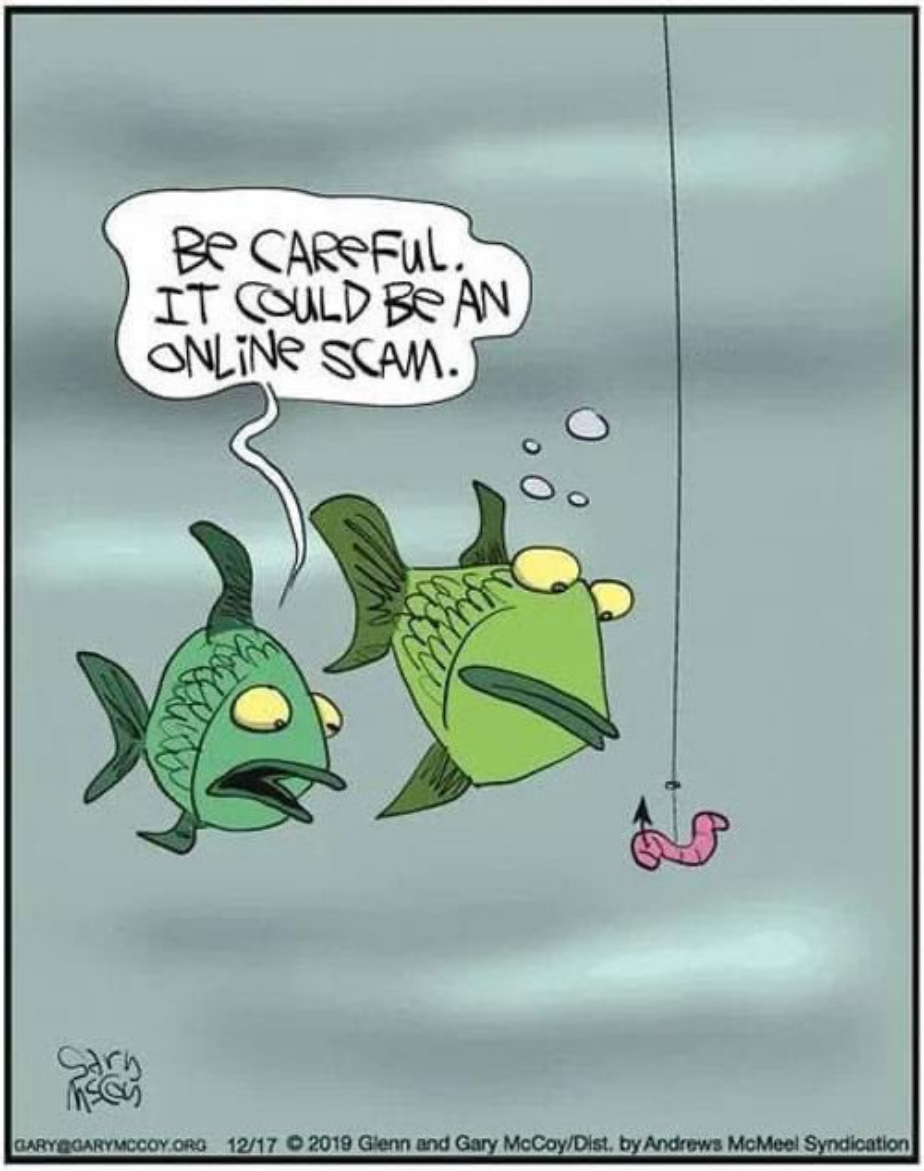
Security Now! #890 - 09-27-22

DarkNet Politics

This week on Security Now!

This week we examine Europol's desire to retain data on non-criminal EU citizens, and we look at the forth 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 ad-blocker extensions, and past Chrome vulnerabilities are leaving embedded browsers vulnerable. Windows 11 actually gets a useful feature, and some US 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 multi-factor 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.



Security News

Can't have it both ways

An interesting conundrum caught my eye last week: The European Data Protection Supervisor (EDPS), which is a European Union independent supervisory authority chartered with monitors European institutions and bodies to assure that they respect citizens' rights to privacy and obey their own data protection rules, filed a lawsuit with the European Court of Justice against the European Union and Europol. Europol is the law enforcement or policing division.

In January of this year, the EDPS (the supervisory agency) published the results of a three-year investigation, They said that they had found that Europol, the law enforcement agency of the European Union (EU), had 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. In other words, data collection without cause or oversight.

The EDPS used its regulatory powers 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 its databases by January 2023.

The reason for the lawsuit filed last week was that the EDPS said that EU lawmakers went behind its back and passed new legislation in June that allowed 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 amendments and stay its 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 that deleting this data will "impact its ability to analyze complex and large datasets at the request of EU law enforcement," which will hinder the EU's ability to detect and respond to threats, such as terrorism, cybercrime, international drugs trafficking, child abuse, and others, many of which involve trans-national investigations at a very large scale. And, they're probably correct in that assumption.

The reason these are difficult problems is that both sides of the dispute can be righteous 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 needs, at the very least, robust safeguards and there's no better safeguard than the deletion of all such data for non-criminal citizens.

Even with governments being well intentioned, Bery Hubert 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 there for a reason.

And 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

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 (through the use of reverse proxies) 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. 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 2022, the Italian Data Protection Authority issued a decision on the use of the tool. In all of these cases, the supervisory authorities found that the use of Google Analytics under the given circumstances was unlawful."*

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 have 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."

Organizations in Denmark that employ Google Analytics, and its use is quite widespread, must therefore assess whether their possible continued use of the tool takes place in compliance with data protection law. If this is not the case, the organization must either bring its use of the tool into compliance, or, if necessary, discontinue using the tool. And there are now four countries which have said that 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 have 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 – but actually within 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. 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, for example by not transferring personal data about visitors to "unsafe" third countries."

So, what are these "supplementary measures" that could be taken? France, the second of the four EU countries to object to Google's Analytics, invested some technical resources to produce a document which answers that question. The document, dated July 20th, a little over two months ago, is titled: "Google Analytics and data transfers: how to make your analytics tool compliant with the GDPR?"

https://www.cnil.fr/en/google-analytics-and-data-transfers-how-make-your-analytics-tool-compliant-gdpr

The French document explains:

> *The Court of Justice of the European Union (CJEU), in its ruling of 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 US legislation does not offer sufficient guarantees in the face of the risk of access by the authorities, particularly the 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 US. 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 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.*
>
> *Only solutions allowing to break this contact between the terminal and the server can address this issue. Beyond the case of Google Analytics, 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. All that 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 are that a Proxy server would be a possible solution. They write:

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 in his recommendations of 18 June 2021. Indeed, such a process would correspond to the use case of pseudonymisation before data export.

As stated in these recommendations, such an export is only possible if the controller has established, through a thorough analysis, that the pseudonymised personal data cannot be attributed to an identified or identifiable individual, even if cross-checked with other information.

It is 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.

The server carrying out the proxyfication must therefore implement a set of measures to limit the data transferred. The CNIL (the group that created this document) considers, in principle, that 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);*
- *The replacement of the user identifier by the proxy server. To ensure effective pseudonymisation, 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) and include a time-varying component (adding a value to the hashed data that evolves over time so that the hash result is not always the same for the same identifier) ;*
- *The removal of external referrer information from the site;*
- *The removal of any parameters contained in the collected URLs (e.g. UTMs, but also URL parameters allowing internal routing of the site);*
- *Reprocessing of information that can be used to generate a fingerprint, such as user-agents, to remove the rarest configurations that can lead to re-identification;*
- *The absence of collection of cross-site or lasting identifiers (CRM ID, unique ID);*
- *The deletion of any other data that could lead to re-identification.*

In other words, it’s a daunting task. They go to add...

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.

In any case, and in accordance with the EDPB recommendations, it will be up to the data controllers to carry out an analysis on this point and to put in place the necessary measures in case they wish to use this type of solution, as well as to verify the maintenance of these measures over time, according to the evolutions of the products.

Establishing a proxy would be a lot for the typical website. But using — to use their term — a proxyfying service would not be prohibitive. A Google Analytics proxying service could be set up somewhere in the EU. Then EU websites would point their Google Analytics 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 connection, it would be able to strip identifying information from their query and insert some randomization to confuse fingerprinters.

So we have another example of the growing tension between privacy and commerce. Can we have both?

I am a Teapot…

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. While UK 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 Lapsu$ gang, who recently breached Uber and Rockstar Games.

I'd love to know how this kid was tracked down. I mentioned that he seemed to be extremely braggadocious about these breaches. The more one struts around crowing, the more clues you inadvertently leave behind.

Mozilla says: No fair!

Mozilla 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 position. And that, as a result, for most people, this placement is sufficient and they will never see or pursue the extra steps necessary to discover alternatives. Right, one of my favorite observations: "The Tyranny of the Default."
https://research.mozilla.org/files/2022/09/Mozilla_Five-Walled-Gardens.pdf

The paper is titled: *"Five Walled Gardens: Why Browsers are Essential to the Internet and How Operating Systems are Holding Them Back."* It might have been titled: "Why Firefox is losing market share and it's no fair."

Now, I know that doesn't make me seem very sympathetic. But I actually am. I love Firefox. 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 would be greatly enhanced if I were using them to view this page.

Mozilla's 66-page paper amounts to them making an absolutely compelling case for exactly how screwed they are going forward. They blame the OS vendors for putting their own self interest first. Welcome to America.

It's unclear to me what this is 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 really is — does appear to be paving the ground for something. Google is currently funding Mozilla to the tune of $450 million per year in return for Firefox defaulting to Google as its search engine. There's the Tyranny of the Default for you, again... Though this time working in Firefox's favor.

On December 27th, 2011 Wired Magazine published: *"Why Google Continues to Fund Firefox"* with the sub-head: *"Google has its own web browser, so why is the company renewing its revenue deal with Mozilla? The answer is simple: Google makes money by putting eyeballs in front of ads and almost a quarter of the web's eyeballs use Firefox."* That's decidedly no longer true. The 2022 market share for the top four browser is:

Google Chrome	77.03%
Safari	8.87%
Mozilla Firefox	7.69%
Microsoft Edge	5.83%

Safari's edge thanks to the gazillion iPhones and iPads since the macOS would not be making a huge dent. But bless its little digital heart, Firefox is hanging in there at #3, still nicely and somewhat amazingly edging out Edge by nearly 2 percentage points.

It's unclear what Firefox's future is. But it's also unclear what good will come from complaining about it.

Vivaldi, Manifest V3, webRequest, and ad blockers

Back in November of 2020, Google announced what they called "Manifest V3" and we talked about it at the time. The concern was the deleterious effect that it would have on Ad Blockers, which came as no surprise to Google critics.

If you recall from two years ago, Google is changing the way Chrome's extensions function. Rather than allowing individual extensions to receive, examine and either drop or forward each of the browser's outgoing requests, as has always been allowed, under Manifest V3 there's a new *"declarativeNetRequest"* API (as it's called) which allows extensions modify and block network requests in what Google calls a privacy-preserving and performant way. What this actually means is that Google remains in control. What occurs under Manifest V3 is:

- Rather than intercepting a request and modifying it procedurally, the extension asks Chrome to evaluate and modify requests on its behalf.

- The extension declares a set of rules: patterns to match requests and actions to perform when matched. The browser then modifies network requests as defined by these rules.

Google claims that: *"Using this declarative approach dramatically reduces the need for persistent host permissions."* And I'm sure that's true. 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.

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] Vivaldi's Ad blocking would continue to be effective even in the face of Manifest 3. In his Friday post, 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. Perhaps, wise to move away from Chrome?*
>
> *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.*
>
> *Our mission will always be to ensure that you have the choice.*

Julian notes that the entire existing V2 API continues to be present for their 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 is my default URL handler, I often use Chrome for ad-hoc Internet research. And things have grown so horrendous on the Net that I could not live without an ad blocker. If Chrome really does become the advertising browser and takes away the ability to suppress the insanity that too many pages have become, they might see a move to Firefox.

https://vivaldi.com/blog/manifest-v3-webrequest-and-ad-blockers/

Sticky Chrome vulnerabilities:
And while we're on the topic of Chrome, A group known as Numen Cyber Labs have published write-ups on a pair of older and long since fixed Chrome vulnerabilities: CVE-2021–38003 and CVE-2022–1364. Both were Chrome 0-days patched in October 2021 and April 2022. And either one could be used for remote code execution attacks against Chrome users. What's interesting and chilling about Numen's observation is that they warns that even though these two security flaws have been patched in the main 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 the likes of Skype and many crypto-wallets.

I thought that was a fascinating observation, and one that we never consider. I often talk glowingly about how the Chromium guys jumped on a report of a new 0-day and pushed out an update after only a day or two. But applications that incorporate Chrome's WebKit engine are taking a snapshot of the engine and may be far more lackadaisical about keeping it up to date. After all, the Chromium engine 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 only because one of their component dependencies was updated. It's unlikely in the extreme. So any and all of such applications might well be inheriting and existing with Chrome's historical vulnerabilities.

SMB authentication rate limiter now on by default in Windows Insider

We all know that I'm not a big fan of Windows 11. That's mostly because of the lies we were told about its hardware system requirements, which never made any engineering sense and which, sure enough, were eventually acknowledged to be untrue. It's still unclear whether I'll be forced to move up from Windows 10 or whether Microsoft will eventually take no for an answer. We'll see, because much as I complained about Win10, I eventually made peace with it. But Windows 11 still looks like a move in the wrong direction.

But in at least one instance it's not. Believe it or not, Microsoft will finally, at long long last, be adding default brute force protection into Win11's notoriously insecure SMB file and printer sharing user authentication. Called the SMB authentication rate limiter, it's currently being tested by Insider builds. As its name suggests, this new feature will significantly rate-limit brute-force attacks against a Windows 11's SMB service. So anyone who either deliberately or inadvertently exposes their SMB service on port 445 to the public Internet 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 2-second default delay after each failed inbound NTLM authentication attempt. This means that if an attacker previously sent 300 brute force attempts per second from a client for 5 minutes — thus 90,000 username & password guesses — the same number of attempts would now take 50 hours. It's 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.

US bill to secure FOSS software

Two US senators, Rob Portman (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 Securing Open Source Software Act (which would make it the SOS Software Act). The goal is to help protect federal and critical infrastructure systems by strengthening the security of open source software. The legislation comes after a hearing convened by Portman and Peters on the Log4j incident earlier this year, and would direct the Cybersecurity and Infrastructure Security Agency (CISA) to help ensure that open source software is used safely and securely by the federal government, critical infrastructure, and others.

The SOS Software Act directs CISA to develop a risk framework to evaluate how open source 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 developing open source software to ensure that government and the community work hand-in-hand and are prepared to address incidents like the Log4j vulnerability. Additionally, the legislation requires the Office of Management and Budget (OMB) to issue guidance to federal agencies on the secure usage of open source software and establishes a software security subcommittee on the CISA Cybersecurity Advisory Committee.

I have a healthy skepticism of bureaucracy and legislators. It's unclear to me that they ever get anything right. But if the Federal government wants to hire a bunch of open source software folks who have been working for free to help in any way they can, it's unclear how that could do anything but help.

Iran vs Albania

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 Iranian's? 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 US 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.

CVE-2019-0604 has been classified by cybersecurity agencies as one of the most exploited bugs throughout 2020, having been abused by both nation-states and ransomware gangs. 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 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 the MEK. Albania has allowed about 3,000 members of the group to settle near Durres, the country's main port. The agencies said that in July 2022, the hackers "launched ransomware on the networks, leaving an anti-MEK message on desktops."

So we have a perfect instance 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 intrusion is every bit as crucial as attempting to keep the bad guys out in the first place.

Closing The Loop

After hearing last week's discussion of the UBER attack which was effective even in the presence of multi-factor authentication, a well-known contributor to our newsgroups posted his thoughts into our "Security Now" newsgroup. His handle is "ferrix" 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 an "MFA fatigue" attack. And I think that they and Greg are correct. So, here's how Greg explained what happened with the Uber contractor:

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 OTP as Steve said, then what he said about brute forcing codes would also have been correct. An attacker could have in theory brute-force logon attempts with codes 000000, 000001, 000002, etc. until matching the correct 6 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.

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 in to 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 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. 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, before even thinking. Or they might see the repeated attack push requests as "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 work day or after lunch. There is a normal 'background radiation' 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 (as far as I can tell) what happened to the Uber external staffer.

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 onto X? Click the matching challenge" Then shows 4 or 5 multiple choice buttons. It's not possible for the user to blindly approve any more, 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.

Orthogonally, please note that the above discussion does not contemplate MiTM 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 properly-implemented FIDO2 (or notionally, SQRL)

Sci-Fi Discovery

I'm now on Book #8 of The Silver Ships, and all I'll say is that anyone who enjoys science fiction stories has many wonderfully 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.

SpinRite

Despite the fact that I've admittedly fallen head over heels for a 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 awhile now, and I have one last known cosmetic thing to fix. It involves the mapping of SpinRites' huge 16 megabyte data transfer blocks to one of SpinRite's screens, its so-called Graphic Status Display (or GSD). Originally, a single transfer block might occupy more than one character cell in the GSD. But today's drives are so massive that many many data transfer blocks will be sharing a single GSD cell. So I removed the logic for managing the cross-cell mapping which simplified and sped-up SpinRite's inner loop. But that also meant that for the first time, on very small drives, since SpinRite's new data transfer blocks are so large, not all of the GSD screen might be used. So I'm fixing the case where that might happen. I'll likely finish that work tonight.

At that point, I won't know why SpinRite is not finished. But neither will I know that it is. So the last thing I will do before I turn the GRC newsgroup 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 in the right place. If anything doesn't work, I'll fix it, then SpinRite will be ready for the group's final external testing.

DarkNet Politics

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 LockBit3.0 ransomware led to some very interesting discussion and conjecture by the industry's ransomware-watching security researchers.

After the fall of Conti, Lockbit3.0 has risen to become the number one ransomware group in the ransomware industry. And they've been making something of a splash in the underground. They recently offered $1000 to anyone who would permanently tattoo their group's logo on their body. And they had a number of takers until they terminated the offer. Today, the group's operations are so extensive that Lockbit's victim count during some weeks has been greater than all 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 — if you can call it that — has been booming for the LockBit3.0 group, things were recently shaken up 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 module — 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 triggered Conti's downfall, it raises the question whether this may be the beginning of the end for Lockbit, as well.

So, a threat actor going by the name Ali Quashji (a Twitter account with no reputation apparently created just for this leak) claims to have hacked several of LockBit's servers and was able to obtain the LockBit3.0 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."*

"The Record", a publication of Recorded Future, often does a great job of pulling things together and polling security researchers. In this instance I thought that some of what they reported was really quite interesting. 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 3xp0rt (whom I'm call "Export"). Several experts and researchers confirmed to The Record that the builder works and 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, they would hope that's true.

A LockBit representative said: *"An affiliate program is not a locker, it is a software package, and most importantly an impeccable reputation that no one can tarnish, no matter what software leaks occur. Few people will agree to pay randomly to a pentester without a reputation, hoping for a successful decryption and deletion of stolen data."*

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. And the reputations of underground criminals has little bearing on whether they get paid. They get paid if there's no alternative, period.

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.

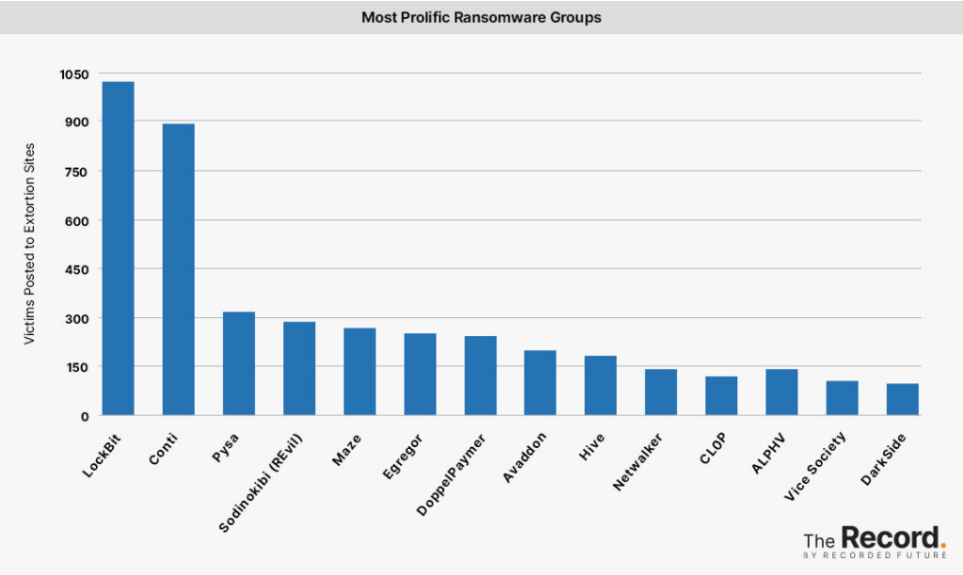
And Recorded Future's own ransomware expert Allan Liska said his team has identified more than 150 "new" ransomware groups just this year, most of them are using stolen Conti or REvil code. Allan said: *"At this time last year, Recorded Future was collecting from about 45 active DLS — meaning Dedicated 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 — is so disturbing. The emergence of turnkey services allows those who are not skilled enough to assemble the required infrastructure 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 is 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."*

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 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 last month in August, including a crippling attack on a hospital about an hour southeast of Paris that disrupted its medical imaging, patient admissions, and other services.

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 Lab's John Hammond explained that the latest edition of LockBit had new features and functionality to encrypt files faster than 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.



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 – note how the ransom note can be completely changed."*

One small upside of the leak may be that security experts can now 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 from insider threats.

Recorded Future's Allan Liska said the leak could be a sign of disgruntled factions within the LockBit group. *"These large RaaS groups are notorious for paying their developers, IABs [Initial Access Brokers] and other support staff very poorly..."* So, it's not necessarily a surprise when someone retaliates.

John Hammond 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, it enables anyone to run the racket,"* he said.

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 it. 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 is that, driven by the promise of easy money, what was once a somewhat blessedly high-level and higher-end form of devastating attack is rapidly moving down into and becoming a commodity available to far lesser capable criminals to use.

Again, in retrospect, this was all inevitable. The lack of true bullet-proof enterprise cybersecurity, which enables an environment of porous security, with the emergence of cryptocurrency, which solved the extortion payment problem, 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.