УДК 04.056.54., 004.493

V. A. Harnaha[1]

NEURAL NETWORKS IN PHISHING ATTACS

[1] Vinnytsia National Technical University

Анотація

З року в рік збільшується число фішингових атак та розмір збитків, які вони завдають економікам різних країні. З кожним роком інструментарій кіберзлочинців все більше розширюється і вони навіть починають використовувати нейромережі для створення досконалих листів зі шкідливим змістом, підвищуючи ефективність нападів.

Ключові слова: фішинг, кіберзлочинці, нейронні мережі.

Abstract

From year to year, the number of phishing attacks and the damage they cause to the economies of various countries are increasing. Every year, the toolbox of cybercriminals expands more and more, and they even begin to use neural networks to create perfect emails with malicious content, increasing the effectiveness of their attacks.

Keywords: **phishing, cybercriminals, neural networks.**

Introduction

By now, we all know about Open AI's ChatGPT, a free neural network chatbot that generates well-written, convincing content in English and other languages and can even write and debug software code. It has been called an AI tipping point, and its implications for everything from college student essays to marketing content and software development are startling, to say the least. There's another area for which ChatGPT and its AI competitors have startling implications as well: phishing. We are not just talking about an AI-empowered leap in phishing sophistication but phishing volume as well. In fact, the implications are so devastating and potentially overwhelming for IT organizations that the only way to fight back against this AI weapon is with other AI weapons[1].

The overview

So, why it is so dangerous that hackers use neural network in phishing? There are a few factors there:

1) There are no more telltale English spelling and grammar mistakes that alerted humans and tools to phishing emails until now. As with college essays and marketing content, neural networks can generate beautifully written, well-structured emails on just about any subject. You just need to enter, "Write an email from the company CEO to employees, subject Urgent Action Required, New Stock Options Plan Announced. Urge employees to click on the attachment today," and in seconds, the ne network will generate a beautifully written, grammatically flawless email doing just that. Foreign hackers can even write phishing emails in another language and use chat bots like ChatGPT to translate them into perfect English, not to mention enhance them[1].
2) Cybercrimes can use ChatGPT or similar tools to refine phishing emails again and again, regenerating them in different and better permutations and styles. They can ask ChatGPT to suggest ideas to convince recipients to open an attachment today. They can train AI tools on large datasets of previous phishing emails or emails from legitimate company senders to generate more convincing phishing emails and create new types of attacks that evade phishing detection systems. Users can leverage scripts that search LinkedIn and other social media for a target company executive and staff names and titles and feed the information to ChatGPT to generate personalized phishing emails[1].
3) You should be ready for a stream of phishing emails now that hackers don't have to spend a lot of time writing and refining them by themselves. Expect the flood to overwhelm users, traditional email filtering tools, and security and IT departments. Prepare for an exponential increase in the number of cybercrimes since nobody needs hacking sophistication to phish anymore and for the use of automated tools on the dark web that empower anyone to generate thousands of auto-

mated personalized phishing emails for multipronged phishing attacks.

4) In addition, ChatGPT can generate very usable code for convincing web landing pages, invoices for business email compromise (BEC) attempts, and anything else hackers need it to generate. So, in the nearest future we would see a lot of different phishing sites[1].

Together these factors are really frightening, and it seems the legacy tools could help here but the answer to AI-empowered phishing lies in AI anti-phishing weaponry. AI-empowered tools have the scale and smarts to address the higher phishing volumes to come. They can harness their understanding of email content, context, metadata, and trusted behavior to detect anomalies characteristic of phishing attempts across hundreds of thousands of emails.

By training themselves on legitimate email content and context, AI tools can determine instantly if an email's language content and style resemble that of equivalent past emails from legitimate senders. In addition, they can evaluate whether an email has come at roughly the same time and day of the month from the same sender as past similar emails, whether it uses the same path to traverse the Internet, and contains the same email headers, bank account numbers, and customer IDs. Zero trust is essential in a phishing environment with such high volumes.

It may be tempting to give up on user training with this powerful new threat, but doing so would be a big mistake. As I noted previously, neural networks may be a critical weapon in the battle against phishing, but users will always be the last line of defense, even at the phishing volumes and sophistication we can expect in the years ahead. Finnaly, a lot of companies develop different tools for detecting fishing e-mails, and we should use them to prevent data leaks. As an example of a complex solution, we can name presented by the Cisco company a new complex IronPort protection tool, which is aimed specifically at combating targeted phishing. This security tool provides protection against targeted phishing through email and web traffic monitoring and message authentication technology [2].

Conclusions

Therefore, in order to protect against new types of phishing attacks, you need to constantly improve your knowledge in cyber security, organize continuous training of staff, and use new comprehensive tools to fight such threats.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Eyal Benishti, Prepare For The AI Phishing Onslaught – Forbes, 2023.
2. Кравченко, В., Руденко, О., Доманов, І. і Казначей, С. (2022) «АНАЛІЗ ФІШИНГ-АТАК. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАПОБІГАННЯ ТА ЗАХИСТУ», Збірник наукових праць; Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, 11(1), с. 85-95. doi: 10.37701/dndivsovt.11.2022.10.

Гарнага Володимир Анатолійович — магістрант групи 1БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: garnaga.v@gmail.com.

Harnaha Volodymyr A. — Department of Information Technology and Computer Engineering, Vinnytsya National Technical University, Vinnytsia, email: garnaga.v@gmail.com.