

CYBER THREAT






INTELLIGENCE REPORT

DATE OF REPORT: DECEMBER 26, 2024
PREPARED BY: RUSHIRAJ SOLANKI ,
CYBERSECURITY ANALYST



I. Executive Summary:

II. Background and Context:



III. IOC Analysis:

- Identified IP Address: 
- Threat Categories: 
- Associated Domains and URLs: 

IV. Detection Methods:









- Security Vendor Analysis: 
- Threat Intelligence Feeds: 

V. Behavior Analysis:




- Open Ports: 
- Network Traffic Analysis: 
- Vulnerability Assessment: 

VI. Risk Assessment:

VII. Malware Persistence and Analysis:

- Introduction: 
- Basic Properties: 
- Description: 
- Detection Aliases: 
- Sandboxing Analysis: 
- MITRE ATT&CK Techniques: 
- Executed Commands: 
- Sigma Rules: 

VIII. Recommendations:

- Immediate Actions: 
- Detection and Response: 
- Long-term Strategies: 

IX. Conclusion:

1. Executive Summary

The purpose of this report is to analyze the IP address **198.1.82.225** for any potential malicious activities. The IP address has been flagged by multiple sources and is associated with suspicious behavior, including email spam and hacking attempts. This report provides a comprehensive analysis of the IP address, its activities, associated malware, and recommendations for mitigating potential threats.



Open Ports	! 14
Vulnerabilities	! 498
Exploit DB	! 17
Policy Violation	! 3
Remote Address	! True

2. Background and Context

Network: 198.1.64.0/18

Autonomous System Number: 46606

Autonomous System Label: UNIFIEDLAYER-AS-1

Regional Internet Registry: ARIN

Country: U S

NetRange: 198.1.64.0 - 198.1.127.255

CIDR: 198.1.64.0/18

NetName: UNIFIEDLAYER-NETWORK-11

NetHandle: NET-198-1-64-0-1

Parent: NET198 (NET-198-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS46606

Organization: Unified Layer (BLUEH-2)

RegDate: 2012-07-02

Updated: 2012-11-14

Ref: <https://rdap.arin.net/registry/ip/198.1.64.0>

OrgName: Unified Layer

OrgId: BLUEH-2

Address: 1958 South 950 East

City: Provo

StateProv: UT

PostalCode: 84606

Country: US

RegDate: 2006-08-08

Updated: 2020-01-31

Ref: <https://rdap.arin.net/registry/entity/BUEH-2>

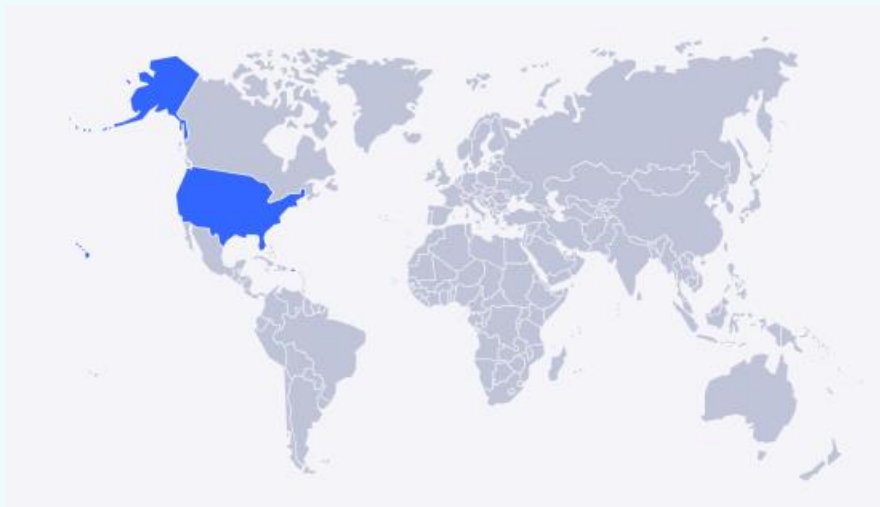
ReferralServer: rwhois://rwhois.unifiedlayer.com:4321

OrgTechHandle: ENO74-ARIN

OrgTechName: EIG Network Operations

OrgTechPhone: +1-877-659-6181

OrgTechEmail: eig-noc@endurance.com



3. IOC Analysis

I. Identified IP Address

- **IP Address:** 198.1.82.225
- **ISP:** WEBSITEWELCOME.COM
- **Organization:** Unified Layer (AS 46606)
- **Location:** United States, Tabiona, Utah

II. Threat Categories

- **Email Spam:** High probability of spam activities.
- **Hacking:** Involvement in brute-force attempts and hacking incidents.
- **Malware:** Presence of Trojan-Dropper malware.

III. Associated Domains and URLs

- **Hostname:** 198-1-82-225.unifiedlayer.com
- **Domain Name:** websitewelcome.com

4. Detection Methods

I. Security Vendor Analysis

The IP address **198.1.82.225** has been flagged by various security vendors, with detailed analysis from VirusTotal indicating a minimal threat profile, but with specific vendors identifying spam and potential malicious activities.

Flagged by:

- **Abusix:** Spam
- **Criminal IP:** Malicious
- **Clean by:** Acronis, AILabs (MONITORAPP), alphaMountain.ai, benkow.cc, and others.




II. Threat Intelligence Feeds

The IP address has multiple reports from distinct sources, suggesting a pattern of malicious behavior:

- **Total Reports:** 7 times from 4 sources.
- **Categories:** Email Spam, Hacking, Brute-Force.
- **Examples:** High probability of spam (Score: 39.60), Rejected on IP Reputation - McAfee Exchange Plug-in (326).



Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

	2024-11-01 13:04:30 (2 months ago)	Email spam / scam (from=<duke@nnpc-london.com> ... helo=<server.usedtestserver.com>)	Email Spam
	2024-10-28 17:21:38 (2 months ago)	Rejected on IP Reputation - McAfee Exchange Plug-in (326)	Email Spam
	2024-10-28 04:49:04 (2 months ago)	Mail/25/465/587-993/995 Probe, Reject, BadAuth, Hack, SPAM -	Email Spam Hacking Brute-Force

5. Behavior Analysis

I. Open Ports

- **Current Open Ports:** 21, 22, 25, 26, 53, 80, 110, 111, 143, 587, 2077, 2095, 2096, 3306.
- **Vulnerable Ports:** 21, 22, 25, 26, 587, 3306.



II. Network Traffic Analysis

The IP address has shown suspicious network activities, including connections initiated by office applications to non-local IP addresses. These activities align with Sigma rules related to potential vulnerabilities and exploitation methods.

EMAIL VOLUME DATA	
	LAST DAY
EMAIL VOLUME	4.3
VOLUME CHANGE	4.65% ↑
SPAM LEVEL	Critical

III. Vulnerability Assessment

The IP address has several vulnerabilities associated with services like OpenSSH and Apache:

- **CVE-2023-38408: Critical - OpenSSH vulnerability.**
- **CVE-2023-31122: High - Apache vulnerability.**
- **CVE-2023-28625: High - Vulnerability affecting multiple services.**

CVE-2023-38408 CWE: 1 TCP 22

GitHub PoC Link

[Upgrade Your Plan](#) ?

CVSS v2 :Not available / None CVSS v3 :NETWORK / Critical

Product: **OpenSSH** (v4.3) ! Vulnerability found.

Vendor: openssh

Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. ^

6. Risk Assessment

❖ **Severity:** High

❖ **Impact:**

- **Reputational Damage:** The association with spam and spoofing activities can damage the sender reputation and negatively impact email deliverability.
- **Network Disruption:** The IP address may be involved in Distributed Denial-of-Service (DDoS) attacks or other network disruptions, affecting service availability.
- **Data Breaches:** There is a significant risk of data breaches and other security incidents due to the malware and hacking attempts associated with this IP address.
- **Legal and Compliance Issues:** Engaging in spamming activities and other malicious behaviors can have serious legal implications, including fines and sanctions for non-compliance with cybersecurity regulations.

❖ **Urgency:** High

❖ **Likelihood:** High

This assessment highlights the serious nature of the threats posed by the IP address 198.1.82.225. The high severity, impact, and likelihood underline the need for immediate action to mitigate potential risks.



7. Malware Persistence and Analysis



I. Introduction

This section provides a detailed analysis of the malware associated with the IP address 198.1.82.225, focusing on its persistence mechanisms, behaviors, and impact. The malware has been identified as a Trojan-Dropper, designed to secretly install other malicious programs and evade detection.

II. Basic Properties

- **MD5:** 04215898aaf389c83c29f04044b1f9df
- **SHA-1:** 90ab5d649525a5be554a135eb3ae69e4f0ceedc
- **SHA-256:**
5efff79fe8ae2ce19fbe3d804033bfc1c7bd90883451adbaa4b17d72629cda11
- **Vhash:** fe43cc098163d8fb4f1b2b088de0949b
- **SSDEEP:**
12288:IWtMwD995UgxoqsE7U3YzL0zdilxFdusroRYodCKM7:fMwDmCfWYzxlxFdH2Yo
- **TLSH:**
T184D4011132E94E07F23B9E715CE2C48B9626FC85EE35C78F3295730E5670690E671B2A
- **File Type:** Outlook internet email (CDFV2 Microsoft Outlook Message)
- **File Size:** 597.50 KB (611840 bytes)

III. Description

Trojan-Dropper programs are designed to secretly install malicious programs embedded in their code on victim computers. They typically save a range of files to various directories on the victim's drive (e.g., Windows directory, Windows system directory, temporary directory) and launch them without any notification. These programs are used by hackers to:

- Secretly install Trojan programs and/or viruses.
- Protect known malicious programs from being detected by antivirus solutions.

IV. Detection Aliases

The malware has been detected and identified by various antivirus software under different aliases:

- Win32:Malware-gen
- Trojan.PasswordStealer.GenericKDS.3240
- PossibleThreat.FORTIEDR.H
- Trojan.Autoit
- Trojan (00564f471)
- Artemis!Trojan
- Trojan:Win32/AutoitInject.HNA!MTB
- Mal/DrodRar-AIC
- TrojanSpy.Win32.SNAKEKEYLOGGER.YXELEZ
- W32/Autoit.OL.gen!Eldorado
- Trojan. SpamMalware-RAR.Gen

V. Sandboxing Analysis

System Summary (17):

❖ Suspicious Activities:

- 1.0: Sigma detected: Suspicious Office Outbound Connections
- 1.0: Sigma detected: Potential WWlib.DLL Sideload
- 1.0: Deletes files inside the Windows folder
- 1.0: Sigma detected: Office Autorun Keys Modification
- 1.0: Creates files inside the system directory
- 0.0: Creates temporary files
- 0.0: Reads software policies
- 0.0: Writes ini files
- 0.0: Classification label
- 0.0: Reads ini files
- 0.0: Uses an in-process (OLE) Automation server
- 0.0: Reads the hosts file
- 0.0: Creates files inside the user directory
- -1.0: Checks if Microsoft Office is installed
- -2.0: Found graphical window changes (likely an installer)
- -2.0: Found window with many clickable UI elements (buttons, textforms, scrollbars etc)

❖ Boot Survival (1):

- 1.0: Creates or modifies Windows services

❖ Hooking and Other Techniques for Hiding and Protection (1):

- 0.0: Disables application error messages (SetErrorMode)

❖ Malware Analysis System Evasion (1):

- 0.0: Checks the free space of hard drives

❖ Networking (1):

- 0.0: URLs found in memory or binary data

VI. MITRE ATT&CK Techniques

❖ Persistence:

- T1543.003: Windows Service (Medium confidence)

• Privilege Escalation:

- T1543.003: Windows Service (Medium confidence)

❖ Defense Evasion:

- T1036: Masquerading (Medium confidence)
- T1070.004: File Deletion (Medium confidence)

❖ Discovery:

- T1083: File and Directory Discovery (Low confidence)
- T1082: System Information Discovery (Low confidence)
- T1018: Remote System Discovery (Low confidence)

VII. Executed Commands

• InputApp:

- C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe -
ServerName:InputApp.AppX9jnwykgrccxc8by3hsrsh07r423xzvav.mca

• WdiSystemHost:

- C:\Windows\System32\svchost.exe -k
LocalSystemNetworkRestricted -p -s WdiSystemHost

• svchost:

- C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
- **Microsoft Edge Update:**
 - "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
- **NetworkService:**
 - C:\Windows\System32\svchost.exe -k NetworkService -p
- **SgrmBroker:**
 - C:\Windows\system32\SgrmBroker.exe
- **W32Time:**
 - C:\Windows\system32\svchost.exe -k LocalService -s W32Time
- **Windows Security Center:**
 - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
- **UnistackSvcGroup:**
 - C:\Windows\system32\svchost.exe -k UnistackSvcGroup
- **Local Security Authority Subsystem Service (lsass):**
 - C:\Windows\system32\lsass.exe

VIII. Sigma Rules

- **Suspicious Office Outbound Connections:**
 - Detection of office applications initiating network connections to non-local IP addresses.
- **Potential WWlib.DLL Sideload:**
 - Detection of WWlib.DLL sideloading, which can be used to execute malicious code.
- **Office Autorun Keys Modification:**
 - Detection of modifications to Office autorun keys, which can indicate persistence mechanisms.

IX. Conclusion

The malware associated with the IP address 198.1.82.225 demonstrates various sophisticated techniques to establish persistence, evade detection, and perform malicious activities. The detailed properties, sandbox analysis, and MITRE ATT&CK techniques provide a comprehensive understanding of the threat posed by this Trojan-Dropper malware.

8. Recommendations

I. Immediate Actions

- **Block IP Address:** Add **198.1.82.225** to block lists to prevent further malicious activities.
- **Monitor Network Traffic:** Implement advanced monitoring to detect any suspicious activities from this IP address.

II. Detection and Response

- **Update Security Systems:** Ensure all security systems and applications are updated to protect against known vulnerabilities.
- **Incident Response Plan:** Develop and implement an incident response plan to address any potential threats from this IP address.

III. Long-term Strategies

- **Employee Training:** Conduct training sessions to educate employees about the risks of email-based attacks and phishing.
- **Regular Audits:** Perform regular security audits to identify and mitigate potential vulnerabilities.

9. Conclusion

The IP address **198.1.82.225** has been identified as a high-risk entity due to its association with malicious activities. The detailed analysis and recommendations provided in this report aim to mitigate the potential threats and enhance overall security posture.

