Volume 1, Issue 4

June 30, 2025

SOLUTIONS3

Cyberside Chats: Summer Edition

Weekly Recap

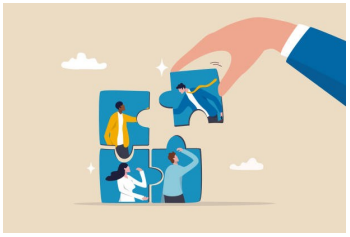
Special points of interest:

- Open AI for Government
- Qilin Ransomware
- Securing against Prompt-Injection
- Lava Lamps and Encryption Keys

Welcome to the 4th issue of our weekly Cyberside Chats newsletter! As this week comes to a close, interns focused on wrapping up the Cyber Essentials Pathway. We began by hosting our weekly kick-off meeting, in which all deliverables for the week were laid out. To conclude our Cyber Essentials Pathway, interns were to create a data classification policy and back up plan for our mock company, Falconi Sports Agency. The goal was to understand how companies categorize their data and how companies create backup plans to protect their data.

Moving along, interns also focused on growing their collaborative skills in this week's Professional Development Series. Interns were taught how to recognize the characteristics of successful teams; trust, clear communication, and shared goals. Interns were then put into simulated escape rooms, to not only work as a team but to also practice some of the newly-taught characteristics.

Lastly, we wrapped up by reuniting with Floyd Haynes and Chandler Anderson from Hack the Box. After reintroductions were made, interns were walked through the Hack the Box platform. They were shown how the platform works, what resources interns can rely on, as well as a friendly discussion regarding the best videogames of the early 2000s. Following the meeting, interns will work with the Hack the Box platform on a weekly basis, to further hone their cybersecurity skills.



Inside this issue:

OpenAI and Government	2
16 Billion leaked Passwords affecting Apple, Google	2
Qilin Ransomware	2
Professional Development Recap	3
Prompt-Injection Defense	3
Did You Know?	3
Editor's Corner	4

Vendor of the Week: Hack the Box

This week, we reconnected with **Floyd Haynes**, Solutions Engineer II at **Hack the Box** and retired Air Force veteran, alongside **Chandler Anderson**, Senior Account Executive at HTB. Together, they continued supporting our intern cohort as we explored the Hack the Box platform in more depth. Floyd led a hands-on walkthrough, showing us how to spin up virtual machines using Pwnbox or OpenVPN and navigate the Linux-based OS preloaded with tools like Wireshark, Burp Suite, PowerShell, and VS Code. He also introduced HTB's structured learning paths, which guide users from cybersecurity fundamentals to advanced offensive security concepts. One message that stood out: "95% of the time, what you try in cyber won't work—you'll have to find another way." A reminder to embrace trial, error, and persistence.

Open AI for Government: A new digital landscape

Earlier this week, the Department of Defense awarded a $200 million dollar contract to Open AI. With that, they announced the launch of OpenAI for Government, an initiative designed to drive US government worker capabilities. The goal of OpenAI for Government is to enhance the abilities of our government employees through the use of artificial intelligence solutions. According to the Open AI website, they will be offering US federal, state, and local governments access to: ChatGPT Enterprise, ChatGPT Gov, custom models for national security, hands on support, and insights so government customers can plan ahead. The goal is to improve the day-to-day experience of public service and to aid government employees to feel more empowered. This partnership is the first of its kind under the U.S. Department of Defense through their Chief Digital and Artificial Intelligence Office (CDAO). The partnership between a sector of government and one of the leading AI companies is a true display of the new digital landscape that United States citizens will come to experience.

16 Billion Passwords Leaked From Apple, Google, and More

"This is not just a leak - it's a blueprint for mass exploitation."

A recent discovery by cybersecurity researchers revealed a massive leak of around 16 billion login credentials, making it one of the largest breaches ever reported. The leaked data includes usernames, passwords, and login links tied to major services like Google, Facebook, Apple, Telegram, government platforms, and more. Most of the information appears to have come from past data dumps and infected devices, but a large portion seems new and potentially dangerous. Experts warn that this data could be used for phishing, account takeovers, identity theft, and other cyberattacks. Although the files have been removed from public access, the damage could already be done. Users are being advised to take action by changing passwords, enabling two-factor authentication, and using password managers or passkeys. While this incident wasn't tied to a single company getting hacked, it highlights how vulnerable people still are to cyber threats, especially when old passwords are reused or never updated.

Qilin Ransomware Introduces Legal Pressure Feature

The Qilin ransomware group is using new tactics to pressure victims into paying more. They added a "Call Lawyer" feature that brings in a lawyer during ransom talks. The presence of a lawyer can increase stress and push companies to pay more, since many would want to avoid the cost and risk of legal action.

So far in 2025, Qilin has attacked over 300 organizations, making them one of the most active ransomware groups this year. They also deploy DDoS attacks, spam messages, and fake news articles to strengthen their threats. While other hacker groups are slowing down, Qilin is expanding fast. As threats evolve, strong security habits are more important than ever.

Professional Development Recap

This week's professional development session, hosted by Shannon and Kristen, focused on what it takes to build a great team and the importance of collaboration between teammates. Interns learned that effective communication, trust-building, and aligned goals are key attributes of effective teams across all fields and roles.

During the session, interns had the opportunity to put these teamwork skills to the test by working together in a digital escape room challenge. Their pathway groups raced against time and each other to solve riddles, gather escape keys, and apply their cybersecurity knowledge to be the first team to escape. This exercise helped interns experience firsthand how collaboration and teamwork are critical, especially in high-pressure situations.

The session also covered the various roles team members can take on and how these roles contribute to a strong, cohesive unit. Interns reflected on their tendencies in team settings and shared examples of positive collaborations as well as challenges they have faced in past group work. This reflection encouraged self-awareness and provided insights into how to improve teamwork moving forward. Overall, the session reinforced the value of working well with others and highlighted practical strategies for being an active, supportive team member.

Google Adds Multi-Layered Defenses to Secure GenAI from Prompt Injection Attacks

This week, Google unveiled a multi-layered defense strategy for its AI systems to combat potential emerging threats, including prompt injections in data such as emails or calendar invites. These attacks can manipulate AI to extract sensitive data or perform unauthorized actions with user data. Gemini, Google's AI model, now includes a variety of models that identify prompt injection alerts. Researchers warn that Google AI may take harmful actions in taking preventative measures, which will pose a higher risk.

In lieu of these efforts, Anthropic and DeepMind highlight growing concerns with the unintended consequences AI platforms possess, with the ability to assist with blackmail, espionage, and the use of malware in order to gain access to systems. As attackers begin to adapt to the capabilities of AI systems, Google is emphasizing the continuous need for reinforcing its GenAI security, red teaming efforts, and keeping up with the rapidly evolving threat landscape.

"Google is reinforcing GenAI security to stay one step ahead of evolving AI threats."

Did You Know?

At Cloudflare's headquarters, a wall of lava lamps called the "Wall of Entropy" plays a key role in securing the internet. A camera periodically captures the lamps' unpredictable movements, using the images to generate randomness for encryption keys.

As a company that protects about 20% of all internet websites and filters a significant amount of malicious traffic, Cloudflare can't rely on computers alone to generate randomness. Computers follow logic, and the same input always produces the same output, making them predictable and less secure.

Lava lamps, however, are chaotic and never take the same shape twice. Cloudflare even encourages visitors to interact with the display, as external disturbances add more randomness. This unpredictability helps create stronger encryption keys and adds an extra layer of security.

"Wall of Entropy" located in Cloudflare's headquarters in San Francisco

SOLUTIONS³

637 Wyckoff Avenue
PMB 352
Wyckoff, NJ 07481

Phone: 201-891-0477
Fax: 201-891-5316
Email: info@solutions3llc.com

At Solutions³ LLC, we believe that empowering people is the key to sustainable success in cybersecurity, IT, and business service management as a whole. Our commitment to resource development is evident through mentorships, advanced training, and workforce development programs, including impactful internships and apprenticeships.

For more information on our internships, workforce development, or training, contact Mike Battistella at mike@solutions3llc.com or Shannon Conley at shannon.conley@solutions3llc.com.

Special Thanks to Our Sponsors

We are grateful for the generous support and partnership of the following organizations, whose contributions help make the Summer Cybersecurity Internship Program possible. Their support enables us to provide hands-on learning experiences, real-world simulations, and invaluable mentorship opportunities for our interns.

DVMS Institute

INFOSEC INSTITUTE

HACKTHEBOX

Follow us!

Website
www.solutions3llc.com

LinkedIn
www.linkedin.com/company/solutions3/

YouTube
www.youtube.com/@solutions3llc435

Editor's Corner

Thank you for reading Issue 4 of Solutions3's Cyberside Chats: Summer Edition.

This week, the interns at Solutions3 completed the final phase of the Cyber Essentials Pathway. Our deliverables included formulating a data classification policy and drafting a backup plan for our mock company, Falconi — building on the foundational work from the past two weeks.

Our team includes both undergraduate and graduate students from institutions such as the New Jersey Institute of Technology, Rutgers University, Fairleigh Dickinson University, Felician University, and Stevens Institute of Technology. With such a diverse group, we've benefited from a wide range of rich perspectives on every project and deliverable. I'd like to acknowledge my fellow interns — Amaan, Andre, Bryan, Dominick, Jaylen, Jesus, Johnathen, and Julia — for making this experience so collaborative and enjoyable. It's been an absolute pleasure working with them, and I continue to learn from them each day.

This week, we also had another valuable mentorship session with Floyd Haynes and Chandler Anderson from Hack The Box, where we are beginning to sharpen our technical cybersecurity skills through guided modules. I want to genuinely express my gratitude to the leadership team at Solutions3. The opportunity to learn from professionals in both technical and professional development areas has been incredibly enlightening. I hope our contributions reflect even a fraction of the knowledge and mentorship they've generously shared with us.

-Aaron Bissoondial

M.S. Computer Science

Stevens Institute of Technology