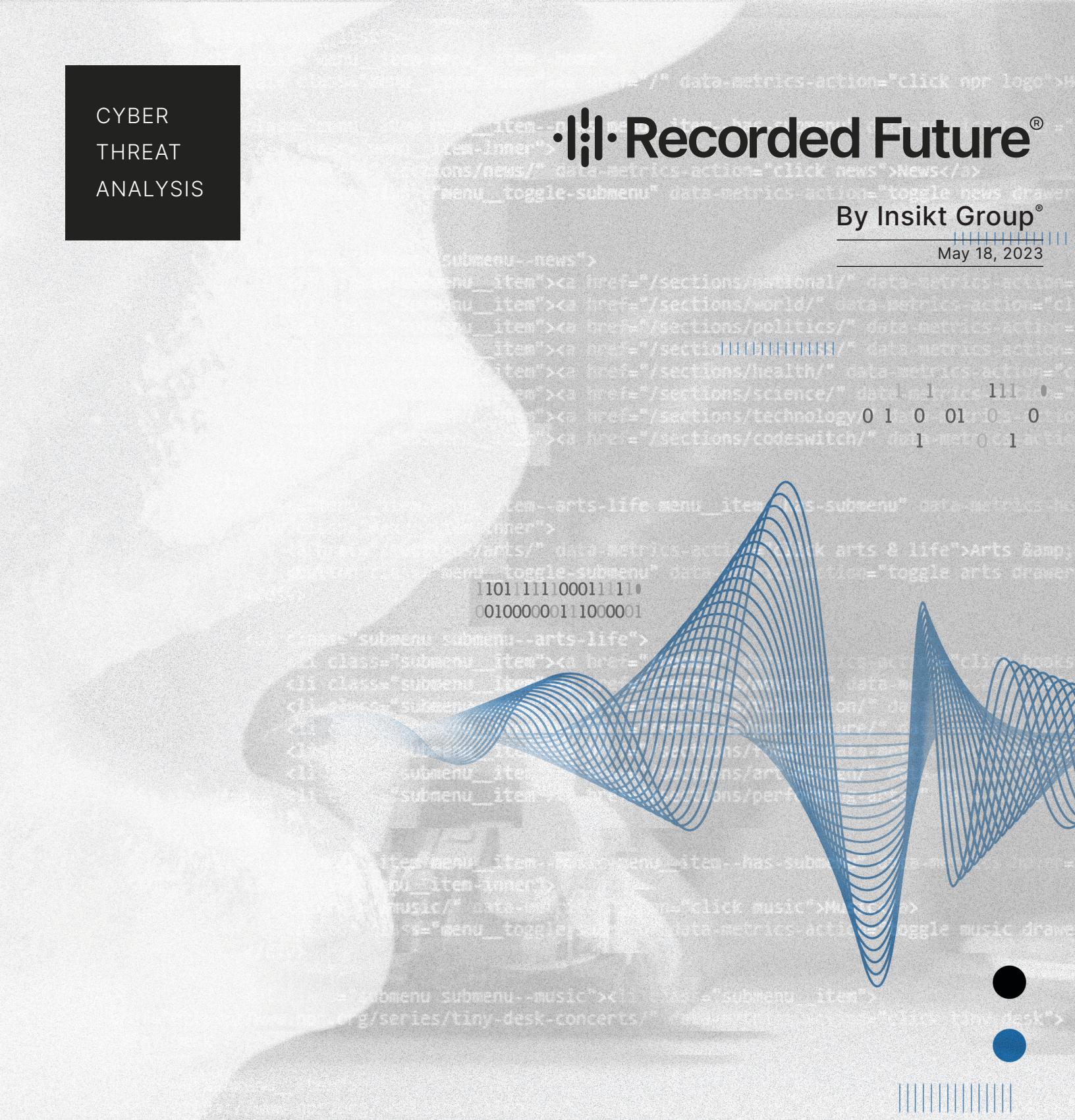
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

May 18, 2023



I Have No Mouth, and I Must Do Crime

Executive Summary

Deepfake voice cloning technology is an emerging risk to organizations, which represents an evolution in the convergence of artificial intelligence (AI) threats. When leveraged in conjunction with other AI technologies — such as deepfake video technology, text-based large language models (LLMs such as GPT), generative art, and others — the potential for impact increases. Voice cloning technology is currently being abused by threat actors in the wild. It has been shown to be capable of defeating voice-based multi-factor authentication (MFA), enabling the spread of misinformation and disinformation, and increasing the effectiveness of social engineering. We are continuously monitoring the emergence of deepfake technologies and their use in cybercrime, as detailed in our April 29, 2021 report "The Business of Fraud: Deepfakes, Fraud's Next Frontier".

As outlined in our January 26, 2023, report "I, Chatbot", open-source or "freemium" AI platforms lower the barrier to entry for low-skilled and inexperienced threat actors seeking to break into cybercrime. These platforms' ease-of-use and "out-of-the-box" functionality enable threat actors to streamline and automate cybercriminal tasks that they may not be equipped to act upon otherwise. Many of the voice cloning platforms referenced in this report are free-to-use with a registered account, thus lowering any financial barrier to entry for threat actors. For those that are not free-to-use, premium prices are negligible — rarely more expensive than $5 per month.

Voice cloning samples that surface on social media, messaging platforms, and dark web sources often leverage the voices of public figures — such as celebrities, politicians, and internet personalities ("influencers") — and are intended to create either comedic or malicious content. This content, which is often racist, discriminatory, or violent in nature, enables the spread of disinformation, as users on social media are sometimes deceived by the high quality of the voice cloning sample. This "proof-of-concept" (POC) work shared by threat actors has inspired a trend on dark web and special-access sources, with threat actors speculating about the emergence of voice cloning as an attack vector. Conversations among threat actors often reference executive impersonation, callback scams, voice phishing ("vishing"), and other attacks that rely on the human voice.

One of the most popular voice cloning platforms on the market is ElevenLabs's Prime Voice AI (elevenlabs[.]io), a browser-based text-to-speech (T2S; TTS) software that allows users to upload "custom" voice samples for a premium fee. While there are a number of voice cloning platforms referenced in this report (such as MetaVoice, Speechify, and so on), ElevenLabs is one of the most accessible, popular, and well-documented, and thus serves as the case study for this research.

Key Findings

- Voice cloning technologies, such as ElevenLabs, lower the barrier to entry for inexperienced English-speaking cybercriminals seeking to engage in low-risk impersonation schemes and provide opportunities for more sophisticated actors to undertake high-impact fraudulent schemes.

- Currently, the most effective use of voice cloning technologies is in generating one-time samples that can be used in extortion scams, disinformation, or executive impersonation. Limitations to the use of voice cloning technologies, especially for enabling real-time, extended conversations and generating prompts in languages other than English, mean that extensive planning is required for fraudulent operations with a higher impact.
- Threat actors have begun to monetize voice cloning services, including developing their own cloning tools that are available for purchase on Telegram, and the emergence of voice-cloning-as-a-service (VCaaS).
- Public interest in AI, including voice cloning technology, has prompted an interest on dark web and special-access sources in AI platforms' potential for abuse. Threat actors are also interested in leveraging multiple AI platforms in concert, thus enabling the convergence of AI threats. However, not all threat actors are confident in their ability to leverage such platforms in their current state — threat actors that do not have an expert grasp of the English language may have the greatest hesitation about using these new technologies.
- In order to mitigate current and future threats, organizations must address the risks associated with voice cloning while such technologies are in their infancy. As these technologies will only get better over time, an industry-wide approach is required immediately in order to preempt further threats from future advances in voice cloning technology.

Voice Cloning

Voice Cloning and Cybercrime

According to a March 20, 2023, blog post from the US Federal Trade Commission (FTC), the genesis of the "fake AI problem" and rise of "synthetic media" created by AI platforms — including voice cloning technology — enables fraudulent actors to "generate realistic but fake content quickly and cheaply, disseminating it to large groups or targeting certain communities or specific individuals". The FTC further argues that "[fraudulent actors] can use deepfakes and voice clones to facilitate imposter scams, extortion, and financial fraud". The post continues by stating that "these new AI tools carry with them a host of other serious concerns, such as potential harms to children, teens, and other populations at risk when interacting with or subject to these tools".

Research using the Recorded Future® Intelligence Cloud surfaces references to the use of voice cloning technology by cybercriminals, dating back to January 1, 2015, on the low-tier Fraudws Forum. These early references do not include the discussion of AI, but rather the use of voice-changing software. Voice-changing software distorts the voice of a threat actor in real-time, whereas voice cloning software "spoofs" a target's identity by creating a unique sample. The first reference to voice cloning as a novel attack vector is on August 24, 2019, in a thread authored by "Mister_X" on the top-tier Russian-language cybercriminal forum XSS.

Conversations related to voice cloning as an attack vector continued to evolve in September 2019. These discussions are primarily concerned with the use of voice cloning technology leveraged in tandem with other tactics — such as caller ID spoofing, automated call ("robocall", "dialing") campaigns,

and vishing. These conversations do not evolve into discussing the use of voice cloning as a stand-alone tool for enabling scams until early 2022, amid the global rise in interest about AI.

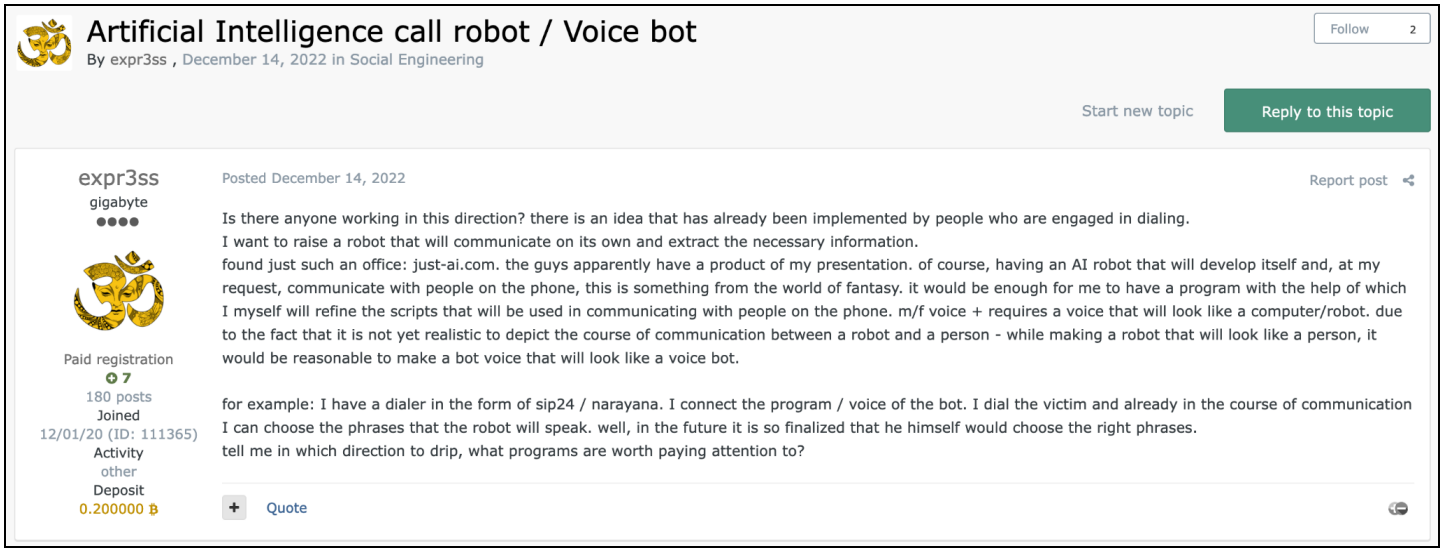


***Figure 1**: "expr3ss" inquiring about the use of AI "voice bots" in criminal "dialing" software (Source: Recorded Future)*

Dark Web Chatter

Threat actors are divided in their optimism over the potential for leveraging voice cloning technology to enable scams. Common concerns expressed on dark web and special-access sources include: procuring access to premium platform accounts while located in the Commonwealth of Independent States (CIS), efficiently utilizing voice cloning technology as a non-native English speaker, and cloning the voices of targets in languages other than English. These concerns have led to the rise of VCaaS, a new form of commodified cybercrime in which voice cloning "specialists" provide tailored voice cloning samples, often advertising their services via Telegram. Several threat actors who have provided such services — such as "DeepFakeSpace" — have since been banned on dark web and special-access sources pending active arbitration cases, due to customer complaints over the perceived lack in voice cloning quality relative to price ($1,000 or more).

Unlike with other forms of AI technology — such as deepfake video technology or LLM chatbots (such as ChatGPT) — threat actors are reluctant to share POC materials related to voice cloning. This may be due to a perceived threat to operational security (OPSEC) in sharing such samples, as many platforms — such as ElevenLabs — prohibit the use of their technology in creating malicious content. These platforms claim to possess the data necessary to identify accounts that have produced malicious content, including payment card data related to the identity of the account owner. This potential law enforcement exposure leads to threat actor trepidation but also (paradoxically) a rise in references to the sale of compromised premium ("paid") accounts on such platforms.

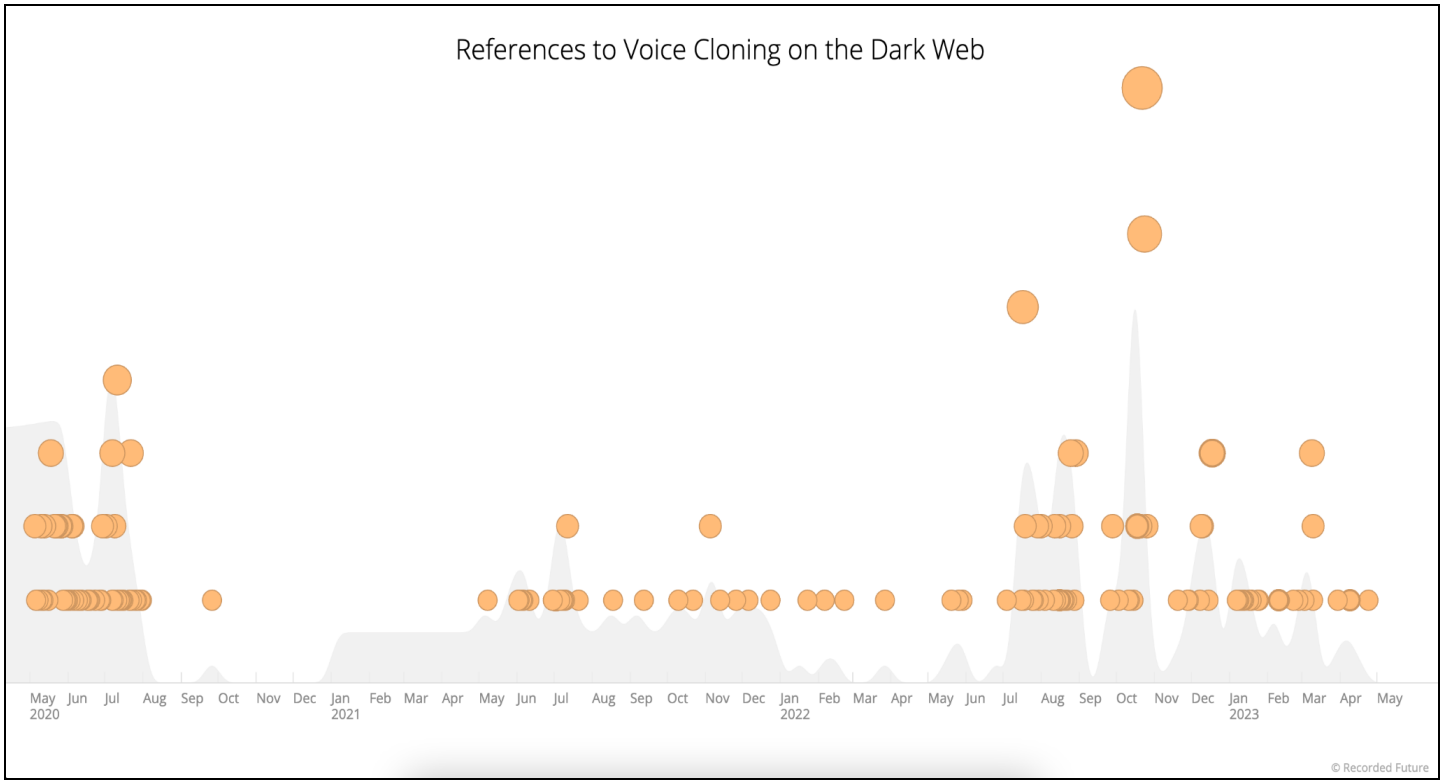


***Figure 2**: References to voice cloning on dark web sources from May 2020 to May 2023 (Source: Recorded Future)*

ElevenLabs's AI Speech Software

In January 2022, ElevenLabs became the subject of attention from journalists and cybersecurity researchers following a series of deepfake voice cloning videos shared on social media, primarily by users of the imageboard website 4chan. These videos were offensive in nature, using the voices of high-profile public figures to create hateful content such as "a generated voice that sounds like actor Emma Watson reads a section of Mein Kampf". This attention has spilled over into the cybercriminal world, prompting several discussions of the platform on dark web sources including the now-defunct English-language forum BreachForums.

According to its official website, ElevenLabs markets itself as "the most realistic and versatile AI speech software, ever". ElevenLabs contains several options for modifying synthetic stock voices to enable text-to-speech translation. In addition to these proprietary voices, premium users can also upload "custom" samples. While these custom samples are intended to be in the voice of the users themselves — with the purpose of using one's own voice to create unique content at scale — threat actors have instead opted to abuse this option by uploading voices of public figures. While this behavior is explicitly prohibited by the ElevenLabs community standards, Insikt Group analysts were able to upload voice samples of English-speaking celebrities, politicians, and executives without issue. Following the widespread abuse of ElevenLabs, its community standards were updated to restrict the use of custom voices to paid users. While this does not mitigate risk entirely, it is a positive change made by ElevenLabs. However, as mentioned earlier, it has led to an increase in references to threat actors

selling paid accounts to ElevenLabs — as well as advertising VCaaS offerings. These new restrictions have opened the door for a new form of commodified cybercrime that needs to be addressed in a multilayered way.

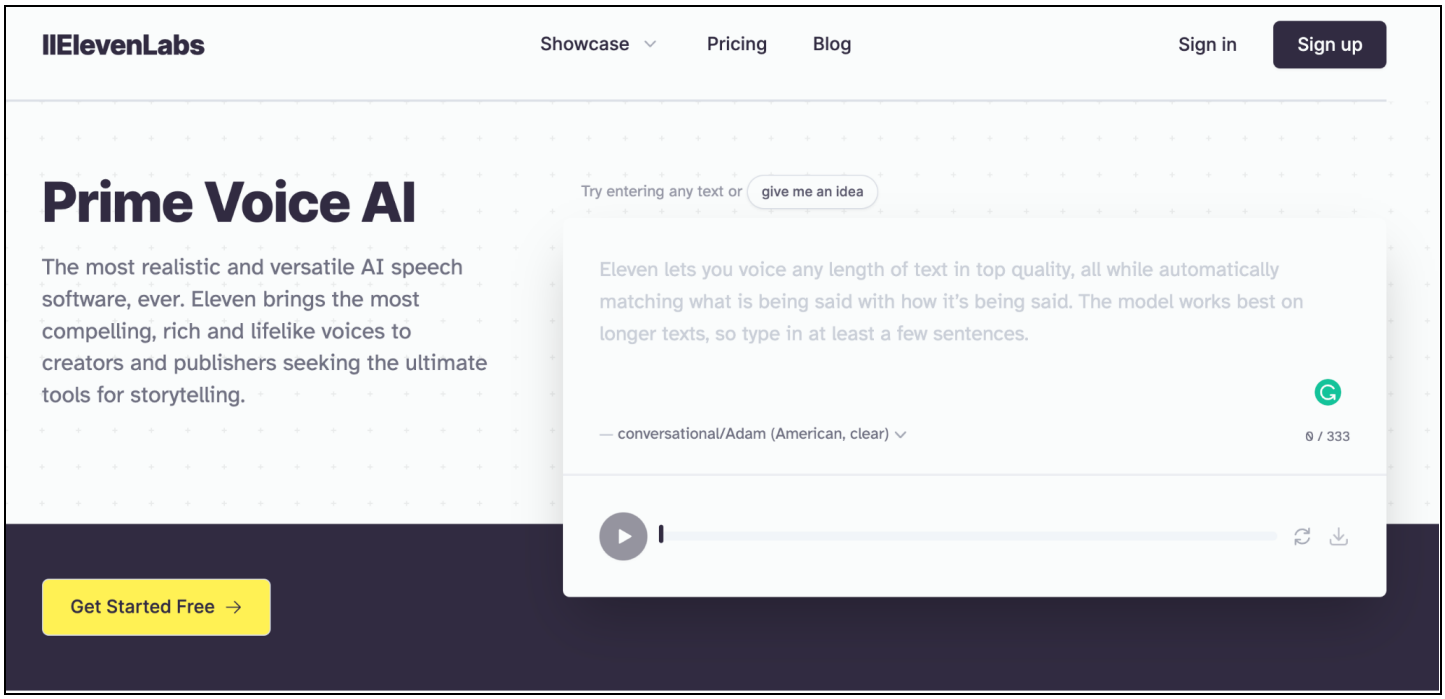


***Figure 3**: The login page for ElevenLabs's text-to-speech platform (Source: ElevenLabs)*

ElevenLabs Goes Viral

Following the announcement of ElevenLabs's updated community standards — which sought to deter users from abusing its "custom" samples feature — much of the viral content involving the use of ElevenLabs's voice cloning technology shifted from offensive to comedic in nature. Social media users — especially on 4chan and Reddit — accused ElevenLabs of "killing their fun" and bowing to "outrage culture". This paradigmatic shift in the use of ElevenLabs has resulted in a number of viral memes, which often include public figures — such as Joe Biden, Joe Rogan, or Jordan Peterson — discussing nonsensical topics (see Figure 4). Some of these memes are subtly political in nature, but do not cross a line that would be considered abuse.

Increased restrictions on ElevenLabs have fueled a desire on dark web and special-access sources to seek alternative voice cloning platforms with more relaxed terms of service that do not require user identification or payment card data to unlock their features. Similar to what has happened since the release of ChatGPT, increased scrutiny and moderation has led to interest among cybercriminals in "jailbreaking" ElevenLabs to circumvent content restrictions. Threat actors have also begun inquiring about ElevenLabs alternatives on dark web and special-access sources — preferably ones that are 100% free to use or anonymous. This has led to a rise in third-party voice cloning services — which are often managed via Telegram or Discord (for example, "Zombie Voice" and "Silero") — and the

emergence of open-source voice cloning software on social media and code repositories. However, alternatives to ElevenLabs, much like those imitating ChatGPT, have drawbacks for cybercriminals.

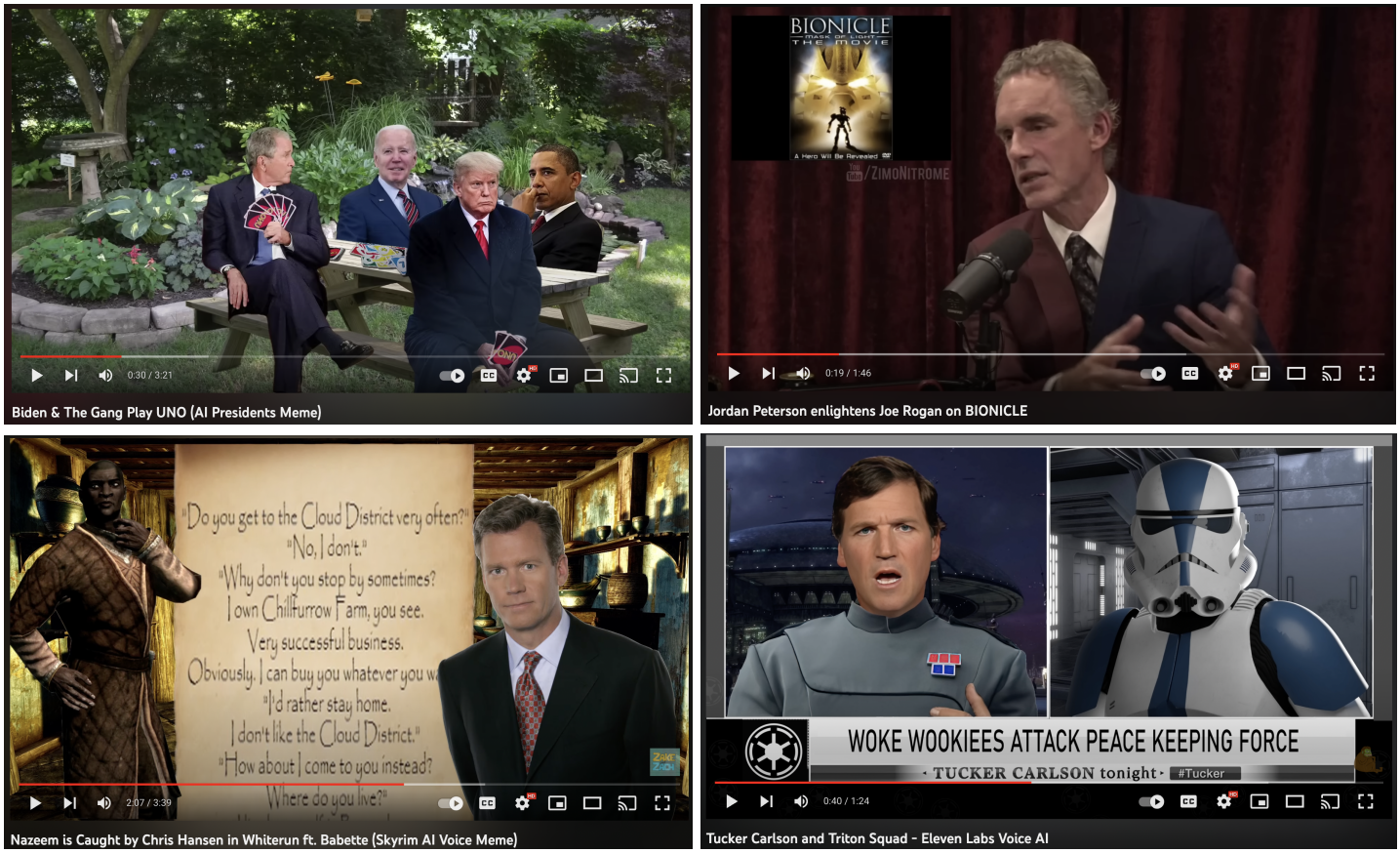


***Figure 4**: Popular examples of "ElevenLabs" memes (Source: YouTube)*

Voice Cloning Alternatives

Restrictions on the abuse of ElevenLabs has fueled an interest in third-party voice cloning platforms that are anonymous, free to use, and have more relaxed community standards. These platforms are less popular online than ElevenLabs and come with drawbacks, which we will discuss later. Some of the most common examples of third-party voice cloning platforms that are discussed on dark web and special-access sources.

Many of these platforms may market themselves as voice cloning services intended for use in audio book voiceovers, film and television dubbing, voice acting, advertising, and other legitimate settings. And in many cases, the use of these platforms for legitimate purposes by enterprises outweighs their malicious use by cybercriminals. However, it is likely that criminals are abusing these platforms, as evidenced by dark web chatter.

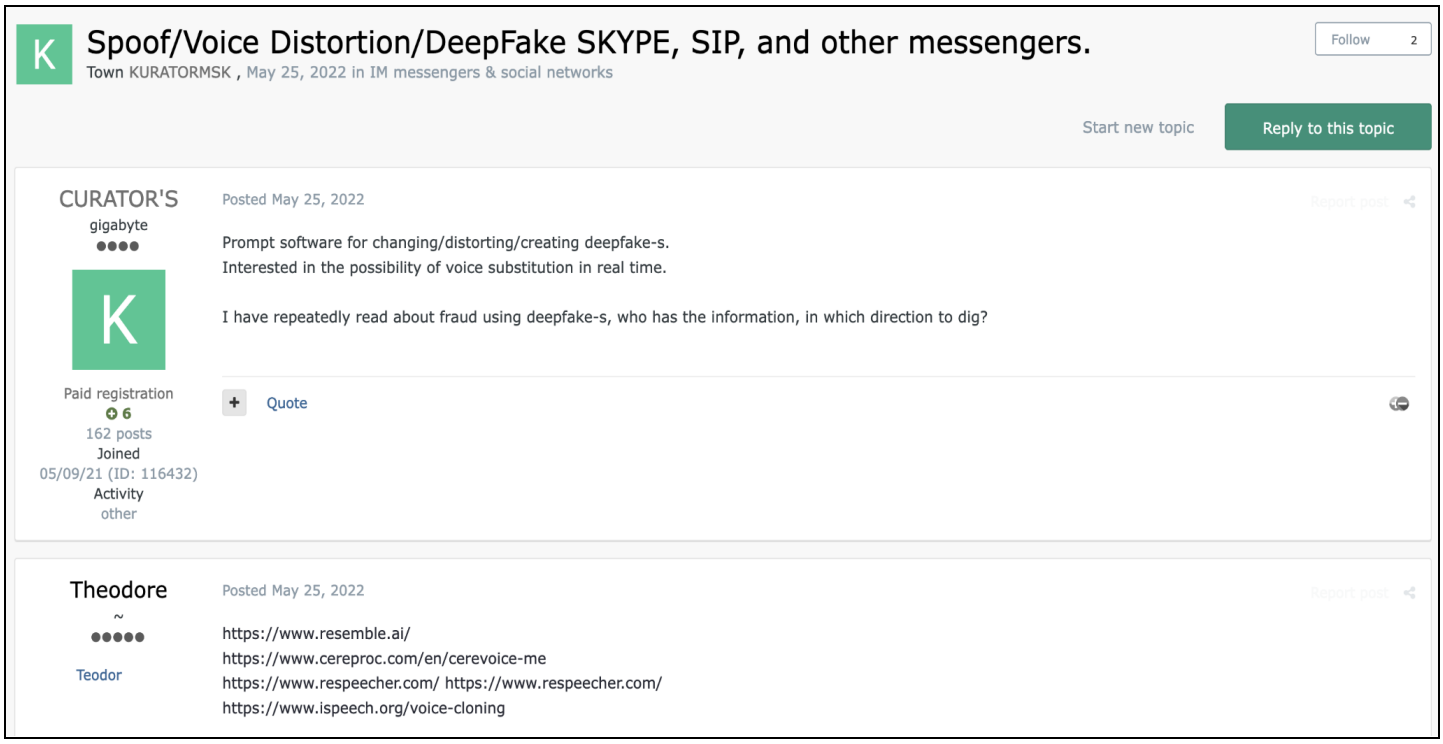


***Figure 5**: "KURATORMSK" crowdsourcing ideas for deepfake voice cloning platforms (Source: Recorded Future)*

Benefits and Drawbacks

According to dark web chatter, there are several purported "benefits" of leveraging third-party voice cloning technologies instead of ElevenLabs. Many of these claims are made by threat actors advertising their own platforms, as well as threat actors who cannot procure access to legitimate ElevenLabs accounts. Therefore, such claims must be evaluated in this context. For example, threat actors have endorsed alternative programs for their "English accent", or Resemble AI for its perceived quality. These platforms are often listed by threat actors in concert with many other open-source or "freemium" AI technologies such as deepfake video technology, generative art and text-to-image (T2I; TTI) software, text-to-video (T2V; TTV) software, and more. As mentioned earlier, these lists and tutorials in part represent the "convergence of AI threats", by which threat actors are seeking to capitalize on a public interest in AI and leverage multiple platforms at once to enable cybercriminal campaigns.

But these third-party platforms also come with drawbacks. We analyzed online samples associated with some of the tools listed above and found that there is a significant drop in custom voice sample quality relative to the quality of ElevenLabs's samples, including in these platforms' "proprietary voices", which are more robotic and unnatural than those produced by ElevenLabs. Many of these platforms — especially including those that are managed entirely via Telegram — are not user-friendly and are more time-consuming than their browser- or client-based counterparts. There are additional limitations on the diversity of proprietary voices and support for languages other than English. For instance, ElevenLabs is capable of cloning voices in Spanish, Portuguese, German, Polish, Hindi, and more while the platforms listed above are largely restricted to English with a British accent, by default. The more

reputable voice cloning platforms that are used by major enterprises, such as Play.ht, also have a higher financial barrier for entry than ElevenLabs.

Threat Analysis

Banking Fraud

In a February 23, 2023, Vice article, technology journalist Joseph Cox was able to break into his bank account using a voice sample generated by ElevenLabs, providing him "access to the account information, including balances and a list of recent transactions and transfers". Cox was able to trick "Voice ID," a voice-based MFA software used by a bank. According to Cox, he recorded a 5-minute sample of his voice using a pre-prepared prompt, downloaded the recordings — including a clone of him stating "my voice is my password" — and played them back over speakerphone to the automated bank helpline.

Voice-based authentication is a common authentication method and security measure implemented by banks that have automated helplines. There are a number of different companies that provide such a service to financial institutions located in the US, UK, Canada, and the broader English-speaking world.

There are limitations to the use of voice cloning for the purpose of banking fraud. For example, voice cloning cannot yet be done in real-time. It requires a user to pre-record anticipated responses to common prompts implemented by automated banking services. If a cybercriminal were to encounter a live human representative, use of the voice cloning to initiate fraud would become much more difficult. In addition, the use of alternative or secondary forms of authentication — such as a complex password, PIN number, Social Security number (SSN), SMS authentication, recovery email account access, a hardware key, and so on — makes voice cloning difficult, if not impossible, to leverage as a sole attack vector.

There are also pending legal hurdles to implementing voice-based authentication that may signal a future shift away from the technology and its use by financial institutions. In a September 13, 2022 Bloomberg article, class action lawsuits were filed in federal courts alleging that the use of voice-based authentication violates the California Invasion of Privacy Act because the collection and storage of biometric data for authentication is often done without the consent of the user. As evidenced by the experiment conducted by Joseph Cox, this form of authentication is also easily defeated through the use of voice cloning tools like ElevenLabs, making it an impractical, if not dangerous authentication method with a broad risk surface.

Disinformation

Voice cloning technology can be used to spread disinformation by creating realistic audio recordings of public figures appearing to say things they never actually said. This can be done by training a voice cloning algorithm with a sufficient amount of audio data from the targeted individual and then

generating a new audio clip with the same voice and tone. Once these audio clips are created, they can be used to create fake news reports, manipulate audio, or spread disinformation through social media platforms. The resulting audio can be made to sound incredibly realistic, making it difficult for listeners to distinguish between what is real and what is fake. This technology can be particularly dangerous in the context of political campaigns or national emergencies.

In January 2023, social media users manipulated a speech by President Joe Blden about the war to make it appear as though President Biden gave a talk attacking transgender people. ElevenLabs's beta version was used in creating the doctored version, and although the quality of the sound in the resulting video was likely not high enough to convince most social media users, the popularity of the doctored video contributed to the increased usage of ElevenLabs's voice-cloning technology to spread misinformation, even in "humorous" forms. Within the first month of ElevenLabs's beta tool being launched, it was used to create audio samples to spread disinformation and inflict reputational damage to high-visibility individuals. Examples included fake clips of Bill Gates purportedly saying that COVID-19 vaccine causes AIDS, actress Emma Watson reading Adolf Hitler's "Mein Kampf", and Hillary Clinton supposedly repeating the same transphobic text used in the Biden clip.

In addition to reputational damage to individuals, doctored audio clips can be used to inflict reputational damage to companies and institutions with potential financial impact. Hany Farid, a professor at the University of California, Berkeley, warns against scenarios where the stock market could be manipulated by fake audio-clips of CEOs saying that their company's profits are down. Fake voice samples that contain negative sentiments by reputable individuals within a company can be used to jeopardize investors' confidence, therefore decreasing the value of the company's stock. This method can be weaponized by fraudulent actors to further already-existing impersonation schemes and commit investment fraud by feeding investors fake information to plummet the price of a stock and then buying the shares themselves at the artificially low price.

AI Music and Copyright Infringement

Voice cloning technology can enable copyright infringement in the creation of AI music by allowing an AI system to produce music that closely mimics the style and sound of an existing artist, without their permission or involvement. This can be done by training an AI system with a large data set of music created by the targeted artist and then generating new music that imitates their style. While this technology has the potential to revolutionize the music industry by enabling the creation of new music with minimal human input, it can also lead to copyright infringement if the generated music is too similar to existing songs. For example, if an AI system is trained to produce music in the style of a particular artist — such as Drake and The Weeknd — and the resulting music sounds almost identical to an existing song, this could be considered copyright infringement if the original artist or record label did not give permission for the use of their work. As AI music continues to gain popularity, it is important for organizations to be aware of the potential copyright implications and take steps to ensure that they are not infringing on the rights of existing artists. This can include using original compositions, obtaining permission from artists and record labels, and conducting regular audits of AI-generated music to ensure that it is not too similar to existing works.

Family Emergency Scams

A family emergency scam is a type of fraud where the scammer poses as a family member or friend in need of urgent financial assistance due to an emergency. In addition to purported family members or friends asking for financial help, scammers also involve fake authority figures, such as a law enforcement officer, lawyer, or doctor, to make the lure more convincing and scare the victim. In an escalation of this method, scammers have been observed using voice cloning technology to replicate the voices of victim's loved ones. In addition to the 9 premade voices offered by ElevenLabs, users with the Starter+ subscription model can upload 1-minute-long voice samples to generate new "voices" in the platform, which can then be used in family emergency scams to make the fraudulent call more believable.

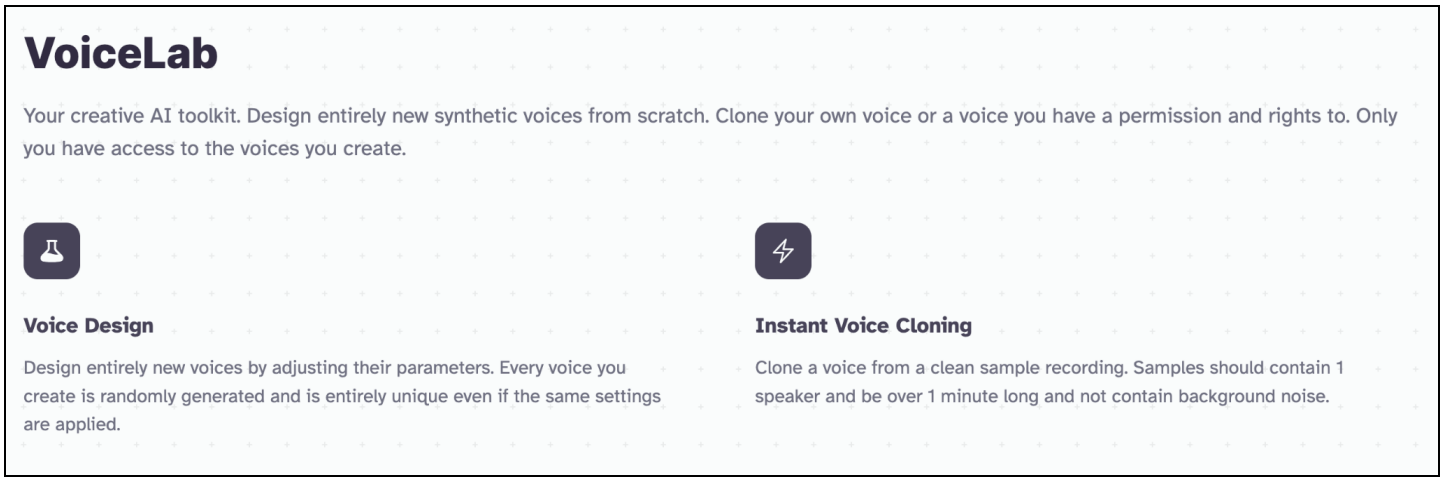


***Figure 6**: ElevenLabs's "freemium" options (prior to their updated community standards), which allowed free users to generate 3 new voices, including by cloning a voice from an audio sample (Source: ElevenLabs)*

Executive Impersonation

From 2019 to 2023, there have been multiple high-profile scams where scammers used voice-cloning technology to impersonate high level executives' voices and defraud enterprises and banking institutions. In early 2020, scammers used voice cloning technology to impersonate the director of a company to contact a banking manager in Hong Kong and request that the manager authorize transfers amounting to approximately $35 million for what they claimed was an acquisition the company was making. In March 2019, scammers impersonated the voice of a chief executive to demand a fraudulent transfer of €220,000 ($243,000) from the chief executive officer (CEO) of a UK-based energy firm.

Over the past year, we have continued to monitor a pair of Russian comedians and pranksters whose activity often aligns with the interests of the Russian state. Russian comedians Vladimir Kuznetsov and Aleksei Stolyarov, more popularly known as "Vovan" and "Lexus", have leveraged their presence on multiple social media platforms to promote their efforts to use phishing emails or other social engineering methods to target persons of interest who have spoken out about the Russian state. The

aim of their efforts is to trick targets into participating in recorded phone calls or video chats in an attempt to embarrass them. In 2021, Vovan and Lexus masqueraded as Leonid Volkov, a politician who served as chief of staff for Alexei Navalny's campaign for the 2018 Russian presidential election, in order to engage with and trick British and Baltic MPs. In response to this event, government officials have publicly stated that the duo relies upon deepfake technology to support these efforts, though the duo have denied this. Regardless, this reporting highlights the concern and mistrust deepfakes can generate within communications at the international level.

Figure 7: *Comparison of a photo of Leonid Volkov (left) and a Zoom screen capture from a Volkov impersonator (right) (Source: Leonid Volkov's Facebook Profile)*

Callback Scams

A callback scam, also known as Wangiri, is a popular fraud technique used to target both individuals and enterprises. The technique refers to when scammers call victims and disconnect after 1 ring, not intending to connect the call. Instead, the scammers hope that the victim will see the missed call and return the call, in which case the victim will be manipulated into staying on the call for as long as possible, often by being placed on hold. The return call is routed through an international number that consequently accumulates international calling fees, unbeknownst to the victim.

In some versions of the scam, the scammers leave fake voicemails claiming that a popular service the victim is likely to be using, will be canceled due to a security concern or payment failure. Voice cloning technology, like the "freemium" version of ElevenLabs, can be used to bolster these scam efforts since the premade voices offered on the platform are similar to automated voice assistants used by legitimate services on customer support phone lines and other customer-facing communications.

Mitigations

Banking Fraud

- Organizations must implement real-time voice analysis software to detect anomalies in voice recordings and distinguish between real and cloned voices. This can include analyzing voice patterns to detect signs of voice cloning technology.
- Organizations can use anti-spoofing technology, such as “liveness” detection, to prevent fraudulent actors from using pre-recorded or synthetic voices to impersonate customers.
- Organizations can implement biometric authentication with multiple modalities, such as voice and facial recognition or voice and fingerprint recognition, to provide an extra layer of security against voice cloning attacks. This can prevent fraudulent actors from gaining access to accounts even if they have cloned a customer's voice. Voice-based authentication is easily defeated through the use of voice cloning, so multiple biometric modalities need to be implemented in order to make such systems more secure.
- Organizations must train their employees on the risks associated with voice cloning and how to identify suspicious activity related to voice cloning attacks. This can include educating employees on how to recognize and report instances of fraud, as well as providing guidelines on how to verify the identity of customers making requests over the phone.
- Organizations must develop a rapid response plan to address incidents of voice cloning fraud. This plan should include clear guidelines on how to respond to suspected fraud incidents, as well as procedures for customer notification and remediation.

Disinformation

- Organizations should launch or fund public awareness campaigns to educate the general public about the risks and consequences of using voice cloning technology to manipulate public opinion. These campaigns should highlight the potential dangers of voice cloning and the ways in which it can be used to deceive people.
- Organizations should monitor and analyze voice recordings to detect signs of voice cloning technology such as unnatural pauses, inflections, or other abnormalities. They can use open-source or proprietary speech analytics tools to identify anomalies in voice recordings.
- Organizations must implement voice cloning detection and prevention measures, such as machine-learning algorithms and AI, to help identify and prevent the use of voice cloning technology for disinformation. These measures can help detect suspicious activity in real-time, allowing organizations to take action before any damage is done.
- The developers of voice cloning technologies must enforce content moderation policies that prohibit the dissemination of false or misleading information through voice recordings. Content moderation policies can involve setting clear guidelines for what constitutes false or misleading information and implementing significant penalties for individuals who violate these policies.
- Combating the abuse of voice cloning technology for disinformation requires a collaborative effort between various stakeholders including governments, technology companies, civil society

organizations, and the media. The cybersecurity industry must foster collaboration between these stakeholders by promoting information-sharing, supporting collaborative research efforts, and convening multi-stakeholder and public forums to discuss strategies for combating voice cloning technology's use in enabling the spread of disinformation.

AI Music and Copyright Infringement

- Organizations should monitor online content to detect instances of copyrighted material being used without permission, including the use of voice cloning technology to replicate the voice of a copyrighted individual.
- Using AI, organizations can create unique voice signatures for their content creators to make it harder for fraudsters to replicate their voices using voice cloning technology. These signatures can include subtle and unique speech patterns, vocal characteristics, and other elements that are difficult to replicate without the knowledge of the organization and the content creator.
- Organizations can use watermarking technology to embed identifying information into their audio recordings, such as the creator's name or copyright information. This can help deter fraudulent actors from using voice cloning technology to copy and distribute copyrighted material without permission.
- Organizations can educate the public on copyright laws and the risks associated with using voice cloning technology to infringe on copyrighted material. This can include raising awareness about the consequences of copyright infringement and promoting legal alternatives for accessing copyrighted content.

Executive Impersonation

- Organizations must enforce executives' use of MFA, which requires multiple forms of identification to access sensitive information or conduct high-risk transactions.
- Organizations can develop unique voiceprints for their executives to make it harder for fraudulent actors to replicate their voices using voice cloning technology. These voiceprints can be created by analyzing the executives' unique speech patterns, vocal characteristics, and other elements that are difficult to replicate.
- Organizations can educate their employees on the risks associated with voice cloning and how to identify suspicious activity related to executive impersonation. This can include providing guidelines on how to verify the identity of executives making requests over the phone.
- Organizations should monitor communications for signs of executive impersonation, such as unusual requests or behavior. This can include analyzing call logs and email communications on company devices to detect anomalies or suspicious activity. If the activity originates from a device that is not registered to the company or an executive, it is likely an impersonation.

Callback Scams

- Organizations should implement call authentication protocols, such as the "Secure Telephone Identity Revisited" (STIR) and "Signature-based Handling of Asserted information using toKENs"

(SHAKEN) framework, to verify the authenticity of incoming calls. This can help prevent callback scams and other types of fraud that use voice cloning technology to impersonate legitimate callers.
- Organizations should monitor call patterns on company devices to detect instances of callback scams or other types of voice cloning fraud. This can include analyzing call origin, duration, frequency, and other metrics to identify suspicious activity.
- Organizations should use call blocking technology to prevent fraudulent calls from reaching employees and customers. This can include blocking calls from known fraudsters or using automated systems to screen incoming calls.

Social Engineering and Family Emergency Scams

- Engage callers in conversation. Since voice cloning cannot be used in real-time, you should ask specific questions related to the caller's personal information or other unique data points to verify their identity before providing access to sensitive information or services.
- Limit the amount of sensitive information disclosed over the phone. When in doubt, hang up the phone and call the family member from a known phone number, or reach out to other people in your family or social circle to verify the emergency.
- Organizations can establish emergency contact verification protocols to confirm the identity of family members who are calling on behalf of employees or customers in emergency situations.

Outlook

As stated in our January 26, 2023, report “I, Chatbot”, open-source and “freemium” AI platforms are now in their infancy, but their quality will only improve over time. These technologies are in a state of constant development and are often trained on user input. The more they are used and abused, the more effective they will be in enabling cybercrime. In order to mitigate risk impact now and in the future, organizations must adopt a multilayered risk mitigation strategy that encompasses education, detection, and the development of defensive tools. In order to defeat AI, an organization must leverage AI. According to Lisa O’Connor of Accenture, in an interview with IT Brew, we need to develop “a good way to focus how we spend defensive dollars”.

The outlook for voice cloning and its use in banking fraud, disinformation, social engineering, copyright infringement, and more is bleak — if we do not immediately adopt an industry-wide approach to mitigating associated risks. Risk mitigation strategies need to be multidisciplinary, addressing the root causes of social engineering, phishing and vishing, disinformation, and more. Voice cloning technology is still leveraged by humans with specific intentions — it does not conduct attacks on its own. Therefore, adopting a framework that educates employees, users, and customers about the threats it poses will be more effective in the short-term than fighting abuse of the technology itself — which should be a long-term strategic goal.

Recorded Future®

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture