Malware Sandbox Analysis & IOC Extraction

Project Type: Threat Intelligence & Malware Analysis

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this project was to perform controlled behavioral analysis of a suspicious executable within an isolated malware sandbox environment. The goal was to observe runtime behavior, identify malicious characteristics, extract Indicators of Compromise (IOCs), and map observed activity to MITRE ATT&CK techniques to support SOC detection, threat intelligence, and DFIR workflows.

Tools & Technologies

- Isolated Windows malware sandbox environment
- Process execution and behavior monitoring
- Network traffic capture and analysis
- File system and registry monitoring tools
- IOC extraction and correlation utilities
- MITRE ATT&CK framework

Technical Steps Performed

- **Sandbox Detonation**
  - Executed the suspicious sample within a controlled and isolated Windows sandbox.
  - Ensured no external production systems were exposed during execution.
- **Process Behavior Monitoring**
  - Observed process creation events and parent–child process relationships.
  - Identified abnormal execution chains indicative of malicious activity.
- **Network Activity Analysis**
  - Captured outbound network connections initiated by the sample.
  - Identified callback domains and IP addresses consistent with command-and-control behavior.
- **File and Registry Monitoring**
  - Recorded file system modifications and registry changes made during execution.
  - Identified artifacts suggesting persistence or configuration changes.
- **MITRE ATT&CK Mapping**
  - Correlated observed behaviors with applicable MITRE ATT&CK techniques.
  - Classified tactics related to execution, persistence, and command-and-control.
- **IOC Extraction**
  - Extracted hashes, domains, and IP addresses.
  - Prepared indicators for SOC ingestion, blocking, and threat hunting.

Findings

- Malicious process behavior was observed during execution, including suspicious child process spawning.
- Network callbacks were detected, consistent with command-and-control communication.
- File system and registry modifications indicated attempts at persistence.
- Detection signatures and IOCs were successfully generated for SOC use.

Outcome

- The analyzed sample was classified as malicious based on observed behavior.
- Actionable IOCs were produced for SIEM correlation, detection engineering, and blocking.
- Findings support SOC analyst triage, threat intelligence enrichment, and DFIR readiness.
- Demonstrated hands-on capability in malware behavioral analysis and SOC-relevant intelligence production.

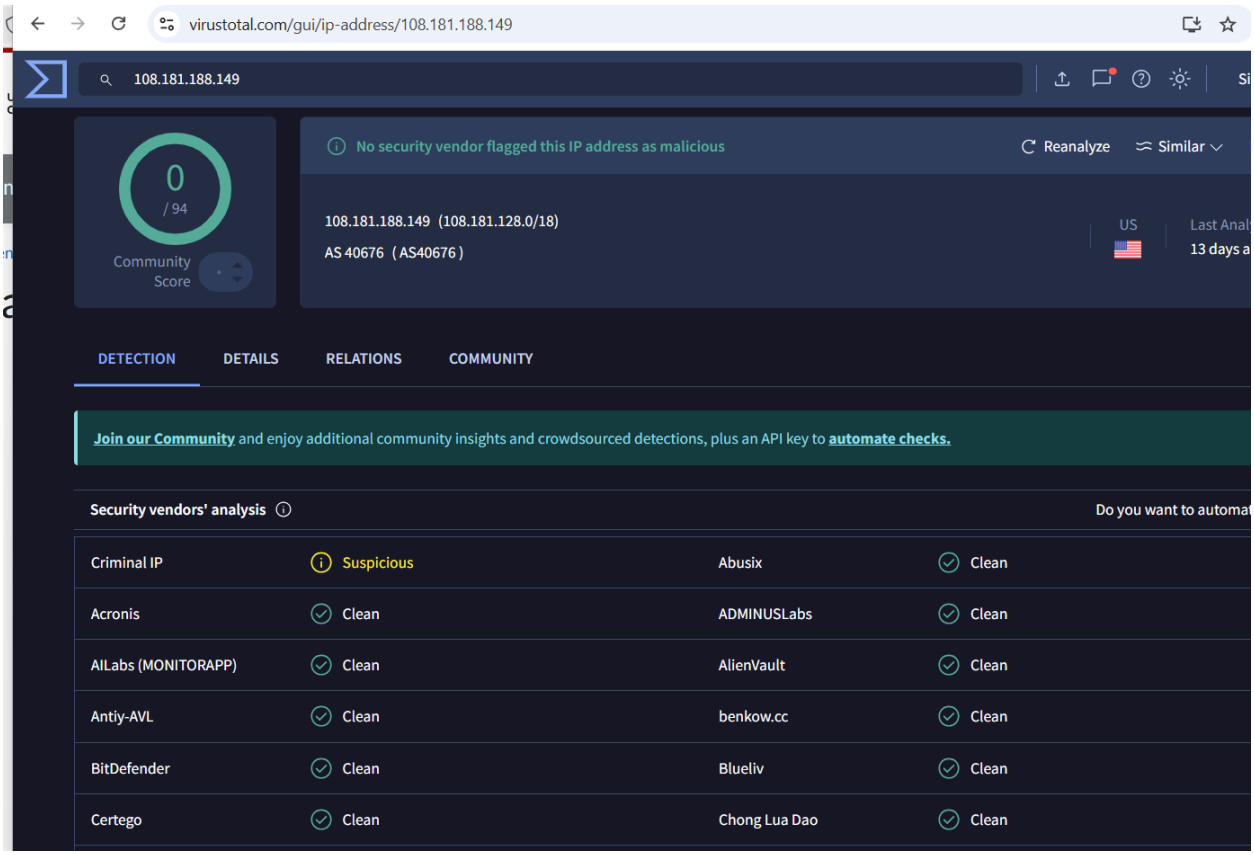
Evidence

- Malware sandbox execution summary screenshots
- Process tree and execution flow captures
- Network callback and traffic analysis screenshots
- File system and registry modification evidence
- Extracted IOC listings suitable for SOC ingestion

Portfolio Status

Project Status: Completed

Evidence: Malware sandbox screenshots, process trees, network activity captures, IOC extraction


virustotal.com/gui/ip-address/108.181.188.149
108.181.188.149
0
/ 94
Community Score
No security vendor flagged this IP address as malicious
Reanalyze
Similar
108.181.188.149 (108.181.128.0/18)
AS 40676 (AS40676)
US
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Criminal IP Suspicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Antiy-AVL Clean
benkow.cc Clean
BitDefender Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean

TALOS-2024-2046

Wavlink AC3000 touchlist_sync.cgi touchlistsync() buffer overflow vulnerability

JANUARY 14, 2025

CVE NUMBER

CVE-2024-36258

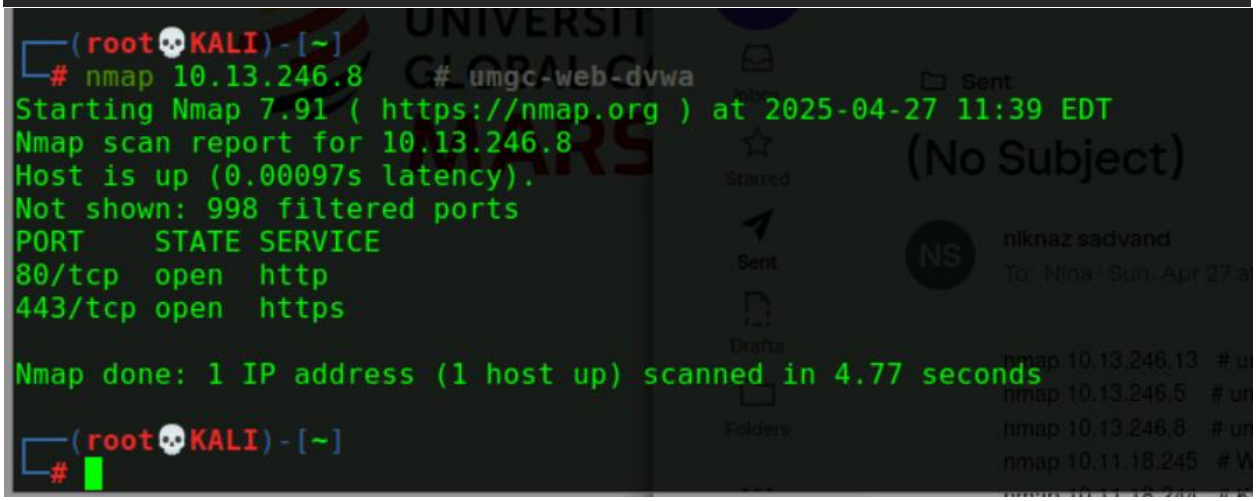
SUMMARY

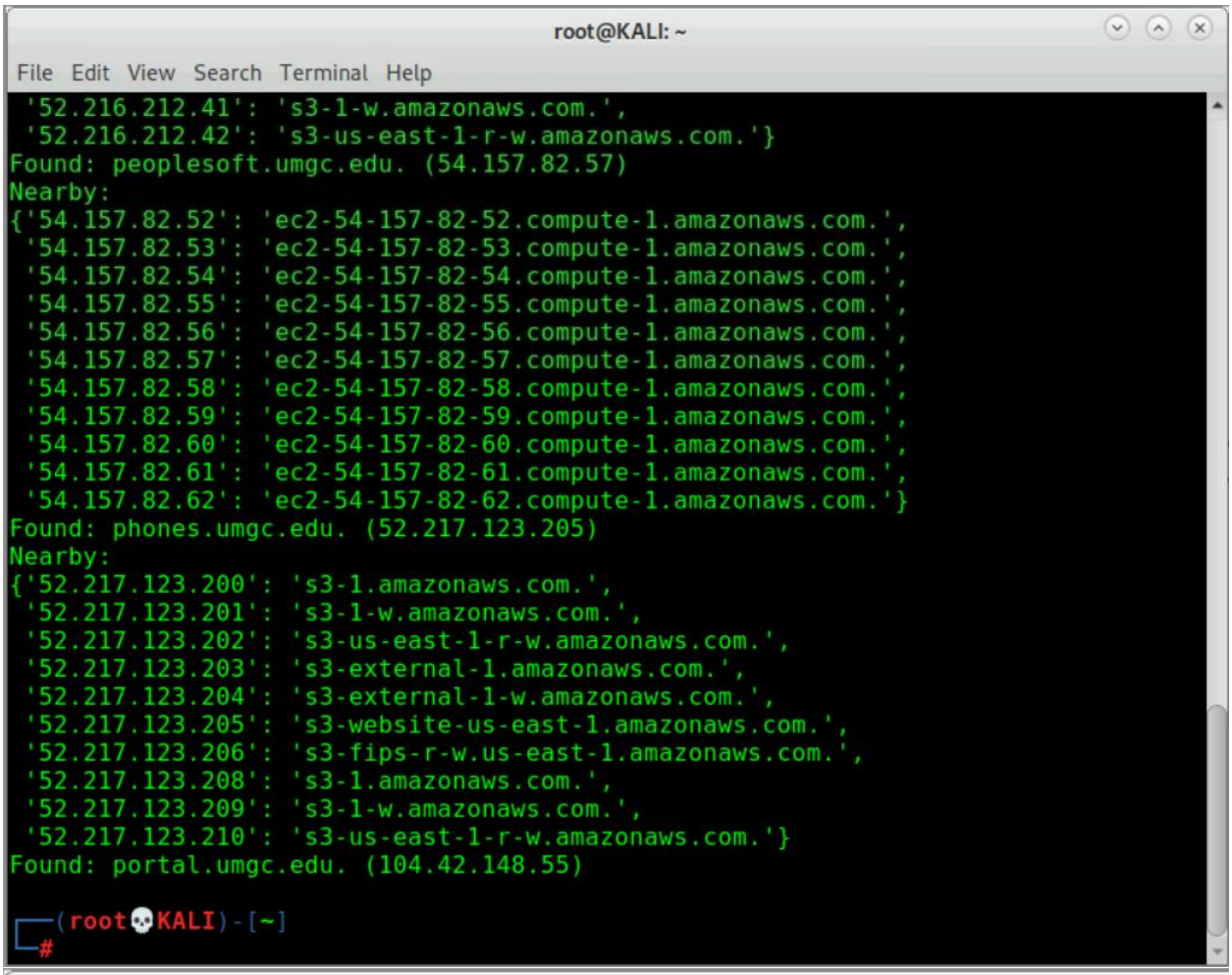
A stack-based buffer overflow vulnerability exists in the touchlist_sync.cgi touchlistsync() functionality of Wavlink AC3000 M33A8.V5030.210505. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send an HTTP request to trigger this vulnerability.

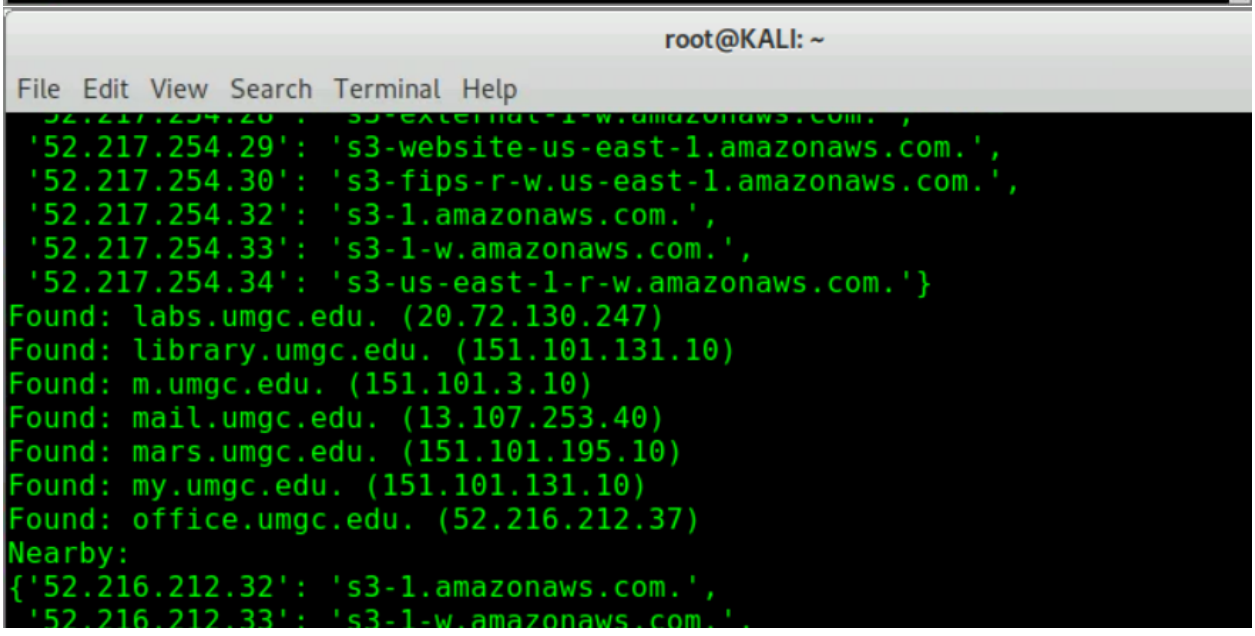
CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

Wavlink AC3000 M33A8.V5030.210505




root@KALI: ~
File Edit View Search Terminal Help
'52.216.212.41': 's3-1-w.amazonaws.com.',
'52.216.212.42': 's3-us-east-1-r-w.amazonaws.com.'}
Found: peoplesoft.umgc.edu. (54.157.82.57)
Nearby:
{'54.157.82.52': 'ec2-54-157-82-52.compute-1.amazonaws.com.',
'54.157.82.53': 'ec2-54-157-82-53.compute-1.amazonaws.com.',
'54.157.82.54': 'ec2-54-157-82-54.compute-1.amazonaws.com.',
'54.157.82.55': 'ec2-54-157-82-55.compute-1.amazonaws.com.',
'54.157.82.56': 'ec2-54-157-82-56.compute-1.amazonaws.com.',
'54.157.82.57': 'ec2-54-157-82-57.compute-1.amazonaws.com.',
'54.157.82.58': 'ec2-54-157-82-58.compute-1.amazonaws.com.',
'54.157.82.59': 'ec2-54-157-82-59.compute-1.amazonaws.com.',
'54.157.82.60': 'ec2-54-157-82-60.compute-1.amazonaws.com.',
'54.157.82.61': 'ec2-54-157-82-61.compute-1.amazonaws.com.',
'54.157.82.62': 'ec2-54-157-82-62.compute-1.amazonaws.com.'}
Found: phones.umgc.edu. (52.217.123.205)
Nearby:
{'52.217.123.200': 's3-1.amazonaws.com.',
'52.217.123.201': 's3-1-w.amazonaws.com.',
'52.217.123.202': 's3-us-east-1-r-w.amazonaws.com.',
'52.217.123.203': 's3-external-1.amazonaws.com.',
'52.217.123.204': 's3-external-1-w.amazonaws.com.',
'52.217.123.205': 's3-website-us-east-1.amazonaws.com.',
'52.217.123.206': 's3-fips-r-w.us-east-1.amazonaws.com.',
'52.217.123.208': 's3-1.amazonaws.com.',
'52.217.123.209': 's3-1-w.amazonaws.com.',
'52.217.123.210': 's3-us-east-1-r-w.amazonaws.com.'}
Found: portal.umgc.edu. (104.42.148.55)
(root KALI)-[~]
#


root@KALI: ~
File Edit View Search Terminal Help
'52.217.254.29': 's3-website-us-east-1.amazonaws.com.',
'52.217.254.30': 's3-fips-r-w.us-east-1.amazonaws.com.',
'52.217.254.32': 's3-1.amazonaws.com.',
'52.217.254.33': 's3-1-w.amazonaws.com.',
'52.217.254.34': 's3-us-east-1-r-w.amazonaws.com.'}
Found: labs.umgc.edu. (20.72.130.247)
Found: library.umgc.edu. (151.101.131.10)
Found: m.umgc.edu. (151.101.3.10)
Found: mail.umgc.edu. (13.107.253.40)
Found: mars.umgc.edu. (151.101.195.10)
Found: my.umgc.edu. (151.101.131.10)
Found: office.umgc.edu. (52.216.212.37)
Nearby:
{'52.216.212.32': 's3-1.amazonaws.com.',