Threat Image

As September dawns, it is time we delve into the realm of smart cities, where technological innovation and data-driven decision-making are reshaping urban landscapes. These innovations hold the potential to create safer, more efficient, and more resilient communities. However, it is important to acknowledge that no technology solution is completely secure.

Smart cities also introduce potential vulnerabilities that, if exploited, could impact national security, economic security, public health and safety, and critical infrastructure operations. So, the benefits must be balanced against the dangers of cyber risks. The U.K. National Cyber Security Centre (NCSC), the U.S. Federal Bureau of Investigation (FBI) and other international security agencies have published a Cybersecurity Best Practices for Smart Cities guide. Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizens' private data, and security of sensitive government and business data. (1)

AI technology is evolving rapidly within the cybercrime underworld, with recent developments raising significant concerns. Just a few weeks ago, "New ChatGPT-Like Tool for Cybercriminals Is Trained on Entire Dark Web," made headlines, introducing WormGPT as a black-hat AI tool similar to ChatGPT. Moreover, the threat landscape has expanded with the emergence of another formidable tool called DarkBART, which closely mirrors Google BART and is based on a South Korean large language model (LLM). The situation becomes even more disconcerting with the impending arrival of DarkBERT, an AI tool that leverages the entire dark web as its source of training. This means that cybercriminals will have access to a collective hive mind of malicious knowledge. Notably, all of these tools are equipped with Google Lens integration and originate from the threat actor known as CanadianKingpin12. (2,3)

An international cybercrime operation across over two dozen African countries has led to 14 arrests and the takedown of numerous malicious IP addresses and malware hosts. The operation, known as Africa Cyber Surge II, aimed to combat cybercriminals and compromised infrastructure, with significant private sector support. The cybercrime activities, including fraudulent art sales, were associated with losses exceeding $40 million. This followed a previous operation, Africa Cyber Surge I, in 2022, resulting in 10 arrests and actions against malicious infrastructure across Africa. Authorities from 25 countries collaborated in this effort led by Interpol and Afripol. (4)

Latest Cyberthreats and Advisories (5)

- Microsoft Warns That Cyberattacks Impacting Sporting Events Are Likely to Increase
- The Sound of Computer Keystrokes Could Be Used to Steal Passwords
- For Android Users, N-Days Are Nearly as Dangerous as Zero-Days
- U.K. Electoral Commission Breach Exposes Data of Millions of British Voters
- Study Reveals That a Shocking 200 Million U.K. Targets Have Had Their Data Compromised

(1) https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf
(2) https://blog.isc2.org/isc2_blog/2023/08/latest-cyberthreats-and-advisories-august-11-2023.html
(3) https://www.darkreading.com/application-security/gpt-based-malware-trains-dark-web
(4) https://cyberscoop.com/africa-cybercrime-operation-interpol/?utm_source=dlvr.it&utm_medium=linkedin
(5) https://blog.isc2.org/