FBI: Ransomware Gangs Employing New Tactics

The FBI has issued a warning about ransomware gangs adopting new tactics, including employing multiple ransomware strains in a single attack, and using destructive tools beyond encryption or theft. These tactics involve custom data theft, wiper tools, and malware to pressure victims into negotiation. Additionally, the FBI has issued a warning regarding the emergence of dual ransomware attacks, where separate ransomware attacks are conducted within hours or days of each other against the same victim. These attacks typically occur within a 10-day timeframe, with the majority happening within 48 hours of each other.

Some ransomware groups are combining two ransomware strains during these attacks, such as AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal variants, making it challenging for defenders to prepare adequately. The use of dual ransomware variants results in data encryption, exfiltration, financial losses, and increased harm to victim entities. This trend has been tracked since early 2021, and it complicates recovery efforts and increases ransom payout potential.

The focus on data destruction is a notable aspect of this advisory, as it underscores the importance of removing all tools/accounts left behind by ransomware actors to prevent the activation of destructive tools. Destructive wipers have been observed in ransomware attacks deployed in the context of war or geopolitical conflict, extending their reach beyond Ukraine to 24 countries in the first half of 2022. The FBI recommends measures such as maintaining offline backups and establishing relationships with local FBI offices to counter these evolving ransomware tactics.

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://therecord.media/ransomware-using-multiple-strains-fbi
2. https://www.darkreading.com/threat-intelligence/fbi-highlights-dual-ransomware-attack-in-rising-cybertrends
3. https://www.ic3.gov/Media/News/2023/230928.pdf