



The Rise of Smart Threats

How AI is Changing Ransomware and Social Engineering

Agenda

1. Introductions
2. AI Fundamentals
3. Applications of AI in healthcare
4. AI regulation
5. Risks of using AI in your business
6. How threat actors could use AI in each phase of a cyber attack
7. Cyber insurance
8. Questions



Story Time

AI Fundamentals

Artificial Intelligence

Simulation of human intelligence by machines

Machine Learning

Leverages data to learn and improve performance without explicit programming

Deep Learning

Uses artificial neural networks with many layers to process complex data

Generative AI

Creates entirely new data (images, text, audio) resembling existing data

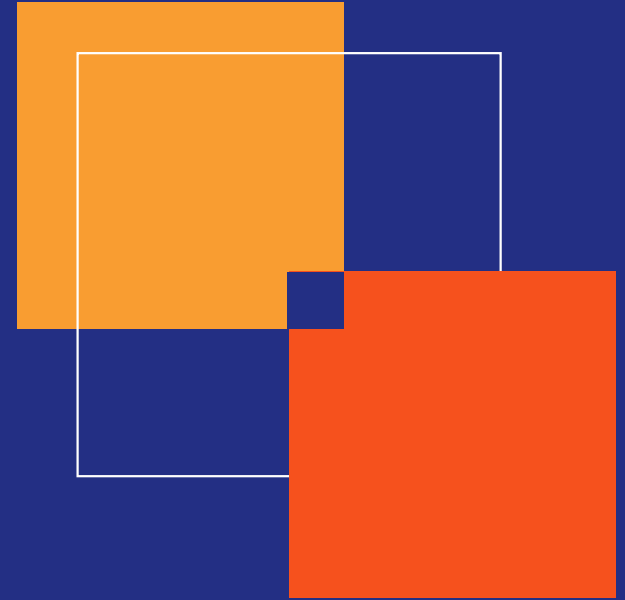
Some AI Use Cases

- Natural Language Processing (NLP): Enabling machines to understand and respond to human language.
- Deep Fakes: Creating realistic but fake media content.
- Image Recognition and Classification: Identifying and categorizing objects within images.
- Speech Recognition: Converting spoken language into text.
- Recommendation Systems: Suggesting products, content, or services based on user preferences.
- Predictive Analytics: Making forecasts based on historical data.
- Computer Vision: Interpreting and understanding visual information.
- Sentiment Analysis: Determining the emotional tone behind text.
- Chatbots and Virtual Assistants: Automated systems for interacting with users.
- Fraud Detection: Identifying fraudulent activities in transactions.

AI Implementation Approaches

- Public/Consumer Offerings
 - Free or paid tiers of ChatGPT, Google Gemini, Microsoft Copilot, and others
- Enterprise Services
 - Managed, hosted service customized to your organization
 - Allows further control of training data and data privacy controls
- Private Deployments/On-Premises Solutions
 - Deploy your own instance (on hardware or in a private cloud)
 - Ensures maximum data privacy by keeping data within your environment

Applications of AI in Healthcare



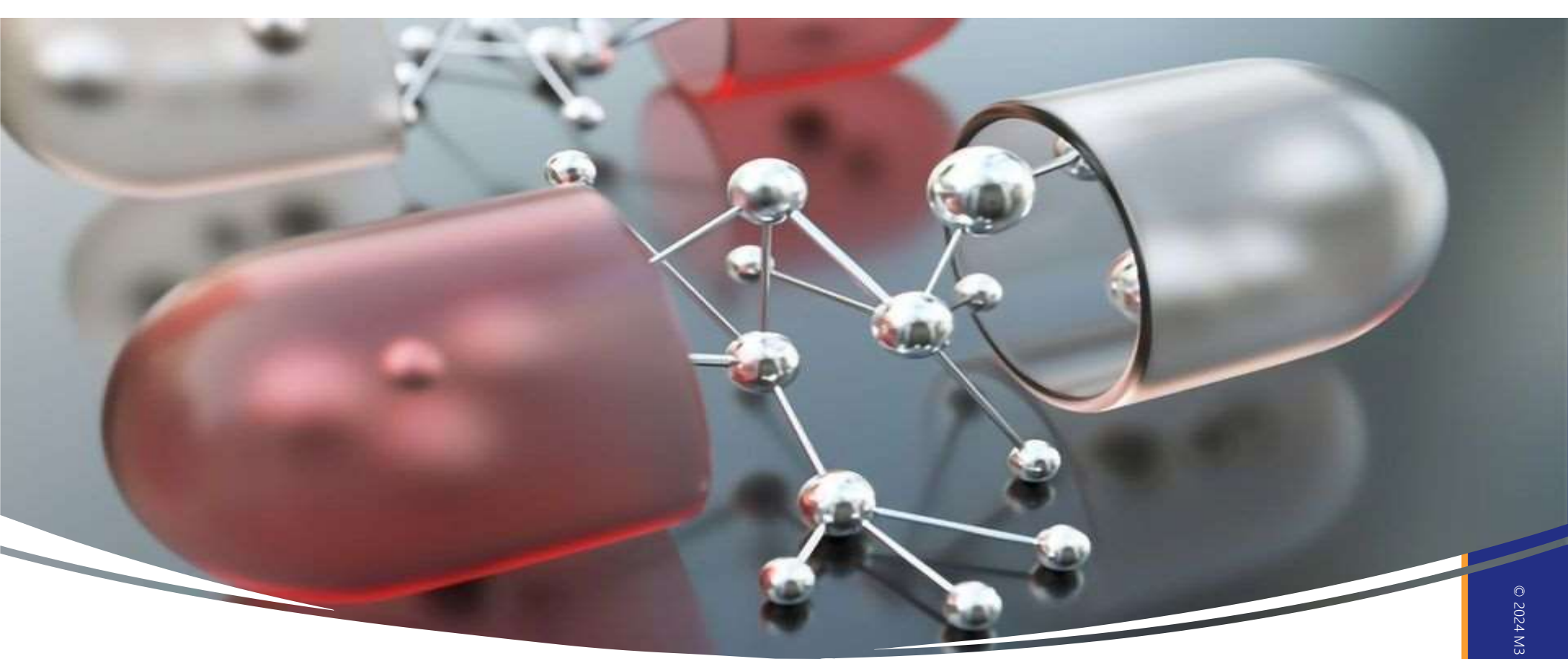
Applications of AI in Healthcare

1. Diagnosis
2. Drug discovery and development
3. Administrative efficiency
4. Patient quality and safety

Diagnosis

- AI is effective at image recognition, which makes AI particularly well suited to specialties such as radiology
- In some cases, AI is outperforming humans
- Potential obstacles





Drug Discovery and Development

- Biopharma can benefit immensely from AI due to the inefficient nature of the industry.
- Drugs will be designed rather than being discovered

Administrative Efficiency

- Admin is a cost driver and a leading factor in provider burnout.
- Epic is working on a tool that will auto generate notes from provider/patient conversations.
- Epic is also working on a tool that will draft responses to patient messages.
- Operating room optimization.



Patient Quality and Safety

- AI can be used to predict major adverse events such as sepsis.

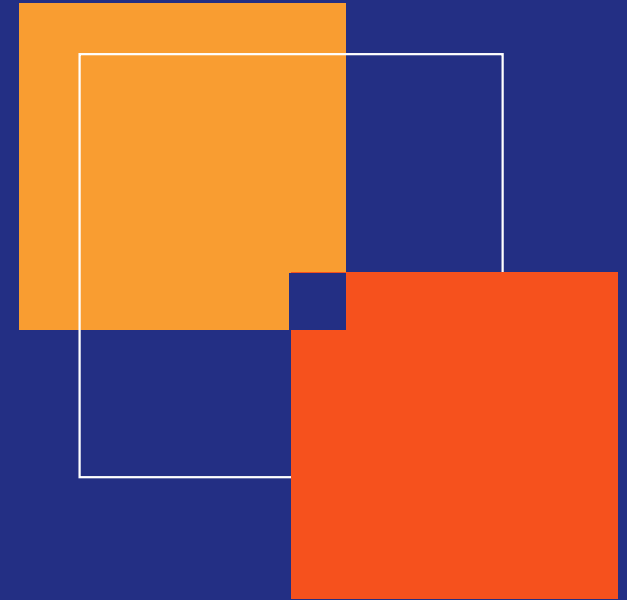


AI Regulation

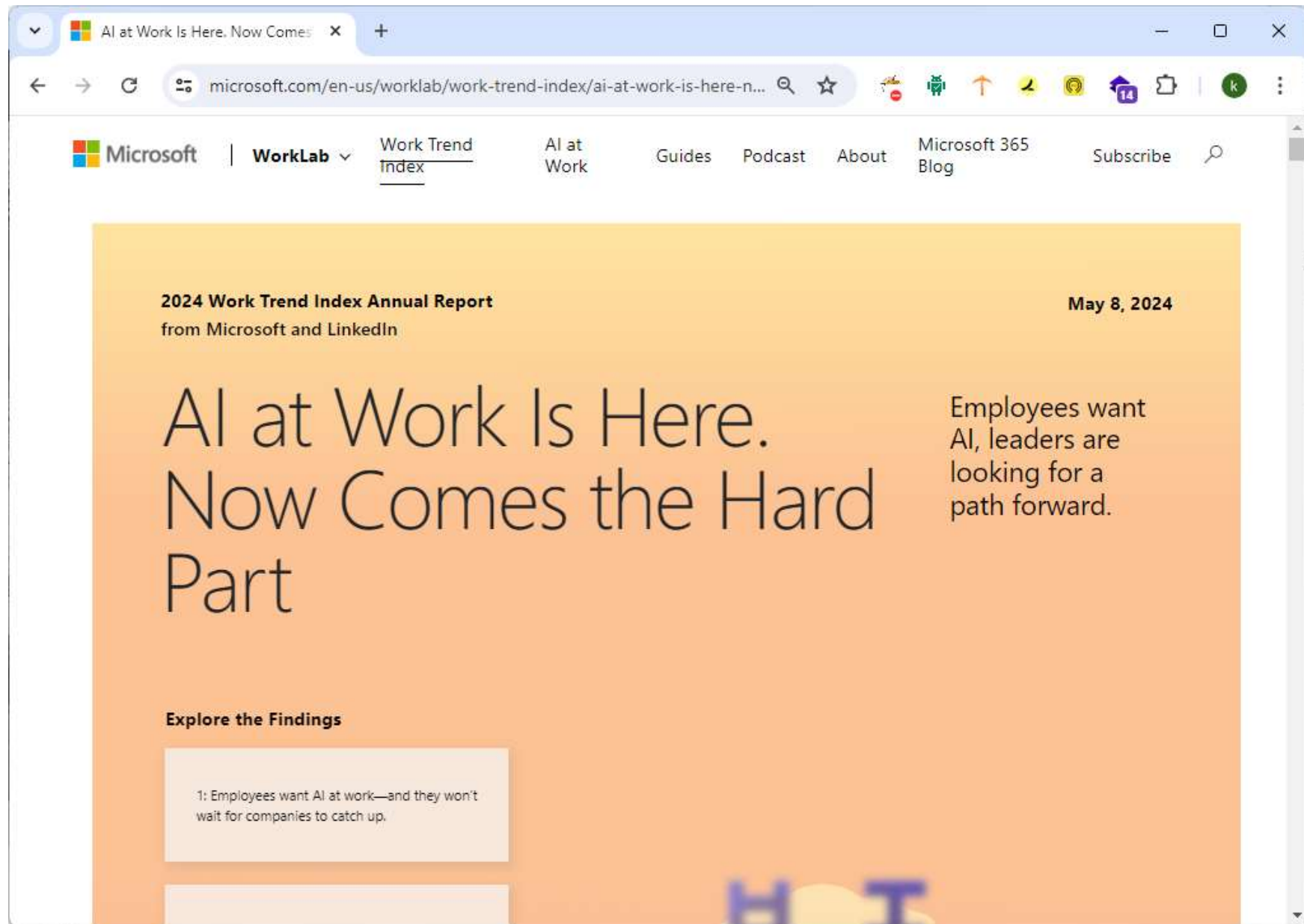
- The October 2023 executive order from the Biden Administration
- The Artificial Intelligence Act passed by the European Parliament
- Similarities and differences between the two



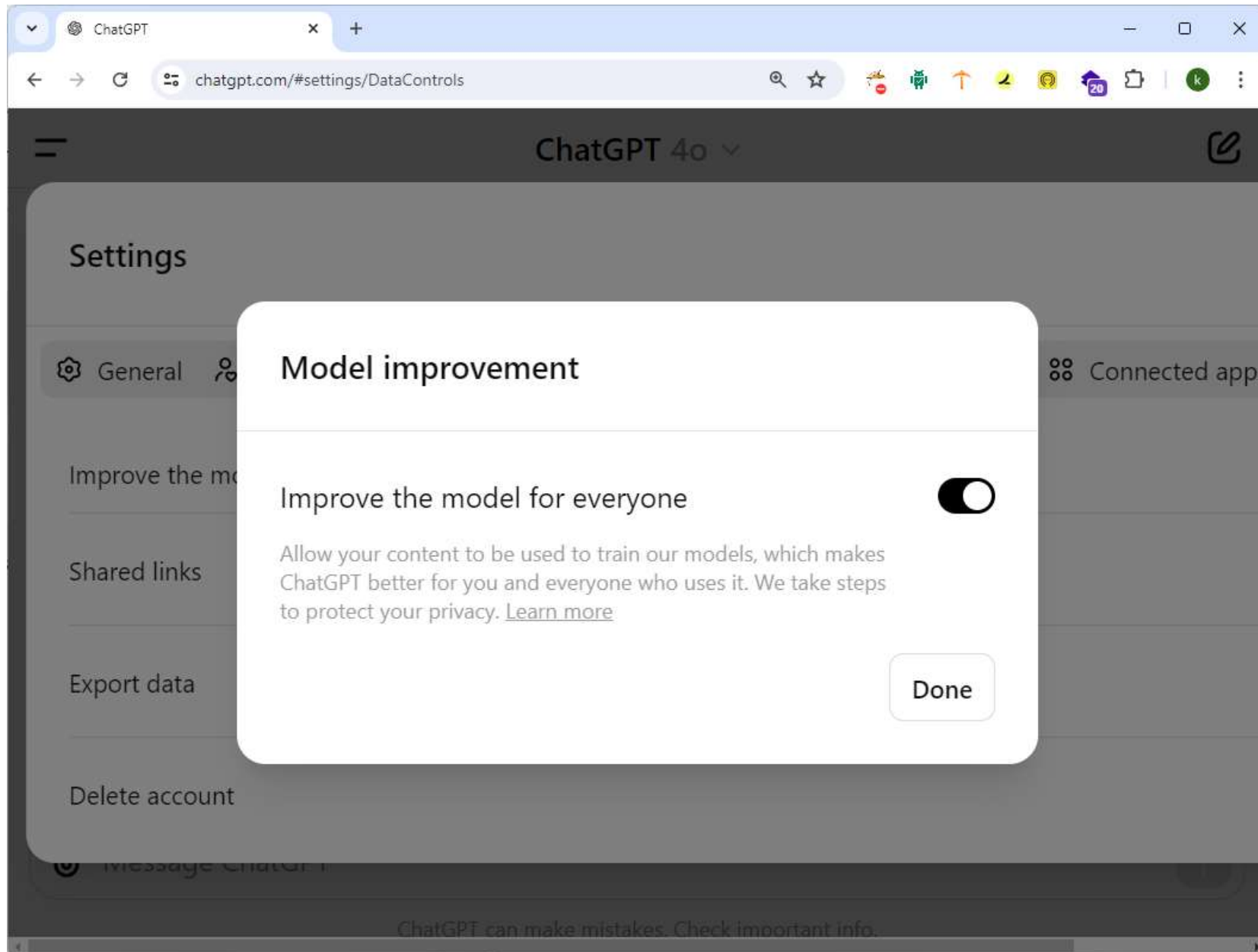
Risks of using of AI in Healthcare



Risks of Using AI in Your Business



Data Leakage Risk



Bias Risk

The screenshot shows a web browser window with the following elements:

- Address Bar:** alumni.berkeley.edu/california-magazine/online/biased-algorithms-exacerbate-rac...
- Navigation:** Membership, Cal Spirit, Get Involved, Give Back, Cal Alumni ASSOCIATION UC Berkeley, Travel, Camp at the Lair, California Magazine.
- Buttons:** JOIN, GIVE.
- Article Title:** Biased Algorithms Exacerbate Racial Inequality in Health Care
- Metadata:** August 12, 2020 by Melba Newsome
- Image:** An illustration of five stylized human figures in light blue lab coats holding hands. From left to right, their heads are brown with a white 'X', brown with a white 'X', light skin with a white checkmark, brown with a white 'X', and brown with a white 'X'. The background is a dark blue network of white lines and dots.

AI Makes Mistakes

ChatGPT 4o ▾

You
Create a table of HITRUST requirements

ChatGPT
Here is a table of HITRUST requirements based on the HITRUST CSF (Common Security Framework):

Requirement ID	Control Domain	Control Objective	Requirement
01.a	Information Security Management Program	Establish and maintain an information security management program	An organization should have an information security management program that includes policies, standards, procedures, and guidelines.
02.a	Access Control	Limit access to information and information systems	Implement policies and procedures to ensure appropriate access controls.
03.a	Human Resources Security	Ensure personnel security	Perform background checks, security training, and define roles and

AI Lies

The screenshot shows a web browser window displaying a CNBC news article. The browser's address bar shows the URL: `cnbc.com/2023/06/22/judge-sanctions-lawyers-whose-ai-writt...`. The CNBC logo is visible in the top left of the page, and a search bar is in the top right. The article is categorized under 'POLITICS' and has a main headline: 'Judge sanctions lawyers for brief written by A.I. with fake citations'. Below the headline, it says 'PUBLISHED THU, JUN 22 2023·2:34 PM EDT | UPDATED THU, JUN 22 2023·3:53 PM EDT'. The author is identified as 'Dan Mangan' with the handle '@_DANMANGAN'. A red 'WATCH LIVE' button is present on the right side of the article header. A 'KEY POINTS' section is located below the author information, containing two bullet points.

POLITICS

Judge sanctions lawyers for brief written by A.I. with fake citations

PUBLISHED THU, JUN 22 2023·2:34 PM EDT | UPDATED THU, JUN 22 2023·3:53 PM EDT

Dan Mangan
@_DANMANGAN

WATCH LIVE

KEY POINTS

- A New York federal judge sanctioned lawyers who submitted a legal brief written by the artificial intelligence tool ChatGPT, which included citations of non-existent court cases.
- In addition to each paying a \$5,000 fine, the attorneys, Peter LoDuca and Steven Schwartz, and their Levidow law firm, were ordered Thursday to notify each judge falsely identified as the author of the bogus case rulings about the

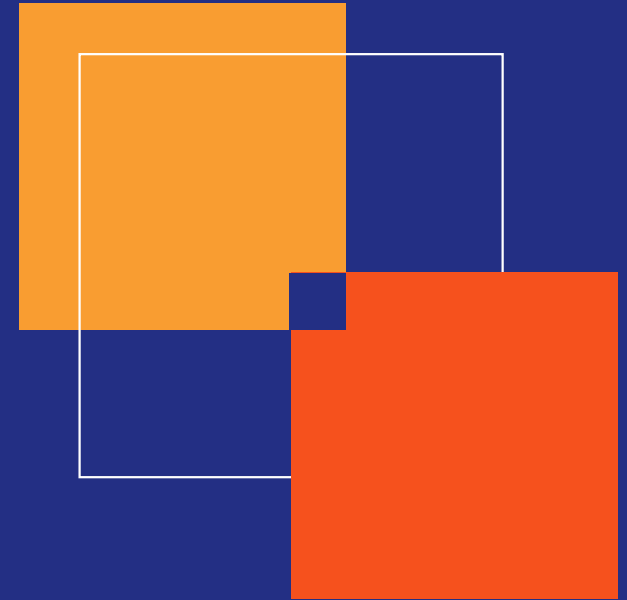
AI Washing

The screenshot shows the top portion of a WilmerHale website. At the top left is a hamburger menu icon. In the center is the WilmerHale logo, consisting of the word 'WILMERHALE' in a serif font followed by a red square containing the white letters 'WH'. To the right is a magnifying glass search icon. Below the navigation bar is a large, dark red banner with white text. The main title of the banner reads 'SEC Enforcement Director Warns Against AI Washing'. Below the title, the date 'APRIL 24, 2024' is centered. At the bottom of the banner, there are two white rectangular buttons: one on the left labeled 'BLOG' and one on the right labeled 'KEEPING CURRENT: DISCLOSURE AND GOVERNANCE DEVELOPMENTS'. The background of the banner is a blurred image of a person in a dark suit sitting at a desk.

On April 15, 2024, Gurbir S. Grewal, Director of the SEC's Division of Enforcement, spoke at a compliance and enforcement conference regarding the challenges and potential missteps associated with the increased use of artificial intelligence (AI).

Analogizing to the recent areas of fraud associated with cryptocurrencies, the SPAC boom, ESG initiatives and

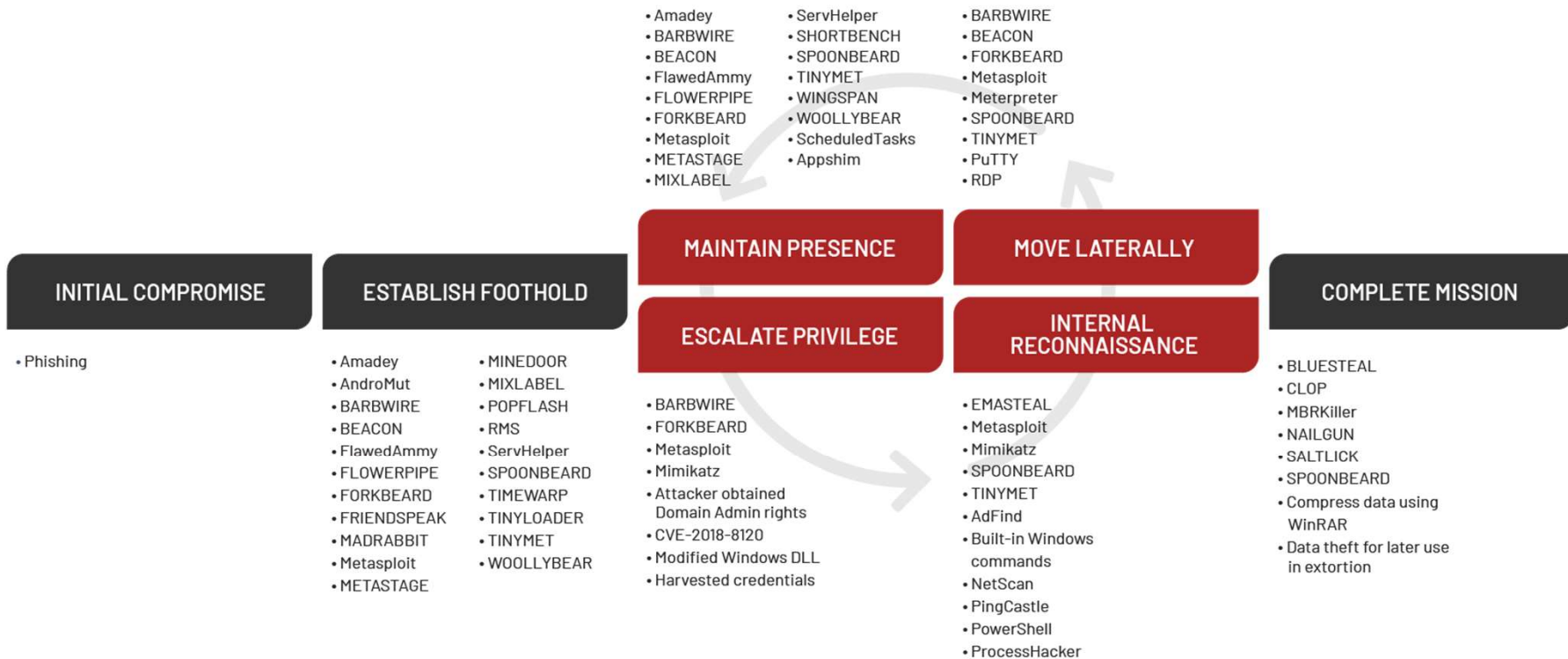
AI's Impact on Cyber Attacks



Generative AI has massively democratized computing to improve adversary operations. It can also potentially lower the entry barrier to the threat landscape for less sophisticated threat actors.

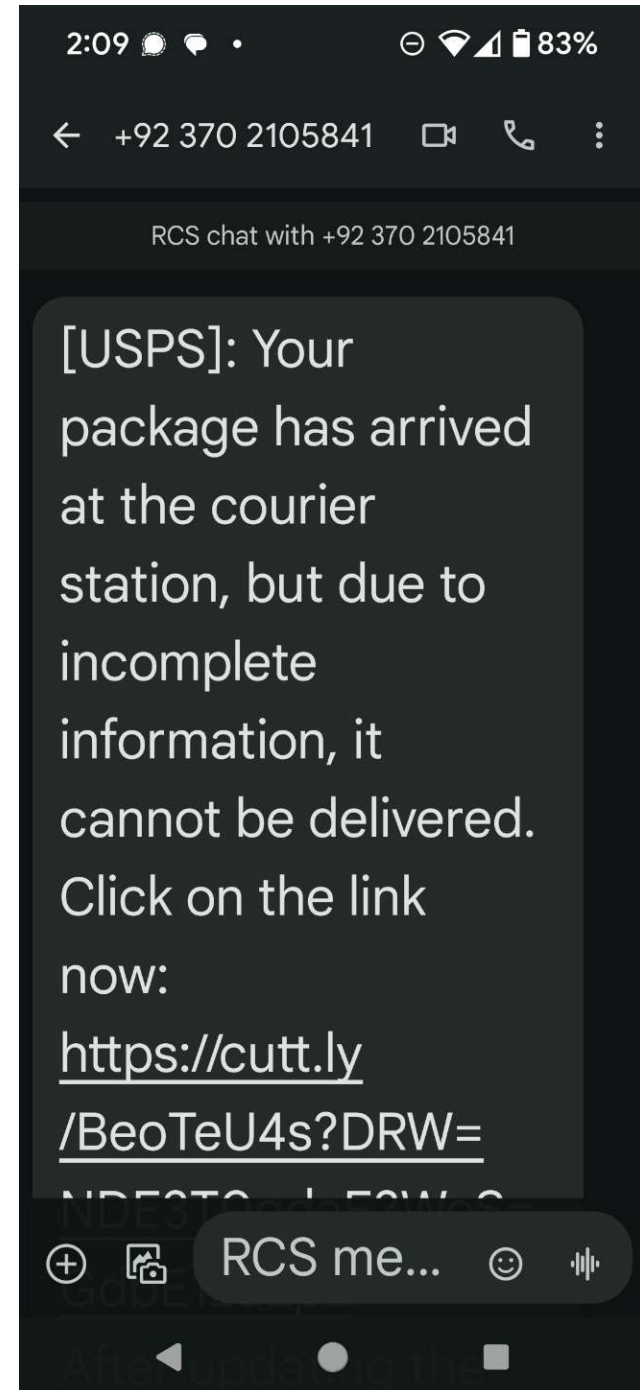
CrowdStrike Global Threat Report 2024

Anatomy of a Ransomware Attack



Identifying Targets and Reconnaissance

- Purposeful Targets
 - Work to intelligently correlate and mine large data sets – “Cell phone numbers of people likely to be patients of X regional hospital”
- Targets of Opportunity
 - Broad scanning – “Check Point firewalls that have not been patched against the vulnerability released in May, 2024”
 - Blind phishing/smishing
 - Mining social media



Gaining Access -

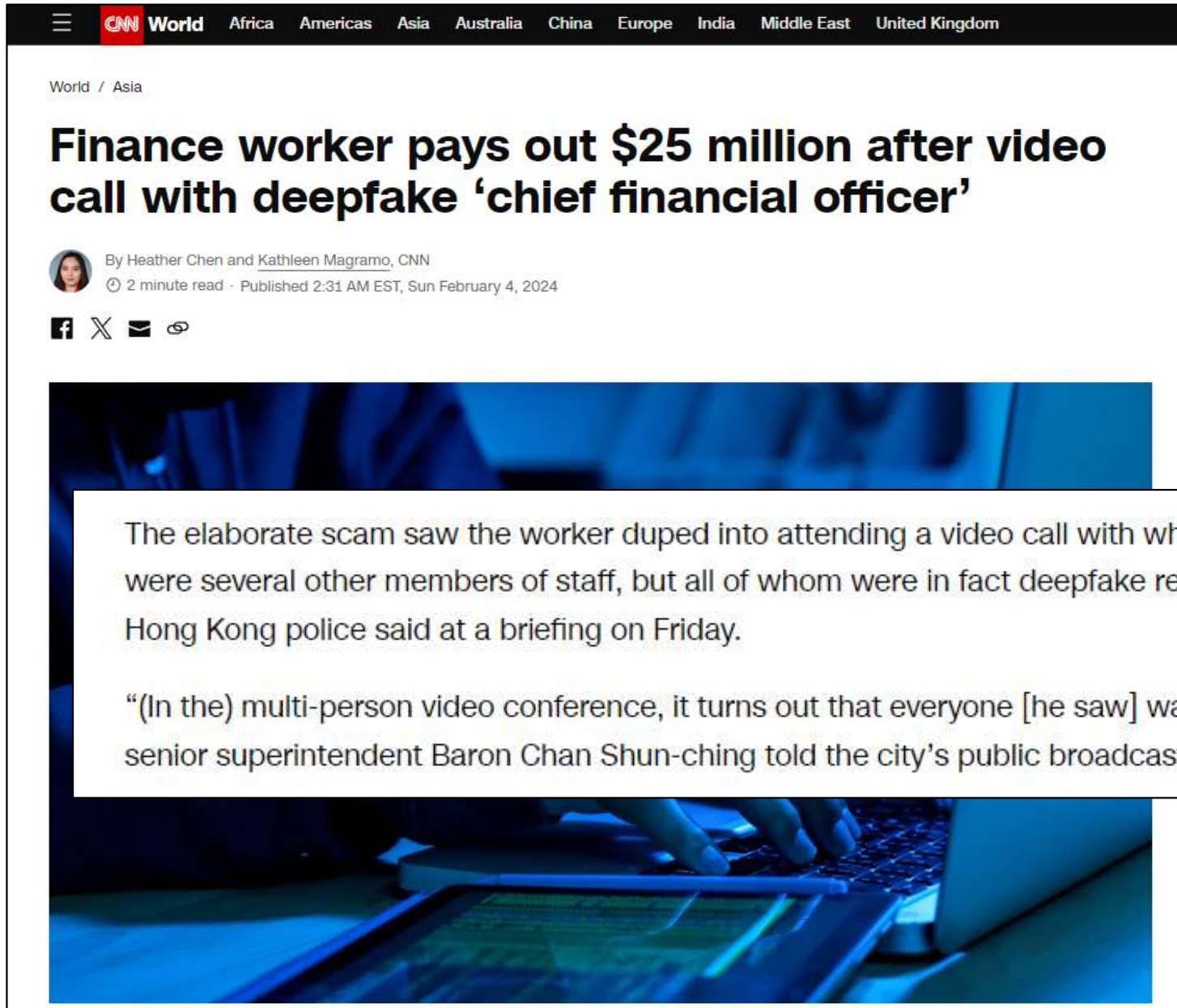
- Vulnerabilities
- Credential Attacks
- Social Engineering

Several Healthcare Data Breaches Unfold From MOVEit Transfer Cyberattack

Allegheny County and other victims of the MOVEit Transfer cyberattacks are starting to reveal the impact the mass-exploited vulnerability has left.



AI Enabled Social Engineering

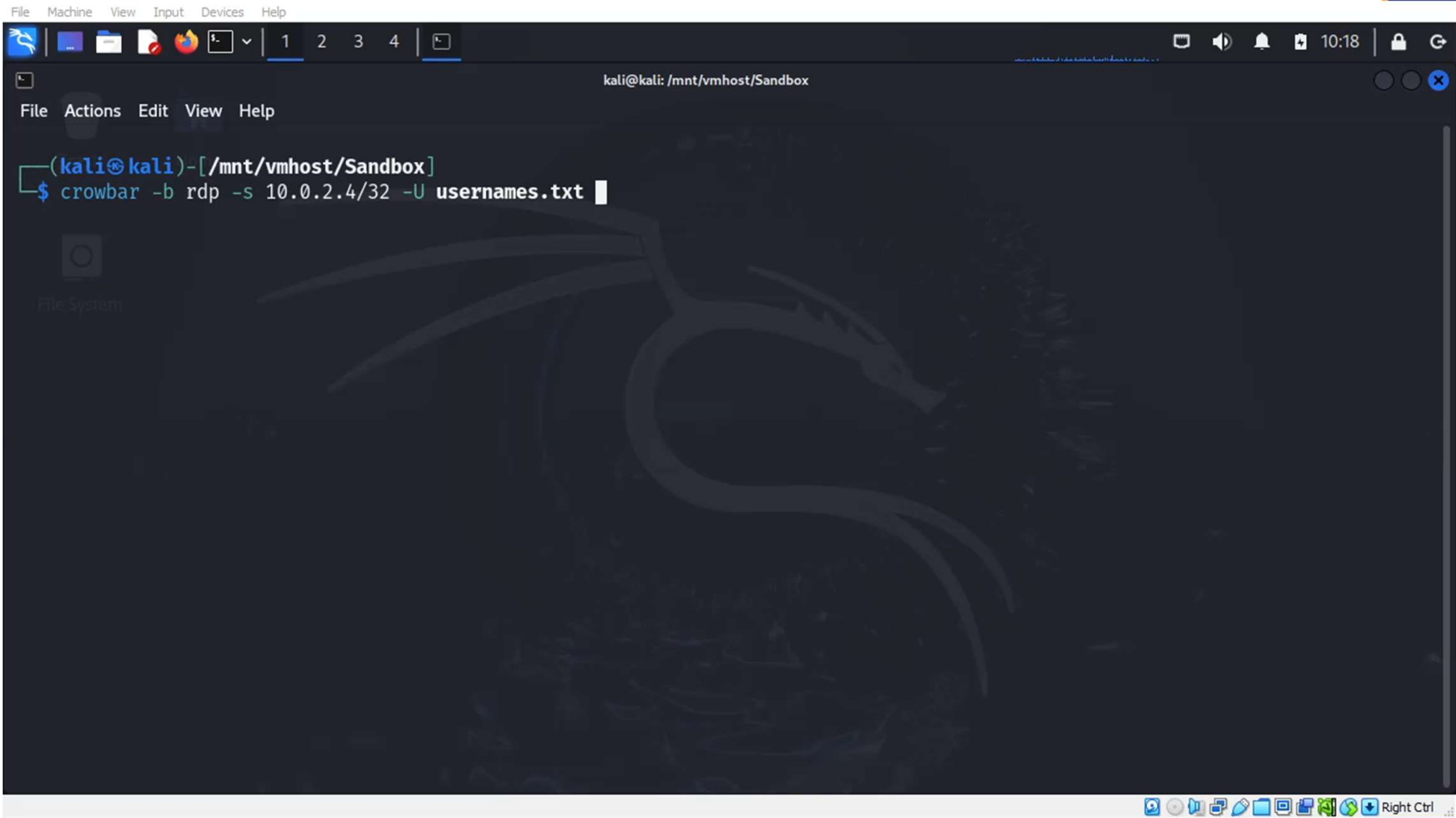


The screenshot shows a news article from CNN World. The navigation bar includes 'World', 'Africa', 'Americas', 'Asia', 'Australia', 'China', 'Europe', 'India', 'Middle East', and 'United Kingdom'. The article title is 'Finance worker pays out \$25 million after video call with deepfake 'chief financial officer''. The byline is 'By Heather Chen and Kathleen Magramo, CNN'. The article is dated '2 minute read - Published 2:31 AM EST, Sun February 4, 2024'. Below the title is a social media sharing bar with icons for Facebook, X, Email, and Print. The main image is a blue-tinted photo of a person's hands typing on a laptop keyboard. A white text box is overlaid on the image, containing the following text:

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

“(In the) multi-person video conference, it turns out that everyone [he saw] was fake,” senior superintendent Baron Chan Shun-ching told the city’s public broadcaster RTHK.

Password Guessing/Password Spraying



The image shows a terminal window on a Kali Linux system. The window title is "kali@kali: /mnt/vmhost/Sandbox". The terminal prompt is "(kali@kali)-[/mnt/vmhost/Sandbox]". The command entered is "crowbar -b rdp -s 10.0.2.4/32 -U usernames.txt". The terminal background features a faint, stylized dragon logo. The window's top bar includes a menu (File, Machine, View, Input, Devices, Help) and a system tray with icons for network, volume, and notifications, along with the time 10:18. The bottom of the window shows a taskbar with various application icons and a "Right Ctrl" button.

```
File Machine View Input Devices Help
kali@kali: /mnt/vmhost/Sandbox
File Actions Edit View Help
(kali@kali)-[/mnt/vmhost/Sandbox]
└─$ crowbar -b rdp -s 10.0.2.4/32 -U usernames.txt
```

Persistence

Ascension cyber attack caused by worker who accidentally downloaded malware

Officials: Attackers accessed 7 of 25,000 servers



Ascension St. John Hospital, Detroit (Copyright 2024 by WDIV ClickOnDetroit - All rights reserved.)

DETROIT - A **cyber attack** that sent Ascension hospitals and health care systems offline in May happened because a worker accidentally downloaded malware, officials said this week.

Defense Evasion

Tech Industry > Artificial Intelligence

ChatGPT Can Generate Mutating Malware That Evades Modern Security Techniques

News By Ash Hill published June 7, 2023

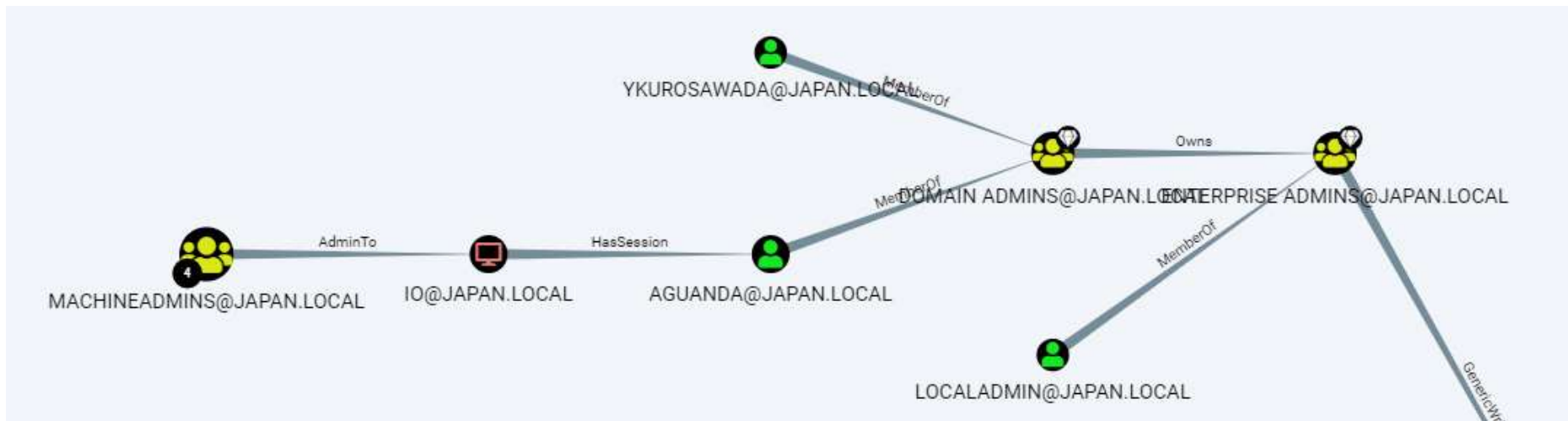
ChatGPT complicates modern IT security with the ability to create mutating malware that's hard to detect with endpoint detection and response (EDR).

[f](#) [X](#) [r](#) [p](#) [F](#) [M](#) [C](#) Comments (47)



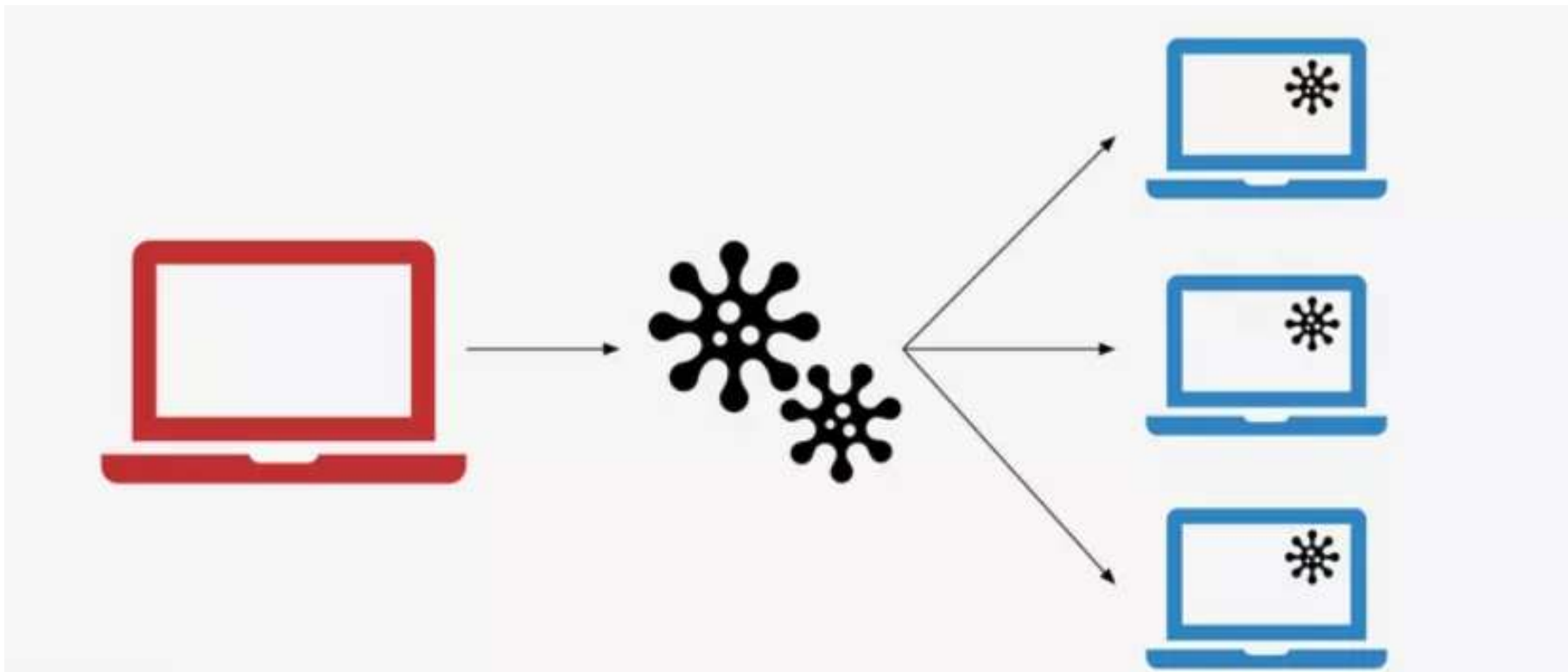
Privilege Escalation, Lateral Movement

- Smarter malware to evade antivirus
- Smarter malware to quickly and automatically find weaknesses and paths through the network



Command and Control

- The attacker still needs to direct the malware
- Creates an opportunity to block the attack at the laptop and at the network perimeter



Data Theft, Exfiltration, Covering Tracks

- Smarter malware to identify and collect sensitive data
- Smarter malware to identify and manipulate audit trails



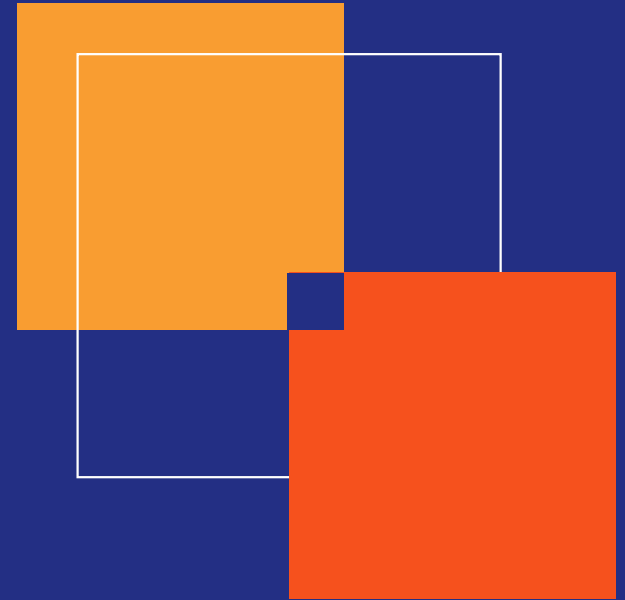
Data Encryption



How to Protect From Emerging Attack Techniques

- Layered best-practice controls
 - Multi-factor authentication
 - Patch management
 - System hardening
 - Centralized anti-virus or EDR
 - Next-generation firewall
 - Account and password security
- Control testing (including vulnerability assessments and penetration testing)
- Reputation and dark web monitoring
- Employee awareness/social engineering exercises
- Transfer risk using cyber insurance

Cyber Insurance



The Insurance Industry and AI

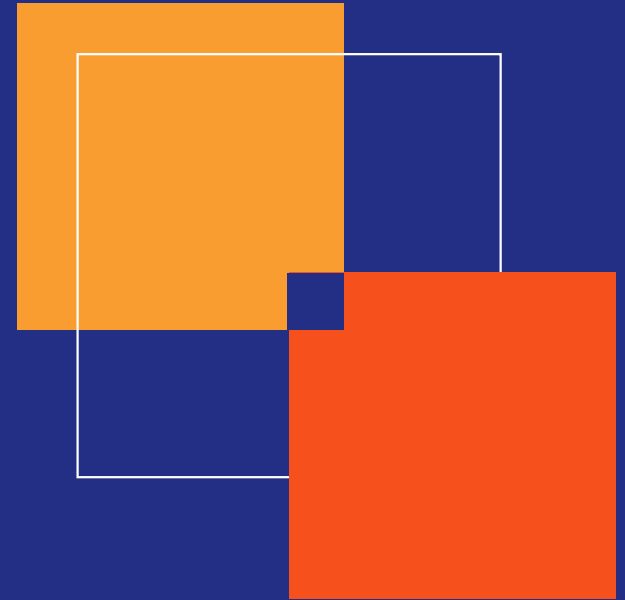
- From a coverage perspective, the industry has largely taken a wait and see approach.
- One insurance company has issued an affirmative AI endorsement.
 - The endorsement expands the definition of security failure and data breach to include an AI security event.
 - The endorsement also expands the trigger for a funds transfer fraud event to include fraudulent instruction transmitted through the use of deepfakes or other AI.
- How does your policy define social engineering?

Reasons why you need a cyber policy

- Claims service
- Coverage
 - Ransomware sublimits
 - Business interruption coverage
 - Dependent business interruption coverage



Top Take-Aways



Top Take-Aways

- Plan for business impacts of AI
 - Address AI in security policies
 - Educate employees
 - Review and evaluate your IT and cybersecurity posture
- Test cybersecurity controls
 - Risk and vulnerability assessments
 - Penetration testing
 - Business continuity and incident response exercises
- Review your cyber insurance policy to ensure you have the proper coverage
 - Social engineering coverage
 - Other restrictions and limitations



Thank you.

Questions?

CONNECT WITH US

800.272.2443

m3ins.com