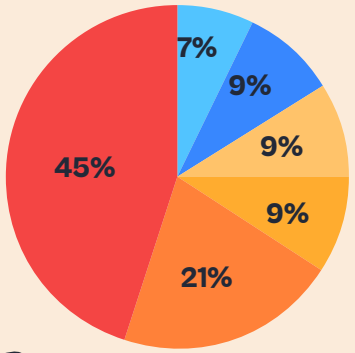
ATTACKING THE HOMELAND:

halcyon

INFOGRAPHIC

How Criminal Ransomware Groups Target State, Local, and Federal Governments

Criminal ransomware groups have expanded their cyber attack operations to a target state and local government entities along with federal ones. With a low cost of entry and a high success rate, these attacks have caused over $70B in damage between 2018 and 2022. With attacks growing at an exponential rate each year, and the real-world consequences of denying access to systems, ransomware has been upgraded to a national security threat by the Biden administration in early 2023.



Sources Leading to Ransomware Attacks

- Email Phishing
- Remote Attack on Server
- Third Party Contractor
- Cloud Misconfiguration
- Remote Desktop Protocol
- USB Drive aka Candy Drop

The amount **58%** of government orgs hit by ransomware in 2022

$70.4 BILLION cost to US government entities in 2018-2022

$ 70,400,000,000

72% OF ATTACKS were successful in **encrypting data**

Average Downtime

17 Days

Sorry We're CLOSED

№1 Cyber Threat

Classified a national security threat in 2023

MORE THAN 230M

US citizens impacted by these incidents

7pm - 7am

76% of attacks happen outside 'working hours.'

Ransomware can make the smallest compromise into a disastrous and costly breach. **Halcyon is built to ensure your organization is resilient against ransomware and advanced attacks.**

Only **58%** of data was actually recovered after the incident

···LOADING···

 Sources: https://www.comparitech.com/blog/information-security/government-ransomware-attacks
https://news.sophos.com/en-us/2022/09/28/the-state-of-ransomware-in-state-and-local-government-2022/
https://www.forbes.com/sites/siladityaray/2023/03/02/ransomware-attacks-upgraded-to-national-security-threat-in-new-white-house-cybersecurity-strategy/?sh=13cedb234996