But the lights are off. So what are you going to do? Well, you get a copper penny, and you stick it in the socket, and then you screw the burned-out fuse on top of it, and oh, look, the lights come back on.

Leo: Yeah. And you just, you know, and you'd better hope the next surge is so powerful it melts the penny.

Steve: And again. So, okay. All this by way of introducing our Picture of the Week, which is the equivalent on an industrial scale.

Leo: Oh, my god.

Steve: If anyone has ever seen like a fuse box that would be protecting a huge, like, a woodworking shop with a bunch of equipment in it, or something that's drawing like an oil derrick or something, where the fuses are cylinders with big thick copper blades on each end. And you stick them in, and the blades are grabbed by receptacles on either end, and there's a pair of them for the hot and the cold line. Anyway, in this picture, apparently because something similar happened, they ran out of fuses, maybe they were stolen, maybe they kept blowing out. Well, first of all, if your fuses keep blowing out...

Leo: That's not good.

Steve: ...there's something wrong.

Leo: Yes.

Steve: Anyway, these industrious people decided, okay, well, you know, these pesky fuses keep blowing out. So they took two very large screwdrivers and just stuck them in in place of these fuses. And boy, I tell you, if these fuses blow...

Leo: You're in trouble.

Steve: You really have some problems.

Leo: Yeah, wow. That's hysterical. I have those screwdrivers. Now that I know I can use them as fuses, I'm set. That's good.

Steve: Actually, I own the one on the right.

Leo: Yeah, me, too. Who doesn't? That's a Stanley.

Steve: Yes, that thing must be a popular screwdriver because both of us have one. Okay. So Albania versus Iran. Risky Business News headlined their story this way. They said: "Albania cuts diplomatic ties with Iran in the first-ever cyber-related escalation." You know, I don't have a strong emotional tie to either Albania or Iran, though it's worth noting that Albania is a member of NATO. Fortunately, at this time, cyberwar mostly amounts to, you know, transient inconveniences; right? Like, you know, some office can't process green cards or something. But what's so worrisome about this is that it feels as though it might be predictive of worse things to come, and eventually perhaps involving global-scale adversaries.

Okay. Anyway, so here's what happened: The Albanian government announced last Wednesday the 7th that it would be cutting all diplomatic relations with Iran in the aftermath of a major cyberattack. And this marks the first time ever that a cyberattack has escalated this severely in the political realm. In a recorded video statement published on YouTube - for anyone who's interested I have the link in the show notes - Albania's Prime Minister Edi Rama said that after concluding an investigation into the incident, they found "indisputable evidence" that Iranian state-sponsored hackers were behind the cyberattack that took place nearly two months prior on July 15th. So they didn't just jump at this immediately. They did some investigating. In fact, they involved Microsoft. That cyberattack crippled multiple Albanian government IT systems.

Rama gave Iranian diplomats one day, 24 hours, to close their embassy and clear out. While the Iranian government naturally denied any involvement in the attack, NATO, the U.S. White House, and the U.K. government all published statements in support of the Albanian government and supported its attribution of the attack to the Tehran regime. The U.S. called Iran's attack on its NATO ally a "troubling precedent" and promised to "take further action to hold Iran accountable." And I did see subsequently, but I didn't track it down, that the U.S. had announced sanctions on Iran specifically due to this attack, this cyberattack on Albania.

And of course, although Iranian officials may deny their involvement, the proof lies in the malware used, which was discovered in the July 15th attack. Both Mandiant and Microsoft have linked back to multiple past instances of Iranian cyber-espionage operations and tooling using the same stuff. Microsoft, which has participated, as I said, in the Albanian government's response to the incident, said it was able to link the incident to four different Iranian APTs, advanced persistent threat groups, and detailed how these four

groups have been working together to breach Albanian government networks at least since last year to establish the proverbial foothold. Then finally in July, under the auspices of the Iranian government, which apparently decided it was time to act, the attack was launched.

Microsoft says the four groups appear to work under the guidance and control of the Iran Ministry of Intelligence and Security (MOIS). The four groups with numerical designations, there's DEV-0842 which deployed the ransomware and the wiper malware. DEV-0861, a different group, gained initial access and exfiltrated data, so now we're seeing specialization among individually identified groups. We have DEV-0166, which exfiltrated the data; and DEV-0133, the group which probed the victims' infrastructure initially.

So both Mandiant - which, by the way, Google, remember, purchased in March for $5.4 billion - and Microsoft concur in their statement that the Iranian attack is directly connected to the Albanian government's harboring thousands of Iranian dissidents, part of an exiled opposition party named the People's, how do you say that, Mujahideen, something like that. Anyway, I meant to look up the pronunciation before the podcast, and I forgot. Anyway, also known as MEK, which I like to say much more easily.

At the request of the U.S. government, MEK was given shelter in Albania in 2016, after the Iranian regime declared the group a terrorist organization and started hunting its members. MEK members were planning to hold an annual summit on July 21st. But that summit, which was titled The Free Iran World Summit, was canceled because of terrorist and bomb threats. Microsoft says that the threats and the July 15th cyberattacks were part of a broader effort from the Iranian government to go after the group and its host country.

So whereas past operations typically involved coordinated social media campaigns, data leaks, vague threats, and declarations from Iranian officials, the deployment of a data wiper and ransomware appears to have crossed a line which Albanian and NATO officials are not taking quietly. Though Albania's prime minister tried to play down the aftermath of the July 15 attack and said the government systems were now restored, the attack crippled government operations and official websites for weeks. And in fact, moments after Iranian officials left the embassy, Albanian police raided the building, which is unusual, in search of any incriminating evidence that might have survived the typical hard-drive bashing and document-burning practices of fleeing diplomats.

Conducting this raid was seen as extreme, but the general sentiment is that NATO partners backed and pushed Albania into this action as a way to signal to other cyber-aggressive countries that a line is being crossed when entire government IT networks are being wiped just because someone wants to attack a dissident group that they're annoyed with and of course attack those who are harboring the group.

Leo: I think that's appropriate. I really do. Don't you?

Steve: Which?

Leo: You have to draw a line in the sand. No, no, to defend.

Steve: Oh, yes. Oh, yes, appropriate to draw the line, absolutely.

Leo: Yeah, you know, this shall not pass.

Steve: And Leo, I mean, the thing that's worrisome about this, as I started off saying, is that what if this is a harbinger? Like what if, I mean, we've talked about how weird it is that like the U.S. and China are apparently right now involved in percolating kind of going on in the background cyberattacks against each other. Well, the problem is cyber is becoming - sorry to use that term in isolation, Leo - the cyber world is becoming...

Leo: Cyberspace, man.

Steve: Yeah. It is, you know, it's becoming where the world operates.

Leo: Yeah.

Steve: And so attacks there are real attacks, increasingly.

Leo: Yes, yes, absolutely. And they can be deadly. I mean, it's no reason to treat it any less seriously than a rocket, a mortar attack, I think. You know?

Steve: Right, right. And so I agree with you completely. I think that it is good...

Leo: Proportional response.

Steve: Yes, that the world said, okay, this is not all right.

Leo: Right.

Steve: You know, we know it was you, Iran. We know why you did it. We know you're not happy. We don't agree with your unhappiness, and you've just attacked a member of NATO.

Leo: Sorry, yeah.

Steve: Even if it was a cyberattack.

Leo: Yeah. Now, I understand the risk is that it will escalate into a worse and worse back-and-forth. But I don't see any way out of that. This is the whole, you know, this is the whole issue of any military force. There are bullies. And so you need a defense. You can't just let bullies be bullies.

Steve: Oh, and wait till you get to the fourth book in this...

Leo: Oh, I can't wait. I can't wait.

Steve: Ohhh. You want some bullies, oh, baby, I've got your bullies. And it ended up being a bit of a back-and-forth. Last Wednesday the diplomats were given one day to clear out and close the embassy. Two days later, last Friday the 9th, Albania was hit by another major cyberattack which has officials once again pointing the finger at Iran. The attack hit Albania's Total Information Management System, as it's called, TIMS, which is an IT platform belonging to Albania's Ministry of Interior, used to keep track of people entering and leaving the country.

According to a series of tweets from Albania's Minister of the Interior, six border crossing points were impacted and experienced border crossing stoppages and delays for at least two days. This included five land crossings at Greece, Kosovo, and several in Montenegro; and at the airport near Albania's capital. Ministry officials blamed the attack on "the same hand," as they put it, that hit Albania's IT network in July, in other words, Iran. So let's hope that the world is watching and recognizes that cyberattacks are not going to be treated like anything less than the attack that they really are, especially when they seriously impact government infrastructure.

Okay. So I feel that I should note something else that I'm seeing constantly which I just skip over, typically without comment on this podcast. And that's crypto heists of this or that also-ran cryptocurrency...

Leo: They're nonstop. They're nonstop. They're constant.

Steve: Oh, my god. From this or that random exchange that no one's ever heard of before, or random newbies being crypto-scammed. So this week I'll give everyone three perfect typical examples, Leo, of what we're both talking about so everyone has a feeling for what they're normally not missing.

Okay. First, get this, the New Free DAO, that's NFD token, whatever the...

Leo: It's a DAO.

Steve: Right, the DAO.

Leo: Autonomous organization, yeah.

Steve: Right, the New Free DAO token lost 99% of its value after a threat actor used a flash loan attack to steal more than $1.5 million worth of crypto from the platform. According to blockchain security firm CertiK, the hacker appears to be the same attacker who also hit DeFi platform New Order four months ago. I know.

Leo: I shouldn't laugh.

Steve: Gripping news, I know.

Leo: I shouldn't laugh because...

Steve: No, but Leo.

Leo: The sad thing is, I don't mind if some bitcoin bro loses his shirt. That's fine. But probably a lot of these people are just suckers, normal people.

Steve: Yes, unfortunately. Also the operators of the Gera cryptocurrency suspended operations last week after a hacker gained control over the platform's "smart contract," which is the name of it, which apparently wasn't so smart, after developers leaked the private key. According to the Gera team, the attacker minted $1.5 million worth of crypto, which they later transferred to their own Ethereum address. The platform has not yet resumed operations. Okay, boo hoo.

And third, Romanian law enforcement raided two penthouses - I got a kick out of the fact that they were in penthouses - two penthouses in Bucharest and detained three suspects. According to a joint investigation with the U.K.'s National Crime Agency, the NCA, the suspects would contact victims - get this, Leo, you're going to love it - the suspects would contact victims of cryptocurrency fraud and defraud them again.

Leo: Oh, that's terrible.

Steve: By posing as financial fraud recovery specialists, and ask for a substantial fee to recover their initial losses.

Leo: Once a sucker, you know. You've got the sucker hat on, they're going to come at you.

Steve: Ohhh.

Leo: You're wearing it.

Steve: Just so everyone knows, there is now a more or less constant flux of these sorts of heists. I mean, cryptocurrency, no one seems to be able to hold onto it. It's just constant.

Leo: This is a great website from Molly White called "Web3 Is Going Just Great," and she has a little counter in the lower right-hand corner of how much money has been lost to crypto fraud. And it is, it's kind of stunning. It's just nonstop.

Steve: What does it show, 10 point something billion dollars?

Leo: $10.669 billion.

Steve: Oh, my lord. Wow.

Leo: I mean, this is a classic, this is a typical headline. "Algorand Foundation discloses $35 million exposure to Hodlnaut."

Steve: Well, you don't want to expose your Hodlnaut, Leo.

Leo: Well, both of these were legit. Hodlnaut was a crypto wallet that halted withdrawals on August 8th. Algorand is a proof-of-stake blockchain, and they foolishly put $35 million into Hodlnaut. And then Hodlnaut was heavily exposed to Terra, which collapsed in May. So Hodlnaut halted withdrawals. Because there's no regulation.

Steve: Because what could possibly go wrong?

Leo: Yeah. No regulation.

Steve: [Crosstalk] running the bank.

Leo: Incredible.

Steve: Oh, goodness.

Leo: Incredible.

Steve: Yes, I, you know, if we titled our podcasts after the show the way you do for MacBreak Weekly, it would be "Never Expose Your Hodlnaut."

Leo: Yeah. And, by the way, I'm laughing only because it's so horrible. And again, if it were bitcoin bros, fine, you know, throw your ill-gotten gains away.

Steve: The Winklevoss brothers or whoever they are.

Leo: Let them lose all the bits in their coin. But it's not, it's sad to say, it's people who are being suckered by NFTs and crypto. Don't be fooled, kids.

Steve: We have some guy, a neighbor in our neighborhood, who's all NFT hopped up. And I just, you know. And some other neighbors who know I'm kind of a computer guy say, should we do anything? I said no. Stay away from...

Leo: Stay as far away as you can.

Steve: Stay away from that guy.

Leo: Yeah, yeah.

Steve: Yeah. I don't, you know, I mean, apparently, if you're Kevin Rose, and you can have a little, what is it, a zombie he's got?

Leo: Oh, he's got - he owns some zombies. But then, and I love Kevin, but I think this is a little sketch, he created his own owls, Moonbirds they call them, and has been selling them, sold them within the first week, $50 million worth of them.

Steve: Ohhh, what...

Leo: And so many that he, you know, it's he and a bunch of other people called The Proof Collective. But it's really - he's one of the big names. There's three people is involved in stuff. So because it's big names in this area, NFT area, people bought in to the tune of $50 million. All of it's speculation. You only buy an NFT because you think someday some sucker's going to come along and buy it for twice as much. Then Kevin, realizing he made a lot of money here, put out a YouTube video saying, no, no, we're going to do good things with the money. Then last week it was announced that Marc Andreessen, Andreessen Horowitz, just put another 50 million into it as an investment. So I think the only thing that...

Steve: That was a good YouTube video.

Leo: The only thing we did wrong, Steve...

Steve: He cannot stop making money, this guy.

Leo: I know. The only thing we did wrong, Steve, is not issuing an NFT early on. That and throwing away the hard drive.

Steve: Ohhh.

Leo: I can only say a hundred times, you know, stop, don't, it's not, you know, this is - Bill Murray's NFT charity auction, that's $185,000, which is immediately stolen. Hours after the auction, a hacker gained access to Murray's crypto wallet and snagged the 119 ETH for themselves. And on and on and on.

Steve: What were those bulbs that were once so popular?

Leo: That was tulip bulbs.

Steve: Tulip bulbs, yeah.

Leo: I just thought that was going to be a good investment.

Steve: That was going to be a big deal.

Leo: I've got them next to my Beanie Babies in the closet.

Steve: Okay. So the White House held a Tech Platform Accountability listening session last Thursday. In a nation founded on the principle of a right to free and open public speech and a free and open press, neither being under the thumb of the government, the question is what responsibility do our social media platforms have, and to what degree, if any, about the content their users publish and which they subsequently host and our search engines find and index. Certainly a good question.

Now, I looked through the list and the titles of the 16 attendees who were invited to participate in this "listening session" last week. If it were possible for bureaucracy to reach a critical mass where its own gravitational attraction would cause it to collapse in upon itself, putting this group into a single room would be inadvisable. Boy, I mean, the titles, you need a line wrap in order to see them. Nevertheless, the listening session occurred, and everyone appears to have survived.

I suppose that a session titled "Tech Platform Accountability" would tend toward the negative. But boy, did this group dump on today's social media offerings. The White House started everyone off with a negative tone, and the meeting's participants appear to have willingly added fuel. The summary of the event is not long, and I think it's worth sharing.

Here's the White House's summary. They said: "Although tech platforms can help keep us connected, create a vibrant marketplace of ideas, and open up new opportunities for bringing products and services to market" - and okay, just so everyone knows, that's the end of the good news part of the summary. They continued: "They can also divide us and wreak serious real-world harms. The rise of tech platforms has introduced new and difficult challenges, from the tragic acts of violence linked to toxic online cultures, to deteriorating mental health and wellbeing, to basic rights of Americans and communities worldwide suffering from the rise of tech platforms big and small."

They said: "Today, the White House convened a listening session with experts and practitioners on the harms that tech platforms cause and the need for greater accountability. In the meeting, experts and practitioners identified concerns in six key areas: competition; privacy; youth mental health; misinformation and disinformation; illegal and abusive conduct, including sexual exploitation; and algorithmic discrimination and lack of transparency." And for what it's worth, I mean, I know we are all sympathetic to the problem that we have. There are certainly problems here.

They said: "One participant explained the effects of anti-competitive conduct by large platforms on small and mid-size businesses and entrepreneurs, including restrictions that large platforms place on how their products operate and potential innovation. Another participant highlighted that large platforms can use their market power to engage in rent-seeking," as the term is, "which can influence consumer prices.

"Several participants raised concerns about the rampant collection of vast troves of personal data by tech platforms. Some experts tied this to problems of misinformation

and disinformation on platforms, explaining that social media platforms maximize 'user engagement' for profit by using personal data to display content tailored to keep users' attention, content that is often sensational, extreme, and polarizing.

"Other participants sounded the alarm about risks for reproductive rights and individual safety associated with companies collecting sensitive personal information, from where their users are physically located to their medical histories and choices. Another participant explained why mere self-help technological protections for privacy are insufficient. And participants highlighted the risks to public safety that can stem from information recommended by platforms that promote radicalization, mobilization, and incitement to violence.

"Multiple experts explained that technology now plays a central role in access to critical opportunities like job openings, home sales, and credit offers, but that too often companies' algorithms display these opportunities unequally or discriminatorily target some communities with predatory products. The experts also explained that the lack of transparency means that the algorithms cannot be scrutinized by anyone outside the platforms themselves, creating a barrier to meaningful accountability.

"One expert explained the risks of social media use for the health and wellbeing of young people, explaining that while for some, technology provides benefits of social connection, there are also significant adverse clinical effects of prolonged social media use on many children and teens' mental health, as well as concerns about the amount of data collected from apps used by children, and the need for better guardrails to protect children's privacy and prevent addictive use and exposure to detrimental content. Experts also highlighted a magnitude of illegal and abusive conduct hosted or disseminated by platforms, but for which they are currently shielded from being held liable and lack adequate incentive to reasonably address, such as child sexual exploitation, cyberstalking, and the non-consensual distribution of intimate images of adults."

Leo: Ugh.

Steve: I know. "The White House officials closed the meeting by thanking the experts and practitioners for sharing their concerns. They explained that the administration will continue to work to address the harms caused by a lack of sufficient accountability for technology platforms. They further stated that they will continue working with Congress and stakeholders to make bipartisan progress on these issues, and that President Biden has long called for fundamental legislative reforms to address the issues."

So it seems clear that, much as with the argument over cryptography, and privacy which creates an inherent lack of accountability when it can be used by criminals for criminal ends, that there's a tension there which I find fascinating because it's created by technology. Well, there's obviously another set of tensions here, you know, that is being created by the technology and, frankly, by the willful conduct of these major tech platforms.

So it seems clear that sooner or later we're going to be subjected to legislation of some form as our various governments attempt to somehow, you know, it's going to come down to micromanaging this incredibly slippery terrain which at least in the United States also employs constitutionally protected freedoms. So I imagine there'll be some time spent in the courts, as well.

Anyway, I wanted to finish by sharing the six bullet point, sort of the takeaways, the targets which were cited as the main focuses, the core principles for reform. The first is "Promote competition in the technology sector." They said: "The American information

technology sector has long been an engine of innovation and growth, and the U.S. has led the world in the development of the Internet economy.

Today, however, a small number of dominant Internet platforms use their power to exclude market entrants, to engage in rent-seeking, and to gather intimate personal information that they can use for their own advantage. We need clear rules of the road to ensure small and mid-size businesses and entrepreneurs can compete on a level playing field, which will promote innovation for American consumers and ensure continued U.S. leadership in global technology. We are encouraged to see bipartisan interest in Congress in passing legislation to address the power of tech platforms through antitrust legislation."

Second: "Provide robust federal protections for Americans' privacy." They said: "There should be clear limits on the ability to collect, use, transfer, and maintain our personal data, including limits on targeted advertising. These limits should put the burden on platforms to minimize how much information they collect, rather than burdening Americans with reading fine print. We especially need strong protections for particularly sensitive data such as geolocation and health information, including information related to reproductive health. We're encouraged again to see bipartisan interest in Congress in passing legislation to protect privacy."

Third: "Protect our kids by putting in place even stronger privacy and online protections for them, including prioritizing safety by design standards and practices for online platforms, products, and services." They said: "Children, adolescents, and teens are especially vulnerable to harm. Platforms and other interactive digital service providers should be required to prioritize the safety and wellbeing of young people above profit and revenue in their product design, including by restricting excessive data collection and targeted advertising to young people." And I for one, I don't have any young kids, never had to raise them in this Internet age. But it would be a terrifying prospect, I think.

Leo: Yeah. The problem - I agree with all of these sort of in principle. The problem's the implementation.

Steve: I'm with you completely, Leo. And I heard you talking last week, it wasn't here, it was in the Techdirt guys...

Leo: Yeah, my dialogue with TWiG, yeah.

Steve: Yes. About some of the ideas that California's legislators have come up with.

Leo: It passed, by the way. It's in law.

Steve: Right.

Leo: And it should be terrifying to you.

Steve: Yes.

Leo: Because you have potentially 18 year olds and under using your site. You want them to. That means you have to design your site, and everybody has to design their site, for the lowest common denominator. And that's ridiculous. That's just absurd. That's not how you protect kids. So, you know, well, let's change the Internet and make it safe for kids. You mean all of it? Yeah, all of it. Okay.

Steve: Yeah. It's very much like the overreach of the grant permission for cookies. It's like, oh, my goodness. Let's fix them rather than make everyone agree to them.

Leo: There are some things I completely agree with. You know, we need to work on privacy protections. I agree. But then they intermix this with this to protect the children, the design of websites, you know, that was all code earlier on about social networks to overturn Section 230 of the DMCA, which is vital to the Internet.

Steve: Yes.

Leo: And it's just it's a fundamental misunderstanding of how it works. And it's politics, and it's very shameful. I'm very disappointed, frankly.

Steve: Yeah. So I'll just skip a lot, just summarize the last three points. There was remove special legal protections for large tech platforms. And here we come to Section 230, just as you were saying, Leo. It's like, you know, how can we make open platforms actually responsible for everything that their participants post. I mean, again, it's a problem that they're not. It's a problem what people are posting. But it's impractical to make them responsible.

Leo: Section 230 makes it possible for them to moderate. The problem is you have some politicians who don't like to be moderated. They call it "deplatforming." And if you make it impossible to moderate, well, that's not good. Get ready. It's going to be bad news.

Steve: Yup. Number five is increased transparency about platforms' algorithms and content moderation decisions. They said: "Despite the central role in American life, tech platforms are notoriously opaque. Their decisions about what content to display to a given user and when and how to remove content from their sites affect Americans' lives and American society in profound ways. However, platforms are failing to provide sufficient transparency to allow the public and researchers to understand how and why such decisions are made, their potential effects on users, and the very real dangers these decisions may pose."

Leo: So California passed a law on this, too, just the other day, which Mike Masnick calls "The Spammers Protection Act." Because it essentially says make it public how you block spam, how you clear stuff out that's bad.

Steve: Decide which is not.

Leo: Yeah.

Steve: What is not.

Leo: Make your algorithms public. And oh, by the way, you can't change them unless you have a period of publishing it and stuff. So all this does is tell people how to game the system. It achieves nothing. I'm sorry. Go ahead. Do your show. You get me all heated up.

Steve: No, no, no, Leo, we like to hear from you.

Leo: I'm all het up now.

Steve: And number six: "Stop discriminatory algorithmic decision-making." They said: "We need strong protections to ensure algorithms do not discriminate against protected groups, such as by failing to share key opportunities equally by discriminatorily exposing vulnerable communities to risky products, or through persistent surveillance." So, yeah.

You know, what was the famous line? We're the government, and we're here to help?

Leo: But, you know, honestly, I don't think we should depend on the tech platforms to regulate themselves.

Steve: No.

Leo: Because they won't.

Steve: No, no.

Leo: So government needs to, but it needs to do so intelligently, not stupidly, and not with a political axe to grind.

Steve: I mean, capitalism has a lot going for it. One of the problems it has, however, is it does tend to form monopolies. It naturally forms monopolies. Someone or group will get bigger than others, and they will use the power of their bigness to continue to accelerate. So that creates positive rather than negative feedback. And it's unstable. So it's a good system, but it needs management.

Leo: Yup, yup, yup.

Steve: And we've got something like that here happening.

Leo: I agree. And so we do need regulation, but boy. Maybe we need people under the age of 50 to do it. Perhaps that's the problem. They just...

Steve: Well, and you know, in the case of the Internet, we also have a single global network carrying services which straddle nations whose governments grant their citizenry widely differing rights and which restrict the behavior of their enterprises in widely different ways. So how does, I mean, presumably they've been trying to so far. How does a single Facebook, Twitter, Instagram, or Google simultaneously satisfy the widely differing requirements of different geographical regions of the globe? You know, I mean, these are hard problems.

Oh, before I leave the subject of governments, Bert Hubert - and you know, Mr. and Mrs. Hubert...

Leo: Why? Why Bert? Why Hubert?

Steve: I don't know. Really? Did you really have to name your son Bert?

Leo: Do you think his real name is Hubert Hubert? Humbert Humbert?

Steve: Oh. Maybe. Anyway, he's a member, or actually he was, of TIB, the Dutch government board that checks the legality and approves communications interception warrants for the Dutch intelligence and security services. Well, as I said, he was, because he resigned last week. The automatic English translation of Bert's blog posting explaining his decision was so atrocious, he said, that he wrote an English version himself. And I'm glad he did because, if I were serving in a government that I believed in, I'd hire this guy in a second based on what he wrote. So here's what he said.

He said: "If either of the civil or the military intelligence and security services of the Netherlands want to use a lawful intercept, SIGINT, or hacking, or some other legal powers, they must first convince their own jurists, then their ministry, and finally the TIB. The TIB then studies if the warrant is legal, and that decision is binding."

He said: "When I joined the regulatory commission, I was very happy to find that the Dutch intelligence and security services were doing precisely the kinds of things you'd expect such services to do. I also found that our regulatory mechanisms worked as intended. If anything was found to be amiss, the services would actually stop doing that. If the ex ante regulator," meaning upfront in advance, he says: "(i.e., my board) ruled a permission to do something was unlawful, it would indeed not happen." He says: "I think it is important to affirm this in public.

"Over the past two years, however, there have been several attempts to change or amend the Dutch intelligence law. The most recent attempt has now cleared several legislative hurdles and looks set to be passed by parliament." He said: "Under this new law, my specific role, technical risk analysis, would mostly be eliminated. In addition, the Dutch SIGINT bulk interception powers would be stripped of a lot of regulatory requirements. Furthermore, there are new powers, like using algorithmic analysis on bulk intercepted data without a requirement to get external approval. Finally, significant parts of the oversight would move from up front ('ex ante') to ongoing or afterwards ('ex post').

"Doing upfront authorization of powers," he says, "is relatively efficient, and is also pleasingly self-regulating. If an agency overloads or confuses its ex ante regulator, they simply won't get permission to do things. This provides a strong incentive for clear and concise requests to the regulator. A regulator that has to investigate ongoing affairs, however, is in a difficult position. It can easily become overloaded, especially if it's

unable to recruit sufficient technical experts. In the current labor market, it is unlikely that a regulator will be able to swiftly recruit sufficient numbers of highly skilled computer experts able to do ongoing investigations of sophisticated hacking campaigns and bulk interception projects. An overloaded regulator does not provide good coverage. It is also vulnerable to starve the beast tactics."

He said: "Once it became clear the intended law would likely pass parliament, I knew I would have to resign anyhow, since I don't agree with the new expanded powers and the changes in oversight. As a member of the regulatory board, I could not share my worries about the new law. The regulatory board itself is staffed with excellent people, but by design the board only operates within the existing law. It is not responsible for formulating or even criticizing any new laws.

"Instead of waiting out the likely passing of the new law, I've decided to leave now. This enables me to speak my mind on what is wrong with the new law. It may not help, but at least it's better than watching democratic backtracking in silence. It has been a great honor to have been part of the regulatory powers board. Its staff and members are an impressive bunch, and I wish them the best of luck with their ongoing and important work. On a final note, if anyone is looking for a government regulator with a proven track record of resigning when things go wrong, know that I'm available."

Leo: That's great. You're hired. Wow. Good for Bert Bert, or whatever his name is. That's great. That's great. Wow.

Steve: Yeah. And it's also worth noting, although Bert didn't mention it in his blog posting, that his TIB flagged several cases of abuse last year that targeted journalists and several cases of broad warrants that intercept bulk traffic over entire global Internet cables.

Leo: Wow.

Steve: So his term for what he sees happening I thought was great. He called it "democratic backtracking." And I thought this was worth sharing since it shows the way democracy will decay if it's not fully understood and continually reinforced. As I said before, it's not an inherently stable system since it is subject to creeping manipulation. You know, just think of the U.S. Tax Code if you need another example of creeping manipulation.

Leo: Oh, yeah.

Steve: You know? Some group of right-minded people originally established the operation of the Dutch regulatory commission to work the way it does today for a reason, for at least some of the reasons Bert has explained. But who knows? Maybe those who did this are now out of power, and those being regulated had been chafing at the limitations the current system deliberately imposes upon them. Yes, it's inconvenient and annoying. It's meant to be. Surveillance of a free and democratic people should not be the default. It should be the exception. And it does seem that initiating the surveillance first and asking for permission, either concurrently or afterward, is far more likely to lead to abuse. Again, the question is what principles do we want to support? So bravo, Bert.

Leo: Bravo, Bert.

Steve: I'm sorry you needed to resign. But that's what people have to do, if they see things happening around them that they cannot participate in, in good conscience.

Leo: Awesome. And I'm glad you gave him a forum. You know?

Steve: Yeah, yeah. Okay. Another near-constant event that I choose to only cover periodically - actually, you and I talked about it after we stopped recording last week, Leo - is horrendous problems occurring in QNAP NAS software. You know, it's just constant. Since it's entirely possible to run a non-QNAP OS on their QNAP hardware, I dearly hope that anyone listening to this podcast will have switched out QNAP's constantly disappointing firmware for any of the Linux or Unix alternatives that are known to run on the hardware. In fact, QNAP's own platform is a Linux derivative. So you can do that. And again, Google will show you how. And if you do need to remain with QNAP, please by all means protect it from the public Internet. We've talked about many ways to do that in the past. Even now QNAP themselves has told their own users not to expose their devices to the Internet, despite the fact that they're network storage.

Leo: That's the whole point.

Steve: I know.

Leo: Okay.

Steve: I know. Okay. So Deadbolt is both a ransomware and a ransomware group that has been plaguing QNAP users and their devices throughout 2022, all year. Since January, thousands of QNAP customers have reported being attacked by the DeadBolt ransomware group. The group demands a ransom of 0.03 bitcoin, currently around $1,100, for the decryption key.

After the initial attacks affected about 3,600 devices last January, the group continued to resurface with campaigns in March, May, and June of this year. They're a persistent bunch. Reddit and other message boards have been flooded with customers lamenting the loss of files that included family photo albums, wedding videos, and more. You know, irreplaceable things. Dozens of users took to Reddit to complain that they were among those attacked in the latest campaign.

In a note to QNAP, the hackers demanded 5 bitcoin, which would be about just shy of $94,000, to reveal details about the alleged zero-day vulnerabilities they initially used to attack its users; and another, whoo, 50 bitcoin, which is just shy of a million dollars, to release a master decryption key that would unlock all of their victims', their users' victim files.

Now, QNAP would not say whether it has considered paying the ransom for the universal decryption key, which is to say, uh, no. But we can be pretty sure that that's not going to happen also when a spokesman said the company's research - so this is the QNAP spokesman said the company's research has shown that the Deadbolt group is attacking legacy versions with known vulnerabilities which have security updates available. Okay.

Sounds logical, reasonable. Maybe true. In other words, they're saying it's the users' fault, not theirs, so they should pay if they want their data back.

Now, some users have disputed QNAP's insistence that only devices that have not been updated are being attacked. And it kind of seems reasonable since the group behind this, the Deadbolt group, are coming up with new ways to do this all the time. And here's a little bit of a gotcha. If ransom is paid, the key provided by Deadbolt may not work. So the security company we've talked of several times, Emsisoft, released its own version of a DeadBolt decryptor after several victims reported having issues with the one they received in exchange for paying a ransom. However, it's not any sort of universal decryptor. It only works with a decryption key supplied by the operators of the DeadBolt ransomware through a ransom payment.

Emsisoft's Fabian Wosar tweeted: "QNAP users who got hit by DeadBolt and paid the ransom are now struggling to decrypt their data because a forced firmware update issued by QNAP removed the payload that is required for decryption." Okay. So this got so bad finally that QNAP took matters into their own hands and forced a firmware update onto their customers, which broke the ability for the ransomware payment, after receiving the decryption key, to function. So, wow. Emsisoft came along and said, okay, we'll fix that for you. And they did. What a mess.

Earlier this year, the security company Censys who runs that IoT search engine - remember we've often talked about Shodan. There's now another kid in town, Censys. And they're doing neat things. Anyway, they have a search engine that goes wide and deep for IoT stuff. They reported - and a QNAP NAS is considered an IoT device. They reported that of the total 130,000 QNAP NAS devices sold, 4,988, so just shy of 5,000 of those servers, exhibited the telltale signs of this specific piece of ransomware. So about 5,000 compromises.

Censys also managed to track the bitcoin wallet transactions associated with an infection and found that of the previous batch of victims, 132 paid ransoms totaling about $188,000. So this is making money for someone who is saying we'll give you all of the stuff you've lost on your NAS for $1,000 in bitcoin. 132 people in that particular batch did so. Censys also created a dashboard to track the number of victims around the world. The majority of the most recent infections are taking place in the U.S., Germany, and the U.K. And it's not over.

Since all of that, and this is really what finally caused this to rise above my QNAP threshold, Censys observed that the number of QNAP NAS devices infected by the same Deadbolt ransomware spiked from 2,144, which was the count on July 9th, to 19,029 on September 4th, which was Sunday before last. The spike arose because the ever-industrious Deadbolt gang exploited, yes, another new zero-day vulnerability in the Photo Station app which is installed on most QNAP NAS systems. So they're finding more new ways in. Again, if you have a QNAP NAS with QNAP software, get it off the Internet. And if you can, put in a replacement software set. And it is possible. There are third-party solutions for QNAP.

Oh, and before we leave the Censys Internet scanning company, it's worth noting that they recently published a "2022 State of the Internet Report" which observed that misconfigurations accounted for 60% of the issues they observed across all Internet-exposed services globally.

Leo: Holy cow. That's a good number. Wow.

Steve: Yeah. They found that software problems only accounted for 12% of all observed problems. That is, software vulnerabilities. So all of these problems are misconfigurations. Now, it's unclear whether placing a QNAP NAS onto the Internet would inherently be considered a misconfiguration of those devices, but it seems pretty clear that it should be. You do not want to put one of those things on the 'Net.

Also, one last IoT note. D-Link is currently being taken over by MooBot, M-O-O-B-O-T. Palo Alto Networks' Unit 42 has identified a three-year-old Mirai botnet variant known as MooBot. It's rapidly finding and co-opting any remaining vulnerable D-Link routers into another army of denial-of-service bots by taking advantage of multiple old and two new, but all patched, exploits. Last Tuesday Unit 42 said: "If the devices are compromised, they will be fully controlled by attackers, who could utilize those devices to further conduct attacks such as distributed denial-of-service."

Okay. So MooBot, which was first identified and disclosed by the Chinese group, the Qihoo 360's Netlab team, back in September of 2019, so three years ago, MooBot has previously targeted LILIN digital video recorders and those Hikvision video surveillance products we were talking about a couple of weeks ago. In the latest wave of attacks discovered by Unit 42 early last month, as many as four different highly critical flaws in D-Link devices are being used in the development of MooBot samples. So the four flaws, the oldest, believe it or not, CVE-2015-2051, carries a CVSS, you know, got to love this one, of 10.0. I mean, it must just be that you connect to the D-Link router and say, "Please, sir, may I enter," and it says, "Oh, by all means, make yourself at home." How do you get a 10.0?

Leo: I don't know. Wow.

Steve: So that one is - it's called the HNAP SOAPAction Header Command Execution Vulnerability. You probably just put a command in the header, and it runs it for you. CVE-2018-6530, so back from year 2018, that's got a CVSS of 9.8. Still right up there with the best of them. This one is the D-Link SOAP Interface Remote Code Execution Vulnerability, sounds kind of generic, but okay. Then the other two are 2022, this year's CVEs, both also carrying scores of 9.8. D-Link goes big. They are both also Remote Command Execution Vulnerabilities.

So as I said, successful exploitation of any one of those four flaws, which all have very low attack complexities, so we're told, is used to remotely launch a WGET command which retrieves the MooBot payload from a remote host. MooBot then, after it's started, parses instructions from a command-and-control server to launch DDoS attacks in ways we're all too familiar with. So although the oldest vulnerability is from 2015, and the next oldest is from 2018, those other two, which are 9.8 remote code execution vulnerabilities, known and patched, were only fixed this year. So anyone who knows anyone who uses a D-Link router should be certain that they have updated recently because these Deadbolt guys are on the prowl, and they're looking for all the routers that they can get themselves into. Okay. Leo?

Leo: Would you like me to do something?

Steve: No. I'm good.

Leo: No? Okay.

Steve: But thank you. Shortly.

Leo: I'm here when you need me, man. I'm just - I just hear your voice.

Steve: Last week...

Leo: Oh, I want to hear about this, yes.

Steve: I introduced our listeners to my latest science fiction reading discovery, Scott Jucha's "The Silver Ships," thanks to one of our listeners. I have been having so much fun ever since.

Leo: Oh, now you've got me. Now I've got to have it.

Steve: Leo, I'm now halfway through the fourth book. Actually I'm at 71%. And I can assert that this is the most engaging and satisfying series of novels I have read in a long, long time. And just wait until you meet the Swei Swee. For those of you who prefer to have books read to them, I'm so glad, Leo, that you said that the reader of this series is someone you know and enjoys listening to.

Leo: Yeah, he's good, yeah.

Steve: Because I wouldn't want anything to spoil the experience of Audible's listeners. My initial mild concern after only the first book was that Scott Jucha's character development might be overly focused upon his story's central character, a young asteroid miner by the name of Alex Racine. Well, that concern has dissolved completely. We now have a broad cast of wonderful characters. And this guy writes so well.

I was trying to put into context for myself how good this book series is. I'm just giddy reading it. I know that there have been times in the past when I have been this thrilled over a science fiction storyline - the Honor Harrington novels, Michael McCollum's Gibraltar Stars trilogy. And I'm sure that some of Peter Hamilton's stories did this, although there was always a lot to wade through with his major work. And there must be others since it is a familiar feeling for me to be so satisfied when I'm reading the inventions of a skilled storyteller who really knows how to weave a yarn and who has come up with a bunch of great new sci-fi technologies, and people, both human and non.

Another thing I've noticed is that, like the best serialized stories, a lot happens in every installment. So far there has been no sense of Scott stringing us along. Even when the action slows down for a while, as almost has to happen from time to time, there turns out to be a real purpose in the way we were spending that time.

And you know, the best books always cause those of us who love to read to immediately wish for amnesia so that the story can be experienced again new. Anyway, this series is the equal of any I've read. And, oh, boy, prepare yourself for a huge surprise at the start of book three.

Leo: Oh, boy.

Steve: So anyway, it is just - it is so good.

Leo: I can't start it till September 22nd.

Steve: I understand.

Leo: I need my Audible credit.

Steve: I know you've got a backlog. I know you have a backlog. Oh, speaking of which, funny you should mention that.

Leo: Yes.

Steve: The tweet from x4jw. He said: "Hi, Steve. Thanks for the recommendation of The Silver Ships series of books. Went to purchase Book 1 on my Audible account and was surprised/delighted to see that Books 2, 3, 4, 5, 7, 8, 9 are all included for free as part of the Audible Plus membership, and I just had to click ADD TO LIBRARY to grab those." He said: "I can understand why Book 1 is not free. Not sure why Book 6 isn't." So again, it's you've got to buy Book 1, then 2, 3, 4, 5, 7, 8, 9 are all free.

Leo: Nice.

Steve: And then he said: "Books 10-20 are also purchase-to-own titles on Audible." He said: "Anyway, just thought 'readers'" - he has in quotes - "using Audible might like to know that they can get 35% of the series for free as part of the Plus subscription service."

Leo: And by the time you're hooked at Book 11, you go buy the rest of them.

Steve: Leo, as I said, I'm at 71% in Book 4. I'm astonished by what this guy has done. It's just, you know, we were talking about bullies. And, oh, in Book 4 there are some people you just want to have get what's coming to them. And, oh, do they ever.

Leo: Oh, I might have to buy this one ahead of time just to get started. I love it that I get so many of them for free. That's good.

Steve: Yeah.

Leo: You know, so the guy who reads it, Grover Gardner, I've spent some time with because he read Steven King's "The Stand." So I've spent at least 48 hours listening to Grover Gardner. Actually listened to several of his audiobooks. He's got, you know, you might at first say, well, I don't like his voice. Just bear with him. I think

for something like this he's a good choice because he's a very clear, simple, easy to understand reader. And it sounds like there's a lot of content here. So this'll be good.

Steve: Ohhh.

Leo: Yeah, I really like Grover Gardner.

Steve: Okay.

Leo: Fun. Thank you.

Steve: Okay. Let's take our break, and then we're going to talk about the EvilProxy Service.

Leo: I appreciate your recommendations, Steve.

Steve: So far. I get a lot of feedback from our listeners saying, you know, they've liked everything I've suggested.

Leo: Oh, it's always great to get them, you know. And we have Stacey's book club, which is a sci-fi book club. I get some, you know, between this show and This Week in Google, that's why my list is so long on Audible, and I'm so far behind. I get so many good recommendations. But I think I might start this sooner than later. You're really selling me. Let's talk about this EvilProxy.

Steve: Oh, boy. So, wow. As you said, and you hit it exactly right, Leo, in retrospect it was obvious that this was going to happen. Last Monday the security research group called Resecurity published their findings about a recently appearing, just last May, new, fully functional, turnkey, Phishing-as-a-Service system known as EvilProxy. Key among the many powerful features of this new underground service debuting on the Dark Web is its effortless ability to intercept SMS, OAuth, and one-time token, multifactor, you know, time-based token, multi-factor authentication flows. As a result, the "Login with some other website" like Google or Facebook, or enter the SMS code we just sent to your phone, or enter the six-digit code displayed on your authenticator, are all effortlessly bypassed and rendered ineffective.

Okay. This is all accomplished by streaming the actual target website, where the naive user believes they are logging in, through a transparent reverse proxy, which I'll explain further in a minute. They're not actually where they think they are. And unless they are scrupulously attentive to the URL being displayed in their browser's URL bar, they will be unwittingly providing their full authentication credentials, including any form of multifactor authentication, to a malicious third-party who will intercept their successful login session token to obtain a full secondary login to their account, with all the rights that arise from that.

Okay. So this sort of proxying is one of the inherent Achilles heels of the way the web works. I remember clearly one summer, when I was deep into the work on SQRL, I brought my work to a halt in order to completely wrap my head around this whole

problem of spoofing because it's a tough one. I felt as though I still didn't have an absolutely crystal clear understanding of exactly where the problem arose, and I needed SQRL to solve it, if it was possible. Anyway, I figured it out. And the result for SQRL was something called CPS, Client Provided Session. And it does indeed, once and for all, completely solve this problem.

Since I'm at work on SpinRite 6.1 I haven't taken the time to determine whether the FIDO2 and the WebAuthn folks also solved this problem. And I guess it doesn't matter whether it does solve it or not, since the Passkeys system is what we'll eventually be getting. In fact, it's live in iOS 16, which is now on iOS devices that are able to take it. But for what it's worth, it is possible to completely solve the problem, and that's another one of the things that SQRL does.

Anyway, remember the wonderful observation which we credit to Bruce Schneier. I mentioned it at the top of the show. He said something to the effect of "Attacks never get weaker, they only ever get stronger." And we're about to see an example of Bruce's observation on steroids. The thing that is so chilling about this new EvilProxy service is exactly that: It's a service. That horrifying, we thought, Log4j Java vulnerability which began the year is certainly a problem. But as we've previously described, it turned out not to be the end of the world for one reason: It was not a slam-dunk, drop-and-go, easy-to-use vulnerability. Every specific instance of its use needed to be deliberately engineered for the specific target where that potential vulnerability might be exploited. And the industry learned an important lesson from that: It matters far less whether something is possible than whether it's easy.

Which brings me to why this new EvilProxy Phishing-as-a-Service facility is so horrifying. The service providers have created an astonishingly powerful, simple-to-use, point-and-click web interface for their service. Through this interface, powerful phishing campaigns can be created by filling out some fields, selecting the required features, and pressing a Create Campaign button. If the Log4j vulnerability never exploded because it was difficult to use, this EvilProxy service promises to be an instant hit because it could hardly be any easier to use.

So that everyone can see for themselves, this week's GRC shortcut of the week, so that's grc.sc/888, will bounce its user's browser to a four-minute Vimeo video. That's Vimeo's number 746 020 364. But you can just put in grc.sc/888. That will show you a video which the EvilProxy service provider uses to market and demo the ease of use of their tool.

Okay. So now let's back up a bit for a bit of a broader overview of Resecurity's discovery from their coverage of this. The title of their report was "EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web." They said: "Following the recent Twilio hack leading to the leakage of two-factor authentication one-time-password codes, cybercriminals continue to upgrade their attack arsenal to orchestrate advanced phishing campaigns targeting users worldwide. Resecurity has recently identified a new Phishing-as-a-Service" - and then they have PhaaS, in fact, in the same way that Ransomware-as-a-Service is RaaS.

Leo: PhaaS.

Steve: Yes. So PhaaS - "called EvilProxy advertised in the Dark Web. On some sources the alternative name is Moloch (M-O-L-O-C-H)."

Leo: Yeah, evil, Moloch.

Steve: "Moloch, which has" - you want some Moloch? - "which has some connection to a phishing kit developed by several notable underground actors who targeted the financial institutions and ecommerce sector previously.

"While the incident with Twilio is solely related to the supply chain, cybersecurity risks obviously lead to attacks against downstream targets, the productized underground service like EvilProxy enables threat actors to attack users with enabled multifactor authentication on the largest scale without the need to hack upstream services."

They said: "EvilProxy actors are using Reverse Proxy and Cookie Injection methods to bypass multifactor authentication - proxyfying victim's session. Previously such methods have been seen in targeted campaigns of advance persistent threat and cyberespionage groups; however, now these methods have been successfully productized in EvilProxy, which highlights the significance of growth in attacks against online services and multifactor authorization mechanisms.

"Based on the ongoing investigation surrounding the result of attacks against multiple employees from Fortune 500 companies, Resecurity was able to obtain successful knowledge about EvilProxy including its structure, modules, functions, and the network infrastructure used to conduct malicious activity. Early occurrences of EvilProxy have been initially identified in connection to attacks against Google and Microsoft customers who have enabled multifactor authentication on their accounts, either with SMS or Application Tokens." In other words, you know, authenticators.

They said: "The first mention of EvilProxy was detected early May 2022. This is when the actors running it released a demonstration video detailing how it could be used to deliver advanced phishing links with the intention to compromise consumer accounts belonging to major brands such as Apple, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, Yandex, and others."

Leo: Was it on YouTube so we could all enjoy it? Geez, Louise.

Steve: I know. And Leo, if you scroll down in the notes, look at some of the screenshots I've attached. I'll get to them in a second.

Then they finished: "Notably, EvilProxy also supports phishing attacks against Python Package Index," which we were just talking about, PyPI. Okay. So in their report these guys embed a screenshot from the EvilProxy control panel showing the entry and options for proxying PyPI login and authentication. It shows that login, password, and session cookies are supported, meaning that they're captured, and the user can choose to have the service running for 10 days for $150, 20 days for $250, or 31 days for $400. So your typical quantity discount schedule.

Leo: God.

Steve: Up at the top of the page we see a .onion URL, so this is all being hosted by a hidden Tor Project Onion Service. And below is the control panel page selector showing a shopping cart icon labeled "Available Services & Prices" next to a circled dollar sign icon labeled "Account Balance." Conveniently, on the left, is an expandable dropdown labeled "Campaign URLs," and underneath that is "Create Campaign."

The Resecurity guys addressed the point of targeting software repositories. They said: "The official software repository for the Python language (Python Package Index PyPI) said last week that project contributors were subject to a phishing attack that attempted to trick them into divulging their account login credentials. The attack leveraged JuiceStealer as the final payload after the initial compromise and, according to Resecurity's Hunter team findings, related to EvilProxy actors who added this function not long before the attack was conducted," suggesting strongly that EvilProxy was the reason that the PyPI system was attacked in a phishing attack.

"Besides PyPI, the functionality of EvilProxy also supports GitHub and npmjs [of course], the JavaScript Package Manager which is widely used by over 11 million developers worldwide, which enables supply chain attacks via advanced phishing campaigns. It's highly likely the actors aim to target software developers and IT engineers to gain access to their repositories."

And again, remember, this is not the EvilProxy people doing the attack. EvilProxy is merely now a service in the same way that ransomware attacks were being conducted by affiliates using the Ransomware-as-a-Service service. So what we have is we have random cybercriminals now starting to leverage the EvilProxy service to launch sophisticated phishing attacks using that service. So we're already seeing evidence of the EvilProxy service in use.

Okay. So how does all this work? As I mentioned before, the Internet, and the World Wide Web specifically, have an inherent problem which is created by the web's brilliantly flexible and powerful underlying technologies. The URL itself, the URL as a thing, was originally intended to be fully human readable, even human typeable. But as we've seen, and we've all watched the evolution of web-hosted services through the past few decades, we've watched the readability and certainly the typeability of URLs virtually disappear. As I'm typing this text into Google Docs, I look up, and I see a URL that appears to be mostly random character gobbledygook.

And significantly, I opened and have been editing this document at this point for the past three hours, yet that was the first time my eyes fell upon this page's URL. Why did I have any reason to believe I was at the right place? I was sure I was because the page looked the way I expected it to look. I never had any doubt. So I never sought or received any further confirmation beyond the composition of the page I'm visiting.

I'm one of the hundreds of thousands of people listening to this podcast. I'm one of us. How do we imagine that a normal Internet user regards all of the utterly indecipherable things that their web browser does? And we've added all of this script-driven automation to the user's experience, too. When a user clicks on a link in a search engine, on a social media site, or in email, they may have noticed their URL bar flickering rapidly as their browser dances among all of today's various third-party link tracking services. Everyone wants to get in there for a piece of the action. So we've fully eliminated any sense from even an unusually savvy user that they should worry about the details of what's going on there. That's just the way things are today.

EvilProxy leverages the "reverse proxy" principle which is made possible by all of this inherent flexibility we've built into the web. Conceptually, the way it works is simple: The bad guys lead their intended victim to a phishing page. We've talked about phishing extensively in the past; right? You know, it's popal.com. That page uses what's known as a reverse proxy to fetch and display from the legitimate page all of the legitimate content the user expects to see, including login pages, and it sniffs their traffic as it passes through the proxy. It's a classic man in the middle. This "in the middle" position allows the middleman to harvest the valid web browser session cookies which are eventually passed back to the victim user, thus using the victim as an authentication mule to provide the usernames, passwords, and even two-factor authentication tokens.

Remember also that, while the man in the middle is able to intercept and forward one-time tokens for their one-time use, they also intercept and obtain the resulting session authentication cookies because the reverse proxy terminates TLS encryption in each direction. It sees everything in the clear. This means that anyone not using some form of additional one-time multifactor authentication will have their username and password stolen in the clear for future use.

The Resecurity guys obtained videos released by the EvilProxy service providers demonstrating the use of their point-and-click setup to steal the victim's session and successfully authenticate through Microsoft two-factor authentication and Google's email services to gain access to the target account. The more you see, the more chilling it all is. I've included the link to Resecurity's full report which embeds additional Vimeo videos for anyone who wants to become even more frightened.

As I noted above, EvilProxy's services are offered on a prepaid account basis. When the end user cybercriminal chooses a service of interest to target Facebook, LinkedIn, whatever the activation will be for a specific period of time, as I said, 10, 20, or 31 days described in the plan's itemized description. And Leo, there's another screenshot further down. Yup, there it is. One of the key actors, using the moniker "John_Malkovich," acts as gatekeeper administrator to vet all new customers. The service is represented on all major underground communities including XSS and Exploit, both of which we've talked about before, and Breached.

Payments for EvilProxy are arranged manually via an operator on Telegram. Once the funds for the subscription are received, they're deposited into the account in the customer portal hosted in TOR. Use of the service is available for $400 per month in the Dark Web hosted in the TOR network. And in the show notes and on the screen in the video we see the options for creating campaigns where Dropbox is used as the phishing target, RubyGems, Yandex, Yahoo, Microsoft, and the list - that looks like the list is about maybe half of the scroll length based on the scroll thumb that we see over on the right. So, and more services are being added continually. And in fact for the Microsoft box we see Xbox.com, Skype.com, OneNote.com, Office.com, MicrosoftOnline.com, Microsoft.com, Live.com, and Bing.com. So you get to choose your target of the phishing attack.

The EvilProxy portal contains tutorials and interactive videos explaining and demonstrating the use of the service and configuration tips. So the bad guys have done a state-of-the-art job in terms of the service usability and configurability of new campaigns, traffic flows, and data collection. After activation, the operator will be asked to provide SSH credentials to further deploy a Docker container and a set of scripts. This approach was likely borrowed from a previous Phishing-as-a-Service called Frappo which the Resecurity guys identified earlier this year.

So what does this all mean? While access to the EvilProxy service requires individual customer/client vetting, cybercriminals now have a cost-effective and scalable point-and-click solution which provides them with all the backend machinery required to enable them to run advanced phishing attack campaigns on their own while having no skill whatsoever about how to actually do the technology. That's all now turnkey, provided for them, just as Ransomware-as-a-Service was. And that includes bypassing state-of-the-art multifactor authentication, which is no protection against any of these.

The appearance of such a service on the Dark Web will undoubtedly lead to a significant increase in account takeover business email compromise activity and cyberattacks targeting the identity of end users, where MFA may now be easily bypassed with the help of tools like this one. And EvilProxy has no corner on the market. All they really did was to fully automate an already existing aspect of advanced cybercrime. They have made it trivial to do. They clearly got the idea from the preceding Ransomware-as-a-Service

control panels, which act just the same. And as we know, those have been way too successful for exactly the same reason that EvilProxy promises to be.

And we know what'll happen next. Other cretins will see it and decide to compete with it. Once multiple such services exist, competition will drive continued evolution in the features and will also drive down the cost to use them. We built a very powerful and capable World Wide Web whose features are increasingly being used against us. The creation of reverse proxy exploitation, followed by an easy-to-use turnkey service, well, it was probably inevitable, but it's certainly not good news.

Leo: Wow. PhaaS.

Steve: Yes, PhaaS. Phishing-as-a-Service. And so now the script kiddies...

Leo: Anybody can do it, yeah.

Steve: Yup. Anybody can do it.

Leo: This is the problem I have with things like the WiFi Pineapple, too. It's like, oh, well, it's a proof of concept. Or you could use it for pentesting. But you really just make it easy for people with malintention and no skill to act out. And that just means more people can do it. Oh, well. I don't understand - it's funny, you and I, and I'm sure all of our listeners have a moral compass and just can't fathom how somebody could do this.

Steve: No, it's why that job offer from the government was so appealing. It's like, wait. You mean I could do this for the U.S. government? And get a paycheck?

Leo: Still get to do it, yeah.

Steve: You know?

Leo: Yeah.

Steve: No, I agree with you. It's, well, and I told you that I have turned down some solicitations in the past.

Leo: Sure.

Steve: They knew I was able to do these things, and they said, I mean, and this was our government, said we'd like you to do this. And I couldn't even do that because...

Leo: I'll say this to anybody who might be teetering on the edge, thinking, well, I could really use the money. Maybe I'm, you know, my family needs the money or

whatever. If you have a moral compass, follow it. You will never go wrong. And at any point when you don't, you will regret it, and it isn't a good thing. You know, just stick with your moral compass. Stick with your moral tenets, your deeply held beliefs. Do what's right. Don't be tempted by what's wrong.

Steve: In the meantime, as a takeaway to our listeners, and to everybody we are talking to knows and loves, be so careful.

Leo: Oh, gosh, yes, yes.

Steve: About clicking links in email. That's the way this happens. That's the starting point for all of this is the innocent-looking, seductive-looking, expected-looking, whatever it is, I mean, this is not the Nigerian prince anymore. Nor is it your car insurance needs to be renewed.

Leo: It's clever. It's very believable. It's very believable.

Steve: Yes. And the problem is this means that we're going to see a dramatic increase in the amount of these sorts of attempts to get us to click something. And it's going to be believable, exactly as you said, Leo. But again, it's a matter of scale. And unfortunately this is going to cut loose a jump in the scale at which these sorts of campaigns occur. I mean, it's probably going to get to the point where smart people refuse to click anything in email.

Leo: Yeah. Or believe anything you see in a text message. I mean, I don't know about you, but I get text messages every day from Amazon and my bank and other companies that aren't my bank, saying, you know, oh, you've got to act now. Something's gone wrong. Quick, call this number. And it's very easy to fall for this. I really, I spend almost I think now every radio show 10 minutes talking about this because people need to hear it and really need to gird their, you know, prepare themselves for battle when they go out on the Internet.

Steve: It's sad.

Leo: Put your armor on. It is sad.

Steve: True.

Leo: It's very sad. You know what's not sad? That this guy here gets a better night's sleep tonight because he did this show. Thanks for listening. Thanks for getting him to do it. Episode 888, which is the super lucky episode. You know that; right? Eight is a very lucky number. Eight eight eight.

Steve: Yes, happy to have it.

Leo: Yeah. You'll find copies of this show in a couple of places. Steve has them. In fact, he has two unique forms of this show at his website, GRC.com. He's got the 16Kb audio, which admittedly is not, you know, hi-fi. But it is a small form factor for people who are bandwidth-impaired. Also those wonderful transcripts Elaine Farris does for every single show, which allow you to read along as you listen, to search for the part you're looking for, all of that plus 64Kb high-quality audio available at GRC.com.

While you're there, check out SpinRite, the for the last 20-some years, more than that, 30 years, the world's finest mass storage maintenance and recovery utility. If you have storage, hard drive or SSD, you need SpinRite. That's Steve's bread and butter, so go there and get a copy. If you buy 6.0 now, you'll get 6.1 as soon as it's done.

Steve: Only slightly delayed due to this new author.

Leo: Damn you, Silver Ships. Now that I know that, I'm not going to read that book. Only slight. Just a little bit. Just a little bit.

Steve: Because I'm a fast reader, and I'm still working on SpinRite.

Leo: Yeah, yeah. Steve's never going to stop working. Just taking, it's good, you need a little break, little down time for the brain. Let the steam cool off a little bit, you know, at the ears, get the smoke out of the ears. You can also find so much other stuff at Steve's site, it's worth visiting, GRC.com. Do leave him feedback there, if you want, GRC.com/feedback. Or on his Twitter account. His DMs are open at @SGgrc.

We have 64Kb audio and video of the show at our website, TWiT.tv/sn. There is a Security Now! YouTube channel, which is probably the easiest way, if you want to share like a little tidbit with a co-worker or a friend or a boss. You just snip it out of the YouTube, makes it very easy. So look for the Security Now! YouTube channel. And of course, you know, the thing most people will end up doing is getting a podcast player and subscribing, because that way you get it automatically every Tuesday afternoon, the minute it's done being polished up and edited.

We do the show live, if you want to get it the soonest, you can watch us do it live at live.twit.tv. Supposed to be 1:30 Pacific, 4:30 Eastern, 20:30 UTC, depending how long MacBreak Weekly goes. Sometimes it's delayed by half an hour or so. Be patient. It will show up on the stream. If you're watching live, chat live at irc.twit.tv. That's Tuesdays. I think that concludes this thrilling, gripping edition of Security Now!.