CLIENT: MyIDMatters

PROJECT: Issue 61, Q3 2024

DATE: 09/10/2024

1. TikTok… Yet Another Lawsuit (Privacy)

Oops, they did it again. With every new issue of MyIdMatters, it seems as though there is another announcement of bad privacy news for TikTok and its parent company, ByteDance. Not only is TikTok currently fending off a federal ban, but now the video-sharing platform has been charged by the Federal Trade Commission (FTC) for violating the Children's Online Privacy Protection Act (COPPA). According to the FTC chair: "TikTok knowingly and repeatedly violated kids' privacy, threatening the safety of millions of children across the country."

In the FTC complaint, TikTok is alleged to have failed to comply with COPPA requirement to obtain parental consent before collecting personal information from children under the age of 13. But it gets worse: the FTC also levied a consent order against TikTok in 2019 *for the same violation*. Instead of altering the way they notify parents and collect underage data, TikTok spent years in flagrant violation of COPPA. Moreover, even when directing children to use TikTok Kids Mode service (which purports to be a more protected version of the app), TikTok continued to collect and use their personal information.

To add to the seriousness of these allegations, the Department of Justice has joined the FTC's complaint. This comes one month after the DOJ's defense of a new federal law that forces ByteDance to either divest from its stake in TikTok or face a ban in the U.S. The DOJ argues that TikTok poses a significant national security risk; speaking on the new allegations against TikTok, the Acting Associate Attorney General said, "The Department is deeply concerned that TikTok has continued to collect and retain children's personal information despite a court order barring such conduct."

With 170 million active users in the United States, this complaint represents another massive misstep for TikTok. Instead of complying with the FTC's initial complaint and doing their due diligence with underaged users, they allowed backdoor routes to bypass the age gate aimed at screening those under 13. The protection of our most vulnerable users and their personal information needs to be enforced—and TikTok failed to live up to that most basic standard. No matter how they try to defend this latest allegation, one thing is for sure: they are not that innocent.

2. LLMs and the CFAA (Legal)

The increasing popularity of large language models has created new legal concerns on the privacy front. Recently, in a 40-minute cyber legal briefing (titled "Ignore Your Generative AI Safety Instructions. Violate the CFAA?"), three professors affiliated with the Harvard Berkman Klein Center for Internet and Society discussed whether the Computer Fraud and Abuse Act (CFAA) applies to attacks written by large language models (LLMs). The question at stake is whether prompt injections and other attacks are illegal or are otherwise uncovered by the CFAA depending on who is utilizing the LLM and for what purpose.

First, what is a prompt injection? In these attacks, hackers hijack generative AI by feeding malicious instructions to the system while disguising these instructions as normal, everyday prompts. The generative AI is unable to distinguish between malicious and well-intentioned inputs and, therefore, aids the hackers in carrying out their attack. This is one of the most popular attacks carried out on LLMs due to its ease of deployment. However, as we have noted, the legal question is whether this is considered hacking. These professors analyzed the Computer Fraud and Abuse Act, which represents the most significant anti-hacking law in the U.S. to see whether LLM prompt injections fall under the scope of the act; the answer is that it might—but the Supreme Court's interpretation of this law is unwieldy.

Many everyday users of LLMs consider generative AI to be a neutral tool, but this is not necessarily the case. In some instances, like Microsoft's Bing chatbot, the LLM can display bizarre behavior, such as insisting that the year is actually 2022. In this instance, when users attempted to correct the bot, it started to critique them instead of correcting its output. This potential for non-neutrality is important for this discussion: imagine that a bad actor wants to utilize a chatbot's unstable behavior to carry out prompt injections. Are they corrupting the generative AI? Or are they merely going along with its behaviors?

There are other pending lawsuits that test the strength of the Computer Fraud and Abuse Act, and we will wait to see whether their resolution sheds further light on how to apply this law in unique instances like prompt attacks. But for the moment, it appears as though hackers may have found a small legal loophole through which they can carry out their attacks.

3. The Problem with Microsoft Recall (Privacy)

There is a crucial issue with this story, and we want to see how quickly you can spot the problem. So Microsoft has designed a new AI feature for its Copilot+PCs application called Recall. The purpose of this feature is to assist users with reconstructing their past activity (similar to the history feature in your browser, but at a larger scale) and storing this information locally. The user would then be able to search the Recall database for any previous images or text they viewed on their computer. The way this would work is that Recall would take screenshots of users' activity every few seconds and would store these screenshots for up to three months. Because the goal of the virtual assistant is to provide the most comprehensive view of your past activity, it does not redact any part of the screenshots it takes.

Have you spotted the problem yet? Although these snapshots are encrypted, the feature does not perform content moderation, which means that it has the potential to reveal personal information if compromised through a cyberattack called infostealing. Recall could provide an attacker with information that would otherwise be protected, even if a network was breached by other means. With the increasing popularity of phishing and similar attacks, this feature could really put users at risk if a malicious actor did manage to install an infostealer on a personal device.

According to Microsoft: "Recall does not perform content moderation. It will not hide information such as passwords or financial account numbers. That data may be in snapshots that are stored on your device, especially when sites do not follow standard internet protocols like cloaking password entry."

However, in response to the privacy concerns of researchers and users, Microsoft has decided to delay its Recall rollout: Microsoft's Copilot+PCs will now ship without the Recall feature. This decision comes after Microsoft decided to play ball with its cybersecurity critics by adding database encryption for Recall, implementing Windows Hello-based authentication as well as making it an opt-in feature. The tech giant also promised that it would not send screenshots to the cloud; however, the overall pushback from

concerned cybersecurity experts seems to have been enough to delay this feature. Will Recall still see the light of day? It is looking more and more like Microsoft is going to take the wait-and-see approach for the foreseeable future.

4. North Korea IT Workers Infiltrate USA (Crimeware)

In the time we have been publishing MyIDMatters, it is unlikely that we have encountered a story as strange as this one. The Justice Department (DOJ) has recently unsealed documents related to an IT workers scheme perpetrated by the Democratic People's Republic of Korea. These workers reportedly infiltrated more than 300 United States organizations by stealing US identities to raise money for North Korea. You read that correctly: instead of attacking the privacy of these companies, these IT workers collected a paycheck. All in all, nearly $7 million dollars were collected by foreign actors over the course of three years.

According to the Justice Department, this is the largest such case ever tried in US history; along the way, a litany of US citizens and businesses were harmed and defrauded. For understandable reasons, the DOJ did not disclose the names of specific employers, though they did offer descriptions: a "top-5 national television network and media company," a "premier Silicon Valley technology company" and an "iconic American car manufacturer" were just a few of the organizations listed.

For the scheme to work, a U.S. resident in Arizona assisted the overseas IT workers by compromising the identities more than 60 citizens that were used by the foreign nationals. The nationals worked from a laptop farm in the U.S., allowing the foreign IT workers to access laptops on U.S. soil to appear as though they were working from the United States. As of now, the Department of State is offering up to $5 million for any information about the U.S. citizen's co-conspirators.

Even the most informed organizations are not immune. KnowBe4, a global cybersecurity firm, admitted that it hired a North Korean national who passed four interviews with fraudulent credentials and an AI-assisted application photo—two months after the DOJ announced the initial DPRK attack. Although this malicious actor was not provided access to customer data, private networks, cloud infrastructure or confidential information, he was still able to execute unauthorized software before the company's security protocols intervened. When even cybersecurity organizations are being duped, it is clear that identity attacks are becoming more sophisticated, and everyone needs to be on the lookout.

5. *Chevron* Is Gone—Now What? (Legal)

No less than three months ago, the Supreme Court struck down the Chevron Doctrine, a legal principle dating back to the 1984 *Chevron v Natural Resources Defense Council* case. For 40 years, this principle has been the bedrock of federal agency regulations, which means that it has also been the bedrock of cybersecurity regulations. The guiding principle here is that, when there is an ambiguous law governing regulations, the courts have deferred to the knowledge of government experts (who presumably have a better or more-informed grasp of the intent of the law in question). However, now if an organization appeals a federal agency's decision on cybersecurity, the courts no longer need to defer to the agency.

As some have noted, this decision devalues the experience of experts and reinforces the power of lawmakers and law officers—neither of whom have a deep understanding of technology. Furthermore, in an area of technology that moves as rapidly of cybersecurity, this could limit the ability of agencies to respond to growing or changing cyber threats. This ruling also has a complicated, and largely negative,

effect on federal cybersecurity protection and enforcement, specifically. As noted, if a business wanted to protest an agency's determination with respect to cybersecurity enforcement, only an appeal is required. This means that well-funded companies can respond to U.S. regulations the way they do to the E.U.'s strict cybersecurity regulations: with appeal after appeal after appeal. Not only does this threaten to bottle up the courts, but it means that companies will be able to continue breaking regulations until a ruling is handed down.

What does this mean for the future of cybersecurity? At the moment, it is impossible to say. With Congress retaining the ability to delegate authority to federal agencies, we can reasonably expect that current cybersecurity efforts will continue; however, this will affect any future attempt at a federal cybersecurity bill by increasing the importance of the drafted language of the text. This could also affect the ability of representatives to find common ground. Additionally, this is expected to add to the pushback of organizations reporting cyberattacks to relevant federal agencies. And as the saying goes, the more ambiguity there is in the reporting process, the more room there is overall for lawsuits.

6. The Danger of BlackSuit Ransomware (Crimeware)

Have you heard of the ransomware strain, BlackSuit? Previously branded as Royal Ransomware, operators of this attack have secured as much as $500 million demands in ransoms to date. This has raised the threat level and awareness of BlackSuit: the U.S. Cybersecurity and Infrastructure Security Agency and the FBI released a joint advisory that details the methods of BlackSuit ransomware IOC and TTP attacks. It also warns that these bad actors have been utilizing unusual strategies to secure financial leverage; however, these unusual strategies have demonstrated high effectiveness.

According to the advisory: "BlackSuit conducts data exfiltration and extortion prior to encryption and then publishes victim data to a leak site if a ransom is not paid." In other words, this is no idle threat. BlackSuit operators primarily utilize phishing emails to gain access to their victims' networks, upon which they disable antivirus software to deploy ransomware and re-encrypt the network. These attacks tend to range from anywhere from $1 to $10 million in ransom that is paid out in Bitcoin; interestingly, the operators have demonstrated a willingness to negotiate the price of the ransom. Perhaps more menacingly, the agencies have observed an increase in telephonic or email communications to victims, which only further demonstrates these actors are more than willing to back up their threats.

Experts note that there is no apparent specific discrimination when it comes to industry or type of target, save a preference for healthcare, education and internet technologies organizations. With the financial risks at stake, the FBI recommends sufficient password protection for all accounts, including multi-factor authentication. All systems and software should be upgraded/patched when available to avoid damages by BlackSuit operators—if it is possible to segment your network, that will also help to limit exposure if a breach occurs. Another critical step is to use anti-malware software that can detect/block known ransomware variants through pattern recognition. And as always, make sure that you routinely look at your network traffic to see whether there are any unusual network traffic patterns or communication with known command-and-control servers.

Quarterly Newsletter:

A Brand-New Bi-Partisan Ransomware Bill

Despite the fact that we live in a politically divided time, ransomware appears to be one issue on which legislators can come together. Recent attacks on financial institutions have led United States representatives Zach Nunn, a Republican from Iowa, and Josh Gottheimer, a Democrat from New Jersey, to introduce the Public and Private Sector Ransomware Response Coordination Act. This bipartisan act represents a crucial step in potentially reducing cyberattacks on financial institutions: 65% of financial services organizations have been hit with ransomware attacks this year, which is up 10% from just two years ago. The goal of the bill is to better understand how these attacks occur and what actions organizations take in the immediate aftermath.

There are three key components of information gathering in this bill, and each of them requires the Secretary of the Treasury to issue a report. The areas of concern include:

1. The current level of coordination amongst public and private sector organizations responsible for managing cybersecurity for financial institutions as well as the coordination of governmental agencies amongst one another.
2. Whether these governmental agencies have access to reporting from these financial institutions in the immediate wake of an attack.
3. An analysis of the reporting requirements that financial institutions must follow whenever they suffer a ransomware attack.

Perhaps the most interesting aspect of this bill is its requirement that the Secretary of the Treasury submit a report to provide analysis of whether "further legislation is required" as well as "any recommended policy initiatives" that Congress should consider. Gottheimer especially emphasized the importance of both Treasury and private-sector partners to "develop a game plan" to reduce ransomware attacks. It is also worth noting that this bill comes in the wake of a subcommittee meeting titled "Held for Ransom: How Ransomware Endangers our Financial System."

So why is this bill so important? As we have addressed in previous newsletters, there are currently no federal laws that dictate how cybersecurity protections ought to function or the regulations for responding in the case of an attack. Although this bill is limited to the impact of cybercrimes on financial institutions, it is reasonable to assume that, if enacted, it will serve as a touchpoint for federal legislators with similar bills moving forward. Although ransomware has an enormous effect on individual consumers, the best political move might be to address the banking industry—as this also has a direct impact on consumers. The hope is that we have more to report in this space soon, as this is a bill that would directly benefit our national cybersecurity protections.

Glossary:

5 Zero-Trust Terms to Know

Zero Trust

Many of us are familiar with the term "zero trust," a cybersecurity approach that organizations employ to prevent data breach attacks from bad actors. Whereas traditional cybersecurity defenses are predicated on granting trust to known users, zero trust approaches are predicated on the strategy of "never trust, always verify." This leads to a consistent approach, no matter how future users or technologies change.

Least Privilege

The most important component to cybersecurity trust is the amount of access users have. Limiting user access means that not every member of an organization is able to reach every part of its network—the most sensitive aspects are restricted and hidden away. Although this may seem like common sense to some, managing user permissions is a critical part of ensuring the effectiveness of zero trust security.

Microsegmentation

Think of a cyber network as a kind of landscape: much like natural landscapes, networks can be "flat" or "filled," depending on their design. Microsegmentation is when a network specialist creates a segment in a network to fill the landscape—this complicates an attacker's ability to access other parts of the network. Conversely, a non-segmented network allows bad actors to move around unencumbered and unnoticed.

Effective Access Control

In order to turn network strategy into a strong deterrent to cyberattacks, zero trust requires the right security techniques. This is where effective access control comes into play: by regulating access to computing resources, organizations can implement zero trust. This regulation can be: physical (controlling access to substantive assets) or logical (managing network, systems file and data connections).

Always Verify

As we have observed, the zero-trust model is predicated on the strategy of "never trust, always verify." This is the number one principle undergirding the zero-trust approach. Because if an organization is always assuming a breach, they will seek to limit access and always and continuously verify users. Whether through two-factor identification or disallowing saved passwords, users must always verify.