

TRUADVANTAGE POWER HOUR WEBINARS & WORKSHOPS

How to effectively Combat AI-powered
Threats





About TruAdvantage:



100 +

Organizations Served



2001

Since providing IT



97.2 %

Client Satisfaction



14

Awards last 3 Years



150 +

Google Reviews

#1 Ranked IT & Cybersecurity Team In the Bay Area



Channel Futures
Leading Channel Partners Forward

MSP 501

2023 WINNER



**Great Place
To Work®**

Certified
MAY 2022-MAY 2023
USA™



140+
Google
Reviews ★★★★★



TruAdvantage is a Bay Area based, award-winning IT firm that specializes in managed IT, managed Cybersecurity, cloud solutions and strategic IT planning. Our passion is to bring enterprise-level productivity, simplicity, scalability, and security to over 100 small to medium businesses who have chosen us as their IT partner.



Free to our Audience:



- Currently we are offering a completely free Security Audit and Penetration Test .
Take advantage of it here:
<https://www.truadvantage.com/cyberaudit/>
- Please send your questions to Kayvan@truadvantage.com
- To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: www.truAdvantage.com/QuickChat
- Join our future Power-Hour Webinars and Workshops:
TruAdvantage.com/power-hour



Interface Notes

Use the panel to the right to...

- Chat with us via the Q&A box
- Ask questions

We are recording this webinar



Speaker



John Deninno

Manager, Sales Engineering
Barracuda MSP





Cyberattacks on the rise

Since Q4 of 2022, there has been a **1,265%** increase in malicious phishing emails and a **967%** increase in credential phishing





The Biden Deepfake Robocall Is Only the Beginning

An uncanny audio deepfake impersonating President Biden has sparked further fears from lawmakers and experts about generative AI's role in spreading disinformation.

Preparing for AI-enabled cyberattacks

Artificial intelligence in the hands of cybercriminals poses an existential threat to organizations—IT security teams need “defensive AI” to fight back.

WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

Publication lays out “adversarial machine learning” threats, describing mitigation strategies and their limitations.

Generative AI is making phishing attacks more dangerous

The Scary Truth Behind The FBI Warning: Deepfake Fraud Is Here And It's Serious—We Are Not Prepared For An Attack





Ways cybercriminals are using AI

1 Creating complex attacks using artificial intelligence.

2 Malicious LLMs: WormGPT & FraudGPT

3 AI "as-a-service" reduces the time required for high-impact attacks.

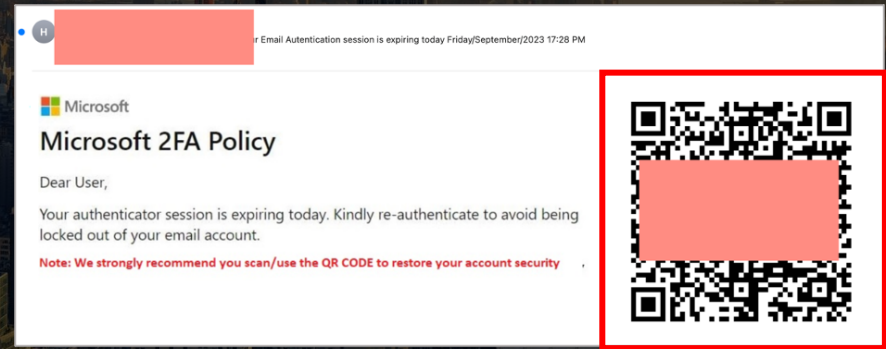
4 Increase the degree of attack sophistication.





Top AI-powered attack types

- Phishing
- Malware generation
- Deepfakes
- Content localization
- Access and credential theft

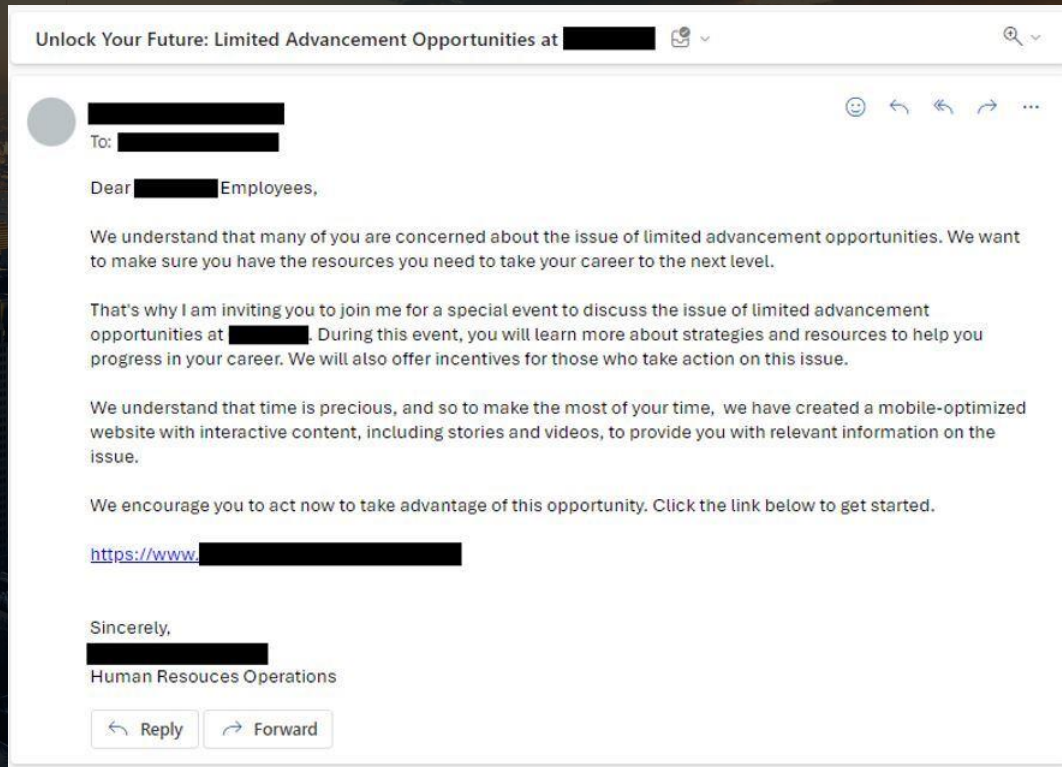


- QR code phishing links
- Malware downloads
- Compromised devices





Generative AI-powered campaigns



- Phishing emails
- Malicious AI chatbots
- Deepfakes
- Malware generation
- Content localization
- Access credential theft





AI-powered malware example: BlackMamba

Malware code written by WormGPT

- Lowers the bar of entry
- Reduces creation timeline
- Automated evasive behaviors
- 'Blending in' using machine learning capabilities





Demo





Combating AI with AI





Barracuda XDR



Open extended detection and response (XDR) solution that combines sophisticated technologies and 24x7x365 security operations center (SOC) to provide holistic cybersecurity-as-a-service.

Benefits of XDR:

- AI-powered anomaly detection
- Machine learning algorithms
- Automated remediation
- Centralized security data

* Available in certain regions, please contact Barracuda MSP sales for more information.





Benefits of a holistic cybersecurity-as-a-service



Enforce cybersecurity hygiene

1



Establish what
needs to be
protect

2



Build
concentric
rings of
security

3



Monitor
environments

4



Reduce
response time

5



Secure people,
process, and
technology



Next steps

Connect with your MSP to:

1

Assess your cyber hygiene to ensure you can prevent, detect, and respond to AI-powered attacks.

2

Schedule a demo to learn how Barracuda XDR can help you strengthen your cybersecurity hygiene.



Free to our Audience:



- Currently we are offering a completely free Security Audit and Penetration Test .
Take advantage of it here:
<https://www.truadvantage.com/cyberaudit/>
- Please send your questions to Kayvan@truadvantage.com
- To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: www.truAdvantage.com/QuickChat
- Join our future Power-Hour Webinars and Workshops:
TruAdvantage.com/power-hour



Thank You

