# Incident Report: Koi Stealer C2 Communication Detected

Date: 2024-09-04 (Based on event timestamps)
Classification: Confirmed Malware Infection / C2 Communication

---

## 1. Executive Summary

On 2024-09-04, an internal host, 172.17.0[.]99, was identified as compromised and actively communicating with a known Command and Control (C2) server. Network traffic analysis confirmed persistent HTTP beaconing to a suspicious external IP address, 79[.]124[.]78[.]197, utilizing the URI /foots.php. This activity was confirmed by threat intelligence sources and further file analysis. The beaconing behavior, combined with reconnaissance attempts against the domain controller, indicates a successful infection by a stealer malware family, likely Koi Stealer.

## 2. Victim Details

- **Hostname:** DESKTOP-RNVO9AT
- **IP Address:** 172.17.0[.]99

## 3. Incident Timeline

- **Initial Access:** The host likely gained initial access by visiting a malicious domain, as indicated by the user's template modandcrackedapk[.]com, which is a known source of cracked software and malware.
- **C2 Communication Initiation:** The host initiated direct IP-based communication with the C2 server at 79[.]124.78[.]197, bypassing DNS-level security controls.
- **Beaconing & Reconnaissance:** Repeated HTTP POST requests to the C2 server were observed, with the tshark stream export confirming this was a persistent "beacon" activity rather than a large data transfer.
- **Lateral Movement Attempts:** The compromised host attempted to conduct reconnaissance and potential privilege escalation activities within the internal network,

targeting the domain controller 172.17.0[.]17 via SMB and Kerberos.

## 4. Technical Analysis

The incident analysis revealed a multi-stage attack. Following an initial compromise, a malware implant established a persistent C2 channel. The lack of DNS traffic to the C2 IP is a strong indicator of a hardcoded IP in the malware's configuration.

The HTTP beaconing traffic, specifically the consistent request to /foots.php, is a signature of this type of malware. The extraction and analysis of the foots.php file itself yielded a 0-byte file with a known, benign hash. This is not a contradiction but a key finding: the file is not the malicious payload, but an artifact of the malware's communication protocol, confirming the host was checking in to the C2 server without transmitting a data payload in that specific stream.

Additionally, the presence of other extracted files (connecttest[.]txt and ProcessMAU[.]txt) further confirmed the attacker's post-exploitation activities. connecttest[.]txt suggests the malware was verifying internet connectivity, while ProcessMAU[.]txt is a strong indicator of reconnaissance, a crucial step before lateral movement or data exfiltration.

## 5. Indicators of Compromise (IOCs)

- **Malicious IP Addresses:**
  - 79[.]124[.]78[.]197 (C2 Server)
- **Malicious Domains:**
  - modandcrackedapk[.]com (Initial Access Vector)
- **Malicious URLs:**
  - hxxp://79[.]124[.]78[.]197/foots.php
- **File Hashes (SHA256):**
  - e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 (Artifact of empty C2 beaconing)
  - 69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820 (Potential reconnaissance file)
- **Suspicious User Agents:**
  - Mozilla/4[.]0 (compatible; MSIE 7[.]0; Windows NT 10[.]0; WOW64; ...) (Associated with C2 communication)

## 6. Recommendations

1. **Quarantine Host 172.17.0[.]99:** Immediately isolate the compromised host from the network to prevent further compromise or data exfiltration.
2. **Network Blocking:** Block all inbound and outbound connections to the malicious IP address 79[.]124[.]78[.]197 at the firewall.
3. **Threat Hunting:** Scan the network for other hosts communicating with 79[.]124[.]78[.]197 or hosts with a DNS query for modandcrackedapk[.]com.
4. **Forensic Investigation:** Conduct a full forensic analysis of 172.17.0[.]99 to determine the initial access vector, full extent of the compromise, and any exfiltrated data.
5. **User Education:** Educate users on the dangers of visiting suspicious websites and downloading pirated or cracked software.