THREAT BRIEF

February 4, 2025

Critical Infrastructure Sectors

- 16 officially recognized sectors
- Vital physical, cyber systems, and networks
- Sectors are interconnected and interdependent

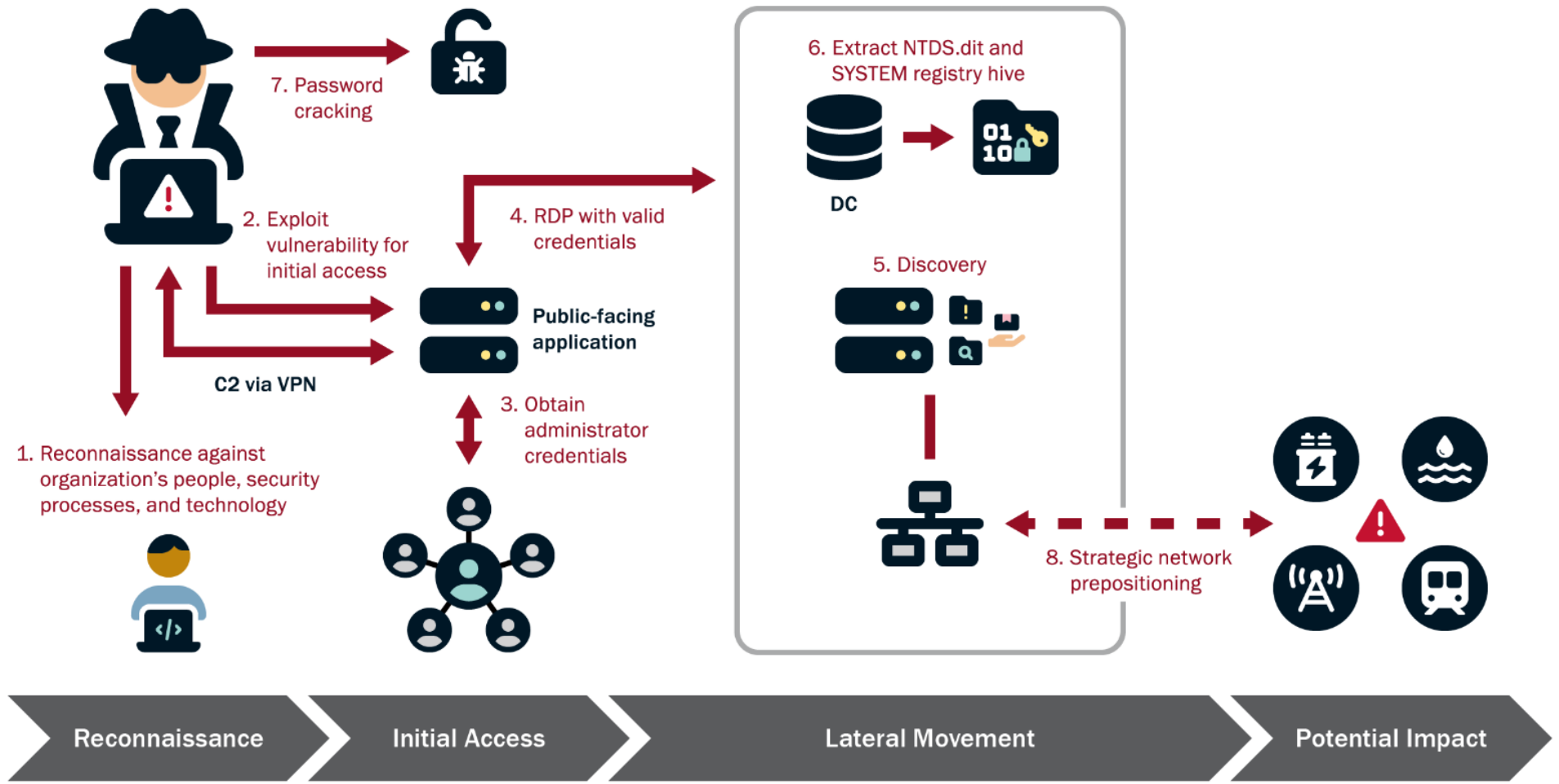
China Roadmap

1. Information technology
2. Computer numerical control machine tools and robotics
3. Aerospace equipment
4. Marine engineering equipment and high-tech ships
5. Advanced rail transportation equipment
6. Energy-efficient and new-energy automobiles
7. Electric power equipment
8. Agricultural equipment
9. New materials
10. Biomedicine and high-performance medical instruments

Volt Typhoon

- Also known as: Vanguard Panda, Bronze Silhouette, Dev-0391, UNC3236, Voltzite, and Insidious Taurus
- Main targets are U.S. critical infrastructure water, communications, transportation
- Threat actors heavily use the Living off The Land (LOTL) techniques
  - Conceal malicious activity with typical behavior
- Behavior is not typical consistent with traditional cyber espionage or intelligence gathering techniques
  - Pre-positioning for disruptive or destructive cyberattacks
  - Response to major crisis or conflicts with the United States

Volt Typhoon's Pattern of Behavior



Volt Typhoon Key Takeaways

- Volt Typhoon activity in multiple critical infrastructure organizations
  - Primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors
- Volt Typhoon threat actors utilize unconventional techniques making activity difficult to detect
- Threat actors are pre-positioning themselves to disrupt functions by moving laterally through multiple networks
- CISA urges critical infrastructure organizations to apply mitigations and hunt for similar malicious activity

- PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)
- Identifying and Mitigating Living Off the Land Techniques | CISA (https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques)

CISA Assessment and Services

Steps to enhance your cybersecurity

1. Vulnerability Scanning (Cyber Hygiene)
   - Web Application Scanning (WAS)

2. Assessments (open enrollment / self service)
   - Cyber Resilience Review (CRR)
   - Cyber Resiliency Essential (CRE)
   - Cyber Infrastructure Survey (CIS)
   - External Dependencies Management (EDM)
   - Ransomware Readiness Assessment (RRA)
   - Incident Management Review (IMR)

3. Technical Services (Invitation only)
   - Remote Penetration Test (RPT)
   - Risk and Vulnerability Assessment (RVA)
   - Validated Architecture Design Review (VADR)

4. Exercises

Cybersecurity Evaluations Tool (CSET)