

Ransomware by Cobalt Group

The Cobalt Group is a financially motivated cybercriminal organization notorious for orchestrating sophisticated cyberattacks employing advanced tactics to infiltrate systems and exfiltrate funds.



Signature behaviors

Custom malware development

Cobalt Group showed that cybercriminals don't need state sponsorship to pull off sophisticated attacks.

Long-term persistence

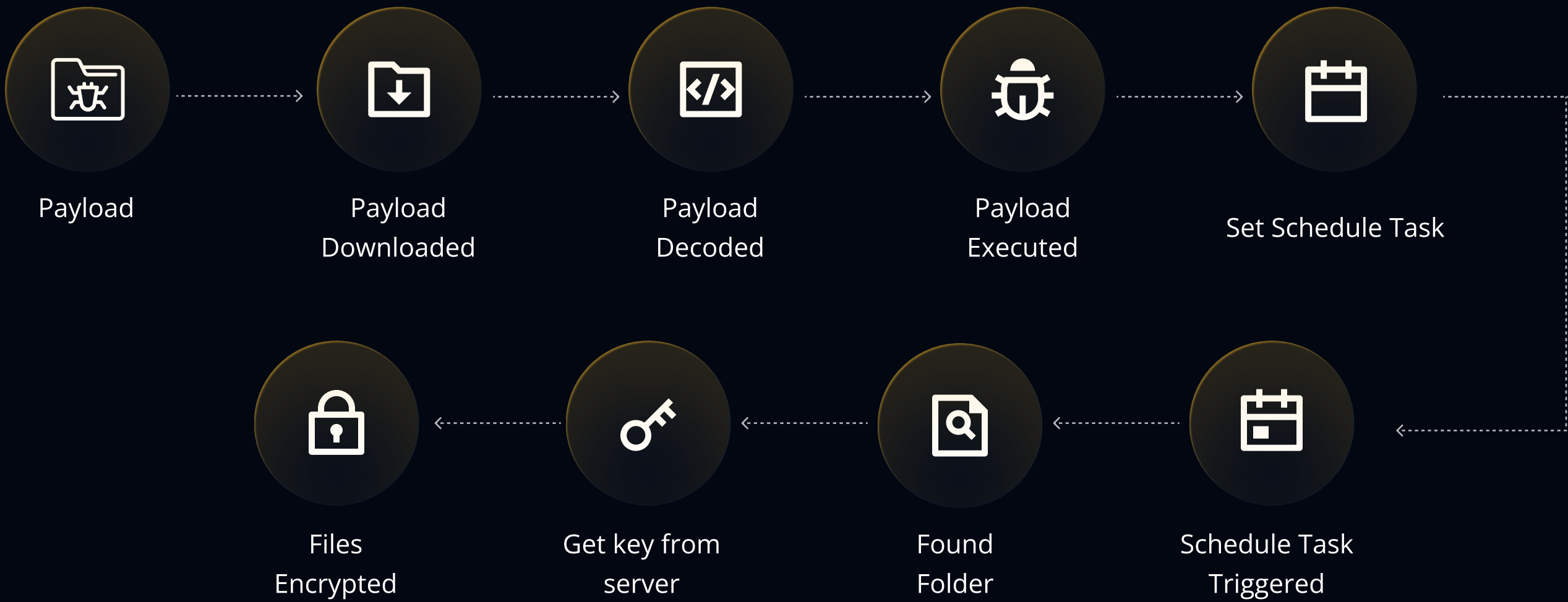
They weaponized legitimate tools (like Cobalt Strike, Mimikatz, CobInt, ATMSpitter, ATMRipper) in innovative ways.

Wide range of malicious activities

Demonstrated the real-world impact of cybercrime on physical assets (e.g., cash machines).

Simulated MITRE Tactics and Techniques

Resource Development (Malware), Initial Access (Drive-by Compromise), Defense Evasion (Exploitation for Defense Evasion), Execution (Malicious File), Execution - Persistence - Privilege Escalation (Scheduled Task/Job), Discovery (File and Directory Discovery), Collection (Data from Local System), Impact (Data Encrypted for Impact).



Book a demo