Hive Pro

Threat Level

Amber

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

# Gold Melody Is Weaponizing Leaked ASP.NET Machine Keys

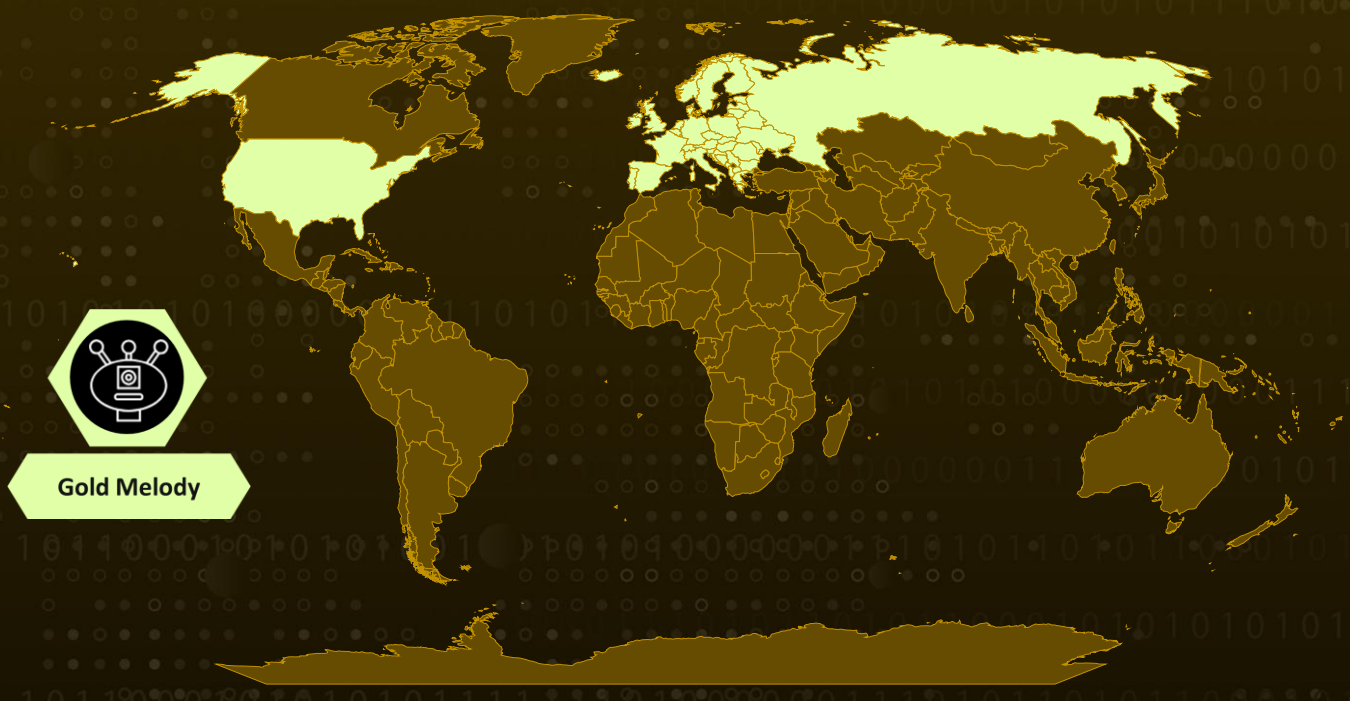

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| July 11, 2025 | A2 | TA2025215 |

# Summary

**Attack Commenced:** October 2024
**Targeted Regions:** Europe and the U.S.
**Targeted Industries:** Financial Services, Manufacturing, Retail, Technology, Transportation, Logistics
**Threat Actor:** Gold Melody (aka Prophet Spider, UNC961)

**Attack:** An Initial Access Broker group known as Gold Melody has emerged at the center of a high-impact campaign targeting ASP.NET applications through leaked machine keys. By quietly exploiting overlooked configuration secrets, the group has been breaching enterprise networks and selling access within underground markets. This growing wave of attacks underscores how minor security oversights can open the door to large-scale compromises, leaving organizations vulnerable to stealthy in-memory exploits and persistent backdoors.

## Attack Regions



# Attack Details

**#1** The Initial Access Broker (IAB) known as Gold Melody, also referred to as Prophet Spider and UNC961, has been circumstantially tied to a campaign exploiting leaked ASP.NET machine keys to infiltrate corporate networks and sell that access to other threat actors. This activity is currently being tracked under the temporary moniker TGR-CRI-0045.

**#2** Notably, one of the tools used in these intrusions has also been associated with another IAB operation by **ToyMaker**. While opportunistic in its targeting, Gold Melody has primarily struck organizations in Europe and the United States. At the center of this operation are ASP.NET machine keys, which secure authentication cookies and ViewState data in web applications.

**#3** Using automated tools, Gold Melody tested these leaked keys against thousands of internet-facing ASP.NET and IIS applications to identify vulnerable systems. Once a valid key was discovered, attackers exploited it to forge authentication cookies, granting themselves administrator-level access to the application. This access enabled them to interact with backend infrastructure, exfiltrate sensitive data, and establish lateral movement within compromised networks.

**#4** By leveraging compromised machine keys, Gold Melody bypassed ViewState Message Authentication Code (MAC) validation. Crafted payloads embedded within ViewState data were then deserialized by vulnerable servers, executing arbitrary code within the application process. These in-memory attacks left minimal forensic evidence, complicating detection and response efforts.

**#5** This campaign represents one of the first extensive, systematic operations where leaked ASP.NET machine keys have been weaponized at scale for initial access brokering, marking a significant evolution in how overlooked configuration secrets are being abused in modern cybercrime.

# Recommendations

**Inventory and Audit Exposed Machine Keys:** Organizations should conduct a comprehensive audit to identify any ASP.NET machine keys stored in public code repositories, cloud storage buckets, or misconfigured servers. Regularly scanning public repositories associated with enterprise developers and contractors can prevent inadvertent leakage.

**Revoke and Regenerate Machine Keys:** If any keys are found to have been exposed or compromised, administrators must immediately revoke and regenerate those keys. Updating application configurations and re-signing authentication cookies and ViewState data ensures that previously compromised keys cannot be used for forging tokens.

**Monitor for Abnormal Authentication Activity:** Continuously monitor authentication logs for unusual patterns such as unexplained administrative logins, changes to ViewState MAC settings, or excessive authentication attempts. Pay close attention to access attempts originating from unfamiliar geographies or infrastructure.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence |
| **TA0004** Privilege Escalation | **TA0005** Defense Evasion | **TA0007** Discovery | **TA0011** Command and Control |
| **T1036.005** Match Legitimate Resource Name or Location | **T1036.010** Masquerade Account Name | **T1046** Network Service Discovery | **T1059** Command and Scripting Interpreter |
| **T1059.003** Windows Command Shell | **T1071** Application Layer Protocol | **T1071.001** Web Protocols | **T1105** Ingress Tool Transfer |
| **T1134** Access Token Manipulation | **T1134.001** Token Impersonation/Theft | **T1136** Create Account | **T1136.001** Local Account |

| | | | |
|---|---|---|---|
| **T1190** Exploit Public-Facing Application | **T1217** Browser Information Discovery | **T1505** Server Software Component | **T1505.003** Web Shell |
| **T1572** Protocol Tunneling | **T1587** Develop Capabilities | **T1587.001** Malware | **T1036** Masquerading |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| URL | hxxp[:]//195[.]123[.]240[.]233[:]443/atm |
| SHA256 | 106506ebc7156be116fe5d2a4d662917ddbbfb286007b6ee7a2b01c9536b1ee4, 87bd7e24af5f10fe1e01cfa640ce26e9160b0e0e13488d7ee655e83118d16697, 55656f7b2817087183ceedeb4d9b78d3abee02409666bffbe180d6ea87ee20fb, 18a90b3702776b23f87738b26002e013301f60d9801d83985a57664b133cadd1, d5d0772cb90d54ac3e3093c1ea9fcd7b878663f7ddd1f96efea0725ce47d46d5, b3c085672ac34f1b738879096af5fcd748953116e319367e6e371034366eaeca, d4bfaf3fd3d3b670f585114b4619aaf9b10173c5b1e92d42be0611b6a9b1eff2, c1f66cadc1941b566e2edad0d1f288c93bf060eef383c79638306638b6cefdf8, 52a72f899991506d2b1df958dd8736f7baa26592d664b771c3c3dbaef8d3114a, d3767be11d9b211e74645bf434c9a5974b421cb96ec40d856f4b232a5ef9e56d, f368ec59fb970cc23f955f127016594e2c72de168c776ae8a3f9c21681860e9c |
| IPv4 | 67[.]43[.]234[.]96, 213[.]252[.]232[.]237, 98[.]159[.]108[.]69, 190[.]211[.]254[.]95, 109[.]176[.]229[.]89, 169[.]150[.]198[.]91, |

| TYPE | VALUE |
| --- | --- |
| IPv4 | 194[.]5[.]82[.]11,<br>138[.]199[.]21[.]243,<br>194[.]114[.]136[.]95,<br>195[.]123[.]240[.]233 |

## References


https://unit42.paloaltonetworks.com/initial-access-broker-exploits-leaked-machine-keys/

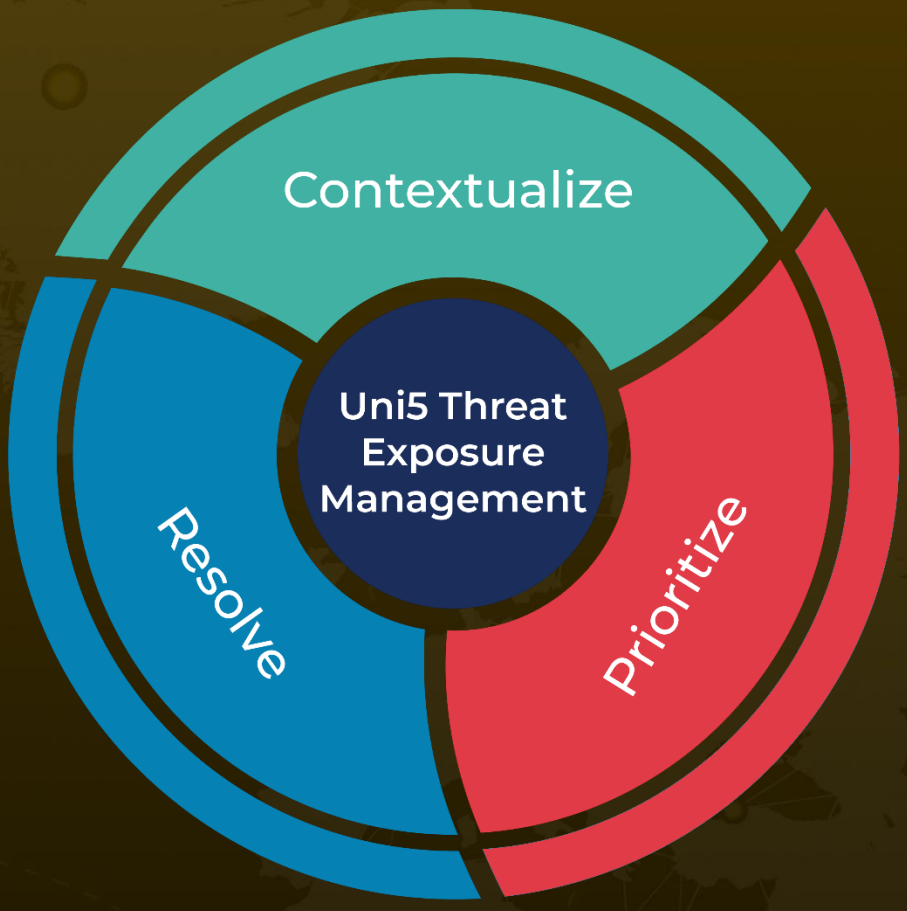
https://www.microsoft.com/en-us/security/blog/2025/02/06/code-injection-attacks-using-publicly-disclosed-asp-net-machine-keys/

https://hivepro.com/threat-advisory/toymaker-unveiling-the-role-of-initial-access-brokers-in-ransomware-attacks/

# 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 11, 2025 • 6:30 AM**



More at www.hivepro.com