Lazarus Group Financial Sector Campaign

CYBER THREAT REPORT
Lazarus Group - Financial Sector Targeting

Overview:
Lazarus Group continues targeting financial institutions worldwide.
This report covers recent activity observed in Q4 2024.

Attack Chain:

1. Initial Compromise:
   T1566.002: Spearphishing Link
   Employees received LinkedIn messages with malicious links

2. Execution:
   T1204.002: User Execution (Malicious File)
   T1106: Native API
   Direct system calls to avoid detection

3. Credential Access:
   T1003.001: LSASS Memory
   Mimikatz-like credential dumping
   T1555: Credentials from Password Stores

4. Lateral Movement:
   T1021.001: Remote Desktop Protocol
   T1021.002: SMB/Windows Admin Shares

5. Command and Control:
   T1071.001: Web Protocols
   HTTPS C2 communication
   T1573.002: Asymmetric Cryptography

Technical Indicators:
Malware Hashes:
  MD5: f1e2d3c4b5a6978012345678901234cd
  SHA1: abc123def4567890123456789012345678 90abcd

Infrastructure:
  C2 IP: 198.51.100.23
  Staging: download.legitimate-cdn.example
  Exfil: storage.cloud-backup.example

Registry Keys:
  HKLM Software Microsoft Windows CurrentVersion Run SystemUpdate

Mitigation:
- Network segmentation
- MFA for all accounts
- EDR deployment