ActioNews

FALL 2022
THE NEWSLETTER OF ACTIONET

Turning VISION into ACTION®

CHAIRMAN'S NOTE

Dear Friends,

One of the greatest Cybersecurity threats facing the world is the creation and proliferation of "Deepfakes", which leverage AI to create or altered images, audio, and video resulting in synthetic content that appears authentic. This takes identity theft, impersonation and disinformation to a new and dangerous level, which can impact markets, funds and the political landscape. Incident response needs to be active and proactive to combat this growing threat.

Moving to the Cloud improves security, redundancy and availability, but monitoring the use of hosted resources is essential to make sure you are not paying for capacity and services that are not needed. Data charges can easily get out of hand. Leveraging tools such as Cloud Insights and CloudCheckr help ensure we are getting the most out of our Cloud Services while actively managing the cost.

We all need to stay connected and maintain the personal touch as we emerge from the pandemic and get back to normal. Hope you had a great Summer and please take care of yourselves and each other!

Ashley W. Chen
Chairman & CEO

IN THIS ISSUE

Protecting Against Deepfakes 1
Controlling the Hidden Cost of the Cloud 3
Navy Gold Coast 2022 . 4
ActioNet Ohana Hike . . 4

Protecting Against Deepfakes

By Banji Agunbiade, Sr. Security Engineer

The tech world is extremely intriguing. Over the past few decades, we have witnessed the creation and evolution of new processes and technologies which have made human lives a bit (or a lot) easier. In the creative tech arena for instance, Adobe has delivered a suite of photo and video modification, animation and editing technologies including Adobe After Effects, Premiere Pro, and the very notoriously popular Photoshop. Whether some of these new capabilities which have put a vast array of creative artistic options on our tables pose any significant national security or enterprise threats is debatable. What is however is not debatable is the clear damage that can be done with deepfakes, a more sinister step up on Adobe's suite of artistic tools.

Deepfake—a combination of the words 'deep learning' and 'fake'—refers to an AI-based technology used to create or alter images, audio, and video resulting in synthetic content that appears authentic. Deepfakes are computer-created artificial videos in which images are combined to create new footage that depicts events, speeches or action that never actually happened. They can be quite convincing and quite difficult to identify as false. If you are the type that worries about the sanctity and integrity of information like me, I bet the red flags are springing up right, left, and center in your mind. A piece of technology that offers the ability to look and sound like anyone, including those authorized to approve payments from a company, and give fraudsters an opportunity to extract potentially vast sums of money should get everyone worried.

A machine learning technique called a "generative adversarial network" or GAN can create fake videos by looking at thousands of a person's photos and approximate those photos into a new image without being an exact copy of any one of the photos, increasing the difficulty of identifying the image as false. GAN is a multi-use technology that can be used to generate new audio from existing audio, or new text from existing text. This piece of tech is very widely used in the movie industry, which accounts for 99% of existing deepfake videos in circulation, mostly within the adult movie segment. GANs are becoming more widely available and some mobile apps already have it powering their consumer face and voice swap offerings. Imagine what damage can be done when a child responds to a real-looking video message from his parent to open the door to a supposed service contractor, who turns out to be anything but a service contractor? Better left to the imagination, right?

> "Deepfakes are computer-created artificial videos that depict events, speeches or action that never actually happened."

So concerned was the FBI about the dangerous misuse

continued on page 2

ActioNews, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews is published quarterly (March, June, September, and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer

Karen Tepera

Contributing Authors

Banji Ogunbiade
Jeff Masiello
Ashley Chen
Jeffrey Abish

"There are a number of deepfake detection tools that can be leveraged to identify deepfakes and be integrated as part of the overall security tool suite."

Deepfake continued from page 1

cases and security threats posed by deepfakes that it issued a public security warning in mid-2021. According to the FBI, hackers are now able to fake their way into a company by stealing a person's personal information to apply for a job, then grab a picture of that person, manipulate the video and sound to impersonate that person during a remote job interview. Suddenly, if care is not taken, you have a fake insider on your hands with access to business data and proprietary information within the company and can now sell that information to competitors or foreign countries. Not where you want to be in today's world where information is the most valuable business asset. This is just one on many damaging scenarios that deepfakes can inflict on an organization.

On the political side of things, you may have seen Jordan Peele's video (not linked here due to language used in the video) depicting former president Barack Obama doing some trash talking, which of course did not happen. This gives you an idea of what level of misinformation and disinformation that can be unleashed on the population utilizing this little piece of tech. In one of the early cases of audio deepfakes, which underlines enterprise vulnerability to deepfakes, some crooks used AI to create an impersonation of a German company's chief executive's voice – and then used the audio to fool his company into transferring $243,000 to a bank account supposedly to pay some contractor for service rendered. Not good! When your customers think you lack basic presence of mind to double check on things, that does not reflect well.

Another scenario that could occur is a PR nightmare: Public opinion can head south by reason of fake videos depicting a CEO or other management staff saying or doing unseemly things. The same outcome may occur when deepfaked influential people share disinformation about a company or products. Not only can this impact reputation, but it can also influence consumer behavior, and potentially affect stock price. Very importantly, for an organization that operates within the government contracting space like ours, it can impact organizational reputation with current and prospective clients.

How can an organization guard against the destructive effects of deepfakes? What measures does ActioNet have on the ground to prevent and mitigate deepfake threats?

ActioNet realizes that humans are the weakest link in the security chain simply because, unlike tools and tech, they have feelings and those feelings can be appealed to, even exploited. This is why social engineering precedes most successful cyber-attacks. Employee training and awareness is a veritable first line of defense when it comes to deepfakes and ActioNet has one of the most robust security training and awareness programs. Deepfakes awareness and mitigation content is being integrated into the security and awareness training curriculum. The training also focuses on how the technology is leveraged in malicious attempts and how this can be detected. This would enable ActioNet employees to spot deepfake-based social engineering attempts. This training can be incorporated into training programs that we deliver to our customers to raise their awareness of this new threat vector and prepare their workforce to identify, report, and prevent these negative impacts.

Detecting false media early can help minimize the impact on your organization. There are a number of deepfake detection tools, many of which are open source, that can be leveraged to identify deepfakes and be integrated as part of the overall security tool suite. Upon full implementation, this will help build an anti-deepfake firewall around the your environment and its people, translating to defense against attempts by malicious actors to influence public opinion through deepfakes.

ActioNet is also incorporating a response strategy that can be set in motion when a deepfake is detected. Roles, responsibilities and required actions will be defined in this plan. The response strategy may include for example, the communications team issuing a press statement that exposes the malicious deepfake, including evidence from the software-based detection tool. The bottom line of "Seeing is believing" doesn't apply as easily anymore. We have to question everything to counter the ever-evolving threats and new tools being developed.

Finally, good processes are immensely helpful in stopping the negative impacts of Deepfakes. ActioNet has ISO 20000, ISO 27001, ISO 9001, CMMI-DEV® Level 4, and CMMI-SVC® Level 4 certifications and vast experience helping agencies improve their security posture, processes, and procedures. If you have any security needs, ActioNet can help.

Controlling the Hidden Cost of the Cloud

By Jeff Masiello, Sr. Cloud Architect

Moving to the cloud is a lot like going shopping while you are hungry. You go into the store, you get what was on your list, but then you see the cookies and the ice cream, and you are going to make that new fish dinner next week with the side of Brussels sprouts. You end up walking out of the store with far more than you needed and certainly some unhealthy things in the process. Building things in the cloud is similar. You move to the cloud, you order some EC2 with a side of S3, then you hear about the nice API and Lambda functions. Somebody offers a nice course of MongoDB with some IoT on the side. And while you are at it, you might as well get the CDK so you can rapidly build and deploy everything through code pipeline, code deploy, and other toys. You walk out with far more than you really needed and a bill that is higher than you really wanted.

Cloud providers are a la carte, and you are paying for everything you are using. Uncontrolled, this leads to extra costs and waste. Cloud Service Providers (CSP) offer native advising capabilities for free which should be leveraged. AWS has Trusted Advisor and Azure has Azure Advisor. These tools, in addition to helping you lock down your environments and create more robust architectures, advise on underused services, and provide recommendations and estimated cost savings.

ActioNet, a Premier Level ServiceNow Partner, leverages the Cloud Insights Tool. Cloud Insights is like Trusted Advisor and Azure Advisor on steroids. Leveraging its ability to give many of the same recommendations of native CSP tools but being cloud agnostic when linked with monitoring, it provides even more in depth forecasting and advising allowing for even more cost savings. Combined with the full power of ServiceNow's capabilities such as configuration management database (CMDB) and automation can provide even larger savings. Speaking of CMDBs, they are critical to controlling costs. You cannot cut costs if you do not even know what you have. CloudCheckr is another tool that can see into your CSP accounts, even across CSPs, and visualize multi-cloud costs and inventories. Both ServiceNow and CloudCheckr can tag resources which may have been missed in your automated DevSecOps pipelines. (You are using those too, right?) They can help enforce tagging strategies which categorizes costs providing more visibility. Tagging not only helps you determine which programs or applications are eating up your budget but provide an inroad to automation capabilities which is where real savings start to come into play.

One simple automation use case is environmental operation hours. The development environment does not need to be on all week. 6am-6pm 5 days a week easily saves 50% on resource costs. Automating operational hours for the testing environment saves even more. In cases where those environments are used less often, more stable applications for example, using your DevSecOps pipeline to simply destroy and rebuild your dev and test environments can provide vastly more savings. It has the additional benefit of ensuring your DR COOP capability is up to date and functional. Other automations such as autoscaling and data lifecycle rules keep on top of data backups, which add considerable cost. In one case, ActioNet started a contract and discovered one application which would take forever to restore or backup. As it turns out, there was an existing backup script that was not documented with three backup scripts running for the same application with no data lifecycle rules. Tens of thousands of snapshots were created every month for a small application. Data charges were thousands of dollars a month. ActioNet added lifecycle rules, added CMDB discovery, and saved the client multiple thousands of dollars a month for that application alone.

All these savings allow you to put more towards R&D, application improvement, staff training and creating a cycle of innovation and growth. It allows you to try all the modern technologies and techniques. It allows you to go shopping while hungry. ActioNet has the experience to help you understand your environment and control your costs. Whether you are just starting a cloud journey or are well on the way but need to get a grip on what you have now, we can help.

"Cloud Insights is like Trusted Advisor and Azure Advisor on steroids. Combined with the full power of ServiceNow's capabilities and automation can provide even larger savings."

ActioNews

- Founded in 1998, 500+ ActioNeters
  - Overall Customer Retention Rate > 98%
  - Annualized Professional Staff Retention Rate > 92%
  - Woman Owned Small Business under NAICS 517311
- CMMI®-DEV Level 4 Externally Assessed
- CMMI®-SVC Level 4 Externally Assessed
- HDI Certified Support Center
- ISO 20000 (ITSM), ISO 27001 (Information Security) and ISO 9001 (Quality) Registered
- GWAC and IDIQ Contract Vehicles
  - **GSA Alliant 2**
  - **GSA MAS**
  - **GSA IT Schedule 70**
  - **GSA OASIS Pool 1**
  - **CIO-SP3 SB OTSB**
  - **CIO-SP3 WOSB OTSB**
  - **DISA Encore III**
  - **Air Force NETCENTS-2**
  - **ARMY ITES-3S**
  - **HHS SPARC**
  - **NAVY Seaport-NxG**
  - **GSA 8a STARS III (JV)**
- "92 out of 100" Rating from Open Ratings
- "Exceeds Customer Expectations" from D&B
- "5A1" the Highest Financial Rating from D&B
- DCAA-Compliant Accounting and EVM System
- Approved Purchasing and Cost Estimating System

"Social engineering precedes most successful cyber-attacks. ActioNet has one of the most robust security training and awareness programs."

ActioNet

ActioNet Exhibits at Navy Gold Coast 2022

By Ashley W. Chen, Founder & CEO

DecisiveInstincts, an SBA approved Mentor Protege Joint Venture between ActioNet and Akamai Intelligence, exhibited at the 34th Annual Navy Gold Coast 2022, September 6 - September 8, 2022 in San Diego, CA. The theme of the Gold Coast 2022 is "Thriving as a Department of the Navy Small Business in a World of Global Challenges."

We had an opportunity to visit over 200 government agencies and industry organizations, including the ten Navy System Commands. We also attended several one-on-one matching making sessions with key government and industry contracting personnel.

At our DecisiveInstincts booth, we all wore ActioNet Hawaii Shirts with DecisiveInstincts Maui Fish Hook Necklaces. Please check out our pictures with Admiral Peter Stamatopoulos, NAVSUP, Jimmy Smith, the NAVY OSDBU Director, and Ricky Clark, the Deputy Director of NIH NITAAC. This was a very productive networking event and we will be back next year!

ActioNet Ohana Hike at Makapu'u Lighthouse Trail

By Jeffrey Abish, President & CAO

On July 2, 2022, ActioNet Ohana did a Summer Group Outing by hiking at the Makapu'u Lighthouse Trail!

The Makapu'u Point trail offers outstanding views of Oahu's southeastern coastline, including Koko Head and the Koko Crater. From the trail's destination at the Makapu'u Head, one is rewarded with magnificent views of the windward coast and offshore islets, as well as the historic red-roofed Makapu'u Lighthouse built in 1909, which makes a stunning picture against the deep blue sea below (the lighthouse itself is off-limits). On a clear day, you may even see Molokai and Lanai.

BTW, have you ever read the novel "From Here to Eternity" by James Jones? This 1953 Oscar Best Picture Winner was filmed in Hawaii and the famous beach scene is at Halona Cove Beach!