Incident Report

Subject: Network Forensics Analysis of Malicious Traffic
Date: September 3, 2025
Source: 2024-11-26-traffic-analysis-exercise.pcap
Victim Host: 10.11.26.183

Executive Summary

A network traffic analysis was performed on the provided packet capture to investigate suspicious activity originating from the internal host 10.11.26.183. The investigation concluded that the host was compromised after making a DNS query for a known malicious domain, modandcrackedapk[.]com. This action resulted in the download of a NetSupport Manager implant, which established a persistent and encrypted Command and Control (C2) channel to 194[.]180[.]191[.]64. Data exfiltration was observed over this channel, confirming a successful breach. The incident began on November 26, 2024, at approximately 02:40:47 UTC.

Incident Timeline

- **02:40:47 UTC:** Victim host 10.11.26.183 initiates a DNS query for the domain modandcrackedapk[.]com.
- **02:40:47 UTC:** DNS server responds, resolving modandcrackedapk[.]com to 193[.]42[.]38[.]139.
- **02:40:48 UTC:** Victim host initiates a TLS (HTTPS) connection to 193[.]42[.]38[.]139, likely for the download of the malicious payload.
- **02:40:51 UTC:** A new and persistent TLS connection is established from the victim host 10.11.26.183 to the C2 server 194[.]180[.]191[.]64 on port 443.
- **02:41:00 UTC onwards:** The victim host begins to send large, encrypted data packets to the C2 server, indicating data exfiltration is in progress.

Technical Analysis

Initial Access

The attack began when the victim host's DNS activity revealed a query for the domain modandcrackedapk[.]com. This domain is flagged as malicious by multiple public threat intelligence sources. The DNS query was resolved to the IP address 193[.]42[.]38[.]139, to which the victim host then established an encrypted TLS connection. This traffic flow indicates that the host visited a web page or was redirected to a malicious domain, leading to the download of a file or a drive-by download event.

Execution & Persistence

While the PCAP does not contain direct evidence of a specific process being executed, the subsequent establishment of a persistent, encrypted C2 channel to 194[.]180[.]191[.]64 strongly implies that a malicious implant was successfully executed. The traffic's User-Agent string, NetSupport Manager/1.3, identified the specific malware as a legitimate remote administration tool that is frequently abused by threat actors to maintain persistence and control over a compromised system.

C2 Communication

The C2 channel was identified by its unique beaconing behavior to the IP address 194[.]180[.]191[.]64 over a TLS-encrypted connection on port 443. The communication stream was characterized by a distinct User-Agent string (NetSupport Manager/1.3) and consistently used the URI /fakeurl[.]htm for its communication. This encrypted channel prevented direct analysis of the commands sent from the attacker to the victim.

Data Exfiltration

Approximately 9 seconds after establishing the C2 channel, the victim host began uploading a significant volume of data to the C2 server. This activity, observed as multiple TCP segments with a TLS Application Data payload, is a clear indicator of data exfiltration. The exact nature of the data cannot be determined due to the TLS encryption.

Indicators of Compromise (IOCs)

Type	Indicator	Context
Malicious Domains	modandcrackedapk[.]com	Initial access domain.
Malicious IPs	193[.]42[.]38[.]139	Host of the malicious file/implant.
Malicious IPs	194[.]180[.]191[.]64	The C2 server IP address.
Suspicious User-Agent	NetSupport Manager/1.3	Identifies the NetSupport Manager implant.
C2 URI Path	/fakeurl[.]htm	Unique URI used in C2 communication.
File Hashes	N/A	No file hashes were recovered as the download was encrypted over TLS.

Recommendations

Based on the findings, the following actions are recommended:

- **Isolate the Host:** Immediately disconnect host 10.11.26.183 from the network to contain the compromise and prevent further data exfiltration or lateral movement.
- **Implement Firewall Rules:** Block all network traffic to and from the identified malicious IP addresses: 193[.]42[.]38[.]139 and 194[.]180[.]191[.]64.
- **Block at the DNS Level:** Update DNS filters or a host firewall to block all queries for the domain modandcrackedapk[.]com.
- **Conduct Endpoint Forensics:** Perform a full scan and forensic analysis of the compromised host to identify the malicious file, any persistence mechanisms, and determine the scope of data exfiltration.

- **User Awareness:** Educate the user on the risks of visiting untrusted websites and downloading files from unauthorized sources.