



Threat Bulletin: Operation SparkRainstorm (Fictional)

Classification: TLP:CLEAR

Date: April 2025

Prepared by: Cyber Threat Intelligence Division

Overview

Operation SparkRainstorm is a fictional cyber threat campaign developed for demonstration and training purposes. It simulates the tactics of a fabricated threat group, APT-C29 “RainDrift”, modeled on the behaviors of advanced adversaries. The operation highlights malware staging, privilege escalation, internal reconnaissance, and credential theft using legitimate tools and behaviors.

⚠️ DISCLAIMER: All indicators, threat actor details, and artifacts in this bulletin are fictional and intended solely for use in controlled educational environments. They are not associated with any real-world threat activity.

Threat Actor Profile

Name: APT-C29 “RainDrift”

Type: Fictional Nation-State Threat Group

Motivation: Intelligence Collection

Targeting Profile: Government, Healthcare, Academic Research

Key Behaviors:

- Uses offensive PowerShell tools (e.g., PowerSploit)
- Avoids compiled malware when possible
- Leverages cloud and decentralized storage for payload hosting

Threat Timeline (Simulated)

Date/Time	Event
2022-03-31 08:32	Initial access via download and execution of svhost32.exe
2022-03-31 08:45	Persistence established using scheduled task WinUpdateService
2022-03-31 09:35	C2 channel opened to 198.51.100.77 using HTTPS
2022-03-31 10:15	Domain enumeration initiated via

FICTIONAL REPORT – FOR TRAINING PURPOSES ONLY
TLP CLEAR

	PowerView commands
2022-03-31 11:10	Lateral movement activity via SMB connections observed
2022-03-31 11:40	NTDS.dit file copied from Domain Controller

Kill Chain and Techniques

Phase	Technique (ID)	Description
Resource Development	T1608.001 – Upload Malware	Payload staged externally for download
Execution	T1059.001 – PowerShell	PowerSploit used for discovery and network enumeration
Credential Access	T1555 – Credentials from Password Stores	NTDS.dit extracted for credential harvesting


SOC Analyst Checklist

- Investigate abnormal PowerShell usage
- Review Sysmon logs for abnormal process execution
- Inspect Active Directory logs
- Monitor DNS and proxy logs for fake domains used in payload delivery
- Check for scheduled task creation: WinUpdateService
- Search for any known fake hashes in file inventory
- Trace outbound connections to known fake IP addresses
- Correlate SMB traffic logs for lateral movement timing
- Use ATT&CK Navigator to visualize attack surface coverage

MITRE ATT&CK Navigator Layer (Summary View)

Tactic	Technique ID	Technique Name
Resource Development	T1608.001	Upload Malware
Execution	T1059.001	PowerShell
Credential Access	T1555	Credentials from Password Stores

Indicators of Compromise (IOCs)

 **All IOCs below are fictional and for training purposes only. Do not use them for real-world alerting or blocking.**

- IP Addresses:
 - 45.67.89.123 – Staging server (FAKE)
 - 198.51.100.77 – C2 endpoint (FAKE)
 - 203.0.113.44 – Exfiltration server (FAKE)
- Domains:

FICTIONAL REPORT – FOR TRAINING PURPOSES ONLY
TLP CLEAR

- stage.sparkrainstorm-demo.net
- updates.win-patchsafe.org
- login.corp-portal.spoofed.co
- Hashes (SHA256):
 - a8b3f6c7e2f9d4c8a9e3a6218cd230e5e9bcabf4e3ab96c1ad5fd9aef9c4c1e0 – svhost32.exe
 - dd1f2a3e857d405d8d85b97b69e94656d8d7e827183b9e91850fdb0e5d7f3f3 – update.dll
 - 8fa9c72b2c8e46a8c0b4d3cba73fc3df163928de2279d3c6d5e28c2b1b4e8e1d – PowerView script
- Scheduled Task:
 - Name: WinUpdateService
 - Path: C:\ProgramData\WinUpdates\update.dll