GPT-Powered MITRE ATT&CK Copilot

Steve Ng
Co-Founder
SporeX Pte. Ltd.
steve@sporex.ai

About SporeX.AI

We are on a mission to enhance the speed and accuracy of threat intelligence analysis using AI technology.

Our vision at SporeX.AI is to be the leading provider of AI-powered cybersecurity solutions, empowering security teams to create a safer and more secure digital world.

Our mission is to eliminate cybersecurity data overload, providing clear, actionable insights through advanced LLM and AI technologies.

Steve Ng
Co-Founder

Jerry Tay
Co-Founder

SPOREX
ARTIFICIAL INTELLIGENCE

The Evolving Threat Landscape in Cybersecurity

Overview of Current Cybersecurity Challenges

- ***Sophisticated Threats***: Cyberattacks are increasingly complex, making traditional security measures less effective.
- ***Skills Gap***: There's a shortage of skilled cybersecurity professionals.
- ***Data Overload***: The sheer volume of security data makes it impossible for humans to analyze everything effectively.

Need for Advanced Solutions

- How conventional tools are failing to keep up with complex cyber threats.
- The critical gap in real-time threat detection and response.
- Deep technical analysis of threats based on the MITRE ATT&CK Framework.

Making Advanced Cybersecurity Accessible

Simplifying Technical Jargon

- We translate complex cybersecurity terms and concepts into more accessible language, making the information easier to understand for executives and professionals across all levels.

Data Synthesis and Reporting

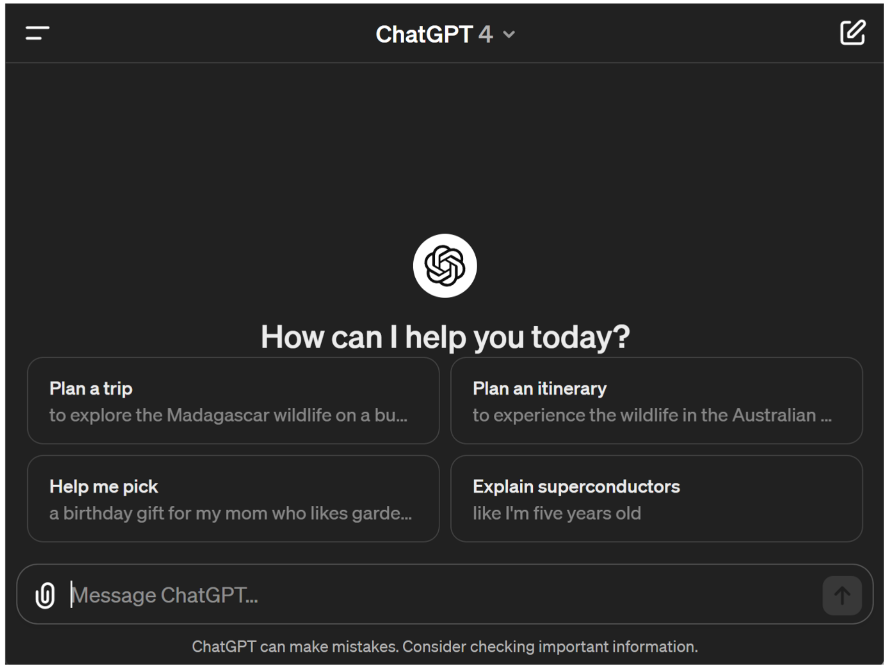
- Our system processes vast amounts of data into concise, comprehensive reports for swift, clear and actionable insights.

Enhancing Framework Usability

- We make it easier for you to adopt and integrate the MITRE ATT&CK framework into your daily operations by automating the identification of relevant tactics and techniques to simplify and streamline incident response.

What are Generative Pre-trained Transformers (GPT)

GPTs are a revolutionary class of artificial intelligence models designed to understand and generate human-like text based on the input they receive.



How can I help you today?

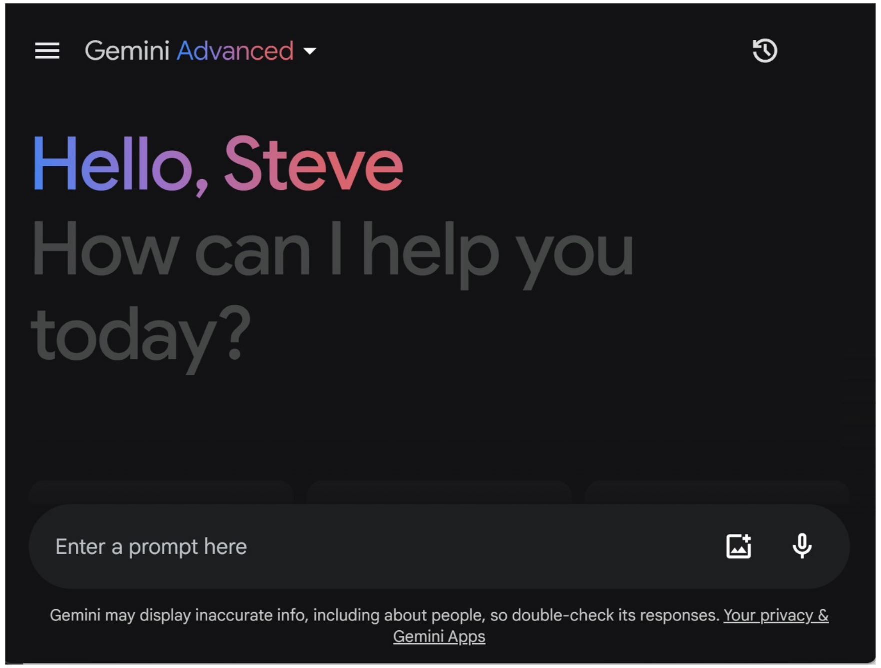
Plan a trip
to explore the Madagascar wildlife on a bu...

Plan an itinerary
to experience the wildlife in the Australian ...

Help me pick
a birthday gift for my mom who likes garde...

Explain superconductors
like I'm five years old

ChatGPT can make mistakes. Consider checking important information.



Hello, Steve
How can I help you today?

Gemini may display inaccurate info, including about people, so double-check its responses. Your privacy & Gemini Apps

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

- **Automated Threat Intelligence Analysis**
- **Dynamic Threat Detection and Response**
- **Enhanced Incident Reporting and Analysis**
- **Customized Security Awareness and Training**
- **Predictive Security Posture Enhancement**

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

1. Automated Threat Intelligence Analysis

Process vast amounts of unstructured data

Automated generation of detailed, context-rich threat intelligence

Reduces the time and effort required for threat analysis

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

2. Dynamic Threat Detection and Response

Development of dynamic detection tools

Enabling quicker and more effective responses to emerging threats

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

3. Enhanced Incident Reporting and Analysis

Automatically generate comprehensive incident reports

Detailed analyses of attack vectors, affected systems, and recommended mitigation strategies

Streamlines the reporting process, ensures consistent and thorough documentation of incidents

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

4. Customized Security Awareness and Training

Create customized training materials and simulations

Improves overall awareness of cybersecurity best practices among employees

The Synergy between GPT and MITRE

The combination of these technologies enhances cybersecurity measures:

5. Predictive Security Posture Enhancement

Analyze historical cyberattack data alongside current cyber trends to forecast future attack vectors

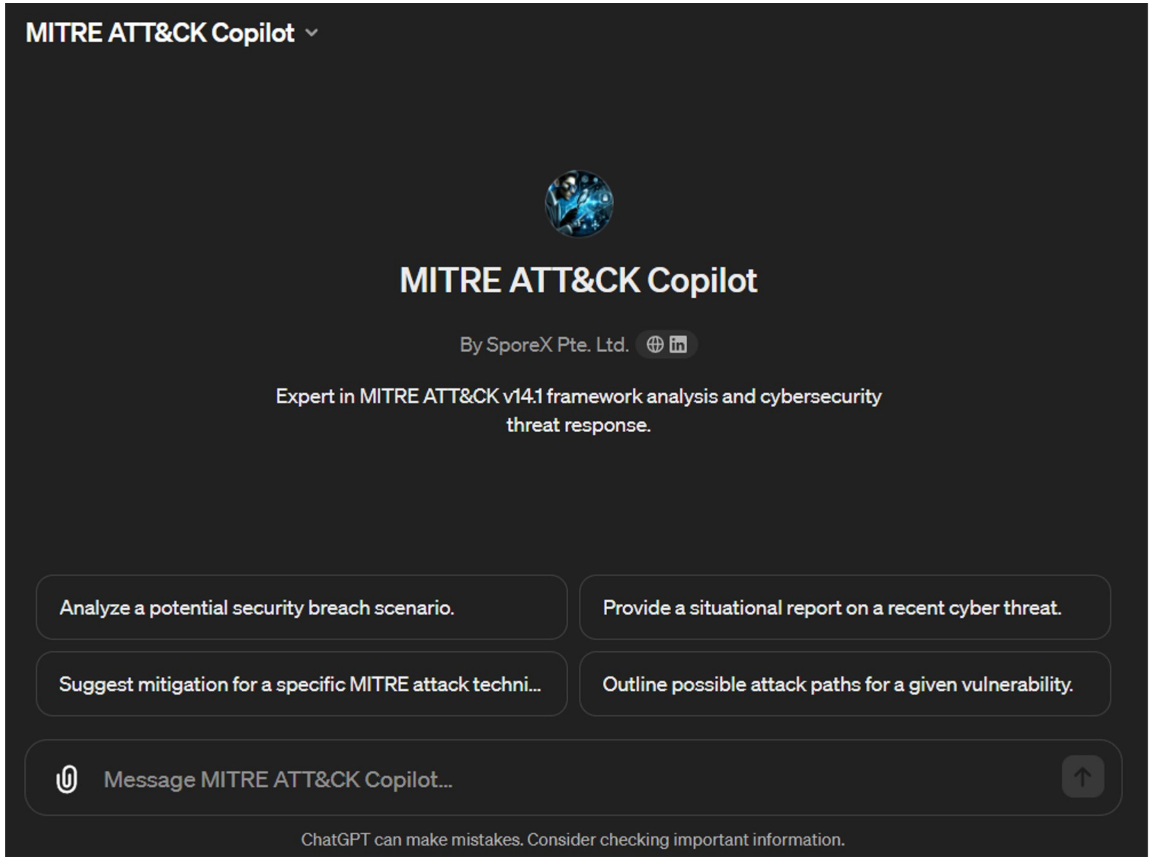
Help organizations proactively adjust their security postures, focusing on relevant defense strategies

Forward-looking approach enables a more adaptive and resilient cybersecurity strategy

Enhancing Threat Intelligence with GPT

Integrating GPT with the MITRE ATT&CK framework can significantly augment threat intelligence capabilities.

- *Comprehensive Data Synthesis & Analysis*
- *Enhanced Situational Awareness*
- *Predictive Threat Modeling*
- *Automated Threat Hunting*
- *Customized Threat Intelligence Reporting*


MITRE ATT&CK Copilot
Analyze a potential security breach scenario.
Provide a situational report on a recent cyber threat.
Suggest mitigation for a specific MITRE attack techni...
Outline possible attack paths for a given vulnerability.
Message MITRE ATT&CK Copilot...

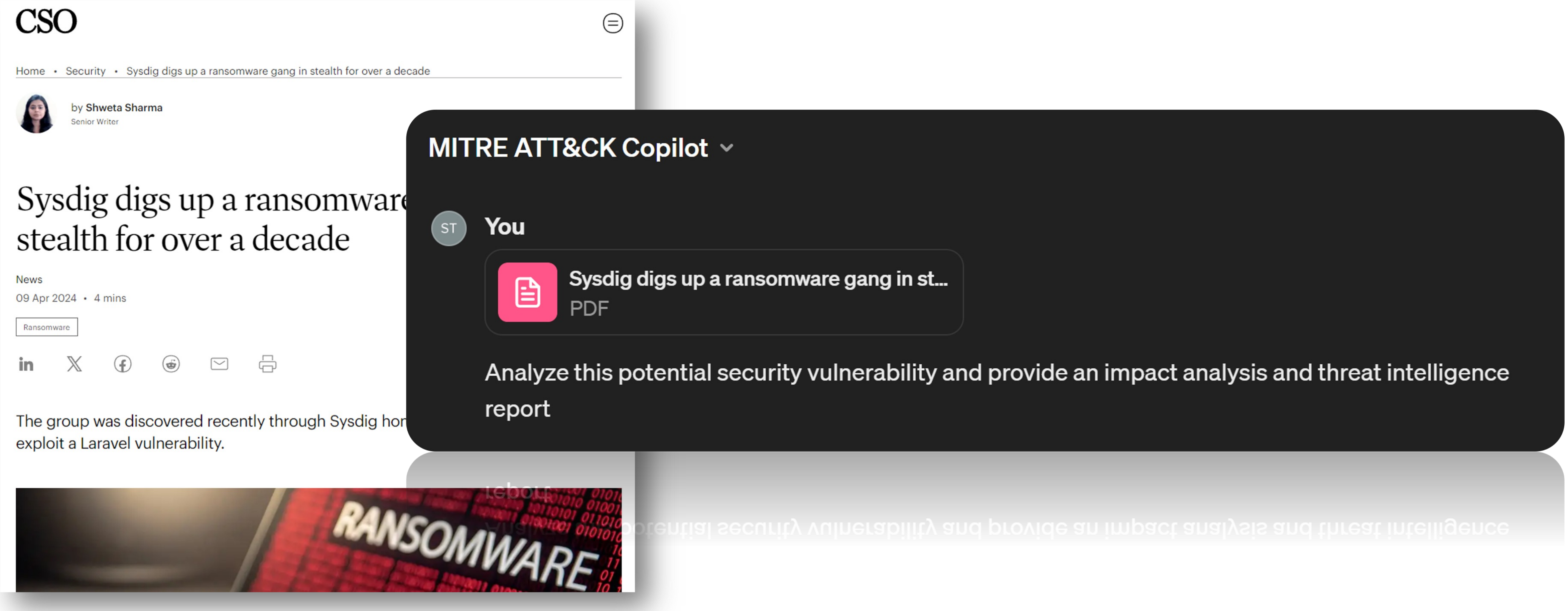
MITRE ATT&CK Copilot

By SporeX Pte. Ltd.

Expert in MITRE ATT&CK v14.1 framework analysis and cybersecurity threat response.

ChatGPT can make mistakes. Consider checking important information.

Example: Enhancing Threat Intelligence with GPT



CSO

Home • Security • Sysdig digs up a ransomware gang in stealth for over a decade

by **Shweta Sharma**
Senior Writer

Sysdig digs up a ransomwar stealth for over a decade

News
09 Apr 2024 • 4 mins

Ransomware

The group was discovered recently through Sysdig hor exploit a Laravel vulnerability.

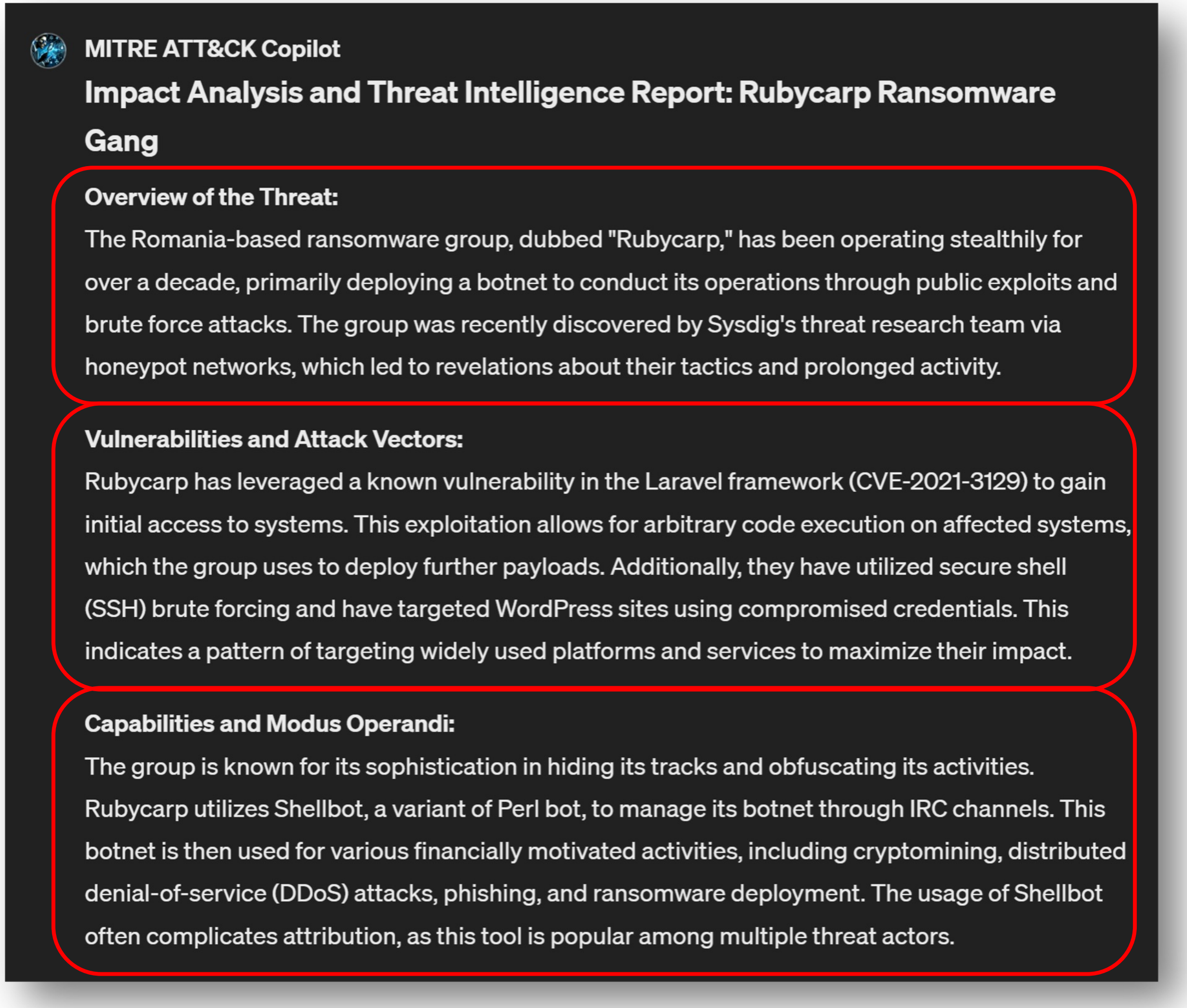
MITRE ATT&CK Copilot

ST **You**

Sysdig digs up a ransomware gang in st...
PDF

Analyze this potential security vulnerability and provide an impact analysis and threat intelligence report

MITRE ATT&CK Copilot



MITRE ATT&CK Copilot

Impact Analysis and Threat Intelligence Report: Rubycarp Ransomware Gang

Overview of the Threat:
The Romania-based ransomware group, dubbed "Rubycarp," has been operating stealthily for over a decade, primarily deploying a botnet to conduct its operations through public exploits and brute force attacks. The group was recently discovered by Sysdig's threat research team via honeypot networks, which led to revelations about their tactics and prolonged activity.

Vulnerabilities and Attack Vectors:
Rubycarp has leveraged a known vulnerability in the Laravel framework (CVE-2021-3129) to gain initial access to systems. This exploitation allows for arbitrary code execution on affected systems, which the group uses to deploy further payloads. Additionally, they have utilized secure shell (SSH) brute forcing and have targeted WordPress sites using compromised credentials. This indicates a pattern of targeting widely used platforms and services to maximize their impact.

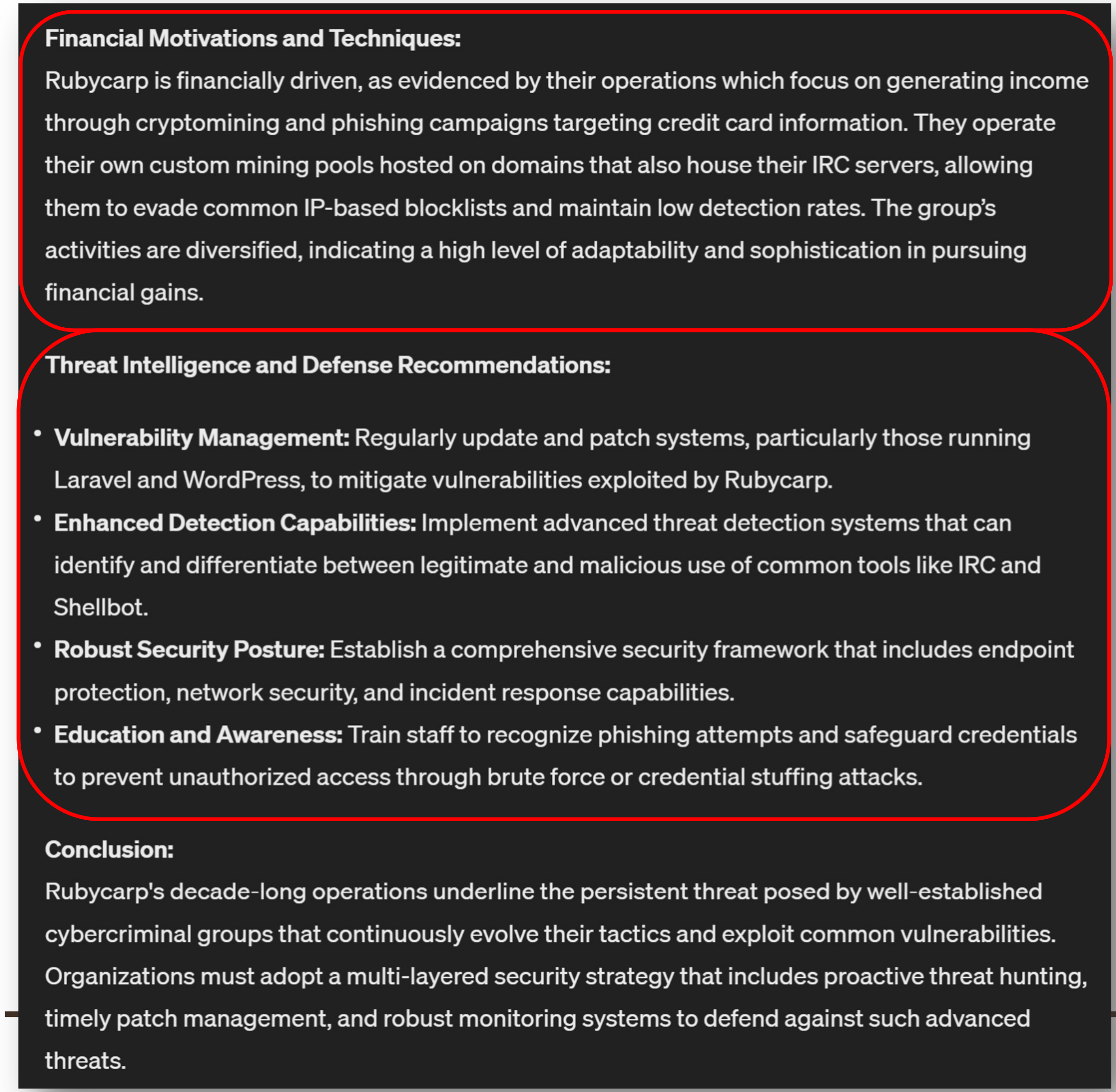
Capabilities and Modus Operandi:
The group is known for its sophistication in hiding its tracks and obfuscating its activities. Rubycarp utilizes Shellbot, a variant of Perl bot, to manage its botnet through IRC channels. This botnet is then used for various financially motivated activities, including cryptomining, distributed denial-of-service (DDoS) attacks, phishing, and ransomware deployment. The usage of Shellbot often complicates attribution, as this tool is popular among multiple threat actors.

Provides an Overview of the Threat "Rubycarp"

Describe the Vulnerabilities, Software Component, CVE and MITRE ATT&CK Tactic, etc

Describe Rubycarp's Capabilities and Modus Operandi

MITRE ATT&CK Copilot



Financial Motivations and Techniques:

Rubycarp is financially driven, as evidenced by their operations which focus on generating income through cryptomining and phishing campaigns targeting credit card information. They operate their own custom mining pools hosted on domains that also house their IRC servers, allowing them to evade common IP-based blocklists and maintain low detection rates. The group's activities are diversified, indicating a high level of adaptability and sophistication in pursuing financial gains.

Threat Intelligence and Defense Recommendations:

- **Vulnerability Management:** Regularly update and patch systems, particularly those running Laravel and WordPress, to mitigate vulnerabilities exploited by Rubycarp.
- **Enhanced Detection Capabilities:** Implement advanced threat detection systems that can identify and differentiate between legitimate and malicious use of common tools like IRC and Shellbot.
- **Robust Security Posture:** Establish a comprehensive security framework that includes endpoint protection, network security, and incident response capabilities.
- **Education and Awareness:** Train staff to recognize phishing attempts and safeguard credentials to prevent unauthorized access through brute force or credential stuffing attacks.

Conclusion:

Rubycarp's decade-long operations underline the persistent threat posed by well-established cybercriminal groups that continuously evolve their tactics and exploit common vulnerabilities. Organizations must adopt a multi-layered security strategy that includes proactive threat hunting, timely patch management, and robust monitoring systems to defend against such advanced threats.

Insights into the Threat's Financial Motivation and Techniques

Take Actions with Threat Intelligence and Defense Recommendations

Revolutionizing Incident Response

Automated Incident Analysis

- Rapidly analyze incident reports and logs to identify the nature and scope of a cyber attack.
- Quickly pinpoint the attack vectors and affected systems
- Significantly reducing the time needed for initial analysis.

Real-time Decision Support

- Suggests the most effective response strategies based on the type of attack, historical data on similar incidents, and best practice guidelines.
- Helps teams make informed decisions quickly, improving the accuracy of the response efforts.

Streamlined Communication

- Automates the generation of incident reports, executive summaries, and updates for stakeholders.
- Ensuring that communication is clear, consistent, and timely.
- Helps facilitate a coordinated response effort.

Future of Cybersecurity with AI

The Evolving Landscape of Cybersecurity with AI Advancements

- Enhanced Threat Detection
- Automated Incident Response
- Behavioral Analytics
- Proactive Risk Assessment

Future of Cybersecurity with AI

Future Trends integrating AI Technologies with Cybersecurity Frameworks

Natural Language Threat Intelligence

Phishing Attack Generation & Defense

AI-Powered Vulnerability Analysis

Automated Incident Response Playbooks

GPT-Powered MITRE ATT&CK Copilot

Key Takeaways

Enhanced Threat Intelligence

Improved Incident Response

Future Potentials

our product ↑

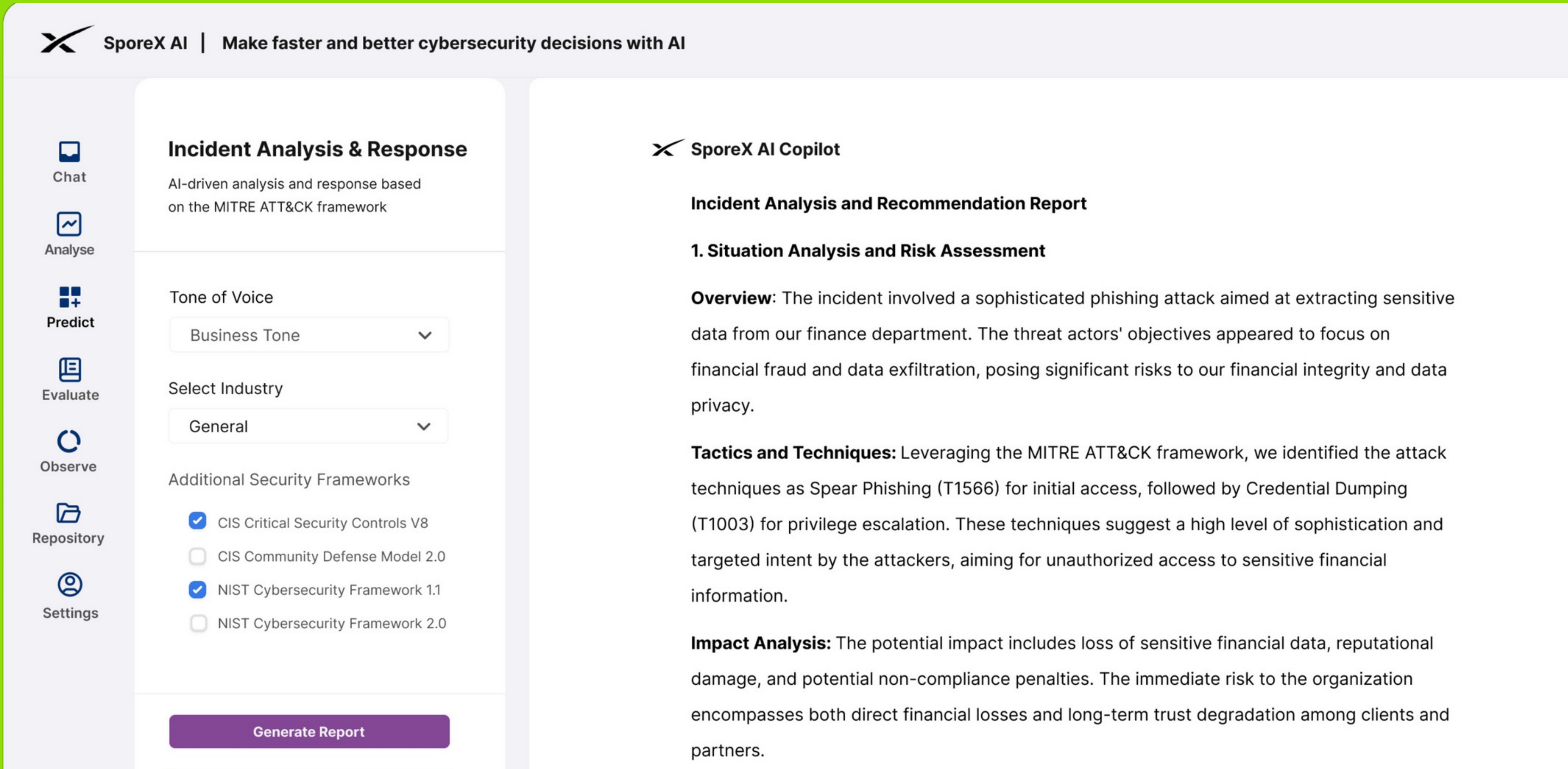
SPOREX
ARTIFICIAL INTELLIGENCE

Unveiling SporeX.AI: AI-Powered Cybersecurity Copilot

Your AI-Powered Partner for Advanced Threat Detection & Response

- **Security Posture Assessment:** Gain a comprehensive view of your security vulnerabilities.
- **Threat Prediction & Detection:** Identify potential attacks before they occur.
- **Incident Analysis & Recommendation:** Receive clear guidance for rapid incident response.
- **User Behavior Analytics:** Uncover insider threats and suspicious activities.
- **SporeX.AI with MITRE ATT&CK Integration:** Amplify threat intelligence and decision-making.

our platform



Incident Analysis & Response

AI-driven analysis and response based on the MITRE ATT&CK framework

Tone of Voice: Business Tone

Select Industry: General

Additional Security Frameworks

- ☑ CIS Critical Security Controls V8
- ☐ CIS Community Defense Model 2.0
- ☑ NIST Cybersecurity Framework 1.1
- ☐ NIST Cybersecurity Framework 2.0

Incident Analysis and Recommendation Report

1. Situation Analysis and Risk Assessment

Overview: The incident involved a sophisticated phishing attack aimed at extracting sensitive data from our finance department. The threat actors' objectives appeared to focus on financial fraud and data exfiltration, posing significant risks to our financial integrity and data privacy.

Tactics and Techniques: Leveraging the MITRE ATT&CK framework, we identified the attack techniques as Spear Phishing (T1566) for initial access, followed by Credential Dumping (T1003) for privilege escalation. These techniques suggest a high level of sophistication and targeted intent by the attackers, aiming for unauthorized access to sensitive financial information.

Impact Analysis: The potential impact includes loss of sensitive financial data, reputational damage, and potential non-compliance penalties. The immediate risk to the organization encompasses both direct financial losses and long-term trust degradation among clients and partners.

Thank you

Try out SporeX.AI MITRE ATT&CK Copilot

https://bit.ly/SporeX-MITRE

Steve Ng
Co-Founder
SporeX Pte. Ltd.
steve@sporex.ai