Network Traffic Analysis Incident Report --- 2025-06-25

Analyst Name : Nizar Aderbaz

1. Executive Summary :

On 26 November 2024, we noticed something unusual was going on with one of our internal machines, IP 10.11.26.183. When we analyzed the network traffic (PCAP), we noticed it was talking to some suspicious and potentially malicious websites and IP addresses. This is indicative of the machine being infected with a Remote Access Trojan (RAT). Below are some of the important findings :

- DNS resolution to a malicious domain : **modandcrackedapk.com**
- HTTPS connection (TLS) to the same domain
- HTTP and POST requests to a rogue IP : **194.180.191.64**
- Suspicious geolocation requests to **geo.netsupportsoftware.com**, typically used by threat actors to identify victim location
- IOC matches with threat signatures from public threat intelligence feeds (VirusTotal, AbuseIPdb)

---

1. Incident Timeline :

Time	Source IP	Destination IP / Domain	Description
2024-11-26 04:50:14	10.11.26.183	modandcrackedapk.com	DNS Query + TLS Session
2024-11-26 04:50:45	10.11.26.183	194.180.191.64	HTTP Request + POST request → Potential Exfiltration
2024-11-26 04:50:45	10.11.26.183	104.26.1.231	GeoLocation lookup ➔ Reconnaissance

---

2. Victim System Information :

- **Hostname** : DESKTOP-B8TQK49
- **Internal IP** : 10.11.26.183

- **MAC Address** : 00:17:e0:b8:29:5e
- **Windows User** : Olivier Q. Boomwald (oboomwald)

---

3. Indicators of Compromise (IOCs) :

4.1 Domains :

- **modandcrackedapk.com** **(VT:10/94)**
- **geo.netsupportsoftware.com** **(8/94)**
- **confirmsubscription.com** **(VT:1/94)**

4.2 IP Addresses :

- **193.42.38.139** (related to modandcrackedapk.com)
- **194.180.191.64** (malicious, VT: 5/94)
- **104.26.1.231** (suspicious, used by geo.netsupportsoftware.com)
- **52.8.34.0, 13.56.30.297** (related to confirmsubscription.com)

4.3 URLs :

- **hxxp[://]194[.]180[.]191[.]64/fakeurl[.]htm**
- **hxxp[://]104[.]26[.]1[.]231/location/loca[.]asp**

4.4 Hashes :

- None found in this analysis

---

4. Conclusion :

Based on the behavior observed, it is **highly likely** that the victim system was infected with a Remote Access Trojan (RAT), possibly from **ETPRO Trojan** family

according to SIEM alert. The attacker likely used it to gain control over the system and exfiltrate sensitive data.

---

5. Recommendations :

- **Isolate the affected system**
- **Document the incident fully and prepare IOC sharing for threat intelligence feeds**
- **Update firewall and IDS/IPS rules to block identified IOCs**
- **Verify if lateral movement occurred within the internal network**
- **Check for persistence mechanisms (registry, scheduled tasks, services)**
- **Correlate PCAP data with endpoint telemetry (Sysmon, EDR logs,…)**
- **Perform YARA scan against memory and disk for known RAT signatures**
- **Audit user accounts and reset credentials**