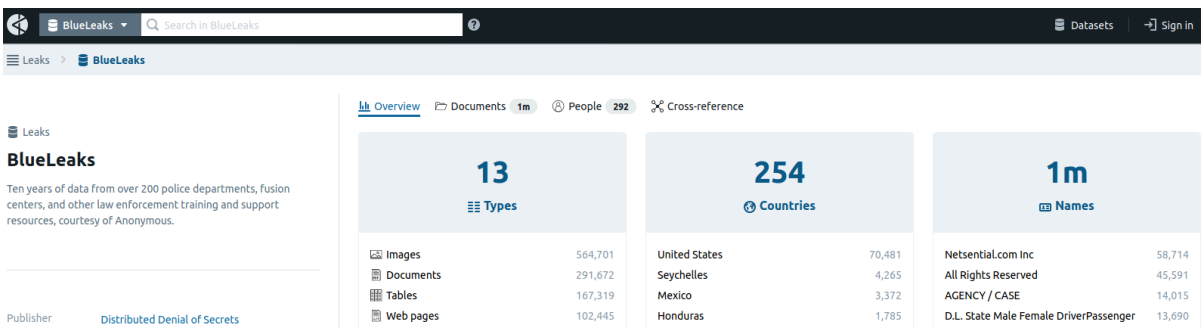
'BlueLeaks' Exposes Files from Hundreds of Police Departments

June 22, 2020 122 Comments

Hundreds of thousands of potentially sensitive files from police departments across the United States were leaked online last week. The collection, dubbed "**BlueLeaks**" and made searchable online, stems from a security breach at a Texas web design and hosting company that maintains a number of state law enforcement data-sharing portals.

The collection — nearly 270 gigabytes in total — is the latest release from **Distributed Denial of Secrets** (DDoSecrets), an alternative to Wikileaks that publishes caches of previously secret data.



A partial screenshot of the BlueLeaks data cache.

In a post on Twitter, DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

Fusion centers are state-owned and operated entities that gather and disseminate law enforcement and public safety information between state, local, tribal and territorial, federal and private sector partners.

KrebsOnSecurity obtained an internal June 20 analysis by the **National Fusion Center Association** (NFCA), which confirmed the validity of the leaked data. The NFCA alert noted that the dates of the files in the leak actually span nearly 24 years — from August 1996 through June 19, 2020 — and that the documents include names, email addresses, phone numbers, PDF documents, images, and a large number of text, video, CSV and ZIP files.

"Additionally, the data dump contains emails and associated attachments," the alert reads. "Our initial analysis revealed that some of these files contain highly sensitive information such as ACH routing numbers, international bank account numbers (IBANs), and other financial data as well as personally identifiable information (PII) and images of suspects listed in Requests for Information (RFIs) and other law enforcement and government agency reports."

(U//FOUO) Data Breach Impacts Some US Fusion Centers and Associated Agencies

The NFCA said it appears the data published by BlueLeaks was taken after a security breach at Netsential, a Houston-based web development firm.

"Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise," the NFCA wrote. "Netsential confirmed that this compromise was likely the result of a threat actor who leveraged a compromised Netsential customer user account and the web platform's upload feature to introduce malicious content, allowing for the exfiltration of other Netsential customer data."

Reached via phone Sunday evening, Netsential Director **Stephen Gartrell** declined to comment for this story.

The NFCA said a variety of cyber threat actors, including nation-states, hacktivists, and financially-motivated cybercriminals, might seek to exploit the data exposed in this breach to

target fusion centers and associated agencies and their personnel in various cyber attacks and campaigns.

The BlueLeaks data set was released June 19, also known as "Juneteenth," the oldest nationally celebrated commemoration of the ending of slavery in the United States. This year's observance of the date has generated renewed public interest in the wake of widespread protests against police brutality and the filmed killing of George Floyd at the hands of Minneapolis police.

Stewart Baker, an attorney at the Washington, D.C. office of **Steptoe & Johnson LLP** and a former assistant secretary of policy at the **U.S. Department of Homeland Security**, said the BlueLeaks data is unlikely to shed much light on police misconduct, but could expose sensitive law enforcement investigations and even endanger lives.

"With this volume of material, there are bound to be compromises of sensitive operations and maybe even human sources or undercover police, so I fear it will put lives at risk," Baker said. "Every organized crime operation in the country will likely have searched for their own names before law enforcement knows what's in the files, so the damage could be done quickly. I'd also be surprised if the files produce much scandal or evidence of police misconduct. That's not the kind of work the fusion centers do."

This entry was posted on Monday 22nd of June 2020 12:33 AM

DATA BREACHES | THE COMING STORM

BLUELEAKS | DISTRIBUTED DENIAL OF SECRETS | JUNETEETH | NATIONAL FUSION CENTER ASSOCIATION | NETSENTIAL | STEPHEN GATRELL | STEPTOE & JOHNSON | STEWART BAKER

122 thoughts on "'BlueLeaks' Exposes Files from Hundreds of Police Departments"

The Sunshine State

June 22, 2020

Good article

DelilahtheSober

June 22, 2020

Thank you Brian I learn so much from you

The Fed

June 22, 2020

Oh My God. This is really bad.

Prez Camacho

-

June 22, 2020

Only if there is something to hide right?!?

Zedd

-

June 22, 2020

That’s not why it’s bad. This is now a blueprint for just about anything stored with this method to be hacked. From private to personal to government. Anything stored in this system is now endangered. Not just what was stolen this time

Zaq

-

June 22, 2020

Security through obscurity is not secure.

pic

-

June 22, 2020

well… Technically it is, until it isn’t.

- Zendo Deb

-

June 22, 2020

No. Not even “technically.” Everything that has been “secured” by obscurity in the past 25 years has been hacked everything.

Programmers – probably at the behest of support managers – put “hidden” back doors into a lot of routers and other bits of networking equipment. Everything that the managers were “sure was fine,” was not fine. “How is a hacker going to find that?” They found it.

Something is ONLY secure if it is secure behind a strong cryptographic cypher. If you think anything else is secure, then you should not be allowed within 10 feet of a computer that contains sensitive information.

Michael

-

June 23, 2020

Well, actually, technically, all modern encryption relies on security through obscurity. After all, that is exactly what a hidden key is. What distinguishes these methods is the precision of the obfuscation.

- David Robinson

-

June 23, 2020

In modern encryption, obscurity is not the magic sauce — probability is. The mathematics allows precise calculation of the strength of the security and allows it to be optimized as

needed. A key is not really hidden — it is available to anyone with the resources to compute it, though that might take until after the heat death of the universe. This is a different order of secret from what people mean by obscurity, e.g., telnet back doors on silly ports, that sort of thing. Those tactics are regularly defeated by persistent idiots.

Andrew

-

June 23, 2020

Security through obscurity is literally a famcy way of saying cryptography. Literally just mathematical obfuscation. Anything in this world can be hacked no matter how secure anything can be broken with enough hands and computational power. Whether stealth or brute force. Nothing is actually secure in this world on the internet. To believe it is secure in anyway? Now that is just tragic folly and you need to go back to college.

needmorename

-

June 23, 2020

Literally no one but yourself takes that view.

SeymourB

-

June 30, 2020

Security through obscurity is a telnet server running on a custom port with full root access to the device without authentication.

Security through obscurity is allowing unauthenticated access to administrative features by simply tacking a path name and/or page name onto an existing http/https connection in a web browser.

There are many ways to illustrate security through obscurity, but none of them follow established best security practices – which your odd definition would include.

security vet

-

June 23, 2020

…the key is not hidden at all – it's in the table sized 2^n where n is the number of keys in say AES 256 – 2^256 (minus a few "easy keys)…

…what's hidden is your choice of a key (by algorithm normally)…

…in other words the key is deterministic – it can be "guessed", that's how you "grind" the solution…

…so yes, it's "security through obscurity"…

Slag

-

June 23, 2020

Security includes a MTBF number based on how long it takes to be overcome. All locks, all doors, all cryptographic keys include this number which allows the judgment of risk vs effort. If you don't have a way to tell how long it will take someone to break your security, you don't have security you have whistling in the dark.

security vet

-

June 23, 2020

Slag:

…actually it's not called mtbf in security, but it works more or less the same…

„„if how long you want to protect the data (your bank account, for example) is longer than the time it takes to "crack" the data then the control is no good…single DES, for example…

…the control in this case being encryption…

security vet

-

June 23, 2020

…the point of encryption as a control is to try and raise the work factor for the adversary so that they don't bother with you or they have to spend so much it's impossible…

…so yes, security through obscurity (the cost exceeds the benefit)…

- Steve

-

June 25, 2020

@Camacho

Yeah…nothing to hide…you've just blown my mind and came up with a great reason to make the encrypted and secret data of every organization and individual in the world public. Nobody would take advantage of that.. right? How about you post all your bank account info, loan info, SSN, CC, health information and everything else in the open on facebook. I mean, you've got nothing to hide right? And I'm sure everyone you know would be thrilled if you hacked them and posted all their data.

eyes rolling

Bill Baxton

-

June 23, 2020

Why? Are you a snitch?

RationalFactualObjectiveLogical

June 22, 2020

This is another act that points to a fundamental problem with U.S. society: millions of people with no vocation or avocation through which to channel their energy. Hobbies, safe free-time pursuits are now only enjoyed by "old people." There are millions of people with

nothing to do, people who are bored, spending their days getting into trouble on-line or meddling in the affairs of others who are minding their own business.

QuestioningEyefortheOldGuy

-

June 22, 2020

Is that what you think these kids are doing with their Xboxes and TikToks? None of what you just said makes sense. We have tons of free time but only old people use it wisely. Please.

ThanksForTheCrapReality

-

June 22, 2020

Kids play video games and stage crap on TikTok as an escape from the crap reality they live in. Imagine being born into a world where the elderly have brazenly left your generation with a dysfunctional environment and hoard the wealth required to fix it.

Thing is, the very same elderly lack the imagination to be able to do that, so they just see a bunch of lazy kids. It's a damnable existence.

Vollinger

-

June 22, 2020

Sounds like something you yelled at your mom before storming up the stairs and slamming the door.

Tom

-

June 22, 2020

I second your opinion

RealVollinger

-

June 22, 2020

Its important to characterize your opponents as children to avoid addressing any of the valid points they make. Very smart! Everyone agrees that you're the most intelligent person here. Great job!

Bob

-

June 22, 2020

The important thing is that you managed to avoid any self-reflection whatsoever.

Frank

-

June 22, 2020

the important thing is that your face is dumb

Bob

-

June 23, 2020

umad

davelog

-

June 22, 2020

Hi, welcome to the generational cycle. This is nothing new, it’s just your turn. You’ll be at the other end of it in a few years as well.

- justshutuppls

-

June 22, 2020

srop with this bull. we need change.

Doar Zevel

-

June 22, 2020

If you want change, try looking in your mom’s sofa.

Or you could GET A JOB!

Zach

-

June 22, 2020

OK boomer

- Alan

-

June 25, 2020

Ouch! You got me! I’m older, more experienced, more educated, and more financially and emotionally stable due to decades of experience and work. If you need any help I’m available. I would suggest that the best way to deal yourself out of all the GOOD torches that are being handed off from my generation to yours is to express sentiments like “OK Boomer”.

Lame

-

June 28, 2020

I think you just proved his point. In fact, you just made clear to me, that humans having limited life spans is a good thing.

Belle Delphine

-

June 28, 2020

Even if everything you said is true, you're still probably dumb enough to believe that coronavirus is a chinese hoax or that the russians hacked voting machines in 2016

Dan

-

July 20, 2020

Ok boomer

John

-

June 22, 2020

Your type needing change is what got us to where we are now. Quit whining and getting offended at everything you hear and see. Grow a pair!! Do you know what that means?

Bob

-

June 23, 2020

Does it mean pretending that the boomers aren't doubling down on increasing catastrophic global warming with their dying breaths?

John

-

June 22, 2020

Couldn't be farther from the truth. Lol. The older generation actually does things for theirselves. We don't have time to be sitting around on our butts dreaming up ways to mess others lives up. We actually have lives.

Ayy

-

June 23, 2020

Older generation does things, like shift all responsibility and consequences of their actions onto the younger generations. A never-ending war on terror started by boomer lies? Must be young people's fault. MULTIPLE economic crashes in our lifetime, with huge corporations and wall street getting shielded from damage and responsibility? Must have been those dang youngsters, you know, the ones either too young or barely getting into the world when this stuff was happening (i.e. impossible for it to be caused by anyone but you fucking boomers). A delusional worshipping of objectively bad and morally empty presidents like Reagan? Yup, that must be the youngsters. You're an idiot that can't open your eyes and see what your generation has actually done. You've built your success on the backs of the exploited, and saved yourselves by building a national debt to compensate for your absolutely terrible monetary policies that encourage selfish behavior. The world will literally be better when you're dead.

Prec

-

June 24, 2020

That was the yuppies, the boomers loved Carter

- Alan

-

June 25, 2020

“The world will be better off when you’re dead.” We all die Ayy. You shouldn’t work so hard on it being a better place when YOU die. You will inherit the single most free and wealthy country in the world. Hell, we owe like 60% of that national debt to ourselves.
Who’s gonna foreclose? Perfect? Hell no. We e haven’t given up yetbut it’s time to start passing s the torch tyou and yours. I for onewe wish you all the bestYou’ll have your own unique perspective on unique problems and you’ll porbably look at your current self with a certain amount of disdain in about 20 years. Based on experience you clearly have yet to achieve, wishing others dead is absolutely the best way to deal yourself out of the future that’s being handed off. It’s certainly s going to take a lot more tcreate a future than n physically threatening and nihilistic smart-ass response. But, should you feel like addressing yourself to making the world “better” in that way… bring it. ‘d say odds are I would die better than you.I.”

- steve

-

June 25, 2020

Or…maybe they’ve read enough to know that IPCC, NASA and NOAA, University of east Anglia etc… ALL can’t even model clouds yet. They’ve NEVER been able too. It’s all nonsense without a model that includes accurate cloud data. Ever wonder why so many dire predictions failed? What worries me is the soon to shift magnetic pole and the giant bulge of water at the equator.

John Links

-

June 22, 2020

Yeah, pretty much is what it means. The younger generation doesn’t have just a lot of snap.

Bob Brown

-

June 22, 2020

Dunno about other old folks, but I’m working on an open access (i.e. free) computing textbook. Turns out I have to do all the diagrams in Adobe Illustrator, which I haven’t used before. There’s certainly no spare time for mischief.

Tyler

-

June 22, 2020

Bob, not that it solves the issues of needing to learn a new piece of software, but there are open source (in your words, free 🙂 alternatives like GIMP or LibreOffice's Draw that can be used as an alternative to Adobe's Illustrator. Draw might be better if you're creating diagrams and flow charts, as GIMP is more comparable to something like Adobe's PhotoShop than it is Illustrator. Just an FYI in case you get sick of paying Adobe's ridiculous subscription fees!

In regards to the article, KoS is one of the best resources in modern times. Thank you for always providing well-written, properly-researched articles.

If you leave a bag of chips open on the ground, humans and critters alike will take as they please. If you leave a bank safe full of cash open and unguarded, only people will take it. Information is as good as cash to both good and evil nowadays, so if you are taking a position to keep sensitive data like medical records, police records, credit records, etc., and have the gall to charge money for it, you better be sure your locks are locked tight. Thanks again for the interesting article.

FrankHarv

-

June 22, 2020

Bob, Please checkout Inkscape for open source AI alternative. GIMP is more graphics centric.
Inkscape is line art compatible.
inkscape.org

Buck Rogers

-

June 22, 2020

It doesn't matter what others have said about "OPEN SOURCE" (I'm also an OpenSource user). THERE IS NOTHING IN THIS OPENSOURCE WORLD THAT CLOSE TO ADOBE … This company is BEYOND everything you and me knows … not even GIMP or InkSpace … not even close to ADOBE.

Eric B.

-

June 22, 2020

A fundamental problem with our society is the racist behavior displayed by many members of our police departments. One political party in particular doesn't seem very interested in reform.

Get a hobby and mind your own business is not a solution for systemic issues of public interest.

A particular group of folks decided to expose the secrets. I, for one, am interested to see what has been hidden for all these years. Have my local police officers been accused of crimes and not charged? How? Why?

Brian Fiori (AKA The Dean)

-

June 22, 2020

Did you actually READ the article? There is likely very little of the kind of information to which you refer in this database.

Eyestrike11

-

June 22, 2020

The statement about the info “not shedding light on police misconduct” and exposing sensitive law enforcement info and even endangering lives was made by a former secretary of Homeland Security. How could the information NOT shed light on police misconduct? You may believe him if you wish. I do not.

- Alan

-

June 25, 2020

Dude…it’s a FUSION database. Interagency crap. You think they’re gonna do COOP work on their dirty laundry? You make your paranoia appear to significantly exceed both your intelligence and your education on general data usage. It most likely wasn’t extremely well secured for good reason. It could even be a DISinformation database. From the point of view of a professional data analyst, his sounds like some low hanging frui to met.

Eyestrike11

-

June 22, 2020

So you believe a former Secretary of Department of Homeland Security? Do you think he has had time to sift through the information?

Brian Fiori (AKA The Dean)

-

June 22, 2020

It’s not as if I’m taking his word as gospel. But it seems rather unlikely that a database like this would contain the kind of information that would be damning to police officers. Now had they gotten into the local and email servers of precincts, then I think there would be a trove of interesting data.

Doubtist

-

June 24, 2020

I would say you’re right that it’s not organized into a format that readily exposes police misconduct because it’s really not specific to that in any way. There may be some misconduct exposed, but it would be along with the entire rest of the data. The exposure would be unlikely to lead to a legally prosecutable outcome in any case of misconduct

however, and the damage to the investigations and cases and systems really could destroy a lot more than anyone has any real reckoning of.

These centers and systems are basically distributed everywhere with specific static oversight regimes in place that have no budget or impetus to improve/redevelop their security methodology and are going to be wide open ongoing to foreign actors and criminal groups alike, and so this problem is going to be exploited in various ways for the foreseeable future. Police reform groups aren't going to be the ones reaping positive results of this, even if a few instances of misconduct are exposed. It just muddies them. This isn't legally presentable evidence and without the pedigree of the chain of custody, anything exposed will be useless to just about any conceivable court process or legal outcome.

Jeff Strubberg

-

June 22, 2020

There is zero "racial justice" data here. This is retribution, plain and simple.

Come to think of it, that applies to most of what we see happening today around this issue…

JSeattle

-

June 22, 2020

I'm all for exposing the misconduct of our police, but unfortunately, most of the really sensitive data is likely to belong to suspects and victims. I'm talking full names, SSNs, DL#s, license plates, home/work addresses, and financial information; not to mention incident reports which may detail what could be the worst days in many of their lives.

So thanks a lot to whoever leaked this for exposing these folks to more suffering. Nice job supporting the movement.

Phil

-

June 22, 2020

I bet the hacker didn't take the time to really understand what they got, being too busy congratulating themselves on having gotten access to anything from the police

No doubt organized crime will download the entire dataset in the expectation that it will get taken down soon, then sift through it

Jonathan

-

June 24, 2020

It seems likely that the person who leaked this information was motivated so heavily by animus that understanding .

There's a lot of that going around — there are some emotionally charged issues out there. However, this is not a mature response. Yes, there are bad police officers out there, but the vast majority of them are great folks doing a tough job. If there is an onus on our police

officers to work harder to be more understanding of the public and its subcultures, the same onus applies to the public and those subcultures to participate in that process constructively.

Chip Douglas

-

June 22, 2020

S0, I guess you had a few minutes between protests and decided to share your wisdom with us. Thanks for nothing.

Nicholas

-

June 22, 2020

This is So stupid that I can only attribute what you just said to higher education. You had to have gone to college to be able to say something so ridiculously idiotic. I guess go back to your jacks and Lincoln logs you fucking mummy. Leaks like these leaks are not only wanted, but necessary. Don't be such a mindless bootlicker, it highlights how irrational you truly are.

Russ

-

June 24, 2020

Constructive things like playing Golf?

…or wasting countless hours on FB?

Don't worry, your parents said you as kids were lazy no accounts. So did their parents, and so on all the way back to the beginning of time. For the Christians out there, check Exodus 21:17. Talk about hating their kids!

Jim

June 22, 2020

Interesting. Good article. Shows a lack of security training. By security professionals. Just because you have a badge, does not mean you are secure. Just because you have information, should it be stored for distribution? Is there material that should not be released? Is security always good? Or can they be wrong every now and then. Love the irony of the subject.

Mikey Doesn't Like It

June 22, 2020

How ironic that, in a profile of DDoSecrets in Columbia Journalism Review (CJR), their one "public" person said:

Best cautions CJR that the group does not steal or solicit theft. "Our "Wanted" page lists only materials known to exist from preexisting breaches and leaks for this reason – there are ethical (not to mention legal) lines that would be crossed in soliciting or committing the actual theft of data." No one in the group, she says, has even suggested stealing or copying information in a way that would break the law.

Talk is cheap…

Jon Marcus

June 22, 2020

Very informative article. I'm not too surprised that the company responsible points the finger at a "compromised customer account" rather than system failure that allowed a customer account to exfiltrate 270GB of raw data.

But I do wish there had been a bit more discussion of the significance of the data. Stewart Baker (who was at the NSA before he served in the GW Bush administration) has always been an intellectual property and government power maximalist at the expense of other rights. Of course he'd claim there's nothing worth investigating in this breach. Perhaps what he says is true, but I'd find it more convincing if someone without Baker's biases actually looked at the data before announcing their certainty that facts will conform to their biases.

Chris C

-

June 22, 2020

Looks like they're trying to emphasize "Compromised account" rather than "was then able to upload documents triggering a complete breakdown of security".

That some account will be eventually compromised should be assumed. From a security perspective, even authenticated users are "untrustworty agents".

Also highlights that "hoarding information is a liability".

bennett

-

June 23, 2020

Sanitize data inputs folks

admin user

June 22, 2020

so if someone makes a comment on twitter they get banned, but exposing government secrets is not just tolerated but encouraged.

anything to make trump look bad…

Catwhisperer

-

June 22, 2020

No, he does a great job of buggering things up on his own…

The Best Coast

-

June 22, 2020

Oh come on… He does a mighty fine job of making himself look not just bad, but downright awful. And criminal.

Nick

-

June 22, 2020

Trump is a child rapist who makes himself look bad. Look at his pathetic rally in Tulsa. He's done.

Chip Douglas

-

June 22, 2020

Hold that thought.
Unless the dems put a hit on him he is going to be re-elected with probably a larger margin than the first time.

Matt

-

June 23, 2020

An even larger margin than before? So, what, -FIVE million votes?

Factchecker

-

June 23, 2020

Actually, the only child rapist out there are democrats… you know, the ones' who frequented old Epstein's island.. like Billy Clinton and his pals, and the Hollyweirdos who can't figure out their gender.

Mahhn

-

June 25, 2020

And Hilldogies #1 Mr Weiner sexting a child – - https://en.wikipedia.org/wiki/Anthony_Weiner#Sexting_scandals,_prosecution,_and_guilty_plea

- frank

-

June 22, 2020

yes, exposing criminal actions by our government is supposed to be celebrated as much as removing hate speech from Twitter. Good job, you noticed how evil those two things are

Ron G

June 22, 2020

So, the unsophisticated Ewoks prevail over the Empire.

There's always an unsecured exhaust port into which a carefully aimed proton torpedo will do maximal damage, if not to actual infrastructure, then at least to egos.

Whose bright idea was it to concentrate 270GB of LE-sensitive data in one place, unencrypted?

nazgulsenpai

-

June 22, 2020

This was my first thought. My only guess is that they might have had VPN tunnels or other remote access mechanisms into databases that feed their websites? You can go to their website and tell rather quickly that it would look at home on IE6@800×600, which might be just a microcosm of their old-school tendencies and perhaps lax security posture.

What's frightening to consider is how many more of these companies might exist, just waiting to be compromised.

SeymourB

-

June 30, 2020

If there's one thing that sharing office space with a company who was developing tech for the police sector, its that their target audience enjoyed incredibly fat budgets (everything they sold had crazy profit margins) and the market had no goddamn clue how anything worked.

Also, they were pretty technologically borderline too, I sighed every time they put another unsecured access point online within range of our space. The couple times I got curious it was attached to their corporate network.

Alan Hodgson

-

June 22, 2020

No one working there now probably even knew they had data from 1996 stored somewhere.

PhantomTramp

June 22, 2020

Stop feedin' them ol' trolls, they will only hang around, heh, heh.

An' get off my lawn..

The Tramp

Archimedes

-

June 24, 2020

Here here…. Get off my lawn. Brilliant.

evilpaul

June 22, 2020

"I'd also be surprised if the files produce much scandal or evidence of police misconduct." Well, I'd suggest the undercover, secret law enforcement do searches for their own names,

like all organized crime in the country purportedly have already done, and adjust accordingly. I'm interested to see what scandal and evidence of police misconduct the files produce every if it isn't "much."

Joe

-

June 22, 2020

For the 5% of "police misconduct" files that you can estimate, 90-95% of the rest of the files contain information about crime victims, human trafficking, murders, what happened during a crime, briefing of situation of events. So think about how much that small part means to you when the rest of the people who sought police services are now searchable by their contact information online.

It appears you can even find crimes against the elderly and children in this data.

Jewtopia

-

June 23, 2020

I went ahead and perused through some files here and there. A surprisingly high number of files are related to combating shoplifting, larceny and credit card fraud resulting in losses of $2k to $10k.

That's just what I have seen. I know there must be more interesting things lying about.

KeepResisting

June 22, 2020

The only way forward is continued resistance to tyranny. Any cop arresting anyone for violating an illegal State pandemic order (which includes any order which violates 18 USC 242) is committing a Federal felony, and if the cop harms the person who they are arresting, it carries a ten year prison sentence. A governor who orders nursing homes to abridge any US right protected by the Constitution, whose order leads to a single death in a single nursing home, can be handed a death penalty. These files will assist in proving these sorts of cases, and done properly, dozens of cops from every city in America will get years in Federal prison for enforcing blatantly unconstitutional orders.

Joe

-

June 22, 2020

Unfortunately, most people don't know what "color of law" is.

Spoiler, it doesn't mean what you think it means.

State laws have huge legal power, especially when emergencies are declared. Simply calling them "illegal" doesn't actually make them so. It isn't intuitive to the armchair protest person… but constitutional rights cannot protect you from state laws so easily.

Habeas corpus can routinely be suspended seemingly defiant of the constitution. Free speech and right to assemble doesn't guarantee anytime and anyplace.
Some states are going to interpret what they can or can't do… and there isn't much you or the federal government can do about it, other than bring it up to SCOTUS, who may not even see the case.

Joe

-

June 22, 2020

It sounds like you are one of those pseudo legal experts who think they are sovereign citizens.

- https://www.youtube.com/watch?v=4_kbkQipgJo

Jonathan

-

June 24, 2020

In every instance I can find where some government authority tried to suspend habeus corpus, the Supreme Court has ruled that attempt unconstitutional. I freely admit that I'm not an attorney or legal scholar and I may have missed some things.

Wrath of God

-

June 22, 2020

You are a real nut case.

Kent Brockman

June 22, 2020

"…so I fear it will put lives at risk".

Rather ironic given the current circumstances, no? What's needed is a "Blue Lives Matter" campaign. LMAO

Jose

-

June 22, 2020

There already is a campaign…it's called "Blue Lives Murder"

Chip Douglas

-

June 22, 2020

You mean black lives matter. There, fixed it for you.

kerberos_dc

June 22, 2020

How can Netsential be that secure when their website looks like it is straight from Geocities or Frontpage?

notaninja

-

June 24, 2020

Secure .. in fat cat contracts, maybe.

scratch scratch scratch

“Now do my back!”

JCitizen

June 22, 2020

It was bound to happen; the advantages of LE agencies to have access to centralized data is also the weakness of the system, it is just a fact.

I suppose June 19 celebrants may have some “fun” with this data.

- Milk

-

June 23, 2020

Sorry, for some reason i can’t change who I’m replying to but the fact of the matter is networking is a joke to half the old bags that make up companies. There’s a reason they all look like they’re from 1998, because they might as well be. Millions and millions and millions of computers at these places still run windows xp. Let alone earlier operating systems. This is their own fault for being unwilling to get with the times and stay up to date with security. It’s not in their budget ♀

biff_tyfsok

June 22, 2020

The part of this I can’t get over is…Dun & Bradstreet’s report on Netsential (the company that was hacked) says they have “5 total employees across all of its locations and generates $420,320 in sales”.

What I want to know is: why is a rinky-dink 5-man Houston shop hosting all this sensitive information? Who was auditing their security? It makes perfect sense to lean on a managed service provider, but this probably shouldn’t have gone to the lowest bidder ya know?

Mikey Doesn't Like It

-

June 22, 2020

@biff_tyfsok

It’s quite simple, really. Many departments don’t have the IT budgets or resources to manage all their data, so they outsource it. Unfortunately, they often don’t appear to do due diligence first, to verify an outside company’s capabilities, security, etc.

What’s been glossed over by most of the political (and irrelevant) posts here is what a few people have picked up on: the information is far more likely to affect crime victims’ data and privacy and potentially compromise investigations. That’s serious.

(For the record, I support reforms in policing — but this isn't the place for that discussion. Let's show Brian and his work the respect he richly deserves by staying on topic.)

Steve

-

June 22, 2020

A most excellent comment. I wholeheartedly agree. Your parenthetical closing remark is right on the mark!

Duke

-

June 23, 2020

This comment is spot on. Our company provides IT services to small police departments in our region.Several of these departments use Windows software that stores lots of sensitive information including personal details of crime victims. The software company came out with a mobile app that allows officers to access this data on their phones. The owner of the software told me "You need to open a port on the firewall to allow our app to access the server." I gave them a big NOPE.

The guy went ballistic and threatened legal action against our company for interfering with his business. I told the vendor: My advice to the decision makers is NOT to allow your app to access this data. If the Chief of Police sends me a written directive that acknowledges our advice and they want the port open anyway, we will certainly do so.

Never heard from him again.

But I'm sure that there are IT companies supporting his other customers that said "the port is open."

J

June 22, 2020

https://patents.google.com/patent/US20030033378A1/en

Inventor
Fred Needham
Stephen Gartrell
Current Assignee
NETSENTIALCOM Inc

Method and apparatus for automatically creating and dynamically managing websites
Abstract
A system for creating and dynamically managing websites includes a set of tables; a database associated with the set of tables; and a software tool for generating a web interface based on the database using the set of tables. A method for creating and dynamically managing websites includes creating a set of tables associated with a database; and generating a web interface based on the database using the set of tables.

Chris C

-

June 24, 2020

You missed the part about ensuring SQLi injection attack vectors are ignored, Mr '–; Bobby Tables

Greg

June 22, 2020

This sickens me. It's about time that the current version of the net become less inter. This mess needs to be throttled back. I really don't like the idea that any crook, any where, ANY, is only a few keystrokes away from my personal information, and now, what could be my Most Personal information. Those guys can never be beat, face it. I'd like to see dialog on what needs to be done to lock down the 'conditional intranets' that need to be created. Yes, the future 'net has to lose some functionality in order to survive. IT guys! Open your minds and get started!

- Milk

-

June 23, 2020

No. If you're worried about 'crooks' being 'a few keystrokes' away from your personal information then you need to secure your information or don't put it on the internet. It's that simple. The internet is free. You're not going to restrict it just because you refuse to educate yourself on how to be safe and secure on it.

Greg

-

June 27, 2020

I am not worried about MY data. My records are already an open book, effectively. So, you missed my point.

bill

June 22, 2020

Great work as always, Brian – have you written what someone can do when the person who manages their website drops out of contact ?

Is it possible to get it back ? What steps can we try to find and get the data and get it back online? (legally, of course)

I'd love to hear any suggestions…

That guy

June 23, 2020

Like the a holes we see looting and burning, now they released people's personal information to the public. What a bunch of righteous social justice warriors. Fighting crime with crime. Lol. They're worse than the police.

Ted wright

June 23, 2020

When will the powers that be learn!! You cant put sensitive info on computer files. You have to do it the old fashioned way paper files and micro fish. Yes it takes up room and takes longer to access and disseminate info. But it is hack proof.

PM

-

June 23, 2020

Would you kindly elaborate on how these tiny swimming creatures are more secure than digital cryptography?

Turkish

June 23, 2020

Haha classic. And I think that for blueleaks in our ecosystem utopia appeared

Curley B Gaston

June 23, 2020

Mary had a little LAMB
its FLEECE was white as SNOW
and everwhere that MARY went
the LAMB was sure to go.

Figure that out and you have your answer.

- Rizal Jose

-

June 23, 2020

Excellent !! Wrote it down.

J

-

June 23, 2020

Mhall,ifwwas.AetMw,tlws2g.

Flap Doggerel

June 23, 2020

“I’ve been active in trying to get people to register to vote. People who don’t vote are deadbeats on the state. I figure a man needs to do his own thinking. What happened to us last night can happen to anyone, white or black. At one time I didn’t think so, but I have changed my mind.”
-Vernon Dahmer

FrankfromBrooklyn

-

June 25, 2020

Thanks for that. I'd never heard of Mister Dahmer.

ACAB2020

June 24, 2020

If the cops aren't doing anything wrong or illegal they have nothing to worry about. They are public servants. Check it out for yourself…

https://hunter.ddosecrets.com/datasets/102

- Alan

-

June 25, 2020

That's ingenious. We should post all the data because "if they aren't doing anything wrong they have nothing to worry about". You first. Go ahead and post all your private medical, financial, and personal info online. Do the same to all your friends, they'll still be your friends because they aren't doing anything wrong and they have nothing to worry about.

No way anybody would abuse access to informationright? S

eems to me that, short of an altogether excessively simplistic world view, this article is a prime exampe of someone that abused access to information in order to make certain those that would abuse information would have access to it. I guess its easy to have that point of view in the Cocoon of safety you've enjoyed because of law enforcement efforts. Good luck when it's gone.

JimB

June 24, 2020

Zoominfo says Netsential.com is a Texas small business with 39 people and $8M/year in revenue that provides website programming and states on their website that "The software is browser based – Anyone on your staff can make updates". Very low tech, how much do you want to be they don't have any cybersecurity professionals on staff? Chances are they didn't even know what they didn't know about security vulnerabilities. Government funded fusion centers should know better than to hire hayseeds like this without checking their credentials and requiring regular penetration testing.

Lame

June 28, 2020

Total amateur hour. Then, trying to blame the hackers for putting lives at risk? Puh-lease. These are the same idiots that want to put back doors into mobile devices to "save the children."

CryptoTapas

July 14, 2020

I am not sure which is worse? the information revealed or the fact that many unassuming people’s data has been made public left to exploit!

globaltel

July 14, 2020

Only temporary SSN’s, which of course would be mathematically linked to the real Id values.

Comments are closed.