In the Boxing Ring
MAY 2024

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the May 2024 edition of In the **Boxing Ring**

This month, we are talking about **Generative AI in Cybersecurity: *Balancing Risks and Rewards***. Artificial intelligence (AI) has revolutionized various domains, and cybersecurity is no exception. Generative AI, a subset of AI that focuses on creating new content, presents both significant opportunities and challenges for securing our digital world. On pages 2 to 3, we discuss the potential dangers and benefits of generative AI in cybersecurity.

In other news, Network Box Hong Kong was at **InnoEx 2024** to exhibit our award-winning security technologies and managed services. Additionally, Network Box Hong Kong welcomed the **Office of the Government Chief Information Officer** (OGCIO) to discuss how Hong Kong could enhance its cybersecurity in the face of ever-evolving cyber threats. And in this month's ***Technology Focus***, we are spotlighting **NBSIEM+**. Did you know Network Box offers existing customers FREE 90 days of storage of non-audit event logs with NBSIEM+?

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2024

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

Generative AI in Cybersecurity:

Balancing Risks and Rewards

Artificial intelligence (AI) has revolutionized various domains, and cybersecurity is no exception. Generative AI, a subset of AI that focuses on creating new content, presents both significant opportunities and challenges for securing our digital world. In this article, we'll explore the potential dangers and benefits of generative AI in cybersecurity.

The Risks

Adversarial Attacks:

- Generative AI models can be manipulated to generate adversarial examples that deceive other AI systems. These crafted inputs can bypass security measures, compromise machine learning models, and lead to unauthorized access.
- For instance, an attacker could create a realistic-looking image that fools an AI-based facial recognition system, granting unauthorized access to a secure facility.

Deepfakes and Misinformation:

- Generative AI enables the creation of deepfakes—realistic videos or audio clips that manipulate content. These can be used to spread misinformation, damage reputations, or even influence elections.
- As detection techniques struggle to keep up, the risk of deepfake-driven disinformation campaigns grows.

Self-Evolving Malware:

- Bad actors are exploring generative AI's potential to create self-evolving malware. These malicious programs can adapt and mutate over time, making them harder to detect and combat.
- Traditional signature-based antivirus solutions may struggle to keep pace with such dynamic threats.

Ethical Concerns:

- Generative AI raises ethical questions about its use. For example, should we allow AI-generated content to be used in court as evidence? How do we ensure transparency and accountability?
- The lack of clear guidelines and regulations poses risks to privacy, fairness, and justice.

The Rewards

Threat Identification:

- Generative AI can enhance threat detection by analyzing patterns and anomalies in network traffic, identifying potential cyber threats.
- It can help security teams stay ahead of evolving attack techniques.

Automated Response:

- While full automation remains a challenge, generative AI can assist in automating routine tasks, freeing up human analysts to focus on more complex issues.
- For instance, it can automatically block suspicious IP addresses or quarantine infected devices.

Enhanced Authentication:

- Generative AI can improve authentication methods. For example, it can create unique biometric templates or analyze behavioral patterns for user identification.
- This strengthens security while minimizing user inconvenience.

Vulnerability Patching:

- AI can predict vulnerabilities by analyzing code and system behavior. Generative AI models can then suggest patches or fixes.
- This proactive approach helps prevent zero-day exploits.

Conclusion

Generative AI is a double-edged sword in cybersecurity. While it offers immense potential for threat detection and response, it also introduces new risks. Striking the right balance requires collaboration between governments, tech companies, and cybersecurity experts. We must harness the benefits while mitigating the dangers to ensure a secure digital future for all.

In summary, generative AI holds promise, but its deployment must be guided by ethical considerations and a commitment to safeguarding our digital infrastructure.

For those intrigued or concerned about the promise of Generative AI, I wonder how many readers got this far into the article before they realized that the above text wasn't written by a human but entirely by Microsoft Copilot (a publicly available Generative AI system)?

As one can see, when given a task (in this case, something like 'write an article about the risks and rewards of generative AI in cybersecurity'), these systems can pull together information from various sources and present it in a clear well-written way with perfect spelling and grammar. What if, instead of a benign article, the AI was instructed to prepare something malicious? This should concern us all. Like most such tools, Generative AI is a two-edged sword offering both risks and rewards - and not understanding the implications of those is a far greater threat than the technology itself.

Network Box HIGHLIGHTS

Network Box Hong Kong
InnoEX 2024

Network Box Hong Kong was at **InnoEX 2024**, which took place at the HK Convention and Exhibition Centre. During the four-day expo, visitors were introduced to Network Box's award-winning security technologies and managed services. Additionally, Network Box Managing Director, Michael Gazeley, gave a talk titled, *"Top 10 cybersecurity facts you need to know."*

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Network Box Hong Kong
OGCIO Visit

Ir. Tony Wong, Hong Kong Government Chief Information Officer, along with Daniel Cheung, Assistant Government Chief Information Officer, visited Network Box to discuss how Hong Kong could enhance its cybersecurity in the face of ever-evolving cyber threats from Hackers, Malware, and vendor supply chain-induced Vulnerabilities.

Network Box Technology Focus

Did you know...

Network Box offers existing customers FREE 90 days of storage of non-audit event logs with NBSIEM+?

The Network Box Security Incident and Event Management Plus (NBSIEM+) system integrates all the security logs and incidents into one centralized system. This allows users to view all security incidents and events for all devices within their network.

For more details about NBSIEM+ and how to subscribe to the service, please visit:

https://network-box.com/nbsiem