Marilyn Bergin | Ramsey, NJ | mbergin305@gmail.com | 201-686-0143 | GitHub: github.com/mbergin123

RDP C2 Simulation – Adversary Emulation & IOC Package

Analyst: Marilyn Bergin
Date: November 2, 2025
Classification: Internal Use – Training/Research

Executive Summary

During a controlled red-team exercise, a simulated RDP Command & Control (C2) channel was established using the Mythic C2 framework to emulate real-world lateral movement and credential brute-force behavior. The activity was conducted to test detection coverage, enrich IOC repositories, and validate alerting in ELK SIEM and LimaCharlie EDR.

Objective

- Evaluate detection capability for unauthorized RDP access and post-exploitation persistence.
- Generate and document Indicators of Compromise (IOCs) for CTI enrichment and detection engineering.
- Map observed behaviors to MITRE ATT&CK TTPs.

Key Findings

- Successful simulation of RDP-based brute-force (T1110) and C2 communications via custom payload (T1071).
- ELK dashboards detected abnormal authentication spikes and network anomalies.
- LimaCharlie EDR isolated the compromised host, confirming response automation integrity.
- Artifacts extracted: malicious scripts, encoded PowerShell payloads, persistence registry keys.

Indicators of Compromise (IOCs)

Type	Indicator	Context / Description
MD5 Hash	`f3a1c7b8d9e23ad7e2d4b4a1b6b0c1df`	Payload used to establish C2 communication (Mythic agent).
IP Address	`192.168.1.105`	Internal testing host acting as C2 server.
Domain	`rdp-control.example.local`	C2 callback domain used

		in simulation.
Registry Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Run\svc_updater`	Persistence mechanism for agent startup.

MITRE ATT&CK Mapping

- T1110 – Brute Force
- T1071 – Application Layer Protocol (C2)
- T1053 – Scheduled Task / Job
- T1547 – Boot or Logon Autostart Execution

Recommendations

- Implement enhanced SIEM detection rules for RDP brute-force threshold alerts.
- Periodically validate SOAR response playbooks for host isolation workflow.
- Update IOC feeds in threat intelligence platforms with identified artifacts.