

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## Microsoft MSHTML Flaw the Silent Doorway for MerkSpy Malware

Date of Publication

July 3, 2024

Admiralty Code

A1

TA Number

TA2024253

# Summary

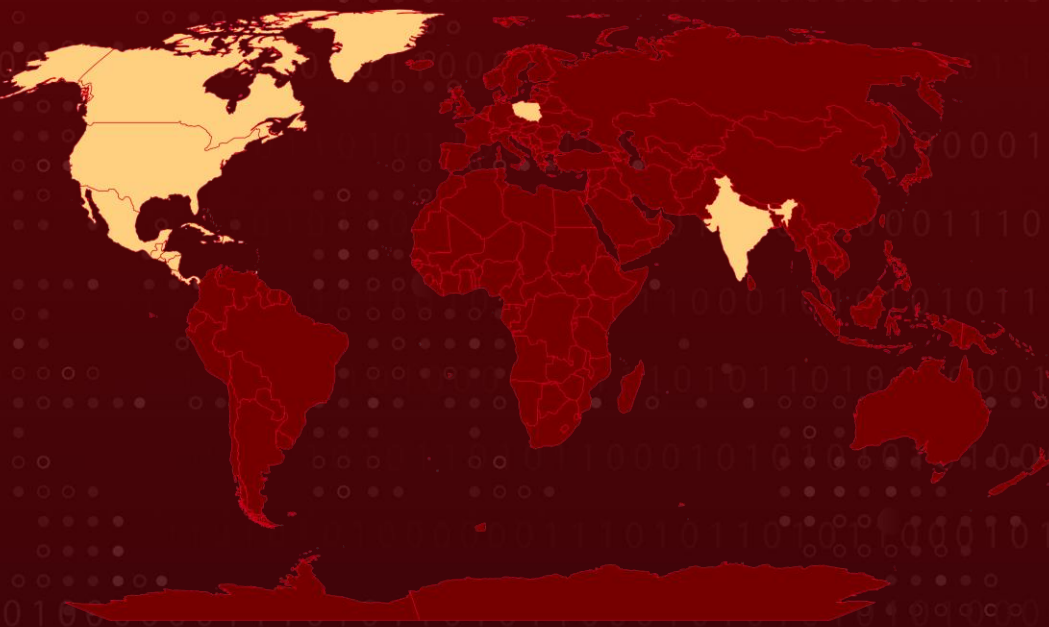
**Malware:** MerkSpy

**Attack Regions:** North America, Poland, and India

**Affected Platform:** Microsoft Windows




**Attack:** A newly discovered campaign is deploying MerkSpy, a sophisticated surveillance spyware engineered to clandestinely monitor and harvest data from a victim's computer without their awareness or consent. Unidentified threat actors are leveraging the previously patched CVE-2021-40444 security vulnerability in Microsoft MSHTML to disseminate MerkSpy.

## Attack Regions



## CVE

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Microsoft MSHTML			

# Attack Details

## #1

A new campaign has emerged, deploying MerkSpy, a surveillance spyware designed to covertly monitor and collect information from a victim's computer without their knowledge or consent. Unknown threat actors are exploiting a now-patched CVE-2021-40444 security flaw in Microsoft MSHTML to deliver MerkSpy.

## #2

This campaign primarily targets users in Canada, India, Poland, and the U.S. The initial attack vector is a deceptive Microsoft Word document masquerading as a job description for a software developer position. Opening the document triggers the exploitation of CVE-2021-40444, a remote code execution vulnerability in the MSHTML component used by Internet Explorer in Microsoft Office.

## #3

This vulnerability allows an attacker to execute arbitrary code on the victim's machine with no further user interaction required beyond opening the document. MerkSpy can record activities such as keystrokes, browsing behavior, and personal information, often transmitting this data to a third party for espionage or theft.

## #4

The spyware establishes persistence on the host by modifying the Windows Registry, ensuring it launches automatically upon system startup and exfiltrates the collected data to external servers controlled by the threat actors.

# Recommendations



**Patch and Update Systems:** Ensure that all software, especially Microsoft MSHTML and related components, are promptly patched with the latest updates to mitigate CVE-2021-40444.



**Implement Endpoint Protection:** Deploy robust endpoint protection solutions that include advanced threat detection and behavior monitoring capabilities to detect and block malicious activities associated with MerkSpy.



**Monitor Network Traffic:** Monitor network traffic for unusual or suspicious activity that may indicate communication with external servers typically used by MerkSpy for data exfiltration.



**Use Multi-Layered Security:** Implement a multi-layered security approach that includes firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions to provide comprehensive protection against advanced threats like MerkSpy.



**Monitoring and Logging:** Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.



**User Education and Awareness:** Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.



## 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>TA0006</u></b> Credential Access	<b><u>TA0007</u></b> Discovery	<b><u>TA0009</u></b> Collection
<b><u>TA0010</u></b> Exfiltration	<b><u>TA0011</u></b> Command and Control	<b><u>TA0042</u></b> Resource Development	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1048</u></b> Exfiltration Over Alternative Protocol	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1203</u></b> Exploitation for Client Execution
<b><u>T1204</u></b> User Execution	<b><u>T1204.002</u></b> Malicious File	<b><u>T1547.001</u></b> Registry Run Keys / Startup Folder	<b><u>T1547</u></b> Boot or Logon Autostart Execution
<b><u>T1543</u></b> Create or Modify System Process	<b><u>T1036</u></b> Masquerading	<b><u>T1027</u></b> Obfuscated Files or Information	<b><u>T1056</u></b> Input Capture
<b><u>T1056.001</u></b> Keylogging	<b><u>T1555</u></b> Credentials from Password Stores	<b><u>T1555.003</u></b> Credentials from Web Browsers	<b><u>T1213</u></b> Data from Information Repositories

## ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08, 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a, 0ffadb53f9624950dea0e07fcffcc31404299230735746ca43d4db05e4d708c6, dd369262074466ce937b52c0acd75abad112e395f353072ae11e3e888ac132a8, 569f6cd88806d9db9e92a579dea7a9241352d900f53ff7fe241b0006ba3f0e22, 6cdc2355cf07a240e78459dd4dd32e26210e22bf5e4a15ea08a984a5d9241067
<b>IPv4</b>	45[.]89[.]53[.]46

## ✂ Patch Link

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444>

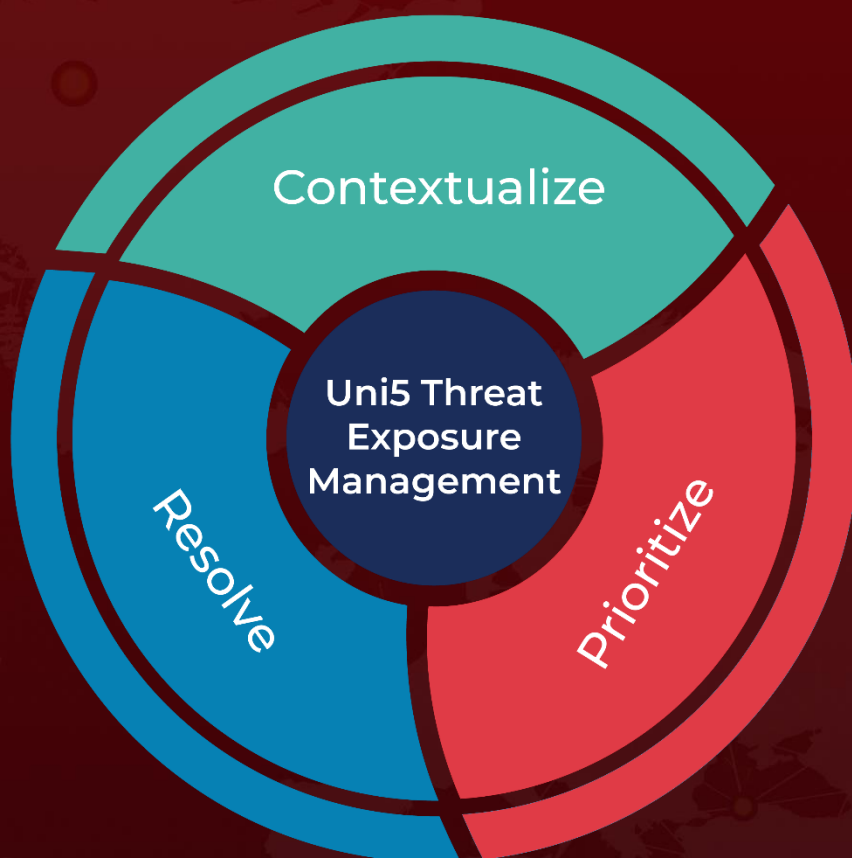
## ✂ References

<https://www.fortinet.com/blog/threat-research/merkspy-exploiting-cve-2021-40444-to-infiltrate-systems>

# 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

**July 3, 2024 • 5:30 AM**

© 2024 All Rights are Reserved by HivePro



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