Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

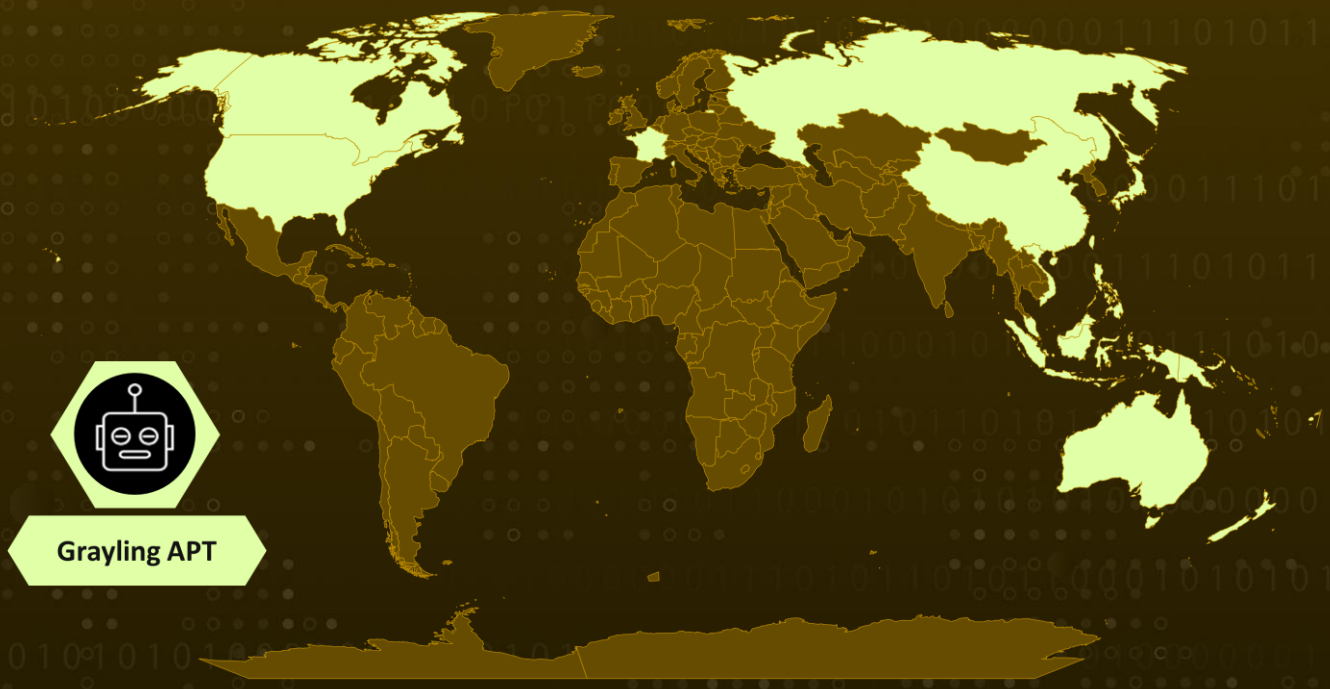
Grayling APT Emerges as a Silent Threat Targeting Taiwan

Date of Publication	Admiralty Code	TA Number
October 11, 2023	A1	TA2023408

Summary

Attack Began: February 2023
Actor Name: Grayling APT
Target Region: Taiwan, Vietnam, U.S, and Asia-Pacific region
Target Sectors: Government, Manufacturing, IT, and Biomedical

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2019-0803	Microsoft Win32k Privilege Escalation Vulnerability	Microsoft Win32k	✓	✓	✓

Actor Details

#1 During a strategic initiative spanning from February to May 2023, the Advanced Persistent Threat (APT) group identified as Grayling systematically targeted a government entity in the Asia-Pacific region, as well as institutions in Taiwan, the United States, and Vietnam, indicating a primary focus on intelligence acquisition rather than for financial reasons.

#2 Grayling, an enigmatic threat actor previously undocumented, has been associated with a series of attacks directed at organizations within the manufacturing, IT, and biomedical sectors in Taiwan. The initial intrusion into victim environments reportedly exploited public-facing infrastructure, utilizing web shells to establish persistent access.

#3 The distinguishing feature of Grayling APT's operations lies in its use of a unique Dynamic Link Library (DLL) sideloading technique through the exported API SbieDll_Hook, facilitated by a custom decryptor for deploying payloads. DLL sideloading serves as a mechanism for loading diverse payloads and executing various post-exploitation tools, such as Cobalt Strike, NetSpy, Mimikatz, and the Havoc framework.

#4 Moreover, Grayling APT demonstrated an exploit leveraging CVE-2019-0803, a privilege escalation vulnerability in Windows. This flaw is triggered when the Win32k component inadequately handles objects in memory, leading to process termination and facilitating Active Directory discovery.

#5 Grayling's tactics have also included terminating all processes enumerated in a file named processlist.txt. The proficient utilization of both proprietary and publicly available tools has become a hallmark of contemporary APTs, enabling them to circumvent security measures, remain undetected, and hinder attribution.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Grayling APT	Unknown **MOTIVE** Information theft and espionage	Taiwan, Vietnam, U.S, and Asia-Pacific region	Government, Manufacturing, IT, and Biomedical

Recommendations

Patch Management: Regularly update and patch software and systems to address known vulnerabilities, especially those exploited by APT groups like Grayling. Prioritize critical patches to prevent exploitation.

Network Security: Enhance network security measures, including firewalls and intrusion detection/prevention systems, to detect and block unauthorized access attempts. Monitor network traffic for anomalous patterns and behaviors indicative of APT activities.

Enable Audit Logging: Activate audit logging for DLL loading events on Windows endpoints. This allows for the collection of detailed information about DLL loads, helping security teams identify anomalous behavior.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**T1070** Indicator Removal	**T1083** File and Directory Discovery
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1543** Create or Modify System Process	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1068** Exploitation for Privilege Escalation	**T1055** Process Injection	**T1562** Impair Defenses

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	d3ktcnc1w6pd1f.cloudfront[.]net
IPv4	172.245.92[.]207, 3.0.93[.]185

TYPE	VALUE
URLs	hxxp://45.148.120[.]23:91/version[.]dll, hxxp://45.148.120[.]23:91/vmtools[.]exe
SHA256	da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9, 79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17, bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec, c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3, 667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c, 87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8, 90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0, 8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2, d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c, 4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba, 9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739, f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b, 525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9, 23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae, 6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50, 5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581, 12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746, ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f, c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e, 245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa, 4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9,

TYPE	VALUE
SHA256	e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3, f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31, 971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f, f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0, c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5, af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889, 1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce, 7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f, 30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6, 74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87, 752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea, 6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814, 803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721, 7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2, a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe, de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c, 1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91, ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf, 1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9, dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548, d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29, b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba,

TYPE	VALUE
SHA256	6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068, 3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b, 5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

Patch Link

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803

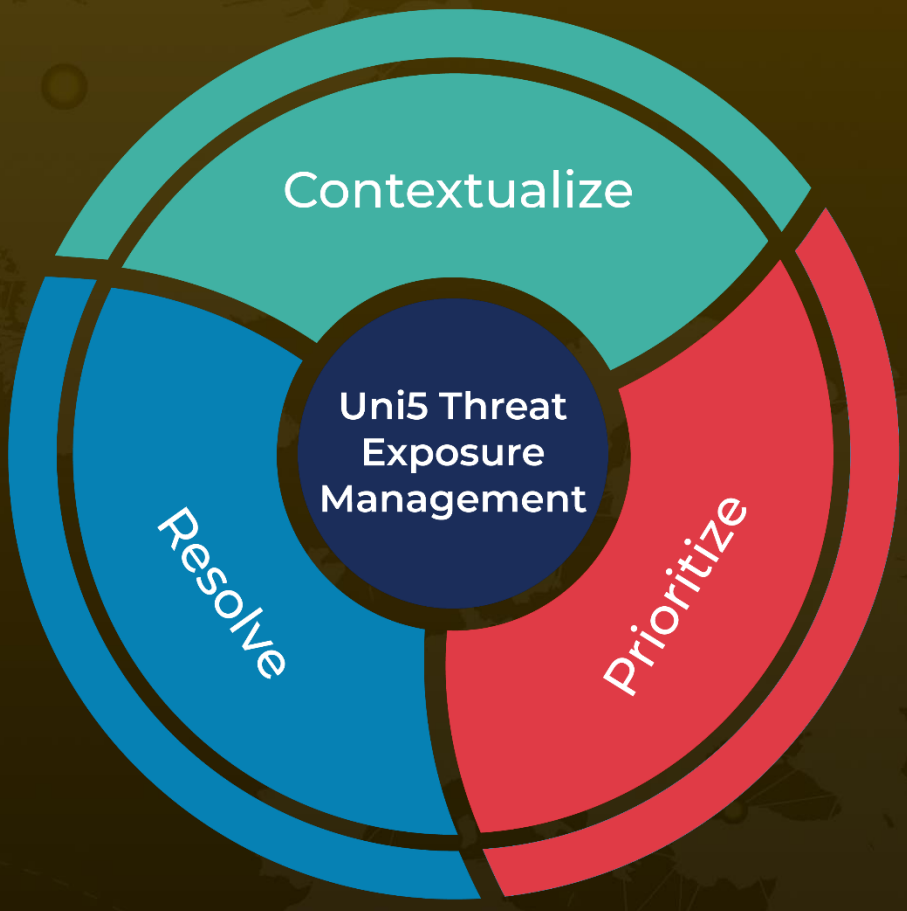
References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-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

October 11, 2023 . 5:00 AM

More at www.hivepro.com