



HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## ZenRAT Targeting Windows Users Through Fake Bitwarden Installs

Date of Publication

September 27, 2023

Admiralty Code

A1

TA Number

TA2023389

# Summary

**First appeared:** July 28, 2023

**Attack Region:** Worldwide

**Affected Platform:** Windows

**Malware:** ZenRAT

**Attack:** ZenRAT is a new malware distributed through fake Bitwarden password manager installers, primarily targeting Windows users. It operates as a modular remote access trojan (RAT) with information-stealing capabilities.



## Attack Regions



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

# Attack Details

## #1

ZenRAT is a newly identified malware strain that is being disseminated through fake installation packages posing as the Bitwarden password manager. This malware primarily targets Windows users while redirecting non-Windows users to a harmless webpage that emulates opensource.com. The precise method of ZenRAT distribution remains undisclosed, although historical practices have involved techniques such as SEO poisoning, adware bundles, or email-based attacks.

## #2

ZenRAT operates as a modular remote access trojan (RAT) with the ability to steal sensitive information. It conducts system reconnaissance by gathering information about the infected machine, including CPU and GPU details, operating system version, RAM, IP address, antivirus software, and installed applications. This data is subsequently transmitted to a command and control (C2) server in a compressed ZIP file.

## #3

Notably, ZenRAT employs a unique communication protocol with specific command identifiers and data structures. It sends plaintext logs to the C2 server, revealing its actions and system checks, which include geofencing, mutex creation, disk size verification, and anti-virtualization measures.

## Recommendations



**Use Trusted Sources:** Only download software from official and reputable sources. Avoid downloading applications or updates from unfamiliar or suspicious websites.



**Verify Download Links:** Always double-check the legitimacy of download links by comparing them to the official website's URLs. Be cautious of slight misspellings or variations in domain names.



**Employ Reliable Antivirus Software:** Keep your antivirus and anti-malware software up to date. Regularly scan your system for potential threats, and configure it to automatically update and perform scans.



**Email Caution:** Be wary of email attachments and links, especially from unknown or unsolicited sources. Verify the legitimacy of email senders before opening any attachments or clicking on links.

## Potential MITRE ATT&CK TTPs

<b><u>TA0006</u></b> Credential Access	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution
<b><u>TA0043</u></b> Reconnaissance	<b><u>TA0010</u></b> Exfiltration	<b><u>TA0009</u></b> Collection	<b><u>TA0011</u></b> Command and Control
<b><u>TA0040</u></b> Impact	<b><u>T1566</u></b> Phishing	<b><u>T1204.002</u></b> Malicious File	<b><u>T1204</u></b> User Execution
<b><u>T1204.002</u></b> Malicious File	<b><u>T1059.003</u></b> Windows Command Shell	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1059.001</u></b> PowerShell
<b><u>T1036</u></b> Masquerading	<b><u>T1608.006</u></b> SEO Poisoning	<b><u>T1608</u></b> Stage Capabilities	<b><u>T1592</u></b> Gather Victim Host Information
<b><u>T1555.003</u></b> Credentials from Web Browsers	<b><u>T1555</u></b> Credentials from Password Stores	<b><u>T1217</u></b> Browser Bookmark Discovery	<b><u>T1560</u></b> Archive Collected Data
<b><u>T1041</u></b> Exfiltration Over C2 Channel			

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPv4:Port</b>	185[.]186.72.14:9890, 185[.]156.72.8:9890
<b>Domains</b>	bitwariden[.]com, crazygameis[.]com, obsploject[.]com, geogebraa[.]com

TYPE	VALUE
SHA256	e0c067fc8e10a662c42926f6cdadfa5c6b8c90d5dff3f0e9f381210180d47d37, d7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536, 8378c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12, f7573ad27ff407e84d3ebf173cbeaaa6aba62eb74b4b2b934bc0433df3d9e066, e318b2c1693bc771dfe9a66ee2cebcc2b426b01547bb0164d09d025467cb9ee3, 60098db9f251bca8d40bf6b19e3defa1b81ff3bdc13876766988429a2e922a06, ba36d9d6e537a1c1ecdf1ace9f170a3a13c19e77f582a5cae5c928a341c1be8d, 986aa8e20962b28971b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76

## References

<https://www.proofpoint.com/us/blog/threat-insight/zenrat-malware-brings-more-chaos-calm>

# 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

**September 27, 2023 • 5:30 AM**

© 2023 All Rights are Reserved by Hive Pro®



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