Incident Response Playbook: Command-and-Control (C2) & External Communication

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction **3**
1.1 Purpose . . . 3
1.2 Scope . . . 3

2 Overview of the Category **3**
2.1 Definition . . . 3
2.2 Common Attack Chain . . . 3
2.3 Primary Risks & Business Impact . . . 3

3 Severity Level Assessment & MTTD / MTTR **4**

4 Tools & Preparation (Recommended) **4**

5 Incident Response Phases **4**
5.1 Identification & Triage . . . 4
5.2 Containment (Immediate / Short-term) . . . 5
5.3 Investigation & Forensic Triage . . . 5
5.4 Eradication . . . 5
5.5 Recovery . . . 6
5.6 Post-Incident Activities . . . 6

6 MITRE ATT&CK Framework Mapping **6**

7 Key Telemetry & Logs to Collect **6**

8 Subcategory Scenarios (Realistic) **6**

9 Appendices **10**
9.1 Appendix A — Useful SIEM / Investigation Queries . . . 10
9.2 Appendix B — Forensic Artifact Locations . . . 10
9.3 Appendix C — Incident Report Template (Summary) . . . 11

1 Introduction

1.1 Purpose

This playbook provides operational guidance for detection, investigation, containment, eradication and recovery for incidents involving **Command-and-Control (C2)** and other suspicious external communications. It covers beaconing behavior, encrypted or covert C2 channels, DGA-generated domains, domain fluxing, and unusual outbound patterns used for data staging or remote control. Audience: SOC analysts, threat hunters, incident responders, network ops, and cloud security teams.

1.2 Scope

Applies to endpoints, servers, network perimeter devices, DNS/DNS resolvers, proxy/HTTP logs, TLS inspection points, egress firewalls, cloud egress (S3, Azure Blob), and threat intel platforms. Includes both direct C2 (HTTP/S, DNS, TCP) and covert channels (DNS tunneling, steganographic payloads, domain fronting).

2 Overview of the Category

2.1 Definition

Command-and-Control (C2) refers to the external communication channels an adversary uses to control compromised hosts, issue commands, stage additional payloads, or exfiltrate data. This category also covers suspicious domain generation algorithm (DGA) activity where large numbers of algorithmically-generated domains are used for redundancy and resilience.

2.2 Common Attack Chain

1. **Initial access:** malware or compromised account establishes code capable of network communication.
2. **Beaconing / Registration:** compromised host initiates periodic callbacks to attacker-controlled infrastructure.
3. **C2 Negotiation:** handshake and possible encryption/authentication of channel; delivery of tasking or secondary payloads.
4. **Data staging / exfiltration:** compressed/encrypted data uploaded via HTTP, DNS or cloud APIs.
5. **Fallback / Resilience:** DGA, fast-flux DNS, or domain fronting to evade takedown.
6. **Impact:** sustained remote control, data theft, additional deployment (ransomware, lateral tooling).

2.3 Primary Risks & Business Impact

- Persistent remote access enabling long-term espionage or large-scale exfiltration.
- Use of C2 to deliver destructive payloads (ransomware, wipers).
- Difficulty in takedown due to DGA or multi-provider infrastructure.
- Reputational and regulatory exposure if data leaves the environment.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	Example	MTTD	MTTR
Critical	Confirmed, sustained C2 controlling multiple high-value hosts, active data exfiltration to external infra or staging in cloud, or DGA-based widespread campaigns.	Multiple file servers beaconing to DGA domains and data staged to attacker S3.	$\leq$ 15 min	Contain within 4 hrs; recovery 24–72 hrs.
High	One or more hosts with confirmed C2 sessions and evidence of lateral staging or secondary payload delivery.	Endpoint with reverse-shell C2 sessions and retrieval of additional payloads.	$\leq$ 1 hr	6–24 hrs.
Medium	Intermittent beaconing or suspicious DNS patterns (possible DGA) without confirmed commanding or exfiltration.	Host performing high-entropy DNS queries to many rare domains.	$\leq$ 2 hrs	12–48 hrs.
Low	Single suspicious outbound connection that appears benign or false positive (e.g., one-off to new SaaS domain).	One host contacting a rare domain once.	$\leq$ 4 hrs	Monitor / minor remediation within 24–72 hrs.

Table 1: Severity Matrix - Command-and-Control & External Communication

4 Tools & Preparation (Recommended)

- **Network Telemetry:** full DNS logs (query+response), proxy/HTTP logs, TLS SNI/JA3/JA3S fingerprints, NetFlow/IPFIX, egress firewall logs, and packet capture at egress chokepoints.
- **Endpoint Telemetry:** EDR with network connection metadata, process tree, memory dumps and socket ownership information.
- **DNS Defenses:** recursive resolver logging, DNS RPZ (response policy zone) for sinkholing, and DNS analytics (entropy, NXDOMAIN ratios).
- **Threat Intel / DGA Detection:** DGA detectors (machine-learning based), blocklists, passive DNS, and domain age/timing analysis.
- **Cloud Controls:** egress controls for cloud storage, CASB, and API gateway logging for uploads.
- **Playbook Resources:** domain takedown contacts, ISP/registrar abuse templates, and legal/forensics contacts for coordination.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- EDR: processes making unusual outbound connections (child processes of Office apps making HTTP requests, rundll32/regsvr32 invoking sockets).

- DNS: high NXDOMAIN rate, repeated queries for many algorithmically-generated domains, or high-entropy domain names.
- Network: small periodic beacons (regular intervals), large outbound uploads to unfamiliar cloud endpoints, or encrypted TLS sessions with uncommon JA3 fingerprints.
- Threat Intel: matching known C2 IPs/domains, passive DNS linking to malicious infrastructure.

Quick actions:

- Validate detection, determine hosts and timestamps, and classify severity with the matrix above.
- Initiate packet capture (PCAP) for the suspect timeframe and collect DNS logs (resolver + recursive).
- Snapshot process memory and network sockets on affected endpoints (preserve chain-of-custody).

5.2 Containment (Immediate / Short-term)

- Block suspicious domains and IPs at the proxy/firewall and sinkhole DGA domains via DNS RPZ where possible.
- Isolate affected hosts via EDR (network quarantine) to prevent further staging or C2 activity.
- Apply ACLs to cloud storage endpoints to prevent further uploads and revoke compromised service credentials.
- Implement increased logging/packet capture for the suspected egress points.

5.3 Investigation & Forensic Triage

- Parse PCAPs, extract HTTP/TLS sessions, and recover any staged files; compute hashes and upload to malware analysis/sandbox.
- Analyze DNS query patterns for DGA heuristics (entropy, length, character distribution, frequency).
- Correlate JA3/JA3S/TLS fingerprints with threat intel to identify tooling (e.g., Cobalt Strike beacon variants).
- Identify lateral staging (which hosts downloaded payloads) and map the timeline of communications.

5.4 Eradication

- Remove C2 stagers, malicious binaries, scheduled tasks and persistence mechanisms from infected hosts (after evidence collection).
- Rotate any keys/tokens or credentials used to stage data; revoke compromised cloud storage tokens and rotate API credentials.
- Update DNS RPZ and proxy rules to block newly identified malicious infrastructure.
- Work with registrars/ISPs to sinkhole or takedown attacker domains where possible.

5.5 Recovery

- Reimage hosts where integrity is uncertain and restore from known-good images.
- Validate that exfiltration channels are closed and review restored systems for persistence.
- Monitor for reappearance of the same C2 patterns for at least 60–90 days.

5.6 Post-Incident Activities

- Produce a full IOC list (domains, IPs, JA3 fingerprints, YARA rules) and publish to internal blocklists and threat-sharing communities.
- Tune DGA detection models and update SIEM correlation rules for beacon intervals and high-entropy domains.
- Conduct a lessons-learned review, tabletop exercises and update playbooks and defensive controls.

6 MITRE ATT&CK Framework Mapping

C2 & External Communication - ATT&CK Mapping

- **Command & Control:** T1071 (Application Layer Protocol), T1095 (Non-Application Layer Protocol), T1105 (Ingress Tool Transfer)
- **Exfiltration:** T1041 (Exfil over C2 Channel), T1567 (Exfil over Web Service)
- **Communications Evasion:** T1573 (Encrypted Channel), T1090 (Proxy)
- **Domain Generation / Fast-flux:** T1483 (Domain Fronting) / DGA techniques (behavioral detection)

7 Key Telemetry & Logs to Collect

- Full DNS logs (queries + responses) with timestamps and client IPs.
- Proxy/HTTP logs including URL, User-Agent, response size, and TLS SNI.
- EDR network metadata (process, destination IP/port, bytes in/out), PCAPs for suspect intervals.
- TLS fingerprints (JA3/JA3S), certificate details (issuer, validity), and passive DNS records.
- Cloud storage access logs and object metadata (user-agent, API key used, source IP).

8 Subcategory Scenarios (Realistic)

Note: Scenarios are operational SOC/IR narratives — detection, investigation steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Endpoint Beaconing (C2 Communication) — Periodic HTTP Beacon to Rare Domain

Summary: EDR flags a process on a marketing workstation creating periodic HTTPS connections every 300 seconds to a rare domain. The traffic is small (few bytes) and occurs at regular intervals — a classic beacon pattern.

Detection:

- EDR: repeated outbound HTTPS connections from `word.exe` child process at regular 5-minute intervals.
- Proxy logs: repeated POSTs to 'xn–random-dga[.]xyz' with small payloads and 200 responses.
- DNS: large number of NXDOMAIN responses for similar high-entropy domains in short windows.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to confirmed periodic beaconing and DGA-like domain pattern.
2. **Immediate containment:** Quarantine the affected host via EDR; block the observed domain and associated IPs at the proxy and DNS RPZ.
3. **Forensic collection:** Snapshot process memory, collect PCAP for beacon intervals, extract TLS certificates and JA3 fingerprint, and harvest any staged payloads.
4. **Hunt:** Search estate for hosts exhibiting the same JA3 fingerprint, DNS patterns, or contacting related NXDOMAIN clusters.

Containment & Eradication:

- Remove the beaconing binary and any persistence (scheduled tasks, registry autoruns). Reimage if root cause unknown.
- Update DGA heuristics and block additional domains observed in passive DNS.
- Deploy IDS/proxy signatures for the observed JA3/HTTP headers to catch variants.

Recovery:

- Restore host from known-good image or cleaned state and validate with endpoint scanning and sandboxing for residual components.
- Monitor for re-beaconing and related domain activity for 60–90 days.

Outcome & Lessons:

- Root cause: user opened a malicious document that deployed a small beaconing implant. Mitigations: strengthen mail/attachment detonation, block suspicious DNS patterns, and improve DGA detection.

Scenario B: Suspicious DGA Traffic — High NXDOMAIN Fast-Fallback

Summary: DNS analytics show a host querying hundreds of different domains per hour with high-entropy labels; many responses are NXDOMAIN but some resolve briefly to fast-flux IPs. Passive DNS links the resolved domains to a known botnet infrastructure.

Detection:

- DNS: spike in unique domain queries from a single host; high entropy and low domain age on resolved names.
- Passive DNS: resolved domains map to a rotating set of IPs across multiple ASNs (fast-flux).
- NetFlow: small outbound connections to many remote IPs following those DNS resolutions.

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* if mapping to known botnet C2 and multiple hosts involved.
2. **Immediate containment:** Apply DNS RPZ sinkhole for matching patterns, isolate infected hosts and block observed IP ranges at the edge.
3. **Forensic collection:** Collect DNS cache, resolver logs, EDR evidence on hosts, and PCAPs for attempted connections to resolved IPs.
4. **Hunt:** Expand search for other hosts with similar high-entropy queries and pivot on passive DNS to identify additional infrastructure.

Containment & Eradication:

- Remove botnet binaries, reimage infected systems, and update endpoint signatures for observed behavior.
- Collaborate with registrar/ISP to takedown malicious hosting and share IOC sets with threat intel partners.

Recovery:

- Validate cleaning via multiple scans and restore from trusted images. Monitor DNS activity for resurgence.

Outcome & Lessons:

- Enhanced DGA detection, improved DNS logging retention, and deployment of RPZ/blackhole policies at recursive resolvers.

Scenario C: C2 over DNS Tunneling — Data Exfil via TXT / DNS A records

Summary: Anomalous spikes in TXT record queries and unusually long subdomain lengths are observed. Analysis shows base64-encoded chunks in DNS requests and responses — used to stage small exfiltration.

Detection:

- DNS: high volume of TXT queries containing long encoded strings from a small set of hosts.
- Egress: repeated small UDP packets to external authoritative DNS servers at non-standard intervals.

- SIEM: correlation with rare external DNS servers flagged by threat intel.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* because DNS tunneling indicates covert channel with exfiltration potential.
2. **Immediate containment:** Block authoritative DNS servers at edge where possible; force endpoints to use corporate resolvers and sinkhole the suspected domains.
3. **Forensic collection:** Capture DNS traffic, extract encoded payloads for decoding and hash analysis, and collect endpoint process/activity linking to queries.
4. **Hunt:** Search for other hosts issuing similar encoded DNS queries and identify possible staging or aggregation nodes.

Containment & Eradication:

- Remove tunneling tool and related persistence; reimage if necessary.
- Implement DNS egress filtering, restrict DNS over HTTPS/TLS to corporate resolvers, and enforce strict DNS policies.

Recovery:

- Validate that data was not exfiltrated (or quantify exposure) and restore systems from trusted images if needed.
- Improve DLP and monitor for encoded data patterns in DNS going forward.

Outcome & Lessons:

- Tightened DNS egress, increased logging and retention, and deployed automated decoders to detect base64-like patterns in DNS queries.

Scenario D: C2 via Cloud Storage (Covert Exfil via S3 / Blob Uploads)

Summary: Detection rules flag atypical uploads to a new external cloud storage endpoint (public S3 bucket). The uploads use an API key that appears to have been exfiltrated from a development host.

Detection:

- Cloud logs: PUT/POSTs to external S3 endpoints from internal service account; object metadata shows unusual user-agent.
- DLP: alerts for document fingerprints present in uploads to unknown buckets.
- EDR: process on dev host launched ‘aws‘ CLI with long-lived API keys.

Investigation & Actions:

1. **Triage & classification:** Classified as *High/Critical* depending on sensitivity of uploaded objects.
2. **Immediate containment:** Revoke API keys, disable the implicated IAM user, and block the destination cloud storage endpoint through network controls if feasible.

3. **Forensic collection:** Snapshot cloud logs (access keys, request IDs), collect object metadata, and capture process/activity on the developer host.

4. **Hunt:** Search for other uses of the same keys and for other keys leaked in repositories or build pipelines.

Containment & Eradication:

- Rotate all affected keys, audit and restrict IAM permissions, and delete attacker-staged objects when legally appropriate.
- Harden CI/CD pipelines and enforce secrets management and scanning to prevent future leaks.

Recovery:

- Restore affected systems and verify backups; implement stricter monitoring of cloud object creation and egress.

Outcome & Lessons:

- Improved secrets hygiene, mandatory use of secrets managers, and automated monitoring/alerting on suspicious cloud uploads.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Splunk: detect high-entropy domains (example)

```
index=dns sourcetype=dns | eval entropy=sha1(host) | where match(host, "^[a-z0
    -9]{8,}\.")
| stats count by host | where count < 5
```

Kusto / Sentinel: periodic beacon detection (example)

```
NetworkConnectionLogs
| where TimeGenerated > ago(1d)
| summarize count() by bin(TimeGenerated, 5m), RemoteUrl, DeviceName
| where count() > 5
```

Bro/Zeek: extract long TXT DNS queries

```
@load policy/frameworks/intel/do_notice
event DNS::response
{
  if ( dns$rcode == "NOERROR" && dns$answers )
    {
      # parse TXT records...
    }
}
```

9.2 Appendix B — Forensic Artifact Locations

- DNS: recursive resolver query logs, stub resolver cache on endpoints, DNS cache on Windows (‘ipconfig /displaydns‘).
- Endpoint: EDR process network connections, memory dumps, and persisted scheduled tasks/services.

- Network: PCAPs at egress, NetFlow/IPFIX, proxy logs, TLS metadata (SNI, certs, JA3).
- Cloud: object metadata, access logs (S3/Azure Blob), API keys usages, and CloudTrail/Azure-Activity.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Severity / Playbook invoked.
- Affected hosts, domains, IPs, cloud objects, and scope of exfiltration (if any).
- Evidence preserved (PCAPs, DNS logs, EDR dumps) and IOCs (domains, JA3, certs, hashes).
- Actions taken with timestamps and owners (containment, eradication, recovery).
- Recommendations and long-term mitigations (DNS RPZ, DGA detection tuning, secrets management changes).