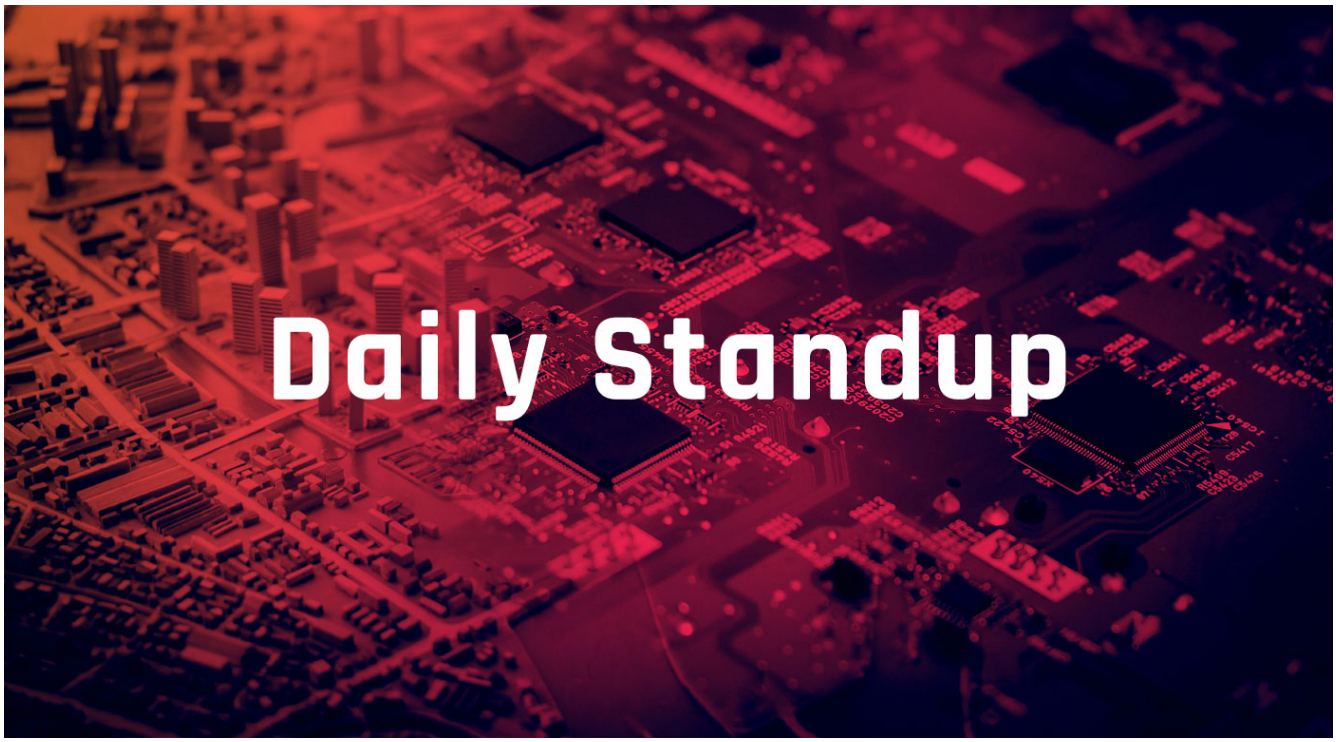
FLASHPOINT

Intelligence Report

Daily Standup

September 25, 2023



India's Biggest Tech Centers Named as Cyber Crime Hotspots (Register)

Target audience: Fraud Teams, Security Ops, Threat Intel/CTI

Summary: *India is grappling with a three-and-a-half year surge in cyber crime, with analysis suggesting cities like Bengaluru and Gurugram – centers of India's tech development – are hubs of this activity. The report – A Deep Dive into Cybercrime Trends Impacting India from the non-profit Future Crime Research Foundation (FCRF) – identified cyber crime hot spots from January 2020 until June 2023. "The analysis of the top 10 cyber crime-prone districts in India reveals several common factors contributing to their vulnerability. These include geographical proximity to major urban centers, limited cyber security infrastructure, socioeconomic challenges, and low digital literacy," states the report. Several of the most cyber crime-prone top geographies house tech hubs. Gurugram and Bangalore – both considered among the top five most attractive cities for the IT industry in Asia – featured for the wrong reasons. Another finding in the report was that of all reported cyber crimes in India, almost half (47.25 percent) involved Unified Payments Interface (UPI) fraud. Debit, credit card and sim swap fraud came in a distant second place with 11.27 percent. Overall, financially motivated crime accounted for 77.41 percent of incidents.*

Analyst comment: The surge in cybercrime in tech hubs such as Bengaluru and Gurugram is attributed to their status as major corporate and IT hubs, geographical proximity to major urban centers, limited cybersecurity infrastructure, and disparities in their populations' digital literacy and cybersecurity awareness. It is crucial for these regions to bolster their cybersecurity infrastructure and initiatives, enhance digital literacy and awareness among their populations, and foster a culture of cyber resilience to mitigate the impact of cybercrime and safeguard against future threats.

See also:

"Programming Asia Pacific Tech Cities as Global Tech Hubs" (CBRE)

"India's New Data Protection Bill May Complicate Companies' Operations" (Flashpoint)

Critical Infrastructure Organizations Warned of Snatch Ransomware Attacks (SecurityWeek)

Target audience: CISO, CIO, Security Engineers, Security Ops, Threat Intel/CTI

Summary: *The FBI and the cybersecurity agency CISA on Wednesday published an advisory warning critical infrastructure organizations of ongoing Snatch ransomware attacks. Active since 2018, Snatch is offered under the ransomware-as-a-service (RaaS) model, and has been targeting organizations in the United States since 2019. Since November 2021, the group has been operating a leaks site, where it threatens to publish stolen data unless a ransom is paid. The Snatch group, the FBI and CISA's advisory explains, typically exploits remote desktop protocol (RDP) vulnerabilities for initial access, but was also seen acquiring compromised credentials from cybercrime forums. The two agencies also note that, in some cases, although a different ransomware family was deployed, the victims were extorted by the Snatch group, which led to the stolen data being posted on two ransomware leaks sites. The FBI and CISA have published indicators of compromise (IoCs) and MITRE ATT&CK tactics and techniques associated with Snatch, as well as a series of recommended mitigations that organizations can implement to improve their cybersecurity posture.*

Analyst comment: These ongoing ransomware attacks by the "Snatch" ransomware group underscore the sophisticated and persistent nature of cybercriminal groups and their multifaceted approaches, including data exfiltration and threats to publish stolen data, to ensure their attacks are successful. To counteract these threats, analysts urge organizations to rigorously enhance their cybersecurity measures, continuously monitor network activities, and educate employees about potential risks and the importance of following security best practices to help prevent such cyberattacks.

See also:

"#StopRansomware: Snatch Ransomware" (CISA)

Snatch Ransomware Blog (Flashpoint Collections)

Associated Press: MGM Resorts Computers Back up after 10 Days Following Crippling Cyberattack (MarketWatch)

Target audience: CISO, CIO, Incident Response, Security Engineers, Security Ops, Threat Intel/CTI

Summary: *MGM Resorts (MGM, -1.32%) brought to an end a 10-day computer shutdown prompted by efforts to shield from a cyberattack data including hotel reservations and credit card processing, the casino giant said Wednesday, as analysts and academics measured the effects of the event. Rival casino owner Caesars Entertainment (CZR, -3.18%) also disclosed last week to federal regulators that it was hit by a cyberattack Sept. 7. It said that its casino and online operations were not disrupted but it could not guarantee that personal information about tens of millions of customers, including driver's licenses and Social Security numbers of loyalty rewards members, had not been compromised. Details about the extent of the MGM breach were not immediately disclosed, including the kind of information that may have been compromised and how much it cost the company. The attack on MGM also has been attributed to Scattered Spider, a group of English-speakers also sometimes known as Øktapus operating under a Russia-based operation called ALPHV or BlackCat.* [Parentheses added]

Analyst comment: These recent cyberattacks are attributed to the threat actor group "Oktapus," which may be related to the group "ALPHV," also known as "BlackCat." The incident cost MGM Resorts up to US$8 million per day, highlighting the vulnerability of even large, technically advanced companies and the significant impact such attacks can have on operations and revenue. Companies should invest in robust cybersecurity infrastructure, regular employee training, and comprehensive incident response plans to enhance their resilience against cyber threats and minimize the incident response costs in the event of a breach.

See also:

"Unknown Amount and Type of Data Encrypted and Held for Ransom with Systems Severely Disrupted by Hackers Employing Blackcat Ransomware" (Cyber Risk Analytics)

"MGM Experiences Widespread Outages; ALPHV Claims Attack" (Flashpoint)

Additional stories are included below, as they are of interest to threat intelligence teams:

"Data Breach Reveals Distressing Info: People Who Order Pineapple on Pizza" (Register)

"Omron Patches PLC, Engineering Software Flaws Discovered During ICS Malware Analysis" (SecurityWeek)

"Car Cybersecurity Study Shows Drop in Critical Vulnerabilities over Past Decade" (SecurityWeek)

"New Stealthy and Modular Deadglyph Malware Used in Govt Attacks" (BleepingComputer)

"China's Offensive Cyber Operations in Africa Support Soft Power Efforts" (SecurityWeek)

"Researchers Discover Attempt to Infect Leading Egyptian Opposition Politician with Predator Spyware" (SecurityWeek)

"Hotel Hackers Redirect Guests to Fake Booking.Com to Steal Cards" (BleepingComputer)

"Government of Bermuda Links Cyberattack to Russian Hackers" (BleepingComputer)

"Air Canada Says Employee Information Accessed in Cyberattack" (SecurityWeek)

"Evasive Gelsemium Hackers Spotted in Attack against Asian Govt" (BleepingComputer)

Please find past standups at https://fp.tools/home/intelligence/standup.