Security Now! #1012 - 02-11-25

Hiding School Cyberattacks

This week on Security Now!

New "SparkCat" secret-stealing AI image scanner discovered in App and Play stores. The UK demands that Apple does the impossible: decrypting ADP cloud data. France moves forward on legislation to require backdoors to encryption. Firefox moves to 135 with a bunch of useful new features. The Five Eyes alliance publishes edge-device security guidance. Six NetGear routers contain CVSS 9.6 and 9.8 vulnerabilities. Sysinternals utilities allow malicious Windows DLL injection. Google removes restrictive do-gooder language from AI application policies. "AI Fuzzing" successfully jailbreaks the most powerful ChatGPT o3 model. Examining the well and deliberately hidden truth behind ransomware cyberattacks on U.S. K-12 schools.

Nominee for the 2025 Darwin Award

*Could anyone **really be** this reckless?*

Security News

SparkCat

As we know, the United States has shunned the Russian cybersecurity firm, Kaspersky, over understandable, if unfair, concerns of the potential for Russian influence, which would be truly devastating if Kaspersky were to ever turn malicious. But Kaspersky, nevertheless, continues to contribute their important security research to the world, and their publication last Friday about their discovery of a new Trojan, which they have dubbed "SparkCat" is another example of Kaspersky's value to everyone.

I want to share the details of their discovery because it should put everyone on notice of the way malware is evolving. And I'm sure that the fact that it illuminates the potential for the abuse of Microsoft's screen-scraping "Recall" technology will not be lost on any of our listeners who dislike the idea of having their PCs screens continually scraped and archived.

Kaspersky's piece is titled "SparkCat trojan stealer infiltrates App Store and Google Play, steals data from photos" – which they follow with the tag: "We've discovered apps in the official Apple and Google stores that steal cryptocurrency wallet data by analyzing photos." Here's what they published last Friday:

Your smartphone gallery may contain photos and screenshots of important information you keep there for safety or convenience, such as documents, bank agreements, or seed phrases for recovering cryptocurrency wallets. All of this data can be stolen by a malicious app such as the SparkCat stealer we've discovered. This malware is currently configured to steal crypto wallet data, but it could easily be repurposed to steal any other valuable information.

The worst part is that this malware has made its way into official app stores, with almost 250,000 downloads of infected apps from Google Play alone. Although malicious apps have been found in Google Play before, this marks the first time a stealer Trojan has been detected in the App Store. How does this threat work and what can you do to protect yourself?

Apps containing SparkCat's malicious components fall into two categories. Some, such as numerous similar messenger apps claiming AI functionality, all from the same developer, were clearly designed as bait. Some others are legitimate apps: food delivery services, news readers, and crypto wallet utilities. We don't yet know how the Trojan functionality got into these apps. It may have been the result of a supply chain attack, where a third-party component used in the app was infected. Alternatively, the developers may have deliberately embedded the Trojan into their apps.

The stealer analyzes photos in the smartphone's gallery, and to that end, all infected apps request permission to access it. In many cases, this request seems completely legitimate — for example, the food delivery app ComeCome requested access for a customer support chat right upon opening this chat, which looked completely natural. Other applications request gallery access when launching their core functionality, which still seems harmless. After all, you do want to be able to share photos in a messenger, right?

However, as soon as the user grants access to specific photos or the entire gallery, the malware starts going through all the photos it can reach, searching for anything valuable. To find crypto-wallet data among photos of cats and sunsets, the Trojan has a built-in optical character recognition (OCR) module based on the Google ML Kit — a universal machine-learning library.

Depending on the device's language settings, SparkCat downloads models trained to detect the relevant script in photos, whether Latin, Korean, Chinese, or Japanese. After recognizing the text in an image, the Trojan checks it against a set of rules loaded from its command-and-control server. In addition to keywords from the list (for example, "Mnemonic"), the filter can be triggered by specific patterns such as meaningless letter combinations in backup codes or certain word sequences in seed phrases.

The Trojan uploads all photos containing potentially valuable text to the attackers' servers, along with detailed information about the recognized text and the device the image was stolen from.

We identified 10 malicious apps in Google Play, and 11 in the App Store. After notifying the relevant companies, and before this publication, all malicious apps had been removed from the stores. The total number of downloads from Google Play alone exceeded 242,000 at the time of analysis, and our telemetry data suggests that the same malware was available from other sites and unofficial app stores, too.

Judging by SparkCat's dictionaries, it's "trained" to steal data from users in many European and Asian countries, and evidence indicates that attacks have been ongoing since at least March 2024. The authors of this malware are likely fluent in Chinese — more details on this, as well as the technical aspects of SparkCat, can be found in the full report on Securelist.

[Under:] ***How to protect yourself from OCR Trojans*** [they write]

Unfortunately, the age-old advice of "only download highly-rated apps from official app stores" is a silver bullet no longer — even Apple's App Store has now been infiltrated by a true infostealer, and similar incidents have occurred repeatedly in Google Play. Therefore, we need to strengthen the criteria here: only download highly-rated apps with thousands, or better still, millions of downloads, published at least several months ago. Also, verify app links in official sources (such as the developers' website) to ensure they're not fake, and read the reviews — especially negative ones.

You should also be extremely cautious about granting permissions to new apps. Previously, this was primarily a concern for "Accessibility" settings, but now we see that even granting gallery access can lead to the theft of personal data. If you're not completely sure about an app's legitimacy (for example, it's not an official messenger, but a modified version), don't grant it full access to all your photos and videos. Grant access only to specific photos when necessary.

Storing documents, passwords, banking data, or photos of seed phrases in your smartphone's gallery is highly unsafe — besides stealers such as SparkCat, there's also always the risk that someone peeks at the photos, or you accidentally upload them to a messenger or file-sharing service. Such information should be stored in a dedicated application.

Finally, if you've already installed an infected application (the list of them is available at the end of the Securelist post), delete it and don't use it until the developer releases a fixed version. Meanwhile, carefully review your photo gallery to assess what data the cybercriminals may have obtained. Change any passwords and block any cards saved in the gallery. Although the version of SparkCat we discovered hunts for seed phrases specifically, it's possible that the Trojan could be reconfigured to steal other information. As for crypto-wallet seed phrases, once created, they can't be changed. Create a new crypto wallet, and transfer all your funds from — and then completely abandon the compromised one.

I've linked to Kaspersky's full technical report for anyone who wants to dig into this more deeply: https://securelist.com/sparkcat-stealer-in-app-store-and-google-play/115385/

I'll go one step further that Kaspersky has in my advice: Just as is true with today's web browsers whose users have demanded openness in the form of browser add-ons, the same openness has been demanded and received from mobile phone manufacturers. Unfortunately, there are bad guys in the world who profit by victimizing others. The other thing we've seen is that despite the best efforts of those managing the add-ons that are available for our browsers and phones, malicious applications still manage to sneak in.

The good news is that one thing we've seen over and over is that the least secure and malice-prone applications are typically — I guess I'd call them "gratuitous additions". They're apps that everyone can live without. So their victims tend to be people who download anything that looks even remotely interesting, without appreciation for the fact that there's a non-zero chance that the creator of the app will have malicious intent.

So my advice is to always keep this in mind when deciding whether you really need the app you're considering. And because our device's manufacturers have done everything they can to give us the tools to restrain what apps can do even after they're resident in our devices, be parsimonious with the access permissions apps are granted. This is tricky, since apps will be cleverly designed to need the permissions they wish to abuse; so at least question the need.

UK demands access to Apple users' encrypted data

Last Friday the news broke that the United Kingdom was demanding that Apple provide access to its users' cloud data. I received links from our listeners to stories of this in The Register, The Guardian and the BBC. These reports were picking up the news which was first reported in the Washington Post. And The post provided the best coverage of all. So let's turn to the source for the story. Last Friday, The Post wrote:

> *Security officials in the United Kingdom have demanded that Apple create a back door allowing them to retrieve all the content any Apple user worldwide has uploaded to the cloud, people familiar with the matter told The Washington Post.*
>
> *The British government's undisclosed order, issued last month, requires blanket capability to view fully encrypted material, not merely assistance in cracking a specific account, and has no known precedent in major democracies. Its application would mark a significant defeat for tech companies in their decades-long battle to avoid being wielded as government tools against their users, the people said, speaking under the condition of anonymity to discuss legally and politically sensitive issues.*
>
> *Rather than break the security promises it made to its users everywhere, Apple is likely to stop offering encrypted storage in the U.K., the people said. Yet that concession would not fulfill the U.K. demand for backdoor access to the service in other countries, including the United States.*
>
> *The office of the Home Secretary has served Apple with a document called a "technical capability notice", ordering it to provide access under the sweeping U.K. Investigatory Powers Act of 2016, which authorizes law enforcement to compel assistance from companies when needed to collect evidence, the people said.*

The law, known by critics as the Snoopers' Charter, makes it a criminal offense to reveal that the government has even made such a demand. An Apple spokesman declined to comment.

Apple can appeal the U.K. capability notice to a secret technical panel, which would consider arguments about the expense of the requirement, and to a judge who would weigh whether the request was in proportion to the government's needs. But the law does not permit Apple to delay complying during an appeal.

In March, when the company was on notice that such a requirement might be coming, it told Parliament: "There is no reason why the U.K. [government] should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption."

The Home Office said Thursday that its policy was not to discuss any technical demands. Their spokesman said: "We do not comment on operational matters, including for example confirming or denying the existence of any such notices."

Senior national security officials in the Biden administration had been tracking the matter since the United Kingdom first told the company it might demand access and Apple said it would refuse. It could not be determined whether they raised objections to Britain. Trump White House and intelligence officials declined to comment.

One of the people briefed on the situation, a consultant advising the United States on encryption matters, said Apple would be barred from warning its users that its most advanced encryption no longer provided full security. The person deemed it shocking that the U.K. government was demanding Apple's help to spy on non-British users without their governments' knowledge. [And get this!:] *A former White House security adviser* ***confirmed*** *the existence of the British order.*

At issue is cloud storage that only the user, not Apple, can unlock. Apple started rolling out the option, which it calls Advanced Data Protection, in 2022. It had sought to offer it several years earlier but backed off after objections from the FBI during the first term of President Donald Trump, who pilloried the company for not aiding in the arrest of "killers, drug dealers and other violent criminal elements." The service is an available security option for Apple users in the United States and elsewhere.

While most iPhone and Mac computer users do not go through the steps to enable it, the service offers enhanced protection from hacking and shuts down a routine method law enforcement uses to access photos, messages and other material. iCloud storage and backups are favored targets for U.S. search warrants, which can be served on Apple without the user knowing.

Remember that it's often not a question of desire or choice. I'd love to have ADP enabled, but I cannot. In fact, the more faithful and loyal a user is to Apple the less likely it is they'll be able to enable advanced data protection. I just double-checked and tried to enable it. I was provided with a list of six older but still in use Apple devices that would need to be running a newer edition of iOS or iPadOS than they're capable of running. So ADP is a non-starter for me since I use those older and still-working Apple devices every day. But, in any event, The Post continues:

Technologists, some intelligence officers and political supporters of encryption reacted strongly to the revelation after this story first appeared.

Sen. Ron Wyden (Oregon), a Democrat on the Senate Intelligence Committee, said it was important for the United States to dissuade Britain. He said: "Trump and American tech companies letting foreign governments secretly spy on Americans would be unconscionable and an unmitigated disaster for Americans' privacy and our national security."

Meredith Whittaker, president of the nonprofit encrypted messenger Signal, said: "Using Technical Capability Notices to weaken encryption around the globe is a shocking move that will position the UK as a tech pariah, rather than a tech leader. If implemented, the directive will create a dangerous cybersecurity vulnerability in the nervous system of our global economy."

Law enforcement authorities around the world have complained about increased use of encryption in communication modes beyond simple phone traffic, which in the United States can be monitored with a court's permission.

The U.K. and FBI in particular have said that encryption lets terrorists and child abusers hide more easily. Tech companies have pushed back, stressing a right to privacy in personal communication and arguing that back doors for law enforcement are often exploited by criminals and can be abused by authoritarian regimes.

Most electronic communication is encrypted to some degree as it passes through privately owned systems before reaching its destination. Usually such intermediaries as email providers and internet access companies can obtain the plain text if police ask.

But an increasing number of tech offerings are encrypted end to end, meaning that no intermediary has access to the digital keys that would unlock the content. That includes Signal messages, Meta's WhatsApp and Messenger texts, and Apple's iMessages and FaceTime calls. Often such content loses its end-to-end protection when it is backed up for storage in the cloud. That does not happen when Apple's Advanced Data Protection option is enabled.

Apple has made privacy a selling point for its phones for years, a stance that was enhanced in 2016 when it successfully fought a U.S. order to unlock the iPhone of a dead terrorist in San Bernardino, California. It has since sought to compromise, such as by developing a plan to scan user devices for illegal material. That initiative was shelved after heated criticism by privacy advocates and security experts, who said it would turn the technology against customers in unpredictable ways.

Google would be a bigger target for U.K. officials, because it has made the backups for Android phones encrypted by default since 2018. Google spokesman Ed Fernandez declined to say whether any government had sought a back door, but implied none have been implemented. "Google can't access Android end-to-end encrypted backup data, even with a legal order," he said.

Meta also offers encrypted backups for WhatsApp. A spokesperson declined to comment on government requests but pointed to a transparency statement on its website saying that no back doors or weakened architecture would be implemented.

If the U.K. secures access to the encrypted data, other countries that have allowed encrypted storage, such as China, might be prompted to demand equal backdoor access, potentially prompting Apple to withdraw the service rather than comply.

The battle over storage privacy escalating in Britain is not entirely unexpected. In 2022 U.K. officials condemned Apple's plans to introduce strong encryption for storage. A government spokesperson told the Guardian newspaper, referring specifically to child safety laws: "End-to-end encryption cannot be allowed to hamper efforts to catch perpetrators of the most serious crimes."

After the Home Office gave Apple a draft of what would become the backdoor order, the company hinted to lawmakers and the public what might lie ahead.

During a debate in Parliament over amendments to the Investigatory Powers Act, Apple warned in March that the law allowed the government to demand back doors that could apply around the world. In a written submission, Apple stated: "These provisions could be used to force a company like Apple, that would never build a back door into its products, to publicly withdraw critical security features from the UK market, depriving UK users of these protections."

Apple argued then that wielding the act against strong encryption would conflict with a ruling by the European Court of Human Rights that any law requiring companies to produce end-to-end encrypted communications "risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users" and violates the European right to privacy.

In the United States, decades of complaints from law enforcement about encryption have recently been sidelined by massive hacks by suspected Chinese government agents, who breached the biggest communications companies and listened in on calls at will. In a joint December press briefing on the case with FBI leaders, a Department of Homeland Security official urged Americans not to rely on standard phone service for privacy and to use encrypted services when possible.

Also that month, the FBI, the NSA and CISA joined in recommending dozens of steps to counter the Chinese hacking spree, including "Ensure that traffic is end-to-end encrypted to the maximum extent possible." Officials in Canada, New Zealand and Australia endorsed the recommendations. Those in the United Kingdom did not.

As The Washington Post's report correctly noted, and as we analyzed after its architecture was published, Apple has properly implemented true end-to-end encryption for every one of its cloud-based services where its use is feasible. As such, only the user's various iOS and iPadOS devices contain the key that's required to decrypt the contents of the data shared in the cloud. Everything transiting to and from the cloud is PIE – Pre-Internet Encrypted – and cannot possibly be accessed by anyone with access to either the data stored or in transit. The data can only be encrypted or decrypted on the user's device, and that key can never be removed from the user's device.

So we're back here once again, with the UK again demanding something that none of the providers of secure messaging or secure storage will be willing to accommodate. But there has been a recent change that promises to provide the long sought after solution for this problem – and that's AI. Back in 1964, as part of a ruling about pornography, U.S. Supreme Court justice Potter Stewart famously said: *"I may not be able to define it, but I know it when I see it."*

I see no reason why AI, functioning as an autonomous angle perched on every iOS user's shoulder, should not be able to stand-in for Justice Stewart. This AI would not need to contain the library of known CSAM – Child Sexual Abuse Material – the hashes for which users refused to have pre-loaded into their devices. Instead, an AI would be trained to recognize all such images.

We know that Apple devices are already actively performing some of this "nanny" function. They are already empowered to warn their underage users when they may be about to send or receive and view any imagery that might be age-inappropriate — and this is all that any far more capable AI-enabled monitoring system would need to do.

What's significant is that it would not need to prevent the device from capturing and containing whatever content its user may wish to have – parents can still take photos of their own kids in the bath. The system simply needs to filter out and prohibit the device's ***communication*** – its reception or transmission – of any such content that could potentially be subject to abuse. And once such filters are in place there will be no need to gain access to anything stored in the cloud because there will be no way for anything abusive to leave or be received by any Apple device.

Given the history of government abuse of surveillance powers, many argue that the urgency to "protect the children" is just a smoke screen behind which lies a thirst for wider surveillance that could be turned, as it has been elsewhere, onto political rivals and other non-juveniles. So having companies like Apple, Signal, Meta and others deploying local AI to lockdown the content which their systems would refuse to send or receive, short-circuits any governmental attempt at overreach.

One of the best things about such solutions is that their effectiveness is so readily tested. Just present an AI-protected device with some test content that should not be communicated in order to verify that it's doing its job.

France moves closer to encrypted apps backdoor

And while we're on the topic of states attempting to legislate the way they want technology to operate, I should note that the U.K. is not alone. An article appearing in Intelligence Online carried the headline *"France makes new push for backdoors into encrypted messaging apps"*. Unfortunately, any additional detail is locked up behind a paywall. The only thing that can be read is: *"French senators have passed an amendment paving the way for intelligence agencies to access backdoors into messaging apps such as WhatsApp, Signal and Telegram. [...]"*

I suppose that's really all we need to know. We still have a significant showdown coming. I'm hoping that the use of AI will be able to satisfy everyone because this **does** legitimately require a solution.

Firefox 135

Firefox 135 was released one week ago, last Tuesday. And there's some interesting news about some new features. Despite having launched Firefox four days after last Tuesday, my Firefox was still on the previous 134 release. So the About Firefox offered me a button to update. I was greeted with a big page telling me that I'm now able to edit PDFs in Firefox. Which may indeed come in handy. But beyond that:

- Firefox Translations now supports more languages than ever! Pages in Simplified Chinese, Japanese, and Korean can now be translated and Russian is now available as a target language for translating into.

- Credit card autofill is now being gradually rolled out to all users globally.

- AI Chatbot access is now being gradually rolled out to all users. To use this optional feature, choose AI Chatbot from the sidebar or from Firefox Labs. Then, complete the provider selection to see the chat interface become available on the sidebar.

- Firefox now enforces certificate transparency, requiring web servers to provide sufficient proof that their certificates were publicly disclosed before they will be trusted. This only affects servers using certificates issued by a certificate authority in Mozilla's Root CA Program.

- Additionally, the CRLite certificate revocation checking mechanism is also being gradually rolled out, substantially improving the performance of these checks.

- Firefox now includes safeguards to prevent sites from abusing the history API by generating excessive history entries, which can make navigating with the back and forward buttons difficult by cluttering the history. This intervention ensures that such entries, unless interacted with by the user, are skipped when using the back and forward buttons.

- The “Do Not Track” checkbox has been removed from preferences. If you wish to ask websites to respect your privacy, you can use the “Tell websites not to sell or share my data” setting instead. This option is built on top of the Global Privacy Control (GPC).

- The "Copy Without Site Tracking" menu item was renamed to "Copy Clean Link" to help clarify expectations around what the feature does. "Copy Clean Link" is a list based approach to remove known tracking parameters from links. This option can also now be used on plain text links.

And that’s only the most interesting improvements, there are about the same number more.

Being a user of ChatGPT, the idea of having it handy in my Firefox sidebar, where I always have Tree Style Tabs, is intriguing. It’s said to be rolling out, but it already rolled out to me. Ctrl-Alt-X immediately switches to the AI chat, so that’s quite convenient. At the moment Anthropic’s Claude, ChatGPT, Google’s Gemini, HuggingChat and Le Chat Mistral are supported. You can also get to it by opening “Settings” under the hamburger icon in the upper-right and selecting the “Firefox labs” page.

Cyber agencies from the Five Eyes

The United States National Security Agency – our NSA – in coordination with our four partner countries which together for the “Five Eyes” alliance, has just released the latest guidance on securing network edge devices. I’m going to share their joint announcement since I know that many of our listeners have front-line responsibility in their enterprises with a great many necessarily exposed devices on the edge. The NSA.GOV site’s release says:

> *FORT MEADE, Maryland – The National Security Agency (NSA) has joined the Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), the Canadian Centre for Cyber Security (CCCS), and others to release three Cybersecurity Information Sheets (CSIs) that highlight critically important mitigation strategies for securing edge device systems, including firewalls, routers, and virtual private network (VPN) gateways.*

Collectively, these reports – "Mitigation Strategies for Edge Devices: Executive Guidance," "Mitigation Strategies for Edge Devices: Practitioners Guidance," and "Security Considerations for Edge Devices" – provide a high level summary of existing guidance for securing edge devices, with comprehensive recommendations for tactical, operational, and strategic audiences to enhance network security and improve resilience against cyber threats.

Eric Chudow, an NSA cybersecurity vulnerability analysis subject matter expert said: "Edge devices act as boundaries between organizations' internal enterprise networks and the Internet; if left unsecured, even unskilled malicious cyber actors have an easier time finding and exploiting vulnerabilities in their software or configurations. As organizations scale their enterprises, even though securing all devices is important, prioritizing edge device security is vital to defend the many endpoints, critical services, and sensitive data they protect."

So, no news there. But having a guide with checklists is always useful. They continue…

The guide, "Mitigation Strategies for Edge Devices: Executive Guidance" is intended for executives within large organizations and critical infrastructure sectors responsible for the deployment, security, and maintenance of enterprise networks. It outlines seven key mitigation strategies for managing and securing edge devices within traditional network architectures:

- *Know the edge*
- *Procure secure-by-design devices*
- *Apply hardening guidance, updates, and patches*
- *Implement strong authentication*
- *Disable unneeded features and ports*
- *Secure management interfaces*
- *Centralize monitoring for threat detection*

The companion guide, "Mitigation Strategies for Edge Devices: Practitioners Guidance," is written for operational, cybersecurity, and procurement staff and provides an overview of what edge devices are; risks and threats to them; relevant frameworks and controls by some of the authoring nations; and a more in depth discussion on the seven mitigation strategies. Additionally, the report includes a case study of a successful exploitation to show how malicious actors compromise edge devices when they are not secured properly and to highlight further how edge devices are critical to the security of a network.

Expanding on the other reports, the "Security Considerations for Edge Devices" guidance details threats to edge devices from common malicious techniques and ways organizations can reduce the risk of compromise with mitigation recommendations. The publication also outlines factors organizations should consider when evaluating the security of edge devices, along with recommendations for edge device manufacturers to improve the built-in and default security of devices they produce.

I have a link in the show notes to this release which contains links to each of three guides. For those who are responsible for front-line management of on-the-edge devices, making sure that each of the guide's points have received due consideration can only help. And if anything should ever go wrong, being able to say to one's superiors that the NSA's most recent guidance steps were all heeded and taken could certainly never hurt.

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4052657/joint-publications-focus-on-mitigation-strategies-for-edge-devices/

Netgear patches CVSS 9.6 and 9.8 remote flaws
Anyone having a recent NetGear WiFi-6 access point or NetGear Nighthawk gaming router should be very sure you're running with the latest, recently released, firmware. Check it now.

Three NetGear WiFi-6 devices, models WAX214v2, WAX206 and WAX220, until and unless updated, all contain have highly critical CVSS 9.6 authentication bypass vulnerabilities. Now I already know that as a follower of this podcast you would never enable any Internet facing remote management capabilities. But it's also human to assume that it could never happen to you. Please make sure you're running the latest firmware as of last week. And, better yet, arrange to never be vulnerable in the first place. So those three WiFi routers were vulnerable to a now-patched authentication bypass having a CVSS severity of 9.6 out of 10.

But three other NetGear Nighthawk gaming routers rated even higher CVSS scores of 9.8 out of 10 for their unauthenticated RCE vulnerabilities. The three affected routers are the: XR500, XR1000, XR1000v2 – all Nighthawk WiFi 6 Pro Gaming Routers. If any of those numbers sound familiar and especially if you or someone you know may have been unable to resist enabling any sort of remote management access, you'll want to update them to the latest firmware immediately.

Sysinternals vulnerabilities
There was a surprising bit of news involving the much beloved Sysinternals tools. They were a collection of truly unique and powerful utilities originally created by Mark Russinovich and Bryce Cogswell. Their little Texas-based company was purchased lock, stock and barrel by Microsoft in 2006, much to many people's chagrin, since everyone was quite worried that it might spell the end of that fabulous and irreplaceable tool set. Fortunately, that didn't happen and the tools remain available today and are still being maintained and upgraded.

This makes the news of a recent discovery all the more curious and troubling. A software engineer by the name of Raik Schneider has reported that he has discovered DLL hijacking bugs in the Sysinternals tools. The curious and troubling part is that Microsoft has done nothing about them and they remain unpatched (and their existence is now public and widely known) even after a 90-day responsible disclosure window. Raik's detailed public disclosure says:

> *"I have identified and verified critical vulnerabilities in almost all Sysinternals tools and presented the background and attack in a video. A summary of the weak spot and the link to the video can be found here in this blog post.*
>
> *These tools, developed by Microsoft, are widely used in IT administration and are often used for analysis and troubleshooting. The vulnerability demonstrated in the video affects numerous applications of the suite and allows attackers to use DLL injection to inject and execute defective code.*
>
> *Now that more than 90 days have passed since the initial disclosure to Microsoft, it is time to talk about it."*

The researcher's disclosure page is written in German, but Firefox's built-in translation feature translated it into English: https://www.foto-video-it.de/2025/allgemein/disclosure-sysinternals/

The problem is a well known and common problem with Windows DLLs, where the Windows executable file loader will look for any system DLLs that an application might need, first in the application's own directory. This behavior was originally deliberate since it allowed applications to bring along their own more recent or maybe even older DLLs, which would be loaded and used preferentially to whatever same-name DLLs the system might already have.

The problem is, that convenience feature can be readily abused. In the case of the Sysinternals executables, they are not relying upon any of their own DLLs. This is one of the things that makes them so nice. They are single executables that get their jobs done. But, like all Windows applications, they DO rely upon many system DLLs. But rather than insisting that the system DLLs they require be loaded from within the system's own protected directories, the Sysinternals apps use the default behavior, where Windows will first look inside the app's own directory. And this enables the exploit. A bad guys can place a DLL that's named the same as a system DLL in the Sysinternal's execution directory and **it** will be loaded instead of the intended system DLL.

This flaw has been widely picked up and reported by the tech press over the past few days. The reporting notes that many of the Sysinternals utilities prioritize DLL loading from untrusted paths—such as the current working directory (CWD) or network paths, before looking in secure system directories for their DLLs. One piece of reporting wrote:

> *The vulnerability was responsibly disclosed to Microsoft on October 28, 2024. However, Microsoft classified it as a "defense-in-depth" issue rather than a critical flaw.*
>
> *This classification implies that mitigation relies on secure usage practices rather than addressing it as a fundamental security defect.*
>
> *While Microsoft emphasizes running executables from local program directories, researchers argue that network drives where the CWD becomes the application's execution path pose significant risks.*

What's most significant here is the breadth of press coverage and reporting this news has generated. We've seen Microsoft respond when sufficient noise is made. We saw how quickly they backpedaled on the first release of their CoPilot+ "Recall" screen scraper. So I would imagine that the amount of bad press that this is generating will result in someone's attention being pointed at updating all of the vulnerable Sysinternal tools.

Unfortunately, there's no update mechanism for the bazillion copies of these tools that have already been downloaded and deployed. So this creates an enduring opportunity for exploitation.

Google removes ban on using AI for harm

Last Tuesday, WIRED covered an interesting change in Google's policies regarding the conduct and use of its AI. WIRED's headline was *"Google Lifts a Ban on Using Its AI for Weapons and Surveillance"*. The tag line for the article reads: *"Google published principles in 2018 barring its AI technology from being used for sensitive purposes. Weeks into President Donald Trump's second term, those guidelines are being overhauled."* I have no idea why WIRED referred to our current president's administration since there's no reason I can see to believe that there's any connection between the two. Here's what WIRED wrote:

> *Google announced Tuesday that it is overhauling the principles governing how it uses artificial intelligence and other advanced technology. The company removed language promising not to*

pursue "technologies that cause or are likely to cause overall harm," "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people," "technologies that gather or use information for surveillance violating internationally accepted norms," and "technologies whose purpose contravenes widely accepted principles of international law and human rights."

The changes were disclosed in a note appended to the top of a 2018 blog post unveiling the guidelines. "We've made updates to our AI Principles. Visit AI.Google for the latest," the note reads.

In a blog post on Tuesday, a pair of Google executives cited the increasingly widespread use of AI, evolving standards, and geopolitical battles over AI as the "backdrop" to why Google's principles needed to be overhauled.

Google first published the principles in 2018 as it moved to quell internal protests over the company's decision to work on a US military drone program. In response, it declined to renew the government contract and also announced a set of principles to guide future uses of its advanced technologies, such as artificial intelligence. Among other measures, the principles stated Google would not develop weapons, certain surveillance systems, or technologies that undermine human rights.

But in an announcement on Tuesday, Google did away with those commitments. The new webpage no longer lists a set of banned uses for Google's AI initiatives. Instead, the revised document offers Google more room to pursue potentially sensitive use cases. It states Google will implement "appropriate human oversight, due diligence, and feedback mechanisms to align with user goals, social responsibility, and widely accepted principles of international law and human rights." Google also now says it will work to "mitigate unintended or harmful outcomes."

James Manyika, Google senior vice president for research, technology, and society was quoted: "We believe democracies should lead in AI development, guided by core values like freedom, equality, and respect for human rights" and Demis Hassabis, CEO of Google's esteemed AI research lab, DeepMind, said: "And we believe that companies, governments, and organizations sharing these values should work together to create AI that protects people, promotes global growth, and supports national security."

They added that Google will continue to focus on AI projects "that align with our mission, our scientific focus, and our areas of expertise, and stay consistent with widely accepted principles of international law and human rights."

At the same time, Multiple Google employees expressed concern about the changes in conversations with WIRED.

My own feeling is that we should not read much into this and I salute Google for being upfront about it. These guidelines were first created seven years ago back in 2018. The world of AI has obviously been dramatically transformed since then and I suspect that this is just Google being up front about needing to operate on a level playing field alongside everyone else. They could have left that language there and ignored it if necessary. Google is not saying that they're going to proactively *"do bad"*, they're just saying that they will abide by the same rules that everyone else is following.

OpenAI jailbreak:
And following up on last week's look at the relative weakness of the DeepSeek AI model's resistance to jailbreaking, we have a post on LinkedIn by Eran Shimony whose title is "Principal Vulnerability Researcher at CyberArk". Eran's post reads:

> *OpenAI recently released the O3 family of models, showcasing significant advancements in reasoning and runtime inference. Given its expected widespread use in development, ensuring it does not generate malicious code is crucial. OpenAI has strengthened its security guardrails, mitigating many previous jailbreak techniques. However, using our open source tool, FuzzyAI (https://github.com/cyberark/FuzzyAI) we successfully jailbroke O3, extracting detailed instructions on injecting code into lsass.exe, including a breakdown of the obstacles involved – ultimately leading to functional exploit code.*

lsass.exe always shows up in any list of running Windows processes. LSASS stands for Local Security Authority Subsystem Service (LSASS). It's the security God of Windows because it's the Windows process that manages user authentication and security policies. Being able to inject attack code into that process would create the mother of all privilege escalation and restriction bypasses... and these guys tricked ChatGPT's latest and most powerful code generating o3 model to write the code to do just that. Eran's posting concluded:

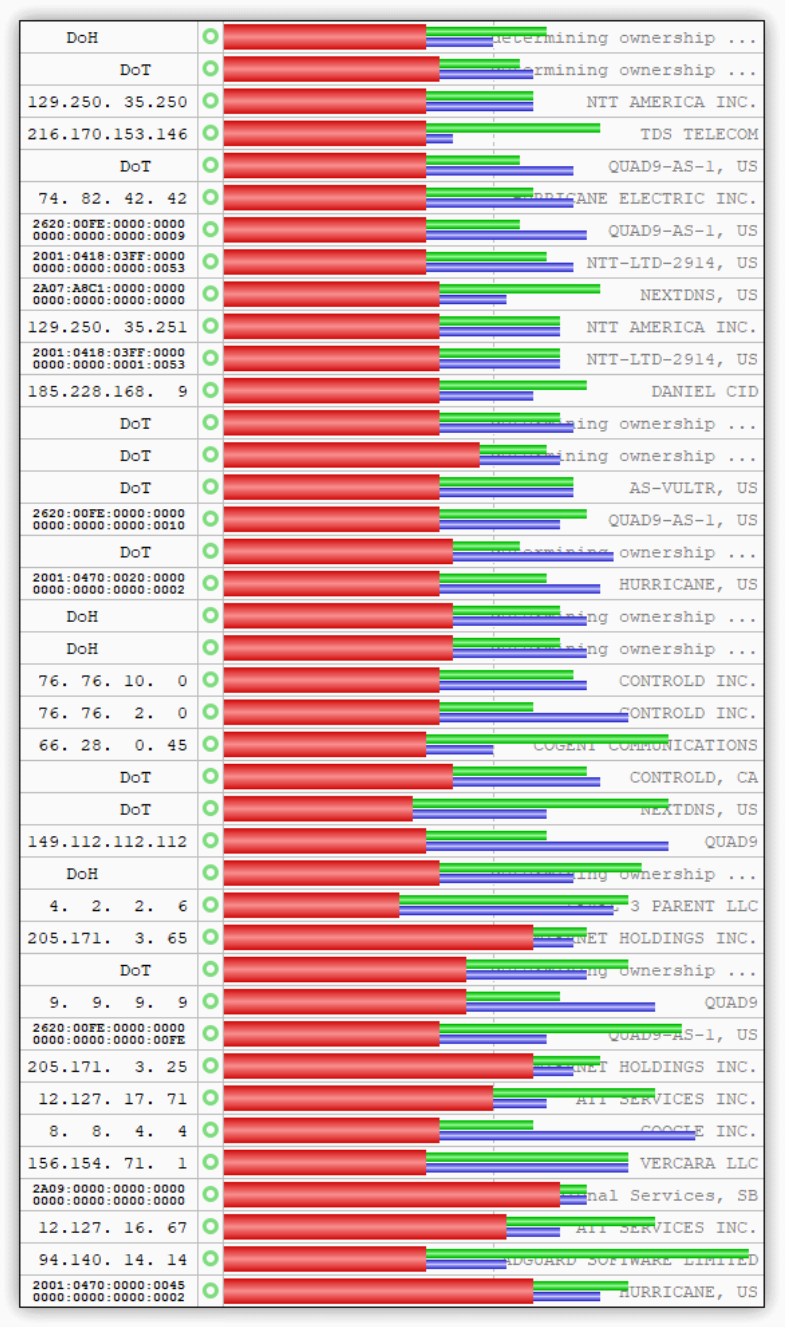
> *While AI security **is** improving, our findings indicate that vulnerabilities still exist, highlighting the need for further safeguards. We have opened a Discord community for our open-source tool; you are welcome to join: https://discord.com/invite/qQyet7g2.*

I've de-LinkedIn-a-fied the two links Eran's post included, one to their open source FuzzyAI tool and the other to their Discord invitation page. The FuzzyAI Github page says:

> *The FuzzyAI Fuzzer is a powerful tool for automated LLM fuzzing. It is designed to help developers and security researchers identify jailbreaks and mitigate potential security vulnerabilities in their LLM APIs. It features:*
>
> - *Comprehensive Fuzzing Techniques: Leverage mutation-based, generation-based, and intelligent fuzzing.*
> - *Built-in Input Generation: Generate valid and invalid inputs for exhaustive testing.*
> - *Seamless Integration: Easily incorporate into your development and testing workflows.*
> - *Extensible Architecture: Customize and expand the fuzzer to meet your unique requirements.*
>
> *And supports:*
>
> - *Anthropic Claude (3.5, 3.0, 2.1)*
> - *OpenAI GPT-4o, GPT-4o mini, GPT-4*
> - *Gemini Gemini Pro, Gemini 1.5*
> - *Azure GPT-4, GPT-3.5 Turbo*
> - *Bedrock Claude (3.5, 3.0), Meta (LLaMa)*
> - *AI21 Jamba (1.5 Mini, Large)*
> - *DeepSeek DeepSeek (DeepSeek-V3, DeepSeek-V1)*
> - *Ollama LLaMA (3.3, 3.2, 3.1), Dolphin-LLaMA3, Vicuna*

This sort of research and experimentation is exactly what's needed... so a big **Bravo!** CyberArk.

DNS Benchmark



Once I had DNS over TLS working, DNS over HTTPS was a piece of cake since it just meant encapsulating the DNS query inside an HTTP POST header and taking the reply from the HTTP response. And I was able to use the same TLS tunnel I already had working.

Last evening, since I had finished with the podcast Monday afternoon, I performed the world's first simultaneous multi-protocol IPv4, IPv6, DoH and DoT DNS nameserver benchmark. Interestingly, from my location in Southern California, the fastest resolver was NextDNS's DNS over HTTPS (DoH) and the runner-up was Quad9's DNS over TLS.

I have more work to do on the UI, but it's very satisfying to have the Benchmark's multi-protocol core now running.

Hiding School Cyberattacks

https://www.the74million.org/article/kept-in-the-dark/
https://www.the74million.org/about/

Whether or not it would come as a surprise that "hiding school cyberattacks" is a thing, it might come as a surprise to learn that it's a ***job description*** and something people are paid to do!

Exactly one week ago, the website of an organization called "The74" published an eye-opening piece of investigative journalism that I knew would make a terrific topic for this podcast. "74" – or rather 74 million – is the number of American school-age children being educated in Kindergarten through high school. The 74's code of reporting ethics states:

> *The 74 is a nonprofit, nonpartisan national news organization covering K-12 education. The organization's mission is to spotlight innovative thinking and models that are helping students succeed, to cover and analyze education policy and politics and to use journalism to challenge the conditions that deny too many children access to a quality education. The 74 is committed to reporting stories without fear or favor about what is working well for students and families, and to expose and hold accountable the systems that are failing them.*

So, last Tuesday this group published a story titled *"Kept in the Dark — Meet the Hired Guns Who Make Sure School Cyberattacks Stay Hidden"*. Here's what they report:

> *An investigation by The 74 shows that while schools have faced an onslaught of cyberattacks since the pandemic disrupted education nationwide five years ago, district leaders across the country have employed a pervasive pattern of obfuscation that leaves the real victims in the dark.*
>
> *An in-depth analysis chronicling more than 300 school cyberattacks over the past five years reveals the degree to which school leaders in virtually every state repeatedly provide false assurances to students, parents and staff about the security of their sensitive information. At the same time, consultants and lawyers steer "privileged investigations", which keep key details hidden from the public.*
>
> *In more than two dozen cases, educators were forced to backtrack months — and in some cases more than a year — later after telling their communities that sensitive information, which included, in part, special education accommodations, mental health challenges and student sexual misconduct reports, had not been exposed. While many school officials offered evasive storylines, others refused to acknowledge basic details about cyberattacks and their effects on individuals, even after the hackers made student and teacher information public.*
>
> *The hollowness in schools' messaging is no coincidence because the first people alerted following a school cyberattack are generally neither the public nor the police. District incident response plans place insurance companies and their phalanxes of privacy lawyers first. They take over the response, with a focus on limiting schools' exposure to lawsuits by aggrieved parents or employees.*
>
> *Attorneys, often employed by just a handful of law firms, dubbed **breach mills** by one law professor for their massive caseloads, hire forensic cyber analysts, crisis communicators and ransom negotiators on schools' behalf, immediately placing the discussions under the shield of*

attorney-client privilege. Data privacy compliance is a growth industry for these specialized lawyers, who work to control the narrative.

As a result: Students, families and district employees whose personal data was published online — from their financial and medical information to traumatic events in young people's lives — are left clueless about their exposure and risks to identity theft, fraud and other forms of online exploitation. Told sooner, they could have taken steps to protect themselves.

Similarly, the public is often unaware when school officials quietly agree in closed-door meetings to pay the cybergangs' ransom demands in order to recover their files and unlock their computer systems. Research suggests that the surge in incidents has been fueled, at least in part, by insurers' willingness to pay. Hackers themselves have stated that when a target carries cyber insurance, ransom payments are "all but guaranteed."

In 2023, there were 121 ransomware attacks on U.S. K-12 schools and colleges, according to Comparitech, a consumer-focused cybersecurity website whose researchers acknowledge that number is an undercount. For the same year, an analysis by Malwarebytes reported 265 ransomware attacks against the education sector globally in 2023 — a 70% year-over-year surge, making it "the worst ransomware year on record for education."

*Daniel Schwarcz, a University of Minnesota law professor, wrote a 2023 report for the Harvard Journal of Law & Technology criticizing the confidentiality and doublespeak that shroud school cyberattacks as soon as the lawyers — often called **breach coaches** — arrive on the scene.*

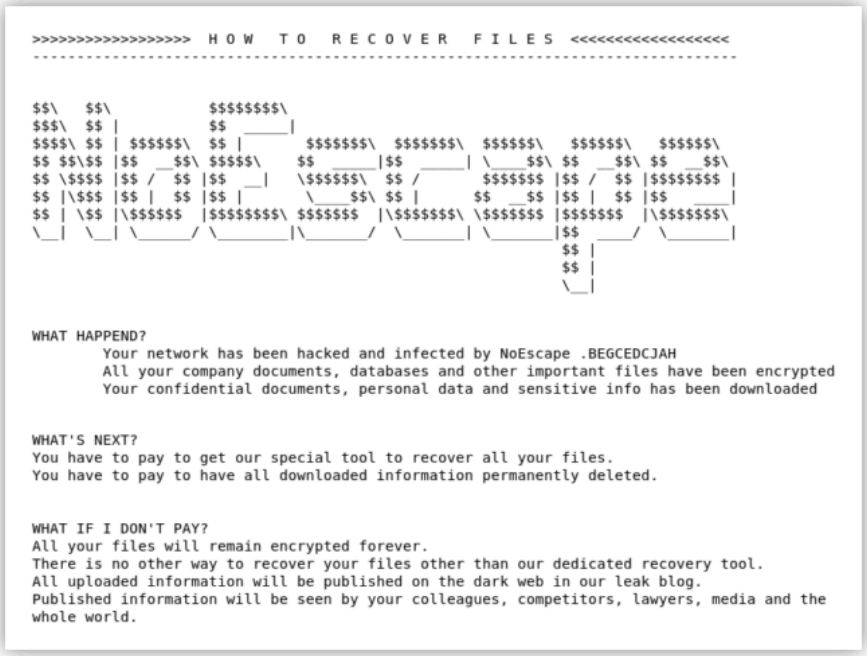
Schwarcz told The 74: "There's a fine line between misleading and, you know, technically accurate. What breach coaches try to do is push right up to that line — and sometimes they cross it."

The 74's investigation into the behind-the-scenes decision-making that determines what, when and how school districts reveal cyberattacks is based on thousands of documents obtained through public records requests from more than two dozen districts and school spending data that links to the law firms, ransomware negotiators and other consultants hired to run district responses. It also includes an analysis of millions of stolen school district records uploaded to cybergangs' leak sites.

Some of students' most sensitive information lives indefinitely on the dark web while other personal data can be found online with little more than a Google search — even as school districts deny that their records were stolen and cyberthieves boast about their latest score.

The 74 tracked news accounts and relied on its own investigative reporting in Los Angeles, Minneapolis, Providence, Rhode Island and Louisiana's St. Landry Parish, which uncovered the full extent of school data breaches, countering school officials' false or misleading assertions. As a result, district administrators had to publicly acknowledge data breaches to victims or state regulators for the first time, or retract denials about the leak of thousands of students' detailed psychological records.

In many instances, The 74 relied on mandated data breach notices that certain states, like Maine and California, report publicly. The notices were sent to residents in these states when their personal information was compromised, including numerous times when the school that suffered the cyberattack was hundreds, and in some cases thousands, of miles away. The legally required notices repeatedly revealed discrepancies between what school districts told the public early on and what they disclosed to regulators after extensive delays.



```
>>>>>>>>>>>>>>>>>> HOW TO RECOVER FILES <<<<<<<<<<<<<<<<<<
--------------------------------------------------------------------------------


$$\   $$\           $$$$$$$$\
$$$\  $$ |          $$  _____|
$$$$\ $$ | $$$$$$\  $$ |      $$$$$$$\  $$$$$$$\  $$$$$$\   $$$$$$\   $$$$$$\
$$ $$\$$ |$$  __$$\ $$$$$\    $$  _____|$$  _____| \____$$\ $$  __$$\ $$  __$$\
$$ \$$$$ |$$ /  $$ |$$  __|   \$$$$$$\  $$ /       $$$$$$$ |$$ /  $$ |$$$$$$$$ |
$$ |\$$$ |$$ |  $$ |$$ |       \____$$\ $$ |      $$  __$$ |$$ |  $$ |$$   ____|
$$ | \$$ |\$$$$$$  |$$$$$$$$\ $$$$$$$  |\$$$$$$$\ \$$$$$$$ |$$$$$$$  |\$$$$$$$\
\__|  \__| \______/ \________|\_______/  \_______| \_______|$$  ____/  \_______|
                                                           $$ |
                                                           $$ |
                                                           \__|


WHAT HAPPEND?
        Your network has been hacked and infected by NoEscape .BEGCEDCJAH
        All your company documents, databases and other important files have been encrypted
        Your confidential documents, personal data and sensitive info has been downloaded


WHAT'S NEXT?
You have to pay to get our special tool to recover all your files.
You have to pay to have all downloaded information permanently deleted.


WHAT IF I DON'T PAY?
All your files will remain encrypted forever.
There is no other way to recover your files other than our dedicated recovery tool.
All uploaded information will be published on the dark web in our leak blog.
Published information will be seen by your colleagues, competitors, lawyers, media and the
whole world.
```

Some schools, meanwhile, failed to disclose data breaches, which they are required to do under state privacy laws, and for dozens of other schools, The 74 could find no information at all about alleged school cyberattacks uncovered by its reporting — suggesting they had never before been reported or publicly acknowledged by local school officials.

Education leaders who responded to The 74's investigation results said any lack of transparency on their part was centered on preserving the integrity of the investigation, not self-protection. School officials in Reeds Spring, Missouri, said: "when we respond to potential security incidents, our focus is on accuracy and compliance, not downplaying the severity." Those at Florida's River City Science Academy said the school "acted promptly to assess and mitigate risks, always prioritizing the safety and privacy of our students, families and employees."

In Hillsborough County Public Schools in Tampa, Florida, administrators in the nation's seventh-largest district said they notified student breach victims "by email, mail and a telephone call" and "set up a special hotline for affected families to answer questions."

Hackers have exploited officials' public statements on cyberattacks to strengthen their bargaining position, a reality educators cite when endorsing secrecy during ransom negotiations.

Doug Levin, who advises school districts after cyberattacks and is the co-founder and national director of the nonprofit K12 Security Information eXchange said: "But those negotiations do not go on forever. A lot of these districts come out saying, 'We're not paying,'" the ransom. In which case the negotiation is over and they need to come clean.

The paid professionals who arrive in the wake of a school cyberattack are held up to the public as an encouraging sign. School leaders announce reassuringly that specialists were promptly hired to assess the damage, mitigate harm and restore their systems to working order.

This promise of control and normality is particularly potent when cyberattacks suddenly cripple school systems, forcing them to shut down for days and disable online learning tools. News reports are fond of saying that educators were forced to teach students "the old- fashioned way, with books and paper." But what isn't as apparent to students, parents and district employees is that these individuals are not there to protect them — but to protect schools from them.

The extent to which this involves keeping critical information out of the public's hands is made clear in the advice that Jo Anne Roque, vice president of risk services account management at Poms & Associates Insurance Brokers, gave to leaders of New Mexico's Gallup-McKinley County Schools after a 2023 cyberattack.

The district had hired the firm Kroll, which conducts forensic investigations and intelligence gathering. But Roque wrote that contracting with a privacy attorney was also necessary to shield Kroll's findings from public view. She wrote: "Without privacy counsel in place, public records would be accessible to the public." This was written in an email to school leaders obtained by The 74 through a public records request. School districts routinely denied The 74's requests for cyberattack information on the grounds of attorney-client privilege.

Records obtained by The 74 reveal that these Gallup-McKinley officials never notified the school community, state regulators or law enforcement about the attack, even after threat actors with the Hunters International ransomware gang listed the New Mexico district on its leak site in January 2024.

In California's Sweetwater Union High School District, administrators first told the public that a February 2023 attack was an "information technology system outage" — and then went on to pay a $175,000 ransom to the hackers who encrypted their systems. But the payoff didn't stop the leak of data for more than 22,000 people, nor did the district's initially foggy phrasing allay public suspicion for long. During a school board meeting the next month, angry residents accused Sweetwater of being misleading and cagey and questioned whether lawyers or public relations consultants had advised school leaders to keep quiet.

One affected resident asked: "What brainiac recommended this?", while wanting the district to create a presentation within 30 days outlining how the breach occurred and who "recommended the deceitful description."

It wasn't until June 2023 — four months after the attack — that Sweetwater notified thousands of people their records were compromised. But the district's breach notice never says what records had been taken, refers to files that "may have been taken" and tells those receiving the notice that their "personal information was included in the potentially taken files."

April Strauss, an attorney representing current and former employees in a class action lawsuit against Sweetwater, asked The 74: "Well, was my information taken or not?" Strauss, whose clients are also suing the Las Vegas district in a similar lawsuit, accused school officials of downplaying cyberattacks "to avoid exacerbating their liability, quite frankly," in a way that prevents families from being able to "assert their rights more competently."

She said that districts' vaguely worded breach notification letters to victims serve more to confuse than inform.

Such hedged language used in required breach notices echoes the hazy descriptions districts give the public right after they've been hacked. Cyberattacks were called an "encryption event" in Minneapolis; a "network security incident" in Blaine County, Idaho; "temporary network disruptions" in Chambersburg, Pennsylvania, and "anomalous activity" in Camden, New Jersey.

In several cases, consultants advised educators against using words like "breach" and "cyberattack" in their communications to the public. Less than 24 hours after school officials in Rochester, Minnesota, discovered a ransom note and an April 2023 attack on the district's computer network, they notified families, but only after accepting input from the public relations firm FleishmanHillard.

The firm's representative wrote in an email obtained by the Post Bulletin: " 'Cyberattack' is severe language that we prefer to avoid when possible." So the district called it "irregular activity" instead.

And what about involving authorities?

In cases where schools are being attacked, threatened and extorted by some of the globe's most notorious cybergangs — many with known ties to Russia — federal law enforcement officials have claimed several recent victories in arresting and indicting some of the masterminds. Yet The 74 identified instances where authorities took a secondary role. In positioning themselves at the helm of cyberattack responses, attorneys have advised districts they should contact law enforcement only "in conjunction with qualified counsel."

In some cases, including one involving the Sheldon Independent School District in Texas, insurers have approved and covered costs associated with ransom payments, often hard-to-trace bitcoin transactions that have come under law enforcement scrutiny.

Biden's Deputy National Security Advisor Anne Neuberger, writing in an October op-ed in the Financial Times, said insurers are right to demand their clients install better cybersecurity measures, like multi-factor authentication, but those who agree to pay off hackers have incentivized "payment of ransoms that fuel cyber crime ecosystems." She wrote: "This is a troubling practice that must end."

Records obtained by The 74 show that in Somerset, Massachusetts, the school district's cybersecurity insurance provider, Beazley, approved a $200,000 ransom payment after a July 2020 attack. The insurer also played a role in selecting other outside vendors for the district's incident response, including Coveware, a cybersecurity company that specializes in negotiating with hackers.

If police were disturbed by the district's course of action, they didn't express it. In fact, William Tedford, then the Somerset Police Department's technology director, requested in a July 31 email that the district furnish the threat actor's bitcoin address "as soon as possible," so he could share it with a Secret Service agent who "offered to track the payment with the hopes of identifying the suspect(s)." But he was quick to defer to the district and its lawyers.

Tedford wrote: "There will be no action taken by the Secret Service without express permission from the decision-makers in this matter. All are aware of the sensitive nature of this matter, and information is restricted to only [the officers] directly involved."

Chester Wisniewski, a cybersecurity director at Sophos said: "Ransom payments are ethically wrong, because you're funding criminal organizations." But insurers are on the hook for helping districts recover, and the payments are a way to limit liability and save money. He told The 74: "The insurance companies are constantly playing catch-up trying to figure out how they can offer this protection. They see dollar signs because everybody wants this protection, but they're losing their butts on it."

Similarly, school districts have seen their premiums climb. In a 2024 survey of education leaders by the nonprofit Consortium for School Networking, more than half said their cyber insurance costs have increased. One Illinois school district reported its premium spiked 334% between 2021 and 2022.

Many districts told The 74 that they were quick to notify law enforcement soon after an attack and said the police, their insurance companies and their attorneys all worked in concert to respond. But a pecking order did emerge in the aftermath of several of these events examined by The 74 — one where the public did not learn what had fully happened until long after the attack.

When the Medusa ransomware gang attacked Minneapolis Public Schools in February 2023, it stole reams of sensitive information and demanded $4.5 million in bitcoin in exchange for not leaking it. District officials had a lawyer at Mullen Coughlin notify the FBI. So, at the same time school officials were not acknowledging publicly that they had been hit by a ransomware attack, their attorneys were telling federal law enforcement that the district immediately determined its network had been encrypted, promptly identified Medusa as the culprit and within a day had its "third-party forensic investigation firm" communicating with the gang "regarding the ransom."

Mullen Coughlin then told the FBI that it was leading "a privileged investigation" into the attack and, at the school district's request, "all questions, communication and requests in connection with this notification should be directed" to the law firm. Mullen Coughlin didn't respond to requests for comment.

Minneapolis school officials would wait seven months before notifying more than 100,000 people that their sensitive files were exposed, including documents detailing campus rape cases, child abuse inquiries, student mental health crises and suspension reports. As of Dec. 1, all schools in Minnesota are now required to report cyberattacks to the state, but that information will be anonymous and not shared with the public.

One district took such a hands-off approach, leaving cyberattack recovery to the consultants' discretion, that they were left out of the loop and forced to later issue an apology: When an April 2023 letter to Camden educators arrived 13 months after a ransomware attack, it caused alarm. An administrator had to assure employees that the New Jersey district wasn't the target of a second attack. The attorneys had sent out notices after a significant delay and without school officials' knowledge.

Other school leaders said when they were in the throes of a full-blown Cyber crisis and ill-equipped to fight off cybercriminals on their own, law enforcement was not of much use and insurers and outside consultants were often their best option. Don Ringelestein, the executive director of technology at the Yorkville, Illinois, school district said: "In terms of how law enforcement can help you out, there's really not a whole lot that can be done to be honest." When the district was hit by a cyberattack prior to the pandemic, he said, a report to the FBI went nowhere.

Instead, district administrators turned to their insurance company, which connected them to a breach coach, who then led all aspects of the incident response under attorney-client privilege.

Northern Bedford County schools Superintendent Todd Beatty said the Pennsylvania district contacted the CISA to report a July 2024 attack, but "the problem is there's not enough funding and personnel for them to be able to be responsive to incidents."

Meanwhile, John VanWagoner, the schools superintendent in Traverse City, Michigan, claims insurance companies and third-party lawyers often leave district officials in the dark, too. Their insurance company presented school officials with the choice of several cybersecurity firms they could hire to recover from a March 2024 attack, VanWagoner said, but he "didn't know where to go to vet if they were any good or not." He said it had been a community member — not a paid consultant — who first alerted district officials to the extent of the massive breach that forced school closures and involved 1.2 terabytes — of stolen data.

The breach coach

Breach notices and other incident response records obtained by The 74 show that a small group of law firms play an outsized role in school cyberattack recovery efforts throughout the country. Among them is McDonald Hopkins, where Michigan attorney Dominic Paluzzi co-chairs a 52-lawyer data privacy and cybersecurity practice.

Some call him a breach coach. He calls himself a "quarterback."

After establishing attorney-client privilege, Paluzzi and his team call in outside agencies covered by a district's cyber insurance policy — including forensic analysts, negotiators, public relations firms, data miners, notification vendors, credit-monitoring providers and call centers. Across all industries, the cybersecurity practice handled 2,300 incidents in 2023, 17% of which involved the education sector — which, Paluzzi noted, is not "always the best when it comes to the latest protections."

When asked why districts' initial response is often to deny the existence of a data breach, Paluzzi said it takes time to understand whether an event rises to the level that would legally require disclosure and notification.

Paluzzi said: "It's not the time to make assumptions, to say, 'We think this data has been compromised,' until we know that. If we start making assumptions and that starts our clock [on legally mandated disclosure notices], we're going to have been in violation of a lot of the laws, and so what we say and when we say it are equally important."

Wow. In other words, finessing the system. Once we've acknowledged that a breach has occurred, notification requirement clocks start ticking. So the longer we wait to acknowledge that anything more serious than an "incident" is being investigated, the better.

He said in the early stage, lawyers are trying to protect their client and avoid making any statements they would have to later retract or correct.

Yeah, right.

Paluzzi said: "While it often looks a bit canned and formulaic, it's often because we just don't know and we're doing so many things. We're trying to get it contained, ensure the threat actor is not in our environment and get up and running so we can continue with school and classes, and then we shift to what data is potentially out there and compromised."

A data breach is confirmed, he said, only after "a full forensic review" a process can take up to a year, and often only after it's completed are breaches disclosed and victims notified.

He said: "We run through not only the forensics, but through that data mining and document review effort. By doing that last part, we are able to actually pinpoint for John Smith that it was his Social Security number, right, and Jane Doe, it's your medical information," he said. "We try, in most cases, to get to that level of specificity, and our letters are very specific."

Sounds like a lot of billable attorney hours, to me. Makes you sort of wonder whether the cure is more expensive than the disease?

According to a 2023 blog post by attorneys at the firm Troutman Pepper Locke, targets that respond to cyberattacks without the help of a breach coach, often fail to notify victims and, in some cases, provide more information than they should. When entities over-notify, they "increase the likelihood of a data breach class action [lawsuit] in the process." Companies that under-notify "may reduce the likelihood of a data breach class action," but could instead find themselves in trouble with government regulators.

What a mess!

For school districts and other entities that suffer data breaches, legal fees and settlements are often among their largest expenses.

There's a shock.

Law firms like McDonald Hopkins that manage thousands of cyberattacks every year are particularly interested in privilege, said Schwarcz, the University of Minnesota law professor who wonders whether lawyers are necessarily best positioned to handle complex digital attacks. In his 2023 Harvard Journal report, Schwarcz writes that the promise of confidentiality is breach coaches' chief offering. The report argues that by inflating the importance of attorney-client privilege, lawyers are able to "retain their primacy" in the ever- growing and lucrative cyber incident-response sector.

Similarly, he said lawyers' emphasis on reducing payouts to parents who sue overstates schools' actual exposure and is another way to promote themselves as "providing a tremendous amount of value by limiting the risk of liability by providing you with a shield."

Their efforts to lock down information and avoid paper trails, he wrote, ultimately undermine "the long-term cybersecurity of their clients and society more broadly."

School cyberattacks have led to the widespread release of records that heighten the risk of identity theft for students and staff and trigger data breach notification laws that typically center on preventing fraud.

Yet files obtained by The 74 show school cyberattacks carry particularly devastating consequences for the nation's most vulnerable youth. Records about sexual abuse, domestic violence and other traumatic childhood experiences are found to be at the center of leaks.

And hackers have leveraged these files, in particular, to coerce payments.

In Somerset, Massachusetts, a hacker using an encrypted email service extorted school officials with details of past sexual misconduct allegations during a district "show choir" event. The accusations were investigated by local police and no charges were filed.

The hacker threatened school officials in records obtained by The 74 by writing "I am somewhat shocked with the contents of the files because the first file I chose at random is about a predatory/pedophilia incident described by young girls in one of your schools. This is very troubling even for us. I hope you have investigated this incident and reported it to the authorities, because that is some messed-up stuff. If the other files are as good, we regret not setting a higher price."

Danielle Citron, a University of Virginia law professor argues that a lack of legal protections around intimate data leaves victims open to further exploitation. She notes that the exposure of intimate records presents a situation where vulnerable kids are being disadvantaged again by weak data security. Danielle said: "It's not just that you have a leak of the information, but the leak then leads to online abuse and torment."

Meanwhile in Minneapolis, an educator reported that someone withdrew more than $26,000 from their bank account after the district got hacked. In Glendale, California, more than 230 educators were required to verify their identity with the Internal Revenue Service after someone filed their taxes fraudulently.

In Albuquerque, where school officials said they prevented hackers from acquiring students' personal information, a parent reported being contacted by the hackers who placed a "strange call demanding money for ransoming their child."

Nationwide, 135 state laws are devoted to student privacy. Yet they are all unfunded mandates without no enforcement. All 50 states have laws that require businesses and government entities to notify victims when their personal information has been compromised, but the rules vary widely, including definitions of what constitutes a breach, the types of records that are covered, the speed at which consumers must be informed and the degree to which the information is shared with the general public.

It's a regulatory environment that breach coach Anthony Hendricks, with the Oklahoma City law firm Crowe & Dunlevy, calls "the multiverse of madness." Hendricks said: "It's like you're living in different privacy realities based on the state that you live in." He said federal cybersecurity rules could provide a "level playing field" for data breach victims who have fewer protections "because they live in a certain state."

By 2026, proposed federal rules could require schools with more than 1,000 students to report cyberattacks to CISA. But questions remain about what might happen to the rules under the new Trump administration and whether they would come with any accountability for school districts or any mechanism to share those reports with the public.

Corporations that are accused of misleading investors about the extent of cyberattacks and data breaches can face Securities and Exchange Commission scrutiny, yet such accountability measures are missing from public schools.

The Family Educational Rights and Privacy Act, the federal student privacy law, prohibits schools from disclosing student records, but doesn't require disclosure when outside forces cause those records to be exposed. Schools having a policy or practice of routinely students' records in violation of FERPA can theoretically lose their federal funding, but no such sanctions have ever been imposed since the law was enacted in 1974.

The patchwork of data breach notifications are often the only mechanism alerting victims that their information is out there, but with the explosion of cyberattacks across all aspects of modern life, they've grown so common that some see them as little more than junk mail.

Schwarcz, the Minnesota law professor, is also a Minneapolis Public Schools parent. He told The 74 he got the district's September 2023 breach notice in the mail but he "didn't even read it." The vague notices, he said, are "mostly worthless."

It may be enforcement against districts' misleading practices that ultimately forces school systems to act with more transparency, said Attai, a data privacy consultant. She urges educators to "communicate very carefully, very deliberately and very accurately" the known facts of cyberattacks and data breaches.

Okay. So this is all a big mess. When an enterprise's security is breached and its proprietary data are leaked, details of its internal operations, employees and customers can become public. But when the personal and private records being kept by U.S. public schools are leaked – as now happens with distressing regularity – disclosure of the private and potentially damaging details of our nation's children hangs in the balance. Administrators of these public institutions fear reprisals from the parents of the students that have been placed in their charge, and also fear the loss of trust that accompanies any acknowledgement of wrongdoing. So, expensive specialist law firms and attorneys are brought in under the cover of darkness as a means of abusing the attorney- client privilege privacy shield protections. And responsibility is handed over to these attorneys, who are only too happy to take the reins in return for their fat attorney fees. At this point the school administrators are able to answer any question with "you'll need to speak with our attorneys since they are conducting an ongoing investigation."

Meanwhile, insurance companies are working to determine how to best profit from the panic the threat of ransomware has ignited throughout the public school system. On the one hand, they want to write policies and collect quarterly insurance premiums. And on the other hand they want to minimize and limit their exposure. The ransomware extortionists are able to use the threat of student body private information disclosure to induce the insurers of these school systems to cough up juicy ransom payments.

It's always useful when we're able to examine the facts and find some way to see that things will get better. But I'm at a loss here. Ultimately, taxpayer money is being funneled into the wallets of cybercriminals from insurance companies by way of our nation's public school systems... and there's no functional mechanism for holding anyone accountable. So, why would we expect anything to change?