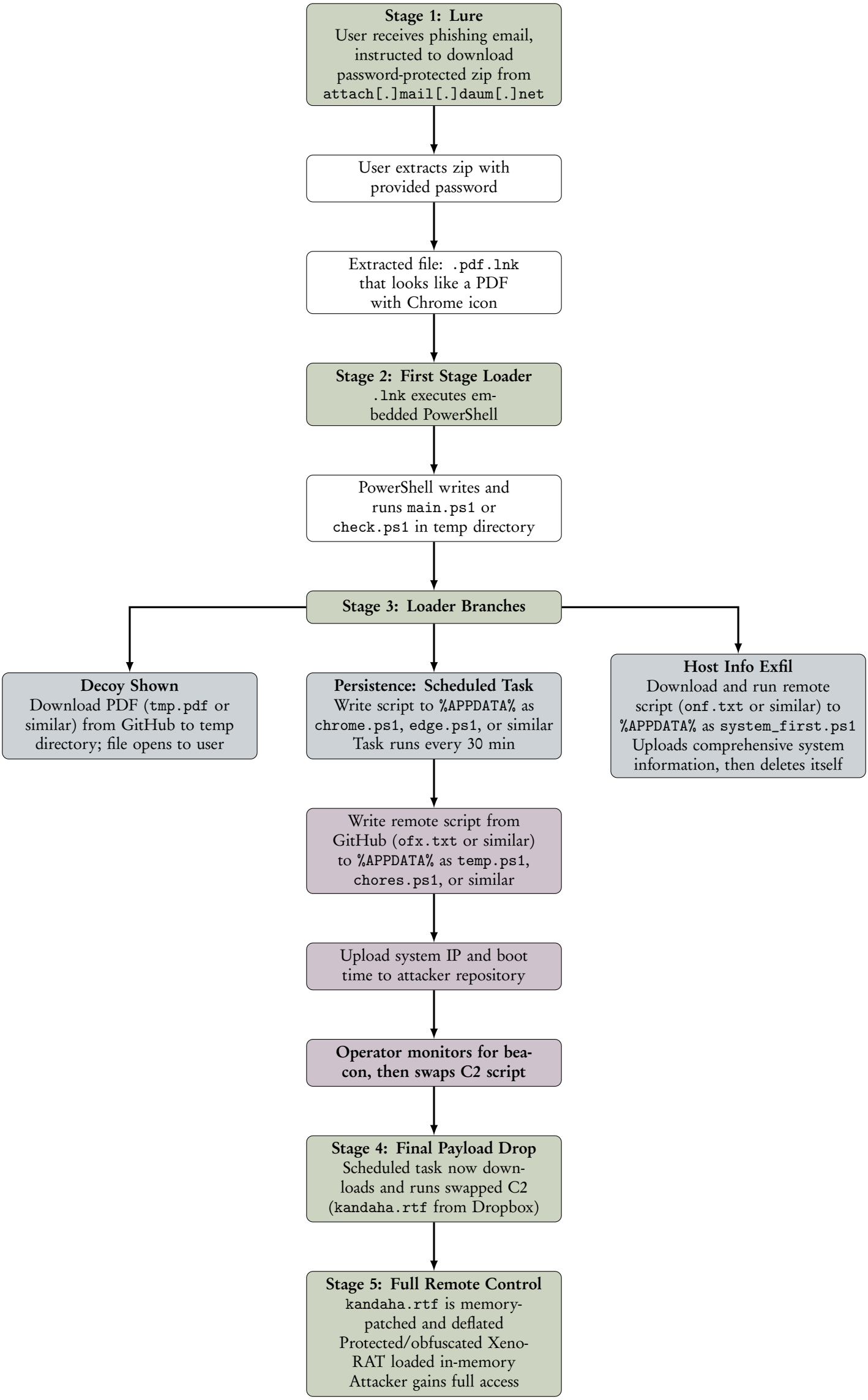
Stage 1: Lure
User receives phishing email, instructed to download password-protected zip from attach[.]mail[.]daum[.]net
User extracts zip with provided password
Extracted file: .pdf.lnk that looks like a PDF with Chrome icon
Stage 2: First Stage Loader
.lnk executes embedded PowerShell
PowerShell writes and runs main.ps1 or check.ps1 in temp directory
Stage 3: Loader Branches
Decoy Shown
Download PDF (tmp.pdf or similar) from GitHub to temp directory; file opens to user
Persistence: Scheduled Task
Write script to %APPDATA% as chrome.ps1, edge.ps1, or similar
Task runs every 30 min
Host Info Exfil
Download and run remote script (onf.txt or similar) to %APPDATA% as system_first.ps1
Uploads comprehensive system information, then deletes itself
Write remote script from GitHub (ofx.txt or similar) to %APPDATA% as temp.ps1, chores.ps1, or similar
Upload system IP and boot time to attacker repository
Operator monitors for beacon, then swaps C2 script
Stage 4: Final Payload Drop
Scheduled task now downloads and runs swapped C2 (kandaha.rtf from Dropbox)
Stage 5: Full Remote Control
kandaha.rtf is memory-patched and deflated
Protected/obfuscated Xeno-RAT loaded in-memory
Attacker gains full access