DarkNet Politics

Description: This week we examine Europol's desire to retain data on non-criminal EU citizens, and we look at the fourth EU nation to declare that the use of Google Analytics is an illegal breach of the GDPR. Has Teapot been caught? Seems like. And Mozilla says it's no fair that operating systems bundle their own browsers. Here we go again. Meanwhile, Chrome's forthcoming V3 Manifest threatens add-on adblocker extensions, and past Chrome vulnerabilities are leaving embedded browsers vulnerable. Windows 11 actually gets a useful feature, and some U.S. legislation proposes to improve open source software security. We revisit the Iran-Albanian cyber-conflict now that we know how Iran got into Albania's networks. And after one important and interesting bit of listener feedback about multifactor authentication fatigue and a quick SpinRite update, we look at some new trends in the dark underworld with the leak of another major piece of cybercrime malware.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-890.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-890-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got a lot planned for you. We'll talk about yet another country joining the growing list of countries prohibiting Google Analytics. What's Google going to do about it? There are some proposals. We'll also talk about Google's V3 Manifest for Chrome. It blocks the blockers. What are you going to do about that? And an inside look at Lockbit, the number one ransom program. They just got hacked. Aww. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 890, recorded Tuesday, September 27th, 2022: DarkNet Politics.

It's time for Security Now!, the show where you get really down and dirty with the technology.

Steve Gibson: That's right.

Leo: Well, not in that way. You know what I mean.

Steve: That's right.

Leo: We get really into it with this guy right here, Steve Gibson. He is the technology wizard we all look to when it comes to understanding better what's going on in the digital world. Hi, Steve.

Steve: Hello, Leo. Great to be with you for our last episode of September. What happened?

Leo: It's so quick. It's just so quick.

Steve: So now we're starting into the fourth quarter of 2022, for Episode 890. So a lot of stuff to talk about. It was a busy week in the security world. We're going to examine Europol's, which is sort of the policing force, the enforcement side of the EU government, their desire to retain data on non-criminal EU citizens, which is not technically legal. And we look at the fourth EU nation, speaking of not legal, to declare that the use of Google Analytics is an illegal breach of the GDPR. We're going to look at the question of whether Teapot has been caught. Seems like. And Mozilla says it's no fair that operating systems bundle their own browsers. So here we go again.

Meanwhile, Chrome's forthcoming V3 Manifest threatens add-on adblocker extensions. And past Chrome vulnerabilities are leaving embedded browsers vulnerable, which is an aspect of Chrome we've never talked about before, or Chromium, rather, you know, the engine. Windows 11 actually gets a useful feature.

Leo: No.

Steve: Yeah, I know, it happened.

Leo: No.

Steve: Really. That's amazing. And some U.S. legislation proposes to improve open source software security. We revisit the Iranian/Albanian cyber conflict, now that we know how Iran got into Albania's networks. And after one important and interesting bit of listener feedback about multifactor authentication fatigue, and a quick SpinRite update, we're going to look at some new trends in the dark underworld with the leak of another major piece of cybercrime malware. Thus today's podcast is titled "DarkNet Politics."

Leo: Ooh. Back to the Picture of the Week, Mr. Gibson.

Steve: So this one was just one I've had in the queue for a while. It shows a fishing line descending down into the frame from off-frame. At the end of it is a hook with a worm stuck there. And we've got two fish that are sort of eyeing this, looking like easy prey. And the smaller one of the two is saying, "Be careful. It could be an online scam."

Leo: Yikes. It's a "fishing" scam.

Steve: And yes indeed, it's a "fishing" scam.

Leo: Ohhh.

Steve: So, okay. So an interesting conundrum caught my eye last week. The European Data Protection Supervisor - who we'll just say EDPS for short, European Data Protection Supervisor - which is - it's the European Union's independent supervisory authority chartered with monitoring European institutions and bodies to assure that they respect citizens' rights to privacy and obey their own data protection rules. This EDPS filed a lawsuit with the European Court of Justice against the European Union and Europol. And as I mentioned at the top of the show, Europol is the law enforcement or policing division.

So going back a few months to January of this year, EDPS, that supervisory agency, published the results of a three-year investigation. They said that they had found that Europol, this law enforcement agency of the EU, had secretly collected - secretly collected - large troves of personal information on EU citizens dating back years, even if those persons had not committed any crimes or were under any investigation of any kind. In other words, data collection without cause or oversight. Which is a violation of privacy laws in Europe.

So the EDPS used its regulatory powers - this is after it learned this back in January - to order Europol to filter its database, deleting any and all information they had on European Union citizens that had not committed any crimes over the past six months. It ordered Europol to scrub this database, all of its databases, by January of 2023.

Okay. So now the reason for the lawsuit, which was filed just last week, was that the EDPS said that EU lawmakers went behind its back and passed new legislation in June to allow Europol to retroactively keep all its previously collected information. In reaction to that action in June, the EDPS said it had "strong doubts as to the legality of this retroactive authorization." And now the EDPS says that this new development actively subverts its independence and authority and wants the court to invalidate the new legal amendments and stay its original decision.

Because of this legislative and enforcement infighting, the EDPS investigation and lawsuit are highly controversial topics among law enforcement officials. In an official response in January, defending its massive data collection, Europol said, and they're probably right about this, that deleting this data will "impact its ability to analyze complex and large datasets at the request of EU law enforcement," and that it would hinder the EU's ability to detect and respond to threats such as terrorism, cybercrime, international drug trafficking, and of course you know what's coming next, child abuse, and others, many of which involve transnational investigations at a very large scale. And as I said, they're arguably correct in that assumption. I mean, the problem is of course abuse of this massive collection and dataset.

So the reason these are difficult problems is that both sides of the dispute can be correct, each from their own perspective. 21st-century crime fighting will be enhanced by massive machine learning datasets used for data analysis. But it's also true that enormous databases of sensitive and personally identifiable information need, at the very least, robust safeguards. And there's no better safeguard than the deletion of all such data for non-criminal citizens.

So anyway, I just thought it was interesting that they're basically fighting with themselves over what it is that they should do. Even with governments being well intentioned, remember our friend Bert Hubert, who resigned from his posting in the Netherlands because a branch of his government was trying to push to or past the limits of the safeguards and boundaries that had previously been put in place for a reason.

Leo: You know, so they said if you haven't committed a crime in the last six months, no information about you. But what about a fingerprint database or a DNA database? What if you committed a crime two years ago, and we've got your fingerprints on record?

Steve: Right.

Leo: And you're saying, no, you're not allowed to have any DNA? You're not allowed to have any fingerprints if I haven't committed a crime in the last six months? I think there's a reason to have an archive.

Steve: You have to imagine that criminals who have been convicted are permanently in a system and not subject to that six-month deletion.

Leo: Okay. But then it should say nobody who's ever been convicted of a crime.

Steve: Right.

Leo: If you've never been convicted of a crime, it shouldn't be in there. I agree with that. That absolutely I agree with. But it says six months, for the last six months.

Steve: It does.

Leo: Which implies that if you did it seven months ago, oh, no, you've still got to delete it. And I think that actually does hinder police work unreasonably.

Steve: Yeah, I agree. So, I mean, there is - and so again it's one of these dilemmas where we could do anything we want. We just have to decide what we want to do. And there are opposing forces that have arguments in both directions.

Leo: Yeah, I understand. Privacy is great, but - and maybe that's the rule. If you haven't committed a serious, maybe it should be serious crime, not a petty theft, but a serious misdemeanor or felony, then we have the right to keep your fingerprints and DNA for as long as we want. Right?

Steve: Yeah. Well, and I liked - a couple weeks ago the way I phrased this about privacy and encryption was that if you had absolute privacy, then that would allow individuals to absolutely escape responsibility. And so it's the - like the system we have in the U.S. with a search warrant is conditional privacy. We're protected against illegal search and seizure, as the phrase goes. But if you convince a judge that there is reason to suspect that the interests of the people will be served by incrementally breaching some privacy, you know, a search warrant, then it can be granted. And in that instance, within the limits of that warrant, an individual's privacy, which is not absolute, is then removed for the sake of enforcement.

Anyway, while we're in the neighborhood, Denmark has become the fourth EU member, joining Austria, France, and Italy, to rule that the use of Google Analytics is illegal in Denmark. The Danish Data Protection Agency ruled this week, actually it was last week, that the use of Google Analytics inside the country is not compliant with the GDPR. The agency told local companies to either adjust the tool for increased privacy - and actually there are no useful adjustments, as we'll see in a second - or stop using it.

The beginning of an explanation published last Wednesday said: "In January 2022, the Austrian Data Protection Authority issued a decision on the use of Google Analytics by an Austrian organization." So that was January of this year. "Since then, the Austrian Data Protection Authority has issued another decision on the use of the tool, and several decisions have also been issued by the French Data Protection Authority. Most recently, in June, the Italian Data Protection Authority issued a decision on the use of the tool," the "tool" meaning Google Analytics. "In all of these cases, the supervisory authorities found that the use of Google Analytics under the given circumstances was unlawful."

The Senior Legal Advisor at the Danish Data Protection Agency said: "The GDPR is made to protect the privacy of European citizens. This means, among other things, that you should be able to visit a website without your data ending up in the wrong hands. We've carefully reviewed the possible settings of Google Analytics and have come to the conclusion that you cannot use the tool in its current form without implementing supplementary measures. Since the decisions by our European colleagues, we have looked into the tool and the specific settings available to you when you intend to use Google Analytics. This has been particularly relevant as Google, following the first Austrian decision, has begun to provide additional settings in relation to what data can be collected by the tool. However, our conclusion is that the tool still cannot, without more, be used lawfully."

Okay. So organizations in Denmark that employ Google Analytics, which is on so many websites...

Leo: Including ours, I might add.

Steve: Yeah.

Leo: Does this mean I can't have anymore Denmark listeners?

Steve: Okay. So that's really a question, right, is like the fact that the GDPR technically reaches us; right? And so we have to be compliant if EU citizens come to websites in the U.S. So anyway, its use is widespread. And organizations in Denmark, after this order, must assess whether their possible continued use of the tool takes place in compliance with data protection law. And the ruling here says it can't. And if it's not the case that they can be compliant, the organization must either bring its use of the tool into compliance or, if necessary, discontinue using the tool. So there are now four countries which have all said it's not possible for the tool to be used in compliance regardless of its settings.

The Senior Legal Advisor said: "A very important task for the Danish Data Protection Agency is to give guidance to citizens about their rights, and to give guidance to Danish organizations in how they comply with data protection law. As is the case with data protection law, we at the Danish Data Protection Agency are neutral to technology, and therefore have no interest in either approving or banning certain products. We are not at all empowered to do so. Following the decisions of our European colleagues, however,

we've experienced a great demand for guidance in relation to specifically Google Analytics, and we have therefore made an effort to look into this specific tool more closely."

Okay. So the message from the Danish Data Protection Agency is that any enterprise's websites that are within Danish jurisdiction - or, again, actually within the reach of the EU's GDPR - which use Google Analytics must put in place a plan to bring their use into compliance by implementing supplementary measures. We'll get to that in one second. And they said: "If it is not possible to implement effective supplementary measures, you must stop using the tool and, if necessary, find another tool that can provide web analytics and allows for compliance with data protection law." Boy, Google must be really getting some headaches with all this. "For example," they said, "by not transferring personal data about visitors to 'unsafe' third countries."

Okay. So what are these "supplementary measures" that could be taken? Well, it turns out that France, the second of the four EU countries to object to Google's Analytics, invested some technical resources to provide a document which answers the question. The document, dated July 20th of this year, a little over two months ago, is titled "Google Analytics and Data Transfers: How to Make Your Analytics Tool Compliant with the GDPR."

Okay. So the French document explains. It says: "The Court of Justice of the European Union (CJEU), in its ruling 16 July 2020, invalidated the Privacy Shield, a mechanism that provided a framework for transfers of personal data between the European Union and the United States. The U.S. legislation does not offer sufficient guarantees in the face of the risk of access by the authorities, particularly intelligence services, to the personal data of European residents.

"Following these formal notices, many actors have sought to identify the technical settings and measures that can allow to maintain the use of Google Analytics while respecting the privacy of Internet users. However, simply changing the processing settings of the IP address is not sufficient to meet the requirements of the CJEU, especially as these continue to be transferred to the U.S. Another idea often put forward is the use of encryption of the identifier generated by Google Analytics, or replacing it with an identifier generated by the site operator. However, in practice, this provides little to no additional guarantee against possible re-identification of data subjects, mainly due to the persistent processing of the IP address by Google.

"The fundamental problem that prevents these measures from addressing the issue of access of data by non-European authorities is that of direct contact, via an HTTPS connection, between the individual's" - now, they call it a "terminal," but we know that's PC and browser or device and browser - "the individual's terminal and servers managed by Google.

"The resulting requests allow these servers to obtain the IP address of the Internet user as well as a lot of information about his terminal. This information may realistically allow the user to be re-identified and, consequently, to access his or her browsing on all sites using Google Analytics." And of course that's 100% true. 100% technically accurate.

Leo: Same thing happens when you do a Google search, but okay.

Steve: Yeah, yeah. They said: "Only solutions allowing to break this contact between the terminal and the server can address the issue."

Leo: So they should ban Google. Seriously.

Steve: Well, yeah, yeah.

Leo: So I don't understand. If the same thing happens when I do a Google search, and you don't want it to happen with Analytics, well, just ban Google. Let's see what happens then.

Steve: So, okay. "So beyond the case of Google Analytics," they said, "this type of solution could also make it possible to reconcile the use of other analytics tools with the GDPR rules on data transfer." Okay. So that all makes sense. The issue is that the user's machine and web browser, or "terminal" as they say here, is posting its analytics directly to a Google domain. So its incoming IP address is always known to Google. To resolve this, the French recommendations, and this is in this formal document that they published, are that a proxy server would be a possible solution.

They say: "In view of the criteria mentioned above, one possible solution is the use of a proxy server to avoid any direct contact between the Internet user's terminal and the servers of the analytics tool, in this case Google. However, it must be ensured that this server fulfills a set of criteria in order to be able to consider that this additional measure is in line with what is presented by the EDPB" - whoever they are - "in his recommendations of 18 June 2021. Indeed, such a process would correspond to the use case of pseudonymization before data export."

They said: "As stated in these recommendations, such an export is only possible if the controller has established, through a thorough analysis, that the pseudonymized personal data cannot be attributed to an identified or identifiable individual, even if cross-checked with other information. It's therefore necessary, beyond the simple absence of a request from the user's terminal to the servers of the analytics tool, to ensure that all of the information transmitted does not in any way allow the person to be re-identified, even when considering the considerable means available to the authorities likely to carry out such re-identification."

So in other words, they're talking about really being serious about erecting a barrier between the EU citizens and anyone downstream of this barrier. So, and they specify what is entailed. They said: "The server carrying out the proxification must therefore implement a set of measures to limit the data transferred. The CNIL" - which is the group that created this document - "considers, in principle, the following is necessary: The absence of transfer of the IP address to the servers of the analytics tool. If a location is transmitted to the servers of the measurement tool, it must be carried out by the proxy server, and the level of precision must ensure that this information does not allow the person to be re-identified, for example, by using a geographical mesh ensuring a minimum number of Internet users per cell." So they're just giving some samples.

And the replacement of the user identifier by the proxy server: "To ensure effective pseudonymization, the algorithm performing the replacement should ensure a sufficient level of collision, i.e., a sufficient probability that two different identifiers will give an identical result after a hash." Okay. Now we start to have a problem because, if you do this, then you're breaking the point of analytics, which is to identify the activity of the site, although you are keeping the specific user who's visiting the site secret, so you are getting pseudonymized per user data still.

Also they specified the removal of referrer information from the site. That's a problem for analytics because analytics wants to know where you are, like where you are on the site,

which is what the referrer information in the query header provides. Also the removal of any parameters contained in the collected URLs, that is, you know, URL tails - UTMs, also URL parameters which may also cause a leakage of information. Also reprocessing of information, they said, that can be used to generate a fingerprint, such as user-agents, to remove the rarest configurations that can lead to re-identification. So make those all look the same. The absence of collection of cross-site or lasting identifiers, a CRM ID or any sort of a unique ID. And the deletion of any other data that could lead to re-identification. In other words, it is a daunting task.

They go on to say: "The proxy server must also be hosted in conditions that ensure that the data it processes will not be transferred outside the European Union to a country that does not provide a level of protection substantially equivalent to that provided within the European Economic Area." So, wow. More and more what we're seeing here is kind of the way they would like the Internet to be in the EU, coming into head-to-head collision with the current operation of the Internet, and asking for huge changes. Establishing a proxy would be a lot to ask for the typical website that just wants to use analytics because it was two lines of JavaScript code, and they got all this amazing information for free.

Leo: Yeah, we want to know how many people visit our site.

Steve: Yeah, and which pages, and what search terms brought them there, you know, and all this cool stuff. A Google Analytics proxying service could be set up somewhere in the EU. Then EU websites would point their Google Analytics JavaScript to that service's domain instead of to analytics.google.com. In that way, the visitors to any of these GDPR-compliant Google Analytics-using websites would have their browsers query the proxy on their behalf. Since the proxy would be terminating their TLS connections, it would be able to strip identifying information from the query, make any changes it wanted to, insert some randomization to confuse fingerprinters, and so on.

So we have another example here of the growing tension between privacy and commerce. And what they're asking for is feasible. But, boy, you know, are they going to enforce it? Are they going to require it? And it would require setting up a local proxy within the jurisdiction of any country or countries that wanted to enforce this level of anonymization through something like Google Analytics and route all the queries through it before it then goes to Google for their data correction.

Leo: And who runs the proxy and sees the information on the proxy?

Steve: I know. Well, so they're saying...

Leo: Sounds like a data grab.

Steve: That would need to be in the EU. And, yeah, it's going to be another centralization.

Leo: Set a third eyeball to watching this and see what happens.

Steve: But their point, of course, is that it's not leaving the EU for the U.S. And so, you know, it is a solution to the problem. But, boy, it's a heavy lift in order to change the

operation of something which has been in place already, what, Leo, like 15 years or 20 years?

Leo: Yeah. And it's going to slow it down dramatically.

Steve: Yup.

Leo: We don't get, you know, when you use Google Analytics, I don't get any individual information about visitors at all.

Steve: Right. You don't, but Google does, and that's their complaint.

Leo: The presumption is that Google does, and does something with it, yeah. By the way, if I were to run a local analytics program, I would get all of that information. I'd get all the IP addresses and everything. This just seems so wrong-headed to me. I don't understand.

Steve: I know.

Leo: I understand what they want. I don't understand how they think this is going to get them there.

Steve: Yeah, well, and again, it's like now we have to agree to cookies wherever we go. Thank you very much.

Leo: Oh, yeah, that's really worked. Oh, boy, has that solved that problem.

Steve: Okay. In last week's network breach review, we were just talking about the Uber and Rockstar Game breaches and the belief that both quite public intrusions were perpetrated by the same teenager. So I wanted to just note for the record that last Thursday the City of London police detained a 17 year old from Oxfordshire on hacking-related charges.

Leo: And it ain't his first rodeo.

Steve: While U.K. officials have not released the suspect's name or other details about his arrest, the teen is widely suspected of being Teapot, a member of the Lapsus$ gang, who recently breached Uber and Rockstar Games. And I would love to know how this kid was tracked down. As I mentioned when we talked about this before, he seemed to be extremely braggadocious about these breaches. And the more one struts around crowing, the more clues you inadvertently leave behind.

Leo: Well, and also this is the same kid that already has been arrested for the Microsoft hack, the earlier Lapsus$ hack. That's what they're saying. So this kid, not only is he braggadocious, but he keeps...

Steve: He's not learning a lesson.

Leo: It's like, he's currently on parole for that. Or probation, I think, not parole.

Steve: Probation, yeah.

Leo: On probation for that.

Steve: It's only probably the fact that he's a minor that I saving him at this point.

Leo: Yes, right. That's right. That's right. Well, I wonder if Lapsus$...

Steve: I mean, these are felonies. These are felonies.

Leo: I wonder if Lapsus$ is a gang, or just this guy, frankly.

Steve: This is felony cyber intrusion.

Leo: Yeah.

Steve: So, wow.

Leo: And he's using, you know, in every case he's used social engineering, you know, posing as somebody, and give me your two-factor kind of thing.

Steve: Okay. So let's take a break, and then we're going to talk about Mozilla saying it's no fair.

Leo: It's no fair.

Steve: It's no fair.

Leo: It's not fair, Mark. Okay. Moving right along, I'm still kind of trying to figure out what we're going to do at TWiT about these GDPR things because that's now, what, four or five countries that won't allow Analytics.

Steve: Everybody who is asked to rule on it rules the way they have to, which is it is a breach of the GDPR.

Leo: Yeah. It requires - and it's I think mostly because GDPR considers IP addresses IIP; right? PII, rather, Personally Identifiable Information.

Steve: Yes. But we know that IP addresses tend to be relatively static. But they're also going way further, talking about unique tokens and referrer headers and, I mean, they're getting aggressive. I mean, this is France saying ooh la la.

Mozilla says "No fair." They recently published a 66-page sour grapes document complaining that they don't own any major platform, whereas Google, Apple, Meta, Amazon, and Microsoft each do. And that each of those major players bundles their respective browsers with their operating systems and quite naturally sets them as the operating system default in the home screen or dock. And that as a result, for most people, this placement is sufficient, and they will never see or pursue the extra steps necessary, as Mozilla says, to discover alternatives. You know, one of my favorite observations, "the tyranny of the default."

So this paper is titled "Five Walled Gardens: Why Browsers Are Essential to the Internet, and How Operating Systems Are Holding Them Back." And they might have been titled the document "Why Firefox is losing market share, and it's no fair." Now, I know that doesn't make me seem very sympathetic. I actually am. I love Firefox. You and I, Leo, talk about it all the time.

Leo: Using it right now, yeah.

Steve: Yup. I've been a Firefox user as my primary browser on every one of my machines for decades. Firefox is the default registered URL handler on every one of my PCs. If a link is clicked, Firefox receives it. What I am aggrieved by is the constant annoyance of the other non-Firefox browsers which, seeing that they are not the chosen one, use every opportunity to suggest that my browsing experience could be greatly enhanced if I were using them to view that page.

So Mozilla's 66-page paper amounts to them making a truly compelling case - I mean, there's no question that this is going on, we know it is - a compelling case for exactly how screwed they are going forward. They blame the OS vendors for putting their own self-interest first. You know, welcome to America.

It's unclear to me what this is actually about. Is this a prelude to another browser wars antitrust lawsuit? I hope not. But some of the language in the 66-page complaint, which is what it actually literally is, is a complaint does appear to be paving the ground for something. And they sort of made an offhand reference to wouldn't it be all better if we could come to an agreement sort of thing. So Google is currently funding Mozilla to the tune of $450 million per year in return for Firefox defaulting to Google as its search engine. So there's the tyranny of the default for you again, this time working in Firefox's favor.

On December 27th of 2011, so 11 years ago, Wired Magazine published "Why Google Continues to Fund Firefox." And their subhead was: "Google has its own web browser, so why is the company renewing its revenue deal with Mozilla? The answer is simple," they write. "Google makes money by putting eyeballs in front of ads, and almost a quarter of the web's eyeballs use Firefox." Now, I was sad to read that 11 years ago because that's

decidedly no longer the case. The 2022 market share for the top four browsers is Google Chrome obviously in first place at 77.03%; Safari in second place at 8.87%. Mozilla Firefox

holding the third place at 7.69%. And to me surprising, Microsoft Edge in fourth place at only 5.83%.

I think it's clear that Safari's edge is thanks to the gazillion iPhones and iPads since the macOS, while it's there, it would not be making nearly as huge a dent. But bless its little digital heart, Firefox is hanging in there at number three, still nicely and somewhat amazingly edging out Edge by nearly two percentage points. But it's unclear what Firefox's future is. They laid off, what was it, 25% of their workforce a year ago. And their deal with Google, I think, is up for something in 2023 is when this - I think it was a three-year deal for Firefox and Mozilla. So people have said, oh, it behooves Google to keep Firefox alive because it keeps them from seeming like a monopolistic entity for antitrust purposes. Who knows?

But anyway, I just thought I'd put a note about the 66-page boohoo note from Mozilla. It's like, yeah, sorry, you don't have an operating system platform of your own. And Leo, you and I know how bad a monoculture is. The idea that everybody is using the same singular Chromium engine is bad because it means those mistakes are universal when they are found.

Leo: Exactly, yeah.

Steve: Yeah.

Leo: Plus, well, I just want competition. I want a variety.

Steve: Yup. It's good.

Leo: Safari's doing all right. But WebKit is in its way like Chromium, kind of a dominant engine. I need Mozilla to succeed. We may have to just start raising money for them or something, if Google pulls out.

Steve: Yeah. So back in November of 2020, Google announced what they called Manifest V3 for Chromium and Chrome. And we talked about it at the time. As I get into this, some of our listeners will go, oh, yeah, I remember. The concern back then was the deleterious effect that it would have on adblockers, that is, this V3 Manifest, which comes as no surprise to Google critics. So as you may recall when we were talking about this before, Google is changing the way Chrome's extensions function. Rather than allowing individual extensions to receive, examine and either drop, modify, or forward each of the browser's outgoing requests, as has always been allowed until now, under Manifest V3 there's a new API called "declarativeNetRequest." And it operates sort of the way its name suggests if you're into APIs, that is, it's declarative rather than - what's the reverse of declarative? I'm blanking on the word.

Leo: Imperative?

Steve: Yeah, imperative. Okay. So this "declarativeNetRequest" allows extensions to modify and block network requests in what Google calls a privacy-preserving and performant way.

Leo: Implicit.

Steve: Well, it actually is. They did say "performant." So what this actually means is that Google remains in control. What occurs under Manifest V3, which by the way is on its way rolling out, is rather than intercepting a request and modifying it procedurally - that was the word I was looking for instead of declarative, procedural - modifying it procedurally, the extension registers with Chrome, asking it to evaluate and modify requests, like matching requests, on its behalf. The extension declares a set of rules, and we're not sure how many there may be. But adblockers need a gazillion. If you've ever seen the rule set on an adblocker, it just, you know, it makes your eyes water.

So the extension declares a set of rules, patterns to match requests, and actions to perform when matched. The browser engine, Chromium, then modifies network requests as defined by these rules. So you can see it's a completely different way of operating, and it's got the adblocker extensions a little nervous. Google claims that: "Using this declarative approach dramatically reduces the need for persistent host permissions." And they're not wrong. I mean, this is an elegant way of solving the problem. But it definitely eliminates control from extensions that they have historically had. But Chrome is also tightening down on and limiting the power of its extensions, and Google cynics are suggesting that it's a move to protect its advertising revenue. Of course they are.

So it's for this reason that the Vivaldi Browser's lead developer took the time to post last Friday that come hell or high water - those are my words, not his - Vivaldi's adblocking would continue to be effective even in the face of Manifest 3. In his post on Friday, Julian wrote: "The move to Manifest V3 makes it more difficult to run content blockers and privacy extensions in Chrome. While some users may not notice a difference, users who use multiple extensions or add custom filter lists may run into artificial limitations set by Google." He says: "Perhaps wise to move away from Chrome?"

He says: "As Vivaldi is built on the Chromium code, how we tackle the API change depends on how Google implements the restriction. The assurance is, whatever restrictions Google adds, in the end we'll look into removing them." He finished: "Our mission will always be to ensure that you have the choice."

So Julian notes that the entire existing V2 API - I'm sorry, yeah, the existing V2 API continues to be present for Chrome's enterprise users. So that means that it's only the consumer who is being hit with this restriction, and that all of the existing code remains accessible somewhere. So it's going to be interesting to watch this one shake out. While Firefox, as I've said, is my default URL handler, I do often use Chrome for ad hoc Internet research. I edit this podcast. The show notes in front of us are done in Google Docs every week. And things have grown so horrendous on the 'Net that I could not live without an effective adblocker any longer. If Chrome really does become an advertising browser and makes the ability to suppress the insanity that too many web pages have become, you know, they might drive a move back to Firefox.

Leo: So I'm with you. And I use Gorhill's UBlock Origin, just like you. And by the way, it has a built-in cookie banner blocker, among other things. It's one of the annoyances features. But do you think there's a legitimate security reason for Google to insist on Manifest V3?

Steve: Yes.

Leo: In other words, that web content API is potentially insecure. It's potentially a problem; right?

Steve: Yes. It's known as the webRequest API. And, I mean, it literally is a "call each extension in turn and let them each look at it, modify it, drop it, or forward it." So, I mean, these extensions as they are now are in the pipeline. And so there is, this is why they use the word "performant."

Leo: Right.

Steve: Because if an extension takes a long time to think about one of these queries that's been handed to it, the whole process slows down. So what Google is doing is Google is trying to compromise here. I mean, and it's a legitimate, you know, attempt at compromise. They're saying we're going to build a screaming fast pattern-matching engine. You put the matches in you want. And it'll be a big regex machine. You put the regular expressions in that you want matched, specify the changes you want made. We'll do them for you.

So what that does is of course it completely eliminates this pipeline, this per-extension processing pipeline which both gives us, Google, the users, everybody, more security, and potentially substantially greater speed because Google is saying we're going to, you know, who knows what they're going to do? They might at launch time, when all the extensions are in place and have registered their list of regex work, Google could compile it, like into some screaming fast blob that just, you know, queries go in, and the results immediately come out the other end. So they can't do that now with the V2 architecture. They need to move to this V3 model. And once again it's going to be a tradeoff. Extensions are going to lose some power.

Leo: I wish we could find some sort of compromise, and I wish it didn't look so much like Google wanted to preserve their ad business.

Steve: I know. And you know, Leo, that keeps coming up, the idea, unfortunately, that the entity offering a browser, which is the thing that displays ads, is the revenue for that entity, I mean, it creates, like it's a built-in conflict of interest.

Leo: Yeah, yeah, of course. Same thing when YouTube search results top the Google search results; you know? You can go on and on. Google self-deals all the time.

Steve: Yeah. Okay. So here's one that had never occurred to me before, while we're on the topic of Chrome. A group known as Numen (N-U-M-E-N) Cyber Labs have published extensive write-ups on a pair of older and long-since-fixed Chrome vulnerabilities, CVE-2021-38003 and 2022-1364. Both were Chrome zero-days patched in October 2021 and April of 2022, respectively. And either one could be used at the time for remote code execution attacks against Chrome users.

What's interesting and chilling about Numen's observation is that they warn that even though these two security flaws have been patched in the main Chromium core and

Chrome browser, the patch gap that exists in software that uses Chrome's WebKit engine as their built-in browser means that many mobile apps are still vulnerable to this, including, and they use this as an example, the most recent release of Skype, which is subject to a zero-day remote-code execution flaw because it uses the Chromium core and has not been patched, even though Chromium was, the most recent one in April and the previous one in October of last year.

I thought that was a fascinating observation, and one, as I said, we've never considered. I often talk glowingly about how the Chromium guys jump on a report of a new zero-day and often push out an update only a day or two later. But applications that incorporate Chrome's WebKit engine, Chromium, are taking a snapshot of the engine and may be far more lackadaisical about keeping that engine snapshot up to date. After all, it's working. Why bother with it? Well, why indeed? After all, the Chromium engine, as we know, is truly a work-in-progress moving target. But that's anathema to projects that want to build from essentially static libraries. I would be willing to bet that very few of them are pushing out new release builds of their application because one of their component dependencies, in this case Chromium, was updated. And as we know, those Chromium updates are happening all the time.

So to me it seems unlikely in the extreme that apps are being that responsible. So any and all of such applications - and again they showed on the screen Skype being taken over - might well be inheriting and existing with Chrome's historical vulnerabilities. This again is another good reason for Google never to talk about them, no matter how old they are. But unfortunately these Numen guys did a complete takedown of both of these. So any app that is using an un-updated Chromium now who sees what Numen Cyber Labs has published, can start poking at any embedded browser engines to see if they're able to take the app over remotely.

So it's a chilling thing that we never really talked about. But it's a consequence of, you know, a browser engine being so complex, being inherently a moving target, yet we get this, as they called it, the patch gap between when the library was taken and what version they're using and when it was built into their app. And are they even bothering? Do they even care? Yikes.

Okay. We all know that I'm not a big fan of Windows 11. That's primarily because of the lies we were told about its hardware system requirements from the beginning, which never made a lick of engineering sense and which, sure enough, were eventually acknowledged to be untrue. I remember Paul and Mary Jo saying, oh, yeah, yeah, yeah, that's not true.

Leo: Although I'm going to add that last week we started talking about a new feature that's rolling out in 22H2 of Windows 11 that does perhaps explain 8th-generation Intel and TPM 2.0.

Steve: Okay.

Leo: And it has to do with virtualization, and I can't remember the exact details. But it perhaps then does make sense that they knew this was coming as a security update, and they wanted to make sure it was supported, and that if you were using Windows 11...

Steve: And they didn't want to drop that they...

Leo: They didn't want to tell anybody yet.

Steve: Well, and they didn't want to allow a subsequent update to Windows 11 to suddenly say, oh, we're sorry.

Leo: Yes.

Steve: You can't have the Windows 11 update because your chip is too old.

Leo: Yeah. Let me look at the notes from last week because you deserve the info, anyway, as best as I can interpret it. There is a hint at why Microsoft chose 8th-gen as the dividing line a year ago, except what was that hint? They didn't put it in the notes. They just said we'll tell you about it. But as I remember, it has something to do with virtualization.

Steve: Interesting. Okay.

Leo: Yeah. So there may be kind of a reason for it; right.

Steve: So some new hardware level thing that the 8th-gen chips have that the previous ones don't.

Leo: Precisely.

Steve: And Windows until now has not depended upon on that.

Leo: Exactly.

Steve: Well, because it ran on all the chips.

Leo: Right, right. And that may be why they say we won't promise to support it if you run it on older hardware. They are allowing people to do that. But you won't get the security, new security feature.

Steve: Right, right. So it's still unclear on Windows 11 whether I will be eventually forced to move away from Windows 10, or whether Microsoft will eventually take no for an answer. You know, I'm still happily - I'm sitting in front of Windows 7 right now. Works great, and they leave me alone. Anyway...

Leo: It's a race between Episode 999 and when Windows 10 is no longer in support. Let's just put it that way.

Steve: That's right. So we'll see; you know? Anyway, okay. So in at least one instance, you know, it looks like they've done something useful. Believe it or not, Microsoft will finally, at long last, be adding default brute force protection into Windows 11's notoriously insecure SMB file and printer sharing user authentication. So it's called the SMB authentication rate limiter concept.

Leo: Woohoo.

Steve: Who would have ever imagined you could do that with a computer?

Leo: Geez. Wow.

Steve: But it turns out, Leo, you need an 8th-generation Intel processor in order to do rate limiting. You can't have it. You could not have it on a - Windows 95 could not have done rate limiting.

Leo: Never. Never in a million years.

Steve: It's too advanced.

Leo: Yes.

Steve: It is an advanced technology. It was reverse-engineered from, where is that place where the UFOs are all seen?

Leo: Yeah, Area 51, yeah.

Steve: Oh, it came out of Area 51. They said, okay, we don't know, we're unable to crack these alien computers, and they won't let us keep guessing passwords. They slow us down. Huh. Isn't it too bad we can't put that into Windows? We'll have to wait till Intel's 8th-generation processors. Anyway, we finally have it. It's currently being tested by insider builds. As its name suggests, this new advanced feature from the aliens will significantly rate-limit brute force attacks against a Windows 11 SMB service. So anyone who either deliberately or inadvertently exposes their SMB services on port 445 to the public Internet, as so many people seem unable to keep from doing, they will receive a modicum of protection.

With the release of Windows 11 Insider Preview Build 25206 Dev Channel today, the SMB server service now incorporates a two-second default delay, that's what the aliens used, Leo, so they didn't want to change anything because that might have broken something, and it might be some magic there. It uses a two-second default delay after each failed inbound NTLM authentication attempt. This means that if an attacker previously sent, for example, 300 brute force attempts per second from a client for five minutes thus 90,000 username and password guesses now the same number of attempts would take 50 hours, rather than five minutes. Somewhat sad to be celebrating such a simple measure that could have been implemented anytime in the past 20 years, but better late than never.

Also, as I mentioned, two U.S. senators, Rob Portman, who's an Ohio Republican, and Gary Peters, a Michigan Democrat, introduced a bill last Thursday in a bid to strengthen the security of open source software. Together they co-sponsored the bipartisan, and I love this one, it's Securing Open Source Software Act. And when I looked at it, I realized it was the SOS Software Act. So Securing Open Source Software Act. The goal is to help protect federal and critical infrastructure systems by strengthening the security of open source software.

And what do you think got their attention? Yup, the legislation comes after a hearing convened by Portman and Peters on the Log4j incident at the beginning of the year, and it would direct our favorite agency, CISA, to help ensure that open source software is used safely and securely by the federal government, critical infrastructure, and others. Now, how they actually do that remains to be seen.

The SOS Software Act directs CISA to develop a risk framework - because, you know, if you're going to be a bureaucrat, you've got to have a framework - a risk framework to evaluate how open source code is used by the federal government. Apparently they don't know now. CISA, oh, we're going to have a risk framework to evaluate how open source software code is used by the federal government. CISA would evaluate how the same framework could be voluntarily used by critical infrastructure owners and operators. This will identify ways to mitigate risks in systems that use open source software. The legislation also requires CISA to hire professionals with experience - they're going to get some money - experience developing open source software to ensure that government and the community work hand-in-hand and prepare to address incidents like the Log4j vulnerability. Yeah, let's prepare.

Additionally, the legislation requires the Office for Management and Budget to issue guidance to federal agencies - wow - on the secure usage of open source software and establishes a software security subcommittee on the CISA Cybersecurity Advisory Committee. So the CISA Cybersecurity Advisory Committee will have a software security subcommittee that is used by the OMB or something. So good luck.

Leo: Yeah.

Steve: I have a healthy skepticism of bureaucracy and legislators. It's unclear to me that they will ever get anything right. But if the federal government wants to hire a bunch of open source software folks, who have been working up till now for free, to help in any way they can, then seems like it could be good. It could help.

Recall that we talked a couple of weeks ago about the Albanian government's unexpectedly strong reaction to Iran's cyberattack on their infrastructure due to Iran being upset with Albania for providing sanctuary to a group of disaffected Iranians. That was the MEK group. Albania closed Iran's embassy and ejected Iran's ambassadors from the country. We believed, without many facts to back it up, that Iran had been maintaining a presence inside of Albania's government networks for quite some time before the attack. That meant that when Iran's rulers said "Let 'em have it!" Iran's cyberwarfare people simply had to flip a switch.

Well, now, last week, some new information has come to light. The CISA and FBI said last Wednesday that hackers connected to Iran's military spent 14 months inside the networks of the Albanian government prior to launching the ransomware attack that caused widespread damage in July. The FBI did not specify which Iranian hacking group was behind the incident, but explained that in their investigation they found the hackers exploited an Internet-facing Microsoft SharePoint through a well-known and long since repaired vulnerability CVE-2019-0604.

That CVE has been classified by cybersecurity experts as one of the most exploited bugs throughout 2020, having been abused by both nation-states and ransomware groups. According to the alert, the hackers were able to maintain continuous access to the network for more than a year, frequently stealing emails throughout 2021. By May of 2022, the actors began moving laterally and examining the network, performing wider credential theft across Albanian government networks.

This all preceded the July cyberattack that crippled the country's government. The FBI confirmed reports from Reuters and researchers that the attacks were launched due to Albania's involvement with the group known as MEK. Albania, as we talked about, when we talked about this a couple of weeks ago, has allowed about 3,000 members of the group to settle near Durres, the country's main port. The agencies said that in July of 2022, the hackers "launched ransomware on the networks, leaving an anti-MEK message on desktops."

So we have a perfect example of, A, why Albania should have updated their instance of SharePoint shortly after patches for the vulnerability were made available; and, B, why having passive intrusion detection present, waiting and watching inside networks, can no longer be considered a luxury. We know that, try as we might, real-world security is imperfect, and the bad guys only need to find a single imperfection. And one of those bits of imperfection might take the form of a single well-meaning employee. So it's most likely that the bad guys will eventually succeed if they are trying hard enough. Therefore, any truly effective and secure solution must assume that a compromise will occur sooner or later.

That being the case, immediate detection of such an intrusion is every bit as critical as attempting to keep the bad guys out in the first place. And the entire government of Albania learned a lesson of not having done either of those two things. They didn't patch SharePoint when it was fixed, and they were completely unaware that they were hosting Iranian intruders in their networks for 14 months. Talk about an advanced persistent threat.

Okay. A piece of closing-the-loop feedback from a listener, and someone I know pretty well from the GRC newsgroups. After hearing last week's discussion of the Uber attack, which was effective even in the presence of multifactor authentication, a well-known contributor to our newsgroups posted his thoughts into the Security Now! newsgroup, which is one of the many that we have at news.grc.com. His handle in the groups is ferrix, F-E-R-R-I-X, and his real-world name is Greg. I was aware last week that something didn't feel right about my take on the multifactor authentication attack. Some people tweeted that it was likely an "MFA fatigue" attack. And I think that they and Greg are correct.

So here's how Greg, who by the way works in MFA (multifactor authentication) professionally, explained what happened with the Uber contractor. He wrote: "When reading about the Uber hack, Steve assumed some details about the MFA that led his discussion slightly astray. I work in providing MFA services for my day job, so I know a bit more pedantic detail than the average bear.

"If the MFA in question was a time-based one-time-password (OTP) as Steve said, then what he said about brute forcing codes would also have been correct. An attacker would have in theory brute force logon attempts with codes 000000, 000001, 000002, et cetera, until matching the correct six digits. It would have been an extremely loud attack since there's a pretty limited time to log in with the current code before it moves out of the window. But that's not what happened here."

He wrote: "Uber is using 'push notification' MFA, like what Okta and Duo do. The user or attacker tries to authenticate to some resource X. The MFA provider pushes a question to

its app on the user's phone, 'Do you want to log into X?' with an Approve button. The simple theory here is the attacker doesn't have the user's phone, there's no real way to attack the secure channel between the MFA provider and its app, and if the attacker repeatedly tries to log in, the user's phone would blow up with loads of spurious push requests to approve, which is very noticeable.

"The security model breaks either when users are naive, or attackers are clever in particular ways. A naive user might approve an attacker's push by rote, even without thinking about it. Or they might see the repeated attack push requests as, 'Well, it looks like something important is trying to run on X, I better approve it,' and thus be tricked.

"A clever attacker would schedule their attacks slowly, and at opportune moments where the real user might be plausibly trying to log into the resource, such as the beginning of the workday or after lunch. There's a normal," he said, "'background radiation'" - using my term deliberately, he put it in quotes - "of false positive push requests that these complex systems generate, as various things try to sign into other things. So it's very reasonable that a user might not realize that they're under attack, and they might tap Accept. This is," he says, "(as far as I can tell), what happened to the Uber external staffer."

He says: "Now let's talk about the mitigation Uber has turned on to improve their security posture, often called 'Verified Push.' The resource logon page now shows a short challenge number or word. The smartphone app now says 'Logging into X? Click the matching challenge,' then shows four or five multiple-choice buttons. Now it's not possible for the user to blindly approve anymore. They must select the button that matches the challenge, which they only know if they are actually looking at the X login page. Else, the attacker would also have to communicate the correct challenge to the user in some out-of-band way, which is a more difficult attack model."

He finishes, saying: "Orthogonally, please note that the above discussion does not contemplate man-in-the-middle attacks between a real user trying to log in and the resource X they're trying to access. In that attack, the attacker can await the session to be validated, then steal the session to do their bidding. To mitigate that threat, the system would need to use a phishing-resistant auth solution such as a properly implemented FIDO2 or, notionally, SQRL." So Greg, thank you for the clarification. And I think he's probably exactly right.

Leo: Yeah, that makes sense, yeah.

Steve: Yeah.

Leo: We actually heard that with earlier Lapsus$ attacks, that they were using this authentication fatigue, yeah.

Steve: Yes. Known as MFA, multifactor authentication, fatigue, where the user just finally says, okay, fine, and lets the bad guy in.

Okay. Briefly, I'm now on Book 8 of The Silver Ships, and all I can say is that anyone who enjoys science fiction stories has many wonderful, original, and different stories waiting for them. Each book places our characters, whom we get to know quite well, in different, wonderful, and interesting situations. As is evident from the fact that I'm already halfway through Book 8, I'm having quite a difficult time putting them down.

And despite the fact that I've admittedly fallen head over heels for this fabulous 24-novel science fiction book series, work on SpinRite is really coming along. I've been fixing every cosmetic thing that I can find for a while now, and I have one last known cosmetic thing to fix. It involves the mapping of SpinRite's now huge 16MB data transfer blocks to one of SpinRite's screens, its so-called Graphic Status Display, which is a grid that represents the aerial storage of the media being tested. Originally, a single transfer block might have occupied more than one character cell in the Graphic Status Display. I remember that floppy disks would do that. So that used to be the case.

I removed the logic from managing that cross-cell mapping because it simplified and sped up SpinRite's inner loop. And nothing matters more than speed. And since drives were so huge these days, there's no way that the number of data transfer blocks on the drive would not be way more than the number of cells in the Graphic Status Display. So I removed the logic for that, and sped things up. But that also meant that for the first time, on very small drives, since SpinRite's new data transfer blocks are so large, and I'll be allocating a minimum of one transfer block per text cell on the Graphic Status Display, not all of the GSD screen might be used on very small drives. I've run across this because I've got a 100MB virtual drive in VirtualBox where I do some of the testing. And it went, whoops, you know, visually. Anyway, so I'm fixing the case where that might happen. And I expect I'll finish that work tonight.

At that point, I won't know that SpinRite is not finished. But neither will I know that it is. So the last thing I will do before I turn the GRC newsgroups gang loose on SpinRite's first fully functional alpha release, will be to simulate various forms of actual data corruption, then carefully watch it always do the right thing, putting individually recovered sectors back into the right place. If anything there doesn't work, I'll fix it. Then SpinRite will be ready for the group's final external testing. And Leo, I'm ready for some final external water.

Leo: Ah. This can be arranged. We have people who will bring you dihydrous oxide in a special container designed to retain all the CO2 goodness. All right. Now it's time to talk about the subject of the day, Mr. Gibson.

Steve: So I brought us all some bad news.

Leo: Oh, no.

Steve: A couple weeks ago with the rise of Phishing-as-a-Service. But, you know, forewarned is forearmed. Right? I've got some more bad news for us this week.

Leo: Oh, no.

Steve: One of the definitions of the word "politics" is "the debate or conflict among individuals or parties having or hoping to achieve power." It is in that sense of "politics" that I titled today's podcast "DarkNet Politics."

Last week's leak of today's preeminent LockBit 3.0 ransomware led to some very interesting discussion and conjecture by the industry's ransomware-watching security researchers. After the fall of Conti, which we covered, remember all that crazy Costa Rica government nonsense?

Leo: Oh, yeah. Oh, yeah.

Steve: LockBit 3.0 has risen to become the number one ransomware group in the ransomware industry. And I hate using that term, but there it is, "industry." And they've been making something of a splash in the underground. They recently offered, get a load of this, $1,000 to anyone who would permanently tattoo their group's logo on their body.

Leo: Oh, no.

Steve: They had a number of takers.

Leo: Oh, no.

Steve: And I saw a photo of one. Until they terminated the offer.

Leo: Yeah?

Steve: Well, and Leo, we know where you have a tattoo of a logo.

Leo: Yes, of the logo of a company near and dear, yes.

Steve: So today, the group's operations are so extensive that LockBit's victim count some weeks has been greater than all the other ransomware families combined. Ever since Conti's leaks, which marked the beginning of Conti's end, and the curious wind-down involving the Costa Rican government that we covered, LockBit has taken over the ransomware throne. Although business - and again, if you can call it that, I hate doing so.

Although business has been booming for the LockBit 3.0 group, things have recently shaken up a bit by a little known threat actor who claims that his group was able to compromise LockBit's servers to obtain and leak the builder and keygen modules essentially all of the heart of the group's code. It seems that within this odd underworld it's not possible to get too big or someone, a rival or an insider, will take you down. Since this is somewhat reminiscent of the leaks which occurred and triggered Conti's downfall, it raises the question whether this may be the beginning of the end also for Lockbit, as well. We'll see.

Okay. So a threat actor going by the name Ali Quashji, which was a Twitter account with no reputation which was apparently created just to host this leak declaration announcement, claims to have hacked several of LockBit's servers and was able to obtain the LockBit 3.0 builder and the keys generator. Researchers at Cyberint grabbed and analyzed the leaked code and declared it to be real and complete. They said: "Looking at the published files, we could find the builder and key generator modules. The first of them build several executables that perform the encryption and loading phases of LockBit's ransomware attack flow, along with ransom note creation."

Well, The Record, which is a publication of Recorded Future, often does a great job when things like this happen of pulling things together and polling security researchers. In this

instance I thought that some of what they reported was really quite interesting. So in what follows, I've merged some of The Record's reporting with my own interpretation and commentary.

The leak of the LockBit 3.0 ransomware encryptor was announced on Wednesday by security researcher - now, we would pronounce his name Export, his handle Export, but it's numeral 3, xp, numeral 0, rt. So, you know, in LEET speak. Anyway, 3xp0rt announced this. Several experts and researchers confirmed to The Record that the builder works and allows anyone to create their own ransomware. There's the phrase of the week: "allows anyone to create their own ransomware." In a message shared by 3xp0rt, someone allegedly connected to LockBit addressed the issue, attributing the leak to a disgruntled affiliate and dismissing the idea that what was stolen could be used by others to replicate what the ransomware group does. Of course, you know, he would hope that's true.

So this LockBit representative was quoted: "An affiliate program is not a locker. It is a software package, and most importantly an impeccable reputation" - oh, give me a break - "that no one" - what is this guy smoking? - "that no one can tarnish."

Leo: Oh, my, yes.

Steve: "No matter what software leaks occur. Few people will agree to pay randomly to a pen tester without a reputation, hoping for a successful decryption and deletion of stolen data." Now, as I said, I don't know what this LockBit representative has been smoking, but no one ever wants to pay anything to any criminal who has breached their network.

Leo: Only the most trustworthy criminals.

Steve: That's right. Only the criminals with a great reputation. Wait, what? And the reputations of underground criminals has little bearing on whether they get paid. They get paid if there's no alternative, period.

Leo: Yeah, yeah.

Steve: Okay. But The Record's reporting noted that several cybersecurity experts expressed significant concern about that very prospect. Emsisoft's threat analyst Brett Callow compared the situation to last year's leak of the builder for the Babuk Locker ransomware. Brett said: "As was the case when Babuk's builder leaked, we may well see other threat actors use LockBit's, which would obviously complicate attribution." Adding to what Brett said, Huntress Senior Security Researcher John Hammond said less skilled adversaries gravitated to the Babuk ransomware tool because it was simple to customize and use. Unfortunately, it wasn't the same quality as this one.

And Recorded Future's own ransom expert Allan Liska said his team has identified more than 150 "new" ransomware groups just this year. Most of them are using stolen Conti or REvil code. Allan said: "At this time last year, Recorded Future was collecting from about 45 active DLSes." That's short for Dedicated Leak Sites. "Today, that's more than 100." He said there is a real proliferation of ransomware groups, most using leaked/stolen code from other ransomware groups. This is the same reason why the emergence of PHAAS Phishing-as-a-Service as I was talking about - is so disturbing. The emergence of turnkey

services allows those who are not skilled enough to assemble the required infrastructure to no longer need to. It's been done for them in return for a piece of their action.

Dick O'Brien, the principal intelligence analyst for Symantec's Threat Hunter Team, said it's a "near certainty" that we will see other attackers reuse LockBit's source code. According to O'Brien, LockBit's success is partly due to the fact that it has a very effective malware "payload." Dick said that "Other ransomware operators could replace their payloads with rebranded variants of Lockbit, and you could see some aspirant groups use this to launch their own ransomware operations." Excuse me for a second.

Leo: I've run out of ads, so...

Steve: Yeah. I think we can ask our editor to remove that.

Leo: These guys are so grandiose, it's so amazing.

Steve: I know. I know. No one is going to use our stolen stuff because they're not us. And only we can bless this with our reputation. It's like, again, what?

Leo: Yeah, they're awful.

Steve: Anyway, researchers have linked more than 1,029 attacks to LockBit since the group began its operation in 2019. The group was considered a marginal player until just last year when it launched LockBit 2.0, a new version of its initial Ransomware-as-a-Service platform. The group revamped again, launching LockBit 3.0 this past summer and quickly supplanted Conti as the most prolific criminal organization. The gang had at least 68 victims just last month, 68 victims in August, so more than two a day on average, including a crippling attack on a hospital about an hour southeast of Paris that disrupted its medical imaging, patient admissions, and other services. You know, as we've seen.

The cybersecurity firm Dragos attributes about one-third of ransomware attacks targeting industrial systems in the second quarter of this year to LockBit, and Huntress Labs' John Hammond explained that the latest edition of LockBit had new features and functionality to encrypt files faster than ever before. He said the leak of the builder software commoditizes the ability to configure, customize, and ultimately generate the executables to both encrypt and decrypt files. I have, just for side interest, a slide showing the relative distribution by number of attacks of ransomware. And LockBit is out in first place, with Conti in second, and then there's like a drop by two thirds for the rest of them that are also-rans that we've talked about from time to time.

In his discussion with The Record, indicating a screenshot of the leaked configuration file, Hammond said: "Anyone with this utility can start a full-fledged ransomware operation. That is so customizable," he said. "Note how the ransom note can be completely changed."

One small upside of the leak may be that security experts now have it, too. So they're able to analyze and explore this builder software and potentially garner new threat intelligence that could thwart ransomware operations. At a minimum, the leak gives cybersecurity experts greater insight into the inner-workings of LockBit, with the

message from LockBit indicating that they have contracted developers and that they suffer, as well, from insider threats.

Leo: Aww.

Steve: Oh, I know. Poor babies. Poor babies. Recorded Future's Allan Liska said the leak could be a sign of disgruntled factions within the LockBit group. He said: "The large RaaS groups" - Ransomware-as-a-Service groups - "are notorious for paying their developers, IABs" - those are the initial access brokers, remember, who find the way in and sell their access - "and other support staff very poorly." So it's not necessarily a surprise when someone retaliates.

John told The Record that after the Conti Leaks were made freely available, the Conti ransomware builder "gained mass adoption from other threat actor groups wanting to quickly and easily spin up their own ransomware operations. Money is the real motive. And when a tool like this is made available," he said, "it enables anyone to run the racket."

One thing to note is that, though it is customizable, the encryptor still changes the victim wallpaper to say "Lockbit Black," and that cannot be easily changed. More skilled operators may attempt to change that. Or lower-tier and less capable groups may prefer to have the legitimacy of looking like a LockBit attack. The bottom line on all this, driven by the promise of easy money, what was once a somewhat blessedly high-level and high-end form of devastating attack is rapidly moving down into and becoming a commodity available to far less capable criminals to use.

And again, in retrospect, this was inevitable. The lack of true bulletproof enterprise cybersecurity, which enables an environment of porous security, with the emergence of cryptocurrency, which solved the extortion payment problem, together has made massively profitable cyber extortion feasible like never before. And now the last tools required to make the perpetration of these cybercrimes trivial are falling into the hands of the script kiddies. God help us.

Leo: Yeah. Well, you know, you can hope that they eat each other alive, you know, that they just, you know, just keep fighting and infighting and all that stuff. But good lord.

Steve: Yeah. And we did see that the sanctions against Russia are what killed Conti because they aligned themselves powerfully with the Russian government and with Russia.

Leo: Right.

Steve: And no one was able or willing to pay them because they were Russian, and they were now sanctioned.

Leo: Yeah. What a story. Golly. Golly. It's an interesting world we live in, and this show shows us in many ways how more and more interesting it gets with all these...

Steve: And Leo, what's so sad is think of all the resources being expended to fight this.

Leo: Oh, I know. Oh, I know. Yeah. Absolutely.

Steve: I mean, it's guaranteed employment for anybody who's interested in cybersecurity, that's for sure.

Leo: Absolutely, yeah. All right. We do this every Tuesday, and if you're not completely dejected, I hope you'll come back again and do it again with us. Tuesdays, 1:30 p.m. Pacific, 4:30 Eastern, 20:30 UTC. Right after MacBreak Weekly. You can watch us do it at live.twit.tv.

Or after the fact on a podcast, Steve's got copies. Actually, he has two unique copies at his website, GRC.com. He's got the 16Kb audio for the bandwidth-impaired, and he has the transcriptions written by Elaine Farris, so you can read as you listen or use them to search or just read them standalone, get all the content that way. He also has 64Kb audio. We do, too, at TWiT.tv/sn, or on YouTube there's a dedicated channel. Or you can subscribe in your favorite podcast player.

Let's see. I guess that means it's time to adjourn this session.