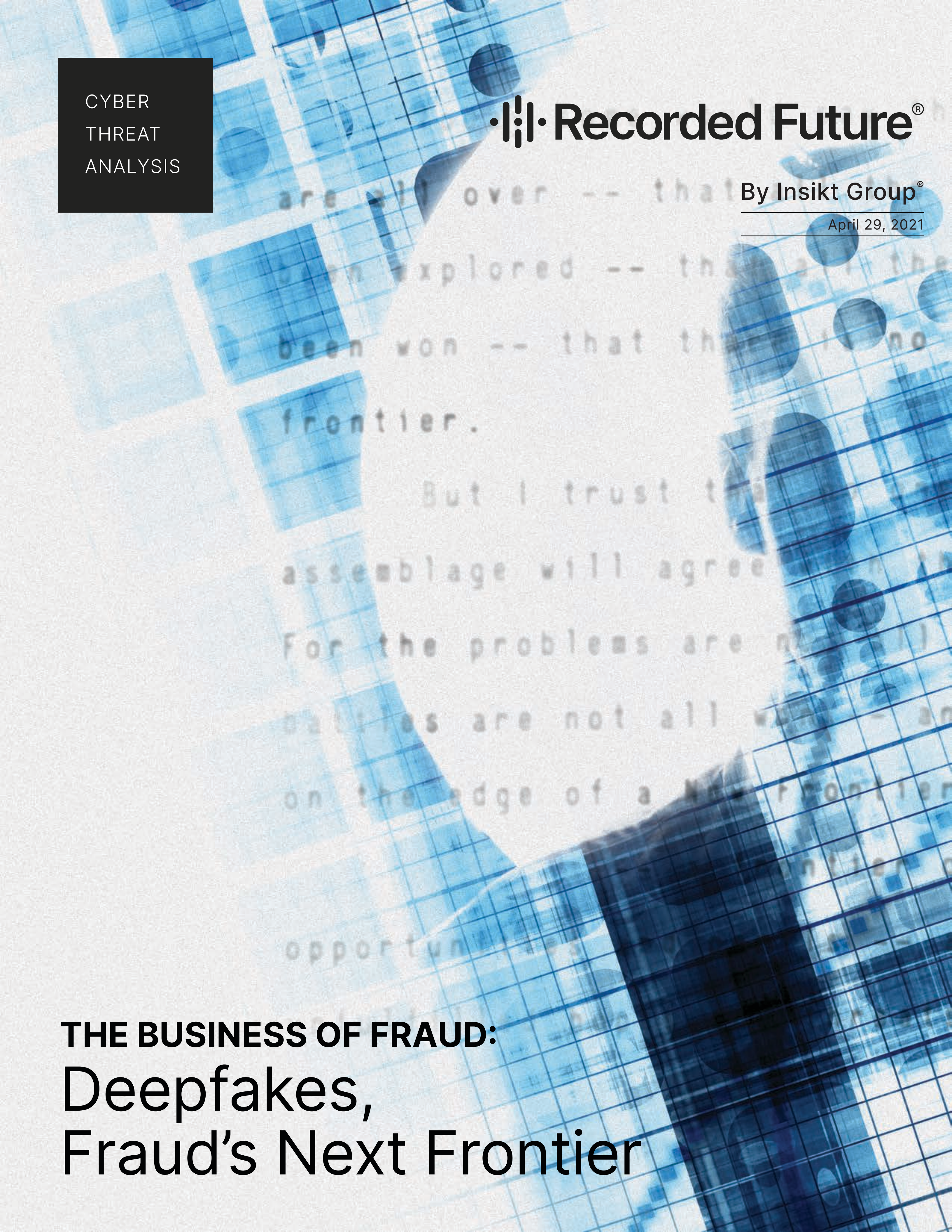


CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

April 29, 2021

THE BUSINESS OF FRAUD: Deepfakes, Fraud's Next Frontier

CYBER THREAT ANALYSIS

Recorded Future analyzed data from the Recorded Future® Platform, dark web, information security reporting, and other open-source intelligence (OSINT) sources to identify the use and prevalence of how threat actors are attempting to advertise, discuss, sell, and purchase deepfake-related services and products that facilitate fraudulent activities. In this report, we define deepfakes as synthetically generated visual and audio content that is being used offensively to target individuals, companies, and security systems. This report is part of our series on the business of fraud.

Executive Summary

Threat actors have begun to use dark web sources to offer customized services and tutorials that incorporate visual and audio deepfake technologies designed to bypass and defeat security measures. Furthermore, threat actors are using these sources, as well as many clearnet sources such as forums and messengers, to share tools, best practices, and advancements in deepfake techniques and technologies. As reported by Insikt Group's Criminal and Underground Team throughout 2020, threat actors are developing customized deepfake products. We believe they will continue to develop these products, as the demand is likely to increase due to corporations incorporating visual and audio recognition technologies into their security measures. Within the next few years, both criminal and nation-state threat actors involved in disinformation and influence operations will likely gravitate towards deepfakes, as online media consumption shifts more into "seeing is believing" and the bet that a proportion of the online community will continue to be susceptible to false or misleading information.

Key Judgments

- Deepfake technology used maliciously has migrated away from the creation of pornographic-related content to more sophisticated targeting that incorporates security bypassing and releasing misinformation and disinformation. Publicly available examples of criminals successfully using visual and audio deepfakes highlights the potential for all types of fraud or crime, including blackmail, identity theft, and social engineering.
- English- and Russian-language dark web forums were identified as the main sources for users to advertise, discuss, share, and purchase deepfake-related products, services, and topics. The most widely used forums were found to be low- to mid-tier forums that have lower barriers to entry, but activities were also found on high-tier forums. Deepfake topics were also identified on Turkish-, Spanish-, and Chinese-language forums.
- The most common deepfake-related topics on dark web forums included services (editing videos and pictures), how-to methods and lessons, requests for best practices, sharing free software downloads and photo generators, general interests in deepfakes, and announcements on advancements in deepfake technologies.
- There is a strong clearnet presence and interest in deepfake technology, consisting of open-source deepfake tools, dedicated forums, and discussions on popular messenger applications such as Telegram and Discord.
- Discussion on most publicly available forums and messengers relating to deepfakes surrounds the education and genuine interest in deepfake technology, in addition to users sharing content and refining their craft, in line with discussions identified on closed dark web sources. In the future, we believe that this otherwise relatively benign community can serve as a basis for individuals to venture into illicit criminal activity using learned deepfake skills.

Background

Deepfakes are digitally altered images that use machine learning algorithms and frameworks, specifically generative adversarial networks (GAN), and artificial intelligence to replace authentic images with fake ones. Academic research into photo and video modifications has been around since the late twentieth century, but as technologies have advanced and become commoditized, deepfake software and applications are now widely available for amateur and recreational uses. The term deepfake was first used in November 2017 on the popular social aggregate website Reddit by a user named "deepfakes", administrator and creator of the subreddit "r/deepfake", who released videos of celebrities' faces being replaced. In some cases, r/deepfake users began posting nude and sexually graphic images which lead to the subreddit being banned in February 2018 for violating Reddit's policies. As deepfake technologies and techniques became available, deepfake users began to create face-altering applications (apps), such as FakeApp (launched in January 2018), as well as apps that removed one's clothing, such as DeepNude (launched in June 2018). This combination of deepfake sexually explicit videos with clothing removal apps drove users to target women and create "revenge porn" that migrated away from celebrities and targeted primarily women:

- In a December 2019 report, the Netherlands-based company Deeptrace that specializes in deepfake detections found at least 8,000 deepfake videos that involved nude women. By November 2019, the number had risen to at least 14,678.
- In October 2020, Sensity AI, a research company that tracks online videos, released a report on the discovery of a new deepfake image network on Telegram. This network uses pix2pix GAN to teach the system to digitally strip a picture of a clothed woman and produce a nude version of the image. Overall, the network contained 7 Telegram channels with over 100,000 members across the channels and was cross advertised on VKontakte (VK), a Russian social media platform. At the end of July 2019 (the end of Sensity's research period), at least 104,852 women had been targeted by the deepfake network.
- In February 2021, an open source reported that Sensity AI identified 90% to 95% of deepfake videos posted online were pornographic, with about 90% of these involving women and likely created without their consent. As of January 2021, the company reported that the number of deepfake videos posted online has doubled every 2 months since 2018. The company has detected an estimated 85,047 deepfake videos.

As identified by Recorded Future in previous investigations, we have observed threat actors and cybercriminals being early adopters and users of new technologies, thinking of ways to leverage them for fraudulent and criminal purposes. Beyond the above-referenced deepfake nudity-related content, the following list outlines several real-world events in which deepfake technologies have been used to facilitate crime or cause political instability or confusion:

- In April 2019, an open source reported that a UK-based energy company was targeted by criminals using a deepfake-generated voice that mimicked the company's CEO. The criminals requested a transfer of $243,000 USD from the company's parent company in Germany to a subsidiary in Hungary. The funds were transferred to a Hungarian bank, which then were sent to a bank located in Mexico. The report indicates that fraudsters used similar tactics used in phishing and business email compromised (BEC) attacks, including urgency and executive orders.
- In June 2019, an open source reported that a deepfake video was publicly released that involved a Malaysian political aide allegedly engaging in a sexual act with a senior cabinet member. This resulted in calls for an investigation into corruption, causing destabilization among coalition government members.
- In December 2018, the government of the African nation Gabon released a video of President Ali Bongo speaking about his health and recovery in Saudi Arabia following a stroke he suffered in August 2018. The video was described, but not proven, as a deepfake, with Gabonese citizens finding it suspicious that President Bongo appeared healthy. The video is described as being one of the reasons used by the opposition to attempt a coup on January 6, 2019. This demonstrates that the concept of deepfakes has penetrated the global zeitgeist to such an extent that just the suggestion of the use of a deepfake can have significant real-world ramifications.

Another event occurred in March 2020 where threat actors targeted a Philadelphia-based lawyer by impersonating the lawyer's son. Despite no deepfake-generated voice of the son being definitively linked to this event, the event has all the hallmarks of a deepfake voice attack: impersonation of the son's voice (purportedly involved in an accident that injured a pregnant woman, which resulted in his arrest and request for $9,000 in bail money) that included the same cadences and commonly used words as well as an urgent demand to wire money quickly.

These events ,coupled with deepfake's successes in generating convincing images of nude women ,highlight the visual and auditory potentials of applying deepfakes .It also highlights the potential for all types of fraud or crime ,including blackmail ,identity theft ,and social engineering ,to benefit from deepfake technology .As highlighted in a February2021 interview ,the COVID 19-pandemic has sped up the need for video and facial recognition securities for two-factor2) FA (and multi-factor) MFA (authentications ,particularly for financial and medical institutions .Financial institutions have stated their concerns on deepfake technologies ,with the biggest fear being online payments and personal banking being most impacted by deepfake images capable of defeating facial recognition defenses.

Threat Analysis

In our report series on automation and commoditization in the criminal underground published throughout 2020, Insikt Group investigated and identified that dark web threat actors are advertising and developing customized, automated tools that are user-friendly and have an array of capabilities. We examined our data sets and open-source reporting to identify how deepfakes are being discussed, what kinds of deepfake-related products and services are being offered, what are the most widely used sources, and major threat actors focused on advertising products and services.

Based on our findings and due to the commoditization of deepfake software and technologies, we believe that threat actors have begun to advertise customized deepfake services that are directed at threat actors interested in bypassing security measures and to facilitate fraudulent activities, specifically fake voices and facial recognition.

Deepfakes and Dark Web Sources

Our research found the following themes and trends of how deepfake technologies were being discussed and advertised across dark web sources from August 1, 2019 to January 31, 2021:

- An increase in dark web source activities on deepfake-related topics began around August 2019, with users taking an interest in editing images and videos (nude women) as well as general knowledge. Beginning in the spring and summer of 2020, we began to see more dark web discussions on deepfake's fraudulent potentials and successes, enhancements in deepfake technologies, and advertisements for customized deepfake-related services.
- Dark web forums (English and Russian languages) were identified as the main sources for users to advertise, discuss, share, and purchase deepfake-related products, services, and topics. The most widely used forums were found to be low- to mid-tier forums that have lower barriers to entry, but activities were also found on high-tier forums. Deepfake topics were also identified on Turkish-, Spanish-, and Chinese-language forums.
- The most common deepfake-related topics on dark web forums included services (editing videos and pictures), how-to methods and lessons, requests for best applications and practices, sharing of free software downloads and photo generators, general interests in deepfakes, and announcements on advancements in deepfake technologies.

Dark Web Forums

The following forums contain the most activities around deepfake-related discussions, from greatest to least: Nulled, Raid Forums, Cracked, Hack Forums, and BlackHatWorld. We identified that deepfake-related forum activities began to increase around August 2019, with a majority of discussion centered around the following themes: deepfake applications and updates, threat actor services, requests for services, sharing of free software that performs deepfakes, and open-source reporting on the technologies capabilities.

We assess that there is not a definitive moment or event that caused this increase; rather, deepfake technology has continued to be discussed by threat actors due to it becoming more common across the internet and media sources, with the conversations focusing on the difficulties of detecting deepfakes, the technology's improvements and applications (for security), and publicly known successes of criminals using deepfake for fraudulent purposes.

One of the major themes identified across dark web forums was threat actors advertising deepfake-related services. In June 2020, the threat actor "skidhackz" authored a forum thread on Hack Forums that detailed their deepfake video services, which included video editing and manipulation. The threat actor requested that an interested buyer supply at least 1,000 photos of the target to maximize authenticity (containing a variety of angles, colorations, facial expressions, and so on) and high-definition video that is at least 540p. The threat actor offered their services for $20 per minute (final video duration) and provided a sample that included a before and after video edit, with the latter using deepfake that incorporated the actress Margot Robbie, which can be seen in Figure 2 below.

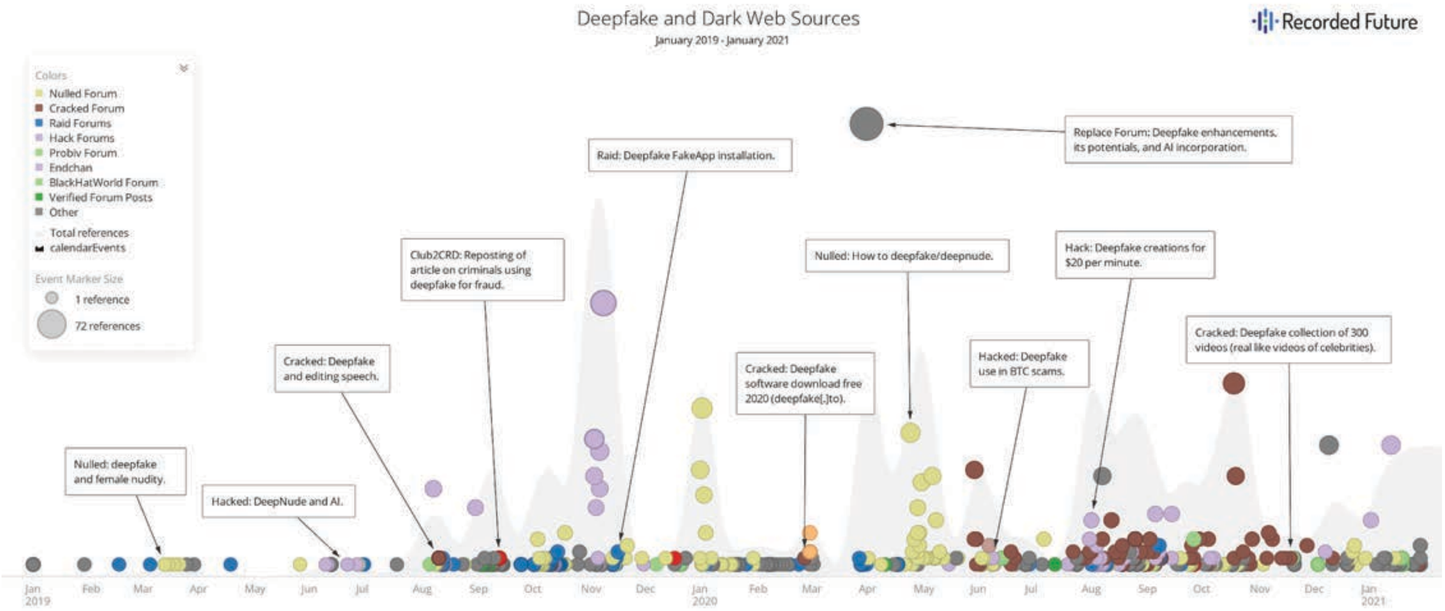
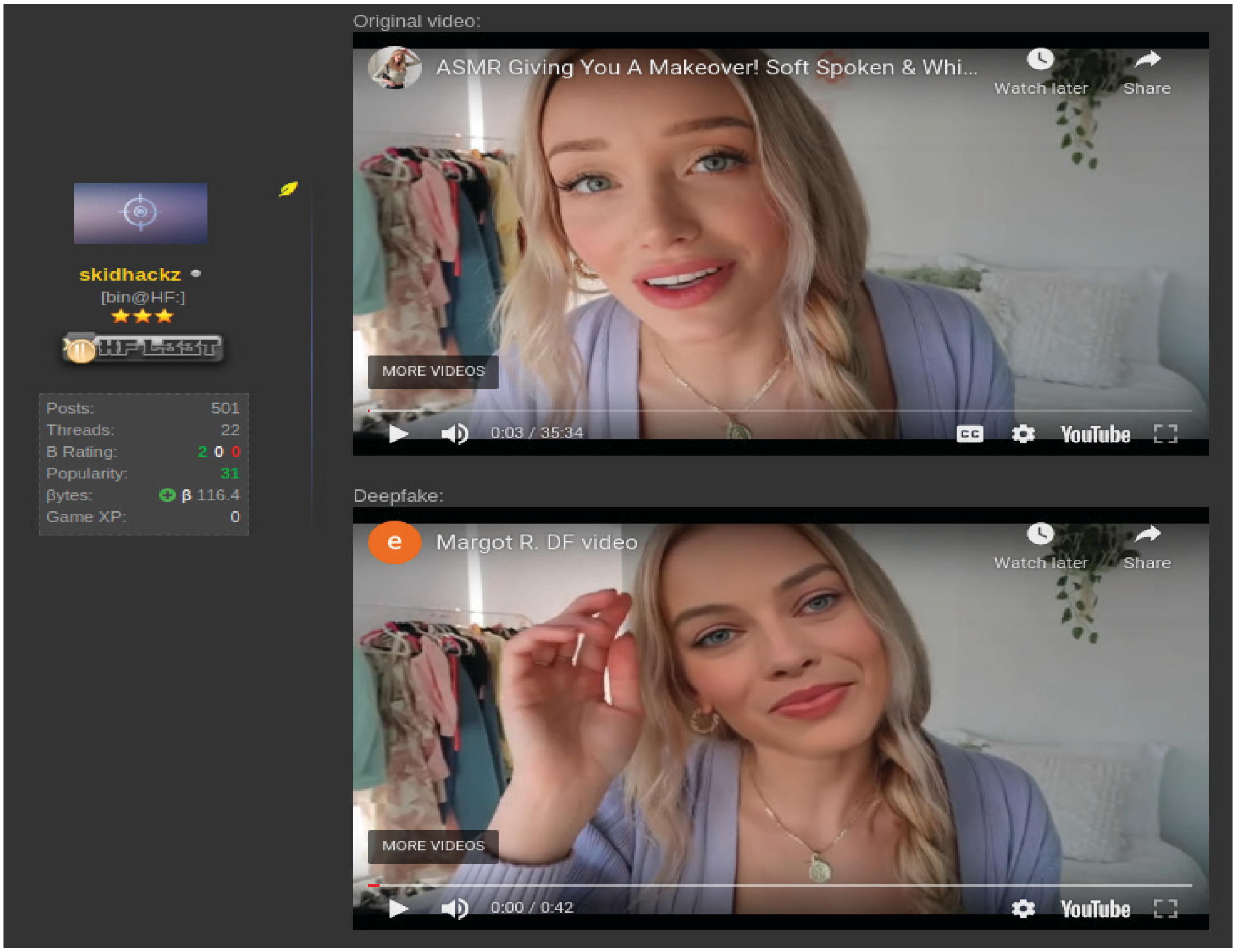


Figure 1: Deepfake activities across dark web sources (Source: Recorded Future)



skidhackz
[bin@HF:]
HF L33T

Posts:	501
Threads:	22
B Rating:	2 0 0
Popularity:	31
βytes:	β 116.4
Game XP:	0

Original video:

Deepfake:

Figure 2: Deepfake video sample posted by skidhackz (Source: Hack Forums)

A sample of services offered by other threat actors across the above mentioned forums ,and others ,include:

Threat Actor	Source	Intelligence
"kakatb"	Darkmoney Forum	In March 2020, the threat actor posted their video editing services and claimed to have over 2 and 11 years of experience in video and photography, respectively. The threat actor states that they apply deepfake to any level of complexity (buyer's requirements), and also performs audio and other video-related services.
"THZ93"	DarkMarket Forum	In January 2020, the threat actor advertised one-on-one training lessons for 1,500 rubles ($20 USD) on face replacement in videos. The threat actor informed interested users on the needed software for the training as well as provided tutorial videos uploaded to VK.
"Ownership"	DarkMarket Forum	In September 2020, the threat actor authored a sales thread that included deepfake and video editing services. Specific offerings by Ownership include: photo editing ($50), video verification and variations ($150), and deepfake (based on a buyer's requests; $250).

In addition to offering services ,we also identified highly credible threat actors requesting collaborative partnerships and posting in search of deepfake services:

Threat Actor	Source	Intelligence
"Buffer"	Exploit Forum	In March 2020, the highly reputable threat actor posted a request for deepfake services that included video and photo editing. The threat actor stated they were willing to pay up to $16,000 for services.
"d54nw"	XSS Forum	In December 2019, the operator posted a request for deepfake services to construct and design fraudulent bank cards, signatures, documents, persons (images), and card numbers that are not detectable via Google or Yandex searches. The threat actor was willing to pay upwards of $1,500 for services and instructed interested professionals to contact them via Jabber.

Deepfakes and Clearnet Sources

Threat actors often discuss and refer others to popular deepfake programs and forums hosted on clearnet sources. Through this, we have identified an overlap in services and techniques between the criminal underground and clearnet discussion of deepfakes, namely:

- The use of forums for educational purposes and intelligence sharing
- The continued desire of forum members to perfect their craft, which can then be used for fraud
- A pivot to less-mainstream messaging services and are generally not moderated at the degree of a clearnet forum or social media platform

We believe that there is very little in the way of individuals making deepfakes for entertainment or curiosity as a hobby — as regularly expressed on clearnet forums — and translating these skills into criminal activities. In our research, we found that criminal activity on clearnet sources relating to deepfake technology is currently isolated to a few varying buckets, namely:

- The unapproved use of likenesses, regarding celebrities, politicians, and high-profile personalities in, for example, movie clips, pornography, or for political purposes (including possible use in disinformation).
- In other situations, we have found individuals using "deepfakes" or similar editing/doctoring tools in isolated criminal incidents as a form of punishment or revenge against a target, namely generating one's likeness inside of a compromising or embarrassing situation.

Applications and tools used for deepfakes have a pre-built infrastructure, and vary in level of complexity from beginner to advanced, but generally have a significantly low barrier to entry. Further, programs used by threat actors on clearnet sources vary on their methods of production; some rely on cloud infrastructure (and as such are likely more accessible), while others use local machines. For local machines, we find that some applications, like MachineTube for example, recommend at least 2 GB of VRAM for rendering. Other tools, such as FaceApp, Avatarify (described later in this section), and Zao, are powerful applications one can master on their smartphone or mobile device with very little education or training required.

The clearnet is a popular place to discuss deepfake technology and for individuals of all levels of expertise to learn and improve their craft. Given the abundance of educational resources, community engagement, and relative ease in creating deepfake technology, it is highly likely that the knowledge base, expertise, and general interest in deepfakes will continue to grow into the future and with it an increased probability of deepfake techniques used in criminal activities.

Applications and Tools

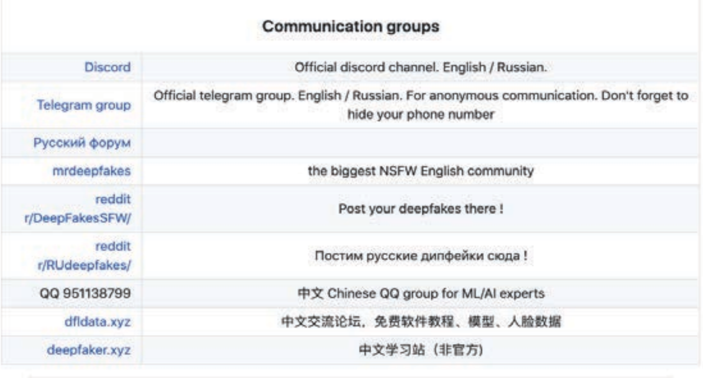
The following applications are among the more popular web-based, downloadable, or mobile tools individuals can use to create deepfake photos and videos. This sampling is almost certainly not exhaustive. According to the visual animation studio Vuild, as of 2019, there are at least 50 popular deepfake tools, covering photo, video, and audio, 3 of which are detailed further below:

Platform	Intelligence
DeepFaceLab	DeepFaceLab is a Python-run, open-source deepfake platform designed by GitHub user "iperov" that is advertised as "the leading software for creating deepfakes". DeepFaceLab is also used by popular deepfake content creators on YouTube as well as the viral TikTok sensation "deeptomcruise." According to iperov, "95% of deepfake videos are created with DeepFaceLab". Gemini Advisory's blogpost on DeepFaceLabs in January 2021 also highlighted how threat actors are using this software due to its availability, advancements, and capabilities of producing deepfakes.
DeepFakesWeb	DeepFakes App is a cloud-based deepfake software, likely based in Japan, The platform for uploading and creating deepfake videos is accessible via web browser at an approximate cost of $2 USD per hour. The website advertises "Responsible Deepfake Technology" to include visible watermarks in content, as well as clear evidence of video manipulation to demonstrate that the video is indeed AI manipulated.
FaceSwap	FaceSwap is an open-source deepfake platform powered by Tensorflow, Keras, and Python and accessible on Windows, macOS, and Linux. FaceSwap maintains an "Ethical Manifesto" which denounces any use of the platform for inappropriate, illicit, or unethical content.
Avatarify	Avatarify is a mobile-based AI face animator available on the Apple App Store as well as Google Play. Avatarify states that the program's "advanced neural network" allows users to record their facial expressions and emotions from their phone on the photo of an individual of their choosing, bringing the photo "alive."

Clearnet Forums

Reddit, Telegram (publicly available channels), and forums dedicated to deepfake tools and technologies are the most popular and widely used clearnet sources for individuals to discuss deepfakes. Many of these forums are based on community interest and education about deepfakes, are easy to access, some with significant traffic and membership (upwards of 400,000 members for at least one), and members of these forums consist of programmers, users, and more discussing techniques, shared applications, and deepfake content. As with any technology tool, any educational resources discussed on these websites, however, can and are likely abused by threat actors.

Broadly, we have found that the more popular and prominent communities on the clearnet relate to DeepFakeLab, likely one of if not the most popular deepfake platforms online right now. We found that the community around this application is substantial, consisting of Russian-, English-, and Mandarin-speaking members. The group is easily accessible through dedicated channels on Discord, Telegram, Reddit, and QQ. These channels are advertised on DeepFakeLab's GitHub page.



Communication groups

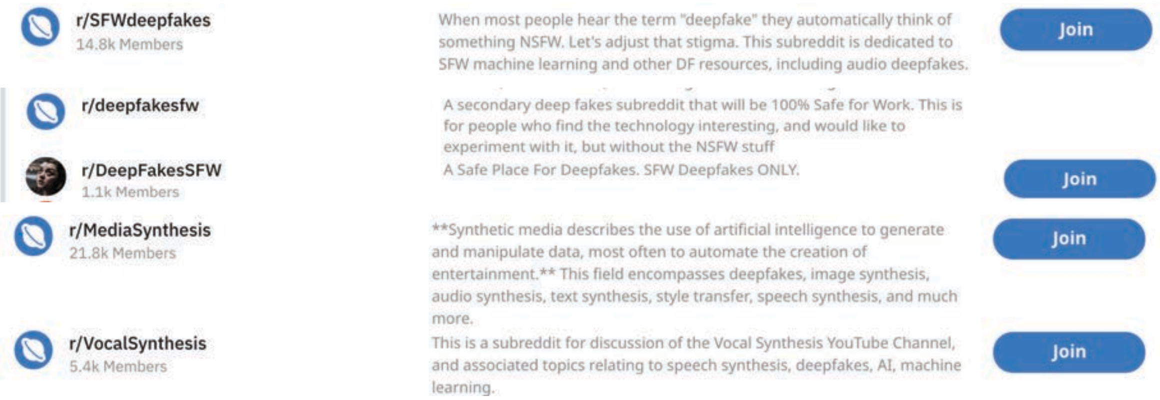
Discord	Official discord channel. English / Russian.
Telegram group	Official telegram group. English / Russian. For anonymous communication. Don't forget to hide your phone number
Русский форум	
mrdeepfakes	the biggest NSFW English community
reddit r/DeepFakesSFW/	Post your deepfakes there !
reddit r/RUdeepfakes/	Постим русские дипфейки сюда !
QQ 951138799	中文 Chinese QQ group for ML/AI experts
dfldata.xyz	中文交流论坛，免费软件教程、模型、人脸数据
deepfaker.xyz	中文学习站（非官方）

Figure 3: DeepFakeLab's community and related communication groups available in English, Mandarin, and Russian

Reddit

Reddit is a popular place to discuss deepfake technology and share created deepfake content within the bounds of Reddit's terms of service. As we discussed earlier in this report, deepfakes likely broke through into the mainstream in 2017 thanks to Reddit user u/deepfakes and their administered subreddit r/deepfake. Though r/deepfake is no longer on Reddit, several other subreddits have sought to take its place for "suitable for work" content, and discussion has also expanded to areas specializing in artificial intelligence, machine learning, and media synthesis.

The majority of subscribers to these subreddits tend to focus on discussing deepfake technologies, sharing and promoting content, and maintaining an overall educational and genuine interest in learning. Criminal and malicious activities on these subreddits are not permitted and are actively discouraged.



r/SFWdeepfakes
14.8k Members

When most people hear the term "deepfake" they automatically think of something NSFW. Let's adjust that stigma. This subreddit is dedicated to SFW machine learning and other DF resources, including audio deepfakes.

r/deepfakesfw

A secondary deep fakes subreddit that will be 100% Safe for Work. This is for people who find the technology interesting, and would like to experiment with it, but without the NSFW stuff

r/DeepFakesSFW
1.1k Members

A Safe Place For Deepfakes. SFW Deepfakes ONLY.

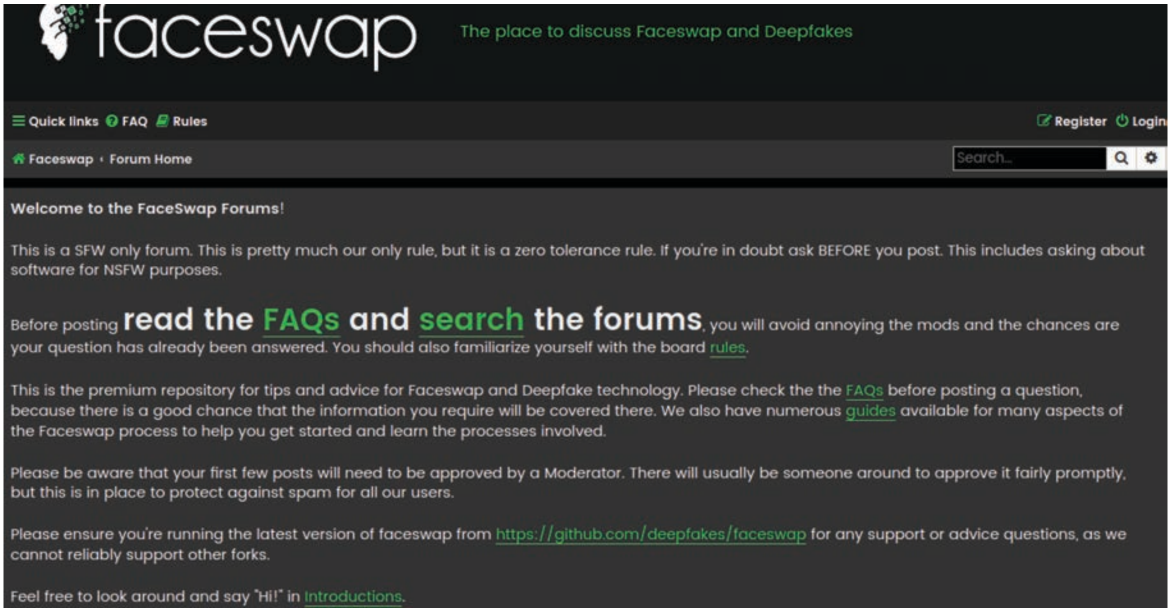
r/MediaSynthesis
21.8k Members

Synthetic media describes the use of artificial intelligence to generate and manipulate data, most often to automate the creation of entertainment. This field encompasses deepfakes, image synthesis, audio synthesis, text synthesis, style transfer, speech synthesis, and much more.

r/VocalSynthesis
5.4k Members

This is a subreddit for discussion of the Vocal Synthesis YouTube Channel, and associated topics relating to speech synthesis, deepfakes, AI, machine learning.

Figure 4: Popular subreddits to discuss deepfake technologies (Source: Reddit)



The place to discuss Faceswap and Deepfakes

Welcome to the FaceSwap Forums!

This is a SFW only forum. This is pretty much our only rule, but it is a zero tolerance rule. If you're in doubt ask BEFORE you post. This includes asking about software for NSFW purposes.

Before posting **read the FAQs and search the forums**, you will avoid annoying the mods and the chances are your question has already been answered. You should also familiarize yourself with the board rules.

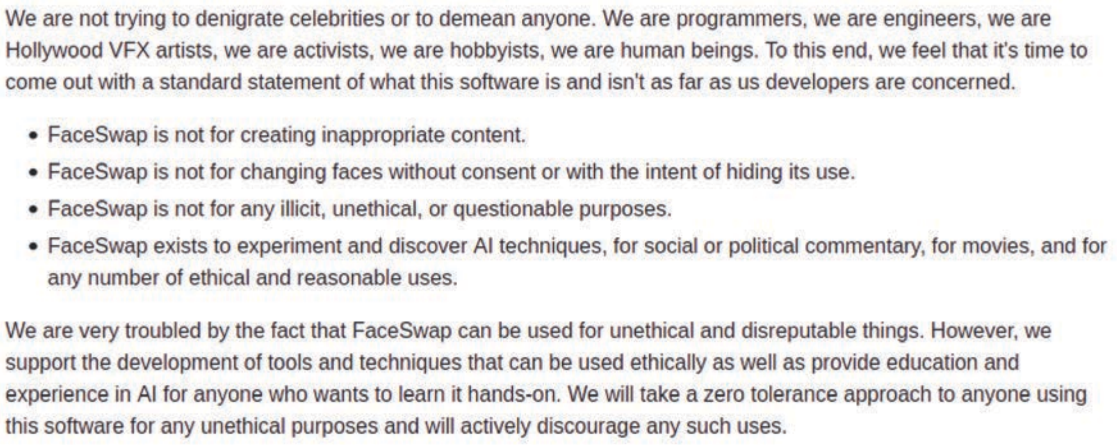
This is the premium repository for tips and advice for Faceswap and Deepfake technology. Please check the the FAQs before posting a question, because there is a good chance that the information you require will be covered there. We also have numerous guides available for many aspects of the Faceswap process to help you get started and learn the processes involved.

Please be aware that your first few posts will need to be approved by a Moderator. There will usually be someone around to approve it fairly promptly, but this is in place to protect against spam for all our users.

Please ensure you're running the latest version of faceswap from https://github.com/deepfakes/faceswap for any support or advice questions, as we cannot reliably support other forks.

Feel free to look around and say "Hi!" in Introductions.

Figure 5: Landing web page for FaceSwap Forum



We are not trying to denigrate celebrities or to demean anyone. We are programmers, we are engineers, we are Hollywood VFX artists, we are activists, we are hobbyists, we are human beings. To this end, we feel that it's time to come out with a standard statement of what this software is and isn't as far as us developers are concerned.

- FaceSwap is not for creating inappropriate content.
- FaceSwap is not for changing faces without consent or with the intent of hiding its use.
- FaceSwap is not for any illicit, unethical, or questionable purposes.
- FaceSwap exists to experiment and discover AI techniques, for social or political commentary, for movies, and for any number of ethical and reasonable uses.

We are very troubled by the fact that FaceSwap can be used for unethical and disreputable things. However, we support the development of tools and techniques that can be used ethically as well as provide education and experience in AI for anyone who wants to learn it hands-on. We will take a zero tolerance approach to anyone using this software for any unethical purposes and will actively discourage any such uses.

Figure 6: FaceSwap's statement on the ethical use of its deepfake technology (Source: GitHub)

FaceSwap Forum

FaceSwap Forum is a popular forum for members to discuss deepfake technologies, namely the free and open-source deepfake software application FaceSwap. FaceSwap is an application powered by Tensorflow, Keras, and Python, available for Windows, macOS and Linux. FaceSwap Forum advertises itself as a "suitable for work only forum" to discuss FaceSwap, and its users include programmers, engineers, video effects artists, activists, and more. Forum administrators take a strong ethical approach to their website, stating that FaceSwap is "not intended for creating inappropriate content", and is not used for "any illicit, unethical, or questionable purposes". Administrators, however, note that FaceSwap is used "for unethical and disreputable things", but support the exploration of deepfake technologies for ethical means. Many criminal and underground forums issue similar statements to avoid any legal responsibility for content discussed, presented, or offered on their forum, as well as to intentionally suppress any suspicion that the forums host or discuss illegal or unethical content.

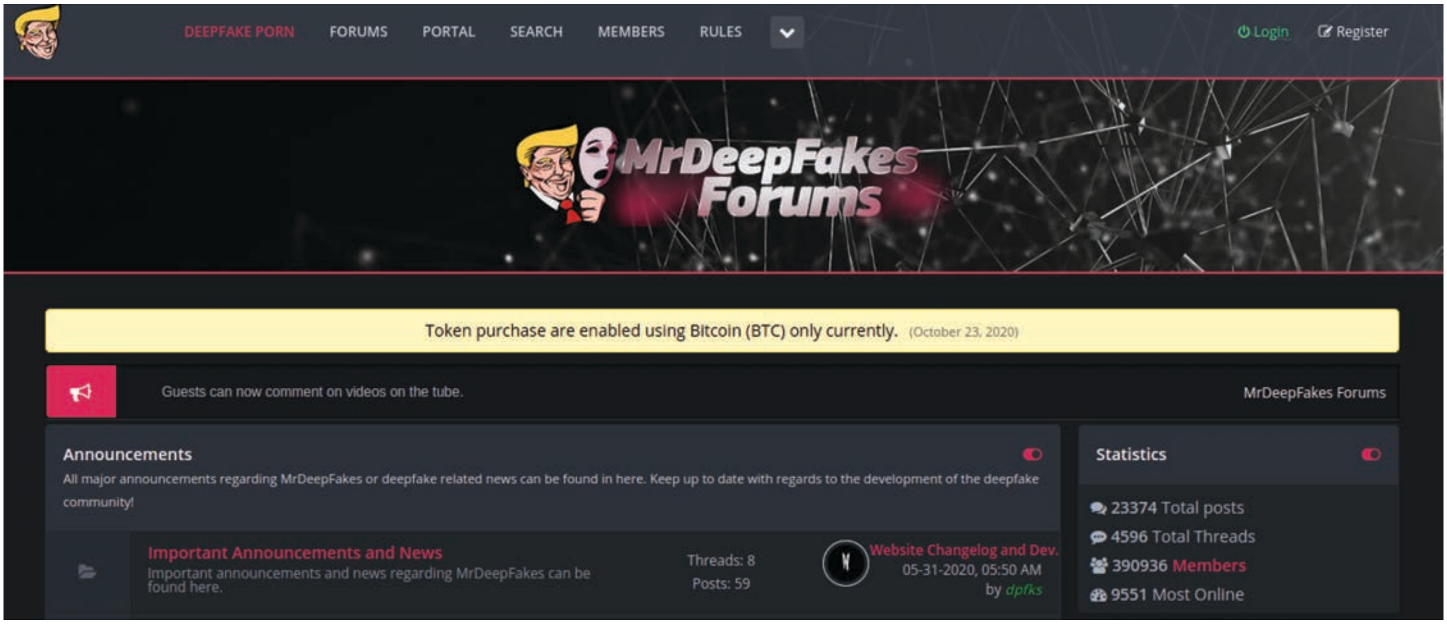
FaceSwap Forum is a small community, with 1,766 members at the time of writing. Discussions on this forum include discussions on content creation, artificial intelligence, training, and research.

MrDeepFakes Forums

MrDeepFakes Forums is a deepfake-centric, English and Russian forum board active since mid-2018, per Recorded Future data. The website serves as a forum to MrDeepFakes, a community-driven deepfake pornography website that primarily targets celebrities "for the sole purpose of entertainment". Currently, the forum hosts over 390,000 members and is highly active, with members discussing and creating deepfake content, sharing creation tools and techniques, and more. Additionally, members have also been found providing templates, "facesets", and model sets for others to mix and match the physical appearance of their targets.

DeepFakeForums

Our investigation into potential clearnet forums uncovered a relatively new forum, DeepFakeForums, currently under construction. The website, according to Recorded Future domain data, was registered and given an active certificate in mid-January 2021. Currently, the website resolves to a XenForo splash page, stating that content is "Coming soon". We do not know specifics about the type of content that is planned to be hosted at this website at this time, though potential content likely ranges between technical discussions of deepfakes, tutorials, and creators posting their deepfake content.



Token purchase are enabled using Bitcoin (BTC) only currently. (October 23, 2020)

Guests can now comment on videos on the tube.

MrDeepFakes Forums

Announcements

All major announcements regarding MrDeepFakes or deepfake related news can be found in here. Keep up to date with regards to the development of the deepfake community!

Important Announcements and News
Important announcements and news regarding MrDeepFakes can be found here.

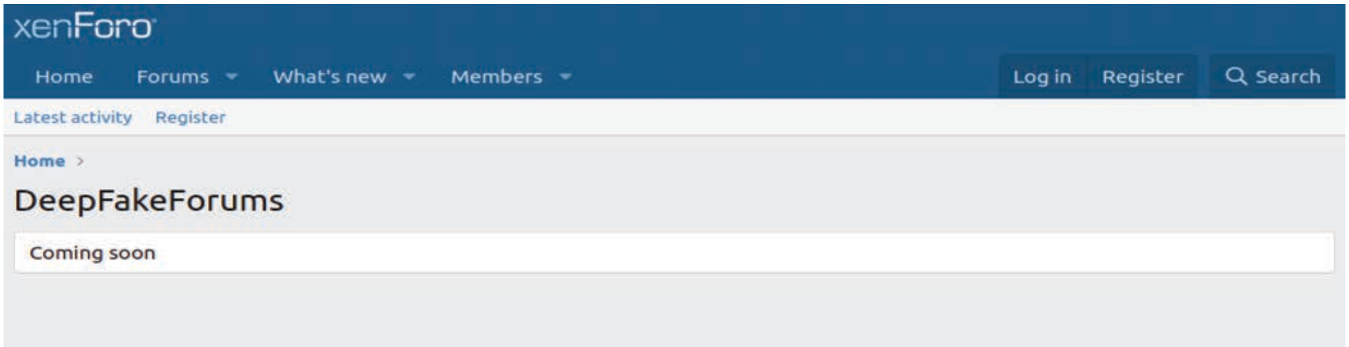
Threads: 8
Posts: 59

Website Changelog and Dev.
05-31-2020, 05:50 AM
by dpfks

Statistics

23374 Total posts
4596 Total Threads
390936 Members
9551 Most Online

Figure 7: Landing web page for MrDeepFakes Forums



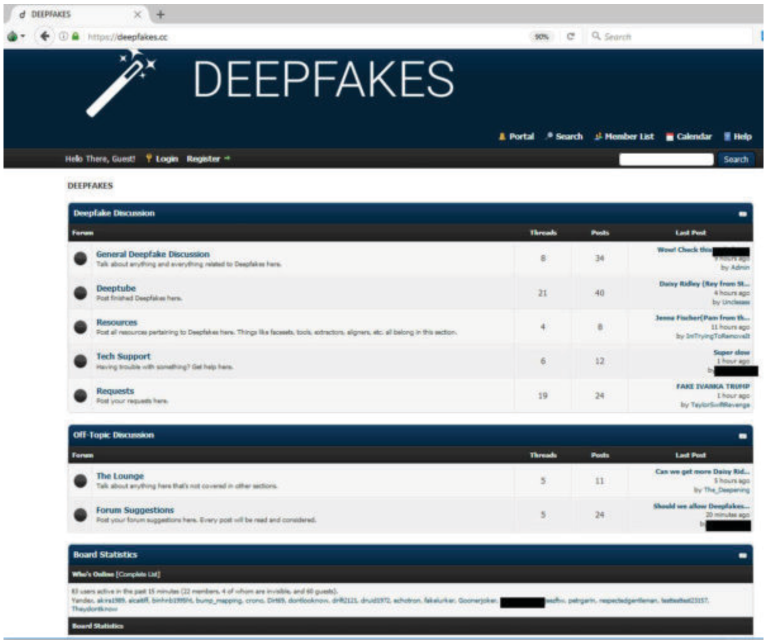
DeepFakeForums

Coming soon

Figure 8: DeepFakeForums under construction, as of March 2021

DeepFakes[.]cc

DeepFakes[.]cc was a popular emerging deepfake forum, with a reported 2,000 or more registered members in early 2018. According to The Register in February 2018, the forum was a popular avenue for "people to publish their finished videos, post requests to make customised fake pornography, and even ask for tech support", much in line with existing forums today. A Malwarebytes investigation into the forum found that administrators were using Coinhive to mine Monero cryptocurrency by deploying hidden mining scripts in the background, driving visitor CPU use up to a full 100%. To ramp up traffic to the forum, and therefore employ additional machines for mining Monero, Reddit users likely affiliated with the site advertised migrating from various deepfake subreddits to DeepFakes[.]cc. Currently DeepFakes[.]cc is no longer active, likely shut down after it was found that the forum actively used Coinhive against visitors. However, the site's age does demonstrate that clearnet interest in deepfakes is not an entirely new phenomenon.



Deepfake Discussion

Forum	Threads	Posts	Last Post
General Deepfake Discussion Talk about anything and everything related to Deepfakes here.	8	34	Wow! Check this [redacted] by Admin
Deeptube Post finished Deepfakes here.	21	40	Daisy Ridley (Rey from St... 4 hours ago by Uncleaaa
Resources Post all resources pertaining to Deepfakes here. Things like facesets, tools, extractors, aligners, etc. all belong in this section.	4	8	Jenna Fischer(Pam from th... 11 hours ago by ImTryingToRemoveIt
Tech Support Having trouble with something? Get help here.	6	12	Super slow 1 hour ago b[redacted]
Requests Post your requests here.	19	24	FAKE IVANKA TRUMP 1 hour ago by TaylorSwiftRevenge

Off-Topic Discussion

Forum	Threads	Posts	Last Post
The Lounge Talk about anything here that's not covered in other sections.	5	11	Can we get more Daisy Rid... 5 hours ago by The_Deepening
Forum Suggestions Post your forum suggestions here. Every post will be read and considered.	5	24	Should we allow Deepfakes... 20 minutes ago b[redacted]

Board Statistics

Who's Online [Complete List]

83 users active in the past 15 minutes (22 members, 4 of whom are invisible, and 60 guests).
Yandex, akira1989, alcatiff, binhnb1999H, bump_mapping, crono, Dirt69, dontlooknow, drift2121, druid1972, echotron, fakelurker, Goonerjoker, [redacted]eadfox, petrgarin, respectedgentleman, testtesttest23157, Theydontknow

Board Statistics

Figure 9: A screenshot of Deepfakes[.]cc in 2018; the forum is no longer online (Source: Malwarebytes)

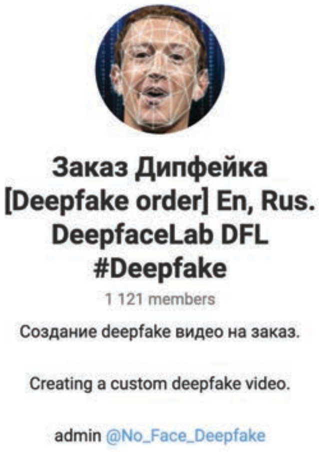
Messenger Platforms

We believe that messenger platforms (such as Telegram and Discord) are likely more of a source of fraud or criminal-related activities compared with clearnet forums. This is likely due to the anonymity of messengers, moderation practices that are less stringent than a clearnet forum, as well as more concentrated knowledge of messenger resources we commonly observe used in other criminal discussions and activities.

Telegram

The deepfake community is strongly represented on Telegram, with at least 12 multilingual communities discussing technical details, techniques, and tips for creating deepfakes, as well as a source of sharing created content. Here are 6 of the most prominent, publicly available communities on Telegram that are active as of March 2021 and have a moderate to large following:

- @NeuroLands
- @RoundDFDB
- @dpfake
- @deepfakeorder
- @MrDeepFakes
- @deepfakes



Заказ Дипфейка
[Deepfake order] En, Rus.
DeepfaceLab DFL
#Deepfake

1 121 members

Создание deepfake видео на заказ.

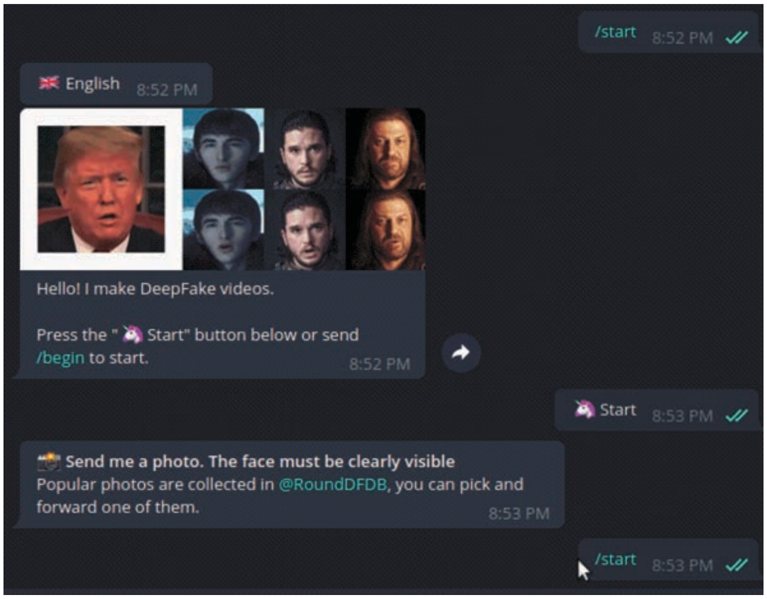
Creating a custom deepfake video.

admin @No_Face_Deepfake

Figure 10: Telegram deepfake channel @deepfakeorder currently has over 1,100 members

Analysis of some of the discussions posted on the @ deepfakeorder involved deepfakes being used in movie clips and politics, as well as the technology, education, and science relating to deepfakes. Private sources, such as closed Telegram groups and direct message channels, are likely to have potentially unethical or criminal use of deepfake technology. The cost and time spent on a deepfake creation video varies based on the specific customer request. According to @deepfakeorder admin @No_Face_Deepfake, their service states that the price of 1 minute of deepfake video starts at $100 USD, and can vary in production between 3 days and 2 weeks "depending on the complexity of the work".

Some channels also allow for in-platform creation of simple deepfake videos through the assistance of a Telegram chat bot, as illustrated in Figure 11:



/start 8:52 PM

🇬🇧 English 8:52 PM

Hello! I make DeepFake videos.

Press the " 🦄 Start" button below or send /begin to start. 8:52 PM

🦄 Start 8:53 PM

📸 **Send me a photo. The face must be clearly visible**
Popular photos are collected in @RoundDFDB, you can pick and forward one of them. 8:53 PM

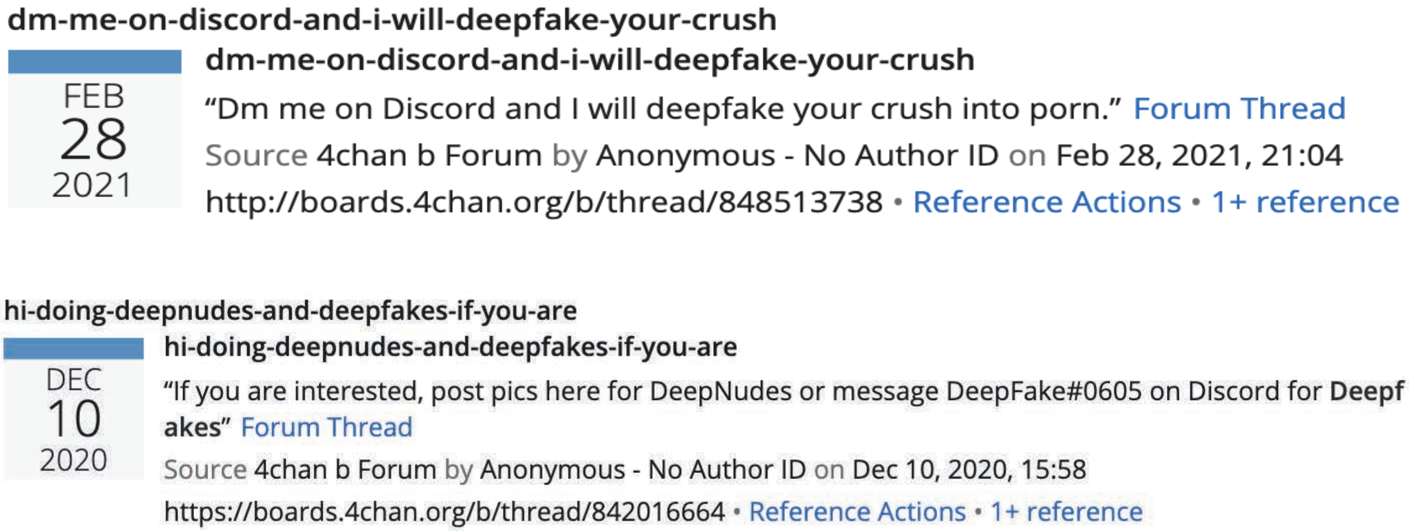
/start 8:53 PM

Figure 11: Telegram bot tutorial on creating a deepfake video via message commands

Discord

We found that the chat service Discord is a popular avenue for threat actors to engage in closed communications about deepfakes, especially to request deepfakes that edit a close contact like a classmate, co-worker, or friend into pornographic images. We have found members of 4chan, for example, advertising deepfake services, requesting individuals to direct message them on Discord with information on a specific target. Personalized deep fakes in this manner can and have been used not only for personal purposes but also as a form of extortion and blackmail, public embarrassment, and fraud.

Through proprietary intelligence ,we have also identified a small number of dedicated deepfake Discord group channels, and we believe it is highly likely that many more exist ,but are probably kept private and among small ,vetted groups of individuals.



dm-me-on-discord-and-i-will-deepfake-your-crush

FEB 28 2021

dm-me-on-discord-and-i-will-deepfake-your-crush

"Dm me on Discord and I will deepfake your crush into porn." Forum Thread

Source 4chan b Forum by Anonymous - No Author ID on Feb 28, 2021, 21:04

http://boards.4chan.org/b/thread/848513738 • Reference Actions • 1+ reference

hi-doing-deepnudes-and-deepfakes-if-you-are

DEC 10 2020

hi-doing-deepnudes-and-deepfakes-if-you-are

"If you are interested, post pics here for DeepNudes or message DeepFake#0605 on Discord for **Deepfakes**" Forum Thread

Source 4chan b Forum by Anonymous - No Author ID on Dec 10, 2020, 15:58

https://boards.4chan.org/b/thread/842016664 • Reference Actions • 1+ reference

Figure 12: Threat actors on 4chan's /b/ forum advertising Deepfake services available through communications on Discord

Outlook and Mitigation Strategies

In a February 2021 interview, Gemini Advisory CEO Andrei Barysevich discussed how deepfake technologies were supplanting older means of identity theft (such as counterfeit licenses and passports) to bypass advancements in security detections. Furthermore, deepfake activities and their criminal use had not been weaponized yet, but the continued improvements in deepfakes in criminal activities suggested that their full implementation was not far off. In March 2021, the FBI released a Flash Alert that malicious threat actors "almost certainly" will be using deepfakes to advance their influence or cyber operations, specifically threat actors "using synthetic content in spearphishing and social engineering in an evolution of cyber operational tradecraft".

We believe that both dark web and clearnet threat actors will continue to adapt and perfect fraudulent methods that use deepfake technologies. As identified and reported by Insikt Group's Cybercriminal and Underground Threat IntelligenceTeam throughout 2020, threat actors are advertising customized services and automated products to facilitate cybercriminal activities and cater to the demand for said services and tools. Threat actors will likely continue to offer customized and automated services for deepfakes technologies, especially as facial and vocal authorization is implemented into security protocols.

Companies have already begun to develop mitigation measures and strategies in anticipation of deepfakes being used fraudulently. In December 2019, Facebook launched the Deepfake Detection Challenge (DFDC) to bring together industry experts to test detection models, incorporate new approaches, and share best practices. In its inaugural debut, DFDC included 2,114 participants that tested customized deepfake detection softwares against videos with 3,500 paid actors; the winning detection software detected 65% of real-world deepfake videos. There is currently not a universally applied method or dedicated software that can fully detect a deepfake video or voice at this time.

Below are mitigation strategies suggested by deepfake experts and practitioners:

- Incorporate internet allowlisting, so as to authenticate objects by hashing images.
- Use deepfake detection algorithms that are continuously refined and improved as the technology evolves and fraud detection techniques in metadata to distinguish authentic from fake material.
- When watching a video, be "alert for warping, distortion, syncing issues or other inconsistencies in images or videos", the FBI warns. "Sometimes profile pictures that bad actors generate for use on [social media], for instance, display consistent eye spacing across multiple images".
- Keep abreast to updates in detection technologies, techniques, and tools as they become available, such as Microsoft's Video Authentication Tool, use of biological signals, detection of phoneme-viseme (mouth shape versus spoken language) mismatches, and OpenFace modeling.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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