



Threat Level

 **Red**

 **CISA: AA24-016A**

HiveForce Labs

# THREAT ADVISORY



**ATTACK REPORT**

## **Androxgh0st Malware Uses Stealthy Tactics in Pilfering Credentials**

Date of Publication

January 19, 2024

Admiralty Code

A1

TA Number

TA2024023

# Summary

**First Seen:** December 2022

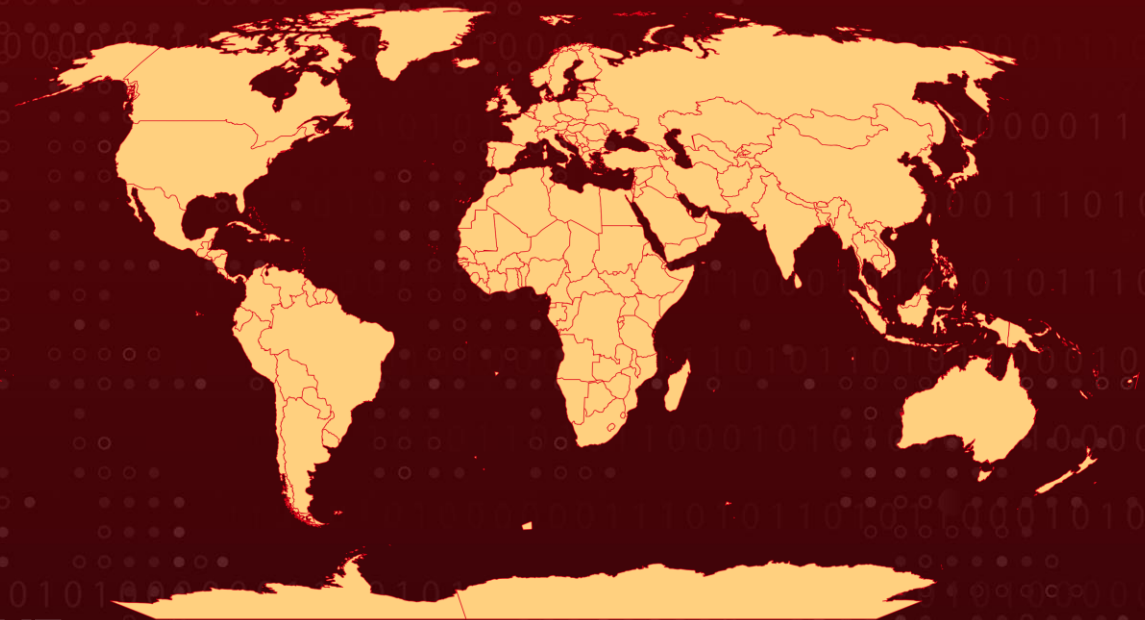
**Malware:** Androxgh0st

**Attack Region:** Worldwide

**Affected Platforms:** Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio.




**Attack:** The Androxgh0st malware is building a botnet, specifically aimed at illicitly obtaining cloud credentials from popular applications such as Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio. This stolen data is then utilized to disseminate additional harmful payloads.

## 🗡️ Attack Regions



## ⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-9841	PHPUnit Command Injection Vulnerability	PHPUnit: 4.8.0 - 5.6.2	❌	✅	✅
CVE-2018-15133	Laravel Deserialization of Untrusted Data Vulnerability	Laravel Framework: 5.5.0 - 5.6.29	❌	✅	✅

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-41773	Apache HTTP Server Path Traversal Vulnerability	Apache HTTP Server versions 2.4.49 or 2.4.50			

# Attack Details

## #1

Malicious actors, utilizing the Androxgh0st malware, are constructing a sophisticated botnet with a specific focus on acquiring cloud credentials illicitly. They then use the stolen data to disseminate additional harmful payloads. Androxgh0st, a Python-scripted malware, is mainly used to target .env files that contain sensitive information, including credentials for well-known applications like Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio, all originating from the Laravel web application framework.

## #2

Initially documented in December 2022, the Androxgh0st malware employs various tactics, including the use of scripts, scanning procedures, and the identification of websites vulnerable to specific exploits. It actively seeks out websites and servers susceptible to remote code execution (RCE) vulnerabilities, specifically targeting the PHPUnit unit testing framework (CVE-2017-9841), Apache HTTP Server (CVE-2021-41773), and Laravel PHP web framework (CVE-2018-15133).

## #3

Androxgh0st encompasses a wide range of functionalities capable to SMTP misuse, including scanning operations, the exploitation of exposed credentials and APIs, and the deployment of web shells. The Androxgh0st botnet diligently searches for websites using the Laravel framework, focusing on identifying exposed root-level .env files containing credentials for additional services.

## #4

Compromised AWS credentials are then used to create new users and user policies, and in some cases, set up new AWS instances for further malicious scanning activities. As threat actors continue to evolve their strategies to capitalize on cloud services, the emergence of tailored tools specifically designed for such services is anticipated, reflecting the targeted exploitation seen in mail services for spamming attacks.

# Recommendations



**Regular Updates:** Keep all operating systems, software, and firmware up to date. Specifically, ensure that Apache servers are not running versions 2.4.49 or 2.4.50.



**URI Configuration:** Verify that the default configuration for all URIs is set to deny all requests unless there is a specific need for accessibility.



**Laravel Application Security:** Ensure that any live Laravel applications are not in “debug” or testing mode. Remove all cloud credentials from .env files and revoke them.



**Credential Review:** On a one-time basis for previously stored cloud credentials, and on an ongoing basis for other types of credentials that cannot be removed, review any platforms or services that have credentials listed in the .env file for unauthorized access or use.



**Anomaly Detection:** Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

## Potential MITRE ATT&CK TTPs

<b><u>TA0043</u></b> Reconnaissance	<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution
<b><u>TA0003</u></b> Persistence	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0006</u></b> Credential Access	<b><u>TA0007</u></b> Discovery
<b><u>TA0009</u></b> Collection	<b><u>TA0011</u></b> Command and Control	<b><u>T1595.002</u></b> Vulnerability Scanning	<b><u>T1583.005</u></b> Botnet
<b><u>T1583.006</u></b> Web Services	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1059.006</u></b> Python	<b><u>T1078</u></b> Valid Accounts
<b><u>T1505.003</u></b> Web Shell	<b><u>T1136</u></b> Create Account	<b><u>T1027.010</u></b> Command Obfuscation	<b><u>T1552.001</u></b> Credentials In Files
<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1046</u></b> Network Service Discovery	<b><u>T1114</u></b> Email Collection	<b><u>T1105</u></b> Ingress Tool Transfer

# ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	<p>hxxp://45.95.147[.]236/tmp.x86_64, hxxp://download.asyncfox[.]xyz/download/xmrig.x86_64, hxxp://main.dsn[.]ovh/dns/pwer, hxxp://raw.githubusercontent[.]com/0x5a455553/MARIJUANA/master/MARIJUANA.php, hxxp://tangible-drink.surge[.]sh/configx.txt, hxxps://chainventures.co[.]uk/.well-known/aas, hxxps://mc.rockylinux[.]si/seoforce/triggers/files/evil.txt, hxxps://pastebin[.]com/raw/zw0gAmpC</p>
SHA256	<p>0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef, 23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066, 59e90be75e51c86b4b9b69dcede2cf815da5a79f7e05cac27c95ec35294151f4, 6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc, bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7, ca45a14d0e88e4aa408a6ac2ee3012bf9994b16b74e3c66b588c7eabaaec4d72, dcf8f640dd7cc27d2399cce96b1cf4b75e3b9f2dfdf19cee0a170e5a6d2ce6b6, De1114a09cbab5ae9c1011ddd11719f15087cc29c8303da2e71d861b0594a1ba</p>
SHA1	<p>06641b9b3b5088c48c7660ad3bf160bc87a929fd, 7d1beb03c32db43f5edd4c28f3c905954e40dbd6, 59ce7486745b08d1adba49f2413133c441194986, 79d3143a47dc02768ff5fda8dbcf464c5cdf115b, 09bd9b17a64b20ba66582dbc3ce08169697177a8, 270e1c883b498eaff08550e823f5cac21bff54e5, 452ec481734a78597b928e29c834d0e43fb2c7e2, 5fae94432540ade68eabce94140c9a5be153b3c8</p>
MD5	<p>95f745a5db131b1ca34e44848fd52edb, 3fae93618edffe4331d18d8b8e6df693, c1070aca9fcff4a32934e6c8aee4ea48, 9039ae16e5aaa63d9ffe88dfaf0f5108, fe53c38f61588efd90af97185e315612, 62a06bea8c6e276b5e532944cfc863e5, 6e793efe40e355643423f53de43952d3, 1fb78440dc44b0900b27260a16d9771e</p>

## Patch Details

<https://www.oracle.com/security-alerts/cpuoct2021.html>

<https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30>

[https://httpd.apache.org/security/vulnerabilities\\_24.html](https://httpd.apache.org/security/vulnerabilities_24.html)

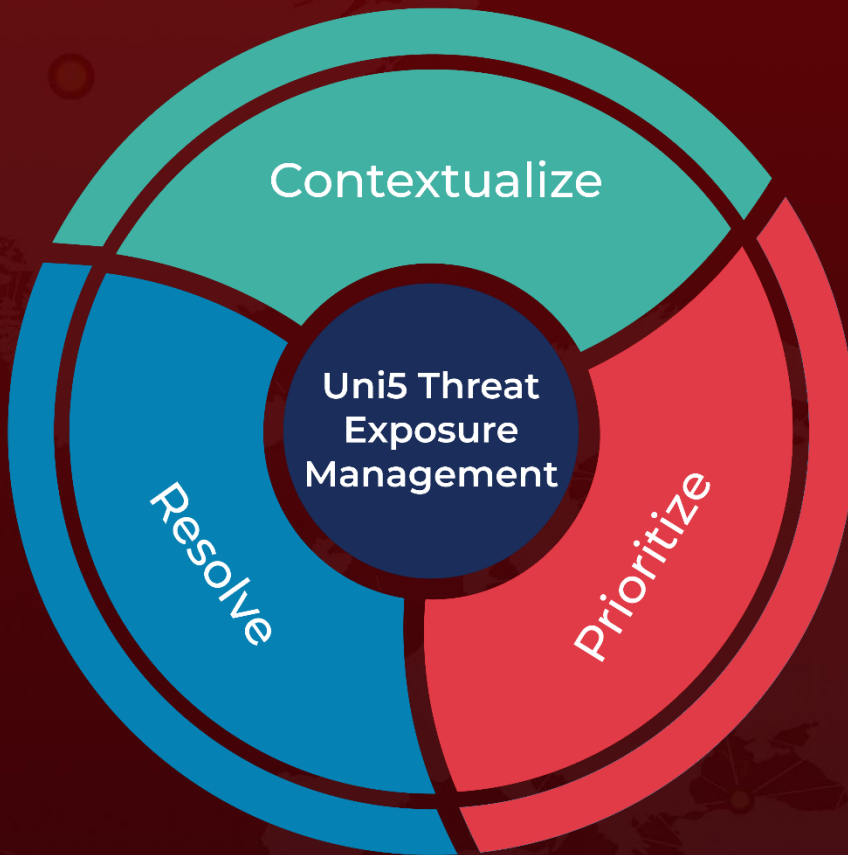
## References

[https://www.cisa.gov/sites/default/files/2024-01/aa24-016a-known-indicators-of-compromise-associated-with-adroxgh0st-malware\\_0.pdf](https://www.cisa.gov/sites/default/files/2024-01/aa24-016a-known-indicators-of-compromise-associated-with-adroxgh0st-malware_0.pdf)

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**January 19, 2024 • 1:00 AM**

© 2024 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)