

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## **APT34 Tightens Cyber Espionage Grip on Gulf with Kernel Exploitation**

Date of Publication

October 14, 2024

Admiralty Code

A1

TA Number

TA2024392

# Summary

**Attack Discovered:** 2024

**Targeted Countries:** United Arab Emirates (UAE) and the broader Gulf region

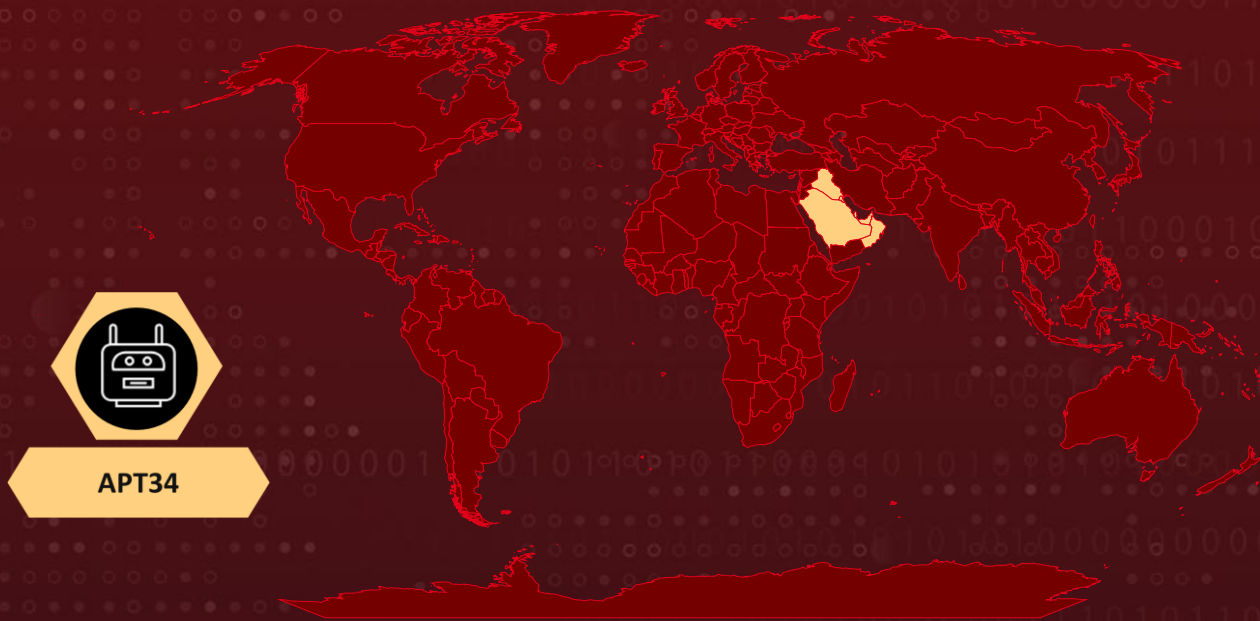
**Targeted Industries:** Governmental Entities and Critical Infrastructure

**Malware:** StealHook, DULLDROP

**Actor:** APT34 (aka Earth Simnavaz, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, DEV-0861, EUROPIUM, Hazel Sandstorm, Scarred Manticore, Evasive Serpens, Yellow Maero, Storm-0861, OilRig)

**Attack:** APT34, also known as Earth Simnavaz, the Iranian state-sponsored hacking group, has been seen exploiting a vulnerability tracked as CVE-2024-30088 in the Windows Kernel. This flaw is being used to target organizations in the United Arab Emirates and the broader Gulf region. The attackers exploit a vulnerable web server to upload a web shell, which allows them to execute remote code and run PowerShell commands. As part of this attack, APT34 has deployed a new backdoor called 'StealHook' to facilitate data exfiltration.

## 🗡️ Attack Regions



## ⚙️ CVE

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-30088	Microsoft Windows Kernel TOCTOU Race Condition Vulnerability	Windows Kernel	❌	✅	✅

# Attack Details

## #1

The Iranian state-sponsored threat group APT34, also known as Earth Simnavaz, has recently been observed exploiting a critical vulnerability, [CVE-2024-30088](#), within the Windows Kernel as part of a highly targeted cyber espionage campaign. This operation is focused on compromising governmental and critical infrastructure networks in the United Arab Emirates (U.A.E.) and the broader Gulf region, highlighting the group's persistent focus on geopolitical espionage.

## #2

The attack chain begins with the infiltration of vulnerable web servers, where the group deploys a web shell to gain remote access and execute arbitrary commands. Once inside the target network, APT34 utilizes the ngrok remote management tool to maintain persistence and facilitate lateral movement, enabling them to reach critical assets such as the Domain Controller. By exploiting CVE-2024-30088, a Windows Kernel Elevation of Privilege vulnerability, the attackers are able to escalate privileges, securing deeper access to sensitive systems and data.

## #3

The attackers employ sophisticated password filter manipulation techniques to capture plaintext passwords, notably utilizing an exfiltration tool called StealHook, which sends stolen credentials as email attachments. By leveraging legitimate Exchange accounts for these emails, they complicate detection efforts, making their activities appear credible. This approach not only facilitates the theft of sensitive credentials but also allows the attackers to maintain a persistent foothold within the compromised network.

## #4

The group's operations employ a sophisticated blend of IIS-based malware, PowerShell scripts, and .NET-based tools, ensuring that their malicious activities remain covert by blending into normal network traffic. These tactics, combined with their exploitation of critical vulnerabilities like CVE-2024-30088, demonstrate Earth Simnavaz's ability to penetrate deeply into high-value networks with relative stealth, posing a significant threat to the region.

## #5

Given the advanced tactics employed by Earth Simnavaz and the strategic importance of their targets, it is imperative for organizations in the Gulf region to take immediate action. Timely patching and vigilance in monitoring network traffic for unusual activity will be crucial in defending against ongoing and future cyber espionage operations orchestrated by this highly capable adversary.

# Recommendations



**Apply Patch:** Install the security patch provided by Microsoft to address the CVE-2024-30088 vulnerability. This patch closes the security gap that allows attackers to exploit vulnerability.



**Network Segmentation:** Isolate sensitive systems such as Domain Controllers and servers with critical data from less secure areas of the network. This minimizes the impact of lateral movement if attackers gain initial access.



**Implement Zero Trust Architecture:** Adopt a Zero Trust security model, where access to resources is continually verified, and trust is never implicitly granted. Use identity and access management (IAM) policies to strictly control user and device permissions.



**Monitor the Registry:** Vigilantly track changes to the Notification Packages registry key located at HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Lsa. Implement auditing through Group Policy to log any unauthorized modifications to password filter DLLs. Maintain a list of trusted DLLs, and regularly check for unexpected changes



**Implement Behavioral Analysis:** Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

## Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0001</b> Initial Access	<b>TA0002</b> Execution	<b>TA0003</b> Persistence
<b>TA0004</b> Privilege Escalation	<b>TA0005</b> Defense Evasion	<b>TA0009</b> Collection	<b>TA0010</b> Exfiltration
<b>TA0011</b> Command and Control	<b>T1588</b> Obtain Capabilities	<b>T1588.006</b> Vulnerabilities	<b>T1190</b> Exploit Public-Facing Application
<b>T1059</b> Command and Scripting Interpreter	<b>T1059.001</b> PowerShell	<b>T1572</b> Protocol Tunneling	<b>T1102</b> Web Service



<b><u>T1132</u></b> Data Encoding	<b><u>T1132.001</u></b> Standard Encoding	<b><u>T1041</u></b> Exfiltration Over C2 Channel	<b><u>T1556</u></b> Modify Authentication Process
<b><u>T1556.002</u></b> Password Filter DLL	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1105</u></b> Ingress Tool Transfer	<b><u>T1078</u></b> Valid Accounts
<b><u>T1078.003</u></b> Local Accounts	<b><u>T1505</u></b> Server Software Component	<b><u>T1505.003</u></b> Web Shell	<b><u>T1048</u></b> Exfiltration Over Alternative Protocol
<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1070</u></b> Indicator Removal	<b><u>T1112</u></b> Modify Registry	<b><u>T1074</u></b> Data Staged
<b><u>T1047</u></b> Windows Management Instrumentation			

## ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	db79c39bc06e55a52741a9170d8007fa93ac712df506632d624a651345d33f91, a24303234e0cc6f403fca8943e7170c90b69976015b6a84d64a9667810023ed7, 6e4f237ef084e400b43bc18860d9c781c851012652b558f57527cf61bee1e1ef, b3257f0c0ef298363f89c7a61ab27a706e9e308c22f1820dc4f02dfa0f68d897, abfc8e9b4b02e196af83608d5aaef1771354b32c898852dff532bd8cfd2ce59d, 43c83976d9b6d19c63aef8715f7929557e93102ff0271b3539ccf2ef485a01a7, ca98a24507d62afdb65e7ad7205dfe8cd9ef7d837126a3dfc95a74af873b1dc5, 7ebbeb2a25da1b09a98e1a373c78486ed2c5a7f2a16eec63e576c99efe0c7a49, c0189edde8fa030ff4a70492ced24e325847b04dba33821cf637219d0dfff3c9, 6d8bdd3e087b266d493074569a85e1173246d1d71ee88eca94266b5802e28112, 27a0e31ae16cbc6129b4321d25515b9435c35cc2fa1fc748c6f109275bee3d6c,

TYPE	VALUE
SHA256	54e8fbae0aa7a279aaedb6d8eec0f95971397fea7fcee6c143772c8ee6e6b498, 1169d8fe861054d99b10f7a3c87e3bbbd941e585ce932e9e543a2efd701deac2, af979580849cc4619b815551842f3265b06497972c61369798135145b82f3cd8, 1d2ff65ac590c8d0dec581f6b6efbf411a2ce5927419da31d50156d8f1e3a4ff, abfc8e9b4b02e196af83608d5aaef1771354b32c898852dff532bd8cfd2ce59d, 98fb12a9625d600535df342551d30b27ed216fed14d9c6f63e8bf677cb730301, edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef, Ca98a24507d62afdb65e7ad7205dfe8cd9ef7d837126a3dfc95a74af873b1dc5

## Patch Link

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088>

## References

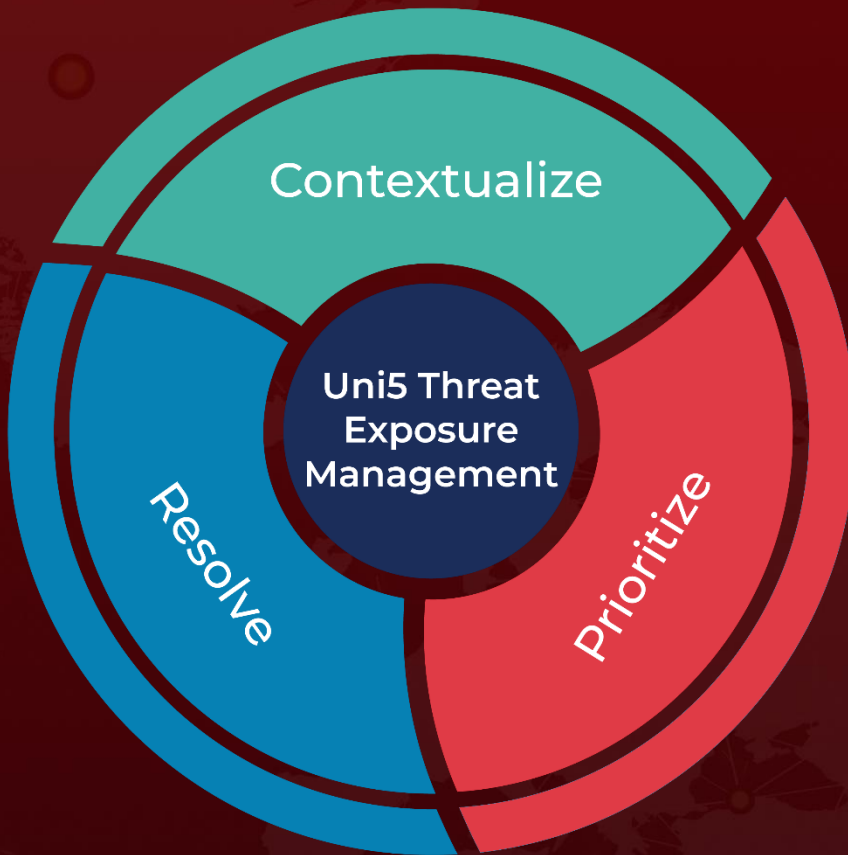
[https://www.trendmicro.com/en\\_us/research/24/j/earth-simnavaz-cyberattacks-uae-gulf-regions.html](https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks-uae-gulf-regions.html)

<https://www.hivepro.com/threat-advisory/microsofts-june-2024-patch-tuesday-addresses-49-vulnerabilities/>

# 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

**October 14, 2024 • 6:20 AM**

© 2024 All Rights are Reserved by Hive Pro



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