**INCIDENT REPORT: 18508**

**Date: 02/09/24**

**Executive summary: Jack has brought in a laptop that is an expensive brick right now. We’ve managed to pull some logs from the hard drive. Analyze these logs and write a report on what you found. There are three different Mal-wares affecting this laptop. They are all well know and popular Malware.**

**Victim details: Jack**

* **IP address: 10.2.8.101**
* **MAC address: 00:12:79:41:c2:aa**
* **Host name: HewlettPacka\_41**
* **User account name:**

**Indicators of compromise (IOCs):**

**SHA256 hash:** 94e60r577c84625da69f785ffe7e24c889bfa6923dc76017c21e8a313e4e8e1

**Malicious HTTP traffic:**

**IP Addresses:**

* 8.208.10.147
* 45.124.85.55
* 198.211.10.238:8080

**Suspicious domains using HTTPS traffic:**

* roankemortgages.com\r\n
* tonmatdoanminh.com\r\n
* 6Aov

Malware Type: Trojan