

HiveForce Labs

# THREAT ADVISORY

**ACTOR REPORT**

## Unveiling the Stealthy Operations of GoldenJackal APT Group

Date of Publication

May 24, 2023

Admiralty code

A1

TA Number

TA2023243

# Summary

**First Appearance:** 2019

**Actor Name:** GoldenJackal APT

**Target Region:** Middle East and South Asia




**Target Sectors:** Government and Diplomatic entities

**Malware:** JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher

## Actor Map



## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows			

# Actor Details

## #1

GoldenJackal, an APT group active since 2019, targets government and diplomatic entities in the Middle East and South Asia. Despite their low profile, they possess advanced capabilities. Their toolset comprises .NET malware, including JackalControl, JackalWorm, JackalSteal, JackalPerInfo, and JackalScreenWatcher. These tools enable them to gain control over victim machines, spread through removable drives, steal sensitive information, monitor web activities, and capture screen images.

## #2

GoldenJackal employs various infection vectors, such as fake Skype installers containing the JackalControl Trojan and a legitimate Skype for Business installer. They also use malicious Word documents that exploit vulnerabilities like Follina to download and execute the malware. For instance, a document titled "Gallery of Officers Who Have Received National And Foreign Awards.docx" was distributed, appearing to collect information about decorated officers in Pakistan.

## #3

In some cases, the exact infection vector remains unknown, but GoldenJackal has been observed compromising systems during lateral movements. They utilize tools like psexec to initiate malicious batch scripts, installing the JackalControl Trojan and gathering system information. This Trojan allows remote control through an HTTPS communication channel with the group's command and control servers.

## #4

GoldenJackal's primary motivation appears to be espionage, given their targeting of government and diplomatic entities and the capabilities of their malware. While their activities have remained relatively unknown, monitoring efforts have provided insights into their operations. As the threat landscape continues to evolve, organizations and security researchers must remain vigilant to detect and defend against sophisticated APT groups like GoldenJackal.

## Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
GoldenJackal APT	Unknown	Middle East and South Asia	Government and Diplomatic entities
	<b>MOTIVE</b>		
	Information theft and espionage		

# Recommendations



**Patch and Update Software:** Ensure that all software, including operating systems, applications, and security tools, are regularly patched and updated with the latest security patches. The GoldenJackal APT group often exploits vulnerabilities in software to gain access to systems. By promptly applying patches and updates, you can address known vulnerabilities and reduce the risk of successful exploitation.



**Implement Strong Security Controls:** Deploy robust security controls to protect your network and endpoints. This should include using a reliable firewall, intrusion detection and prevention systems, antivirus and anti-malware solutions, and email filtering mechanisms. These security measures can help detect and block malicious activities associated with the GoldenJackal APT group, such as malicious attachments, phishing emails, or command-and-control communications.



**Implement Least Privilege and Access Controls:** Enforce the principle of least privilege by granting users only the necessary permissions required to perform their tasks. Limit administrative privileges and implement strong access controls to prevent unauthorized access to sensitive systems and data. Regularly review and update user access privileges to ensure that only authorized individuals have access to critical resources.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0011</u></b> Command and Control	<b><u>TA0007</u></b> Discovery
<b><u>TA0009</u></b> Collection	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence
<b><u>T1027</u></b> Obfuscated Files or Information	<b><u>T1219</u></b> Remote Access Software	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1112</u></b> Modify Registry
<b><u>T1021</u></b> Remote Services	<b><u>T1003</u></b> OS Credential Dumping	<b><u>T1056</u></b> Input Capture	<b><u>T1574</u></b> Hijack Execution Flow
<b><u>T1055</u></b> Process Injection	<b><u>T1090</u></b> Proxy	<b><u>T1566</u></b> Phishing	<b><u>T1218</u></b> System Binary Proxy Execution

<b><u>T1566.001</u></b> Spearphishing Attachment	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1021</u></b> Remote Services	<b><u>T1041</u></b> Exfiltration Over C2 Channel
<b><u>T1555</u></b> Credentials from Password Stores	<b><u>T1005</u></b> Data from Local System	<b><u>T1102</u></b> Web Service	<b><u>T1113</u></b> Screen Capture
<b><u>T1204</u></b> User Execution	<b><u>T1204.002</u></b> Malicious File	<b><u>T1036</u></b> Masquerading	<b><u>T1221</u></b> Template Injection
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1092</u></b> Communication Through Removable Media	<b><u>T1053</u></b> Scheduled Task/Job

## ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>MD5</b>	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c 8c1070f188ae87fba1148a3d791f2523 c05999b9390a3d8f4086f6074a592bc2 5de309466b2163958c2e12c7b02d8384 a491aefb659d2952002ef20ae98d7465 1072bfeee89e369a9355819ffa39ad20
<b>URLs</b>	hxxp://abert-online[.]de/meeting/plugins[.]php hxxp://acehigh[.]host/robotx[.]php hxxp://assistance[.]uz/admin/plugins[.]php hxxp://cnom[.]sante[.]gov[.]ml/components/com_avreloaded/views/po pup/tmpl/header[.]php hxxp://info[.]merysof[.]am/plugins/search/content/plugins[.]php hxxp://invest[.]zyrardow[.]pl/admin/model/setting/plugins[.]php hxxp://weblines[.]gr/gallery/gallery_input[.]php hxxp://www[.]wetter-bild[.]de/plugins[.]php hxxps://ajapnyakmc[.]com/wp-content/cache/index[.]php hxxps://asusiran[.]com/wp-content/plugins/persian- woocommerce/include/class-cache[.]php hxxps://asusiran[.]com/wp- content/themes/woodmart/inc/modules/cache[.]php

TYPE	VALUE
URLs	<p> <a href="https://croma[.]vn/wp-content/themes/croma/template-parts/footer[.]php">https://croma[.]vn/wp-content/themes/croma/template-parts/footer[.]php</a>  <a href="https://den-photomaster[.]kz/wp-track[.]php">https://den-photomaster[.]kz/wp-track[.]php</a>  <a href="https://eyetelligence[.]ai/wp-content/themes/cms/inc/template-parts/footer[.]php">https://eyetelligence[.]ai/wp-content/themes/cms/inc/template-parts/footer[.]php</a>  <a href="https://finasteridehair[.]com/wp-includes/class-wp-network-statistics[.]php">https://finasteridehair[.]com/wp-includes/class-wp-network-statistics[.]php</a>  <a href="https://gradaran[.]be/wp-content/themes/tb-sound/inc/footer[.]php">https://gradaran[.]be/wp-content/themes/tb-sound/inc/footer[.]php</a>  <a href="https://mehrganhospital[.]com/wp-includes/class-wp-tax-system[.]php">https://mehrganhospital[.]com/wp-includes/class-wp-tax-system[.]php</a>  <a href="https://meukowcognac[.]com/wp-content/themes/astra/page-flags[.]php">https://meukowcognac[.]com/wp-content/themes/astra/page-flags[.]php</a>  <a href="https://nassiraq[.]iq/wp-includes/class-wp-header-styles[.]php">https://nassiraq[.]iq/wp-includes/class-wp-header-styles[.]php</a>  <a href="https://new[.]jmcashback[.]com/wp-track[.]php">https://new[.]jmcashback[.]com/wp-track[.]php</a>  <a href="https://news[.]lmond[.]com/wp-content/themes/newsbook/inc/footer[.]php">https://news[.]lmond[.]com/wp-content/themes/newsbook/inc/footer[.]php</a>  <a href="https://pabalochistan[.]gov[.]pk/new/wp-content/cache/functions[.]php">https://pabalochistan[.]gov[.]pk/new/wp-content/cache/functions[.]php</a>  <a href="https://pabalochistan[.]gov[.]pk/new/wp-content/themes/dt-the7/inc/cache[.]php">https://pabalochistan[.]gov[.]pk/new/wp-content/themes/dt-the7/inc/cache[.]php</a>  <a href="https://pabalochistan[.]gov[.]pk/new/wp-content/themes/twentyfifteen/content-manager[.]php">https://pabalochistan[.]gov[.]pk/new/wp-content/themes/twentyfifteen/content-manager[.]php</a>  <a href="https://sbj-i[.]com/wp-content/plugins/wp-persian/includes/class-wp-cache[.]php">https://sbj-i[.]com/wp-content/plugins/wp-persian/includes/class-wp-cache[.]php</a>  <a href="https://sbj-i[.]com/wp-content/themes/hamyarwp-spacious/cache[.]php">https://sbj-i[.]com/wp-content/themes/hamyarwp-spacious/cache[.]php</a>  <a href="https://sokerpower[.]com/wp-includes/class-wp-header-styles[.]php">https://sokerpower[.]com/wp-includes/class-wp-header-styles[.]php</a>  <a href="https://technocometsolutions[.]com/wp-content/themes/seofy/templates-sample[.]php">https://technocometsolutions[.]com/wp-content/themes/seofy/templates-sample[.]php</a>  <a href="https://www[.]djstuff[.]fr/wp-content/themes/twentyfourteen/inc/footer[.]php">https://www[.]djstuff[.]fr/wp-content/themes/twentyfourteen/inc/footer[.]php</a>  <a href="https://www[.]perlesoie[.]com/wp-content/plugins/contact-form-7/includes/cache[.]php">https://www[.]perlesoie[.]com/wp-content/plugins/contact-form-7/includes/cache[.]php</a>  <a href="https://www[.]perlesoie[.]com/wp-content/themes/flatsome/inc/classes/class-flatsome-cache[.]php">https://www[.]perlesoie[.]com/wp-content/themes/flatsome/inc/classes/class-flatsome-cache[.]php</a>  <a href="https://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php">https://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php</a>  <a href="https://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php">https://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php</a>  <a href="https://www[.]pak-developers[.]net/internal_data/templates/template.html">https://www[.]pak-developers[.]net/internal_data/templates/template.html</a>  <a href="https://www[.]pak-developers[.]net/internal_data/templates/bottom.jpg">https://www[.]pak-developers[.]net/internal_data/templates/bottom.jpg</a> </p>

## Patch Link

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190>

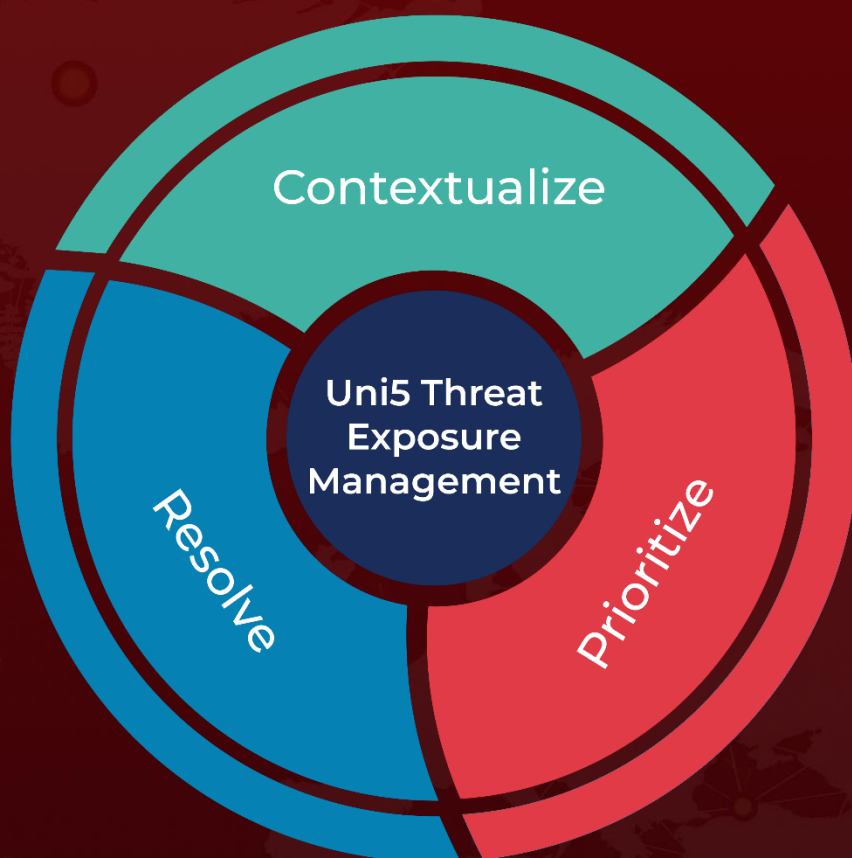
## References

<https://securelist.com/goldenjackal-apt-group/109677/>

# 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

**May 24, 2023 • 6:00 AM**

© 2023 All Rights are Reserved by HivePro



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