Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

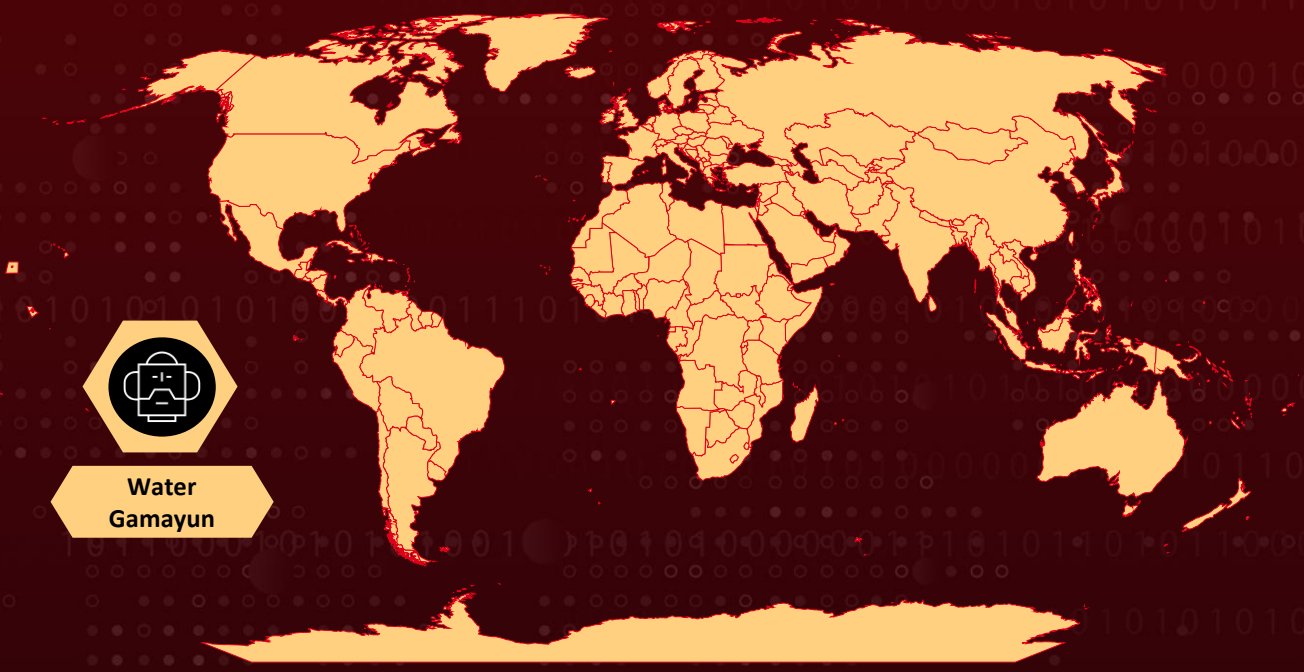
# Water Gamayun's MSC EvilTwin Attack Targets MMC Framework

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 28, 2025 | A1 | TA2025097 |

# Summary

**Attack Commenced:** April 2024
**Targeted Countries:** Worldwide
**Malware:** EncryptHub stealer, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader
**Targeted Platform:** Windows
**Threat Actor:** Water Gamayun (aka EncryptHub and Larva-208)
**Attack:** CVE-2025-26633 is a critical zero-day vulnerability in the Microsoft Management Console (MMC) framework, exploited by the Russian threat actor group Water Gamayun. This vulnerability, also known as MSC EvilTwin, allows attackers to execute malicious code by manipulating .msc files through the Multilingual User Interface Path (MUIPath). By creating deceptive file structures, attackers can trick the system into loading malicious content instead of legitimate files, leading to unauthorized access and data theft.

## Attack Regions



## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2025-26633 | MSC EvilTwin (Microsoft Management Console Security Feature Bypass Vulnerability) | Microsoft Management Console | ✓ | ✓ | ✓ |

# Attack Details

**#1**

CVE-2025-26633 is a critical zero-day vulnerability in the Microsoft Management Console (MMC), actively exploited by the Russian threat actor Water Gamayun (also known as EncryptHub or Larva-208). This vulnerability, known as MSC EvilTwin, enables attackers to bypass security features and execute malicious code by exploiting improper neutralization of user input. The attack is triggered when victims are convinced to open a malicious file or click on a malicious link, allowing attackers to gain unauthorized access and execute payloads.

**#2**

Water Gamayun uses this vulnerability to deploy various malware strains, including data stealers like Rhadamanthys and Stealc, backdoors like DarkWisp and SilentPrism, and other malicious tools such as EncryptHub stealer. The attack leverages the MSC EvilTwin technique by creating two .msc files, one legitimate and one malicious, with identical names. The malicious file is placed in a directory exploiting the Multilingual User Interface Path (MUIPath) feature, tricking the system into loading it instead of the legitimate file. This allows attackers to maintain persistence and execute further stages of their attack.

**#3**

The group also employs a PowerShell-based trojan loader that automates these techniques. Delivered through seemingly legitimate MSI files, the loader decodes and writes both clean and malicious .msc files to specific directories. Once executed, the malicious payload connects to command-and-control servers to download additional malware or exfiltrate sensitive data. The stealthy nature of this attack highlights the need for heightened awareness and proactive measures against such advanced persistent threats.

# Recommendations

**Apply Security Updates Promptly:** Ensure that all affected Windows systems receive the latest security patches provided by Microsoft. This is the most effective step to protect against exploitation of this vulnerability.

**Restrict Execution of Unsigned .msc Files:** Configure system policies to prevent the execution of unsigned or untrusted .msc files. This reduces the likelihood of malicious MMC files being executed.

**Limit User Privileges:** Adopt the principle of least privilege by granting users only the access necessary for their roles. Limiting administrative rights can minimize the impact of potential exploits.

**Strengthen Endpoint Security:** Deploy Endpoint Detection and Response (EDR) solutions to detect and prevent unauthorized code execution. Utilize Behavior-Based Threat Detection to identify suspicious actions linked to MSC EvilTwin. Ensure all security software is updated to detect EncryptHub stealer, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0004**<br>Privilege Escalation | **TA0001**<br>Initial Access | **TA0042**<br>Resource Development | **TA0002**<br>Execution |
| **TA0003**<br>Persistence | **TA0010**<br>Exfiltration | **TA0005**<br>Defense Evasion | **TA0011**<br>Command and Control |
| **T1218.014**<br>MMC | **T1218**<br>System Binary Proxy Execution | **T1543**<br>Create or Modify System Process | **T1566**<br>Phishing |
| **T1204**<br>User Execution | **T1189**<br>Drive-by Compromise | **T1059.001**<br>PowerShell | **T1036**<br>Masquerading |
| **T1068**<br>Exploitation for Privilege Escalation | **T1047**<br>Windows Management Instrumentation | **T1059**<br>Command and Scripting Interpreter | **T1041**<br>Exfiltration Over C2 Channel |
| **T1059.003**<br>Windows Command Shell | **T1222**<br>File and Directory Permissions Modification | | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
| --- | --- |
| SHA256 | 015f0fdf24a19b98447fab5fa16abf929c1cf9be33e9455ce788909dd5a8dbfe,<br>045a1cbcc99c53c092bb61d43b89a6f7308fd01d9ceaeb9a72bbf81669dcbef8,<br>0943b0f328282504c2661cd56e4bd83e3b3e5a4cce89e2e5523f83a2d535a07e,<br>0ac748baaad6017e331a8d99aae9e5449a96ba76fb7374f5d8c678ae52b7db9f,<br>1b3309c7a4c3940eff1e1ab1905641b23ea743c4f11d82107ce36fa1ec2299e9,<br>20da5e4736a91eb6aa55892d1497c724fb16767da43ccf3227db5c9647bb0793,<br>22bf8f6a408f59a1a9a1871b2a809851e0e4c0e75ca9ed14867f9bbdcf9363d2,<br>2aeb9aeca5739ea1cb5a30d284d65e36fe18f47db9e5e504063d982b9c3bc3e9,<br>3761060c509b9444bdd3d0e65d7f68e39ff5c52fa87fdc59db02c1553e21e403,<br>405d1dcdbba56bce99a308734c39ac8ca62ffb55dbd69565293a79b468e4dad1,<br>413dea8ea8cb09cd3ac49531a8e0a13f767c09f78fb77856f4668377532a64ef,<br>43eab8488dce80c1086aafdf4594b1a438347e32275abeaa8b2bb14475fb3f98,<br>47e4142fa6ab10a2d7dc0423d41f9bdbb3ced0f4fae5c58b673386d11dd8c973,<br>4e6f35ab5eb9242335bee01d6df9b50f665043f9930a630df7e170b904f52a24,<br>5357279bad530c3af89713aaf6befe19a22e438f22952aed46097590130551fa,<br>5f6dbe487af0fe7d1cf9beca7e31fcd804d6bdfe9a80308d7aeb3ed9abd9bba3,<br>60f5d8eadaba230b95339011daf4800f81e35ac721bf908f68ed8191388addcb,<br>691087ec9b50022d3e23695c0b41e2927cb4c4825a1f5fd7e2f21ae3465e8973,<br>6b99530953010dd8061a3a328c04c30653bba26439dd30a752262582b0d02933,<br>6df96984d5ba709282b6c92287262bd81f980811b58b0c03b9b421ba1e580c6b, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 725df91a9db2e077203d78b8bef95b8cf093e7d0ee2e7a4f55a30fe200c3bf8f,<br>7f8bd2d63bb95d61fcbdb22827c3a3e46655f556da769d3880c62865e6fde820,<br>86e4115111e88bbaf09fe73cfc8255a4aac64f7ffed4a3229bbc8d626566f0c8,<br>94ee2227696da3049ff67592834b4b6f98186f91e6d1cd1eeec44f24b9df754b,<br>969c7ee8709a519c4a4878b230d4ba7f81fb9563320b5983f8f1f95d4d215ece,<br>97a766db470c44347b65a0bc282582f96a47d96ed8d7946f4da33775d384033a,<br>9854322760307c04aacd78f136e4d1496950811ee2f24978915d7cd322ecb36c,<br>9b830c2979cbce45573aa21d765adda76f52db254155ae49648ef5050ceaf774,<br>9d2aaa8672d583af4c03c23127d6cac509799a49ff9293ed63628d5b710b7528,<br>9e9ca325f44eeff4087bb67052536ba565da18e70e5b29c79ed77c14c5548131,<br>ab58281273e7299f86cfadc1c8235789379543339035c5b4d80becd785bad552,<br>ad95786b2402c6a2cc36a513937a10503aff74e180ea1213cbfe40ca820d3b13,<br>af4d26b987093be6b442e655ffdafa8e1542e80f6a47a6895aa523f2f180025c,<br>b1b3d27deb35dd8c8fed75e878adae3f262475c8e8951d59e5df091562c2779b,<br>b1fa0ded2f0cc42a70b7a0c051f772cd6db76b15d50ec119307027e670998728,<br>b3ed3f2bc5334e54ca8d6020d37da0764f123fa5717638229422bd95a028097b,<br>b4f66a5e2876e04db93aae029049a07efed2d6dca05c89c393fe5aba03b949a7,<br>b7b72d141ed56c8e5a924dfa959771548883b88e84646150447f85eb97f88e62,<br>ba195a227fb76e8820d6db36cd00c89095b88faf01471fcdd9c0c7de61a63a5d,<br>bad43a1c8ba1dacf3daf82bc30a0673f9bc2675ea6cdedd34624ffc933b959f4,<br>bb563180196989dcee91417aa56d6f1bfc9320b2427536c200dffcd784774906,<br>cbb84155467087c4da2ec411463e4af379582bb742ce7009156756482868859c, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | cd301bdc07518027567a5ed242ae2075f9f0bdf73315e99d4d949280f151fefe, cedf4589428ae05d3d2dca1d1bd7fa28f6cafe54a077a6090f873053e04fd5ce, cfafc9b2d6cbc65769074bab296c5fbacc676d298f7391a3ff787307eb1cbce0, d639cd267b05b4cd420e4547dd7aa4d99fff2d070598de044c7cf0d1b99cd264, d76c25e2761210783055b43349370253d794e94ee913a2be7596b9554eacf107, db3fe436f4eeb9c20dc206af3dfdff8454460ad80ef4bab03291528e3e0754ad, e31ce5803bb68222eeac117614ddb92ed3c137bcf129f873d44960ab9d8bab33, f381a3877028f29ec7865b505b5c85ce77d4947d387d3f30071159fa991f009a, f5c97f23543e904944120ef738f300049eae85c3b0bf8b86b346572f7bc6dec1, Fcfb94820cb2abbe80bdb491c98ede8e6cfa294fa8faf9bea09a9b9ceae35bf3, 80055590cf6573c6ef381c9b834c35c1a5e7463aedbcf4b5427a903f1e588c50, 5588d1c5901d61bb09cd2fc86d523e2ccbc35a0565fd63c73b62757ac2ee51f5 |
| SHA1 | 2d91246aa4916f519e96bbb091ae18518141d7fb, 56b1fb146753add245fb21df3f63ad3eb1110c46, 631705a952626a37e87e0f66ff11ed82636d4746, 707e73fcb3ad430cd2f5f2a8d864ea95831f01b6, 86b0d17461a208a6190f7da925c8cb14cf33784e, 87c46845f57dc9ca8136b730c08b5b5916ca0ad3, a225bee48074feac53c7cb2f3929a41f7b4a71d3, d8d946a6df1649972694312e299aeff3cf2afb9b, ffb72adff6e099a9deb418c5d40abd8cf9b12c42 |
| MD5 | 011827ebdf113755102a47987b718587, 06b419c9fd1fd280d35f2b9b8ac40a75, 3c4bb1da1a85e000a3abc4ef49771b19, 6e90358d70a4a4c6d49dab693267a381, 87792cf4bd370f483a293a23c4247c50, 9a7d80b9f8afc7ec88c1e92b143a263b, 9f17d0e2a2e20f8141bf55d374c358b2, abaa46bc704842d6cc6f494c21546ae6, e59a025f9310d266190b91f5330fde8d, |

| TYPE | VALUE |
| --- | --- |
| Domains | fuckedserver[.]net, encrypthub[.]net, encrypthub[.]org, Ciphercall[.]net, cryptolabstudio[.]com, raw.githubusercontent.com, skorikjr.github[.]io, raw.githubusercontent[.]com |
| IPv4 | 82[.]115[.]223[.]182 |

## Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

## References

https://www.trendmicro.com/en_us/research/25/c/cve-2025-26633-water-gamayun.html

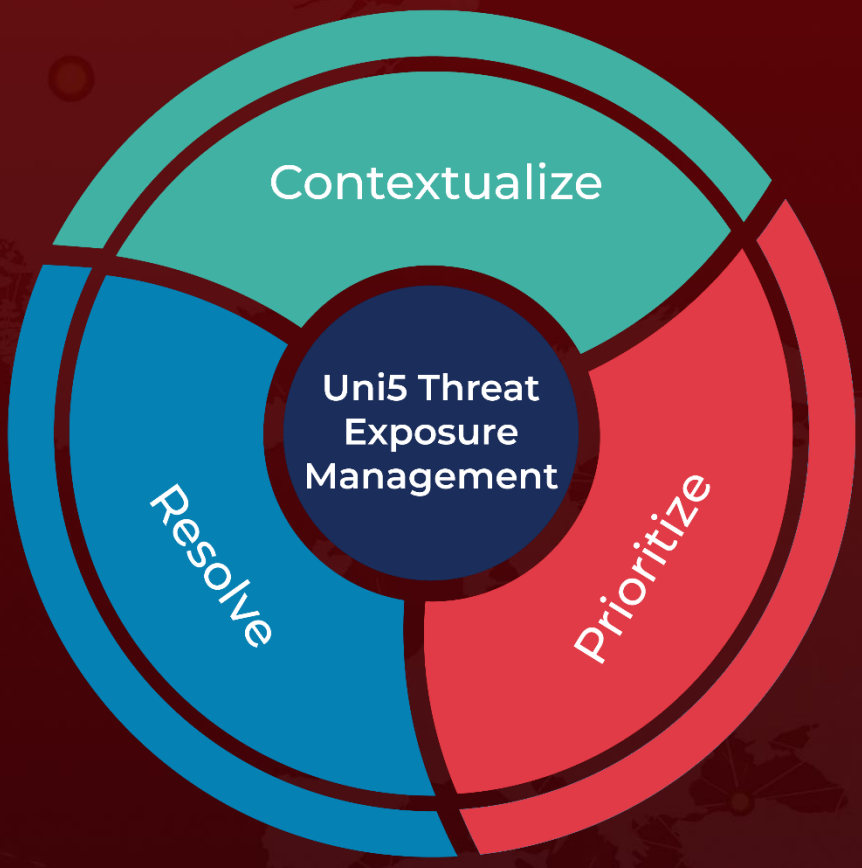
https://documents.trendmicro.com/assets/txt/IOCs_MSCEvilTwin_42J5iaVT.txt

https://hivepro.com/threat-advisory/microsofts-march-2025-patch-tuesday-fixes-active-zero-day-exploits/

# 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

**March 28, 2025 • 2:30 AM**



More at www.hivepro.com