www.pwc.com/ng

Improve Your Cyber Security Posture With Artificial Intelligence

The rate at which cybercriminals are launching attacks against companies around the world is alarming. These attacks are becoming more frequent such that they can no longer be ignored anymore by business owners and stakeholders.

Cyber criminals keep advancing with new attack strategies and different attack vectors to compromise systems and exploit their victims with the use of artificial intelligence technology (AI) or solutions.

Artificial Intelligence (AI) technology or solutions can learn to recognize patterns in human behavior, such as convincing people that a video, phone call, or email is genuine and then convincing them to compromise networks and hand over sensitive information.

pwc

July 2021

Successful Cyber-Attack Defense Strategy

Cyberattacks are becoming more prevalent, and they have been identified as one of the most strategically significant risks confronting the world today. In recent years, we have seen digital attacks on governments and owners of critical infrastructure, local and global private companies, educational institutions, and non-profit organizations.

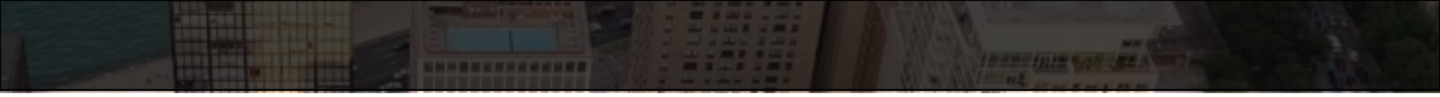
1. **Adoption of Artificial Intelligence to Combat Criminal Attacks:** The Emotet trojan, one of the most notorious pieces of modern malware, is a prime example of a prototype-Artificial Intelligence (AI) attack. Emotet's primary distribution method is spam-phishing, which is typically accomplished through invoice scams that trick users into clicking on malicious email attachments. The authors of Emotet have recently added a new module to their trojan that steals email data from infected victims. Although the source of such email exfiltration capability was not divulged, Emotet was recently observed sending out structured phishing emails on a global level. This means it can quickly insert itself into existing email threads and strongly urge the victim to click on a malicious attachment, which further appears in the final malicious email.

2. **Cyber Criminal Attack Vector:** The criminals behind the creation of Emotet, on the other hand, could easily use Artificial Intelligence (AI) to amplify this attack. The overall current cost of a data breach in companies that did not provide security automation was 95 percent higher, according to the “2019 Cost of such a Data Breach Report”. Security automation is defined as "enabling security technologies that augment or replace human intervention in the target identification and containment of cyber exploits or breaches," according to Phonemon.

3. **Boosting Cyber Security Posture with Artificial Intelligence (AI):** If the cybercriminals can use Artificial Intelligence (AI) technology or solutions, then every organization can adopt the use of Artificial Intelligence (AI) to automate their processes and help mitigate Cybersecurity Risk thereby protect the organization's Data. This can be achieved by:

   - Automating Patch Management Process
   - Detecting new Threats and obtaining Threat Intelligence in Real Time
   - Effectively Managing Incident Response
   - Automating Vulnerability and Penetration Testing
   - Conduct Third-Party Risk Assessment
   - Error Handling and Risk-Effective Analysis (keeping your cyber security error-free)

4. **Return on Investment with Artificial Intelligence:** Business leaders must approach Artificial Intelligence (AI) investment in the same way they would any other technology investment. This implies that it must serve a specific purpose and achieve a specific goal, it must be measured using benchmarks and key performance indicators (KPIs) and you must hold yourself and your teams accountable for those figures. Consider the overall prospective ROI of the business. If a bottleneck operation exists in the automation process, productivity must always be increased throughout the organization, not just in one area.



Questions for Business and Security Leaders?

01 Do you actively draw lessons and technical resources from publicised breaches?

02 Do your teams know how to incorporate those lessons into their work to improve security and incident response?

03 Do you proactively hunt for threats in your environment, instead of only reacting to alerts?

How PwC Nigeria's Cybersecurity and Privacy Practice Helps Businesses to Create Value:

At PwC we help you build resilience so that you can confidently adapt and grow. We bring the right capabilities and experience to aid the delivery of your objectives. Our team of dedicated professionals have significant business and technical experience to help you address your most complex imperatives. We leverage the power of our global network to provide organizations with deeper, broader and timely expertise on evolving cybersecurity and privacy challenges.

Our services include:

- CISO as a Service
- Cyber Transformation
- Cyber Risk Management and Quantification
- Technical Assessments - Cyber Penetration Testing and Application Security
- Security Standards Compliance Management
- Cyber Incident Response and Investigations
- Third Party Security Assessments
- Privacy Maturity Assessments and Compliance
- Training and Awareness (Digital Risk and Cybersecurity Academy)

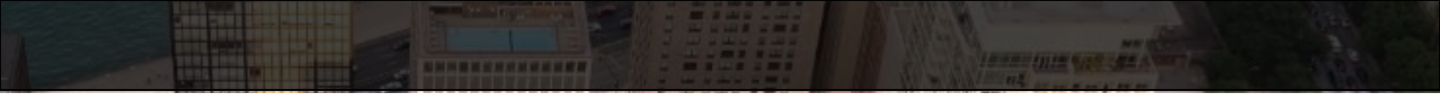
For more information, please contact:

Wunmi Adetokunbo-Ajayi
Partner Digital Risk and Cyber Security, PwC.
wunmi.adetokunbo-ajayi@pwc.com

Nkiruka Aimienoho
Director Cyber Security, Privacy and Resilience, PwC.
nkiruka.aimienoho@pwc.com

Chika Nwachukwu
Manager Digital Risk and Cyber Security, PwC.
chika.nwachukwu@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.



References

Cyber Criminal Attack Vector

Zdnet, Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation, January 2021
Kaspersky Lab, Emotet: How to best protect yourself from the Trojan, 2021
Malwarebytes, Emotet, 2021
F-Secure, Trojan:W32/Emotet, 2021
Zdnet, This trojan malware is now your biggest security headache, March 2021

Adoption of Artificial Intelligence to Combat Criminal Attacks:
Boosting Cyber Security Posture with AI
BioMed Central Ltd, Crime Science: AI-enabled future crime, August 2020
Centre for European Policy Studies (CEPS), Artificial Intelligence and cybersecurity, April 2021
Verizon: 2019 Data Breach Investigations Report, 2019
TechnologyAdvice-eWeek, How AI is Mishandled to Become a Cybersecurity Risk, April 29, 2021
Coordinated Business Systems Ltd, Six Simple Ways to Improve Your Cybersecurity, Apr 30, 2018
Tech Republic, How to combat the latest and most aggressive botnets, November 12, 2020

Return on Investment with Artificial Intelligence:
Forbes, Five Ways To Improve Your Company's Cybersecurity, Dec 1, 2020
Britannica, Alan Turing and the Beginning of AI,17 Jun 2021
Forbes, 10 Powerful Examples Of Artificial Intelligence In Use Today, Jan 10, 2017

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.