BLACK BASTA ATTACK TIMELINE

Tuesday, September 20 — DAY 1

- **Phishing Emails Delivered** — NOON EST
- First Attempt to Contact C2 — 12:02 EST
- AMP Alert Triggered — 12:05 EST
- Contact Established with C2 Domain — 12:38 EST
- Kerberoasting Begins — 13:45 EST

Wednesday, September 21 — DAY 2

- Download of RClone to Facilitate Data Exfiltration — 18:26 EST
- Outbound Connection to FTP Server — 18:26 EST
- **Quadrant Alerts Client**

Thursday, September 22 — DAY 3

- New Account "Adimius" Created via Compromised Account — 13:30 EST
- "Adimius" Account Added to Domain Admins — 13:31 EST
- Using RDP, Cobalt Strike beacons Copy/Pasted onto New Hosts — 18:34 EST
- "tox5.exe" Downloaded — 18:53 EST
- Black Basta Ransomware Detonated via RDP — 19:59 EST
- Client Team attempts to Lockout Threat Actor — 20:00 EST
- Threat Actor retaliates, resetting 31 passwords, including Admins — 20:02 EST
- Cables physically removed, severing connections — 20:45 EST
- **THREAT MITIGATED**

QUADRANT INFORMATION SECURITY