

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## The Kuiper Ransomware Surge and Its Dark Origins

Date of Publication

December 19, 2023

Admiralty Code

A1

TA Number

TA2023512

# Summary

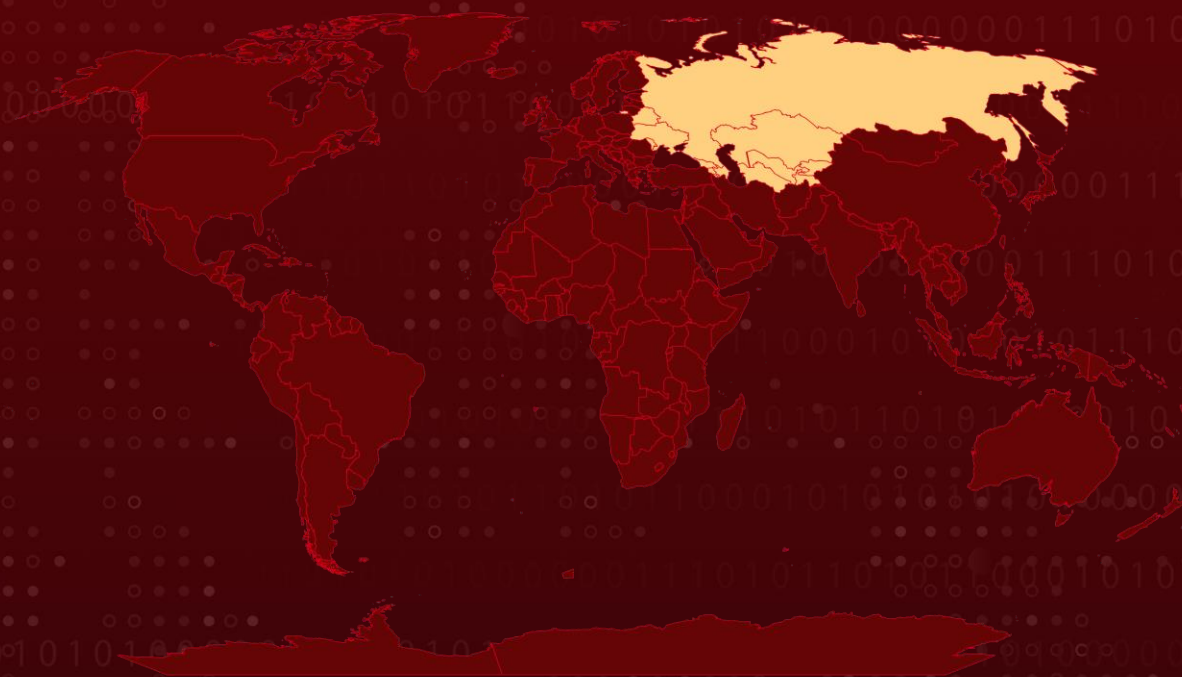
**First Seen:** September 2023

**Malware:** Kuiper ransomware

**Attack Region:** Commonwealth of Independent States (CIS)




**Attack:** In a predominantly Russian Dark Web forum, a sophisticated ransomware-as-a-service (RaaS) project named "KUIPER" was introduced. The Kuiper ransomware, developed in Golang, is compatible with Windows, Linux, and OSX systems, and is associated with a suspected intrusion at a government financial department in Africa.

## Attack Regions



## CVEs

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server			

# Attack Details

## #1

On September 22, 2023, the threat actor group known as "RobinHood" unveiled a new ransomware-as-a-service (RaaS) initiative named "KUIPER" within a predominantly Russian language Dark Web forum. The Kuiper ransomware provides a range of sophisticated services, including support for data exfiltration and cryptocurrency mixing.

## #2

Robinhood has a documented history of buying and selling access to entities within the financial sector, and there are indications of a suspected Kuiper intrusion at an African government financial department. The KUIPER RaaS, meticulously crafted in Golang, boasts compatibility with Windows, Linux, and OSX systems. It utilizes a combination of RSA, ChaCha20, and AES for file encryption.

## #3

The threat actor showcases the capability to establish their initial access points via exploiting ProxyLogon. Before commencing encryption procedures, Kuiper halts services and processes to avoid detection by widely-used antivirus and EDR solutions, including Windows Defender. Following this, it methodically removes malicious code and wipes out system backups, thereby heightening the intricacy of the recovery process.

## #4

Kuiper orchestrates actions to notify system users of the encryption and strategically limits the creation of forensic artifacts. All encrypted files are rebranded to include the ".kuiper" file extension. Additionally, a ransom note is deposited in each folder containing encrypted files.

# Recommendations



**Enhance Network Security Measures:** Strengthen network security protocols to guard against potential infiltrations by Kuiper ransomware and related threat clusters. Employ robust firewalls and intrusion detection systems, and regularly update security software to mitigate vulnerabilities.



**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.



**Zero-Trust Architecture:** Consider adopting a zero-trust architecture, where no device or user is inherently trusted, and verification is required from everyone trying to access resources. This approach can limit the lateral movement within a compromised network.



**Backup and Recovery:** Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

# Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0007</u></b> Discovery	<b><u>TA0008</u></b> Lateral Movement	<b><u>TA0011</u></b> Command and Control
<b><u>TA0010</u></b> Exfiltration	<b><u>T1657</u></b> Financial Theft	<b><u>T1018</u></b> Remote System Discovery	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1055</u></b> Process Injection	<b><u>T1059.001</u></b> PowerShell
<b><u>T1070.001</u></b> Clear Windows Event Logs	<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1082</u></b> System Information Discovery	<b><u>T1071</u></b> Application Layer Protocol
<b><u>T1071.001</u></b> Web Protocols	<b><u>T1490</u></b> Inhibit System Recovery	<b><u>T1486</u></b> Data Encrypted for Impact	<b><u>T1659</u></b> Content Injection
<b><u>T1047</u></b> Windows Management Instrumentation			

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA1</b>	90dd8718560a23faddf99e64b52175d1d765397c
<b>MD5</b>	84820f3eb491a2fde1f52435cd29646c
<b>IPv4</b>	91.92.251[.]25
<b>File Path</b>	C:\\Users\\Public\\safemode.exe

## Patch Link

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855>

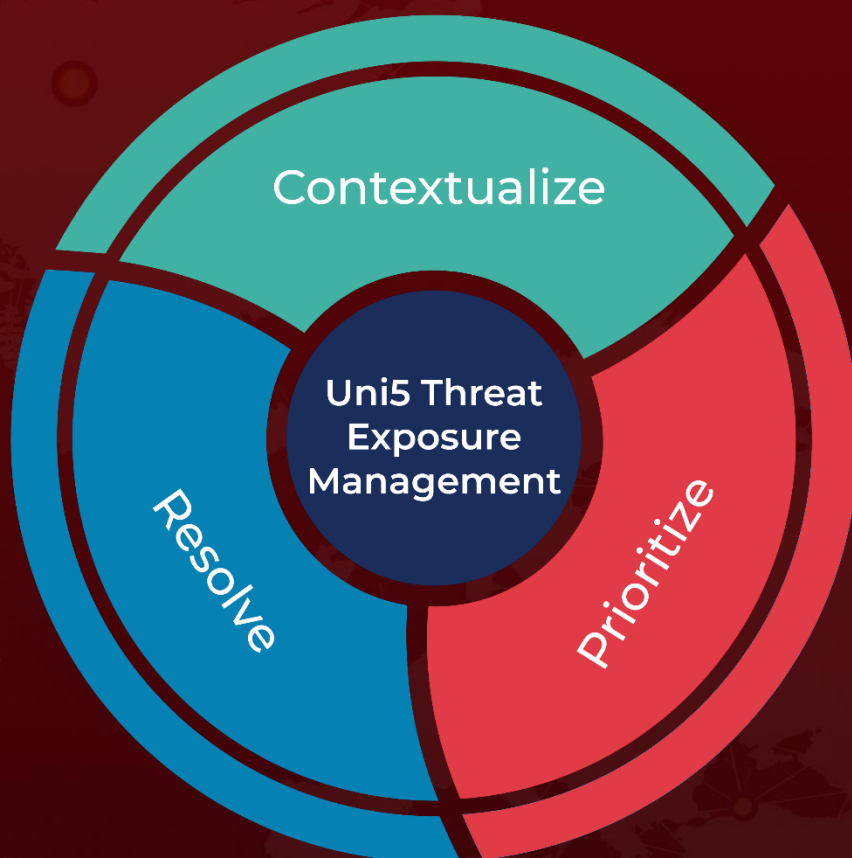
## References

<https://stairwell.com/resources/kuiper-ransomware-analysis-stairwells-technical-report/>

# 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

**December 19, 2023 • 9:30 PM**

© 2023 All Rights are Reserved by Hive Pro<sup>®</sup>



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