ISSUE
January
2025

CYBERTimes

by CyberIntel

this issue

OpenAI says hackers keep trying to use its services for cyber attacks

OpenAI has disrupted more than 20 attempts to use its models since the beginning of the year, but said the attempts to use its tools to disrupt elections or build malware appear to have largely failed — as had a targeted phishing attack against staff.

OpenAI described threat actors using ChatGPT to debug malware, writing content for fake social media accounts and creating disinformation articles, the company warned in a report.

"Activities ranged in complexity from simple requests for content generation, to complex, multi-stage efforts to analyze and reply to social media posts," the company added. "They even included a hoax about the use of AI."

CyberIntel Groundbreaking Technology bypasses VPN

CyberIntel's innovative technology leverages cutting-edge algorithms and machine learning to identify vulnerabilities in VPN protocols commonly used by hackers. By exploiting these weaknesses, our proprietary patent technology can quickly and accurately trace the precise location of hackers, providing real-time tracking capabilities for law enforcement agencies. This breakthrough advancement in cybersecurity allows for swift and effective measures to be taken against cyber threats, ensuring a safer digital landscape for all users.

How it works?

The CyberGuard proprietary technology developed by CyberIntel leverages advanced packet inspection techniques and machine learning algorithms to analyze encrypted traffic passing through the suspect's VPN connection. By identifying unique patterns and anomalies in the data packets, CyberGuard can perform deep packet inspection to uncover the real IP address and geolocation of the hacker suspect, even when they are using a VPN to mask their identity and location. Additionally, CyberGuard's sophisticated network mapping capabilities allow it to trace the suspect's connection path and accurately pinpoint their precise location, enabling cyber investigators to track and apprehend the hacker with pinpoint accuracy.

The awareness created by our groundbreaking technology will act as a strong deterrent against cybercrime. Criminal elements will come to realize that their attempts at ransomware and other malicious hacks now carry a significant risk of detection and capture. By instilling fear and apprehension among hacker communities, we anticipate an immediate reduction in the incidence of hacking by over 80%. CyberGuard's seal stands as a singular commitment to safeguarding digital landscapes worldwide, heralding a new era where cybercriminals are held accountable and cyber integrity is staunchly protected.

Why do businesses need zero trust?

Digital transformation is making traditional perimeter-based cybersecurity models ineffective and irrelevant. Data is no longer simply contained within a single environment controlled by the business it belongs to, as was the case in the past. The rapid increase of remote working, BYOD, and IoT over the last ten years has created multiple endpoints for the average business, leaving ample opportunity for malicious attacks.

What's more, the hacker tool kit has never been more innovative with an abundance of techniques at their disposal. What's more, the growth and increasing sophistication of generative AI is only going to make the situation worse.

Cyber attacks are steadily increasing year-on-year, according to research from Check Point. With a 30% rise in weekly attacks on corporate networks in Q2 2024, and a 25% rise compared to Q1 of this year, the security firm estimates that there are now an average of 1,636 attacks per organization, per week.

CyberIntel's Global Commercial Launch

We anticipate at least an 80% decrease in cyber attacks in the first year alone due to our powerful message. ***We will win the cyber war!***

Our new CyberIntel commercial serves as a powerful tool in combating hacker criminals by unveiling the capabilities of our proprietary patent technology. By vividly illustrating how this technology can instantly trace and locate hackers within seconds, the commercial is designed to strike fear into the hearts of potential cybercriminals. Through compelling visuals and persuasive messaging, the commercial aims to create a sense of urgency among hackers, deterring them from targeting our customers.

Furthermore, the commercial acts as a beacon of awareness within the cybersecurity realm, shedding light on the harsh consequences that hackers may face if they attempt to breach our systems. By showcasing the efficiency and effectiveness of our technology in action, the commercial not only educates viewers but also instills a sense of caution and wariness among potential perpetrators. This heightened awareness serves as a vital deterrent, dissuading hackers from even contemplating the idea of targeting our clientele.

Moreover, the impact of this commercial transcends mere advertisement; it is a strategic move to significantly reduce hacker attacks. With a strategic media placement and a targeted audience reach, the commercial is poised to make a resounding impact on cybercriminal activities. By leveraging the fear factor and showcasing the unmatched tracking capabilities of our technology, the commercial is poised to witness a drastic reduction in hacker attacks by up to 80% within the first year alone.

In essence, our new CyberIntel commercial is not just a marketing tool but a potent weapon in the fight against cybercrime. Through its innovative approach, with its compelling narrative and strategic dissemination, the commercial stands as a formidable force that will deter hackers, safeguard our customers, and significantly curtail cyberattacks in the digital landscape.

We will win the cyber war!

Furthermore, the fear of being easily caught and facing severe consequences for their actions will significantly deter hackers from targeting our customers. The combination of swift detection, strong identification, and efficient response to potential threats creates a hostile environment for hackers, making it increasingly challenging for them to operate undetected. With our hacker locator capability constantly monitoring and protecting our systems, hackers are left with limited opportunities for successful breaches, ultimately making them think twice before attempting any malicious activities.

Technology Solutions for Casinos

A very well known Casino giant expects $100 million hit from hack that led to data breach

An exterior view of the casino hotel hotel, after the Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023

The casino Resorts International said on Thursday a cyberattack last month that disrupted its operations would cause a $100 million hit to its third-quarter results, as it works to restore its systems.

One of the world's largest gambling firms, the casino giant shut down its systems after detecting the attack to contain damage, it said. It expects to also incur less than $10 million as a related one-time cost in the quarter ended on Sept. 30.

After the attack last month, customers posted social media images showing slot machines with error messages and queues at hotels in Las Vegas.

The casino hotel giant has declined to comment on whether it was asked for or paid any ransom.

CyberIntel's CyberGuard Patent Technology

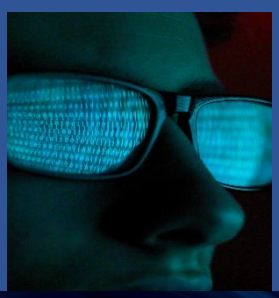
By deploying real-time intrusion detection systems and machine learning algorithms, CyberIntel not only thwarts hacker attempts through dynamic threat isolation and behavioral analysis but also employs sophisticated digital forensics. This enables pinpoint accuracy in tracing cyber attackers through their digital trail, often hidden within complex networks, to their precise geolocations using cutting-edge geo-mapping technologies. Such proactive measures mitigate financial losses of billions annually.

This Month's Cybersecurity Tips

Q: Is blocking hacker attacks enough?

A: While blocking hack attacks is a crucial component of cybersecurity, it is not enough to fully deter future incidents. Focusing solely on defensive measures can create a reactive rather than proactive security posture, leaving systems vulnerable to innovative or sophisticated attack methods that evolve over time.

The key strategy to effectively combating cybercrime lies in identifying and apprehending the perpetrators behind these attacks. This approach not only disrupts the criminal activities of specific hackers or hacking groups but also serves as a significant deterrent to others When hackers witness consistent law enforcement activity leading to prosecutions and penalties, they are more likely to think twice before attempting to infiltrate a system.



CyberIntel is

Equipped, Armed and Ready!

CyberIntel is strategically equipped to revolutionize the security landscape in the casino industry by implementing state-of-the-art cybersecurity measures that not only thwart cyber threats but also proactively hunt down cyber criminals. By employing cutting-edge intrusion detection systems (IDS) integrated with advanced machine learning algorithms, CyberIntel can identify and learn attack patterns to preemptively block unauthorized access attempts. Furthermore, through the deployment of real-time threat intelligence platforms combined with sophisticated IP geo-location tracing technologies, CyberIntel can pinpoint cyber-attacks to their source, enabling swift engagement of law enforcement agencies for apprehension of suspects. This multi-layered defense strategy minimizes the risk of data breaches and significant financial losses, safeguarding casinos against potential revenue depletion — estimated to save billions annually — by preserving customer trust and ensuring uninterrupted operations.

Continual Enhancement

In today's ever-evolving digital landscape, staying ahead of cyber threats requires continuous innovation and adaptation. Our approach to improving hacker locator technology is driven by a commitment to maintaining cutting-edge performance in threat detection and mitigation.

Upcoming Plans

- **Launch Global Commercial**

  Launch global commersial to bring awareness to our propietary patent technology (CyberGuard Hacker & Ransomeware locator. Our goal is to let hackers know they need to think twice before hacking our customers because we will find you!

- **Launch Global Marketing Campaign of to release the latest version CyberGuard**

  Our goal is to get our CyberGuard in every american to assure they are not only safe and secure while online, but we will find these hacker suspects. We want to give our users pease of mind while surfing online.

- **Release Webcam Shield**

  Release our new propietary patent technology app called Webcam Shield. Our new app will blcok prepdators and pedaphlia and trace their location to apprehend.the suspects. No more spying on victims privacy web cams.

- **Launch Major Marketing Campaign for Webcam Shield**

  Launch global commersial to bring awareness to our propietary patent technology (Webcam Shield Predator & Pedaphilia Locator). It's time to put these discusting criminals away.

CyberIntel
powered by PC Logic

32565 GOLDEN LANTERN ST
UNIT 163
DANA POINT CA 92629-3247
www.pclogic.com